User Guide

MEG5000

Modular Edge Gateway for IoT

Control Card + Expansion Card 1 + Expansion Card 2

robustOS

Guangzhou Robustel Co., Ltd.
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel MEG5000, including introduction, installation, configuration and operation.

Trademarks and Permissions

robustel、robustOS are trademarks of Guangzhou Robustel Co., Ltd.. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

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

Technical Support

Tel: +86-20-82321505
Email: support@robustel.com
Web: www.robustel.com

Important Notice

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

Safety Precautions

General

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

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

Using the Gateway in Vehicle

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

Protecting Your Gateway

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

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

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EU	The European RoHS2.0 2011/65/EU Directive was issued by the European parliament and the European Council on 1 July 2011 on the restriction of the use of certain Hazardous substances in electrical and electronic equipment.
	On June 4, 2015, the Official Journal of the European Union published the RoHS2.0 Amendment Directive (EU) In 2015/863, four phthalates (DEHP, BBP, DBP, DIBP) were officially included in the list of restricted substances in Appendix II of RoHS 2.0 (2011/65/EU). From July 22, 2019, all electronic and electrical products exported to Europe (except medical and monitoring equipment) must meet this restriction; from July 22, 2021, medical equipment and monitoring equipment will also be included in the scope of control.
2012/19/EU	The European WEEE 2012/19/EU Directive was issued by the European parliament and the European Council on 24 July 2012 on waste electrical and electronic equipment.
2013/56/EU	The European 2013/56/EU Directive is a battery Directive which published in the EU official gazette on 10 December 2013. The button battery used in this product conforms to the standard of 2013/56/EU directive.

Table 2: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	o	o	o	o	o	o
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o

o:

Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.

X:

Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.

Document History

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

Date	Firmware Version	Document Version	Change Description
26 Jan.,2018	1.0.0	v.1.0.0	Initial release
22 May., 2018	1.0.0	v.1.0.1	Added frequency bands for AU region.
29 Jun., 2018	1.0.0	v.1.0.2	Revised the company name.
12 Dec., 2018	1.0.0	v.1.0.3	• Revised the operating environment. • Revised the input current. • Revised the EMC. • Revised the specifications of Led indicators. • Revised the Channel • Revised the MAC address description of ACL • Revised the delay range of DIDO • Revised the defaults of high level and low level width of DIDO • Revised the input range of the level pulse width in DIDO • Delete the support for Robustlink of serial port • Added description of baud rate in the serial port • Added the description of flow control in the serial port • Delete the description of Robustlink in the serial port protocol • Delete the switch of enable NAT Traversal in the IPsec page • Added support for AES192 and DHgroup • Added the upload of the CA certificate on the web page • Added the serial port selection on the GPS page • Revised the antenna interface description of Wifi on the specifications • Revised the serial port type • Delete the uplink and downlink rates of the cellular network module in specification • Revised the description of firewall whitelist • Revised the description of firewall filter rule • Revised the description of IPsec • Revised the description of OpenVPN • Revised the description of GRE
19 Dec., 2018	1.0.0	v.1.0.4	Revised the description of approvals
30 Jan., 2019	1.0.0	v.1.0.5	Revised the Certifications

			Revised the Frequency bands of Wifi
18 Sep., 2019	1.0.0	v.1.0.6	• Revised the Regulatory and Type Approval Information • Revised the Approvals
Dec. 25, 2021	1.0.0	v.1.0.7	1. Revised the company name 2. Revised *Regulatory and Type Approval Information* 3. Revised *Disclaimer*

Contents

Chapter 1 Product Overview

1.1 Key Features

MEG5000, Robustel Modular Edge Gateway for Internet of Things (IoT), is a most configurable and manageable cellular gateway. The MEG5000 features three scalable cards supporting various interfaces to meet changing demands for industrial IoT applications. It is developed to provide application of calculation, and performs real-time data analysis and intelligent processing at the edge of sensor, which is more effective and secure. With quick-to-deploy and easy-to-customize, the MEG5000 gateway can be tailored to your industrial needs.

MEG5000 is a powerful gateway developed from RobustOS, a Robustel self-developed and Linux-based operating system which is designed to be used in Robustel devices. The RobustOS includes basic networking features and protocols providing customers with a very good user experience. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C, Python or Java. It also provides rich Apps to meet fragmented IoT market demands.

- Main control card + expansion card*2
- Flexible interfaces supporting numerous industrial applications
- High performance, high reliability and high throughput for data processing
- Quick customization meeting rapid market promotion
- Custom development based on integrated Linux environment, and providing edge computing power
- Embedded mSATA SSD providing data logging
- Real-time running temperature
- RobustOS + SDK + App
- Support IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Support WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- Support dual SIM card switching backup
- WiFi supports 2.4 GHz/5 GHz software switching and supports Captive Portal function
- Support SMS, Email, DI/DO, SNMP Trap and RobustLink event alarms
- Support Modbus RTU to TCP、Modbus Master

- Support DHCP server
- Support IP Pass-through
- Support RobustVPN cloud platform, providing simple and secure remote access for industrial equipment such as PLC
- Robust industrial design (Wide input voltage, desktop or wall mounting or DIN rail mounting)

1.2 Package Contents

Before installing your MEG5000, verify the kit contents as following.

Note: The following pictures are for illustration purposes only, not based on their actual sizes.

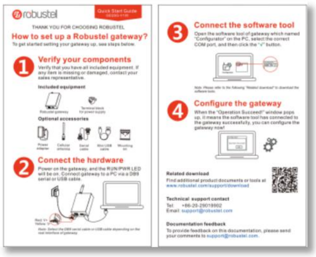
- 1 x Robustel MEG5000 Modular Edge Gateway for IoT

- 1 x 3-pin 3.5 mm female terminal block with lock for power supply

- 1 x 9-pin 3.5 mm female terminal block for DI/DO connections

- 1 x 2-pin 3.5 mm female terminal block for CAN and serial ports

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



Quick Start Guide

THANK YOU FOR CHOOSING ROBUSTEL

How to set up a Robustel gateway?

To get started setting your gateway up, see steps below.

1 Verify your components

Verify that you have all included equipment. If any item is missing or damaged, contact your sales representative.

Included equipment

Optional accessories

2 Connect the hardware

Power on the gateway, and the RUN/PWR LED will be on. Connect gateway to a PC via a DB9 serial or USB cable.

Note: Select the DB9 serial cable or USB cable depending on the real interface of gateway.

3 Connect the software tool

Open the software tool of gateway which named "Configurator" on the PC, select the correct COM port, and then click the "√" button.

Note: Please refer to the following "Related download" to download the software tools.

4 Configure the gateway

When the "Operation Succeed!" window pops up, it means the software tool has connected to the gateway successfully, you can configure the gateway now!

Related download

Find additional product documents or tools at www.robustel.com/support/download

Technical support contact

Tel: +86-20-29019902

Email: support@robustel.com

Documentation feedback

To provide feedback on this documentation, please send your comments to support@robustel.com.

Note: If any of the above items is missing or damaged, please contact your Robustel sales representative.

Optional Accessories (sold separately)

- 3G/4G SMA cellular antenna (stubby/magnet optional)

Stubby antenna

Magnet antenna

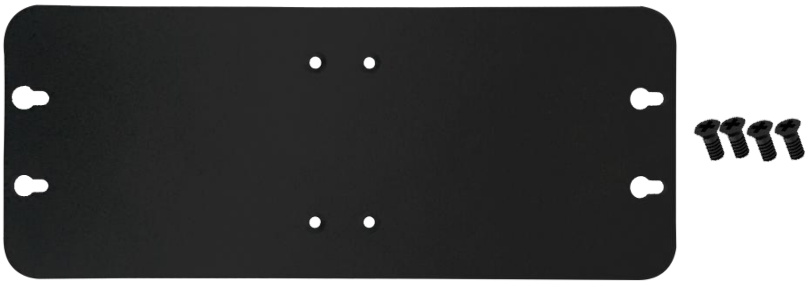
- RP-SMA WiFi antenna (stubby/magnet optional)

Stubby antenna

Magnet antenna

- GPS antenna

- Wall mounting kit



- 35 mm DIN rail mounting kit

- L-type screwdriver

- Ethernet cable

- RS-232 serial cable (DB9 male to DB9 female)

- AC/DC power adapter (24V DC, 1.5 A; EU/US/UK/AU plug optional)

1.3 Specifications

Cellular Interface

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA, female
- SIM slot: 2 (3.0 V & 1.8 V)
- Standards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE

Ethernet Interface

- Number of ports: 1 x 10/100/1000 Mbps WAN (ETH0) + 8 x 10/100 Mbps LAN (ETH1~ETH8)
- Magnet isolation protection: 1.5 KV

WiFi Interface

- Number of antenna interfaces: Support up to 4 antennas (WiFi1 + WiFi2 + WiFi3 + WiFi4)
- Connector: RP-SMA, male
- Standards: 802.11a/b/g/n/ac, supporting AP and Client modes
- Frequency bands: 2.4 GHz
5 GHz
- Security: Open, WEP, WPA, WPA2
- Encryption: AES, TKIP, WEP64, WEP128
- Data speed: Up to 1300 Mbps

GPS/GLONASS Interface (Optional)

- Number of antennas: 1 x GPS/GLONASS
- Connector: SMA female with 50 ohms impedance
- Acquisition sensitivity: GPS: greater than -148 dBm
  GLONASS: greater than -145 dBm
  Navigation sensitivity: GPS: greater than -163 dBm
  GLONASS: greater than -157 dBm
  Tracking sensitivity: GPS: greater than -165 dBm
  GLONASS: greater than -161 dBm
- Horizontal position accuracy: GPS: 2.5 m
  GLONASS: 2.6 m
- Protocol: NMEA-0183 v4.10

Serial Interface

- Number of ports: 2 x RS-232 + 1 x RS-485 + 1 x CAN
- Connector: DB9 female socket
- Baud rate: 300 bps to 115200 bps
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)
- CAN: Data+ (H), Data- (L)

Digital Input / Digital Output

- Number of ports: 2 x DI (dry/wet) + 2 x DO (on/off)
- Connector: 9-pin 3.5 mm female socket
- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: “V+” +5V DC (DI), 30V DC (DO)
- Absolute maximum ADC: 300 mA

Others

- 1 x RST button
- LED indicators - 1 x RUN(Main control card), 1 x RUN(Expansion Card 2), 1 x MODEM, 1 x USR, 3 x RSSI
  1 x Activity indicator + 1 x Link up indicator for each Ethernet port

Software (Basic features of RobustOS)

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, HTTPs, DNS, ARP, BGP, RIP, OSPF, NTP, SMTP, Telnet, VLAN, SSH2, DDNS, etc.
- VPN tunnel: IPsec, OpenVPN, GRE
- Firewall: DMZ, anti-DoS, Filtering (IP/Domain name/MAC address), Port Mapping, Access Control
- Management: Web, CLI, SMS
- Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU Gateway

App Center (Available Apps for RobustOS)

- Apps*: L2TP, PPTP, DMVPN, RobustVPN, VRRP, QoS, Captive Portal, WLAN Multi AP, SNMP, Language, RobustLink

Power Supply and Consumption

- Connector: 3-pin 3.5 mm female socket with lock
- Input voltage: 12 to 60V DC
- Input current: 12V@3A
  24V@1.5A

Physical Characteristics

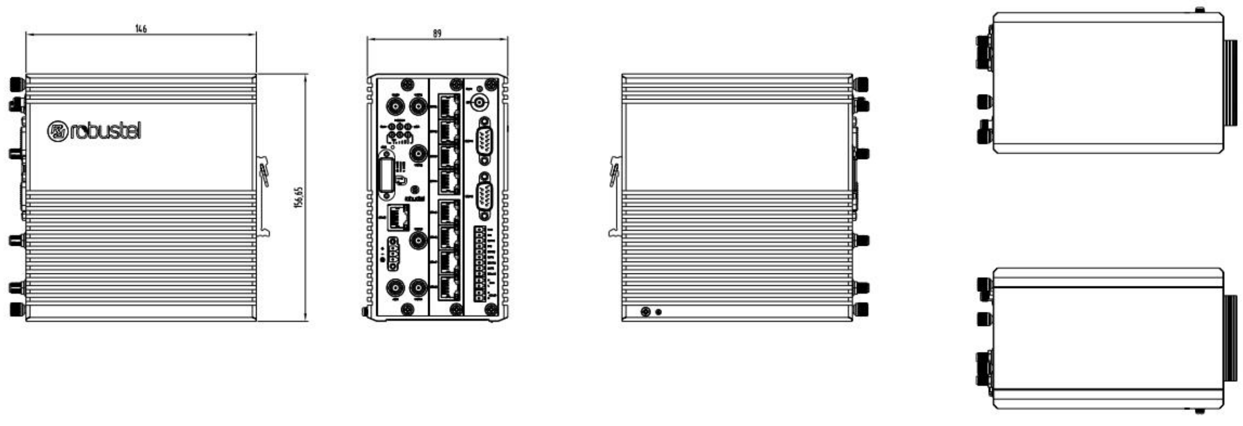
- Ingress protection: IP30
- Housing & Weight: Metal, 1600 g
- Dimensions: 157 x 145 x 89 mm
- Installations: Desktop, wall mounting and 35 mm DIN rail mounting
-

Approvals

- Environmental: RoHS2.0, WEEE

Request on demand. For more Apps please visit www.robustel.com.

1.4 Dimensions



Front View Side View Rear View Top&Bottom View

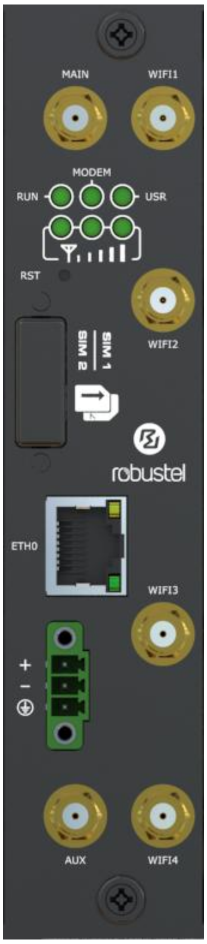
1.5 Ordering Information

Model	MEG5000-4L	MEG5000-NU
Gateway Type	LTE Gateway	--
Antenna Number	2	--
Air Interface	GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE	--
Frequency Bands 4G*	AU: B1/B2/B3/B4/B5/B7/B8/B28, B40 EU: B1/B3/B7/B8/B20/B28/B31, B38/B40 US: B2/B4/B5/B13/B17/B25, B41 JP: B1/B3/B8/B9/B18/B19/B21/B28, B41 CN: B1/B3, B38/B39/B40/B41	--
3G	WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+: B1/B2/B5/B6/B8/B9/B19 TD-SCDMA: B34/B39 CDMA (CDMA 1X/EVDO): R0/A BC0/BC1/BC10	--
2G	850/900/1800/1900 MHz	--
Operating Environment	-40 to +65 °C/ -10-+65 °C （with WIFI） 5 to 95% RH	-40 to +65 °C -10-+65 °C （with WIFI） 5 to 95% RH

**For more information about 4G frequency bands in different countries, please contact your Robustel sales representative.*

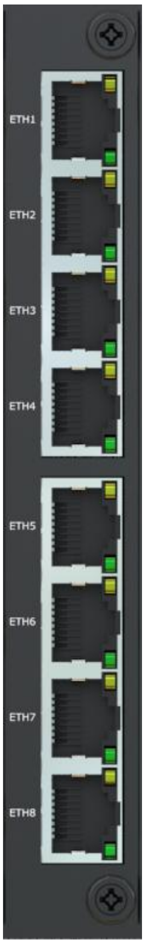
Chapter 2 Hardware Installation

2.1 Plug-in Cards



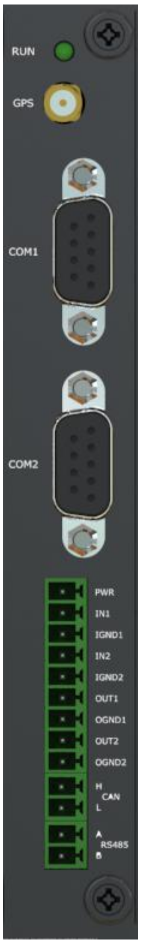
Main Control Card

- 2 x cellular SMA antenna
- 4 x WiFi antenna
- 6 x LED indicator
- 2 x SIM slot
- 1 x Gigabit WAN port/ Gigabit Fiber
- 1 x power interface



Expansion Card 1

- 8 x Megabyte LAN Ethernet
- 1 x mSATA SSD

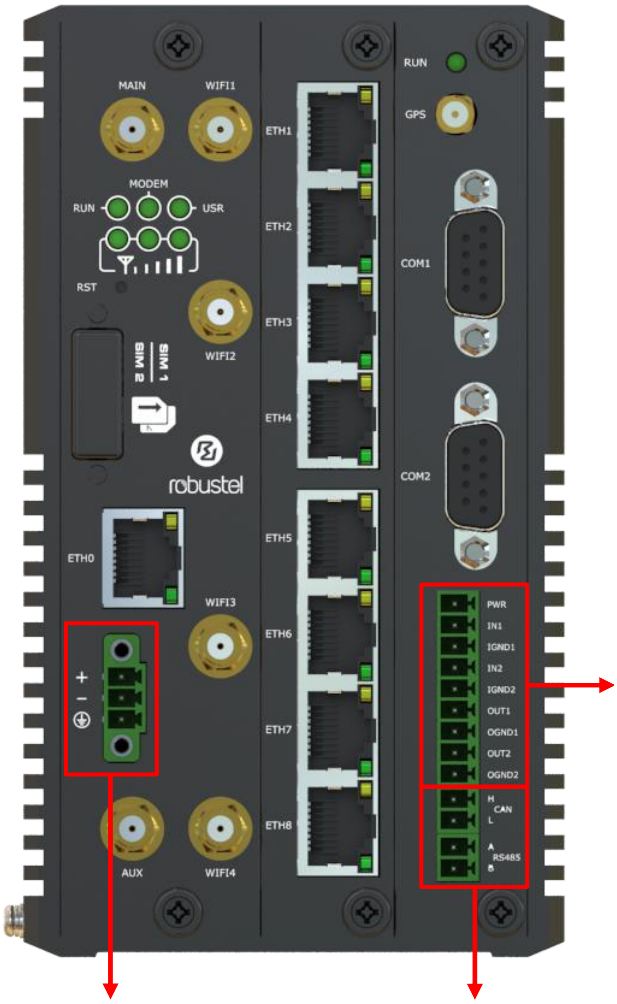


Expansion Card 2

- 1 x RUN LED indicator for card running status
- 1 x GPS antenna
- 2 x RS-232
- 2 x Digital Input
- 2 x Digital Output
- 1 x CAN
- 1 x RS-485

2.2 PIN Assignment

The MEG5000 has been designed to be placed on a desktop. Below is the front view of the MEG5000.

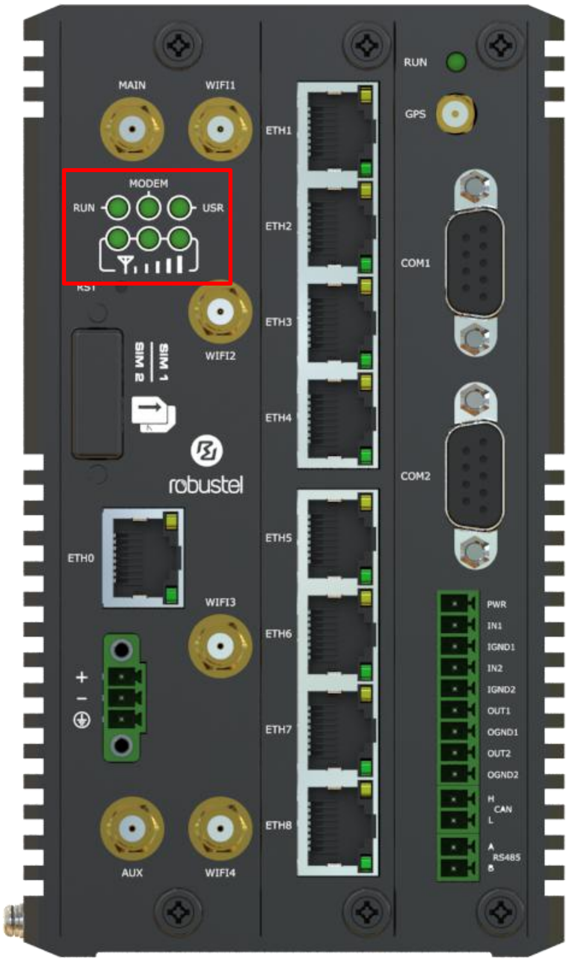


PIN	DI/DO	Direction
1	--	--
2	IN1	Gateway ← Device
3	IGND1	--
4	IN2	Gateway ← Device
5	IGND2	--
6	OUT1	Gateway → Device

PIN	Polarity
14	Positive
15	DGND
16	PGND

PIN	CAN	RS-485	Direction
10	H	--	--
11	L	--	--
12	--	Data+(A)	Gateway ↔ Device
13	--	Data- (B)	Gateway ↔ Device

2.3 LED Indicators

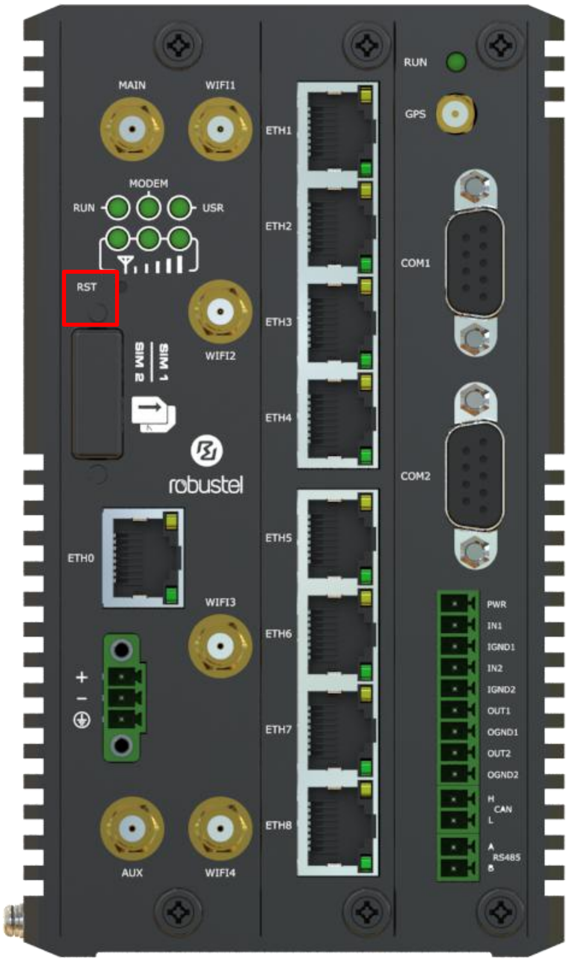


Name	Color	Status	Description
RUN	Green	On, fast blinking (250 mSec blink time)	Gateway is powered on (System is initializing)
		On, blinking (500 mSec blink time)	Gateway starts operating
		Off	Gateway is powered off
MODEM	Green	On, solid	Link connection is working
		Off	Link connection is not working
USR-SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used
USR-NET	Green	On, solid	Network is joined successfully and worked in an optimum one
		On, blinking	Network is joined successfully but worked in a lower-level than standard
		Off	Network is not joined or joining
USR-WiFi	Green	On, solid	WiFi is enabled and working properly
		On, blinking	Data is sent and received via WiFi port.
		Off	WiFi is disabled or not working properly

USR-OpenVPN	Green	On, solid	OpenVPN connection is established
		Off	OpenVPN connection is not established
USR-IPsec	Green	On, solid	IPsec connection is established
		Off	IPsec connection is not established
●●●	Green	On, 3 solid lights	High Signal strength (21-31) is available
		On, 2 solid lights	Medium Signal strength (11-20) is available
		On, 1 solid light	Low Signal strength (1-10) is available
		Off	No signal

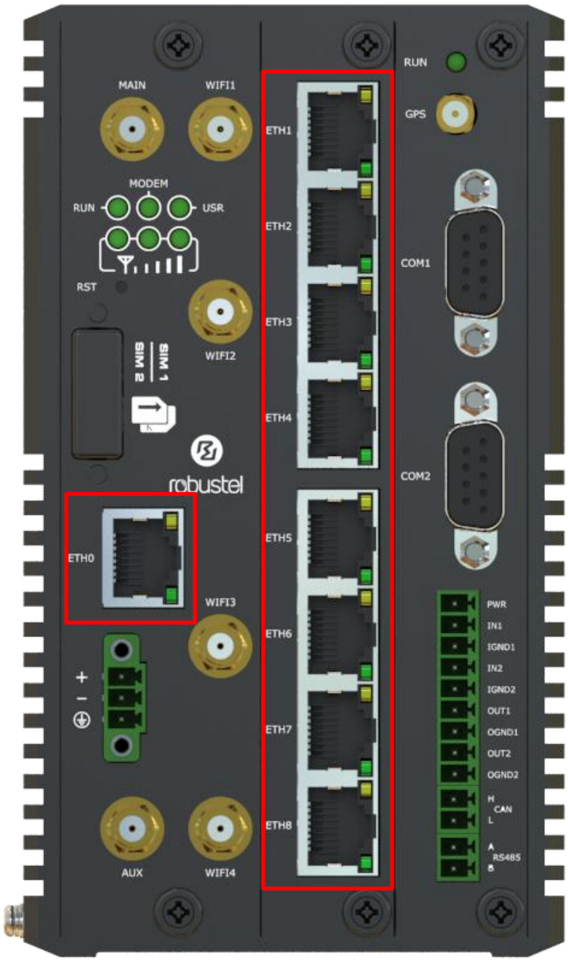
Note: You can choose the display type of USR LED. For more details, please refer to **3.29 Service > Advanced**.

2.4 Reset Button



Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 3 seconds after powering up the gateway, press and hold the RST button until all six LEDs start blinking one by one, and release the button to return the gateway to factory defaults.

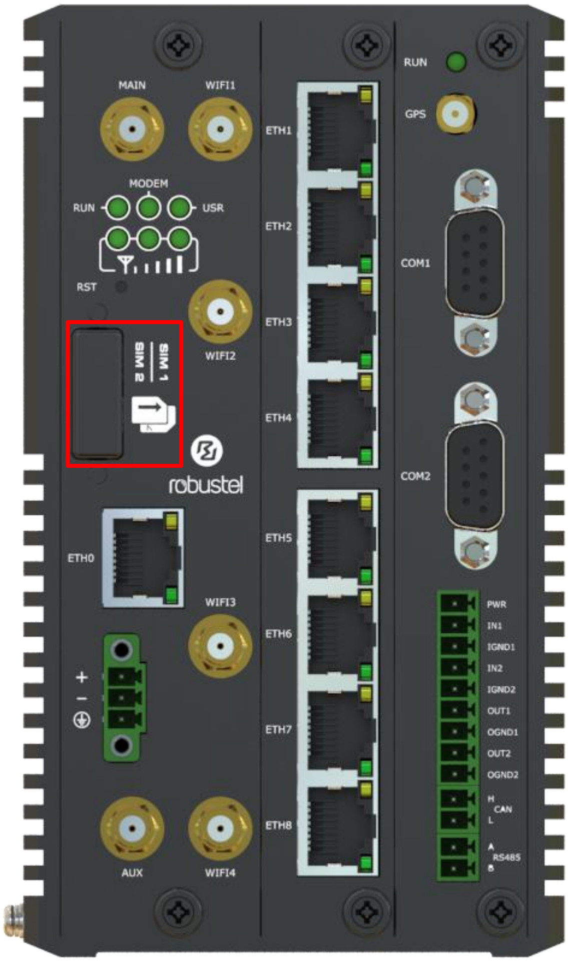
2.5 Ethernet Port

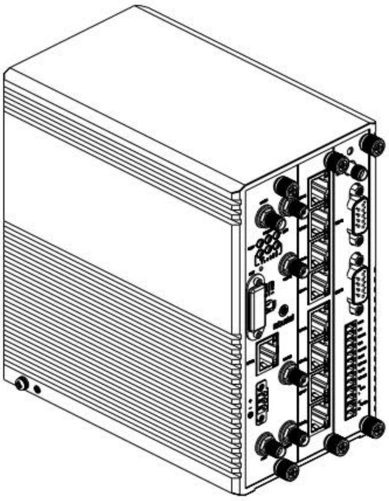


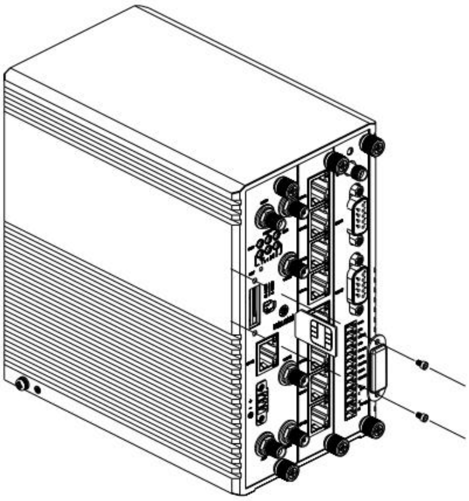
There are nine Ethernet ports on MEG5000, including one WAN port and eight LAN ports. Each Ethernet port has two LED indicators. The yellow one is an Activity indicator, while the green one is a Link up indicator. For details about status, see the table below.

Indicator	Status	Description
Activity indicator	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established
Link up indicator	On, solid	Ethernet port is working properly
	Off	Ethernet port is disconnected

2.6 Insert or Remove SIM Card







Insert or remove the SIM card as shown in the following steps.

- **Insert SIM card**

1. Make sure gateway is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot.
3. To insert SIM card, press the card with finger until you hear a click
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

- **Remove SIM card**

1. Make sure gateway is powered off.
2. To remove slot cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot.
3. To remove SIM card, press the card with finger until it pops out and then take out the card.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

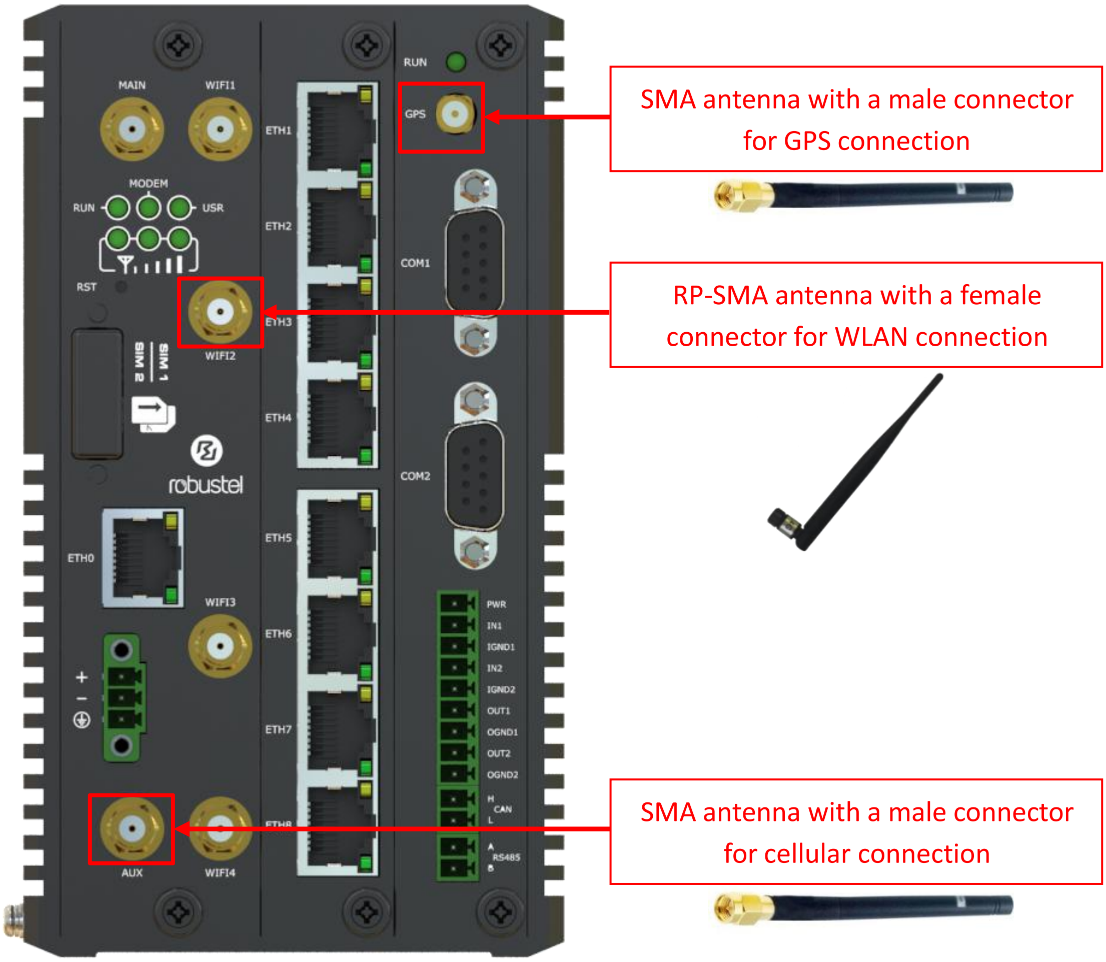
Note:

1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.
4. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away from electricity and magnetism.
7. Make sure gateway is powered off before inserting or removing the card.

2.7 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the gateway’s antenna connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance.

Note: Recommended torque for tightening is 0.35 N.m.



SMA antenna with a male connector for GPS connection

RP-SMA antenna with a female connector for WLAN connection

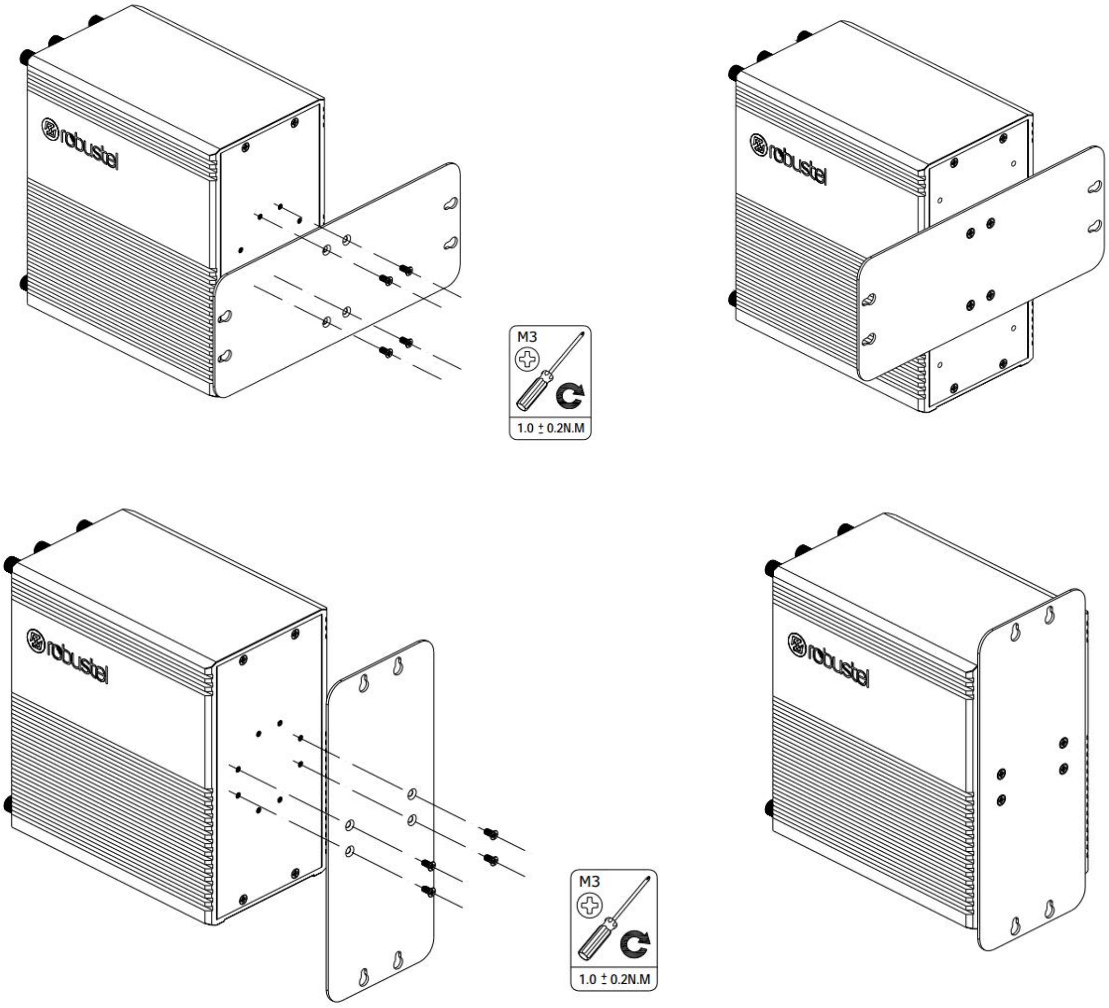
SMA antenna with a male connector for cellular connection

2.8 Mount the Gateway

The gateway can be placed on a desktop or mounted to a wall or a DIN rail.

Two methods for mounting the gateway

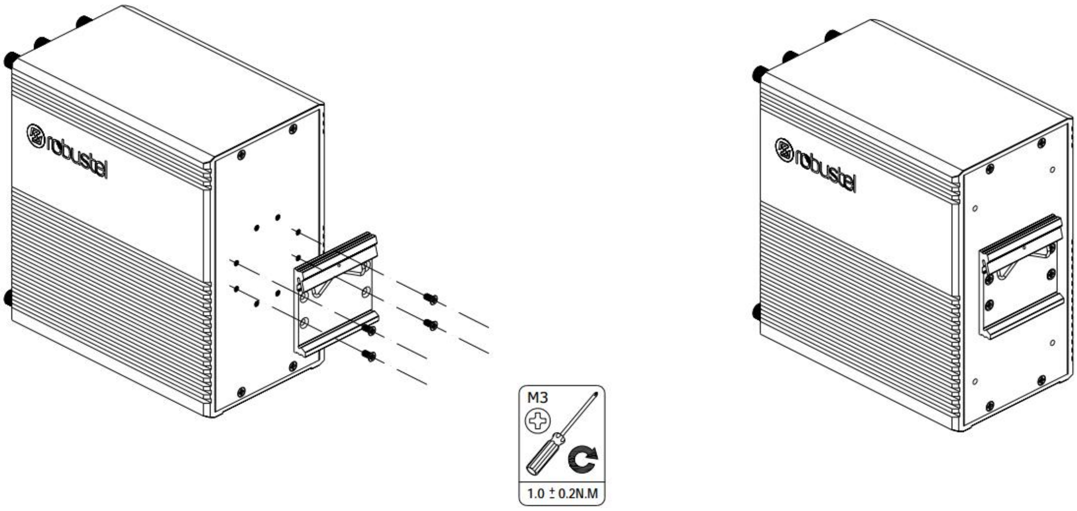
- Wall mounting (measured in mm)



Use 4 pcs of M3*6 flat head Phillips screws to fix the wall mounting kit to the gateway, and then use 2 pcs of M3 drywall screws to mount the gateway associated with the wall mounting kit on the wall.

Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

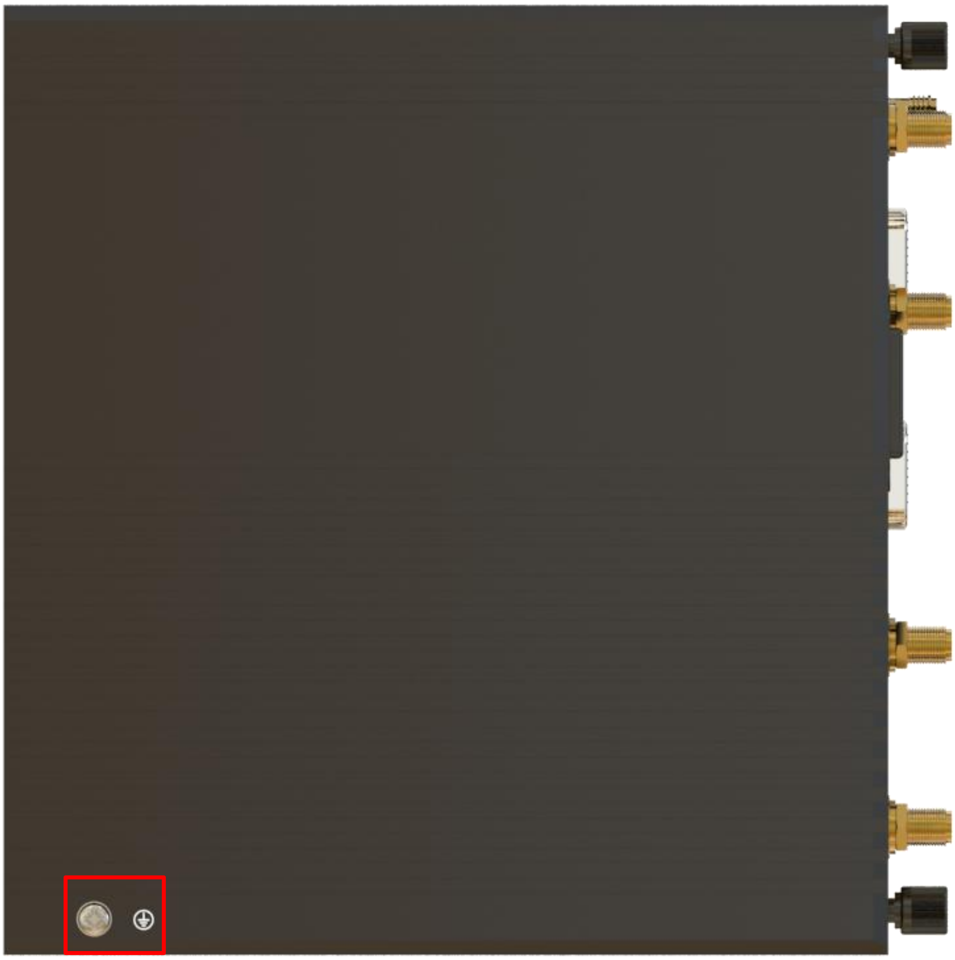
- DIN rail mounting (measured in mm)



Use 4 pcs of M3*6 flat head Phillips screws to fix the DIN rail to the gateway, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

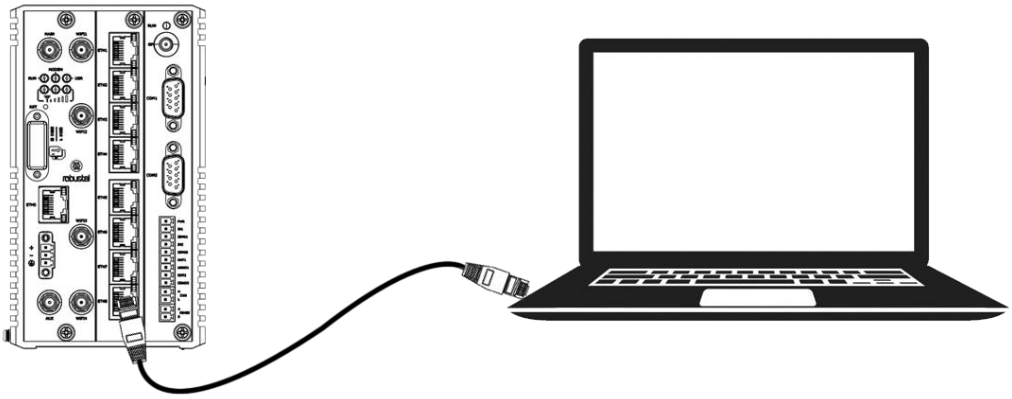
2.9 Ground the Gateway



Gateway grounding helps prevent the noise effect due to electromagnetic interference (EMI). Connect the gateway to the site ground wire by the ground screw before powering on.

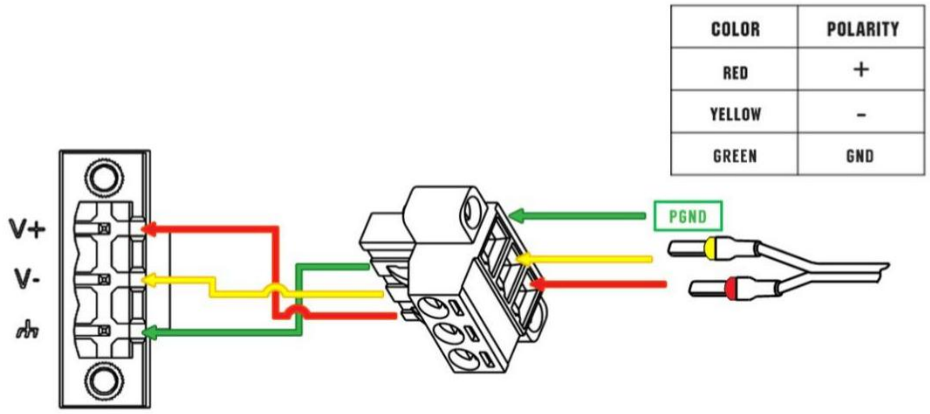
Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.

2.10 Connect the Gateway to a Computer



Connect an Ethernet cable to any port marked ETH0~ETH8 at the front of the gateway, and connect the other end of the cable to your computer.

2.11 Power Supply



COLOR	POLARITY
RED	+
YELLOW	-
GREEN	GND

MEG5000 supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Note: The range of power voltage is 12 to 60V DC.

Chapter 3 Initial Configuration

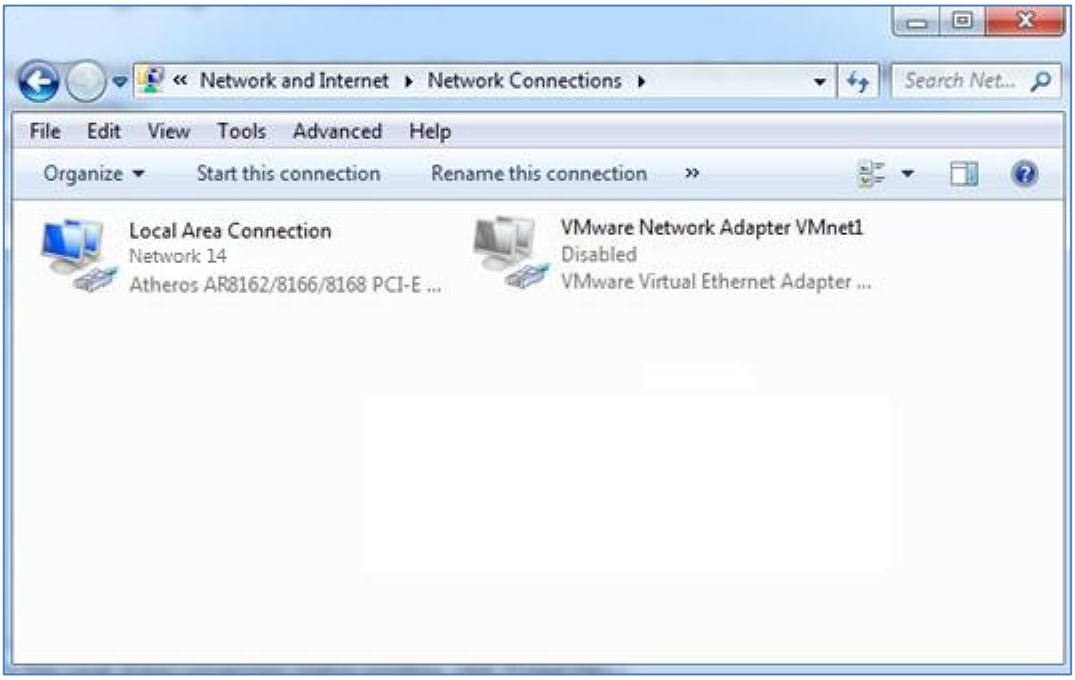
The gateway can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the gateway, 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 gateway. 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 gateway. If you encounter any problems accessing the gateway 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 gateway.
Note: If your device is not with Expansion Card 1, please connect the network cable to the port of the control card. If it is with Expansion Card 1, the control card port should be not used for web configuration because it is as the WAN port. So connect the cable to any LAN port of Expansion Card 1 to configure.

3.1 Configure the PC

There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the gateway. Please refer to the steps below.

Here take **Windows 7** as example, and the configuration for windows system is similar.

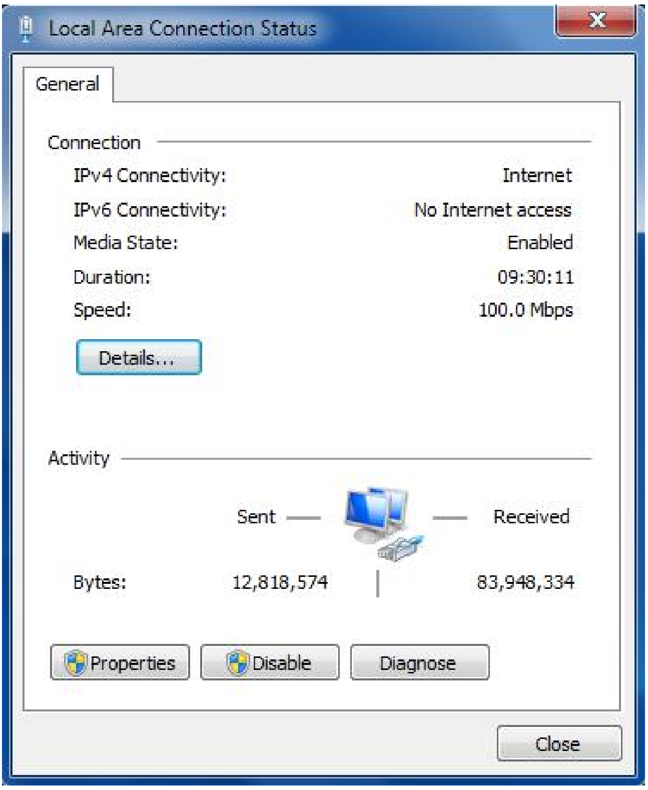
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



Local Area Connection
Network 14
Atheros AR8162/8166/8168 PCI-E ...

VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

2. Click **Properties** in the window of **Local Area Connection Status**.



Local Area Connection Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 09:30:11

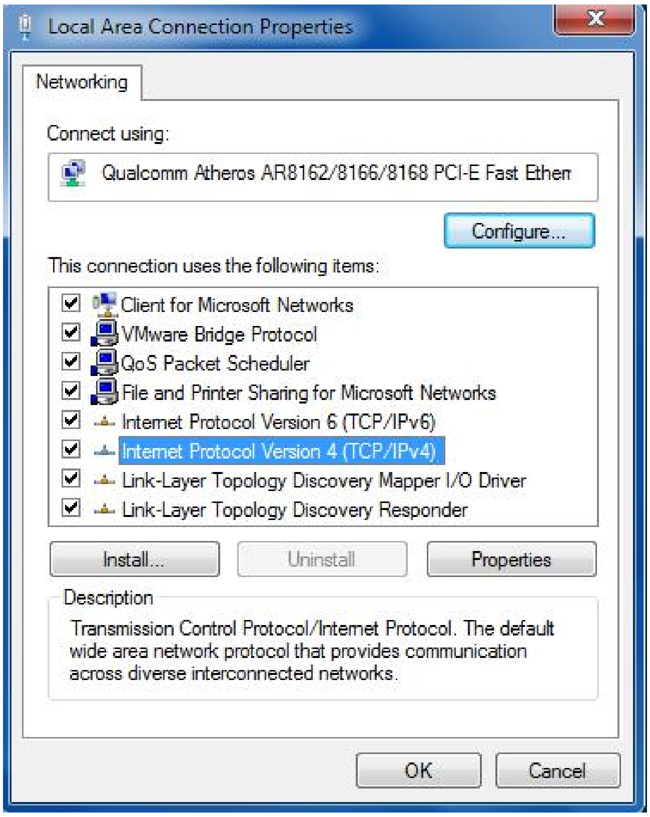
Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 12,818,574 | 83,948,334

3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Local Area Connection Properties

Networking

Connect using:

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

This connection uses the following items:

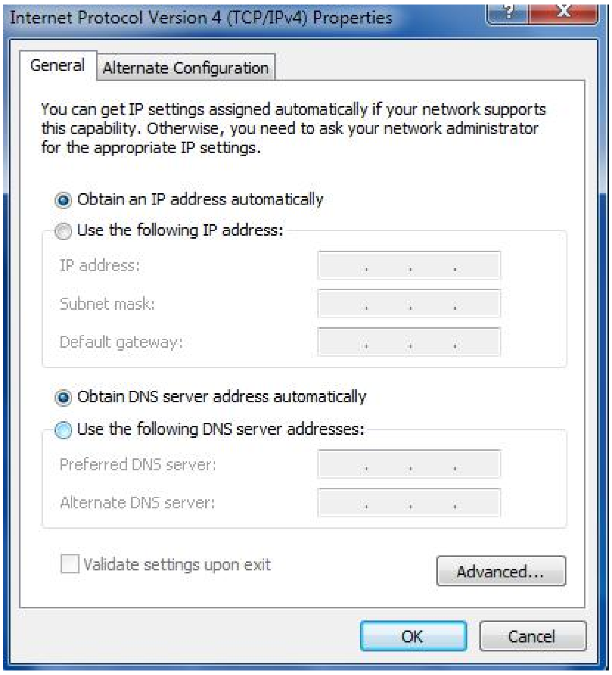
- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery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

Description

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

4. Two ways for configuring the IP address of PC.

Obtain an IP address automatically:



Internet Protocol Version 4 (TCP/IPv4) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

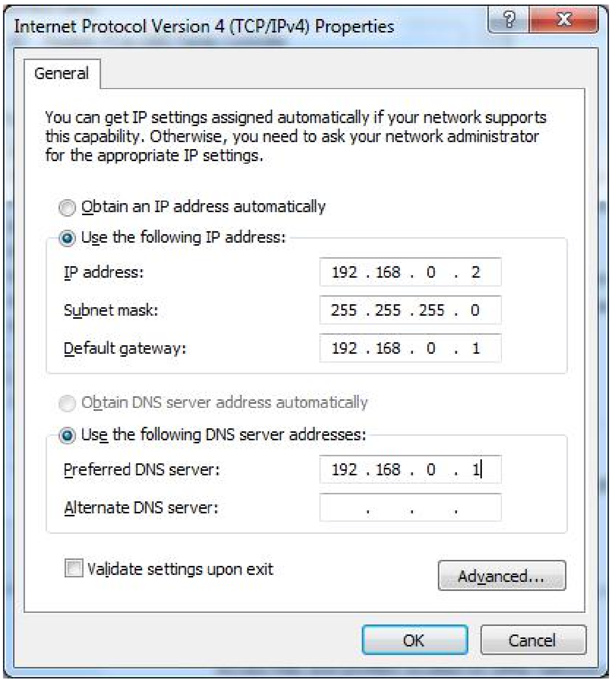
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Use the following IP address:

(Configured a static IP address manually within the same subnet of the gateway)



Internet Protocol Version 4 (TCP/IPv4) Properties

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

5. Click **OK** to finish the configuration.

3.2 Factory Default Settings

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

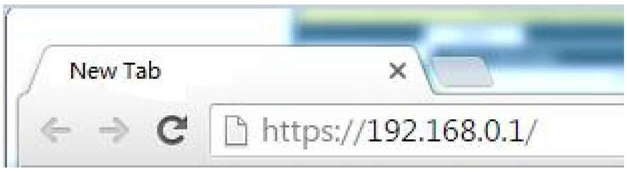
Item	Description
Username	admin
Password	admin
ETH0	With Expansion Card 1--WAN mode Without Expansion Card 1--192.168.0.1/255.255.255.0, LAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
ETH2	192.168.0.1/255.255.255.0, LAN mode
ETH3	192.168.0.1/255.255.255.0, LAN mode
ETH4	192.168.0.1/255.255.255.0, LAN mode
ETH5	192.168.0.1/255.255.255.0, LAN mode
ETH6	192.168.0.1/255.255.255.0, LAN mode
ETH7	192.168.0.1/255.255.255.0, LAN mode
ETH8	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

3.3 Log in the Gateway

To log in to the management page and view the configuration status of your gateway, please follow the steps below.

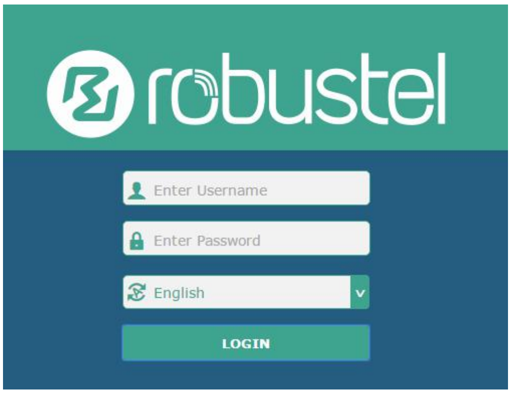
1. On your PC, open a web browser such as Internet Explorer, Google and Firebox, etc.
2. From your web browser, type the IP address of the gateway into the address bar and press enter. The default IP address of the gateway is 192.168.0.1, though the actual address may vary.

   Note: If a SIM card with a public IP address is inserted in the gateway, enter this corresponding public IP address in the browser's address bar to access the gateway wirelessly.



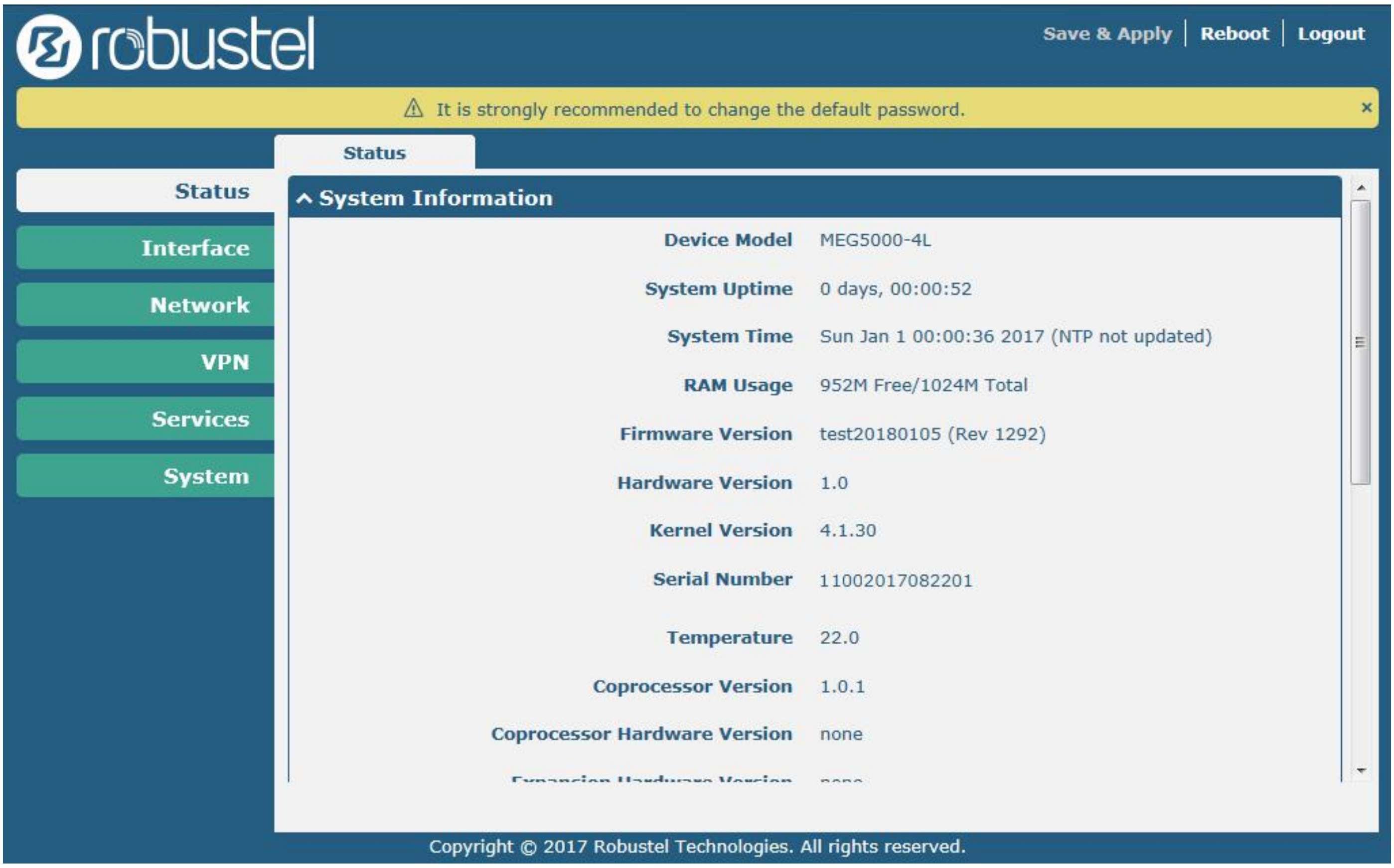
3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are "admin".

   Note: If enter the wrong username or password over six times, the login web will be locked for 5 minutes.



3.4 Control Panel

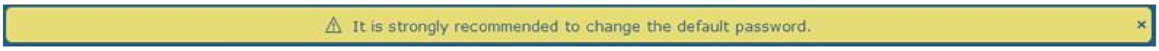
After logging in, the home page of the MEG5000's web interface is displayed, for example.



Device Model	MEG5000-4L
System Uptime	0 days, 00:00:52
System Time	Sun Jan 1 00:00:36 2017 (NTP not updated)
RAM Usage	952M Free/1024M Total
Firmware Version	test20180105 (Rev 1292)
Hardware Version	1.0
Kernel Version	4.1.30
Serial Number	11002017082201
Temperature	22.0
Coprocessor Version	1.0.1
Coprocessor Hardware Version	none
Expansion Hardware Version	none

Copyright © 2017 Robustel Technologies. All rights reserved.

Using the original password to log in the gateway, the page will pop up the following tab



It is strongly recommended to change the default password.

Click the × button to close the popup window. It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **4.6.6 User Management**.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into gateway's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to reboot the gateway. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	Reboot
Logout	Click to log the current user out safely. After logging out, 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 save 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:

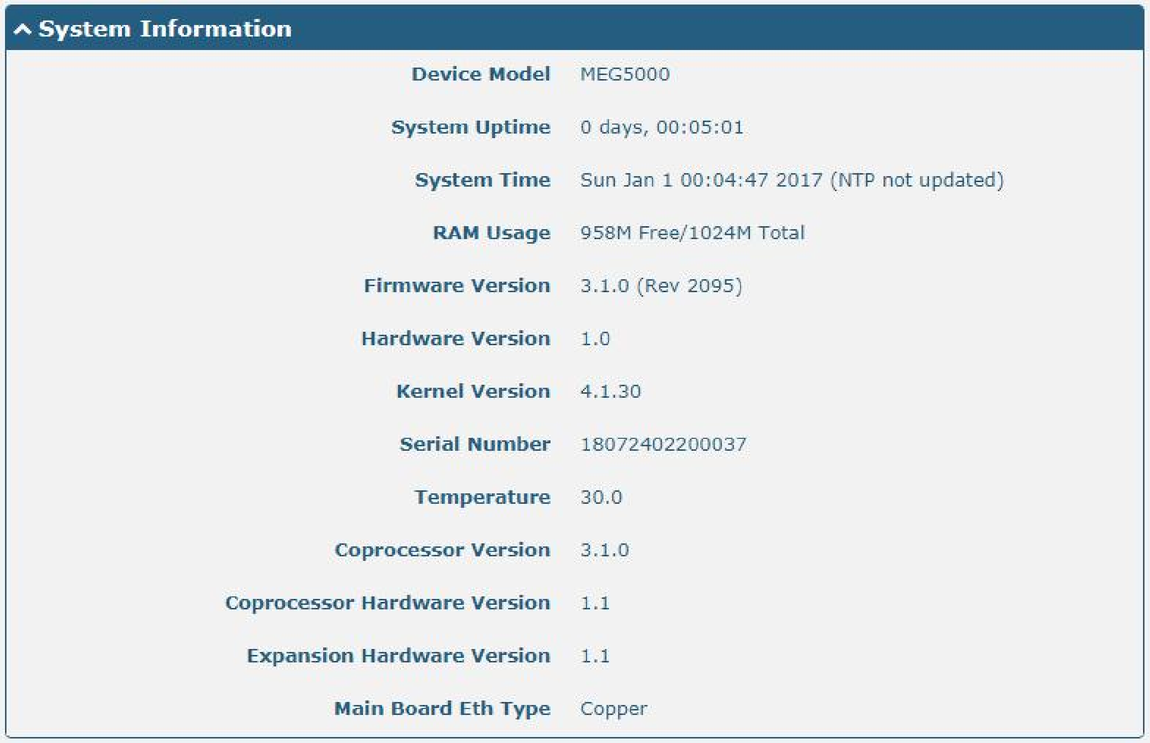
1. Modify in one page;
2. Click Submit under this page;
3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click Save & Apply.

Chapter 4 Gateway Configuration

4.1 Status

4.1.1 System Information

This page allows you to view the System Information, Internet Status and LAN Status of your Gateway.



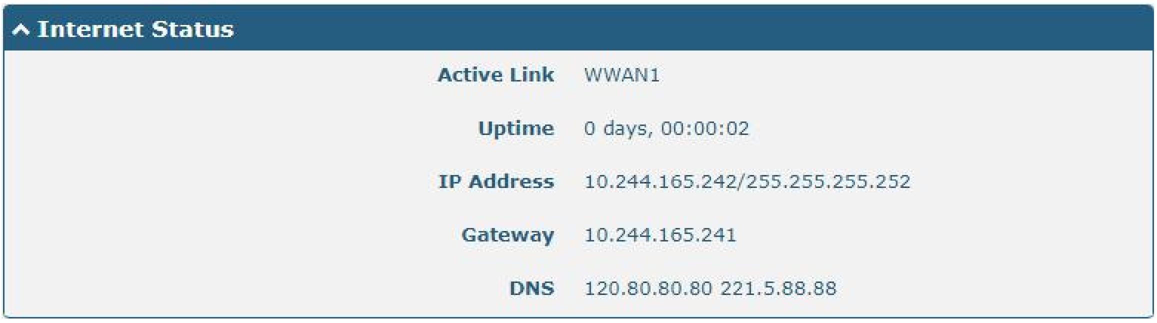
^ System Information

Device Model	MEG5000
System Uptime	0 days, 00:05:01
System Time	Sun Jan 1 00:04:47 2017 (NTP not updated)
RAM Usage	958M Free/1024M Total
Firmware Version	3.1.0 (Rev 2095)
Hardware Version	1.0
Kernel Version	4.1.30
Serial Number	18072402200037
Temperature	30.0
Coprocessor Version	3.1.0
Coprocessor Hardware Version	1.1
Expansion Hardware Version	1.1
Main Board Eth Type	Copper

System Information	
Item	**Description**
Device Model	Show the model name of your device.
System Uptime	Show the current amount of time the gateway has been connected.
System Time	Show the current system time.
RAM Usage	Show the free memory and the total memory.
Firmware Version	Show the firmware version running on the gateway.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.
Temperature	Show the temperature of the device.
Coprocessor Version	Show the firmware version of the coprocessor.
Coprocessor Hardware Version	Show the hardware version of the coprocessor.
Expansion Hardware Version	Show the hardware version of the expansion card.
Main Board Eth Type	Show the ETH type of the main board, Fiber or Copper.

4.1.2 Cellular Status

This section shows the cellular status information of the gateway.



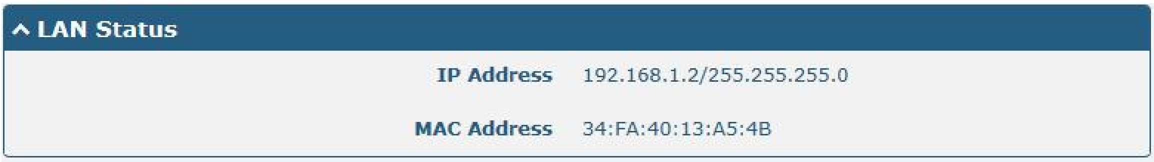
^ Internet Status

Active Link	WWAN1
Uptime	0 days, 00:00:02
IP Address	10.244.165.242/255.255.255.252
Gateway	10.244.165.241
DNS	120.80.80.80 221.5.88.88

Cellular Status	
Item	**Description**
Active Link	Show the current active link. WWAN1, WWAN2, WAN or WLAN
Uptime	Show the current amount of time the link has been connected.
IP Address	Show the IP address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current primary DNS server and secondary server.

4.1.3 Internet Status

This section shows the Internet status information of the gateway.



^ LAN Status

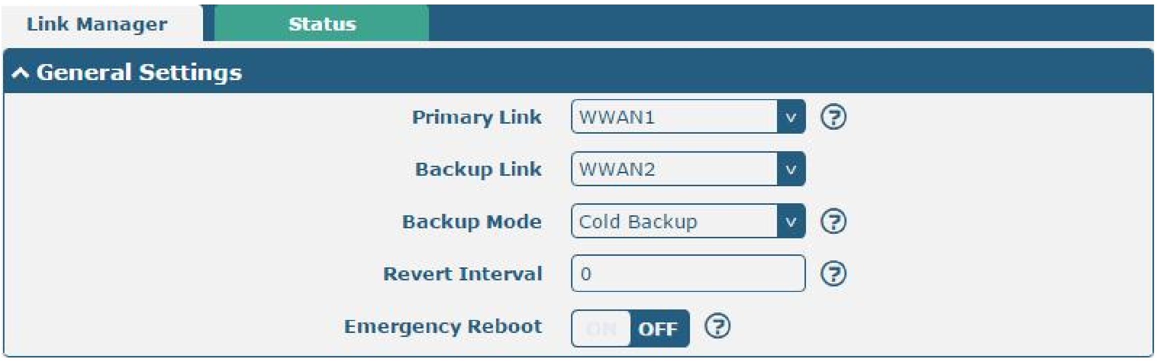
IP Address	192.168.1.2/255.255.255.0
MAC Address	34:FA:40:13:A5:4B

Internet Status	
Item	**Description**
IP Address	Show the IP address and the Netmask of the gateway.
MAC Address	Show the MAC address of the gateway.

4.2 Interface

4.2.1 Link Manager

This section allows you to setup the link connection. Link manager is a network link backup feature that provides backup of mobile networks and Ethernet links.



^ General Settings

Primary Link: WWAN1

Backup Link: WWAN2

Backup Mode: Cold Backup

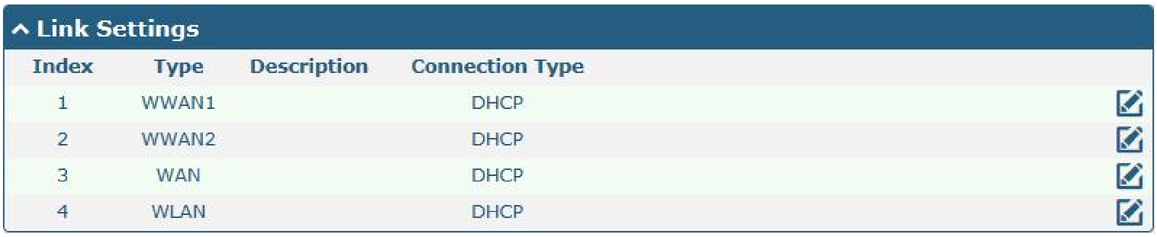
Revert Interval: 0

Emergency Reboot: ON OFF

General Settings @ Link Manager		
Item	**Description**	**Default**
Primary Link	Select from "WWAN1", "WWAN2", "WAN" or "WLAN". • WWAN1: Select to make SIM1 as the primary wireless link • WWAN2: Select to make SIM2 as the primary wireless link • WAN: Select to make WAN as the primary wired link • WLAN: Select to make WLAN as the primary wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **4.2.5 WiFi (Optional)**.	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN" or "None". • WWAN1: Select to make SIM1 as backup wireless link • WWAN2: Select to make SIM2 as backup wireless link • WAN: Select to make WAN as the backup wired link • WLAN: Select to make WLAN as the backup wireless link **Note:** WLAN link is available only if enable WiFi as Client mode, please refer to **4.2.5 WiFi (Optional)**. • None: Do not select any backup link	WWAN2
Backup Mode	Select from "Cold Backup", "Warm Backup" or "Load Balancing". • Cold Backup: The inactive link is offline on standby • Warm Backup: The inactive link is online on standby • Load Balancing: Use two links simultaneously **Note**: MEG5000 do not support warm backup and load balancing in the situation of two WWAN links.	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. **Note:** Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

Note: Click ? for help.

Link Settings allows you to configure the parameters of link connection, including WWAN1/WWAN2, WAN and WLAN. It is recommended to enable Ping detection to keep the gateway always online. The Ping detection increases the reliability and also costs the data traffic.

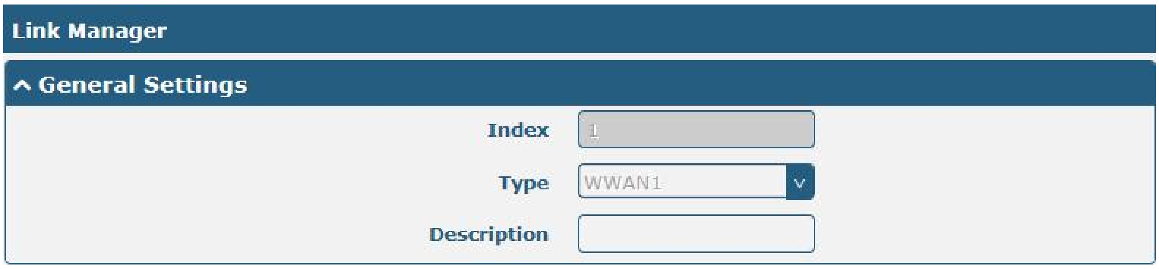


^ Link Settings

Index	Type	Description	Connection Type	
1	WWAN1		DHCP	✎
2	WWAN2		DHCP	✎
3	WAN		DHCP	✎
4	WLAN		DHCP	✎

Click ✎ on the right-most of WWAN1/WWAN2 to enter the configuration window.

WWAN1/WWAN2

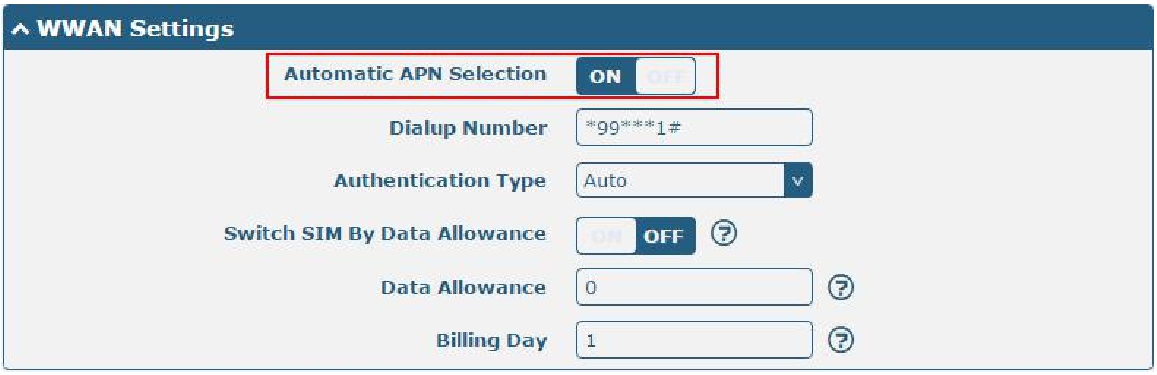


Link Manager

^ General Settings

Index	1
Type	WWAN1
Description	

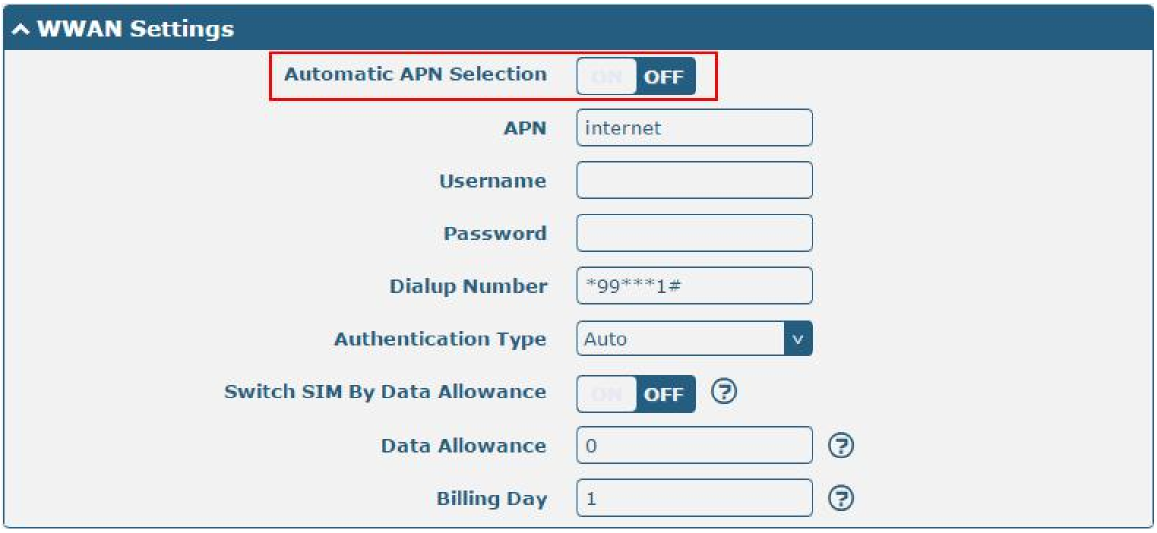
The window is displayed as below when enabling the “Automatic APN Selection” option.



^ WWAN Settings

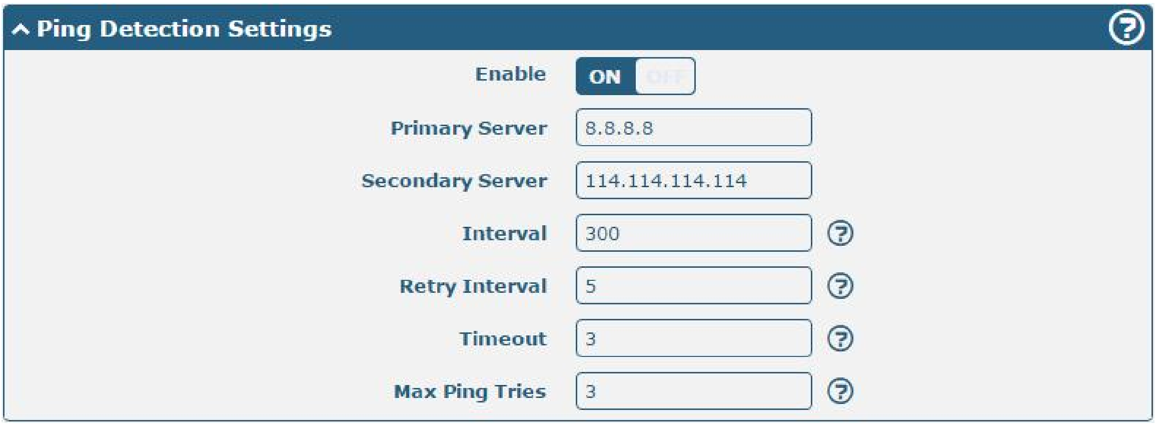
Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

The window is displayed as below when disabling the “Automatic APN Selection” option.



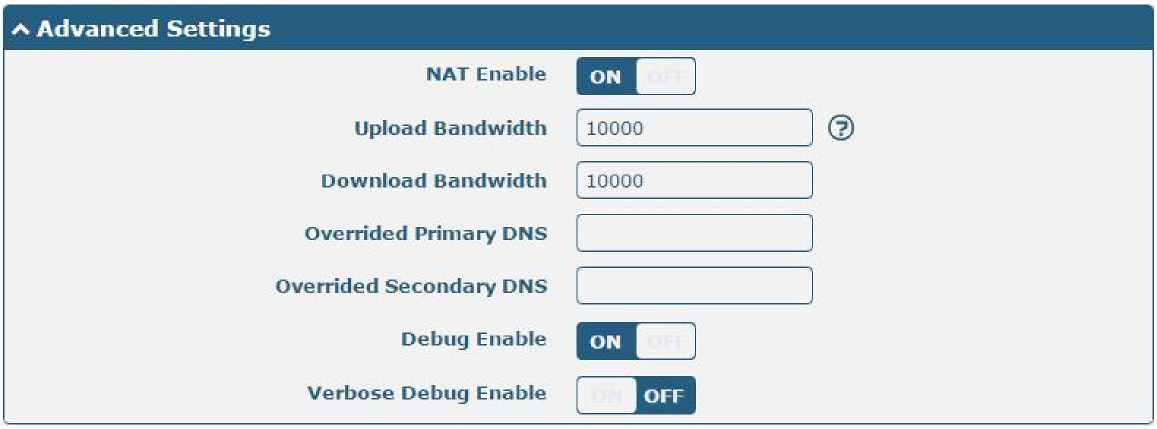
^ WWAN Settings

Automatic APN Selection	OFF
APN	internet
Username	
Password	
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1



^ Ping Detection Settings

Enable	ON
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3



^ Advanced Settings

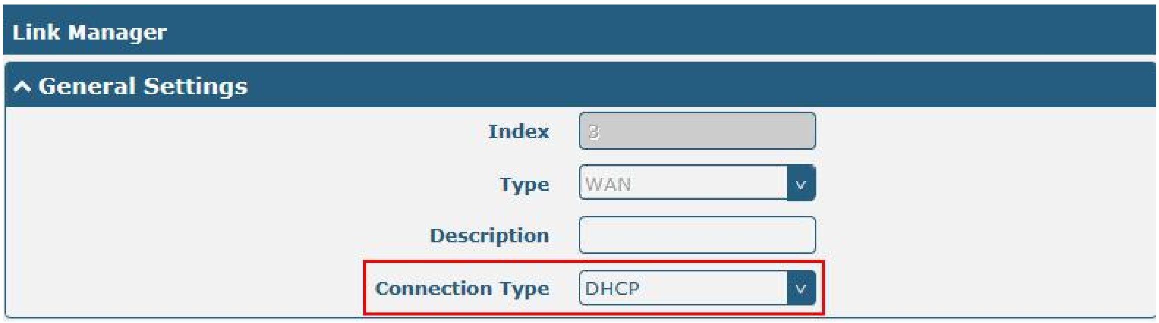
NAT Enable	ON
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link. It can be null.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. **Note**: Only used for dual-SIM backup.	OFF

Link Settings (WWAN)		
Item	**Description**	**Default**
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in **Interface > Link Manager > Status > WWAN Data Usage Statistics**. 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keep alive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the gateway will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
Upload Bandwidth	Set the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WAN

Gateway will obtain IP automatically from DHCP server if choosing "DHCP" as connection type. The window is displayed as below.

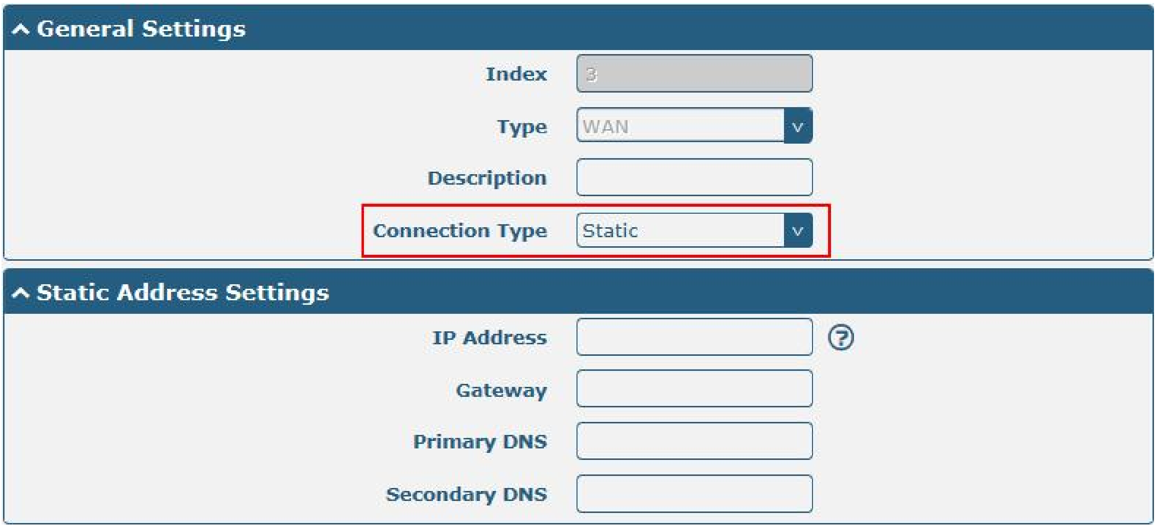


Link Manager

^ General Settings

Index	3
Type	WAN
Description	
Connection Type	DHCP

The window is displayed as below when choosing "Static" as the connection type.



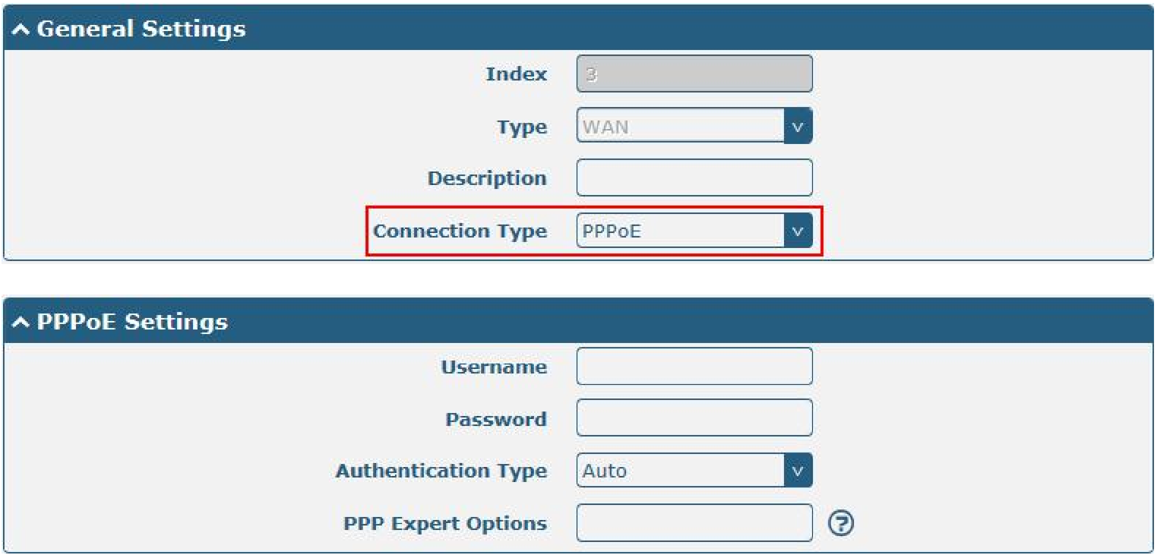
^ General Settings

Index	3
Type	WAN
Description	
Connection Type	Static

^ Static Address Settings

IP Address	
Gateway	
Primary DNS	
Secondary DNS	

The window is displayed as below when choosing "PPPoE" as the connection type.

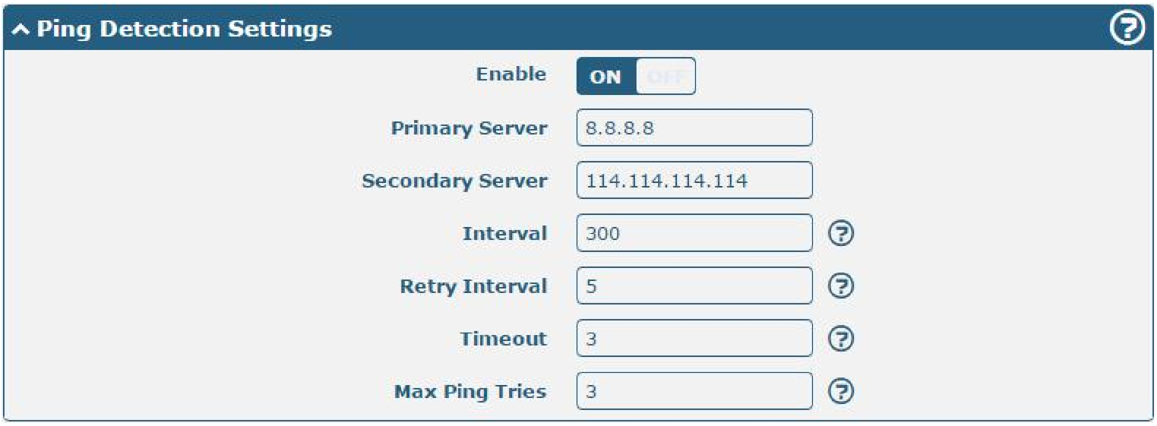


^ General Settings

Index	3
Type	WAN
Description	
Connection Type	PPPoE

^ PPPoE Settings

Username	
Password	
Authentication Type	Auto
PPP Expert Options	



Ping Detection Settings

Enable: ON

Primary Server: 8.8.8.8

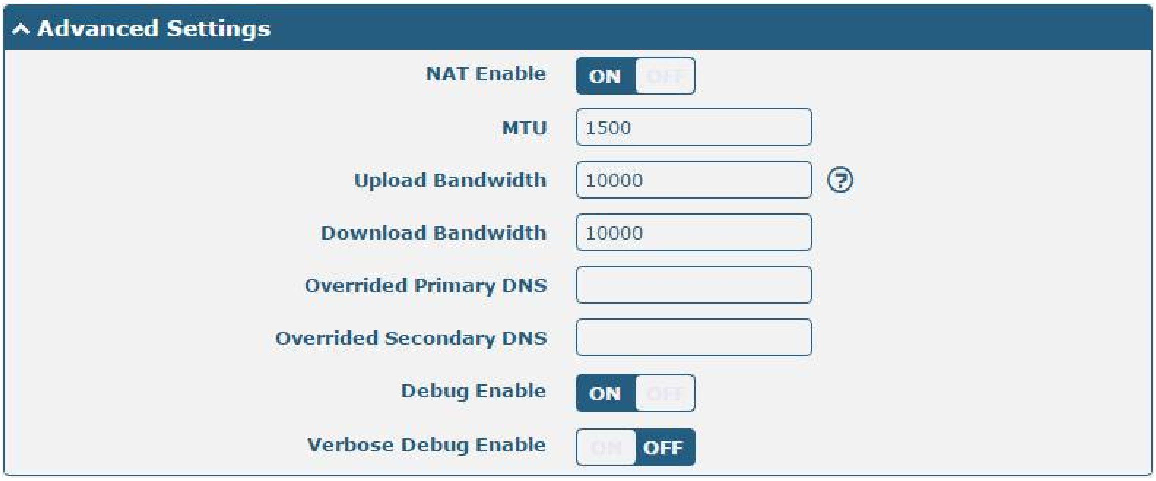
Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Max Ping Tries: 3



Advanced Settings

NAT Enable: ON

MTU: 1500

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Debug Enable: ON

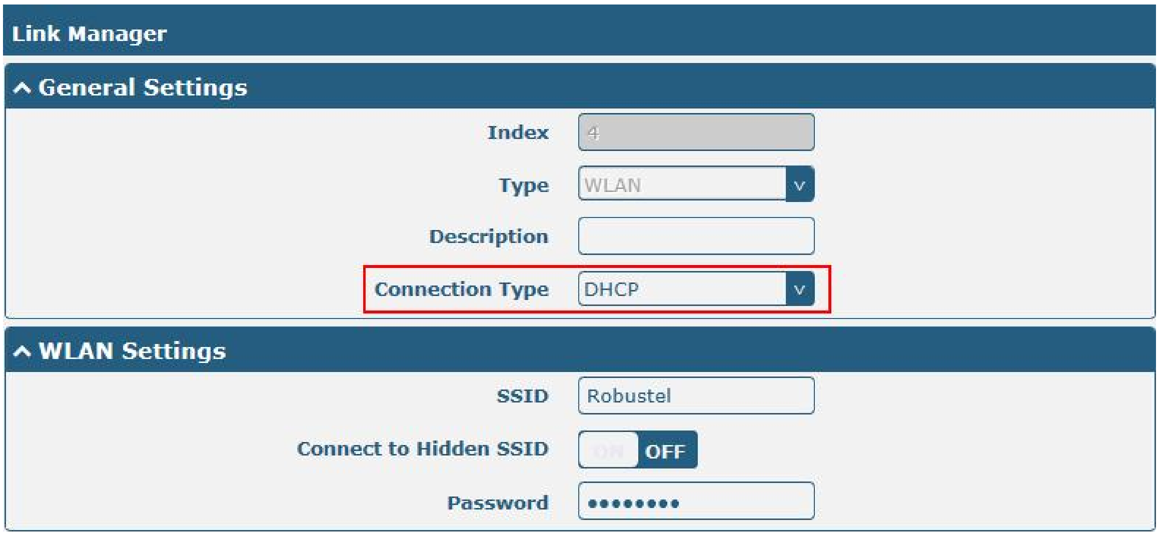
Verbose Debug Enable: OFF

Link Settings (WAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link. It can be null.	Null
Connection Type	Select from “DHCP”, “Static” or “PPPoE”.	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the IP address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null

Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the gateway will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WLAN

Gateway will obtain IP automatically from the WLAN AP if choosing “DHCP” as the connection type. The specific parameter configuration of SSID is shown as below.



Link Manager

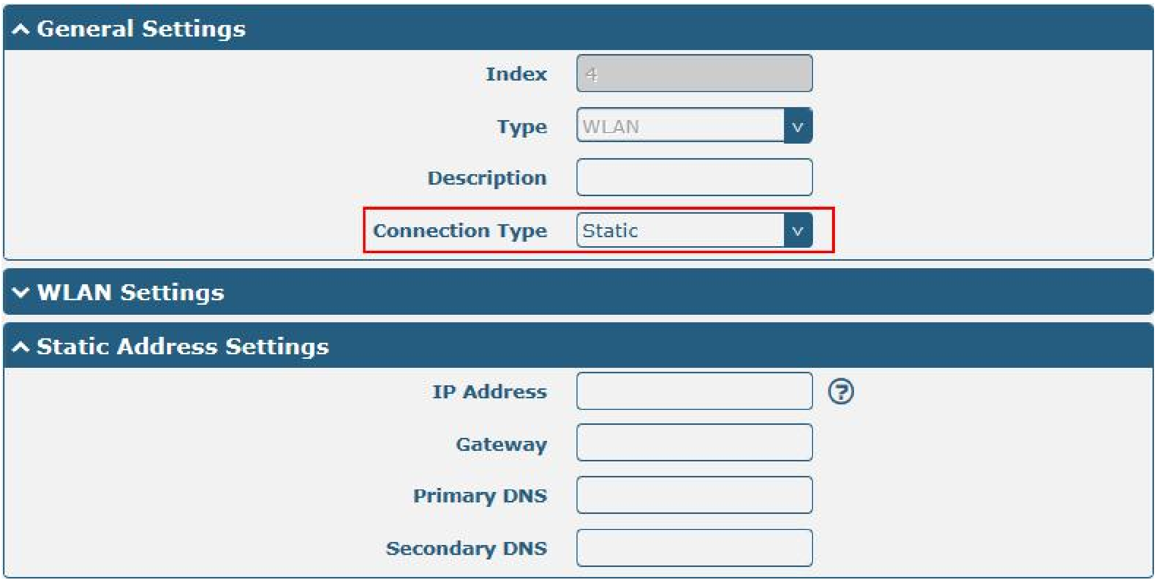
^ General Settings

Index	4
Type	WLAN
Description	
Connection Type	DHCP

^ WLAN Settings

SSID	Robustel
Connect to Hidden SSID	OFF
Password	••••••••

The window is displayed as below when choosing "Static" as the connection type.



^ General Settings

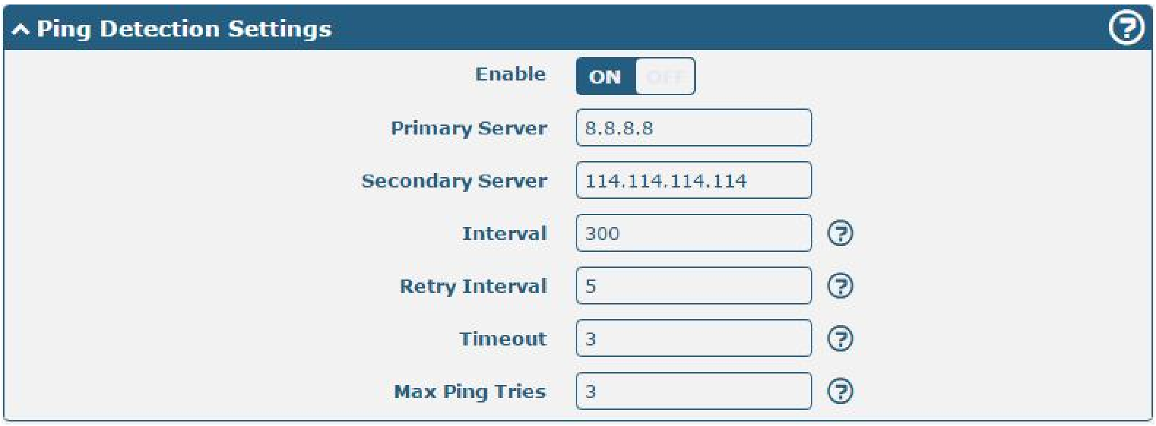
Index	4
Type	WLAN
Description	
Connection Type	Static

v WLAN Settings

^ Static Address Settings

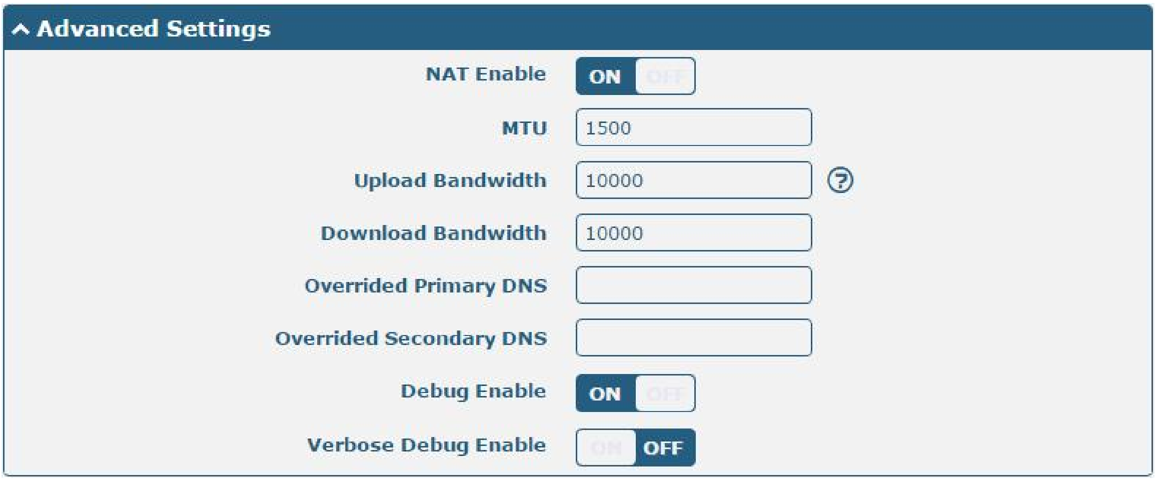
IP Address	
Gateway	
Primary DNS	
Secondary DNS	

MEG5000 does not support the **PPPoE** WLAN Connection Type.



^ Ping Detection Settings

Enable	ON
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3



^ Advanced Settings

NAT Enable: ON

MTU: 1500

Upload Bandwidth: 10000

Download Bandwidth: 10000

Overrided Primary DNS:

Overrided Secondary DNS:

Debug Enable: ON

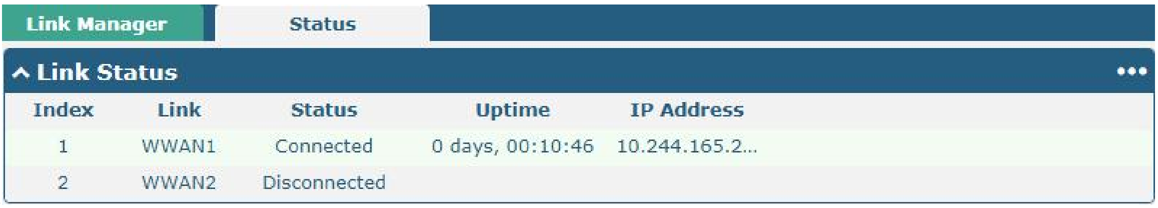
Verbose Debug Enable: OFF

Link Settings (WLAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from “DHCP” or “Static”.	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your gateway wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When gateway works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your gateway wants to connect.	Null
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the gateway will ping again every retry interval.	5

Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

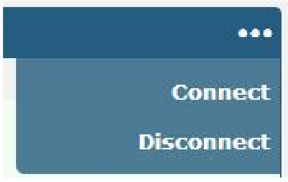
Status

This page allows you to view the current status of link connection.

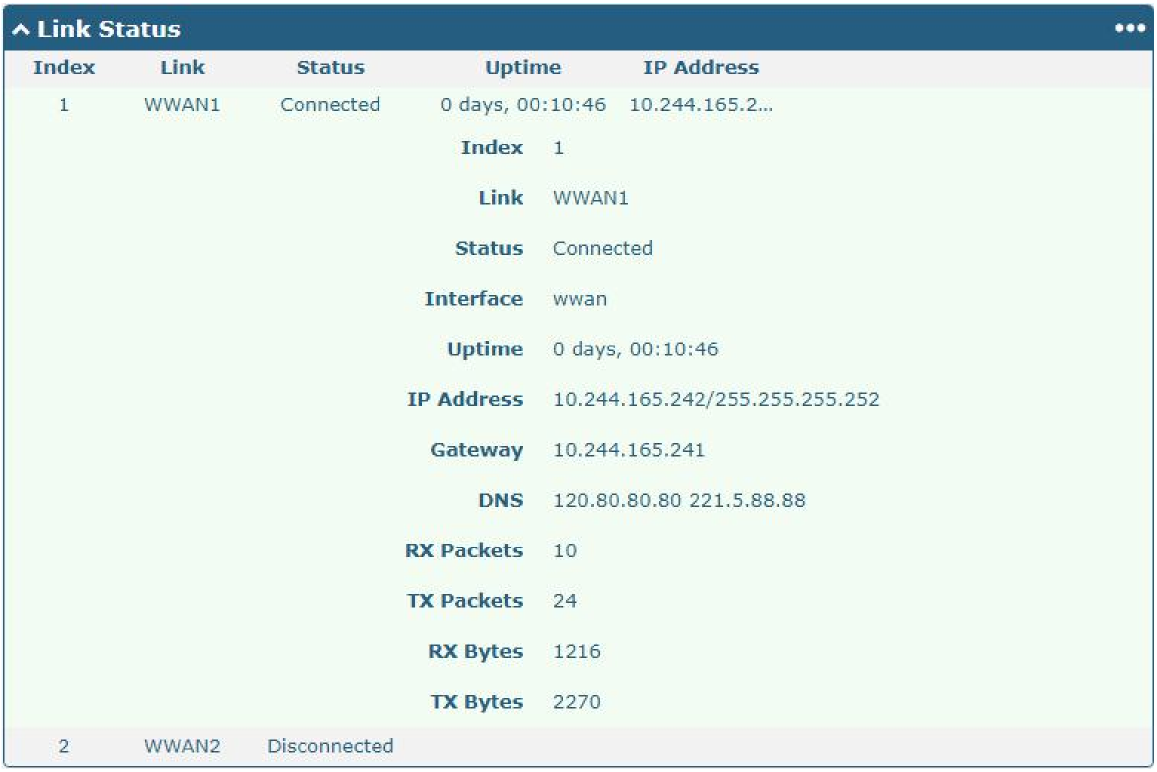


Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:10:46	10.244.165.2...
2	WWAN2	Disconnected		

Click the right-most button ••• to select the connection status of the current link.

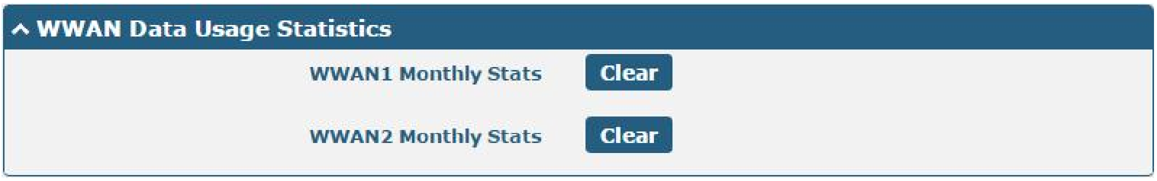


Click the row of the link, and it will show the details information of the current link connection under the row.



Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:10:46	10.244.165.2...
2	WWAN2	Disconnected		

Index	1
Link	WWAN1
Status	Connected
Interface	wwan
Uptime	0 days, 00:10:46
IP Address	10.244.165.242/255.255.255.252
Gateway	10.244.165.241
DNS	120.80.80.80 221.5.88.88
RX Packets	10
TX Packets	24
RX Bytes	1216
TX Bytes	2270

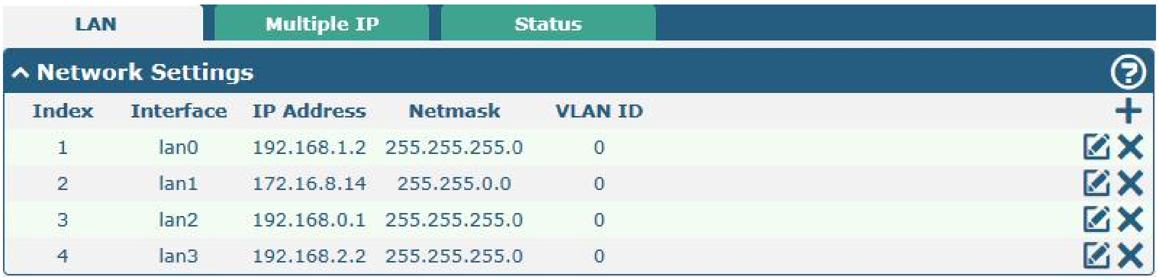


Click the Clear button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance**.

4.2.2 LAN

This section allows you to set the related parameters for LAN port. There are eight LAN ports on MEG5000, including ETH1~ETH8. The ETH1~ETH8 can freely choose from lan0~lan7, but at least one LAN port must be assigned as lan0. The default settings of ETH1~ETH8 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN

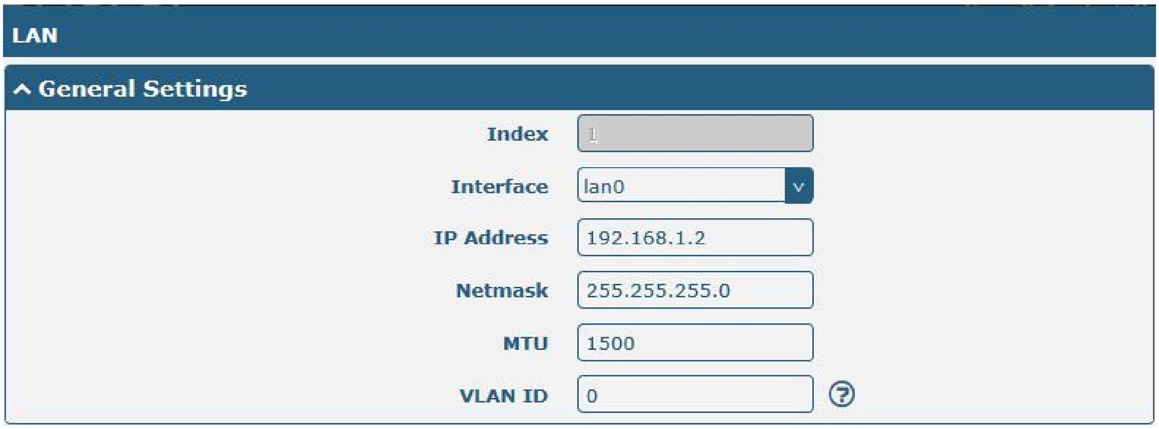


^ Network Settings

Index	Interface	IP Address	Netmask	VLAN ID
1	lan0	192.168.1.2	255.255.255.0	0
2	lan1	172.16.8.14	255.255.0.0	0
3	lan2	192.168.0.1	255.255.255.0	0
4	lan3	192.168.2.2	255.255.255.0	0

Note: Lan0 cannot be deleted.

You may click ＋ to add a new LAN port, or click ✕ to delete the current LAN port. Now, click ✎ to edit the configuration of the LAN port.

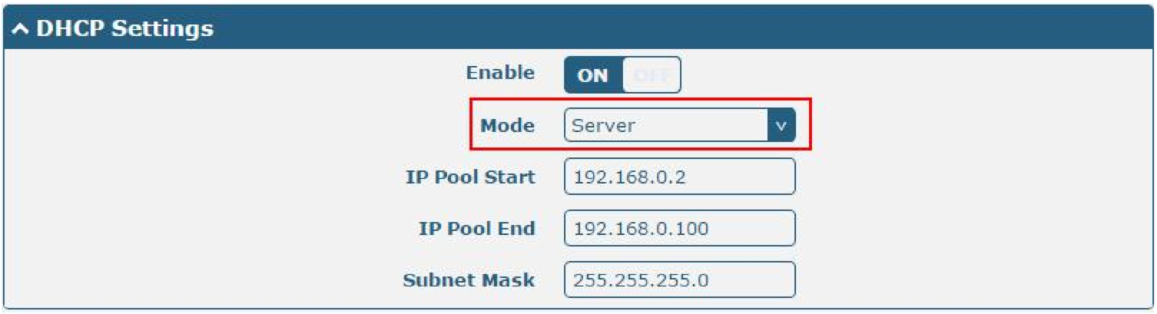

LAN

^ General Settings

Index	1
Interface	lan0
IP Address	192.168.1.2
Netmask	255.255.255.0
MTU	1500
VLAN ID	0

General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. **Note:** Lan1 is available only if it was selected by one of ETH1~ETH8 in **Ethernet > Ports > Port Settings**, and so on.	lan0
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500
VLAN ID	Enter the corresponding VLAN ID of the LAN port to group the ETH ports of the same LAN to a same vlan.	0

The window is displayed as below when choosing "Server" as the mode.



DHCP Settings

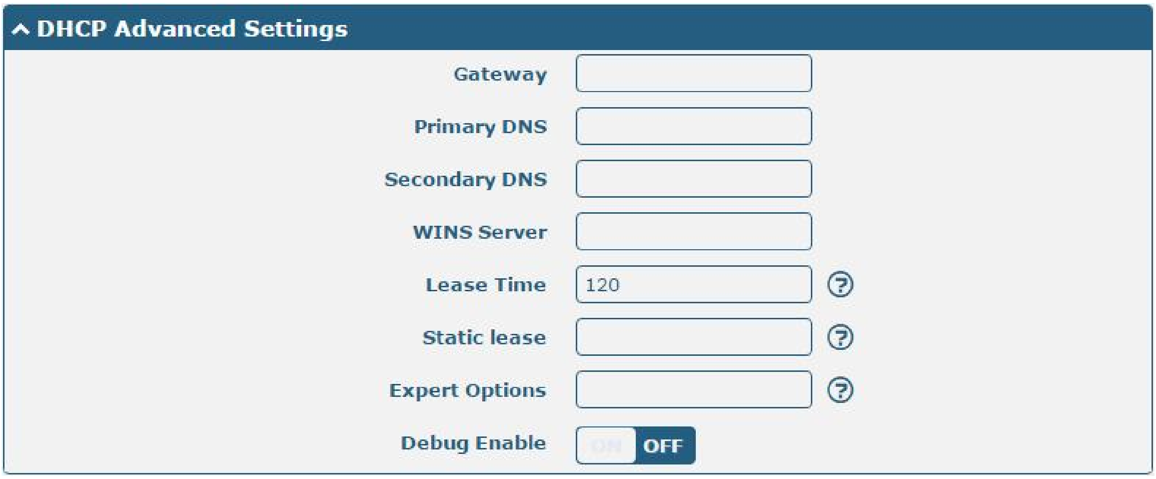
Enable: ON

Mode: Server

IP Pool Start: 192.168.0.2

IP Pool End: 192.168.0.100

Subnet Mask: 255.255.255.0



DHCP Advanced Settings

Gateway:

Primary DNS:

Secondary DNS:

WINS Server:

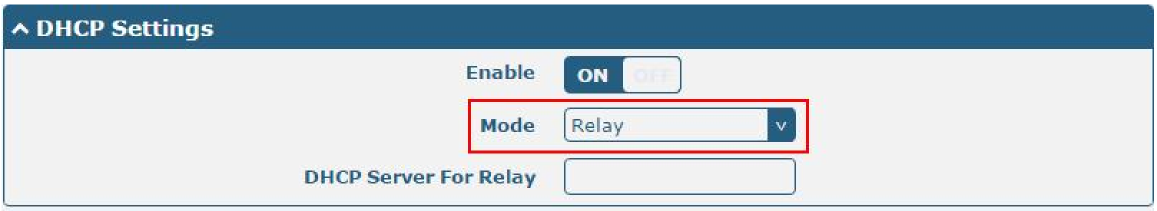
Lease Time: 120

Static lease:

Expert Options:

Debug Enable: OFF

The window is displayed as below when choosing "Relay" as the mode.

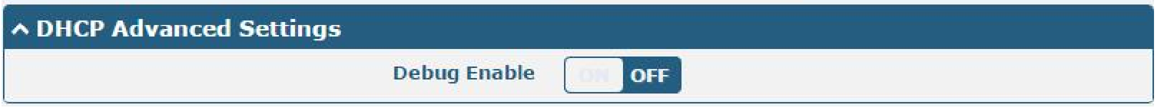


DHCP Settings

Enable: ON

Mode: Relay

DHCP Server For Relay:



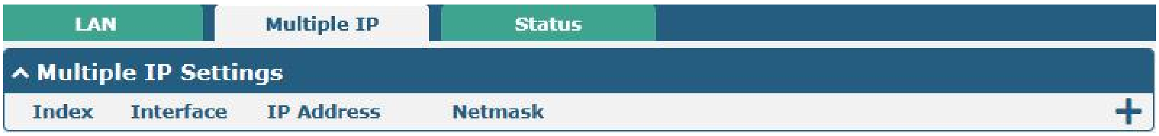
DHCP Advanced Settings

Debug Enable: OFF

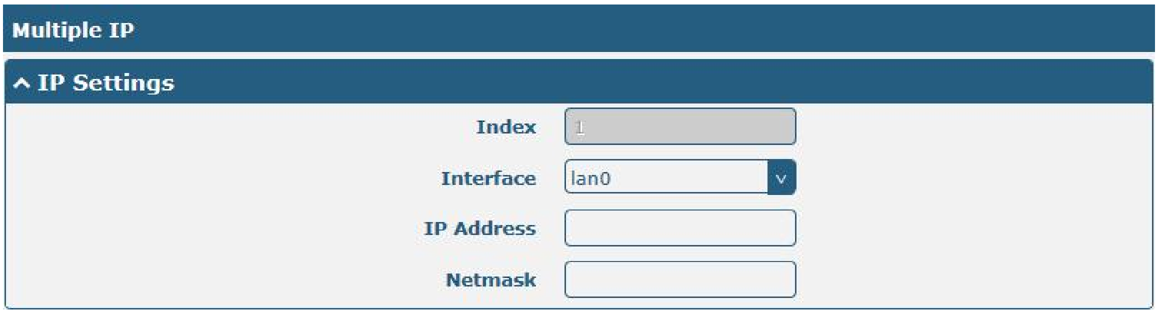
LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from "Server" or "Relay". • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Gateway can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in a same subnet	Server
IP Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2

LAN		
Item	**Description**	**Default**
IP Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
Gateway	Define the gateway assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF

Multiple IP



You may click ✎ to edit the multiple IP of the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click + to add a multiple IP to the LAN port



Index: 1

Interface: lan0

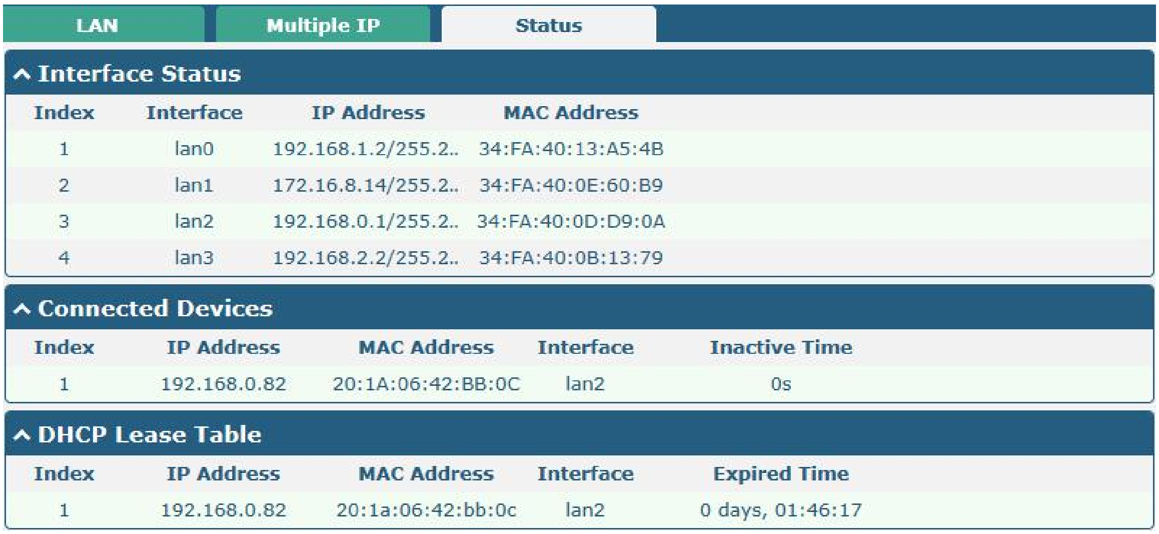
IP Address:

Netmask:

IP Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port.	--
IP Address	Set the multiple IP address of the LAN port.	Null
Netmask	Set the multiple Netmask of the LAN port.	Null

Status

This section allows you to view the status of LAN connection.



^ Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.1.2/255.2..	34:FA:40:13:A5:4B
2	lan1	172.16.8.14/255.2..	34:FA:40:0E:60:B9
3	lan2	192.168.0.1/255.2..	34:FA:40:0D:D9:0A
4	lan3	192.168.2.2/255.2..	34:FA:40:0B:13:79

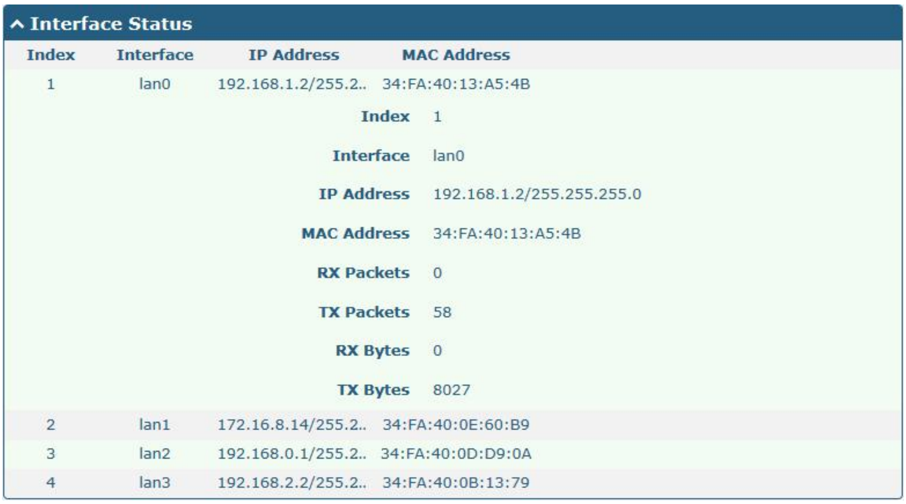
^ Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.82	20:1A:06:42:BB:0C	lan2	0s

^ DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.82	20:1a:06:42:bb:0c	lan2	0 days, 01:46:17

Click the row of status, the details status information will be displayed under the row. Please refer to the screenshot below.



^ Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	192.168.1.2/255.2..	34:FA:40:13:A5:4B

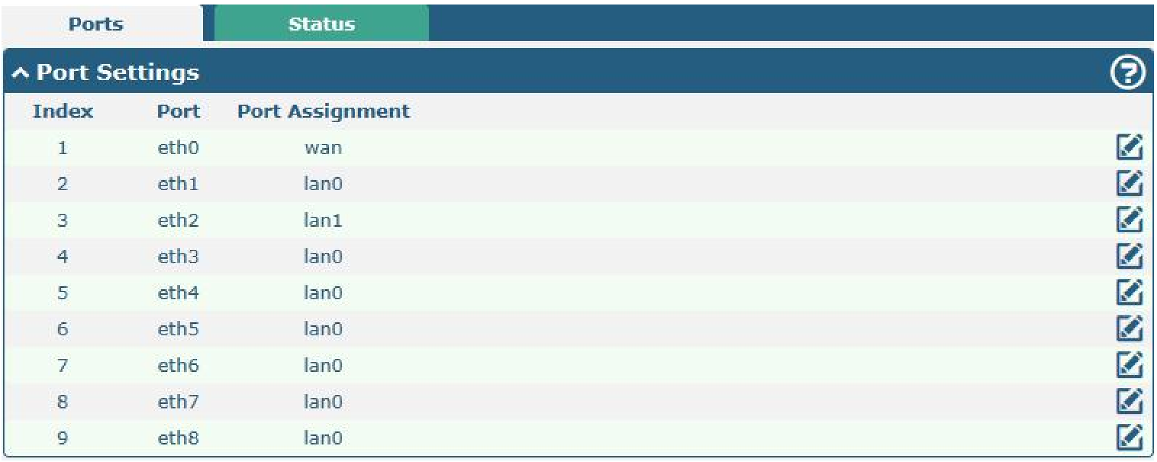
Index	1
Interface	lan0
IP Address	192.168.1.2/255.255.255.0
MAC Address	34:FA:40:13:A5:4B
RX Packets	0
TX Packets	58
RX Bytes	0
TX Bytes	8027

Index	Interface	IP Address	MAC Address
2	lan1	172.16.8.14/255.2..	34:FA:40:0E:60:B9
3	lan2	192.168.0.1/255.2..	34:FA:40:0D:D9:0A
4	lan3	192.168.2.2/255.2..	34:FA:40:0B:13:79

4.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There are nine Ethernet ports on MEG5000, including ETH0~ETH8. The ETH0 on the gateway can be configured as either a WAN port, while ETH1~ETH8 can only be configured as LAN ports. The ETH1~ETH8 can freely choose from lan0~lan7, but at least one LAN port must be assigned as lan0. By default, ETH1~ETH8 are lan0, and their IP are 192.168.0.1/255.255.255.0.

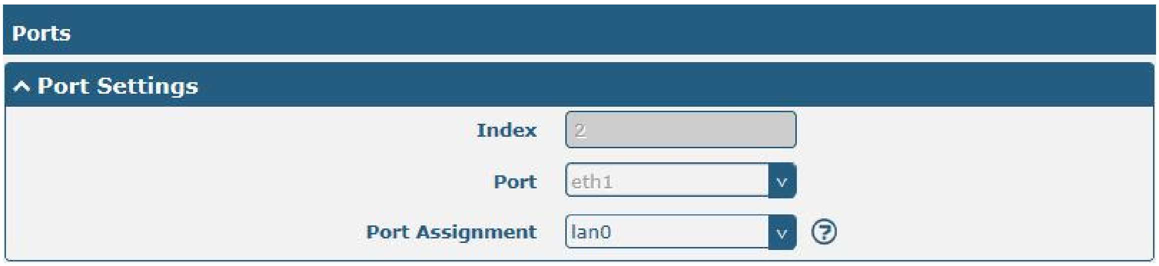
Note: If MEG5000 is not with Expansion Card 1, ETHO can be assigned as either WAN port or LAN port; when assigned as LAN port, it can be as lan0 only.



Port Settings

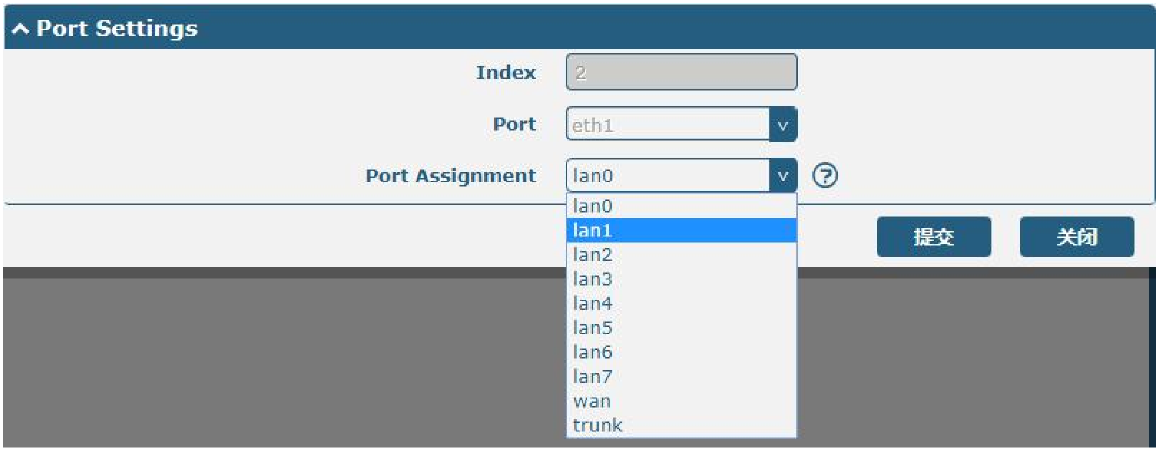
Index	Port	Port Assignment	
1	eth0	wan	✎
2	eth1	lan0	✎
3	eth2	lan1	✎
4	eth3	lan0	✎
5	eth4	lan0	✎
6	eth5	lan0	✎
7	eth6	lan0	✎
8	eth7	lan0	✎
9	eth8	lan0	✎

Click ✎ button of eth1 to configure its parameters. The port assignment can be changed by selecting from the drop down list.


Ports

Port Settings

Index: 2
Port: eth1
Port Assignment: lan0

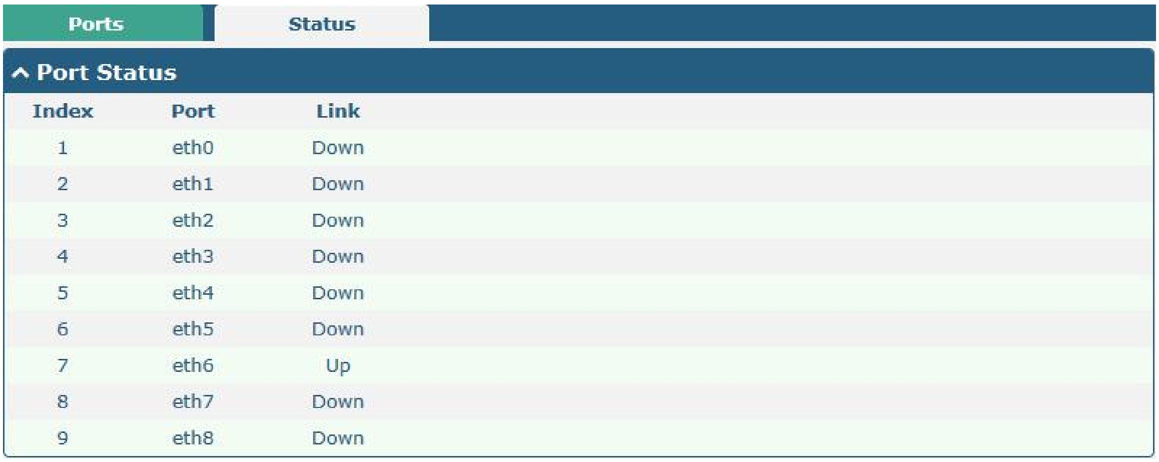

Port Settings

Index: 2
Port: eth1
Port Assignment: lan0

Port Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--

Port Assignment	Choose the Ethernet port's type, as a WAN or a LAN port. Trunk port is used for connection with that of the exchanger. The package received by trunk port will be with VLAN tag.	lan0

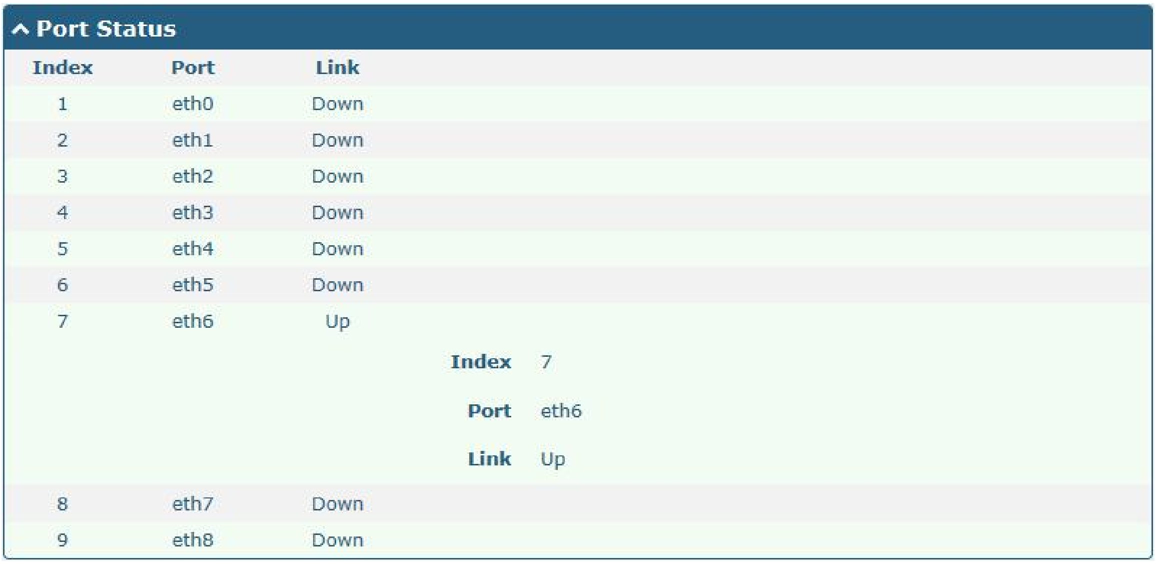
This column allows you to view the status of Ethernet port.



^ Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down
6	eth5	Down
7	eth6	Up
8	eth7	Down
9	eth8	Down

Click the row of status, the details status information will be displayed under the row. Please refer to the screenshot below.



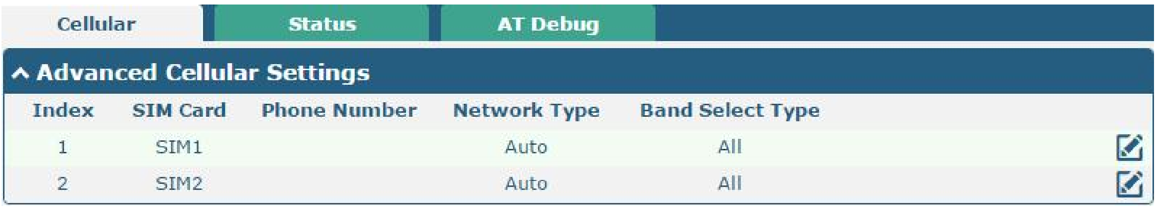
^ Port Status

Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Down
5	eth4	Down
6	eth5	Down
7	eth6	Up
8	eth7	Down
9	eth8	Down

Index 7
Port eth6
Link Up

4.2.4 Cellular

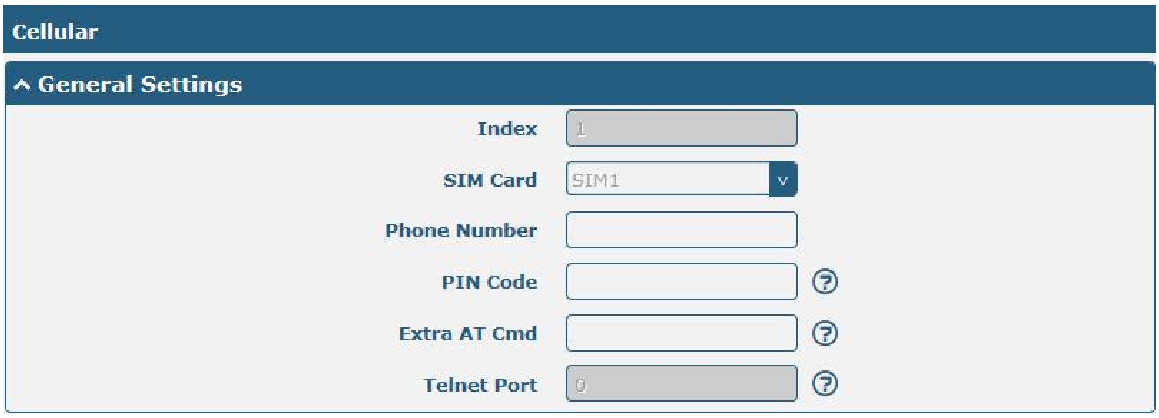
This section allows you to set the related parameters of Cellular. The MEG5000 has two SIM card slots, but do not support two SIM cards online simultaneously due to its single-module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	✎
2	SIM2		Auto	All	✎

Click ✎ of SIM 1 to edit the parameters.

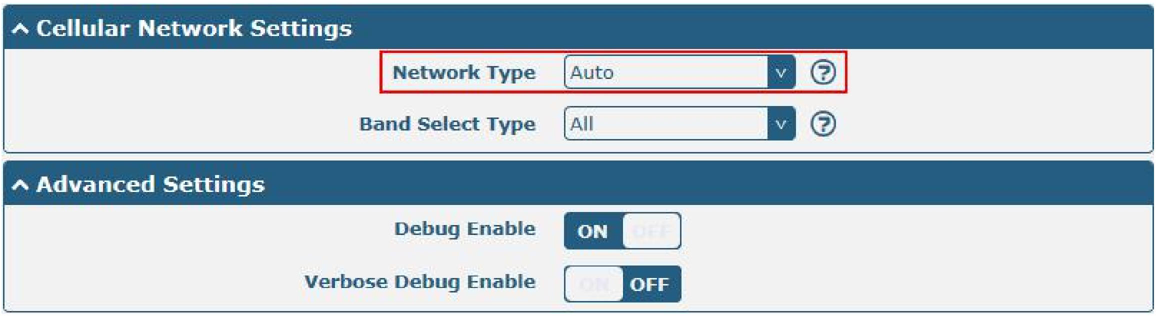


Cellular

General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

The window is displayed as below when choosing “Auto” as the network type.



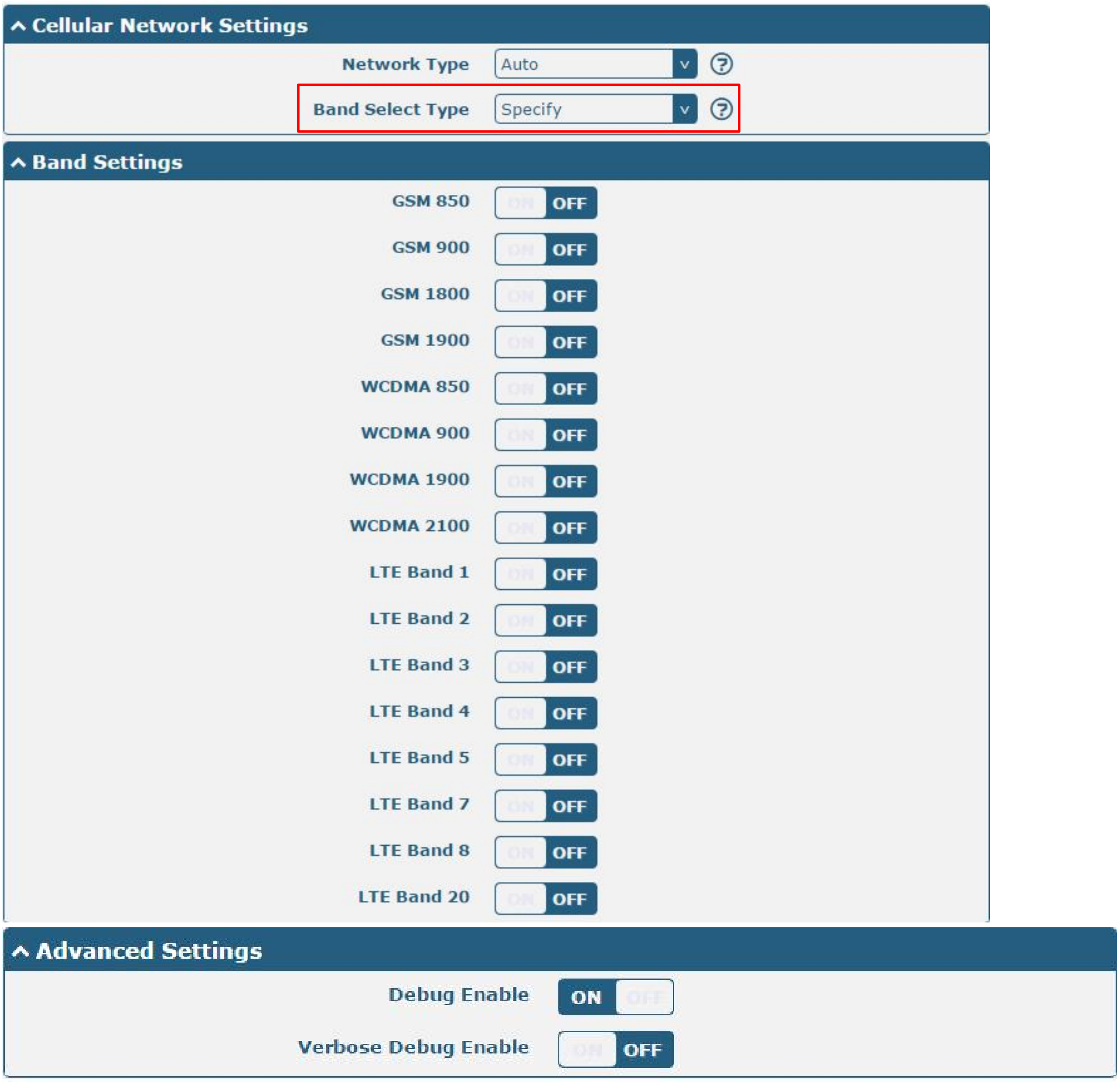
Cellular Network Settings

Network Type	Auto
Band Select Type	All

Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF

The window is displayed as below when choosing “Specify” as the band select type.



^ Cellular Network Settings

Network Type: Auto

Band Select Type: Specify

^ Band Settings

GSM 850: OFF

GSM 900: OFF

GSM 1800: OFF

GSM 1900: OFF

WCDMA 850: OFF

WCDMA 900: OFF

WCDMA 1900: OFF

WCDMA 2100: OFF

LTE Band 1: OFF

LTE Band 2: OFF

LTE Band 3: OFF

LTE Band 4: OFF

LTE Band 5: OFF

LTE Band 7: OFF

LTE Band 8: OFF

LTE Band 20: OFF

^ Advanced Settings

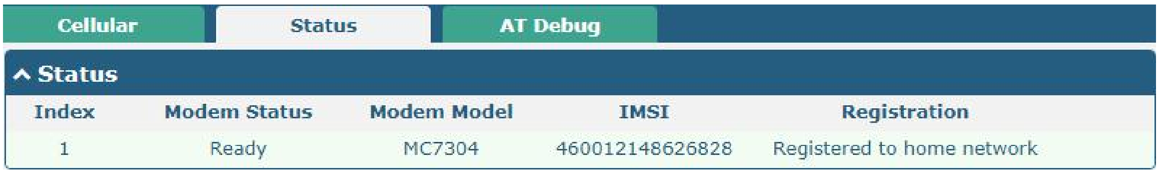
Debug Enable: ON

Verbose Debug Enable: OFF

Cellular		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		

Cellular		
Item	**Description**	**Default**
Network Type	Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", "4G First". • Auto: Connect to the best signal network automatically • 2G Only: Only the 2G network is connected • 2G First: Connect to the 2G Network preferentially • 3G Only: Only the 3G network is connected • 3G First: Connect to the 3G Network preferentially • 4G Only: Only the 4G network is connected • 4G First: Connect to the 4G Network preferentially	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

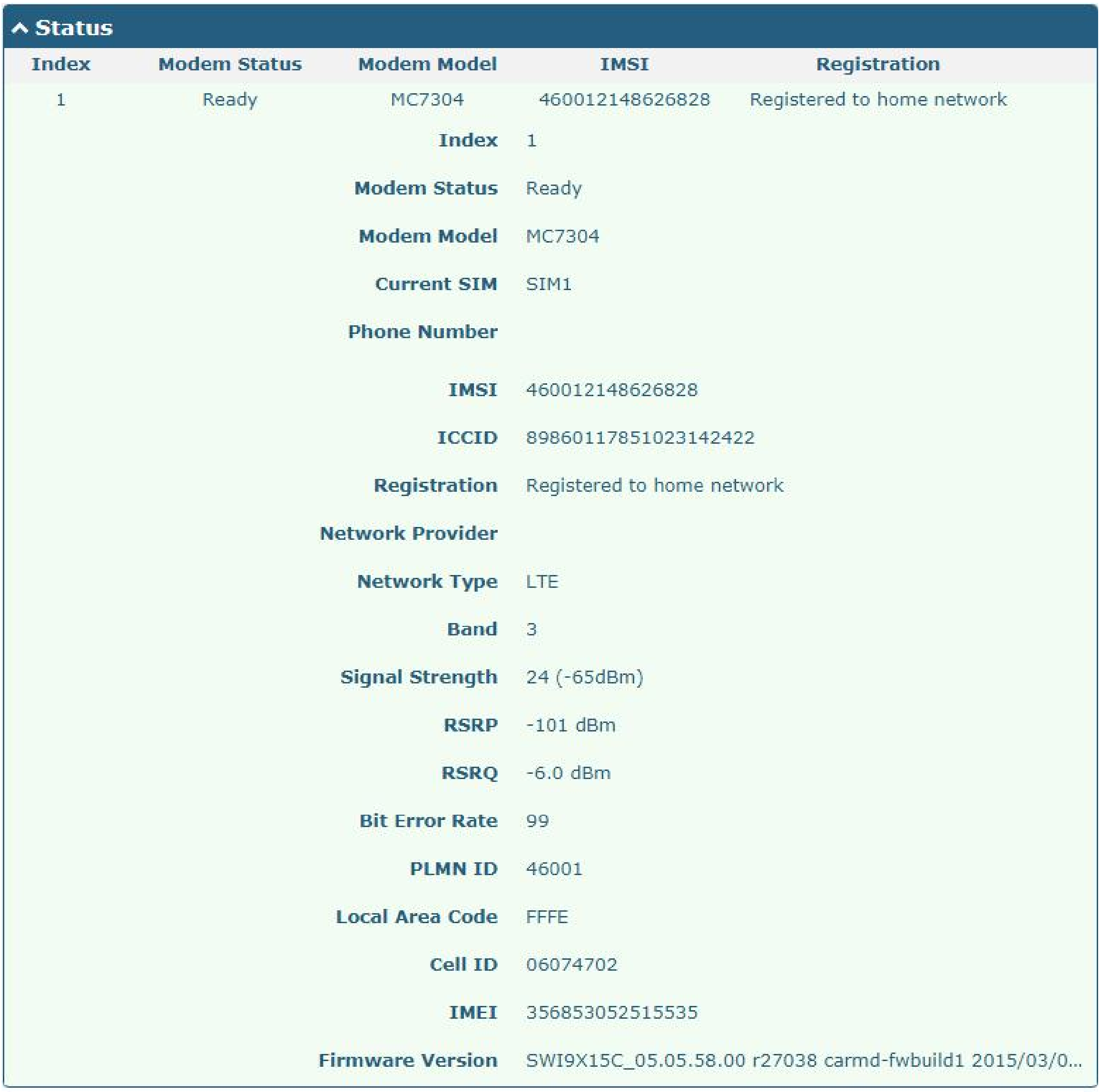
This section allows you to view the status of the cellular connection.



^ Status

Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	MC7304	460012148626828	Registered to home network

Click the row of status, the details status information will be displayed under the row.



^ Status

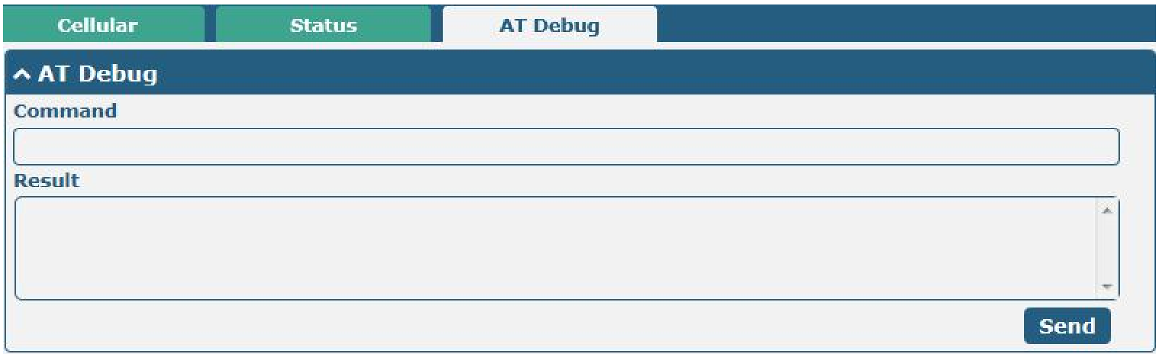
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	MC7304	460012148626828	Registered to home network

Index	1
Modem Status	Ready
Modem Model	MC7304
Current SIM	SIM1
Phone Number	
IMSI	460012148626828
ICCID	89860117851023142422
Registration	Registered to home network
Network Provider	
Network Type	LTE
Band	3
Signal Strength	24 (-65dBm)
RSRP	-101 dBm
RSRQ	-6.0 dBm
Bit Error Rate	99
PLMN ID	46001
Local Area Code	FFFE
Cell ID	06074702
IMEI	356853052515535
Firmware Version	SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/0...

Status	
Item	**Description**
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your gateway is using.
Phone Number	Show the phone number of the current SIM. **Note:** This option will be displayed if enter manually in **Cellular > Advanced Cellular Settings > SIM1/SIM2 > General Settings > Phone Number**.
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.
Band	Show the band of the current network.

Status	
Item	**Description**
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the Reference Signal Receiving Power (RSRP) of the current network.
RSRQ	Show the Reference Signal Receiving Quality (RSRQ) of the current network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the gateway.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.



AT Debug		
Item	**Description**	**Default**
Command	Enter the AT command that you want to send to cellular module in this text box.	Null
Result	Show the AT command responded by cellular module in this text box.	Null
Send	Click the button to send AT command.	--

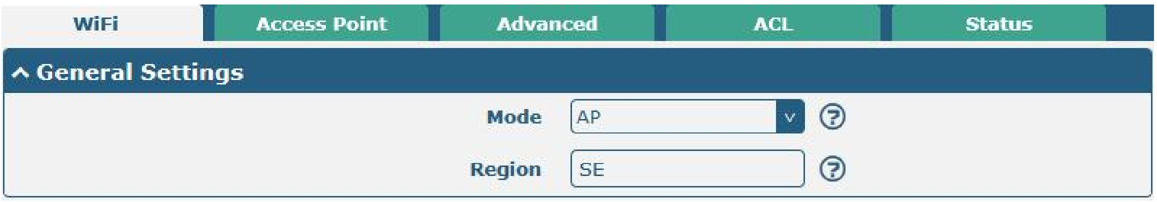
4.2.5 WiFi (Optional)

This section allows you to configure the parameters of two WiFi modes. Gateway supports either WiFi AP mode or Client mode, and defaults as AP.

WiFi AP

Configure Gateway as WiFi AP

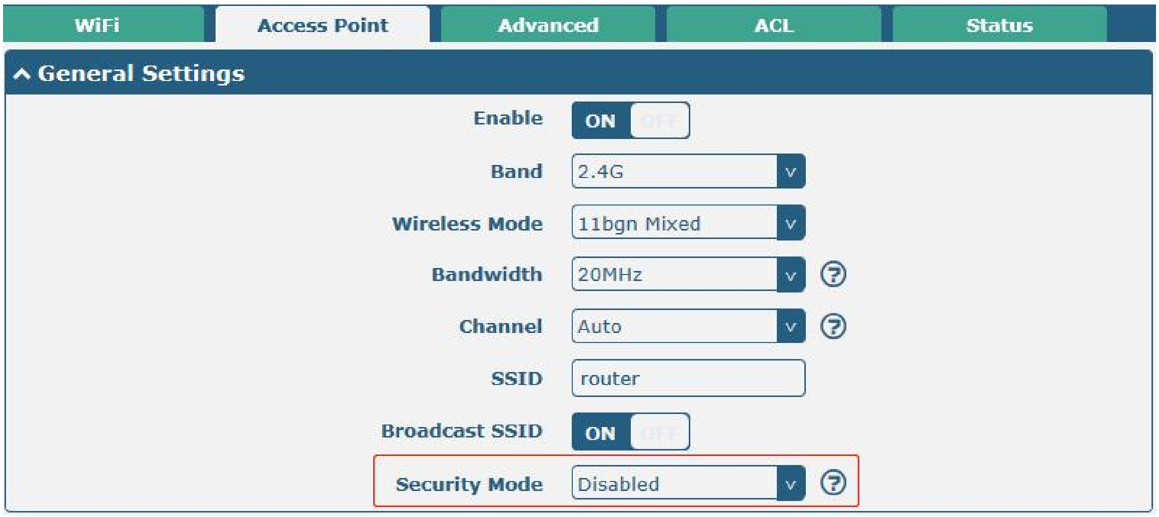
Click **Interface > WiFi > WiFi**, select “AP” as the mode and click “Submit”.



Mode	AP
Region	SE

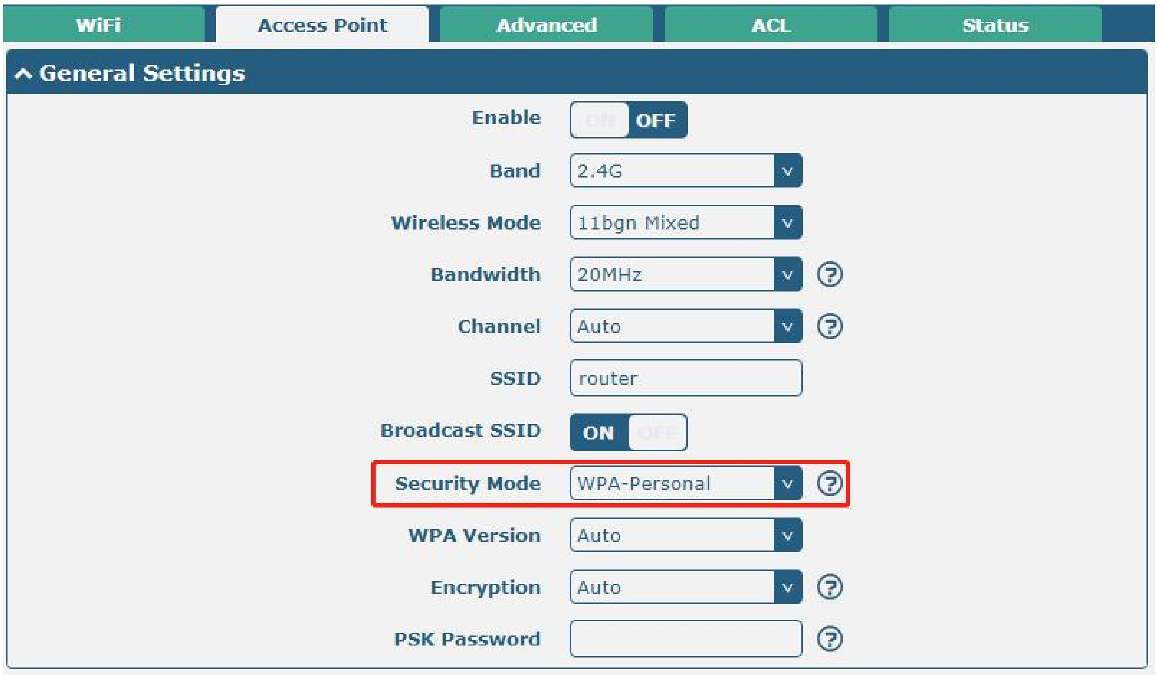
Note: Please remember to click **Save & Apply > Reboot** after finish the configuration, so that the configuration can be took effect.

Click the **Access Point** column to configure the parameters of WiFi AP. By default, the security mode is set as “Disabled”.



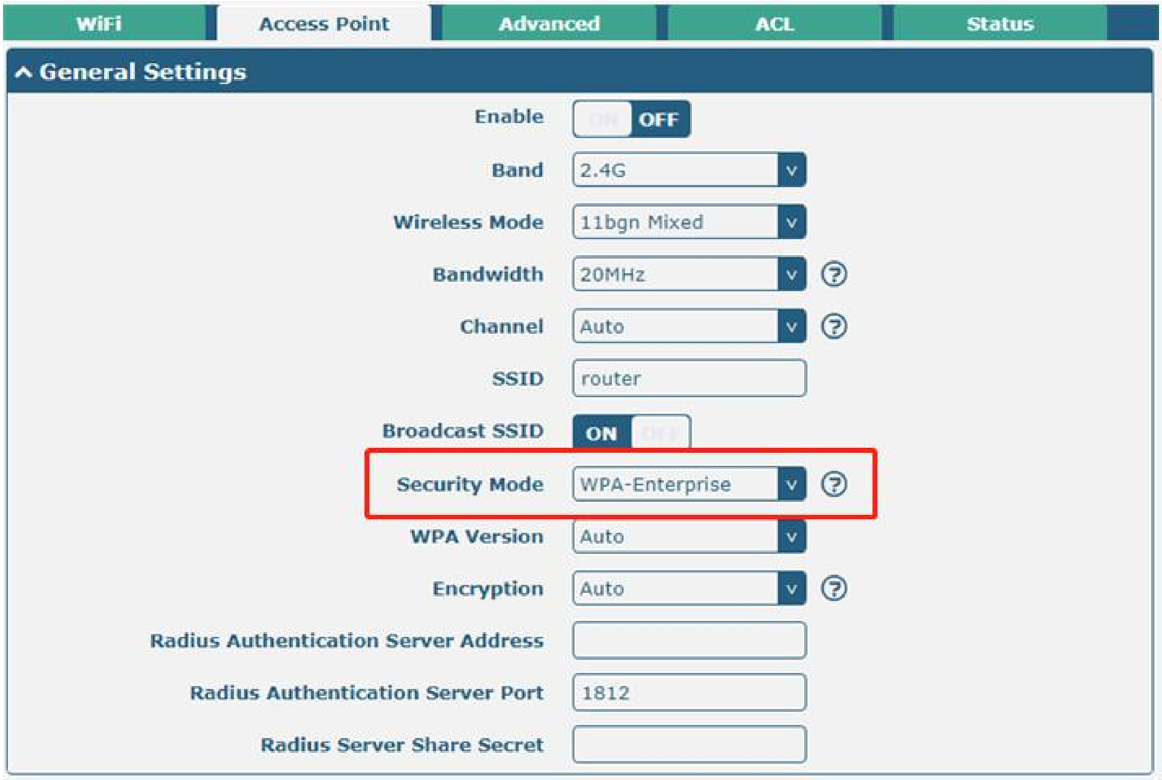
Enable	ON
Band	2.4G
Wireless Mode	11bgn Mixed
Bandwidth	20MHz
Channel	Auto
SSID	router
Broadcast SSID	ON
Security Mode	Disabled

The window is displayed as below when setting “WPA-Personal” as the security mode.



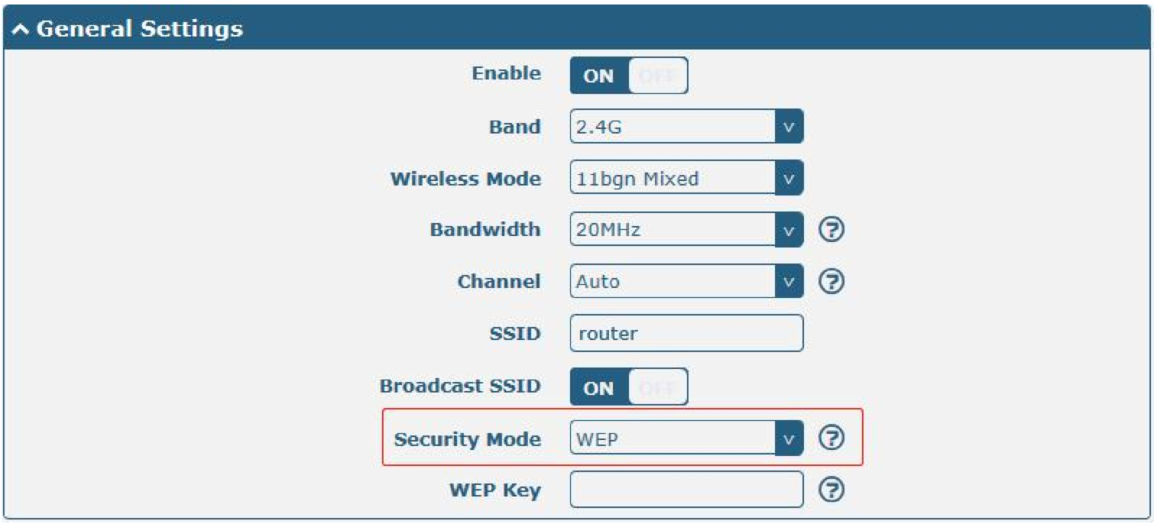
Enable	ON OFF
Band	2.4G
Wireless Mode	11bgn Mixed
Bandwidth	20MHz
Channel	Auto
SSID	router
Broadcast SSID	ON OFF
Security Mode	WPA-Personal
WPA Version	Auto
Encryption	Auto
PSK Password	

The window is displayed as below when setting “WPA-Enterprise” as the security mode.



Enable	ON OFF
Band	2.4G
Wireless Mode	11bgn Mixed
Bandwidth	20MHz
Channel	Auto
SSID	router
Broadcast SSID	ON OFF
Security Mode	WPA-Enterprise
WPA Version	Auto
Encryption	Auto
Radius Authentication Server Address	
Radius Authentication Server Port	1812
Radius Server Share Secret	

The window is displayed as below when setting “WEP” as the security mode.



Enable: ON OFF

Band: 2.4G

Wireless Mode: 11bgn Mixed

Bandwidth: 20MHz

Channel: Auto

SSID: router

Broadcast SSID: ON OFF

Security Mode: WEP

WEP Key:

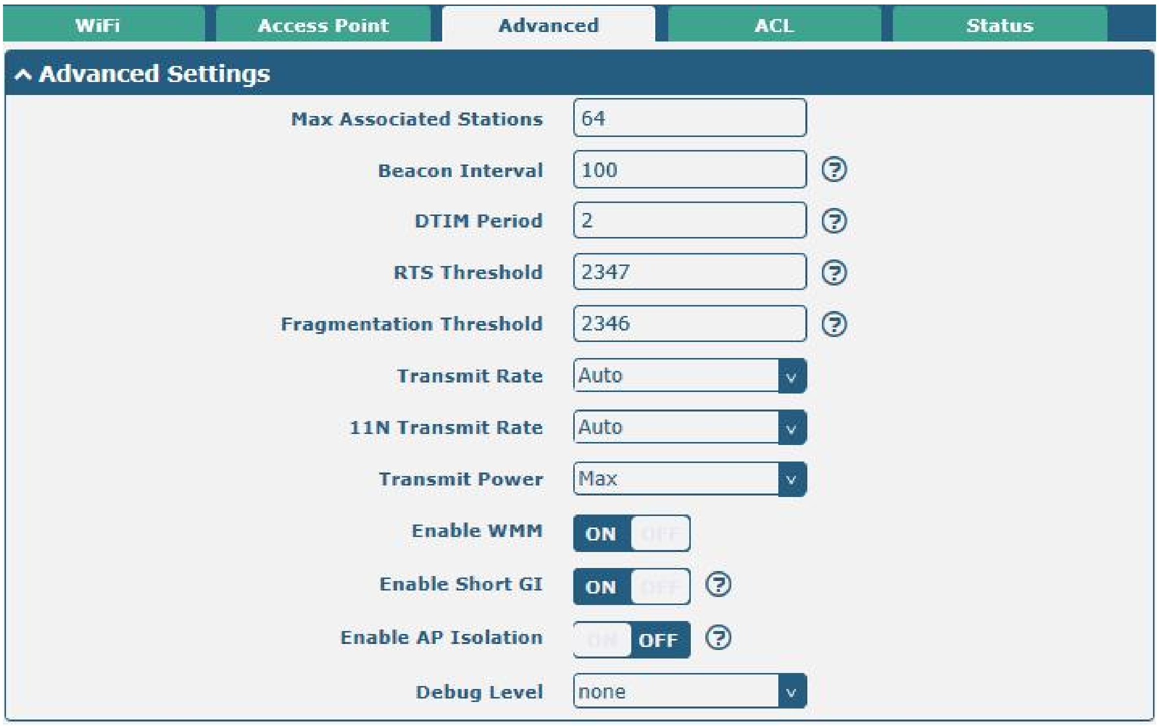
General Settings @ Access Point		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Band	Select from “2.4G” or “5G”. • 2.4G: strong fade resistance ability and penetrability, large coverage area • 5G: week fade resistance ability and penetrability, small coverage area	2.4G
Wireless Mode	When 2.4 G frequency band is selected, “11bgn Mixed”, “11b only”, “11g only” and “11n only” are optional. • 11bgn Mixed: mix three protocols for backward compatibility • 11b only: IEEE 802.11b, 11 Mbps~2.4GHz • 11g only: IEEE 802.11g, 54 Mbps~2.4GHz • 11n only: IEEE 802.11n, 450 Mbps When 5G is selected, “11n only” and “11ac only” are optional. • 11n only: IEEE 802.11n, 450 Mbps • 11ac only: IEEE 802.11n, 1.3 Gbps	11bgn Mixed/ 11n Only
Bandwidth	When 2.4G frequency band is selected, you choose “20 MHz” or “40MHz”. When 5G is frequency band is selected, select “20MHz”, “40MHz” or “80MHz”. **Note**: 40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20Mhz bandwidth.	20MHz
Channel	When 2.4G frequency band is selected, the channel that different bandwidth can choose is as follows.	auto

General Settings @ Access Point		
Item	**Description**	**Default**
	• Auto: Gateway will scan all frequency channels until the best one is found • 1~11 channel will be fixed to work with this channel Following are the frequency of 1~11 channel: 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz • The frequency of 3~11 channels of 40MHz bandwidth available channel: 3–2422 MHz 4–2427 MHz 5–2432MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz When 5G frequency band is select, the optional channels for bandwidths are as below • The frequency of 36~165 channels of 20MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz • The frequency of 36~165 channels of 40MHz bandwidth available channels: 36–5180 MHz	

General Settings @ Access Point		
Item	**Description**	**Default**
	40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz(802.11ac is unavailable) • The frequency of 36~165 channels of 80MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz(802.11ac is unavailable) **Note:** All available channels of 2.4G and 5GHz WiFi in different bandwidths are listed above. Web parameters should be configured due to the different available channels in different countries and areas.	
SSID	Enter the Service Set Identifier, the name of your wireless network. 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. Enter 1 to 32 characters.	router
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the gateway AP, you need to manually enter the SSID of gateway AP at WiFi client side.	ON

General Settings @ Access Point		
Item	**Description**	**Default**
Security Mode	Select from "Disabled", "WPA-Personal", "WPA-Enterprise" or "WEP". • Disabled: User can access the WiFi without password **Note**: It is strongly recommended for security purposes that you do not choose this kind of mode. • WPA-personal: WiFi access protection, only one password is provided for identity authentication • WPA-enterprise: provide EAP authentication interface, authenticate identity via Radius authentication server or other expansion authentications • WEP: Wired Equivalent Privacy provides encryption for wireless device's data transmission	Disabled
WPA Version	Select from "Auto", "WPA" or "WPA2". • Auto: Gateway will choose automatically the most suitable WPA version • WPA2 is a stronger security feature than WPA	Auto
Encryption	Select from "Auto", "TKIP" or "AES". • Auto: Gateway will choose automatically the most suitable encryption • TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication • AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP **Note:** The security mode will affect wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.	Auto

General Settings @ Access Point		
Item	**Description**	**Default**
PSK Password	Enter the Pre share key password. When gateway 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. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812
Radius Server Share Secret	Enter the shared secret of radius authentication server.	Null
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

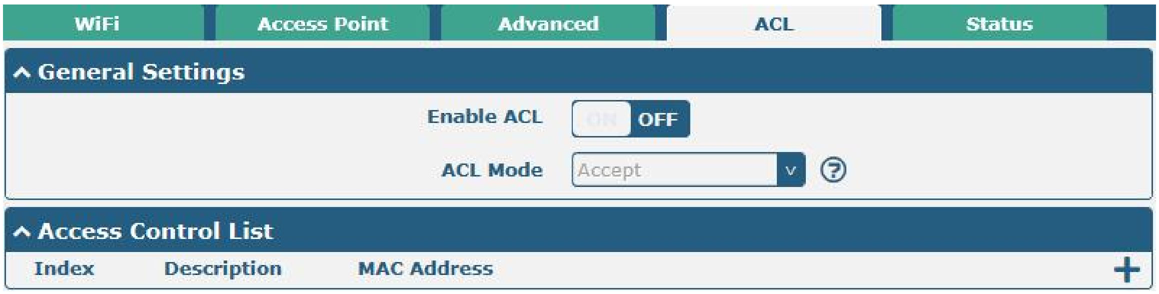


^ Advanced Settings

Max Associated Stations: 64
Beacon Interval: 100
DTIM Period: 2
RTS Threshold: 2347
Fragmentation Threshold: 2346
Transmit Rate: Auto
11N Transmit Rate: Auto
Transmit Power: Max
Enable WMM: ON
Enable Short GI: ON
Enable AP Isolation: OFF
Debug Level: none

Advanced Settings		
Item	**Description**	**Default**
Max Associated Stations	Set the max number of clients allowed to access the gateway's AP.	64
Beacon Interval	Set the interval of time in which the gateway AP broadcasts a beacon which is used for wireless network authentication.	100

Advanced Settings		
Item	**Description**	**Default**
DTIM Period	Set the delivery traffic indication message period and the gateway AP will multicast the data according to this period.	2
RTS Threshold	Set the "request to send" threshold. When the threshold set as 2347, the gateway AP will not send detection signal before sending data. And when the threshold set as 0, the gateway AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a WiFi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Set the transmit rate. You can choose Auto or specify a Transmit Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is default to "Auto".	Auto
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the gateway will isolate all connected wireless devices. The wireless device cannot access the gateway directly via WLAN.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning" or "none".	none



General Settings

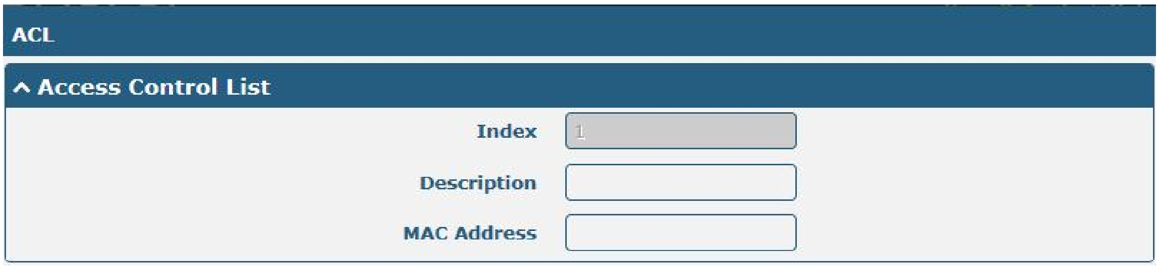
Enable ACL: OFF

ACL Mode: Accept

Access Control List

Index	Description	MAC Address

Click + to add a MAC address to the Access Control List. The maximum count for MAC address is 64.



ACL

Access Control List

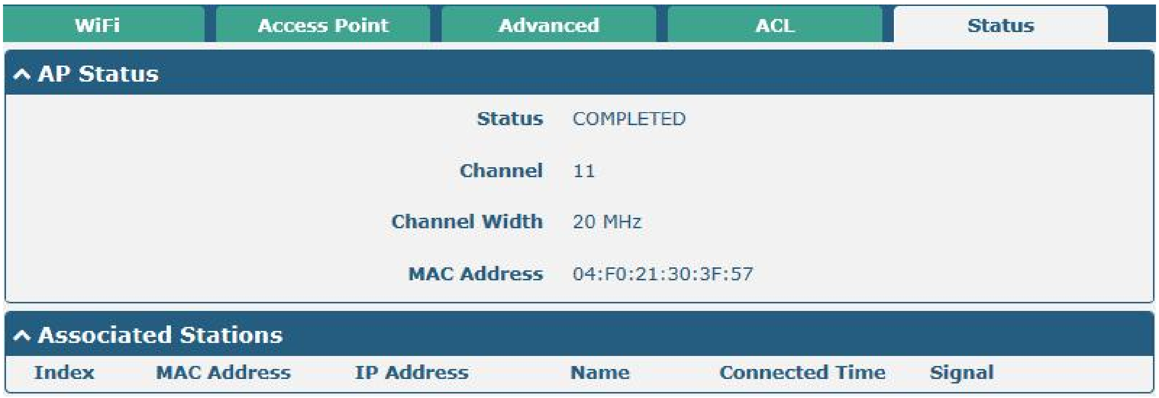
Index: 1

Description:

MAC Address:

ACL		
Item	**Description**	**Default**
General Settings		
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from "Accept" or "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**: Gateway can only allow or deny devices which are included in "Access Control List" at one time.	Accept
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here. Only support the formats: aa:bb:cc:dd:ee:ff.	Null

This section allows you to view the status of AP.



Status COMPLETED

Channel 11

Channel Width 20 MHz

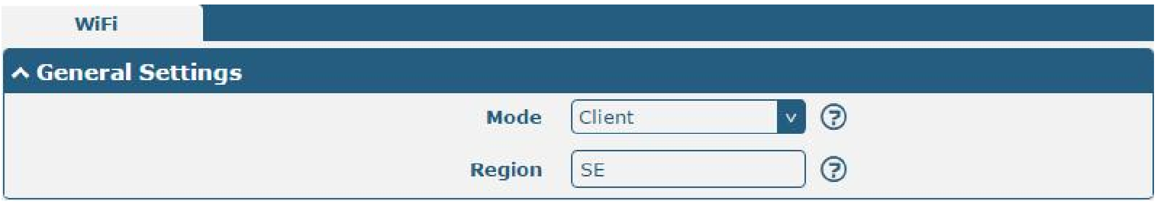
MAC Address 04:F0:21:30:3F:57

Note: WiFi is off by default. Follow the steps below to enable it and configure the gateway as WiFi client.

WiFi Client

Configure Gateway as WiFi Client

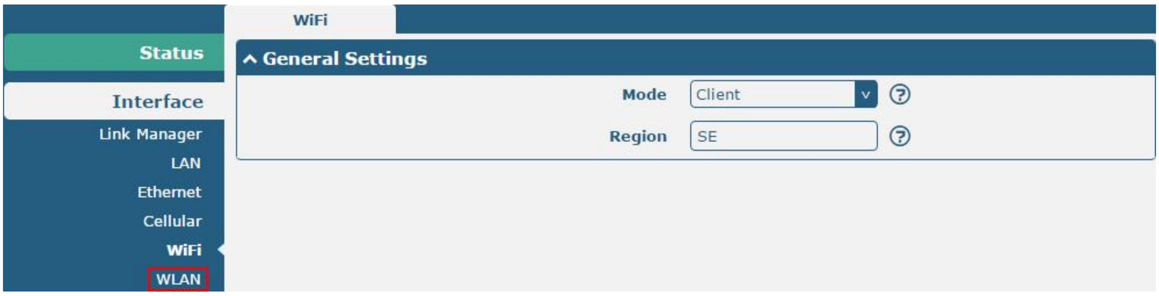
Click **Interface > WiFi > WiFi**, select "Client" as the mode and click "Submit".



Mode Client

Region SE

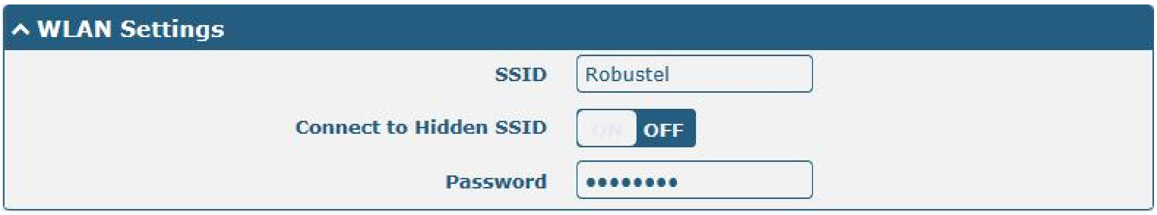
And then a "WLAN" column will appear under the Interface list.



Mode Client

Region SE

Click **Interface > Link Manager > Link Settings**, and click the edit button of WLAN, then configure its related parameters.



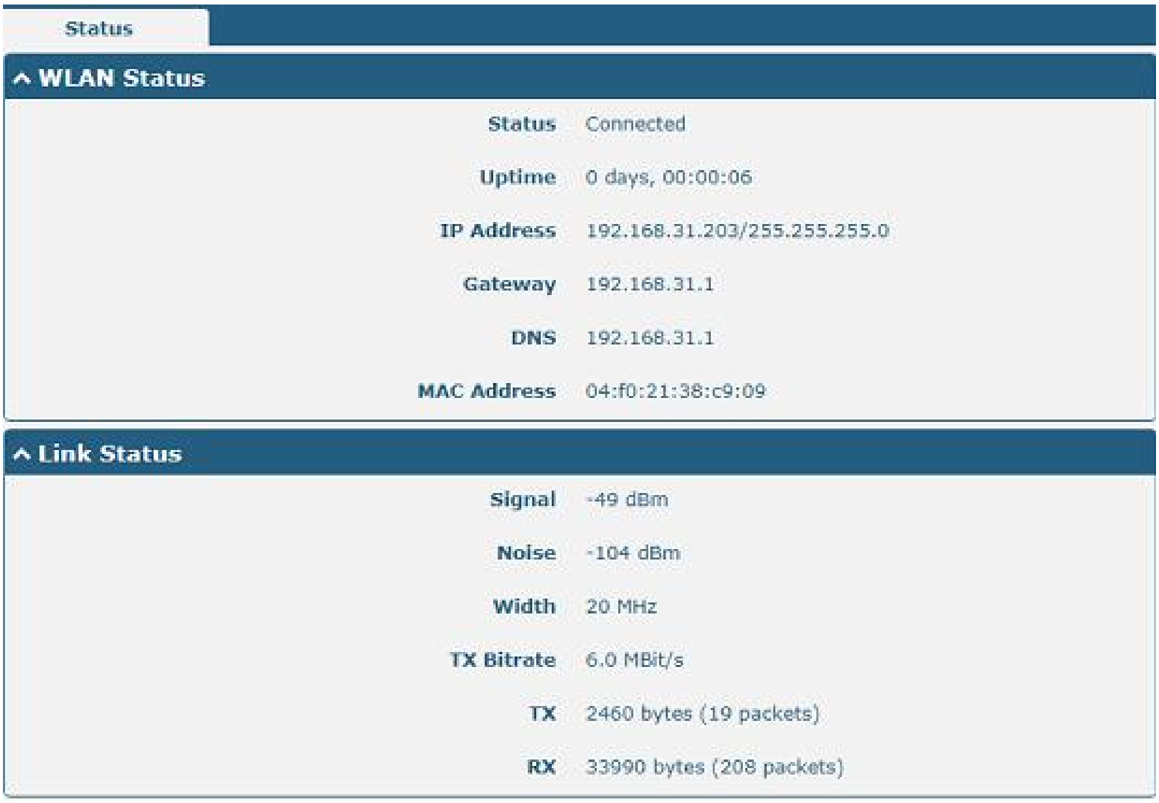
WLAN Settings

SSID Robustel

Connect to Hidden SSID OFF

Password ••••••••

Click **Interface > WLAN** to configure the parameters of WiFi Client after setting the mode as Client. Please remember to click **Save & Apply > Reboot** after finish the configuration, so that the configuration can be took effect.

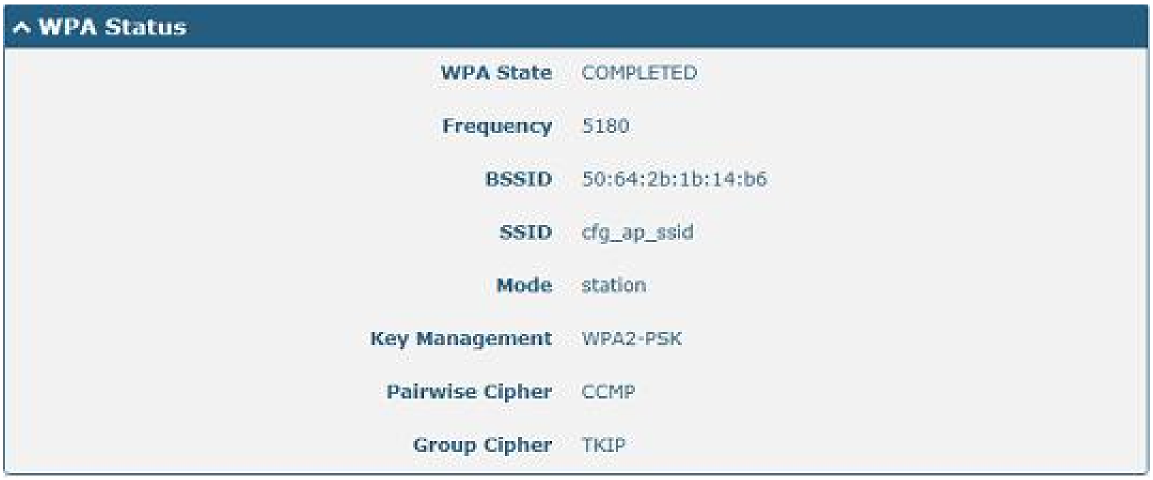


WLAN Status

Status	Connected
Uptime	0 days, 00:00:06
IP Address	192.168.31.203/255.255.255.0
Gateway	192.168.31.1
DNS	192.168.31.1
MAC Address	04:f0:21:38:c9:09

Link Status

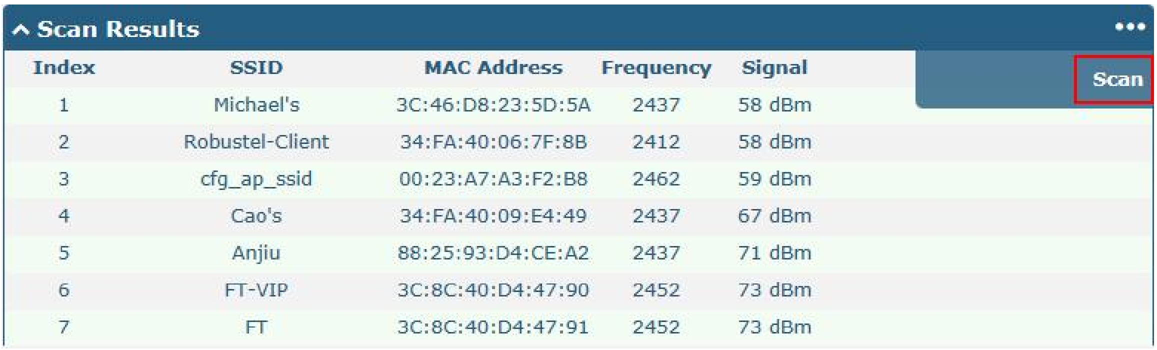
Signal	-49 dBm
Noise	-104 dBm
Width	20 MHz
TX Bitrate	6.0 MBit/s
TX	2460 bytes (19 packets)
RX	33990 bytes (208 packets)



^ WPA Status

WPA State	COMPLETED
Frequency	5180
BSSID	50:64:2b:1b:14:b6
SSID	cfg_ap_ssid
Mode	station
Key Management	WPA2-PSK
Pairwise Cipher	CCMP
Group Cipher	TKIP

This window allows you to scan for all available SSIDs in your area and connect to one of those shown on the "Scan Results" list.



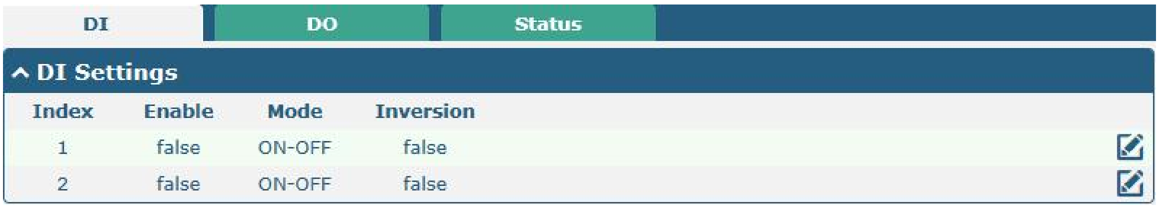
^ Scan Results

Index	SSID	MAC Address	Frequency	Signal
1	Michael's	3C:46:D8:23:5D:5A	2437	58 dBm
2	Robustel-Client	34:FA:40:06:7F:8B	2412	58 dBm
3	cfg_ap_ssid	00:23:A7:A3:F2:B8	2462	59 dBm
4	Cao's	34:FA:40:09:E4:49	2437	67 dBm
5	Anjiu	88:25:93:D4:CE:A2	2437	71 dBm
6	FT-VIP	3C:8C:40:D4:47:90	2452	73 dBm
7	FT	3C:8C:40:D4:47:91	2452	73 dBm

4.2.6 DIDO

This section allows you to set the DI and DO parameters. Digital Input and Digital Output are the specific interfaces for MEG5000. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

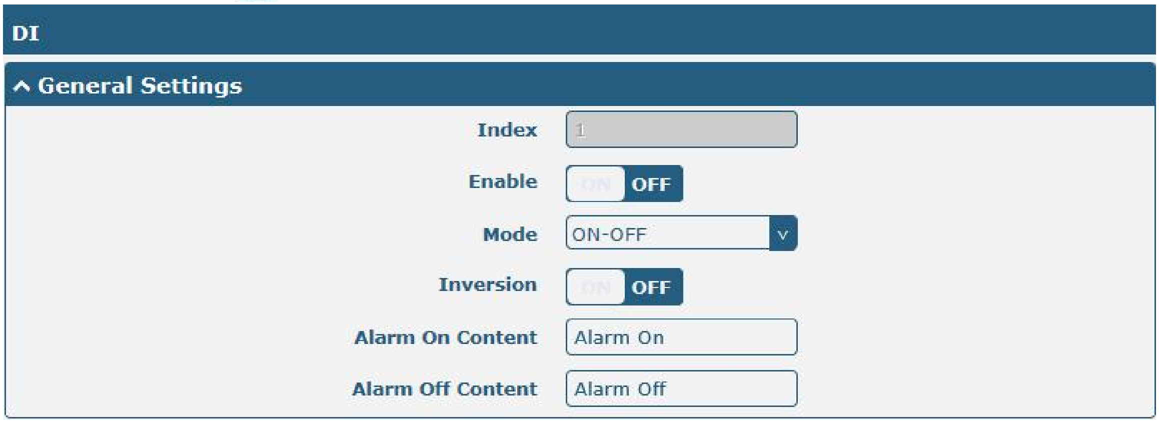
DI



^ DI Settings

Index	Enable	Mode	Inversion
1	false	ON-OFF	false
2	false	ON-OFF	false

Click the right-most 📝 button of index 1 as below. The default mode is “ON-OFF”.

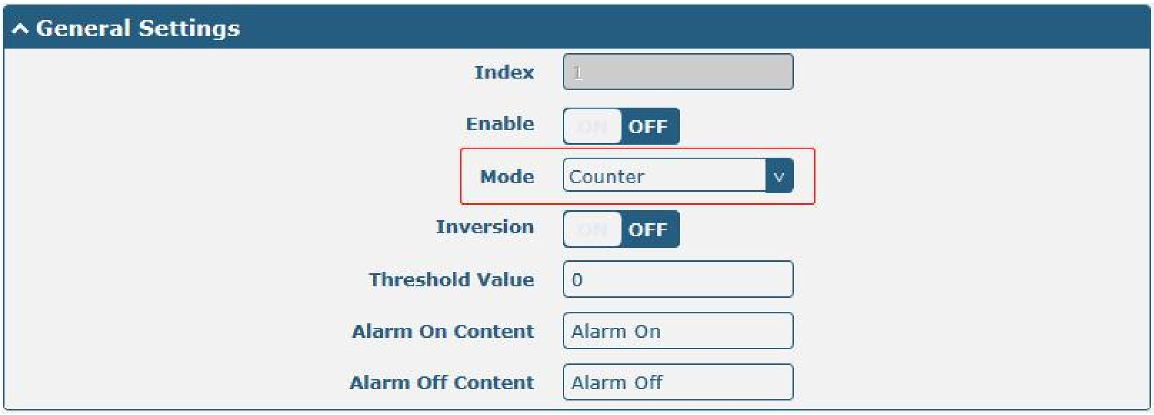


DI

General Settings

Index	1
Enable	ON OFF
Mode	ON-OFF
Inversion	ON OFF
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

The window is displayed as below when choosing “Counter” as the mode.



General Settings

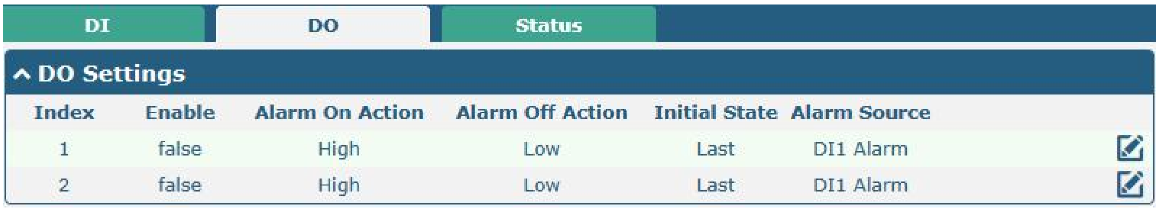
Index	1
Enable	ON OFF
Mode	Counter
Inversion	ON OFF
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

General Settings @ DI		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DI.	OFF
Mode	Select from “ON-OFF” or “Counter”. • ON-OFF: DI interface support ON and OFF mode (high or low level electrical) trigger DI alarm. The mode default to ON, and OFF mode is available only when enabling the inversion feature ON—Under this mode, DI alarm status will be triggered to ON when DI interface open from GND or input a high level electrical (logic 1), on the contrary DI alarm status will be trigged to OFF when DI interface connect to GND or input a low level electrical (logic 0) OFF—Under this mode, DI alarm status will be triggered to ON when DI interface connect to GND or input a low level electrical (logic 0), on the contrary DI alarm status will be trigged to OFF when DI interface open from GND or input a high level electrical (logic 1) • Counter: Event counter mode	ON-OFF
Inversion	Click the toggle button to enable/disable this option. Enable to set DI mode as OFF mode.	OFF
Threshold Value	Set the threshold vale. It will trigger alarm when event counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm	Null

General Settings @ DI		
Item	**Description**	**Default**
	again. Enter 0 to 65535 digits. (0=will not trigger alarm) **Note**: This option is only available when DI under the "Counter" mode.	
Alarm on Content	When alarm is on, show its content	Alarm On
Alarm off Content	When alarm is off, show its content.	Alarm Off

Note: It defaults as high alarm, while turns to low alarm after enabling the "Inversion" button.

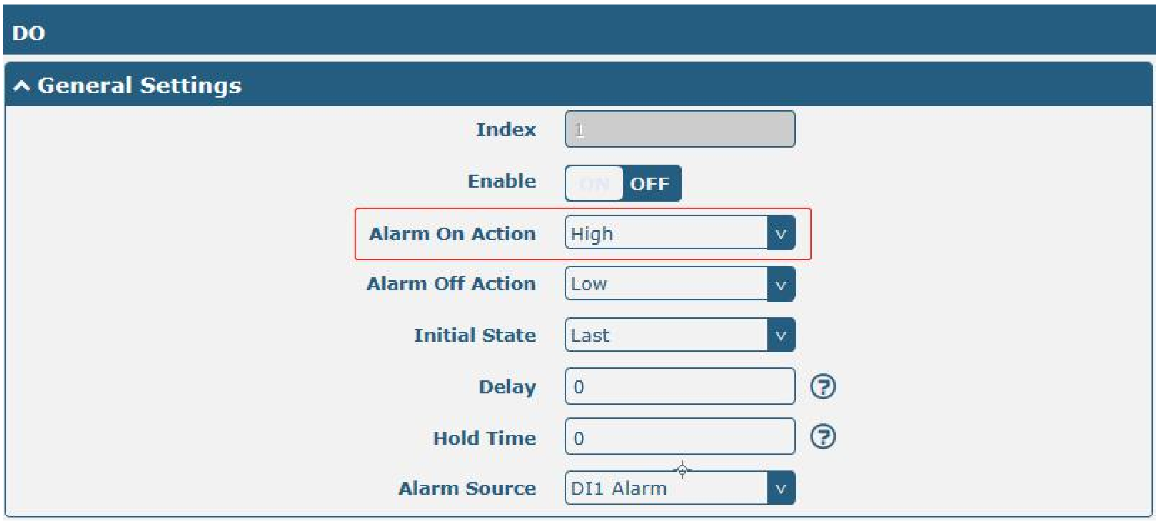
DO



DO Settings

Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source
1	false	High	Low	Last	DI1 Alarm
2	false	High	Low	Last	DI1 Alarm

Click to enter the DO configuration window.

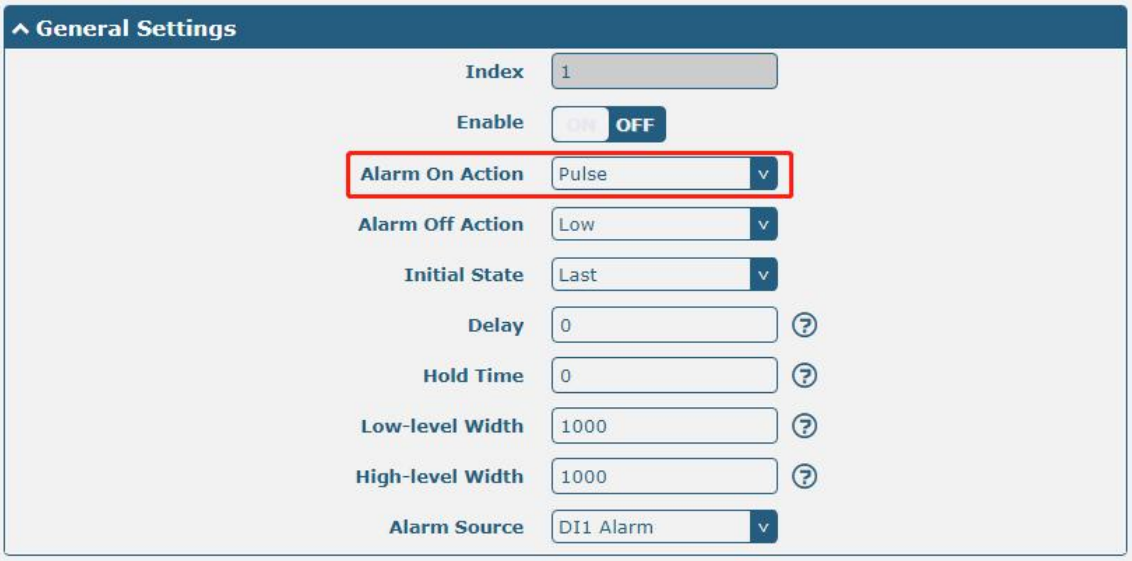


DO

General Settings

Index	1
Enable	ON OFF
Alarm On Action	High
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Alarm Source	DI1 Alarm

The window is displayed as below when choosing "Pulse" as the alarm on action.



General Settings

Index: 1

Enable: ON OFF

Alarm On Action: Pulse

Alarm Off Action: Low

Initial State: Last

Delay: 0

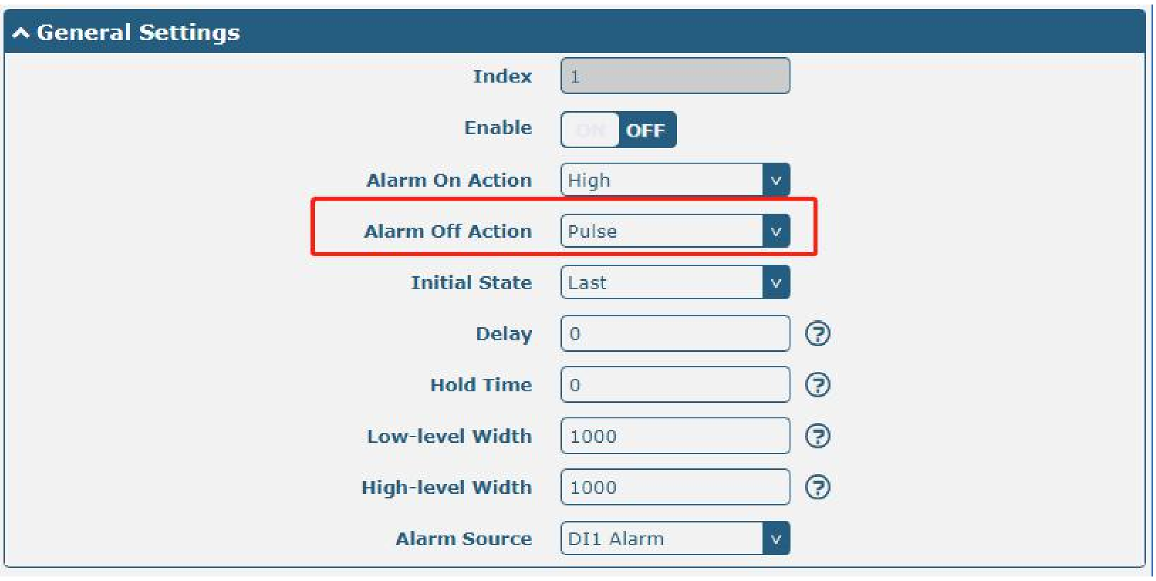
Hold Time: 0

Low-level Width: 1000

High-level Width: 1000

Alarm Source: DI1 Alarm

The window is displayed as below when choosing "Pulse" as the alarm off action.



General Settings

Index: 1

Enable: ON OFF

Alarm On Action: High

Alarm Off Action: Pulse

Initial State: Last

Delay: 0

Hold Time: 0

Low-level Width: 1000

High-level Width: 1000

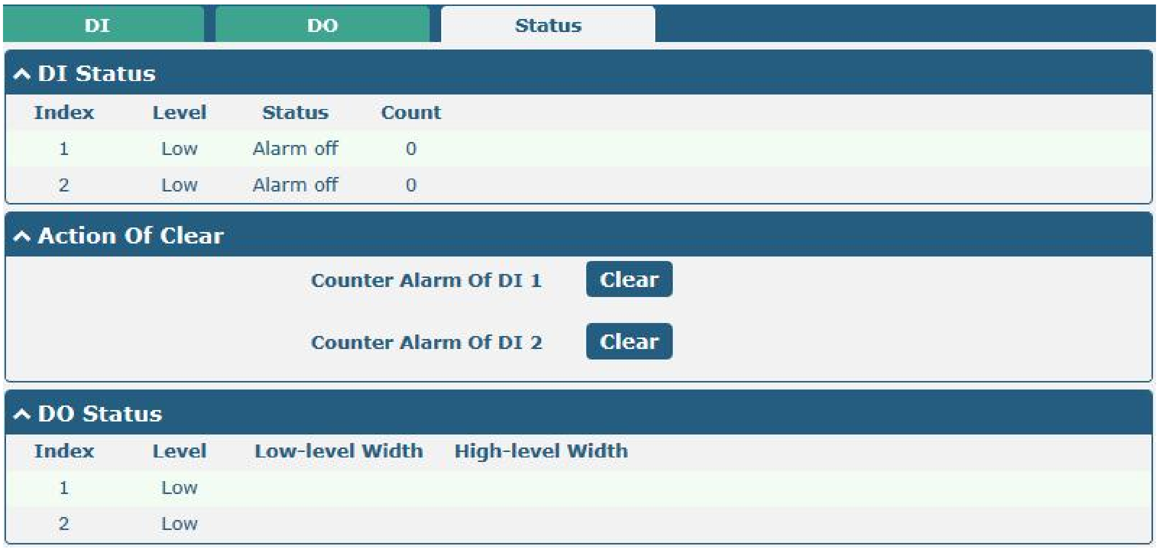
Alarm Source: DI1 Alarm

General Settings @ DO		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from "High", "Low" or "Pulse". • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	High

General Settings @ DO		
Item	**Description**	**Default**
Alarm Off Action	Digital Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. • High: a high electrical level output • Low: a low electrical level output • Pulse: Generates a square wave as specified in the pulse mode parameters when triggered	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. • Last: DO’s status will consist with the status of last power off • High: DO interface is in high electrical level • Low: DO interface is in low electrical level	Low
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000ms. (0=generate pulse without delay)	0
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 255 seconds. (0=keep on until the next action)	0
Low-level Width	Set the low-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1000 to 3000 ms.	1000
High-level Width	Set the high-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1000 to 3000 ms.	1000
Alarm Source	Digital Output initiates according to different alarm source. Selected from “DI1 Alarm”, “DI2 Alarm”. DI1/DI2 Alarm: Digital Output triggers the related action when there is alarm from Digital Input.	DI1 Alarm

Status

This window allows you to view the status of DO and DI interfaces. It also can clear the counter alarm of DI in here. Click Clear button to clear DI1 or DI2 monthly usage statistics info for counter alarm.



^ DI Status

Index	Level	Status	Count
1	Low	Alarm off	0
2	Low	Alarm off	0

^ Action Of Clear

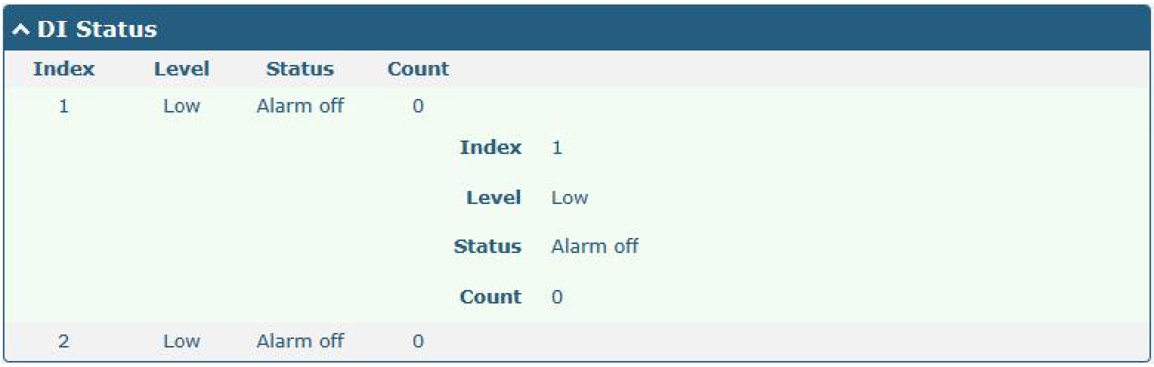
Counter Alarm Of DI 1 Clear

Counter Alarm Of DI 2 Clear

^ DO Status

Index	Level	Low-level Width	High-level Width
1	Low		
2	Low		

Click one row to view.



^ DI Status

Index	Level	Status	Count
1	Low	Alarm off	0

Index 1

Level Low

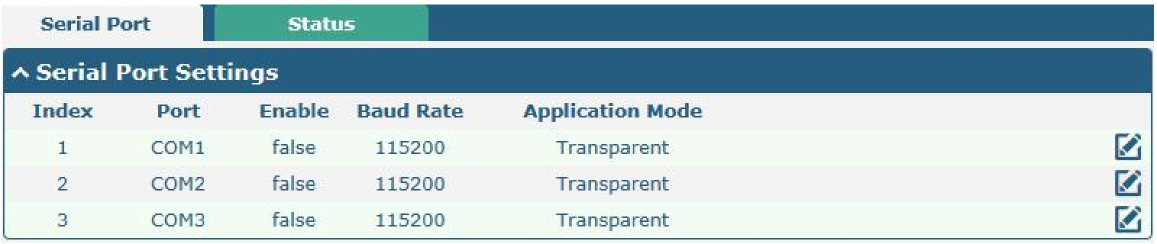
Status Alarm off

Count 0

Index	Level	Status	Count
2	Low	Alarm off	0

4.2.7 Serial Port

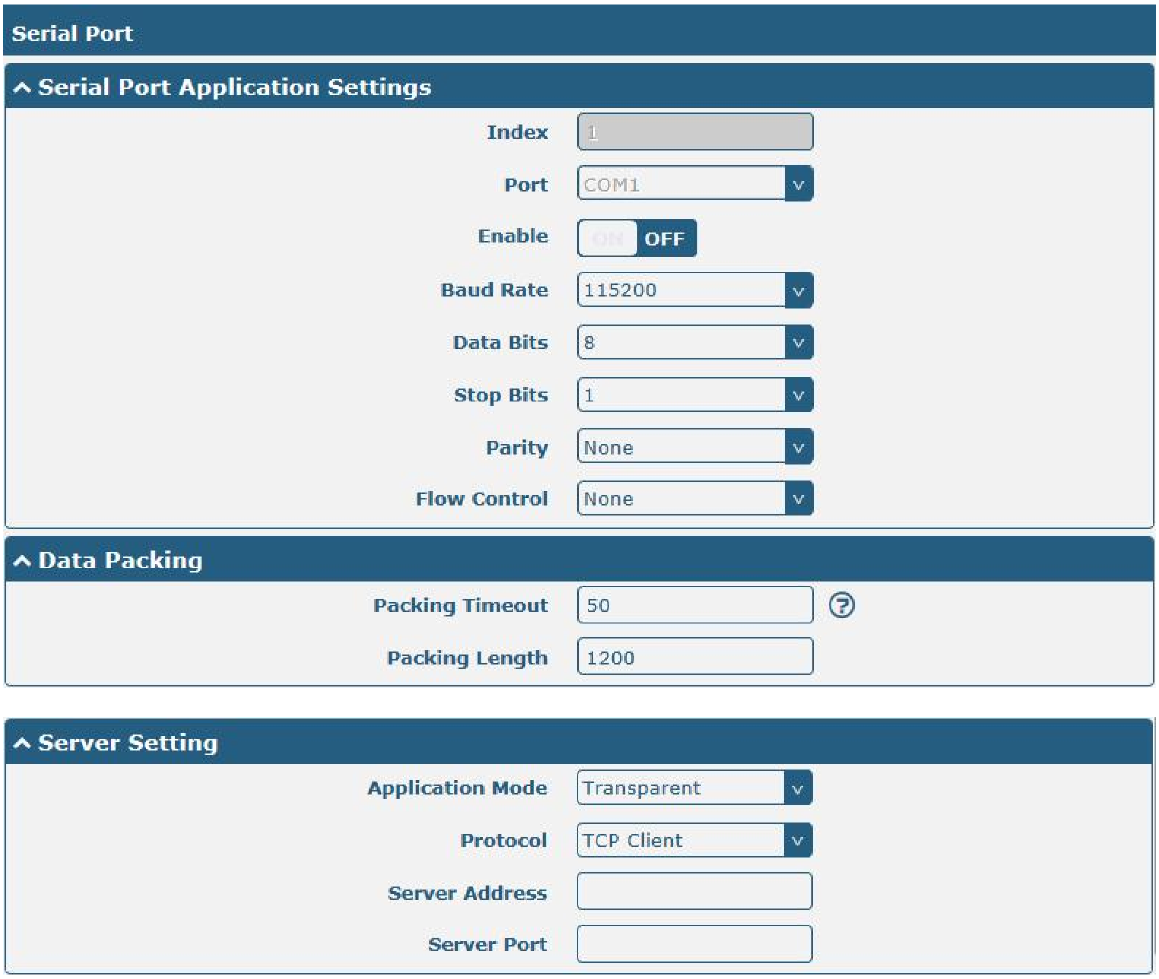
This section allows you to set the serial port parameters. MEG5000 supports two RS-232s and one RS-485. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission.



^ Serial Port Settings

Index	Port	Enable	Baud Rate	Application Mode	
1	COM1	false	115200	Transparent	✎
2	COM2	false	115200	Transparent	✎
3	COM3	false	115200	Transparent	✎

The window is displayed as below when Clicking the right-most ✎ button of COM1.



Serial Port

^ Serial Port Application Settings

Index	1
Port	COM1
Enable	ON OFF
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

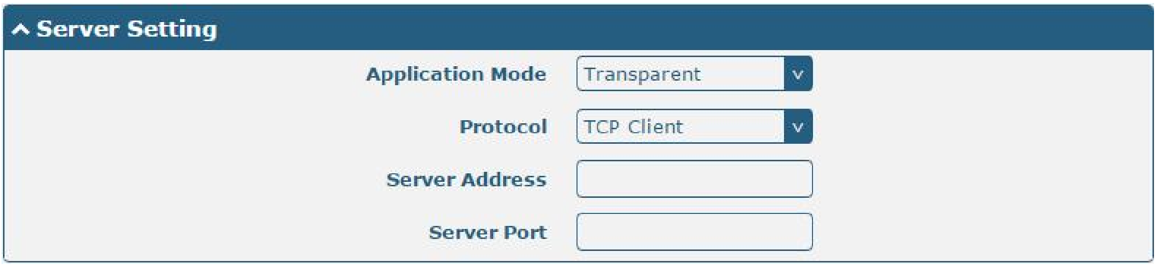
^ Data Packing

Packing Timeout	50
Packing Length	1200

^ Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

- The window is displayed as below when choosing "Transparent" as the application mode and "TCP Client" as the protocol.



Server Setting

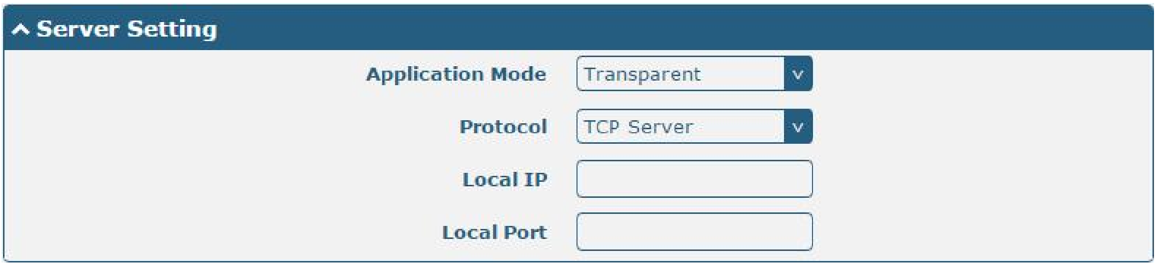
Application Mode: Transparent

Protocol: TCP Client

Server Address

Server Port

The window is displayed as below when choosing "Transparent" as the application mode and "TCP Server" as the protocol.



Server Setting

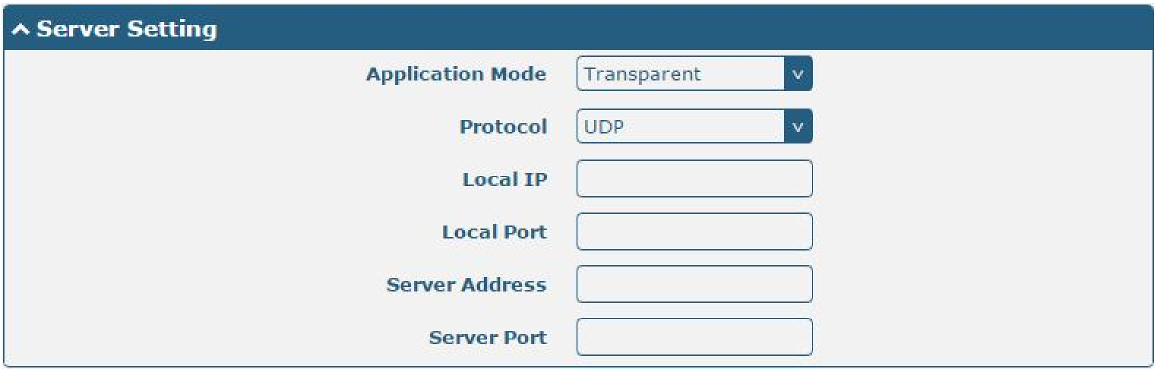
Application Mode: Transparent

Protocol: TCP Server

Local IP

Local Port

The window is displayed as below when choosing "Transparent" as the application mode and "UDP" as the protocol.



Server Setting

Application Mode: Transparent

Protocol: UDP

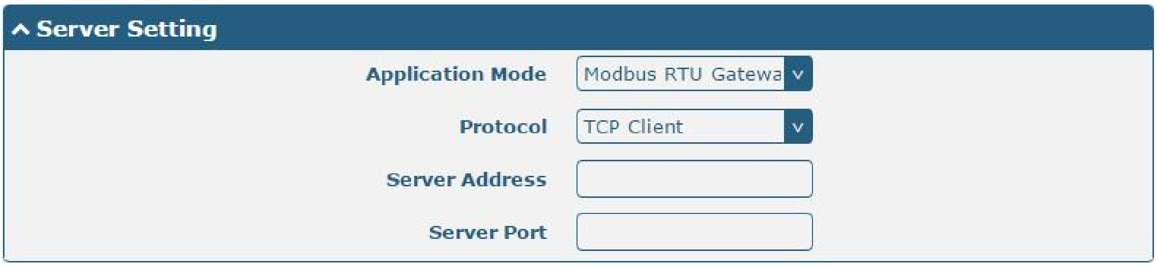
Local IP

Local Port

Server Address

Server Port

- The window is displayed as below when choosing "Modbus RTU Gateway" as the application mode and "TCP Client" as the protocol.



Server Setting

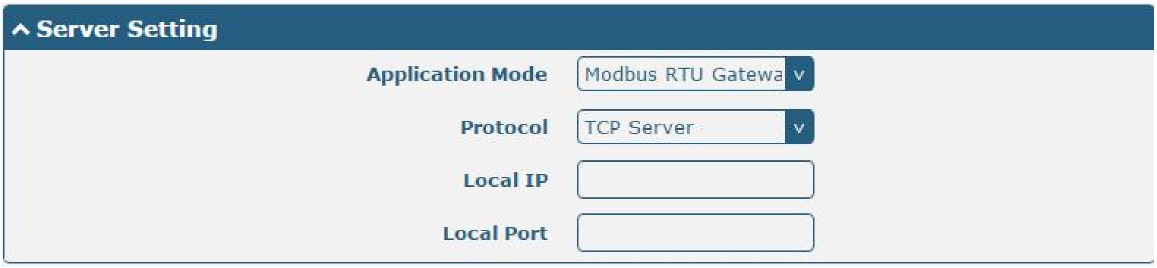
Application Mode: Modbus RTU Gatewa

Protocol: TCP Client

Server Address

Server Port

The window is displayed as below when choosing "Modbus RTU Gateway" as the application mode and "TCP Server" as the protocol.



^ Server Setting

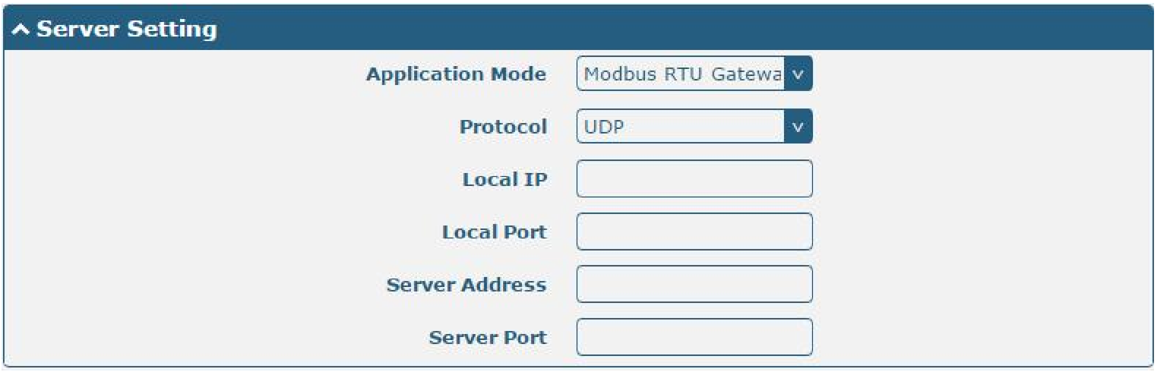
Application Mode: Modbus RTU Gatewa

Protocol: TCP Server

Local IP

Local Port

The window is displayed as below when choosing “Modbus RTU Gateway” as the application mode and “UDP” as the protocol.



^ Server Setting

Application Mode: Modbus RTU Gatewa

Protocol: UDP

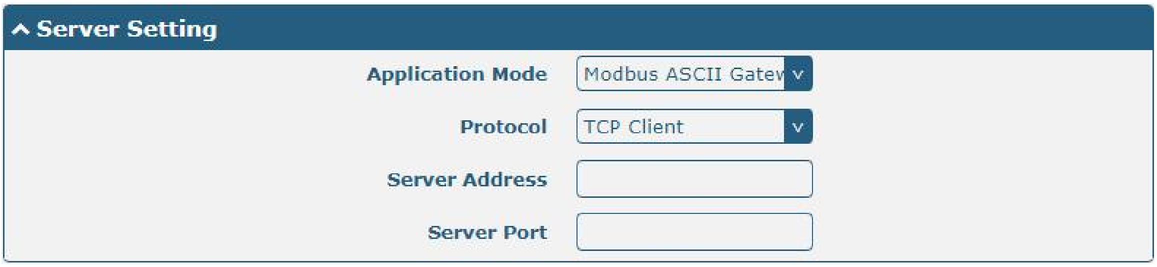
Local IP

Local Port

Server Address

Server Port

- The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Client” as the protocol.



^ Server Setting

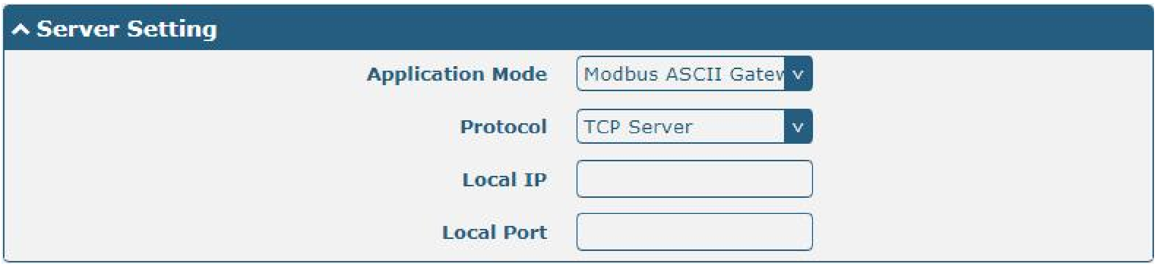
Application Mode: Modbus ASCII Gatev

Protocol: TCP Client

Server Address

Server Port

The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Server” as the protocol.



^ Server Setting

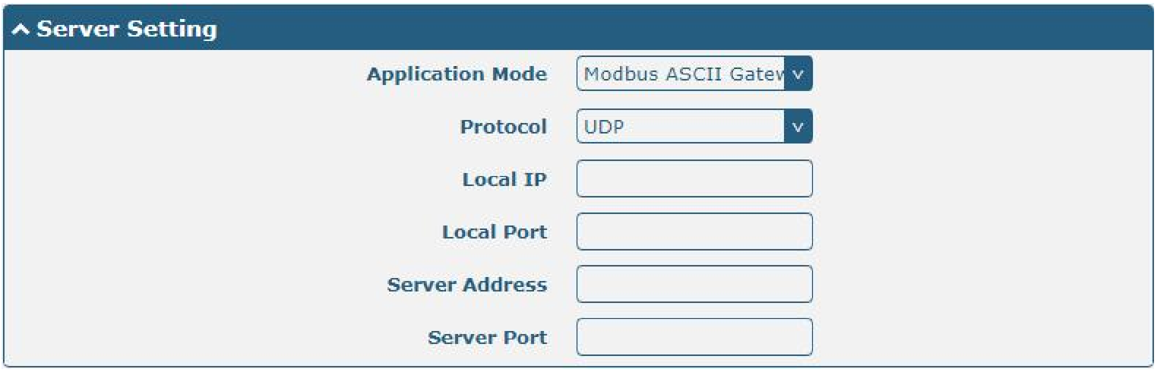
Application Mode: Modbus ASCII Gatev

Protocol: TCP Server

Local IP

Local Port

The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “UDP” as the protocol.



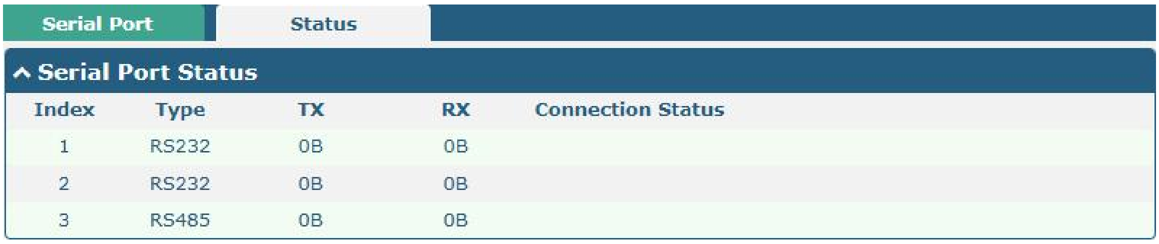
^ Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

Serial Port		
Item	**Description**	**Default**
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	--
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" , "115200" or "230400". Note: BCOM1 and COM2 do not support 230400 Baud Rate	115200
Data Bits	Select from "7" or "8".	8
Stop Bits	Select from "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow Control	Select from "None", "Software" or "Hardware". Note: software flow control and hardware flow control is not support.	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. **Note**: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200
Server Setting		
Application Mode	Select from "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway". • Transparent: Gateway will transmit the serial data transparently • Modbus RTU Gateway: Gateway will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa • Modbus ASCII Gateway: Gateway will translate the Modbus	Transparent

Serial Port		
Item	**Description**	**Default**
	ASCII data to Modbus TCP data and sent out, and vice versa	
Protocol	Select from "TCP Client", "TCP Server", "UDP" or "Robustlink". • TCP Client: Gateway works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name • TCP Server: Gateway works as TCP server, listening for connection request from TCP client • UDP: Gateway works as UDP client	TCP Client
Server Address	Enter the address of server which will receive the data sent from gateway's serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter gateway's LAN IP which will forward to the internet port of gateway.	Null
Local Port @ Transparent	Enter the port of gateway's LAN IP.	Null
Local IP @ Modbus	Enter the local IP of under Modbus mode.	Null
Local Port @ Modbus	Enter the local port of under Modbus mode.	Null

Click the "Status" column to view the current serial port type.



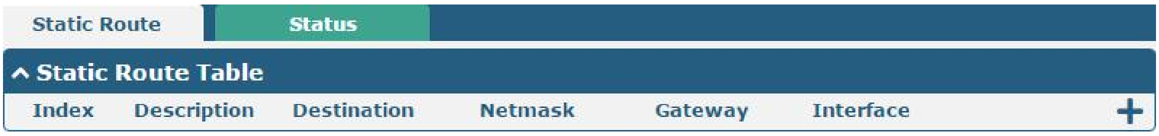
Serial Port Status

Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS232	0B	0B	
3	RS485	0B	0B	

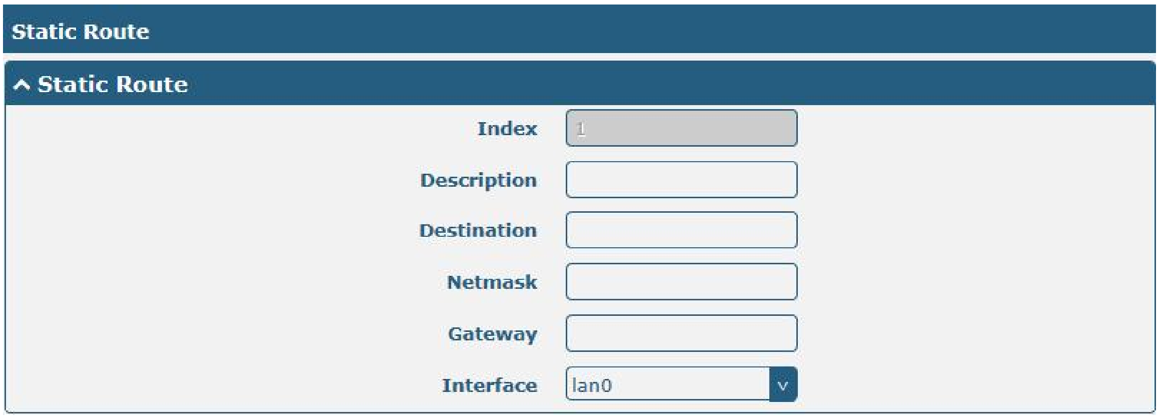
4.3 Network

4.3.1 Route

This section allows you to set the static route. Static route is a form of routing that occurs when a gateway uses a manually-configured routing entry, rather than information from a dynamic routing traffic. Route Information Protocol (RIP) is widely used in small network with stable use rate. Open Shortest Path First (OSPF) is made gateway within a single autonomous system and used in large network.



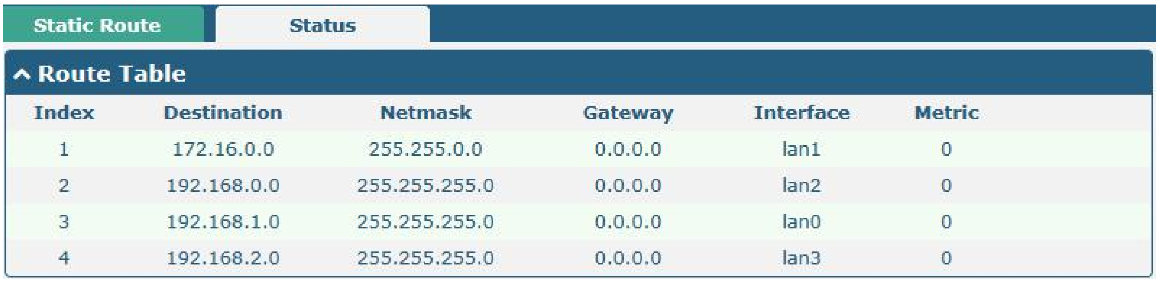
Click + to add static routes. The maximum count is 20.



Index	1
Description	
Destination	
Netmask	
Gateway	
Interface	lan0

Static Route		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan

This window allows you to view the status of route.

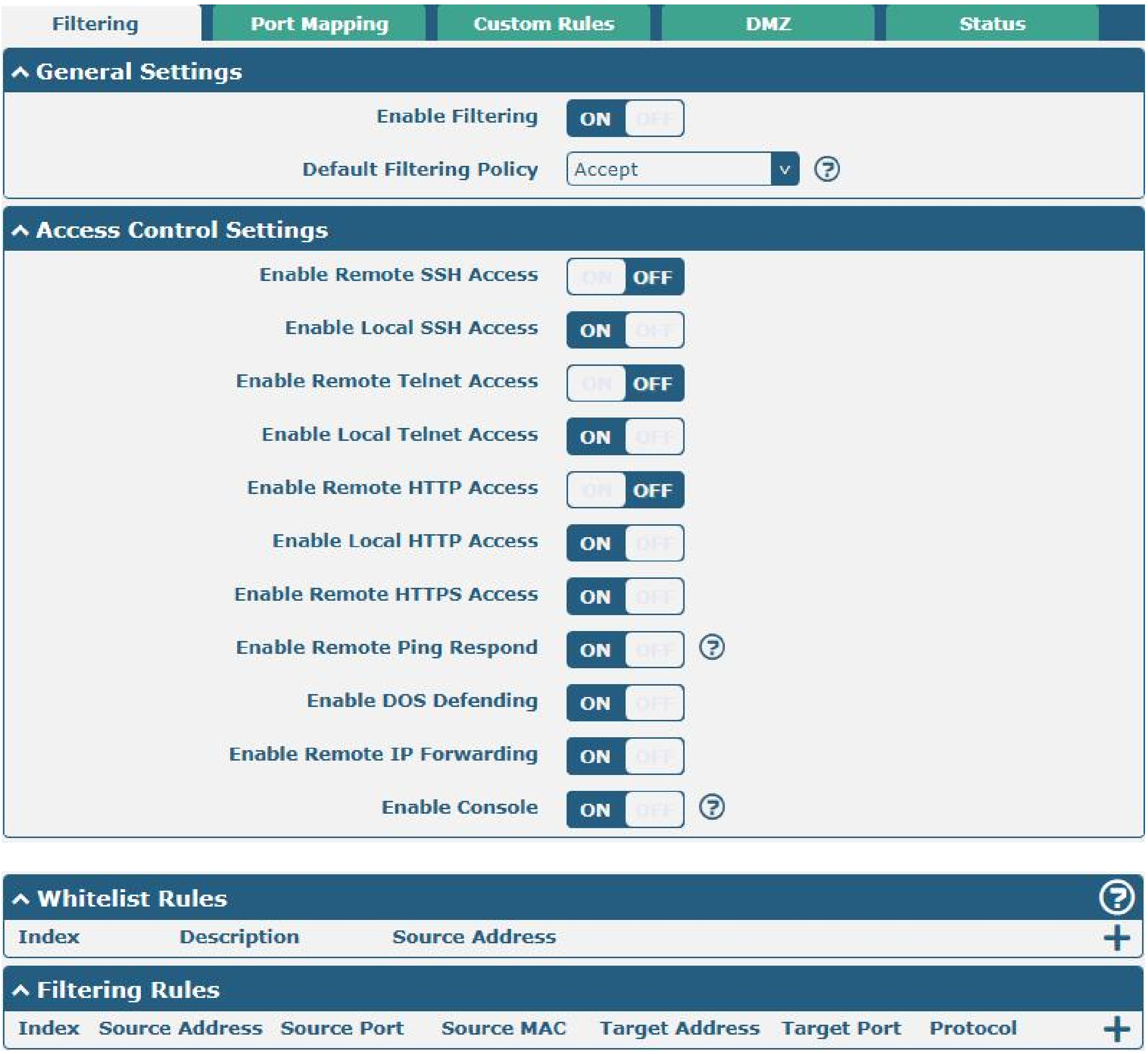


Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	172.16.0.0	255.255.0.0	0.0.0.0	lan1	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan2	0
3	192.168.1.0	255.255.255.0	0.0.0.0	lan0	0
4	192.168.2.0	255.255.255.0	0.0.0.0	lan3	0

4.3.2 Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ. The filtering rules can be used to either accept or block certain users or ports from accessing your gateway. The window is displayed as below when Clicking **Network > Firewall > Filter.**



General Settings

Enable Filtering	ON
Default Filtering Policy	Accept

Access Control Settings

Enable Remote SSH Access	OFF
Enable Local SSH Access	ON
Enable Remote Telnet Access	OFF
Enable Local Telnet Access	ON
Enable Remote HTTP Access	OFF
Enable Local HTTP Access	ON
Enable Remote HTTPS Access	ON
Enable Remote Ping Respond	ON
Enable DOS Defending	ON
Enable Remote IP Forwarding	ON
Enable Console	ON

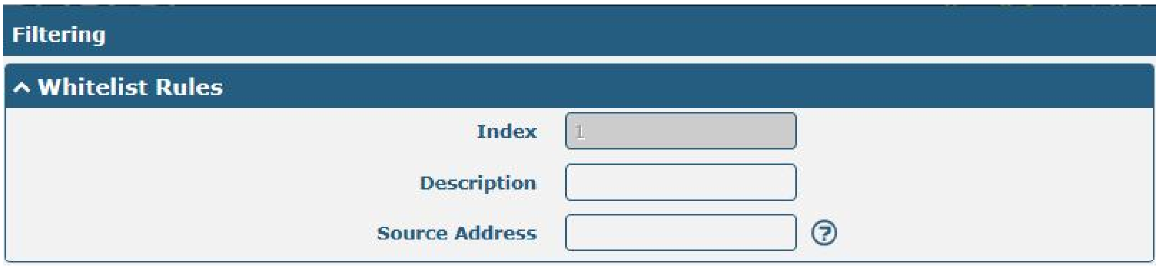
Whitelist Rules

Index	Description	Source Address

Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol

Click + to add a whitelist rule. The maximum count is 50.

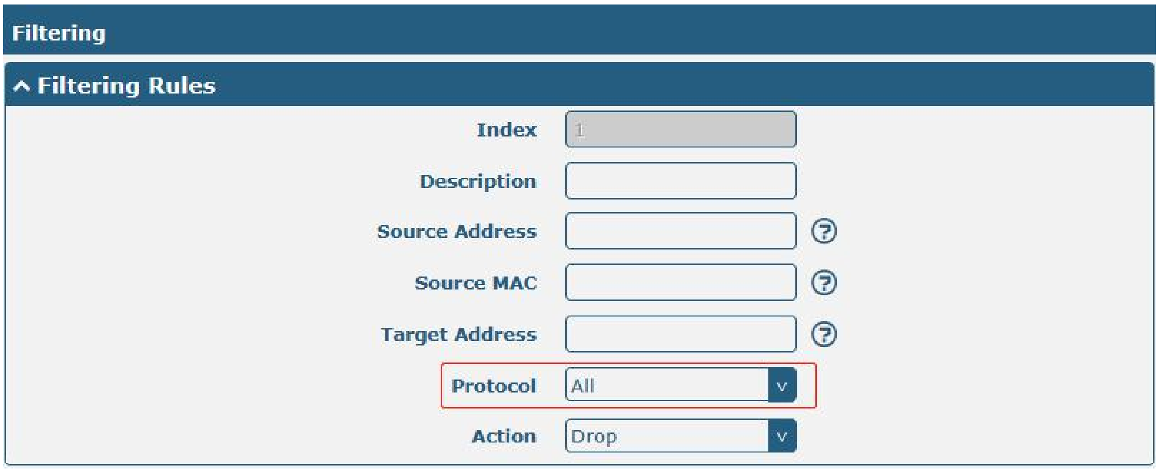


Filtering

^ Whitelist Rules

Index	1
Description	
Source Address	

Click + to add a filtering rule. The maximum count is 50. The window is displayed as below when defaulting “All” or choosing “ICMP” as the protocol. Here take “All” as an example.

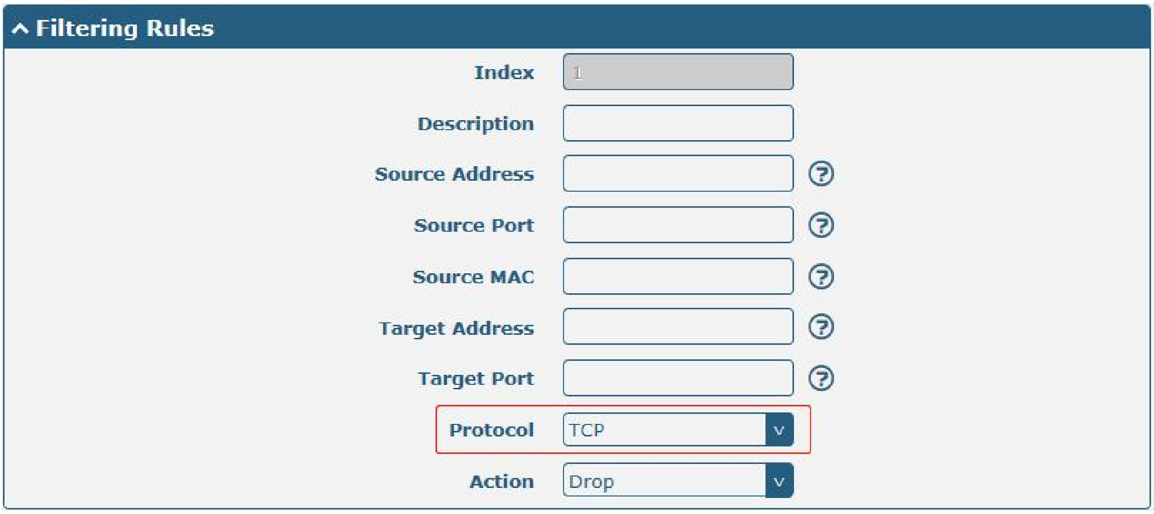


Filtering

^ Filtering Rules

Index	1
Description	
Source Address	
Source MAC	
Target Address	
Protocol	All
Action	Drop

The window is displayed as below when choosing “TCP”, “UDP” or “TCP-UDP” as the protocol. Here take “TCP” as an example.



^ Filtering Rules

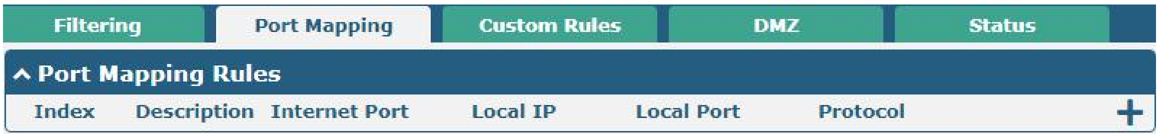
Index	1
Description	
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	TCP
Action	Drop

Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON

Filtering		
Item	**Description**	**Default**
Default Filtering Policy	Select from "Accept" or "Drop". Cannot be changed when filtering rules table is not empty. • Accept: Gateway will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Gateway will drop all the connecting requests except the hosts which fit the accept filter list	Accept
Access Control Settings		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the gateway remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the gateway locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the gateway remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the gateway locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the gateway remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the gateway locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the gateway remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the gateway will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the gateway will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable Remote IP Forwarding	Click the toggle button to enable data package of WAN port to be forwarded to LAN port of gateway.	OFF
Enable Console	Click the toggle button to enable/disable this option.	ON
Whitelist Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist.	Null
Source Address	Enter the source address for this whitelist.	Null
Filtering Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter the target address which the access originator wants to access.	Null
Target Port	Enter the target port which the access originator wants to access.	Null

Filtering		
Item	**Description**	**Default**
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP” or “TCP-UDP”. **Note**: It is recommended that you choose “All” if you don’t know which protocol of your application to use.	All
Action	Select from “Accept” or “Drop”. • Accept: When Default Filtering Policy is drop, gateway will drop all the connecting requests except the hosts which fit this accept filtering list • Drop: When Default Filtering Policy is accept, gateway will accept all the connecting requests except the hosts which fit this drop filtering list	Drop

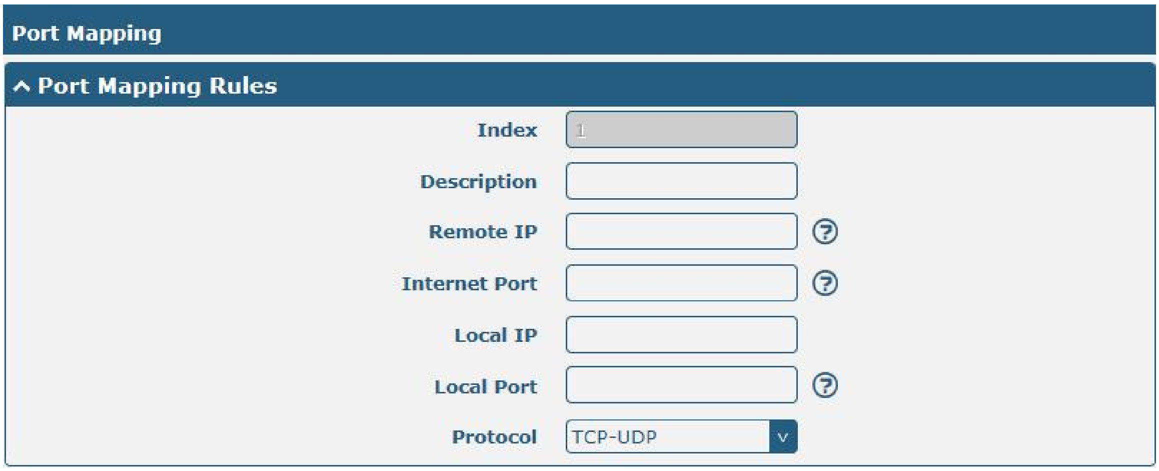
Port mapping refers to manually define which port of intranet IP will receive data from some internet ports. Click **Internet > Firewall > Port Mapping**.



^ Port Mapping Rules

Index	Description	Internet Port	Local IP	Local Port	Protocol	+

Click + to add port mapping rules. The maximum rule count is 50.



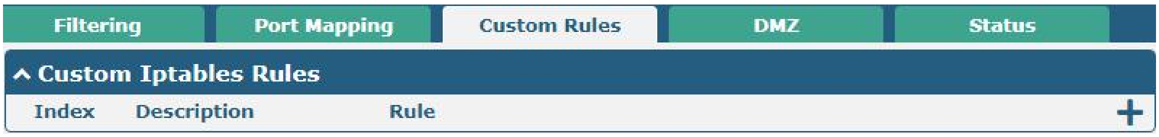
Port Mapping

^ Port Mapping Rules

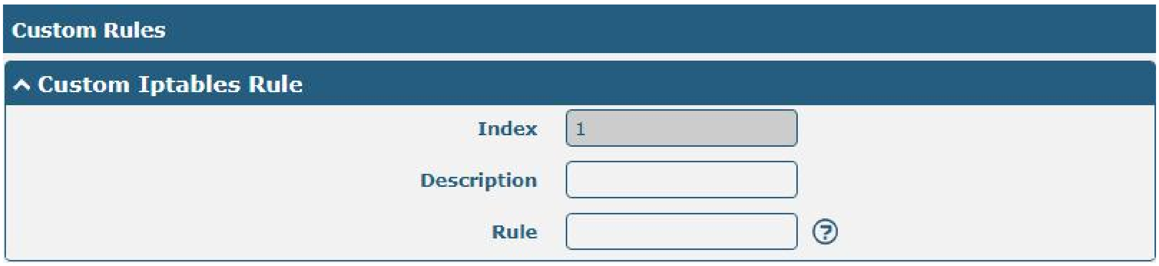
Index	1
Description	
Remote IP	
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

Port Mapping Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of gateway which can be accessed by other hosts from internet.	Null
Local IP	Enter gateway’s LAN IP which will forward to the internet port of gateway.	Null
Local Port	Enter the port of gateway’s LAN IP.	Null
Protocol	Select from “TCP”, “UDP” or “TCP-UDP” as your application required.	TCP-UDP

"Custom Rules" meets customer's demand for personal filtering of IP package, filter data usage of a website for example. Users can add any iptables rules which meet the iptables rule format standard in this list.



Click + to add custom rules. The maximum rule count is 50.

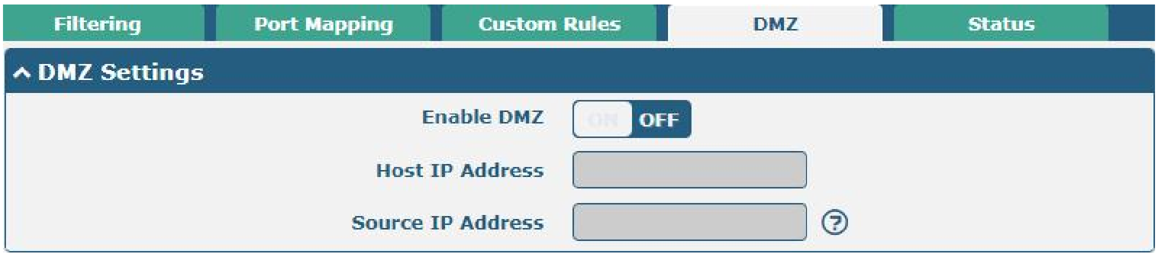


Index: 1

Custom Iptables Rule		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this rule.	Null
Rule	Specify one iptables rule. e.g -I INPUT -s 192.168.0.2 -j ACCEPT	Null

DMZ（Demilitarized Zone）means isolation zones or unmilitary area. It is a buffer between a non-secure system and a security system in order to solve the problem that the access user of the external network cannot access the internal network server after installing the firewall. A DMZ host is an intranet host that has open access to a specified address except for the ports that are occupied and forwarded.

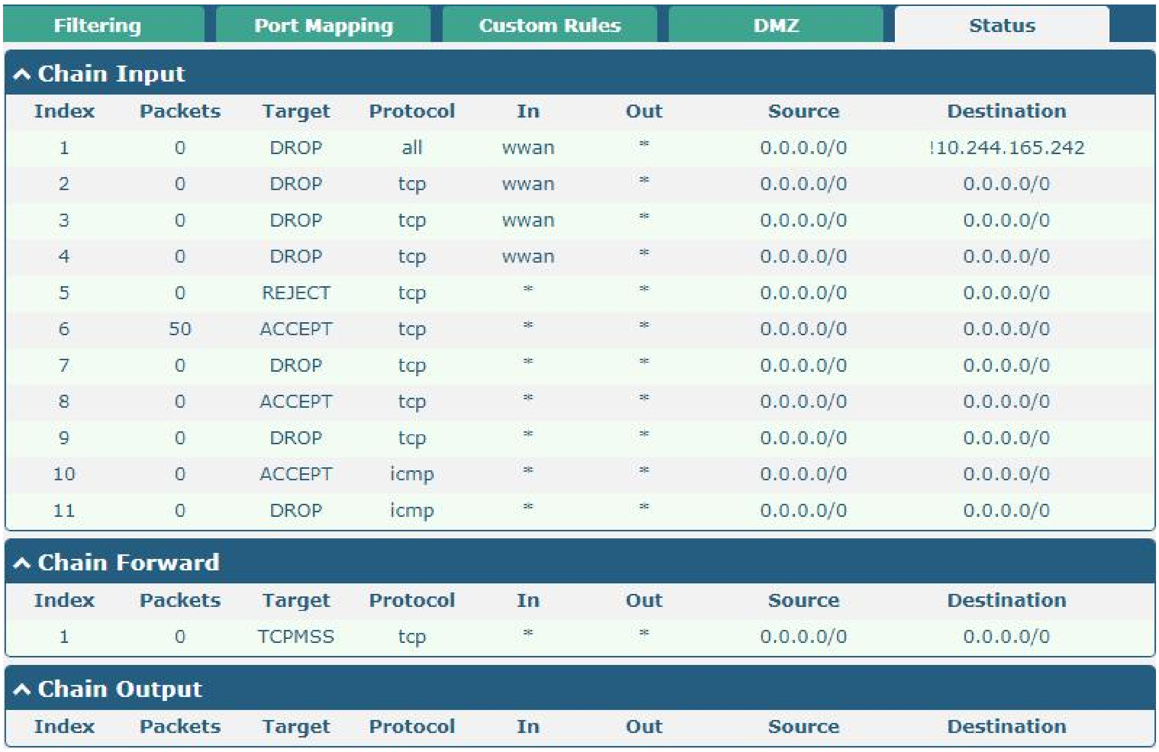
The window is displayed as below when Clicking **Network > Firewall > DMZ.**



Enable DMZ: ON OFF

DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ. 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 on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

Click “Status” to view all rules of INPUT, FORWARD and OUTPUT.



^ Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	wwan	*	0.0.0.0/0	!10.244.165.242
2	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
4	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
5	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	50	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Forward

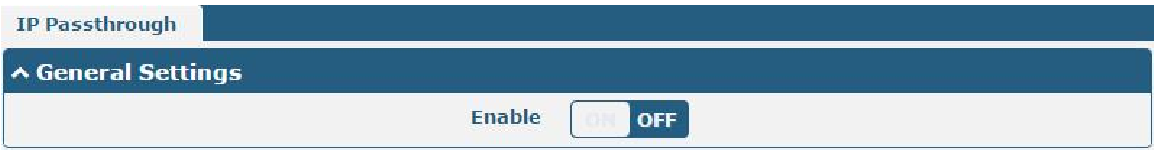
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

^ Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

4.3.3 IP Passthrough

Click **Network > IP Passthrough > IP Passthrough** to enable or disable the IP Pass-through option.



^ General Settings

Enable ON OFF

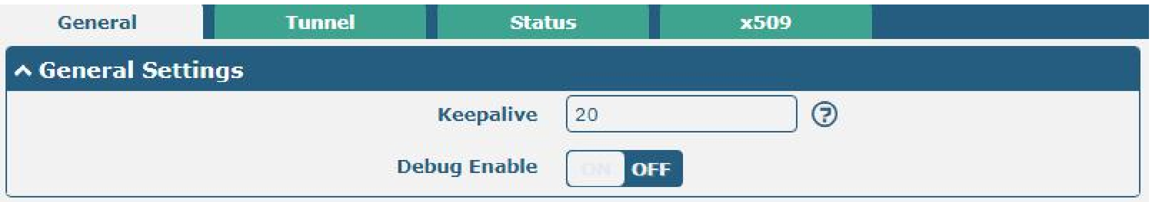
If gateway enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the gateway; and after the gateway dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

4.4 VPN

4.4.1 IPsec

This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

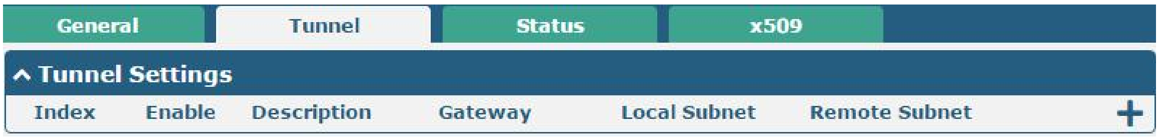
Click **VPN> IPsec> General** to set the IPsec parameter.



Keepalive: 20

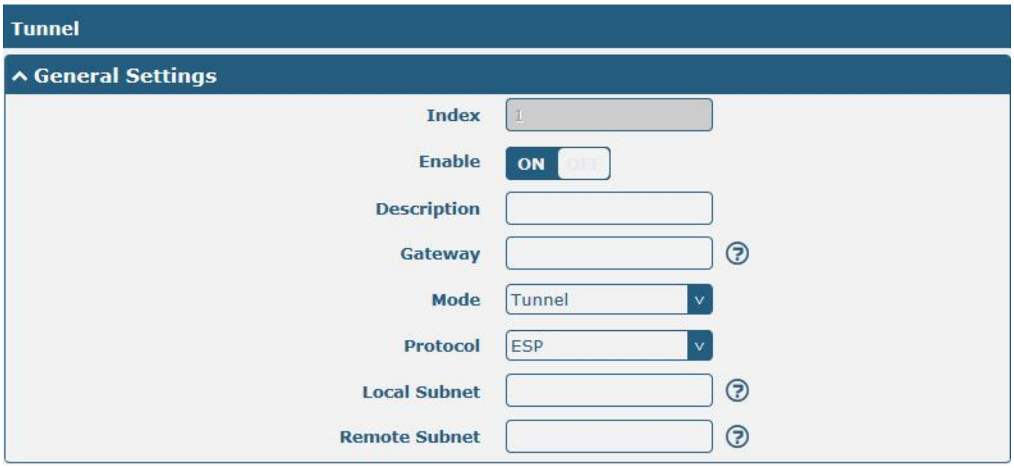
Debug Enable: OFF

General Settings @ General		
Item	**Description**	**Default**
Keepalive	Set the keepalive time, measured in seconds. The gateway will send packets to NAT server every keepalive time to avoid record remove from the NAT list.	20
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN information output to the debug port.	OFF



Index	Enable	Description	Gateway	Local Subnet	Remote Subnet

Click + to add tunnel settings. The maximum count is 6.



Index: 1

Enable: ON

Description:

Gateway:

Mode: Tunnel

Protocol: ESP

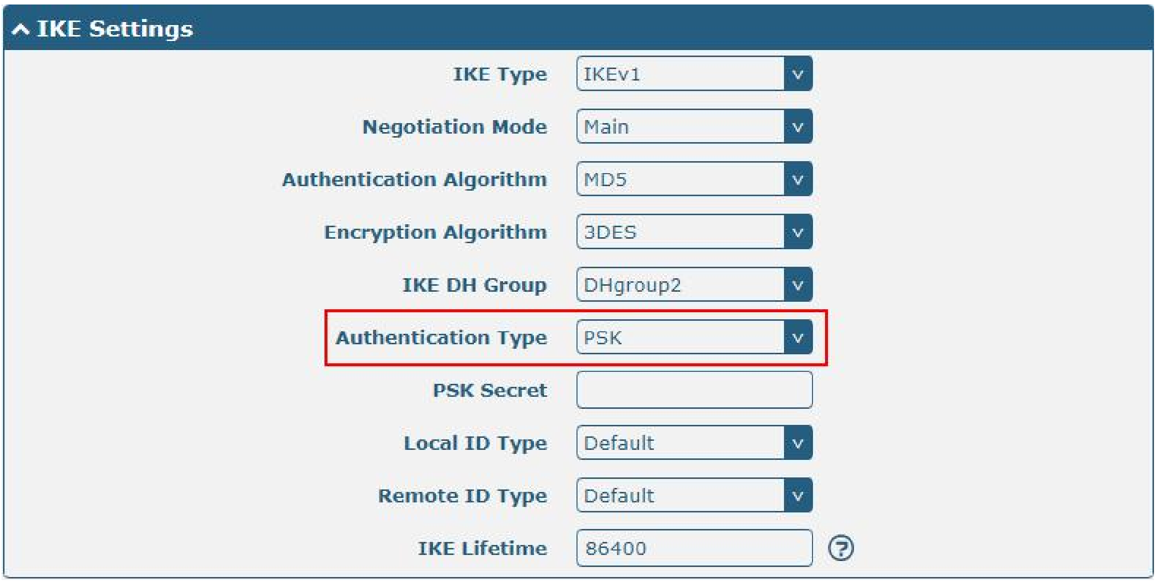
Local Subnet:

Remote Subnet:

General Settings @ Tunnel		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null

Gateway	Enter the address of remote IPsec VPN server. 0.0.0.0 represents for any address.	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 gateway, in which the gateway is the actual destination	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". • ESP: Use the ESP protocol • AH: Use the AH protocol	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null

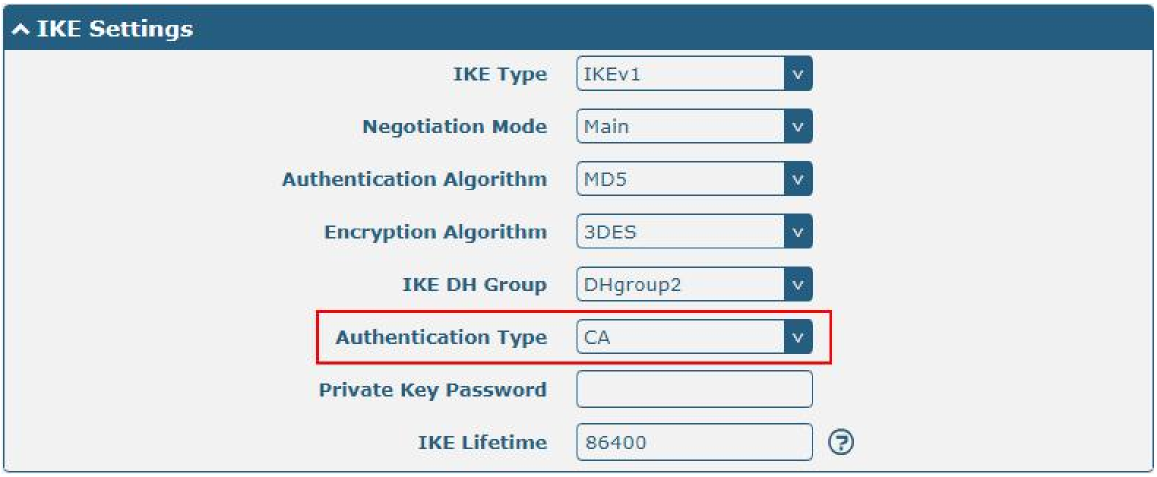
The window is displayed as below when choosing "PSK" as the authentication type.



^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

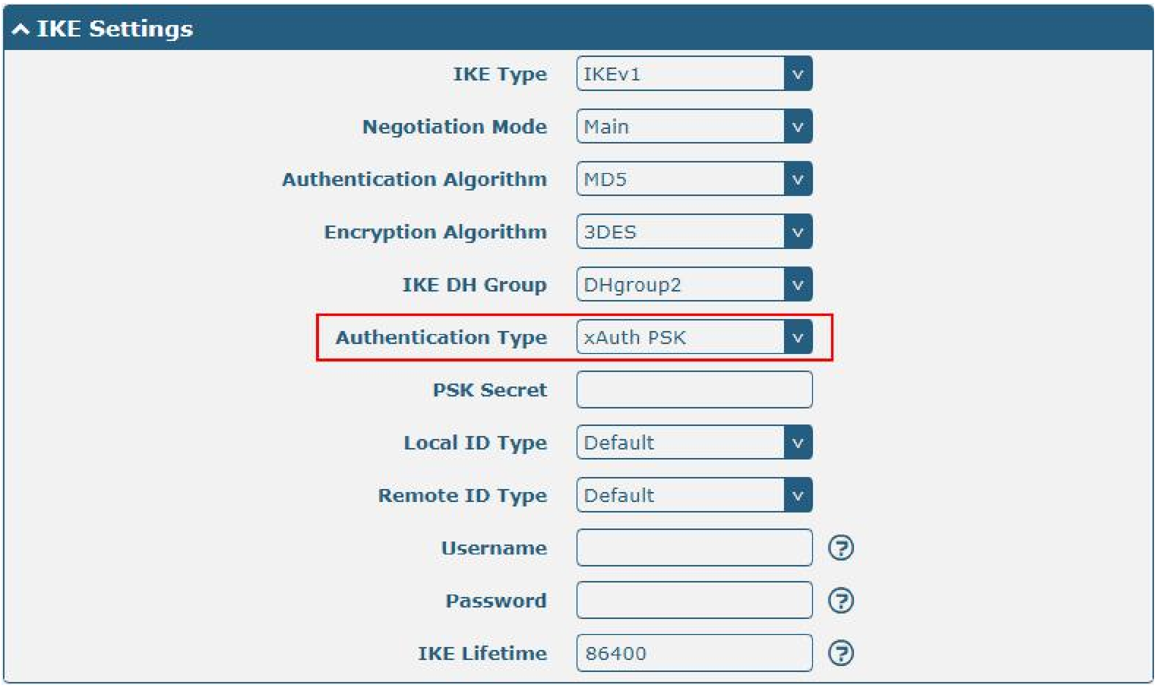
The window is displayed as below when choosing “CA” as the authentication type.



^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

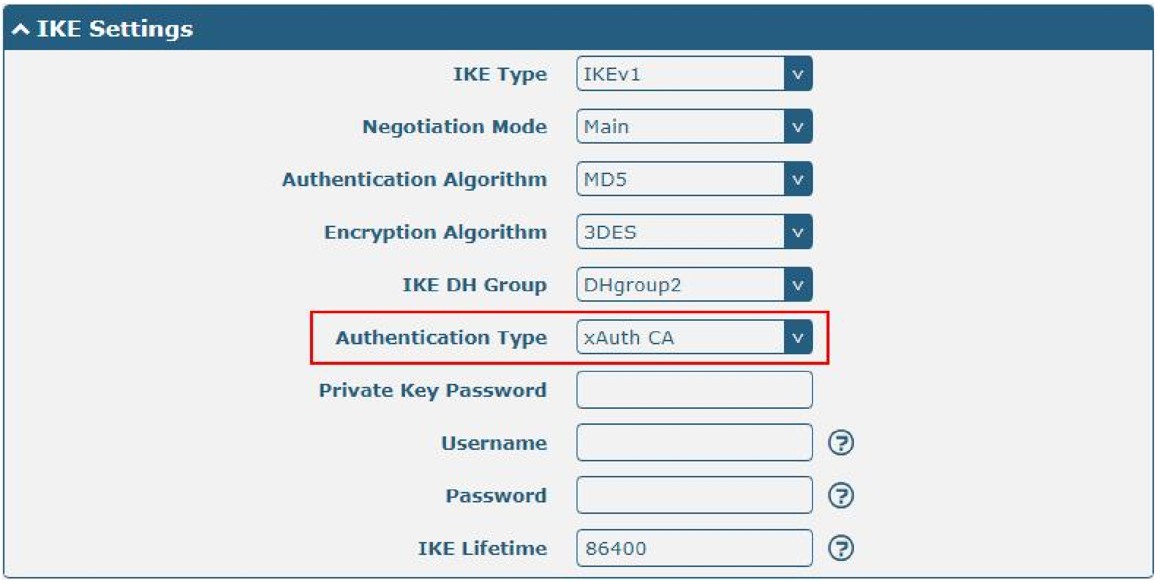
The window is displayed as below when choosing “xAuth PSK” as the authentication type.



^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

The window is displayed as below when choosing “xAuth CA” as the authentication type.



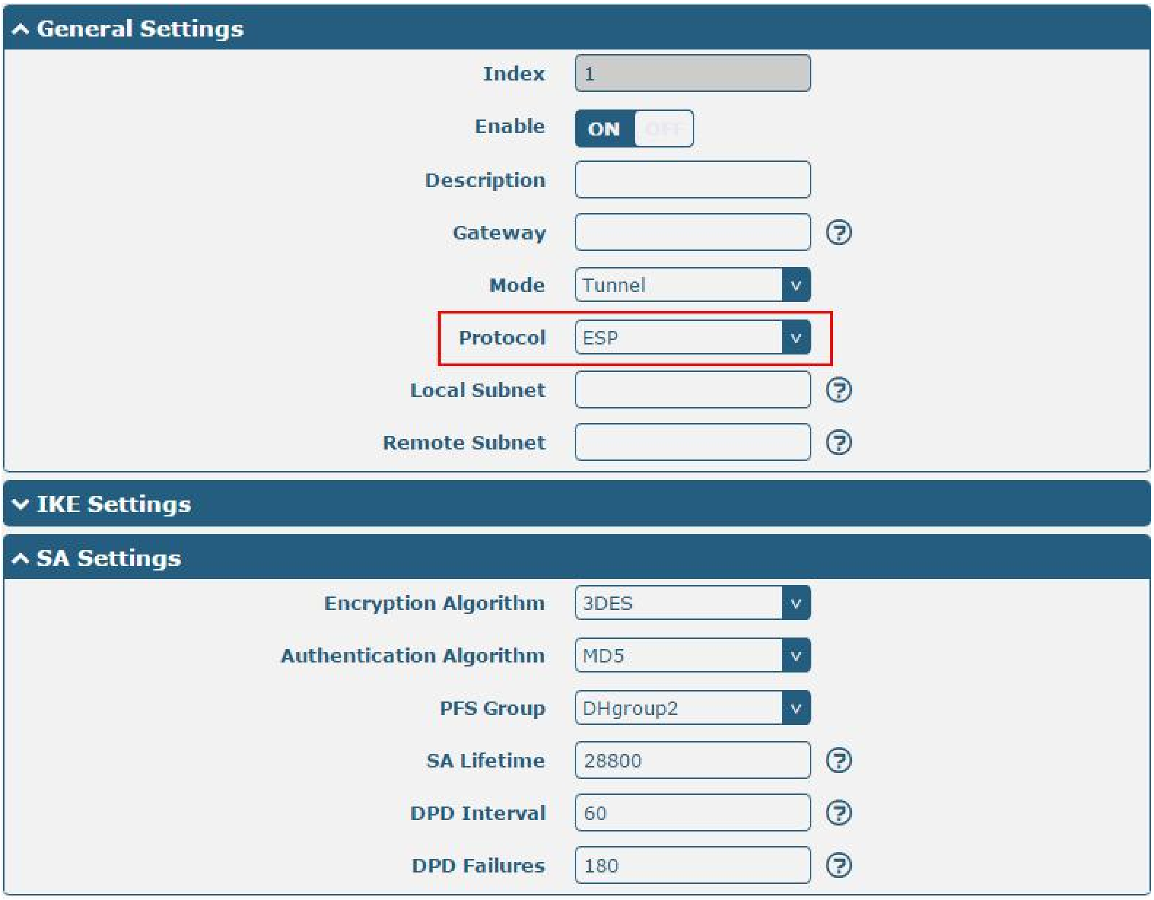
^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE Settings		
Item	**Description**	**Default**
IKE Type	Select from "IKEv1" or "IKEv2" as IKE version.	IKEv1
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", "SHA1", "SHA2 256" or "SHA2 512" to be used in IKE negotiation.	MD5
Encrypt Algorithm	Select from "3DES", "AES128" and "AES256"to be used in IKE negotiation. • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	3DES
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" "or "DHgroup18" to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from "PSK", "CA", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. • PSK: Pre-shared Key • CA: x509 Certificate Authority • xAuth: Extended Authentication to AAA server	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com	Default
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 under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication	Null

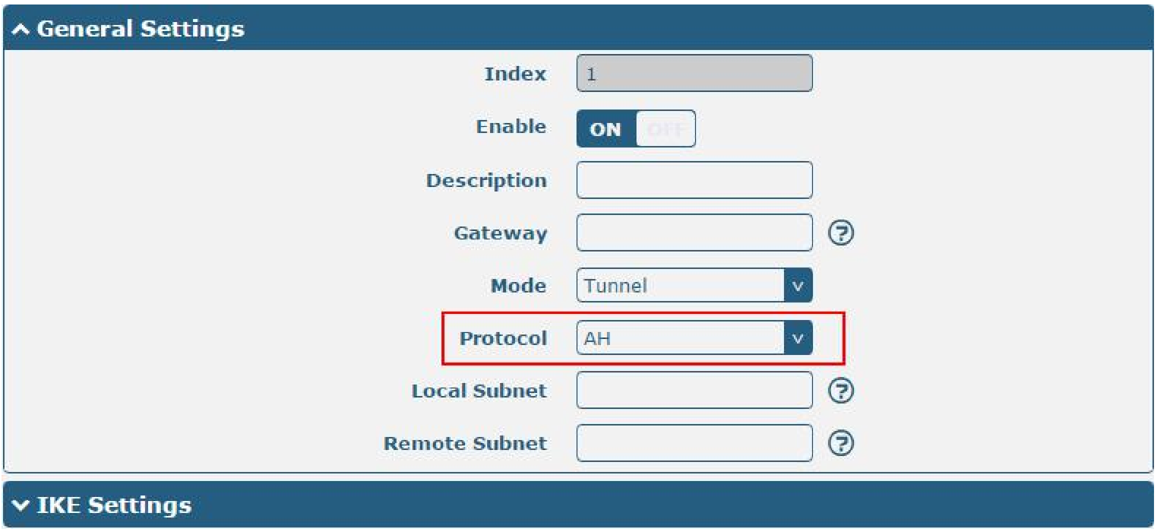
IKE Settings		
Item	Description	Default
	types.	

If click **VPN > IPsec > Tunnel > General Settings**, and choose **ESP** as protocol. The specific parameter configuration is shown as below.

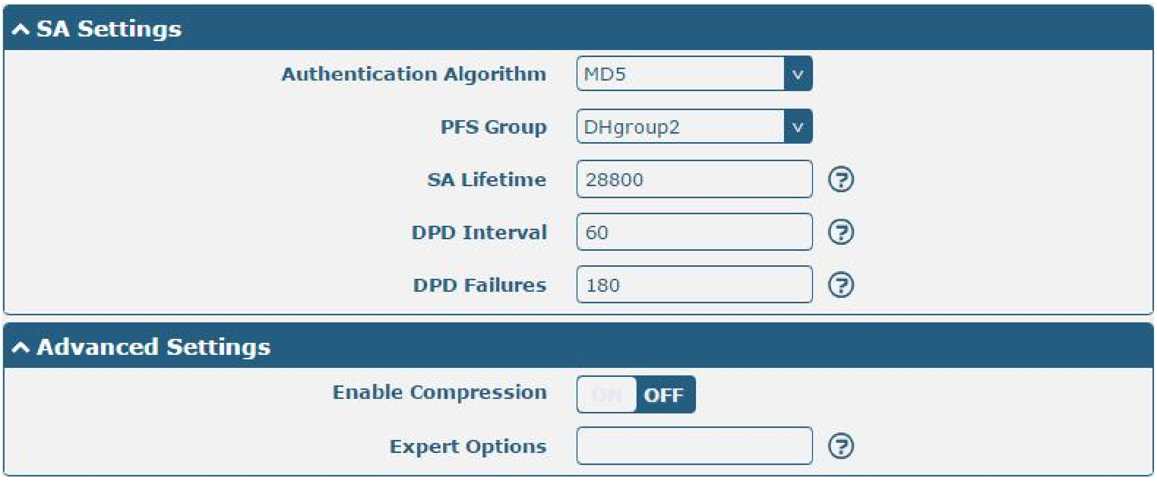


Index: 1
Enable: ON
Description:
Gateway:
Mode: Tunnel
Protocol: ESP
Local Subnet:
Remote Subnet:
Encryption Algorithm: 3DES
Authentication Algorithm: MD5
PFS Group: DHgroup2
SA Lifetime: 28800
DPD Interval: 60
DPD Failures: 180

If choose **AH** as protocol, the window of SA Settings is displayed as below.



Index: 1
Enable: ON
Description:
Gateway:
Mode: Tunnel
Protocol: AH
Local Subnet:
Remote Subnet:



SA Settings

Authentication Algorithm: MD5

PFS Group: DHgroup2

SA Lifetime: 28800

DPD Interval: 60

DPD Failures: 180

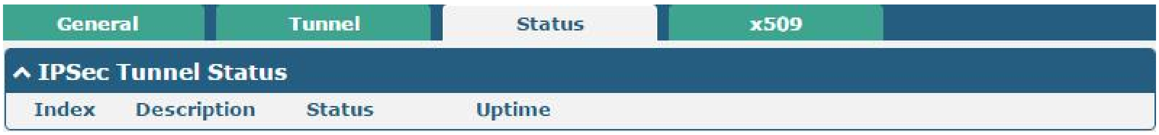
Advanced Settings

Enable Compression: ON OFF

Expert Options:

SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from “3DES”, “AES128”, “3AES192” or “AES256” when you select “ESP” in “Protocol”. 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”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in SA negotiation.	MD5
PFS Group	Select from “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating 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 is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	60
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

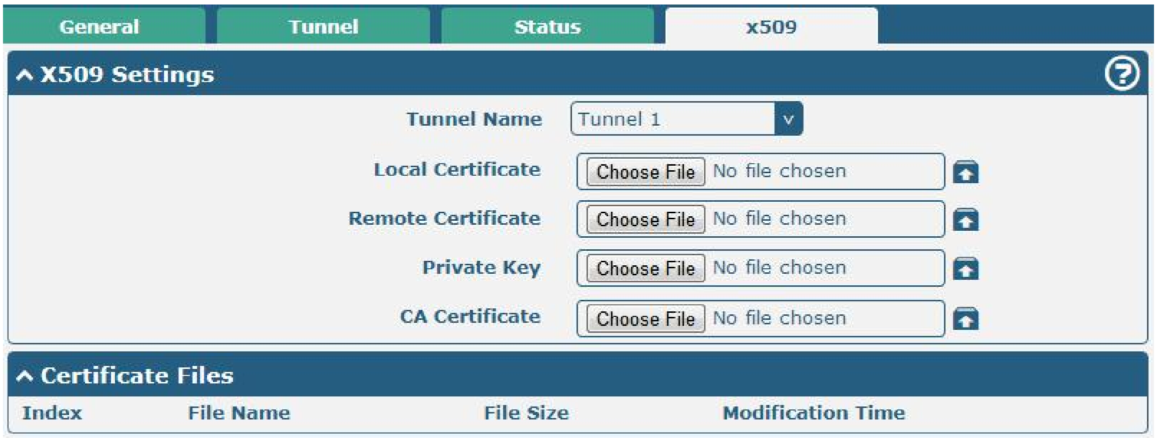
This section allows you to view the status of the IPsec tunnel.



IPSec Tunnel Status

Index	Description	Status	Uptime

User can upload the X509 certificates for the IPsec tunnel in this section.



X509 Settings

Tunnel Name: Tunnel 1

Local Certificate: No file chosen

Remote Certificate: No file chosen

Private Key: No file chosen

CA Certificate: No file chosen

Certificate Files

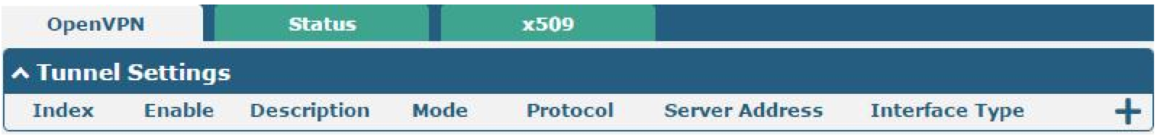
Index	File Name	File Size	Modification Time

x509		
Item	**Description**	**Default**
	X509 Settings	
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Local Certificate	When the authentication type of IPSec is CA or xAuth CA, this device needs the certificate.	--
Remote Certificate	When the authentication type of IPSec is CA or xAuth CA, this terminal device of IPSec needs the certificate.	--
Private Key	Choose the right private key file to import into the gateway.	--
CA Certificate	Choose the right CA Certificate to import into the gateway.	
	Certificate Files	
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	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

4.4.2 OpenVPN

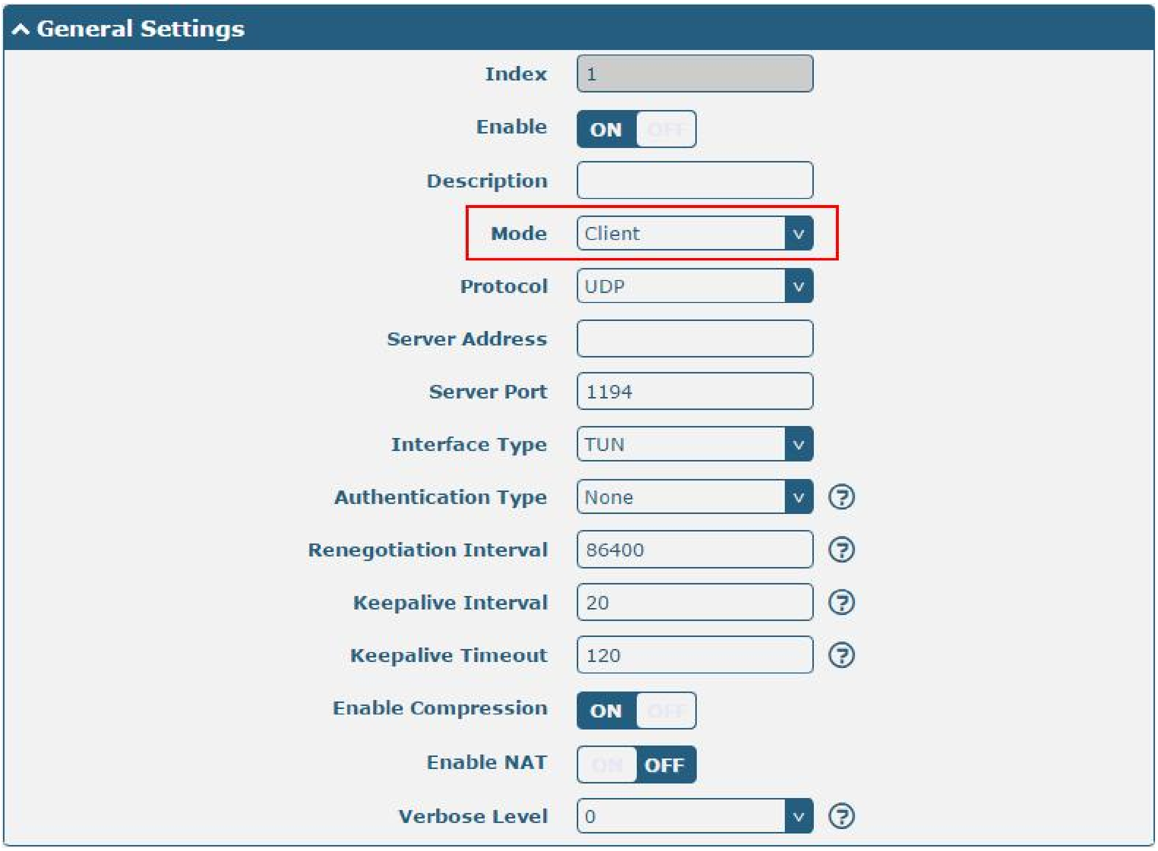
This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Gateway supports point-to-point and point-to-points connections.

If click **VPN > Open VPN > Open VPN,** the window is displayed as below.



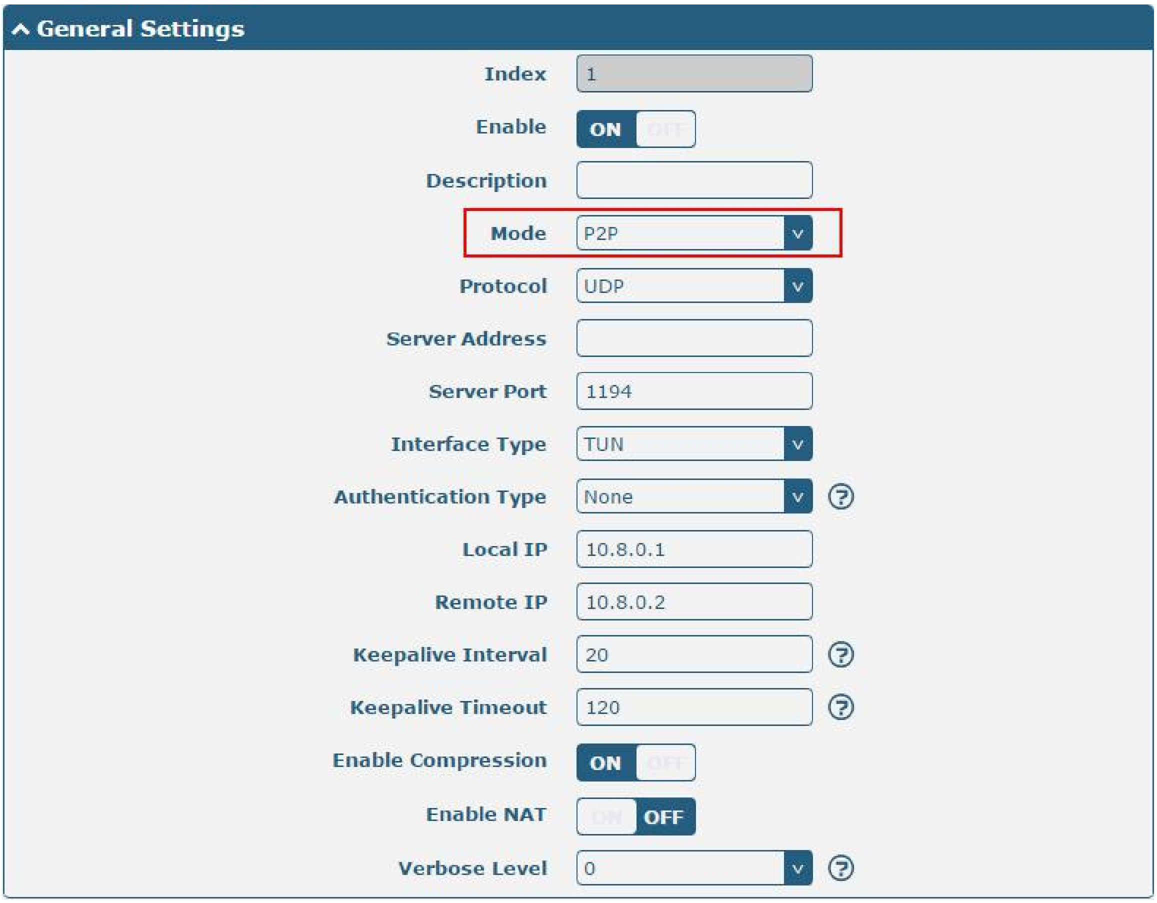
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click + to add tunnel settings. The maximum count is 5. The window is displayed as below when choosing "None" as the authentication type. By default, the mode is "Client".



Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

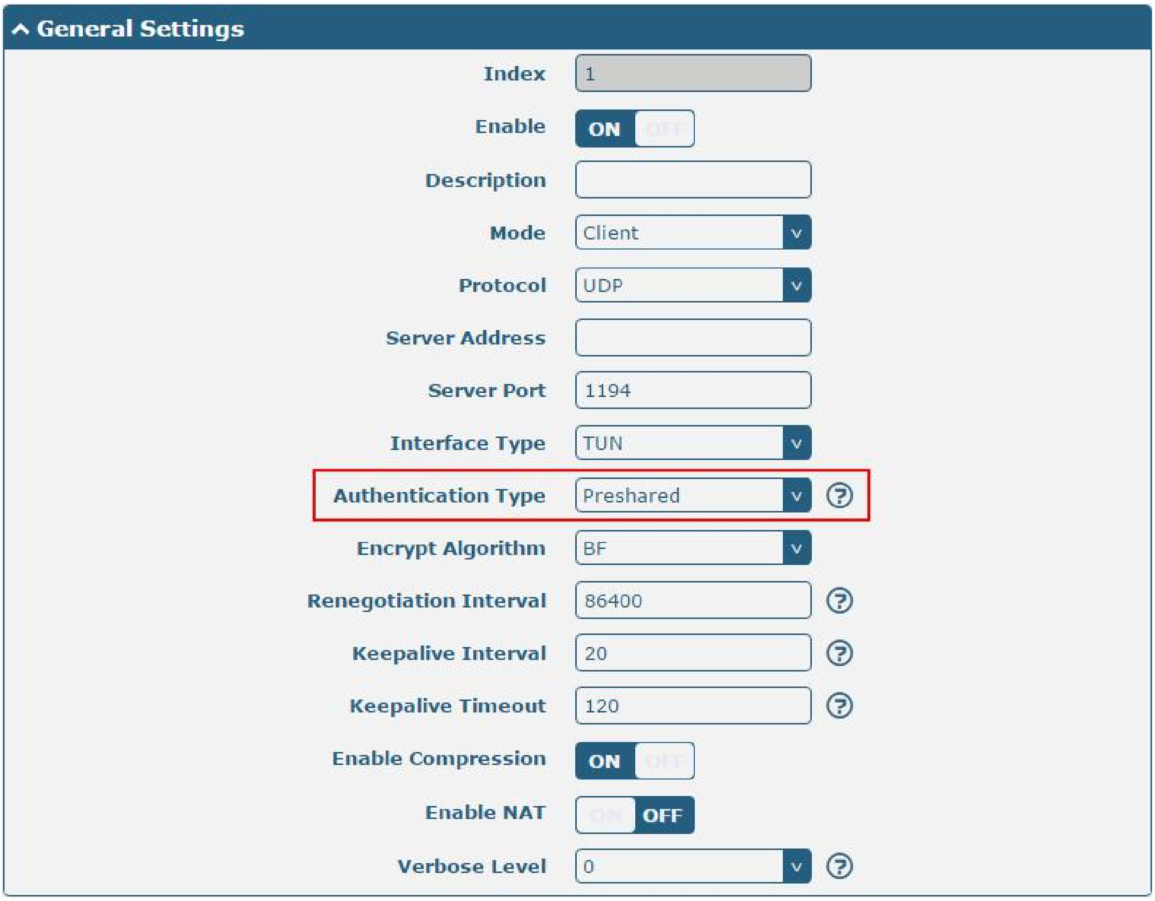
The window is displayed as below when choosing “P2P” as the mode.



General Settings

Index	1
Enable	ON
Description	
Mode	P2P
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

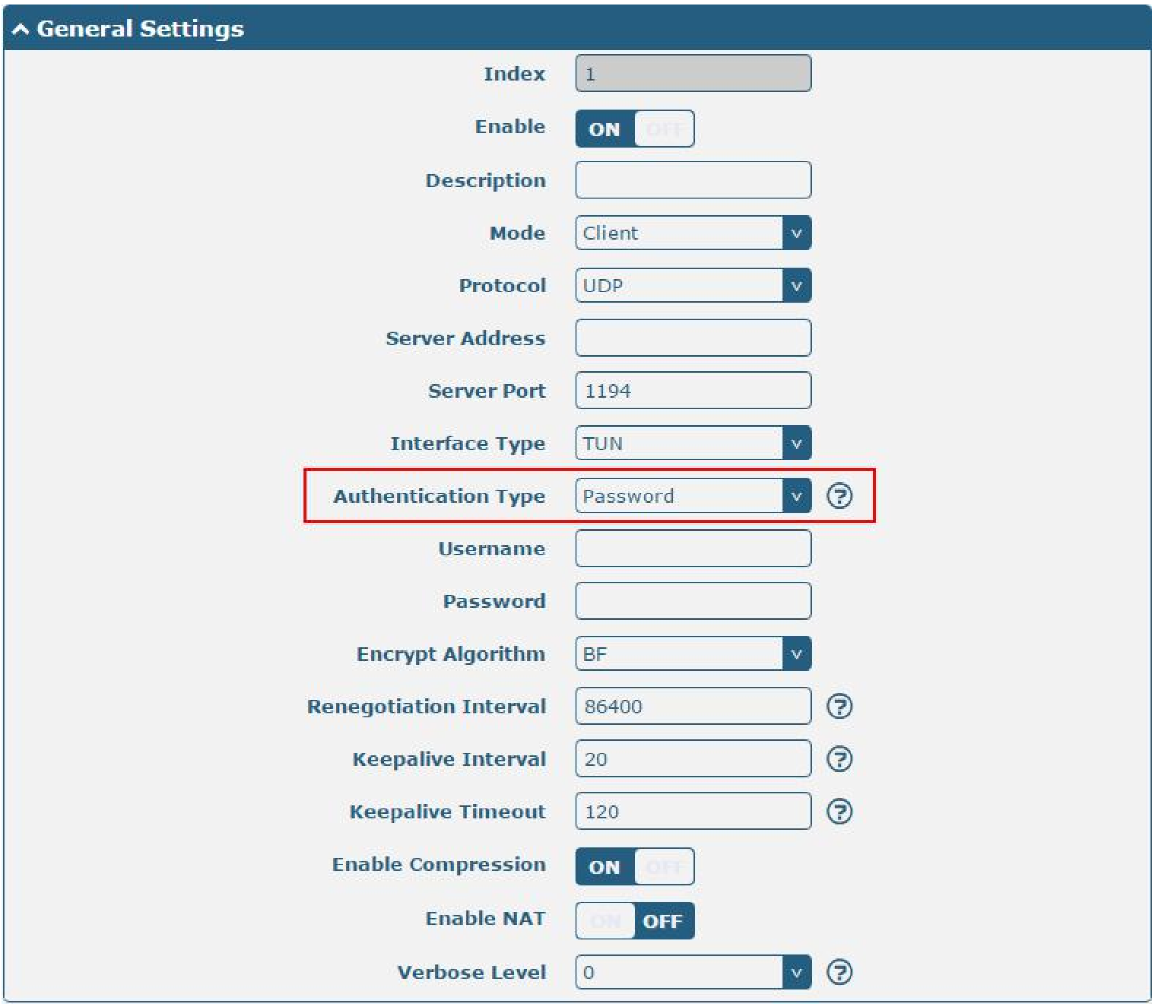
The window is displayed as below when choosing “Preshared” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

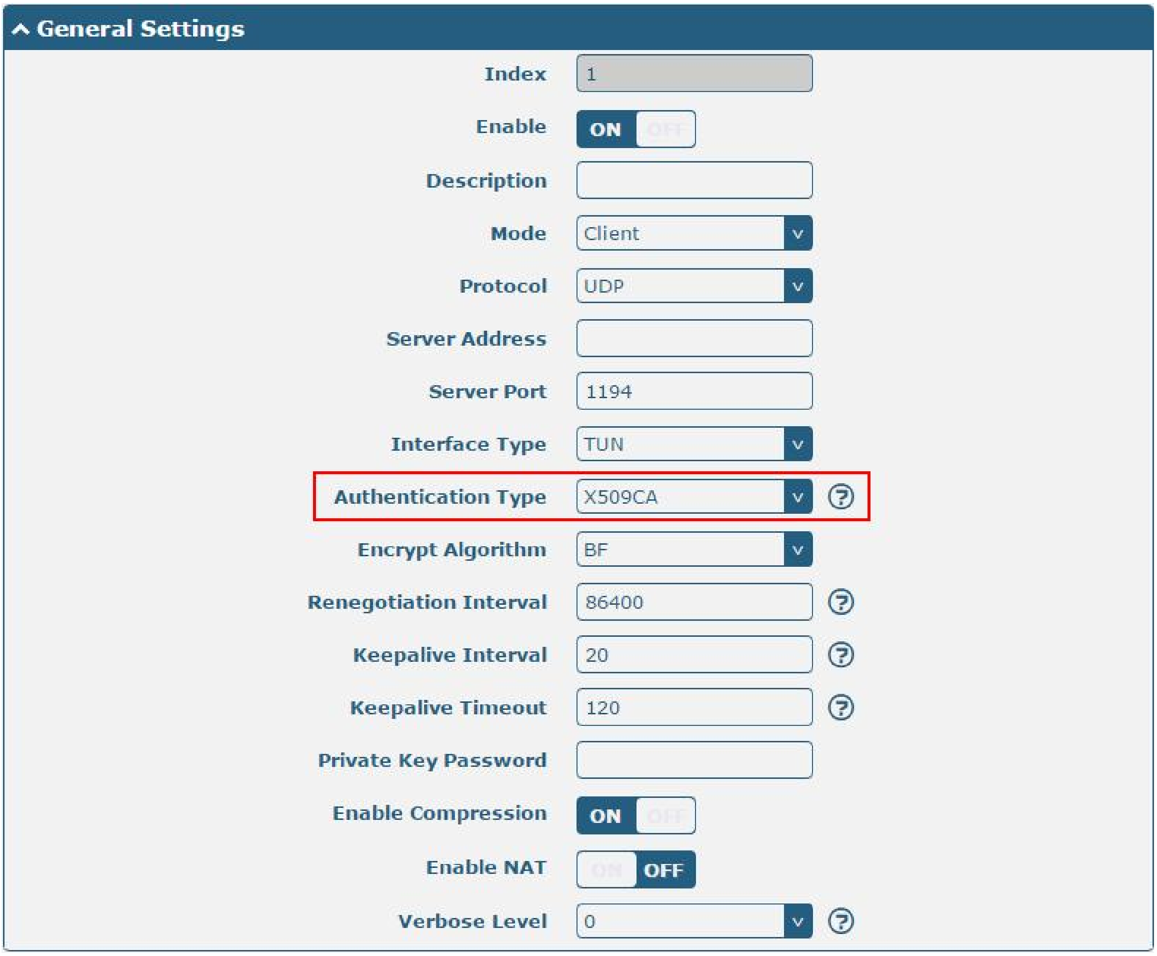
The window is displayed as below when choosing “Password” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

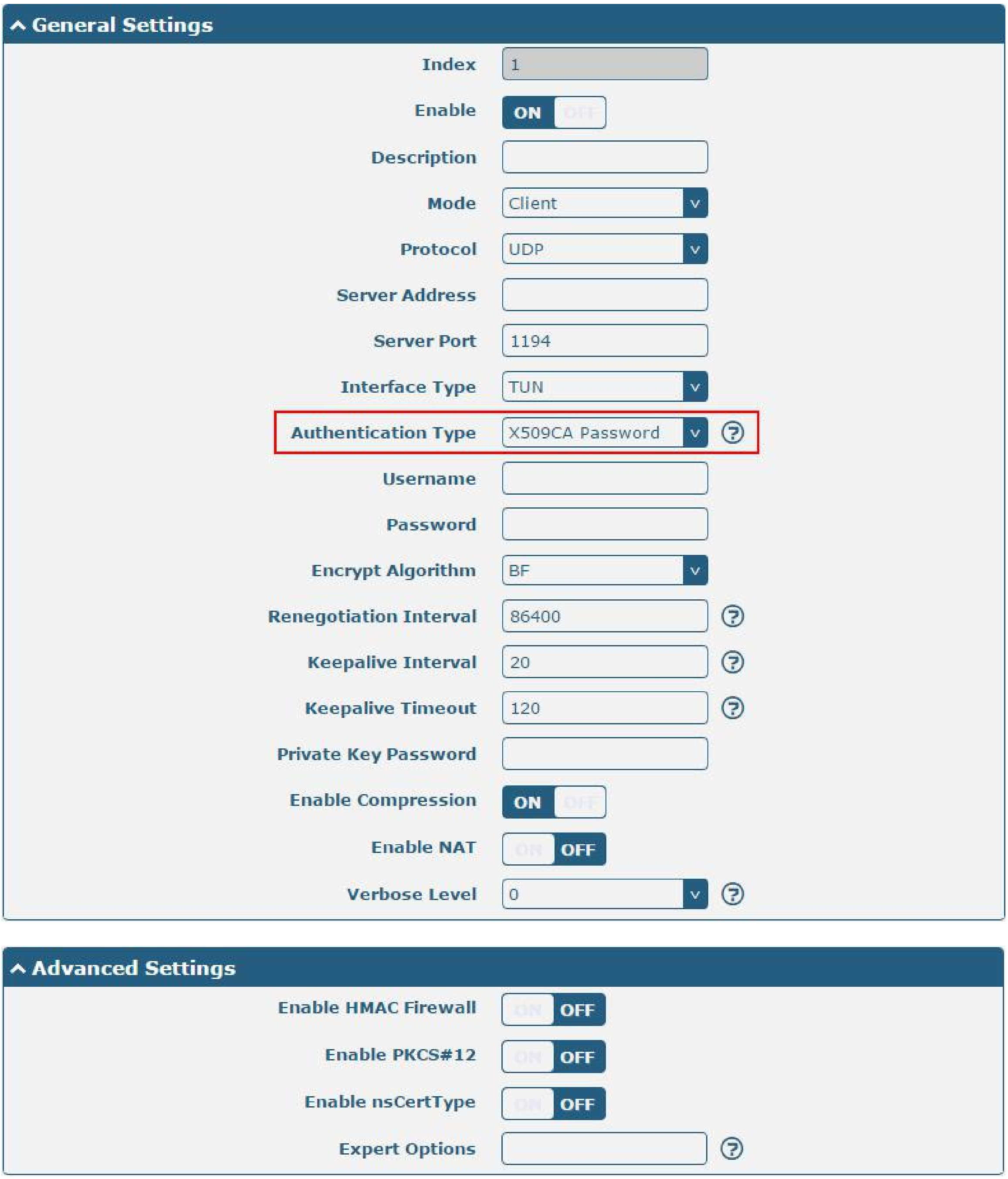
The window is displayed as below when choosing “X509CA” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

The window is displayed as below when choosing “X509CA Password” as the authentication type.



General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Username	
Password	
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

Advanced Settings

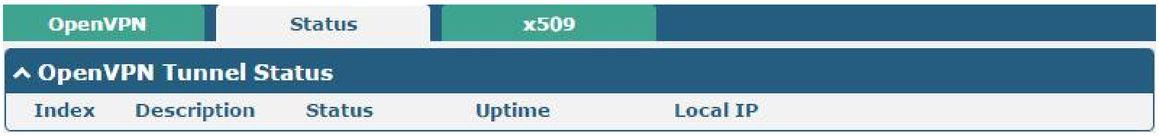
Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	

General Settings @ OpenVPN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null

General Settings @ OpenVPN		
Item	**Description**	**Default**
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194
Interface Type	Select from "TUN" or "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". **Note:** "None" and "Preshared" authentication type are only working with P2P mode.	None
Username	Enter the username used for "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for "Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". • BF: Use 128-bit BF encryption algorithm in CBC mode • DES: Use 64-bit DES encryption algorithm in CBC mode • DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES192: Use 192-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Enter the private key password under the "X509CA" and "X509CA Password" authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind gateway will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. • 0: No output except fatal errors • 1~4: Normal usage range • 5: Output R and W characters to the console for each packet read and write • 6~11: Debug info range	0

Advanced Settings @ OpenVPN		
Item	**Description**	**Default**
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null

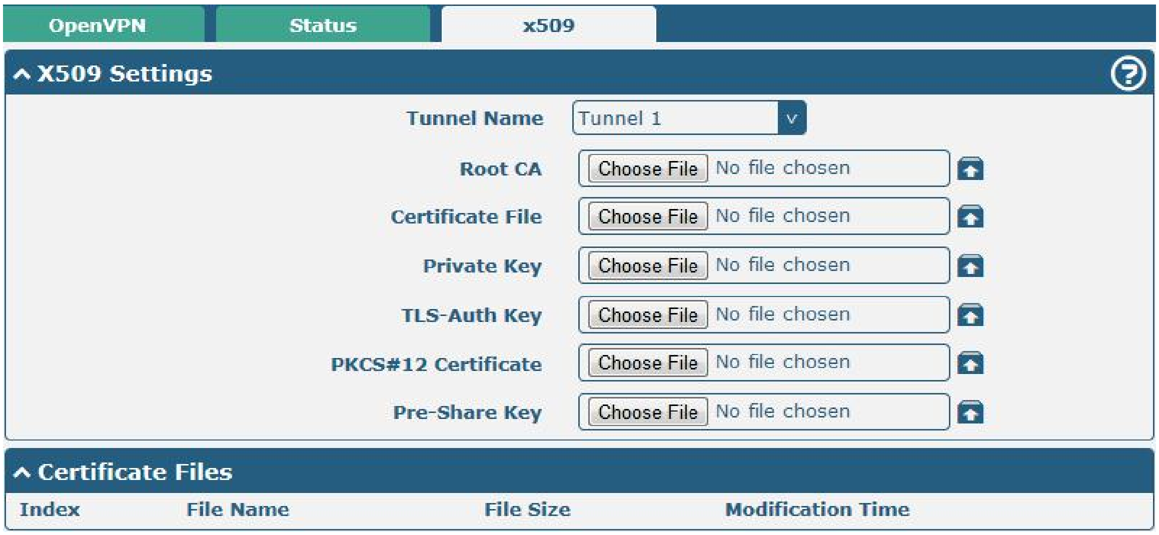
This section allows you to view the status of the OpenVPN tunnel.



^ OpenVPN Tunnel Status

Index	Description	Status	Uptime	Local IP

User can upload the X509 certificates for the OpenVPN in this section.



^ X509 Settings

Tunnel Name	Tunnel 1
Root CA	Choose File No file chosen
Certificate File	Choose File No file chosen
Private Key	Choose File No file chosen
TLS-Auth Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen
Pre-Share Key	Choose File No file chosen

^ Certificate Files

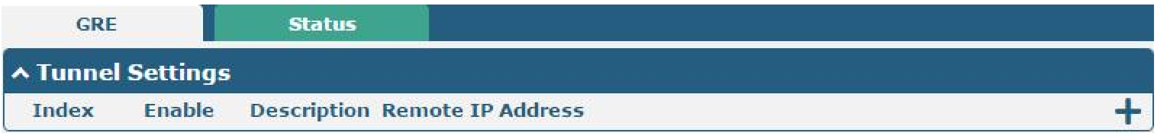
Index	File Name	File Size	Modification Time

x509		
Item	**Description**	**Default**
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Root CA	Choose the root certificate signed to OpenVPN client.	--
Certificate Files	Choose the certificate file for OpenVPN client.	--
Private Key	Choose the private key for OpenVPN client.	--
TLS-Auth Key	Choose the TLS-Auth Key.	--
RKCS# 12 Certificate	Choose the certificate file with PKCS#12 format.	--
Pre-Share Key	Choose the pre-share key generated by the OpenVPN tool.	--
Certificate Files		

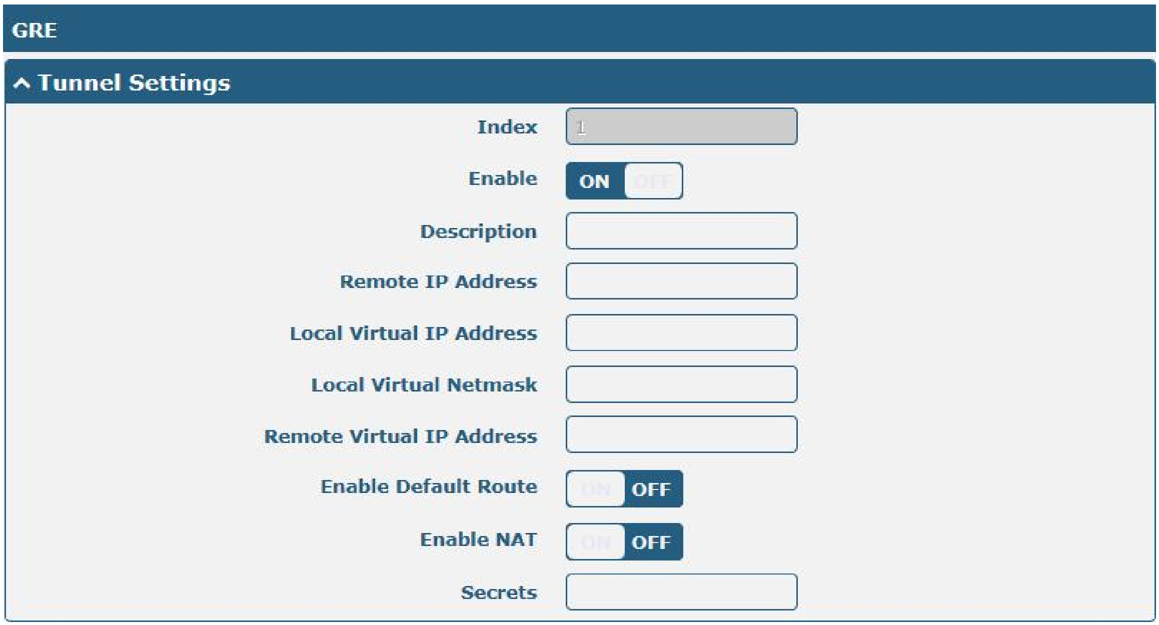
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

4.4.3 GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. There are two main uses of the GRE protocol: enterprise internal protocol encapsulation and private address encapsulation.



Click + to add tunnel settings. The maximum count is 5.


GRE

^ Tunnel Settings

Index 1

Enable ON

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask

Remote Virtual IP Address

Enable Default Route OFF

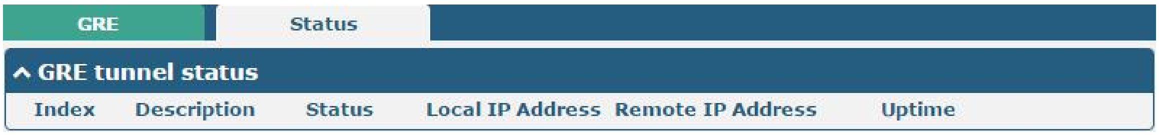
Enable NAT OFF

Secrets

Tunnel Settings @ GRE		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the gateway will go through the GRE VPN.	OFF

Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when gateway under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null

This section allows you to view the status of GRE tunnel.



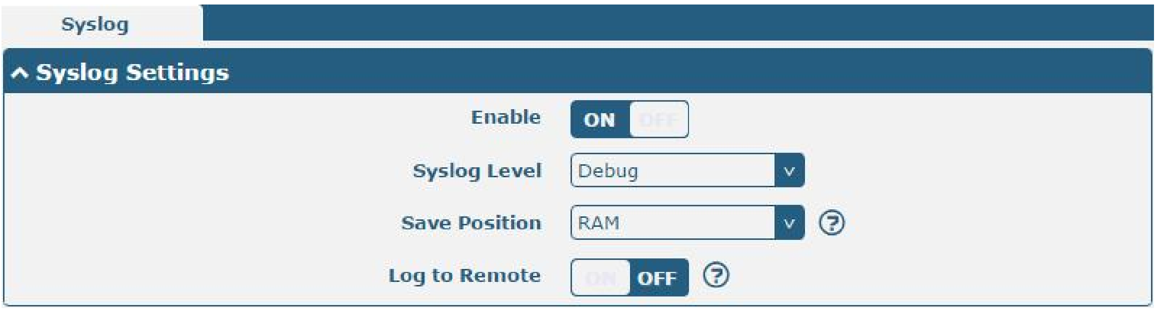
^ GRE tunnel status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

4.5 Services

4.5.1 Syslog

This section allows you to set the syslog parameters. By default, the “Log to Remote” option is disabled. The system log of the gateway can be saved in the local, also supports to be sent to remote log server and specified application debugging.



^ Syslog Settings

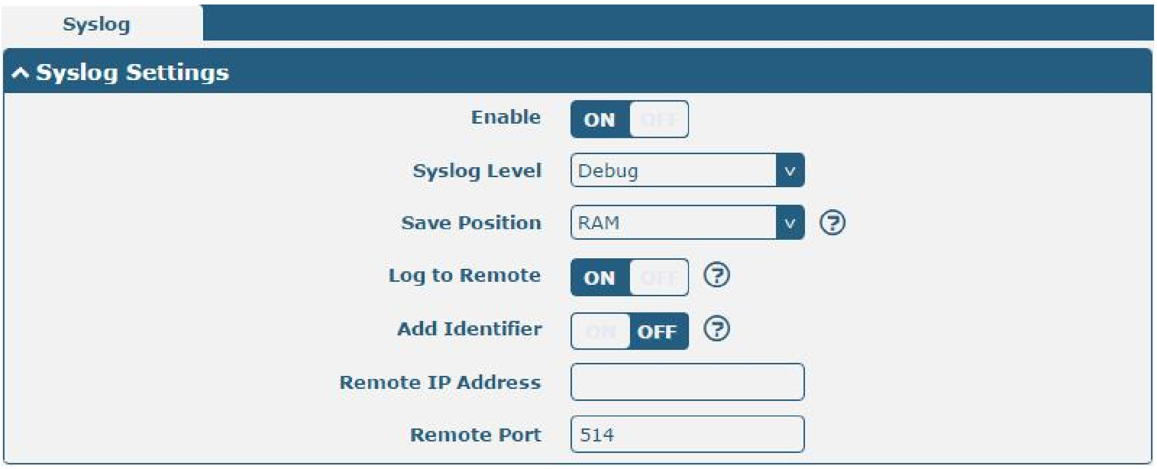
Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: OFF

The window is displayed as below when enabling the “Log to Remote” option.



^ Syslog Settings

Enable: ON

Syslog Level: Debug

Save Position: RAM

Log to Remote: ON

Add Identifier: OFF

Remote IP Address:

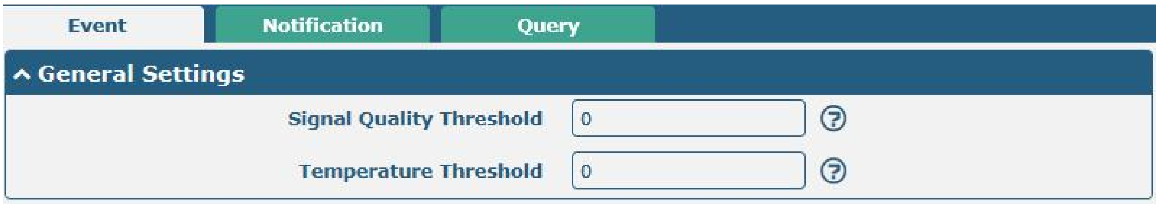
Remote Port: 514

Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to	Debug

	high. **Note:** The lower level will output more syslog in details.	
Save Position	Select the save position from “RAM”, “NVM” or “Console”. Choose “RAM”. The data will be cleared after reboot. **Note**: It's not recommended that you save syslog to NVM for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow gateway sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

4.5.2 Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur. Gateway events can also be reported via SNMP-TRAP and RobustLink.

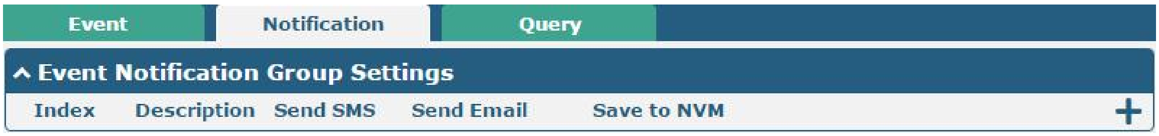


General Settings

Signal Quality Threshold: 0

Temperature Threshold: 0

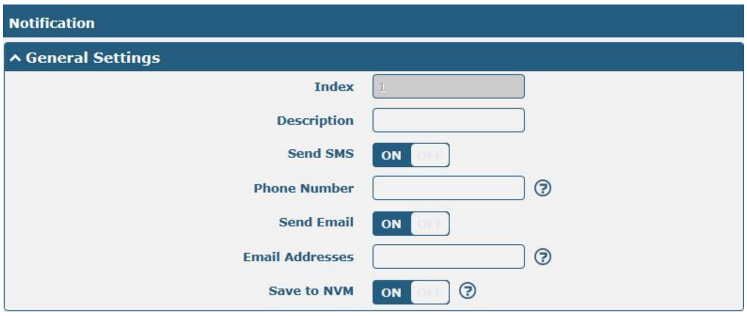
General Settings @ Event		
Item	**Description**	**Default**
Signal Quality Threshold	Set the threshold for signal quality. Gateway will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0
Temperature Threshold	Set the temperature threshold, used to trigger event notification for excessive temperature. Enable this notification in the “Notification” bar. When the temperature is higher than the threshold value of the event, 0 means to turn off this feature.	0



Event Notification Group Settings

Index	Description	Send SMS	Send Email	Save to NVM

Click + button to add an Event parameters.



Notification

General Settings

Index: 1

Description:

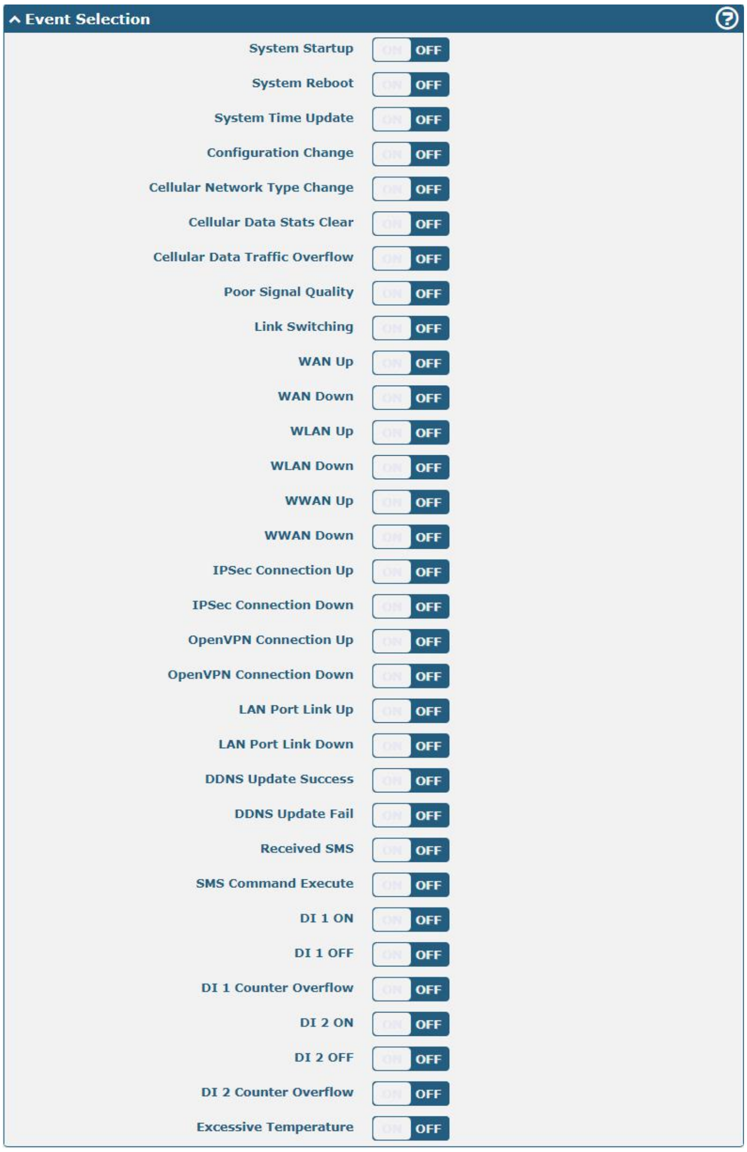
Send SMS: ON

Phone Number:

Send Email: ON

Email Addresses:

Save to NVM: ON

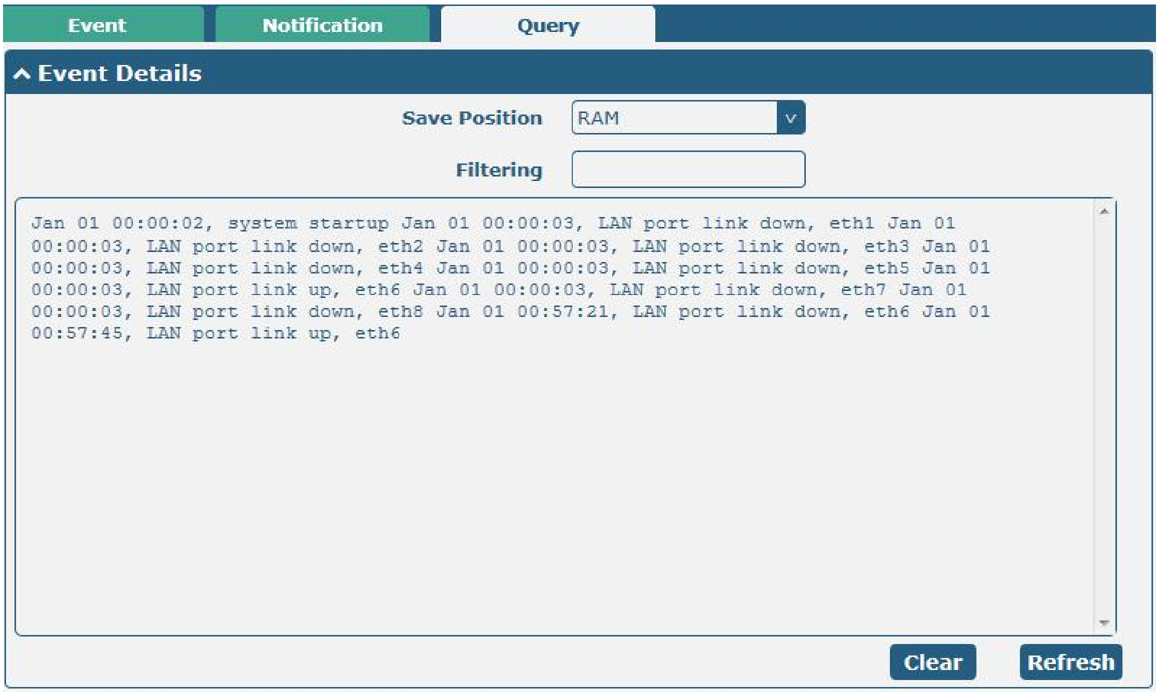


^ Event Selection

System Startup	OFF
System Reboot	OFF
System Time Update	OFF
Configuration Change	OFF
Cellular Network Type Change	OFF
Cellular Data Stats Clear	OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	OFF
Link Switching	OFF
WAN Up	OFF
WAN Down	OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF
IPSec Connection Up	OFF
IPSec Connection Down	OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
DDNS Update Success	OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF
DI 1 ON	OFF
DI 1 OFF	OFF
DI 1 Counter Overflow	OFF
DI 2 ON	OFF
DI 2 OFF	OFF
DI 2 Counter Overflow	OFF
Excessive Temperature	OFF

General Settings @ Notification		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.24 Services > Email", and use ';'to separate each number.	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified email box via Email if event occurs. Set the related email address in "3.24 Services > Email".	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.



Save Position: RAM

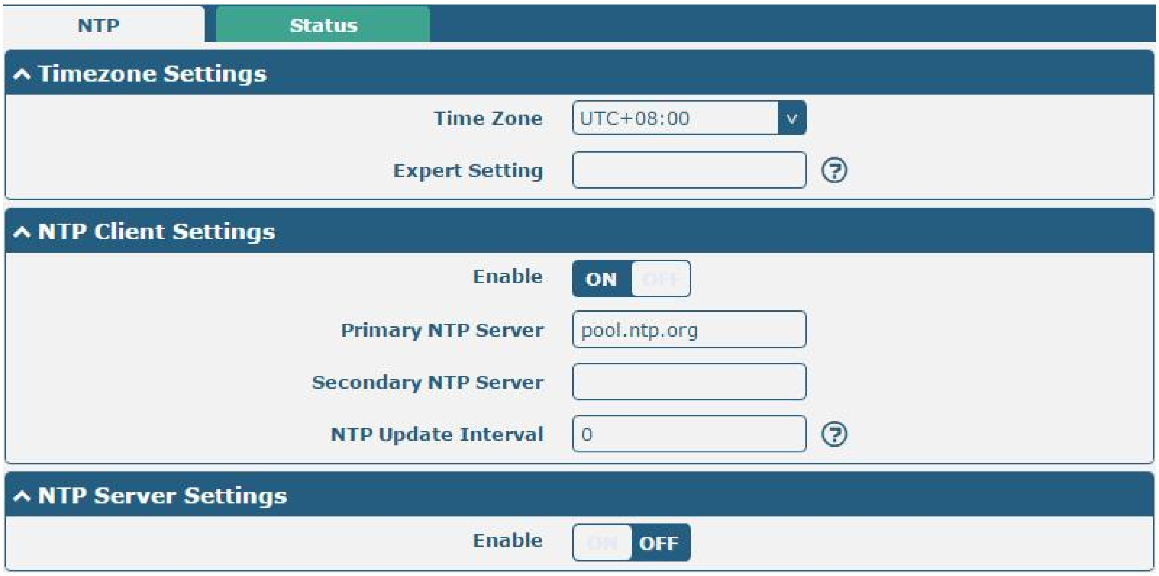
Filtering:

```
Jan 01 00:00:02, system startup Jan 01 00:00:03, LAN port link down, eth1 Jan 01
00:00:03, LAN port link down, eth2 Jan 01 00:00:03, LAN port link down, eth3 Jan 01
00:00:03, LAN port link down, eth4 Jan 01 00:00:03, LAN port link down, eth5 Jan 01
00:00:03, LAN port link up, eth6 Jan 01 00:00:03, LAN port link down, eth7 Jan 01
00:00:03, LAN port link down, eth8 Jan 01 00:57:21, LAN port link down, eth6 Jan 01
00:57:45, LAN port link up, eth6
```

Event Details		
Item	**Description**	**Default**
Save Position	Select the events' save position from "RAM" or "NVM". • RAM: Random-access memory • NVM: Non-Volatile Memory	RAM
Filtering	Enter the filtering message based on the keywords set by users. 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

4.5.3 NTP

This section allows you to set the related NTP (Network Time Protocol) parameters, including Time zone, NTP Client and NTP Server.



^ Timezone Settings

Time Zone: UTC+08:00

Expert Setting:

^ NTP Client Settings

Enable: ON

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

NTP Update Interval: 0

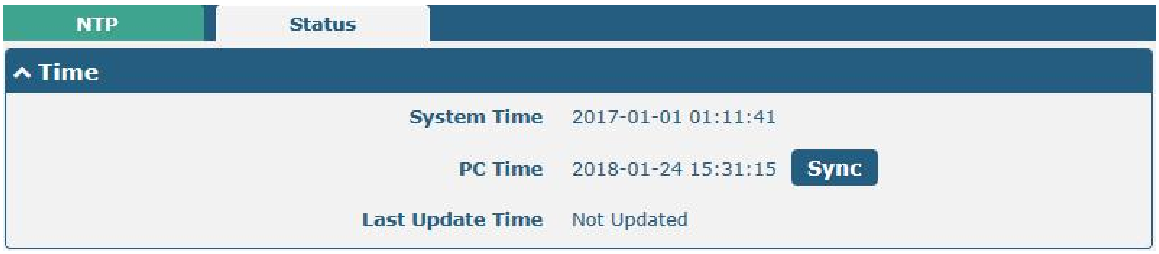
^ NTP Server Settings

Enable: OFF

NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	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 Settings		
Enable	Click the toggle button to enable/disable this option. Enable to synchronize time with the NTP server.	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) synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0
NTP Server Settings		
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

This window allows you to view the current time of gateway and also synchronize the gateway time.

Click **Sync** button to synchronize the gateway time with the PC's.



^ Time

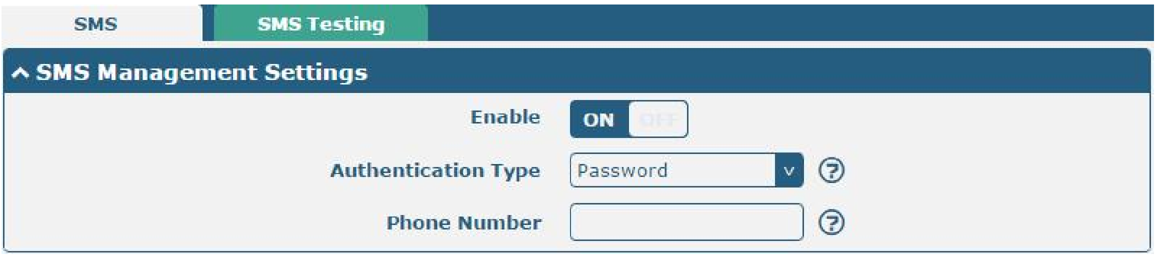
System Time: 2017-01-01 01:11:41

PC Time: 2018-01-24 15:31:15

Last Update Time: Not Updated

4.5.4 SMS

This section allows you to set SMS parameters. Gateway supports SMS management, and user can control and configure their gateways by sending SMS. For more details about SMS control, refer to **4.2.2 SMS Remote Control**.



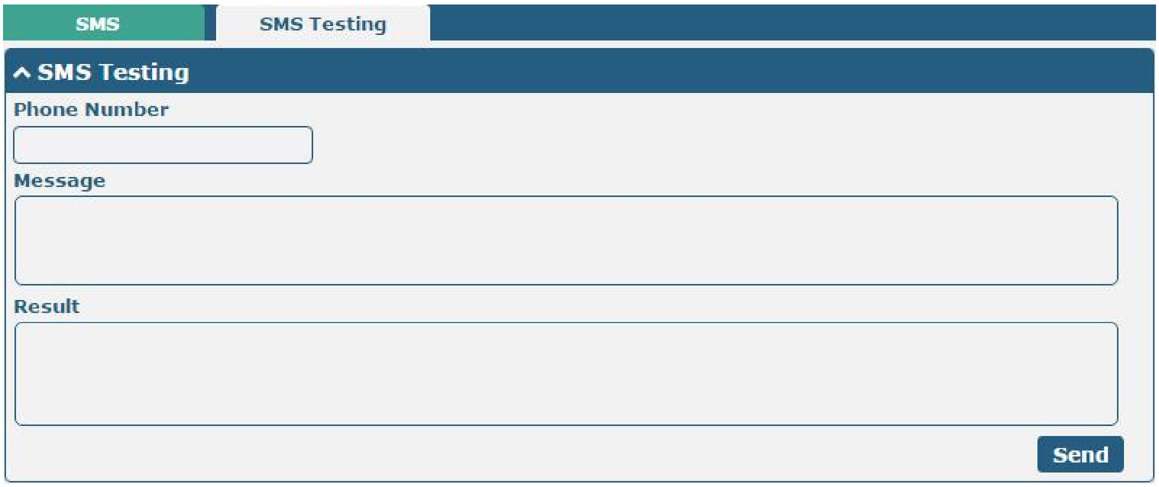
Enable: ON

Authentication Type: Password

Phone Number:

SMS Management Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the SMS Management option. **Note**: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "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 authentication, and 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 used for SMS management, and use '; 'to separate each number. **Note**: It can be null when choose "Password" as the authentication type.	Null

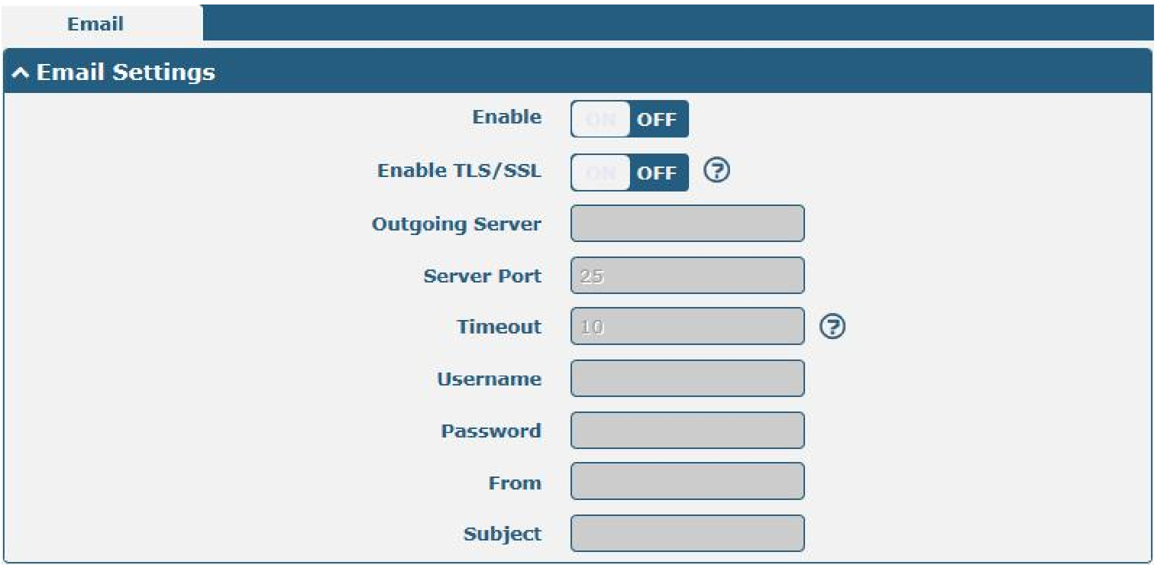
User can test the current SMS service whether it is available in this section.



SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter the specified phone number which can receive the SMS from gateway.	Null
Message	Enter the message that gateway will send it to the specified phone number.	Null
Result	The result of the SMS test will be displayed in the result box.	Null
Send	Click the button to send the test message.	--

4.5.5 Email

Email function supports to send the event notifications to the specified recipient by ways of email.

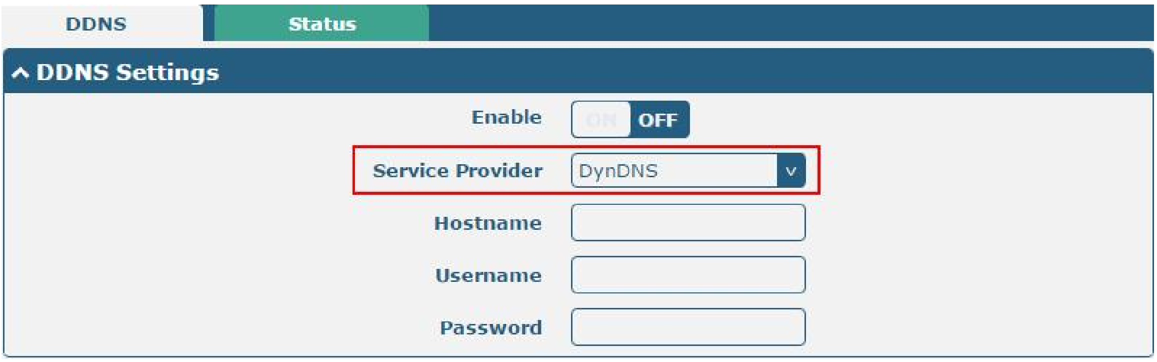


Enable: ON OFF
Enable TLS/SSL: ON OFF
Outgoing Server:
Server Port: 25
Timeout: 10
Username:
Password:
From:
Subject:

Email Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn’t receive the email over this time, it will try to resend.	10
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

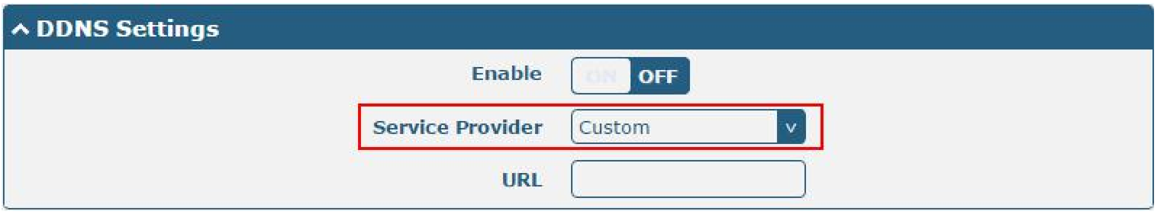
4.5.6 DDNS

This section allows you to set the DDNS parameters. The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows you 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 gateway, which is assigned to you by your ISP. The service provider defaults to “DynDNS”, as shown below.



Enable: OFF
Service Provider: DynDNS
Hostname
Username
Password

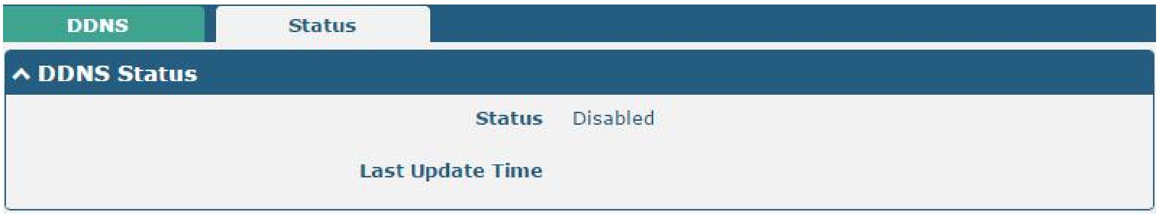
When “Custom” service provider chosen, the window is displayed as below.



Enable: OFF
Service Provider: Custom
URL

DDNS Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. **Note:** the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click “Status” bar to view the status of the DDNS.

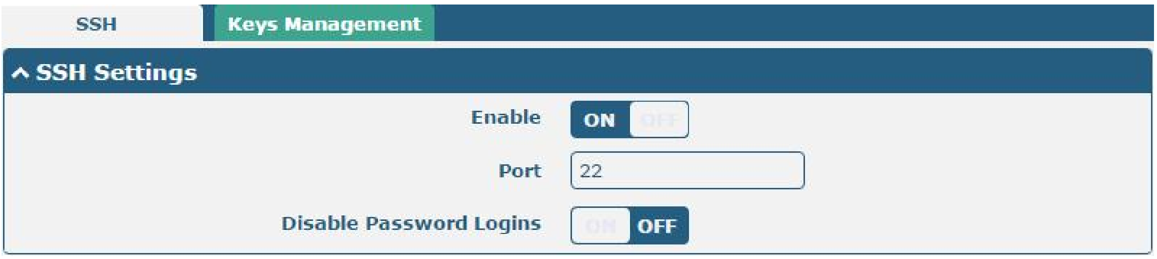


Status: Disabled
Last Update Time

DDNS Status	
Item	**Description**
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

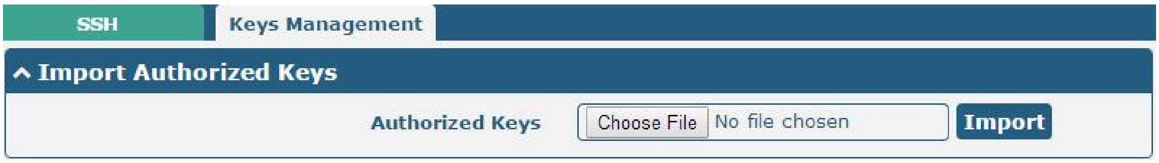
4.5.7 SSH

Gateway supports SSH password access and secret-key access.



Enable: ON
Port: 22
Disable Password Logins: OFF

SSH Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable this option. When enabled, you can access the gateway via SSH.	ON
Port	Set the port of the SSH access.	22
Disable Password Logins	Click the toggle button to enable/disable this option. When enabled, you cannot use username and password to access the gateway via SSH. In this case, only the key can be used for login.	OFF

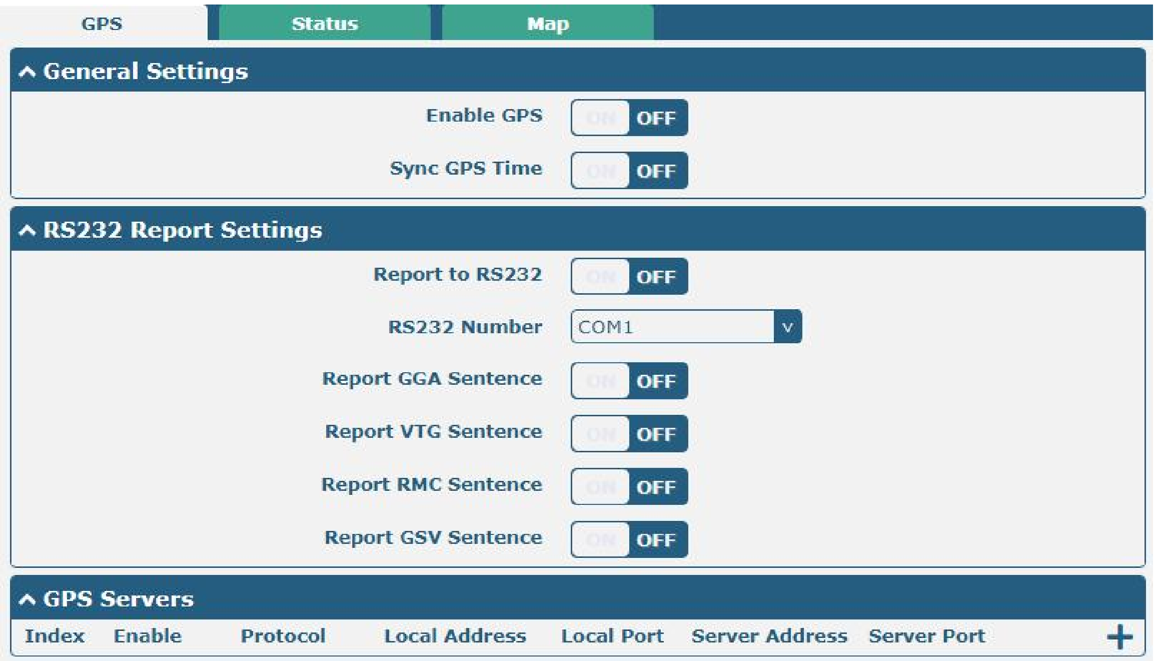


Authorized Keys: No file chosen

Import Authorized Keys	
Item	**Description**
Authorized Keys	Click on “Choose File” to locate an authorized key from your computer, and then click “Import” to import this key into your gateway. **Note**: This option is valid when enabling the password logins option.

4.5.8 GPS

This section allows you to set the GPS setting parameters.



GPS | Status | Map

General Settings

Enable GPS: ON OFF

Sync GPS Time: ON OFF

RS232 Report Settings

Report to RS232: ON OFF

RS232 Number: COM1

Report GGA Sentence: ON OFF

Report VTG Sentence: ON OFF

Report RMC Sentence: ON OFF

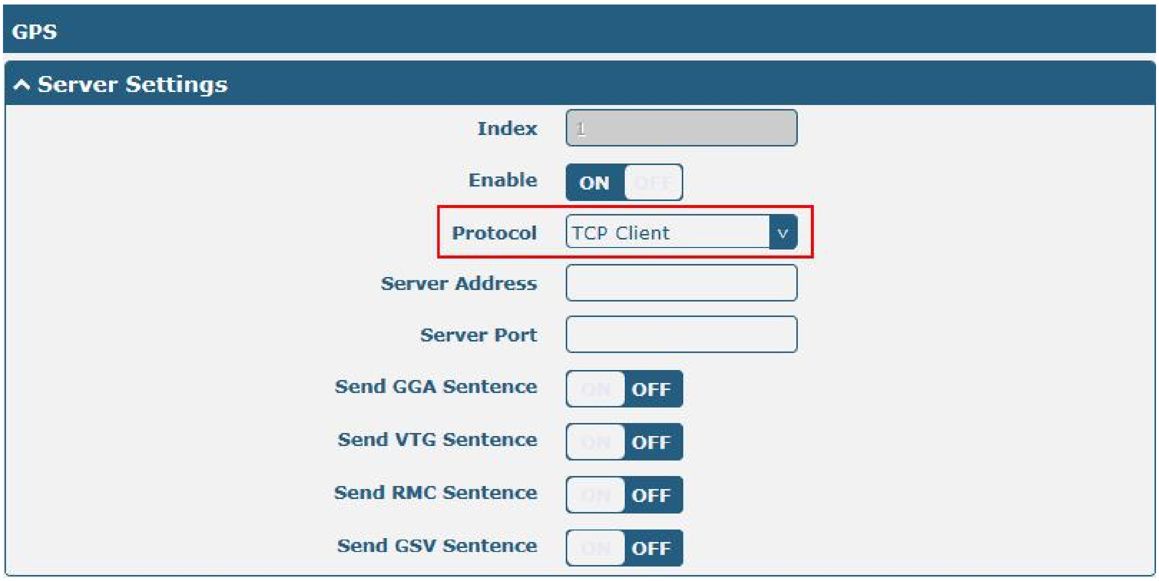
Report GSV Sentence: ON OFF

GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	+

GPS		
Item	**Description**	**Default**
General Settings		
Enable GPS	Click the toggle button to enable/disable the GPS option.	OFF
Sync GPS Time	Click the toggle button to synchronize the GPS time.	OFF
RS232 Report Settings		
Report to RS232	Submit the GPS information via RS232.	OFF
RS232 Number	Submit the GPS information via COM1 or COM 2.	COM1
Report GGA Sentence	Submit the GGA information.	OFF
Report VTG Sentence	Submit the VTG information.	OFF
Report RMC Sentence	Submit the RMC information.	OFF
Report GSV Sentence	Submit the GSV information.	OFF

The window is displayed as below when choosing “TCP Client” as the protocol.

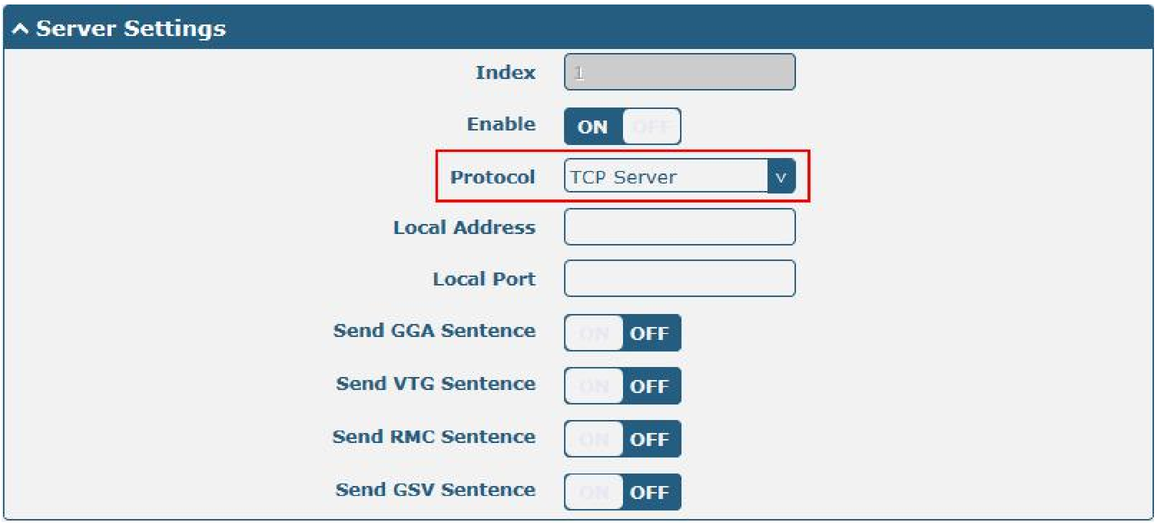


GPS

Server Settings

Index	1
Enable	ON
Protocol	TCP Client
Server Address	
Server Port	
Send GGA Sentence	OFF
Send VTG Sentence	OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

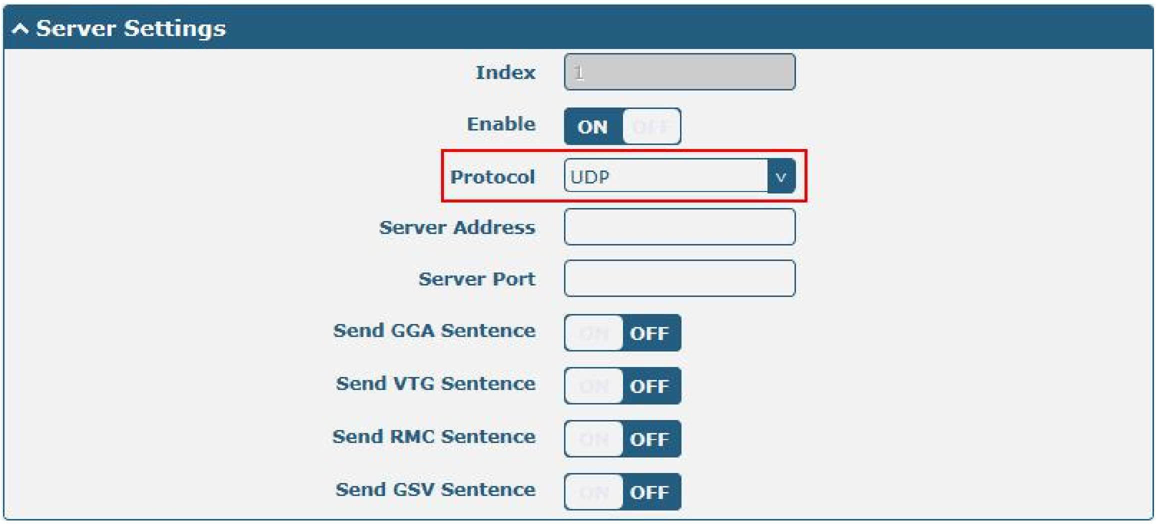
The window is displayed as below when choosing “TCP Server” as the protocol.



Server Settings

Index	1
Enable	ON
Protocol	TCP Server
Local Address	
Local Port	
Send GGA Sentence	OFF
Send VTG Sentence	OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

The window is displayed as below when choosing “UDP” as the protocol.

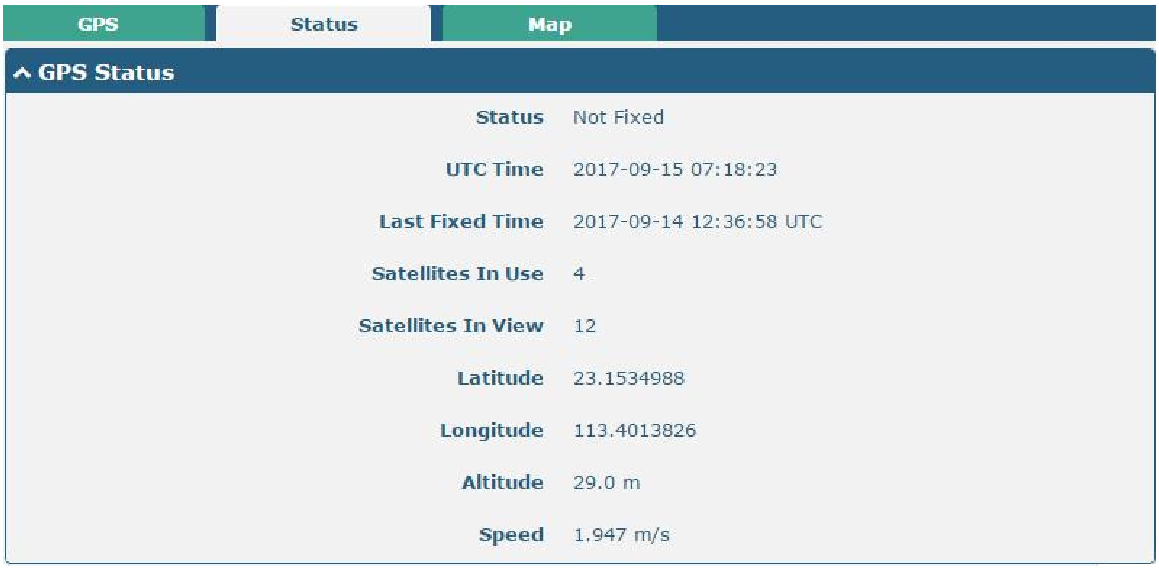


Server Settings

Index	1
Enable	ON
Protocol	UDP
Server Address	
Server Port	
Send GGA Sentence	OFF
Send VTG Sentence	OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

Server Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the GPS server settings.	ON
Protocol	Select from “TCP Client”, “TCP Server” or “UDP”.	TCP Client
Server Address @TCP Client	Set the address of the TCP Client.	Null
Server Port @TCP Client	Set the port of the remote TCP Server.	Null
Local Address	Set the local address when the gateway set as a TCP Server.	Null
Local Port	Set the local port when the gateway set as a TCP Server.	Null
Server Address @ UDP	Set the address of the TCP Server.	Null
Server Port @ UDP	Set the port of the remote TCP Server.	Null
Send GGA Sentence	Send GGA information in NMEA format.	OFF
Send VTG Sentence	Send VTG information in NMEA format.	OFF
Send RMC Sentence	Send RMC information in NMEA format.	OFF
Send GSV Sentence	Send GSV information in NMEA format.	OFF

Click the “Status” column to view the current status.



Status Not Fixed

UTC Time 2017-09-15 07:18:23

Last Fixed Time 2017-09-14 12:36:58 UTC

Satellites In Use 4

Satellites In View 12

Latitude 23.1534988

Longitude 113.4013826

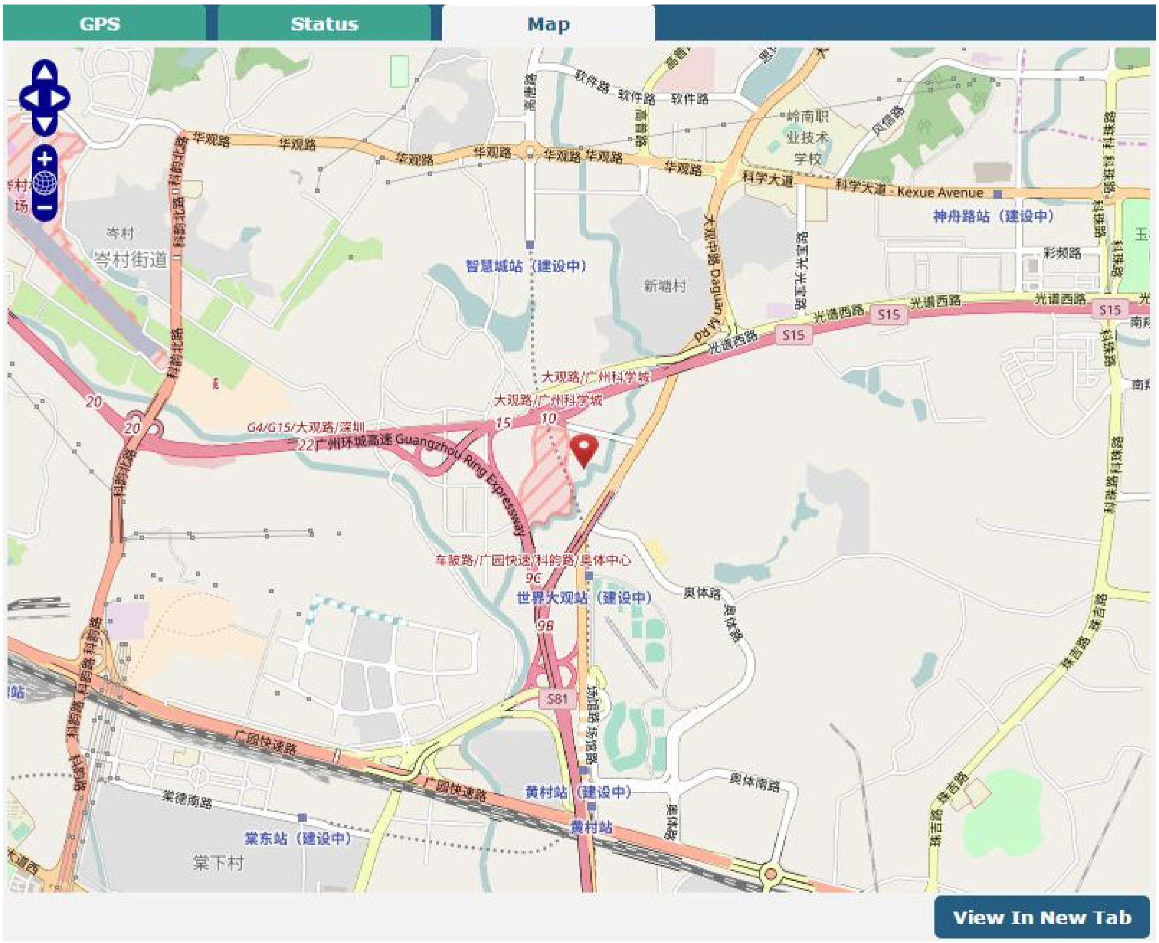
Altitude 29.0 m

Speed 1.947 m/s

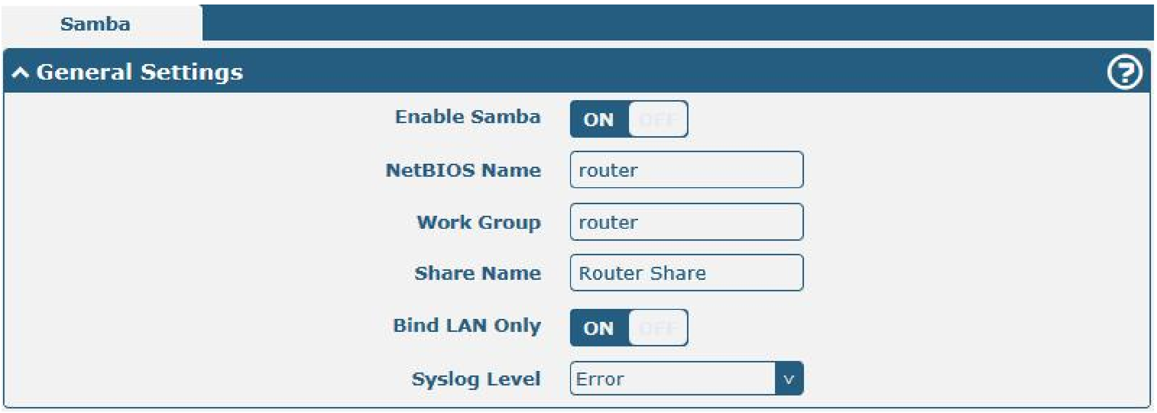
GPS Status	
Item	**Description**
Status	Show the GPS Status. GPS status includes “NO Fix”, “2D Fix” and “3D Fix”.
UTC Time	Show the UTC of satellites, which is world unified time, not local time.
Last Fixe Time	Show the last positioning time.
Satellites In Use	Show the satellite quantity in use.
Satellites In View	Show the satellite quantity in view.
Latitude	Show the latitude status of gateway.
Longitude	Show the longitude status of gateway.
Altitude	Show the altitude status of gateway.

GPS Status	
Item	**Description**
Speed	Show the horizontal speed of gateway.

Click “Map” column to view the current location of the gateway.



4.5.9 Samba

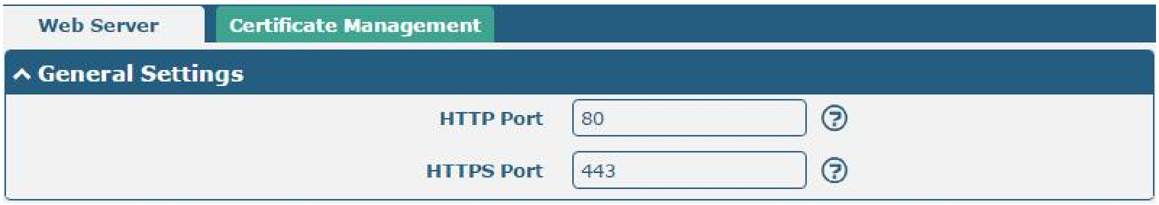


Enable Samba: ON
NetBIOS Name: router
Work Group: router
Share Name: Router Share
Bind LAN Only: ON
Syslog Level: Error

General @ Samba		
Item	**Description**	**Default**
Enable Samba	Click the toggle button to enable/disable Samba.	ON
NetBIOS Name	Enter the name of NETBIOS protocol for communication with Windows.	router
Work Group	Enter the work group.	router
Share Name	Enter share name.	Router Share
Bind LAN Only	Click the toggle button to bind LAN only.	ON
Syslog Level	Select the level of Syslog, with "Debug", "Info", "Notice", "Warn" and "Error" available.	Error

4.5.10 Web Server

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

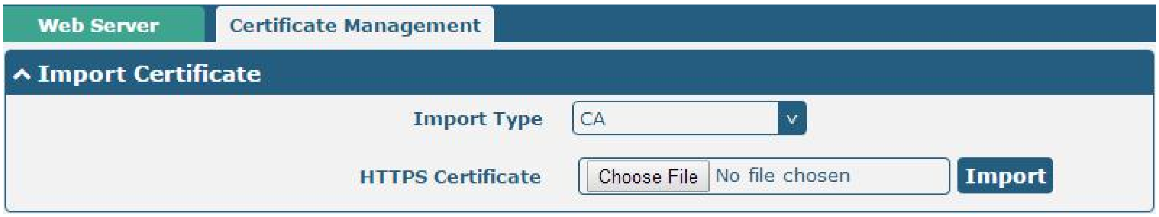


HTTP Port: 80
HTTPS Port: 443

General Settings @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in gateway's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the gateway with other HTTP Port number except 80, only adding that port number then you can login gateway's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in gateway'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 gateway with other HTTPS Port	443

	number except 443, only adding that port number then you can login gateway's Web Server. **Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	

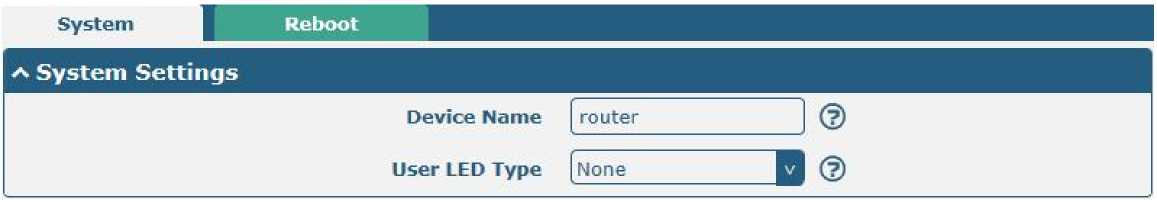
This section allows you to import the certificate file into the gateway.

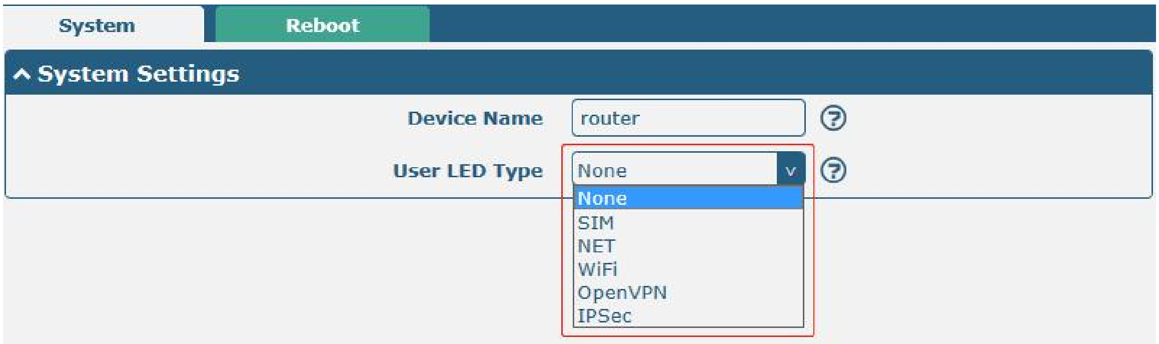


Import Certificate		
Item	**Description**	**Default**
Import Type	Select from “CA” and “Private Key”. • CA: a digital certificate issued by CA center • Private Key: a private key file	CA
HTTPS Certificate	Click on “Choose File” to locate the certificate file from your computer, and then click “Import” to import this file into your gateway.	--

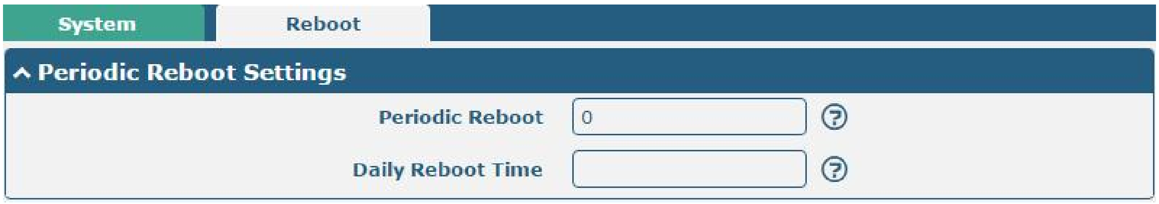
4.5.11 Advanced

This section allows you to set the Advanced and parameters.





System Settings		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	router
User LED Type	Specify the display type of your USR LED. Select from "None", "SIM", "NET", "WiFi", "OpenVPN" or "IPSec". • None: Meaningless indication, and the LED is off • SIM: USR indicator showing the SIM status • NET: USR indicator showing the NET status • WiFi: USR indicator showing the WiFi status • OpenVPN: USR indicator showing the OpenVPN status • IPSec: USR indicator showing the IPsec status **Note**: For more details about USR indicator, see "2.3 LED Indicators".	None



^ Periodic Reboot Settings

Periodic Reboot: 0

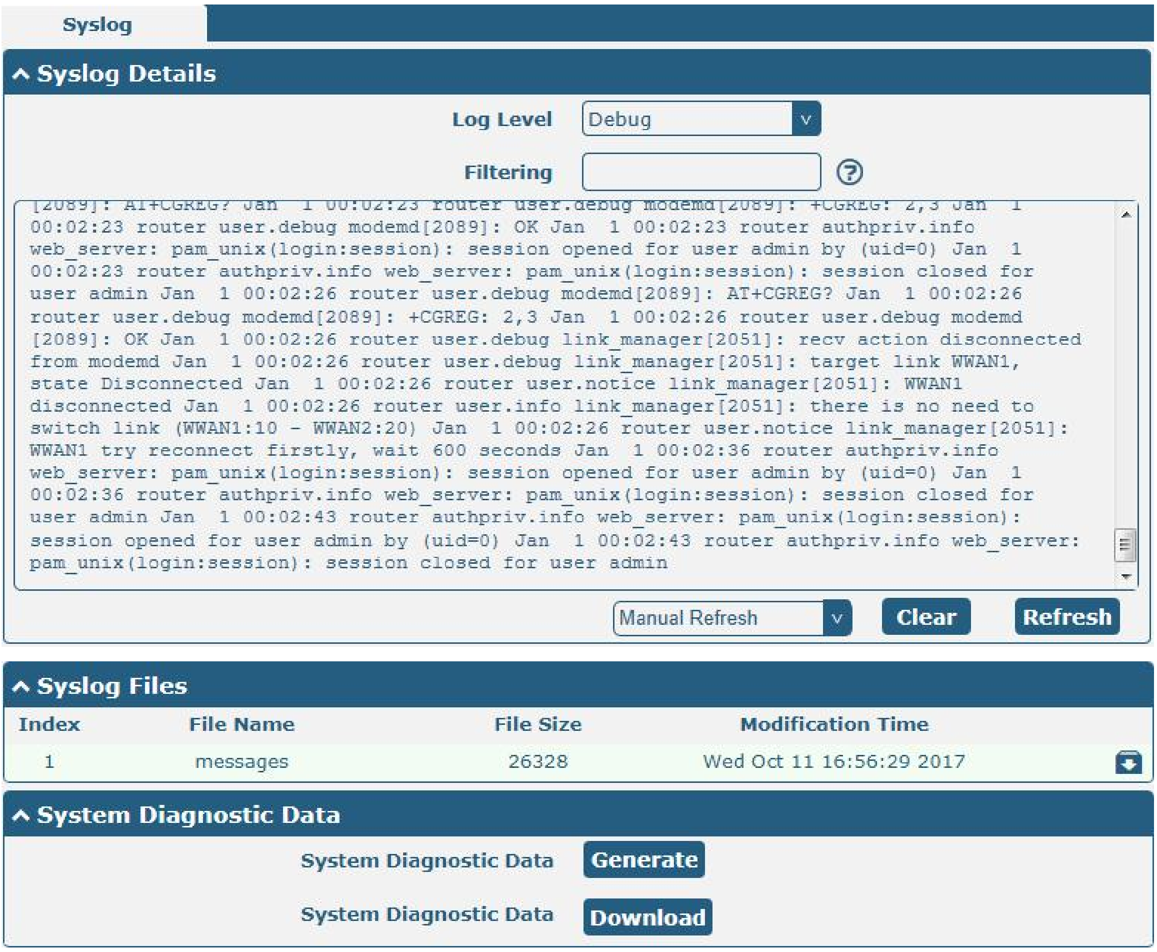
Daily Reboot Time:

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

4.6 System

4.6.1 Debug

This section allows you to check and download the syslog details. Click **Service > Syslog > Syslog Setting** to enable the syslog.



Log Level: Debug

Filtering:

```
[2089]: AT+CGREG? Jan  1 00:02:23 router user.debug modemd[2089]: +CGREG: 2,3 Jan  1
00:02:23 router user.debug modemd[2089]: OK Jan  1 00:02:23 router authpriv.info
web_server: pam_unix(login:session): session opened for user admin by (uid=0) Jan  1
00:02:23 router authpriv.info web_server: pam_unix(login:session): session closed for
user admin Jan  1 00:02:26 router user.debug modemd[2089]: AT+CGREG? Jan  1 00:02:26
router user.debug modemd[2089]: +CGREG: 2,3 Jan  1 00:02:26 router user.debug modemd
[2089]: OK Jan  1 00:02:26 router user.debug link_manager[2051]: recv action disconnected
from modemd Jan  1 00:02:26 router user.debug link_manager[2051]: target link WWAN1,
state Disconnected Jan  1 00:02:26 router user.notice link_manager[2051]: WWAN1
disconnected Jan  1 00:02:26 router user.info link_manager[2051]: there is no need to
switch link (WWAN1:10 - WWAN2:20) Jan  1 00:02:26 router user.notice link_manager[2051]:
WWAN1 try reconnect firstly, wait 600 seconds Jan  1 00:02:36 router authpriv.info
web_server: pam_unix(login:session): session opened for user admin by (uid=0) Jan  1
00:02:36 router authpriv.info web_server: pam_unix(login:session): session closed for
user admin Jan  1 00:02:43 router authpriv.info web_server: pam_unix(login:session):
session opened for user admin by (uid=0) Jan  1 00:02:43 router authpriv.info web_server:
pam_unix(login:session): session closed for user admin
```

Manual Refresh

Index	File Name	File Size	Modification Time
1	messages	26328	Wed Oct 11 16:56:29 2017

System Diagnostic Data: Generate

System Diagnostic Data: Download

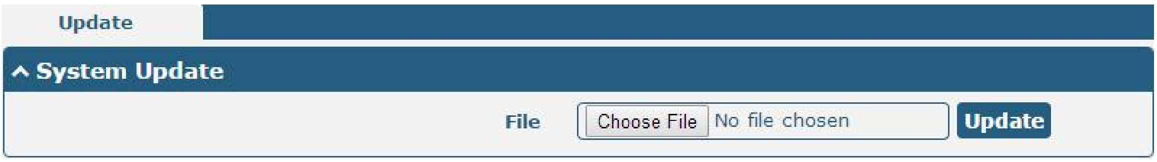
Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.	Null
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds” or “30 Seconds”. You can select these intervals to refresh the log information displayed in the follow box. If selecting “manual refresh”, you should click the refresh button to refresh the syslog.	Manual Refresh
Clear	Click the button to clear the syslog.	--
Refresh	Click the button to refresh the syslog.	--

Syslog Files		
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		
Generate	Click to generate the syslog diagnosing file.	--
Download	Click to download system diagnosing file.	--

4.6.2 Update

This section allows you to upgrade the firmware of your gateway. Click **System > Update > System Update**, and click on "Choose File" to locate the firmware file to be used for the upgrade. Once the latest firmware has been chosen, click "Update" to start the upgrade process. The upgrade process may take several minutes. Do not turn off your Gateway during the firmware upgrade process.

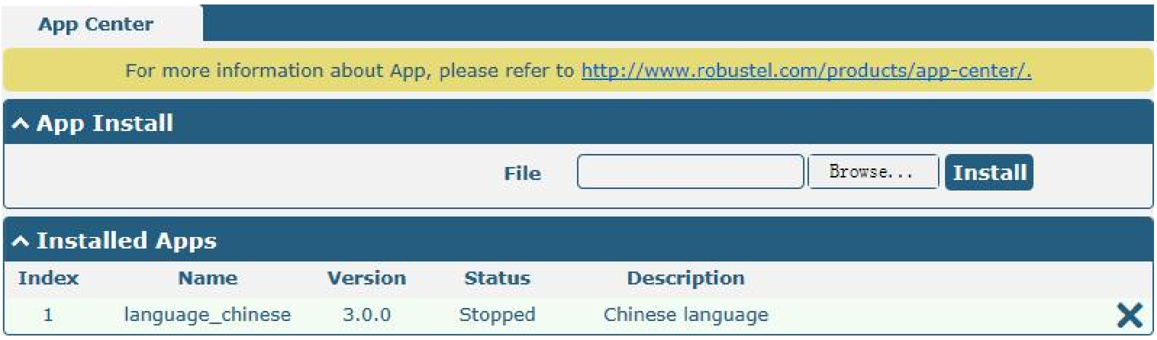
Note: To access the latest firmware file, please contact your technical support engineer.



4.6.3 App Center

This section allows you to add some required or customized applications to the gateway. Import and install your applications to the App Center, and reboot the device according to the system prompts. Each installed application will be displayed under the "Services" menu, while other applications related to VPN will be displayed under the "VPN" menu.

Note: After importing the applications to the gateway, the page display may have a slight delay due to the browser cache. It is recommended that you clear the browser cache first and log in the gateway again.

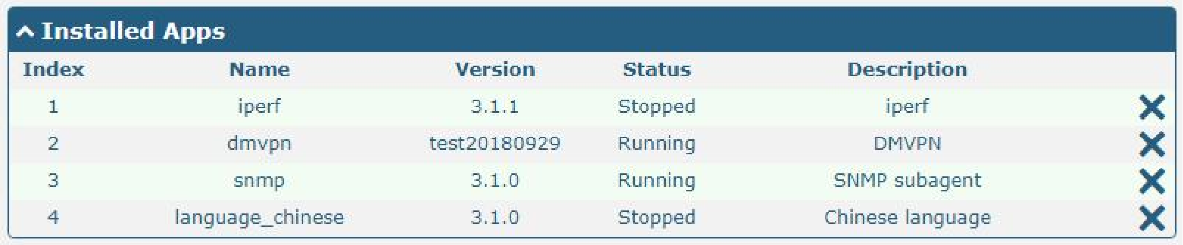


For more information about App, please refer to http://www.robustel.com/products/app-center/.

Index	Name	Version	Status	Description	
1	language_chinese	3.0.0	Stopped	Chinese language	✕

成功安装的 App 会在以下列表里显示，单击✕即可卸载该 App。

The window is displayed as below when successfully installed apps. Click ✕ to uninstall the app.



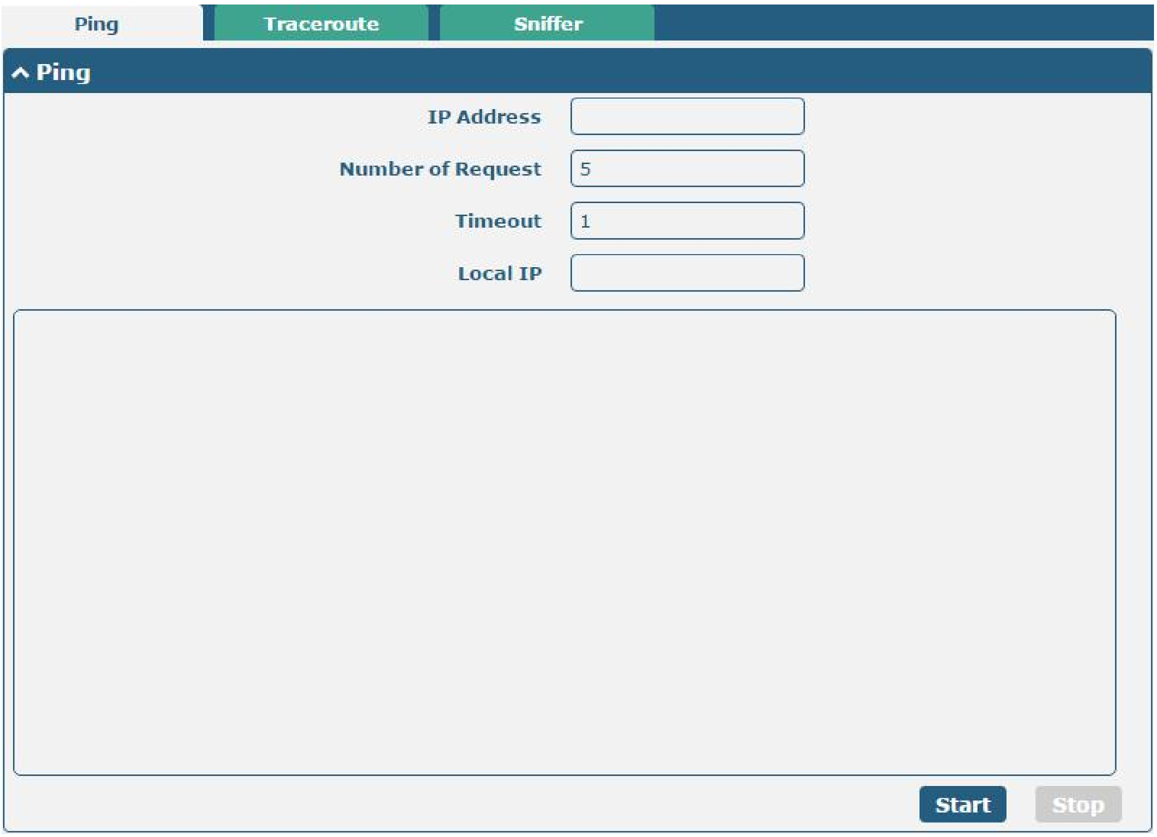
^ Installed Apps

Index	Name	Version	Status	Description	
1	iperf	3.1.1	Stopped	iperf	✕
2	dmvpn	test20180929	Running	DMVPN	✕
3	snmp	3.1.0	Running	SNMP subagent	✕
4	language_chinese	3.1.0	Stopped	Chinese language	✕

App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your computer, and then click **Install** to import this file into your gateway. **Note**: File format should be *xxx.rpk*, e.g. *MEG5000-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
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 for this App.	Null

4.6.4 Tools

This section provides users three tools: Ping, Traceroute and Sniffer. Ping is used to detect the network connectivity of the gateway.



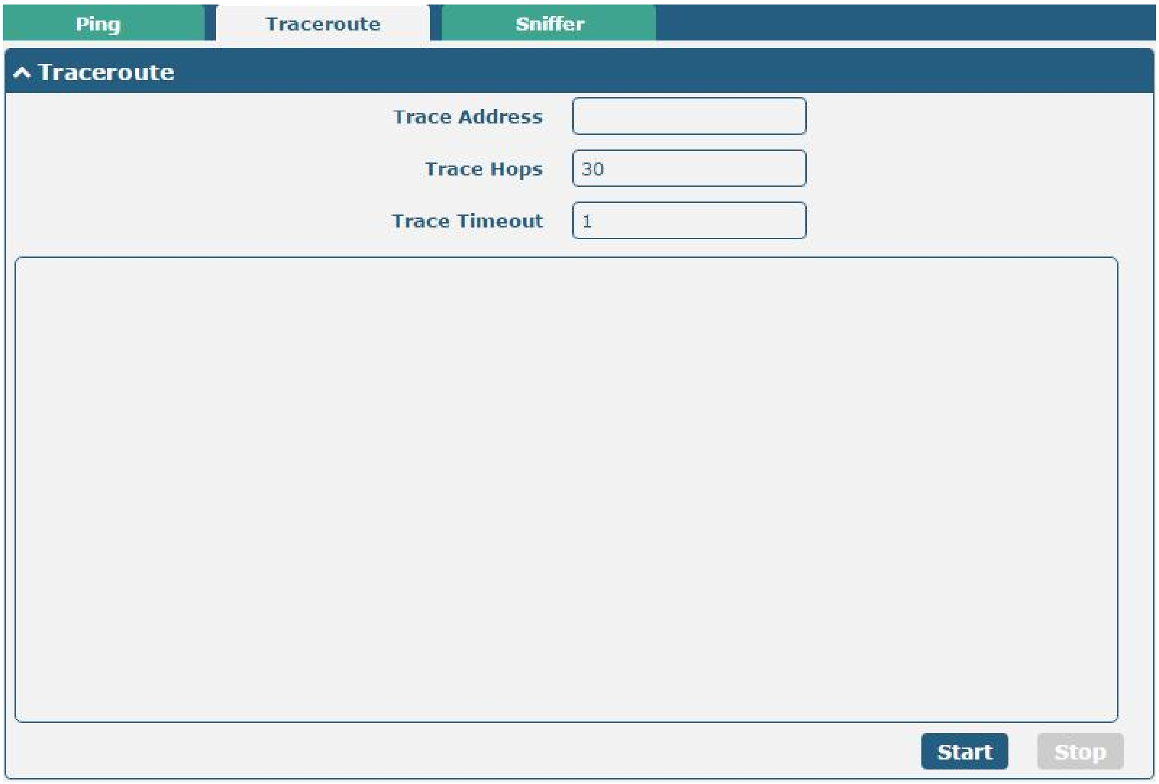
IP Address

Number of Request 5

Timeout 1

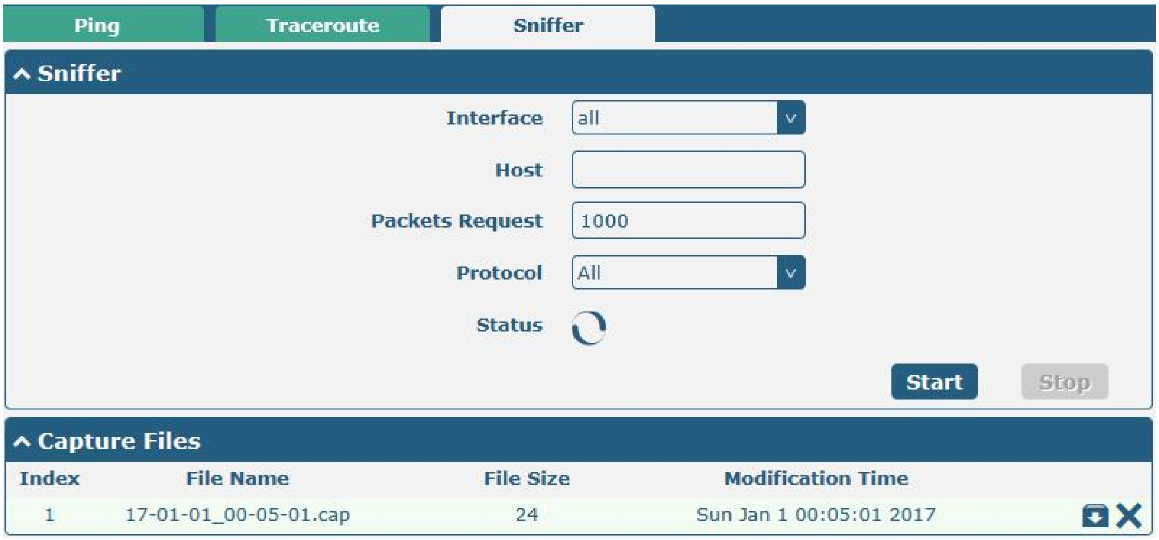
Local IP

Ping		
Item	**Description**	**Default**
IP address	Enter the ping's destination IP address or destination domain.	Null
Number of Requests	Specify the number of ping requests.	5
Timeout	Specify the timeout of ping requests.	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.	--



Trace Address
Trace Hops 30
Trace Timeout 1

Traceroute		
Item	**Description**	**Default**
Trace Address	Enter the trace's destination IP address or destination domain.	Null
Trace Hops	Specify the max trace hops. Gateway will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify the 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.	--



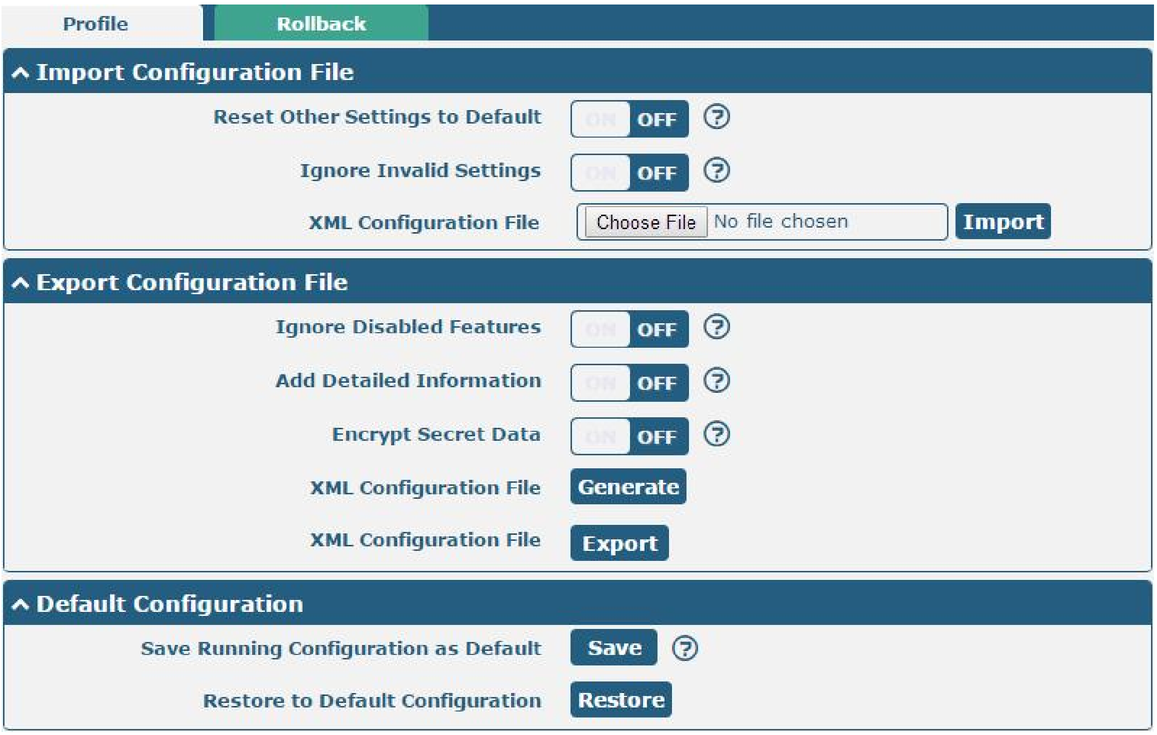
Interface all
Host
Packets Request 1000
Protocol All
Status

Index	File Name	File Size	Modification Time
1	17-01-01_00-05-01.cap	24	Sun Jan 1 00:05:01 2017

Sniffer		
Item	**Description**	**Default**
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number from 10 to 40000 that the gateway can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
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 you click this button, a new log file will be displayed in the following 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

4.6.5 Profile

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



^ Import Configuration File

Reset Other Settings to Default: ON OFF ?

Ignore Invalid Settings: ON OFF ?

XML Configuration File: Choose File No file chosen Import

^ Export Configuration File

Ignore Disabled Features: ON OFF ?

Add Detailed Information: ON OFF ?

Encrypt Secret Data: ON OFF ?

XML Configuration File: Generate

XML Configuration File: Export

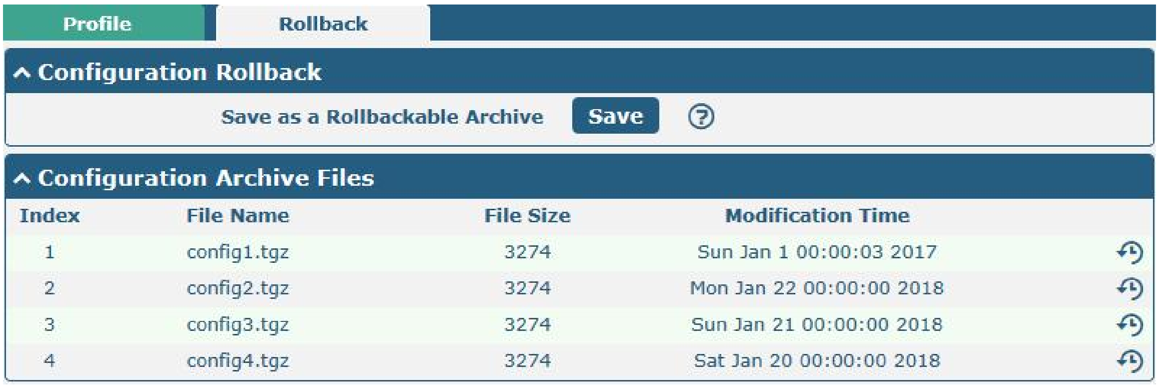
^ Default Configuration

Save Running Configuration as Default: Save ?

Restore to Default Configuration: Restore

Profile		
Item	**Description**	**Default**
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as "ON" to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as "OFF" to ignore invalid settings.	OFF

XML Configuration File	Click on Choose File to locate the XML configuration file from your computer, and then click Import to import this file into your gateway.	--
Export Configuration File		
Ignore Disabled Features	Click the toggle button as “OFF” to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as “On” to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as “ON” to encrypt the secret data.	OFF
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click this button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click this button to restore the factory defaults.	--



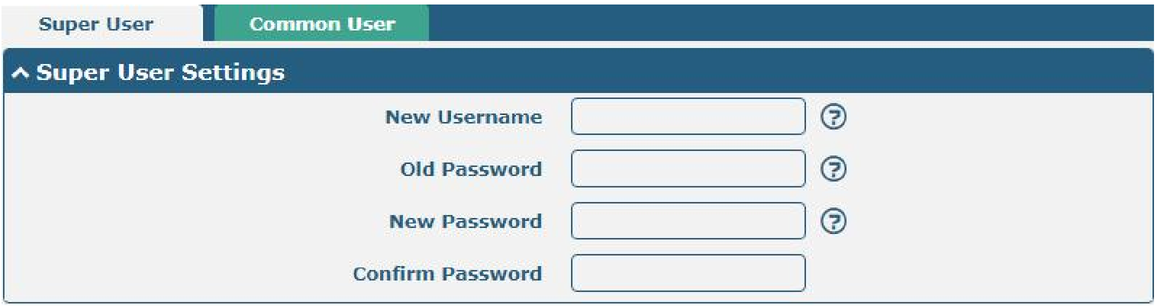
Index	File Name	File Size	Modification Time
1	config1.tgz	3274	Sun Jan 1 00:00:03 2017
2	config2.tgz	3274	Mon Jan 22 00:00:00 2018
3	config3.tgz	3274	Sun Jan 21 00:00:00 2018
4	config4.tgz	3274	Sat Jan 20 00:00:00 2018

Rollback		
Item	**Description**	**Default**
Configuration Rollback		
Save as a Rollbackable Archive	Create a save point manually. Additionally, the system will create a save point every day automatically if configuration changes.	--
Configuration Archive Files		
Configuration Archive Files	View the related information about configuration archive files, including name, size and modification time.	--

4.6.6 User Management

This section allows you to change your username and password, and create or manage user accounts. One gateway has only one super user who has the highest authority to modify, add and manage other common users.

Note: Your new password must be more than 5 character and less than 32 characters and may contain numbers, upper and lowercase letters, and standard symbols.



^ Super User Settings

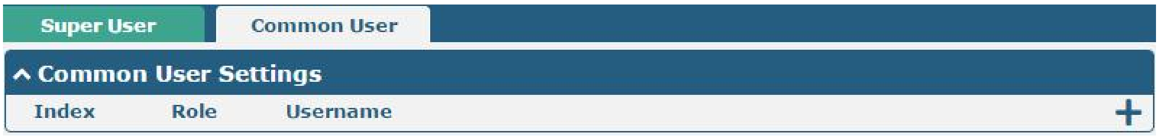
New Username

Old Password

New Password

Confirm Password

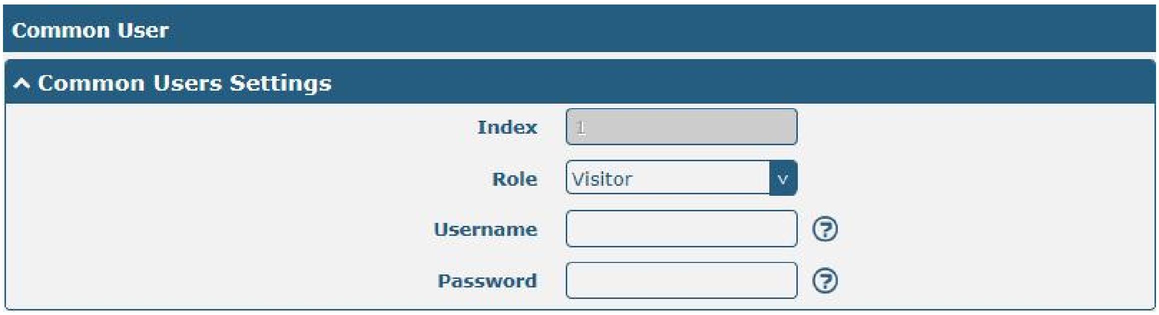
Super User Settings		
Item	**Description**	**Default**
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Old Password	Enter the old password of your gateway. The default is “admin”.	Null
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Confirm Password	Enter the new password again to confirm.	Null



^ Common User Settings

Index	Role	Username

Click + button to add a new common user. The maximum rule count is 5.



Common User

^ Common Users Settings

Index: 1

Role: Visitor

Username

Password

Common User Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. • Visitor: Users only can view the configuration of gateway under this level • Editor: Users can view and set the configuration of gateway under this level	Visitor

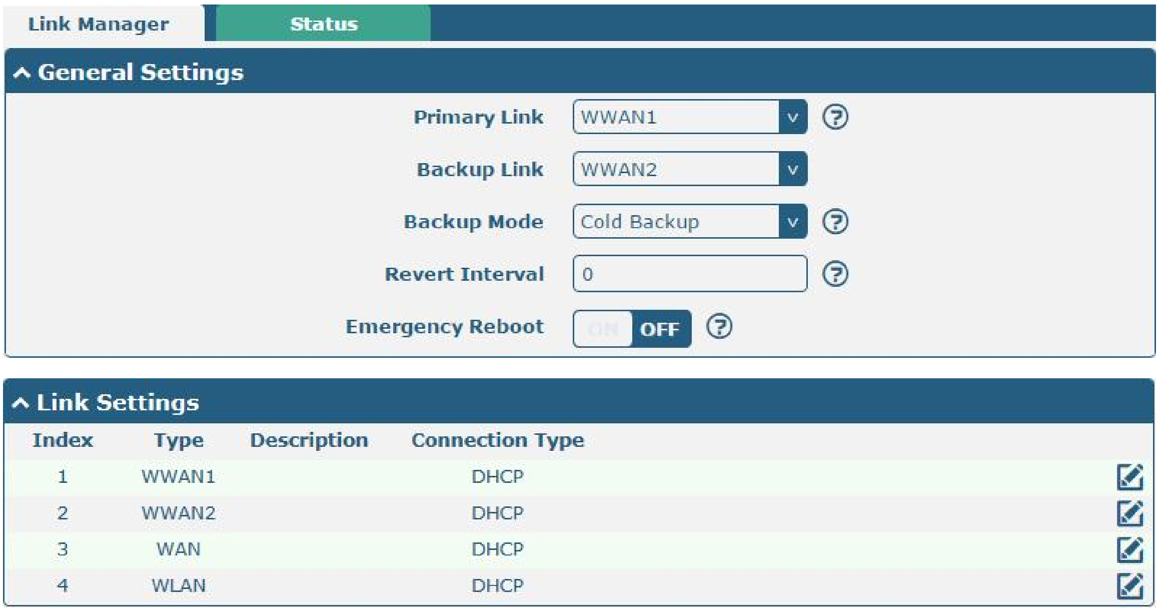
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	Null

Chapter 5 Configuration Examples

5.1 Cellular

5.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the gateway correctly and insert two SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > Link Manager > General Settings**, choose “WWAN1” as the primary link, “WWAN2” as the backup link and “Cold Backup” as the backup mode.



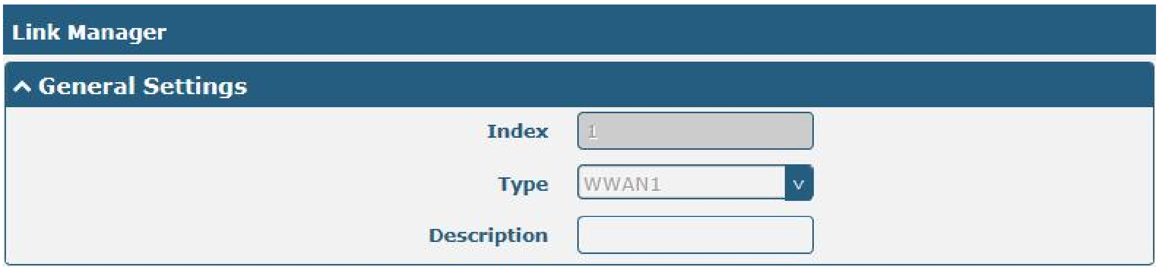
General Settings

Primary Link	WWAN1
Backup Link	WWAN2
Backup Mode	Cold Backup
Revert Interval	0
Emergency Reboot	ON OFF

Link Settings

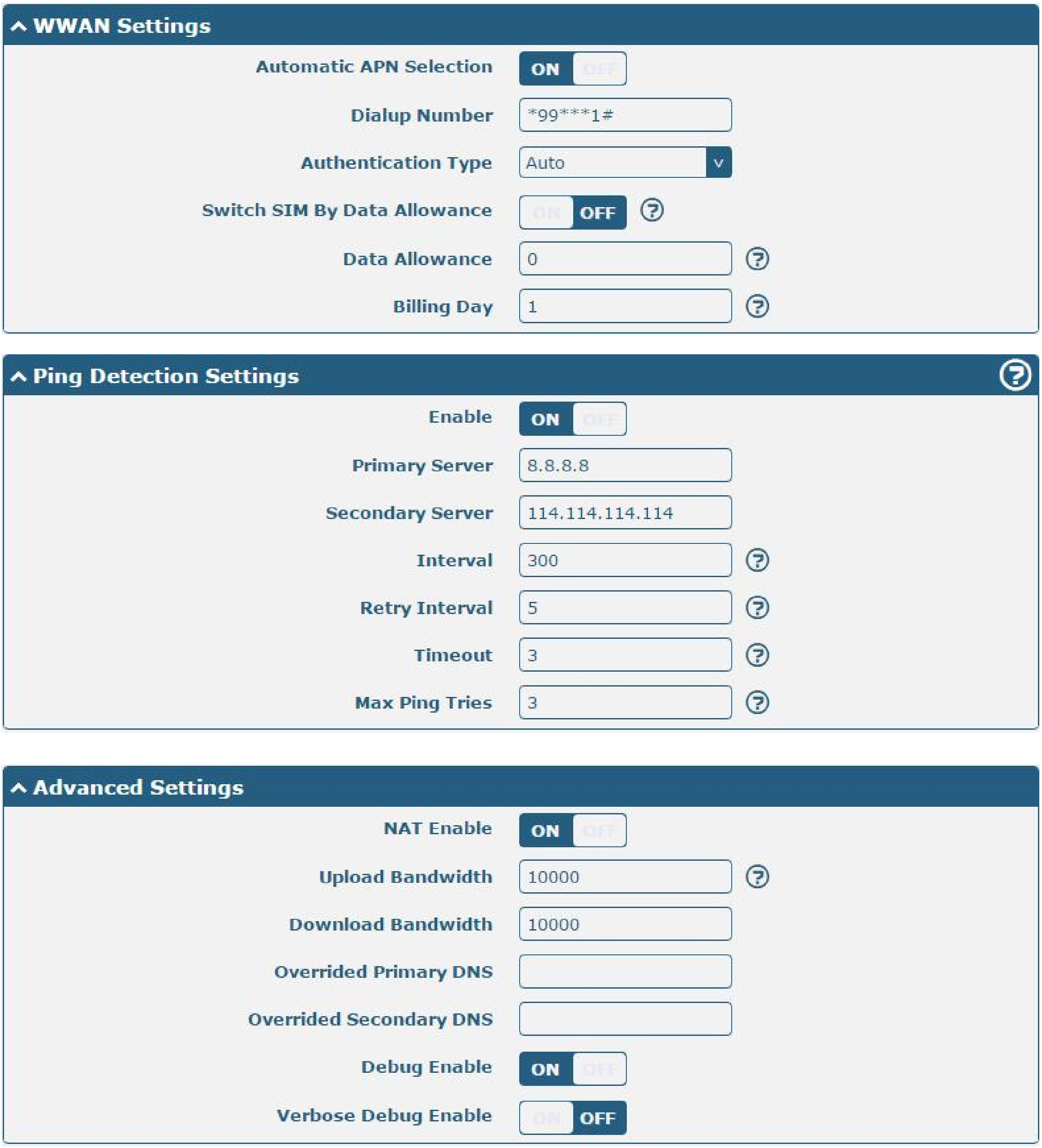
Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP
3	WAN		DHCP
4	WLAN		DHCP

Click the edit button of WWAN1 to set its parameters according to the current ISP.


Link Manager

General Settings

Index	1
Type	WWAN1
Description	



^ WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

^ Ping Detection Settings

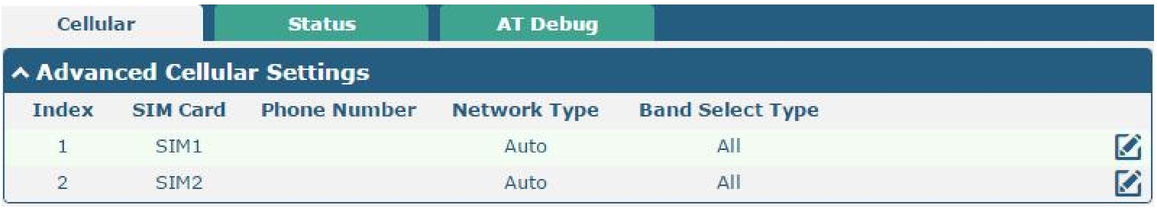
Enable	ON
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3

^ Advanced Settings

NAT Enable	ON
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click **Submit > Save & Apply** for the configuration to take effect.

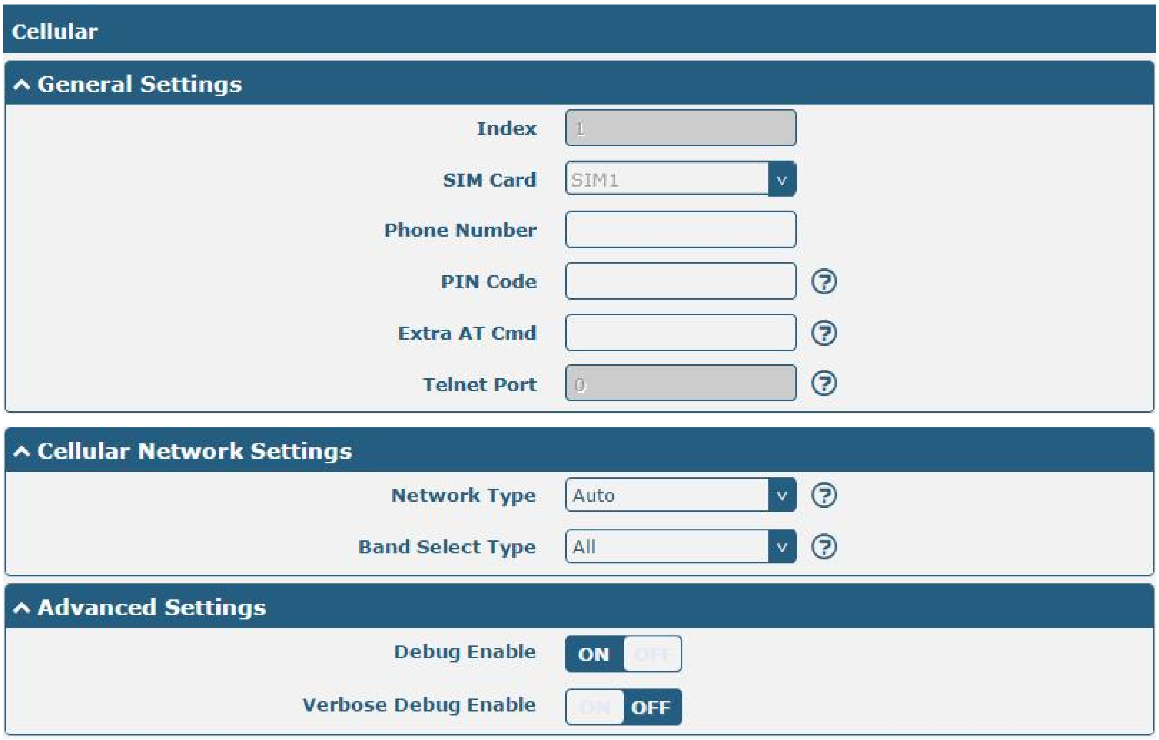
The window is displayed below by clicking **Interface > Cellular > Advanced Cellular Settings**.



^ Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click the edit button of SIM1 to set its parameters according to your application request.



Cellular

^ General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

^ Cellular Network Settings

Network Type	Auto
Band Select Type	All

^ Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF

When finished, click **Submit > Save & Apply** for the configuration to take effect.

5.1.2 SMS Remote Control

The gateway supports remote control via SMS. You can use following commands to get the status of the gateway, and set all the parameters. There are three authentication types for SMS control. You can select from “Password”, “Phonenum” or “Both”.

An SMS command has the following structure:

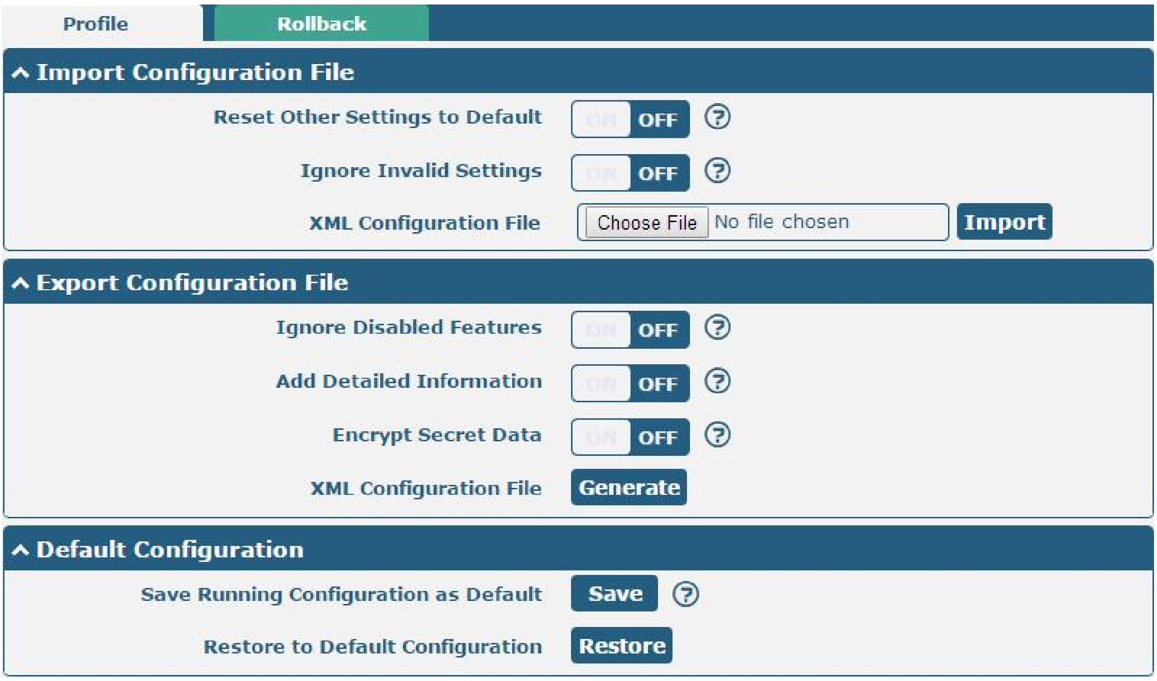
1. Password mode—**Username: Password; cmd1; cmd2; cmd3; …cmdn** (available for every phone number).
2. Phonenum mode—**Password, cmd1; cmd2; cmd3; … cmdn** (available when the SMS was sent from the phone number which had been added in gateway’s phone group).
3. Both mode-- **Username: Password; cmd1; cmd2; cmd3; …cmdn** (available when the SMS was sent from the phone number which had been added in gateway’s phone group).

SMS command Explanation:

1. User name and Password: Use 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, more details about CLI cmd please refer to **Chapter 5 Introductions for CLI**.

   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.

   Go to **System > Profile > Export Configuration File**, click **Generate** to generate the XML file and click **Export** to export the XML file.



XML command:

```
<lan>
<network max_Entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.10.66</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS cmd：

set lan network 1 interface lan0
set lan network 1 ip 172.16.10.66
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500

3. The semicolon character (‘;’) is used to separate more than one commands packed in a single SMS.
4. E.g.

   admin:admin;status system

   In this command, username is “admin”, password is “admin”, and the function of the command is to get the system status.

   SMS received:

   hardware_version = 1.0
   firmware_version = "1.0.0"
   kernel_version = 4.1.30
   device_model = MEG5000
   serial_number = 11002217110001
   uptime = "0 days, 05:17:45"
   system_time = "Sun Jan 1 05:17:02 2017"

admin:admin;reboot

In this command, username is “admin”, password is “admin”, and the command is to reboot the Gateway.

SMS received:

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is “admin”, password is “admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received:

OK

OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

In this command, username is “admin”, password is “admin”, and the commands is to configure the LAN parameter.

SMS received:

OK

OK

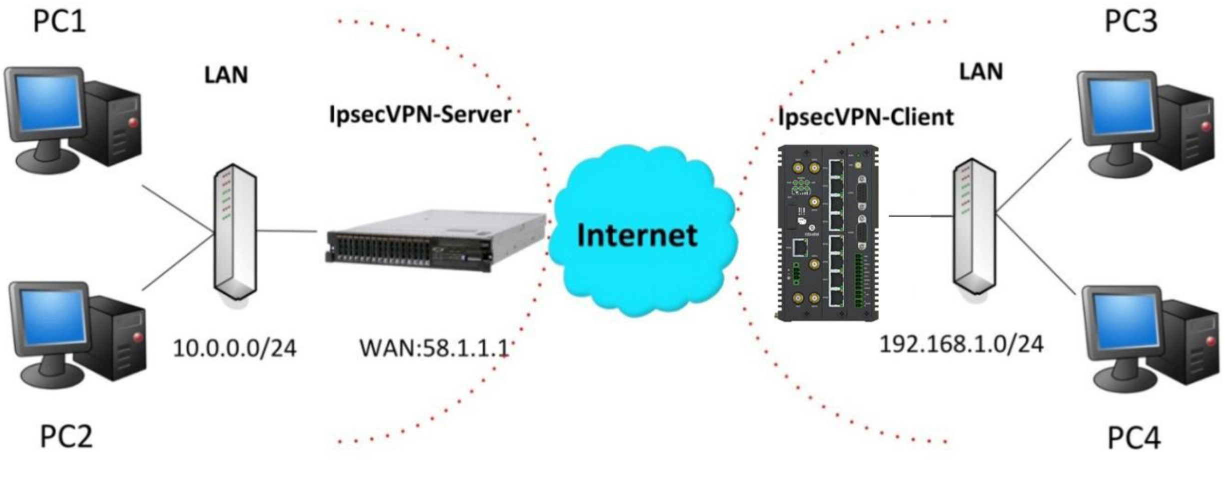
OK

OK

5.2 VPN Configuration Examples

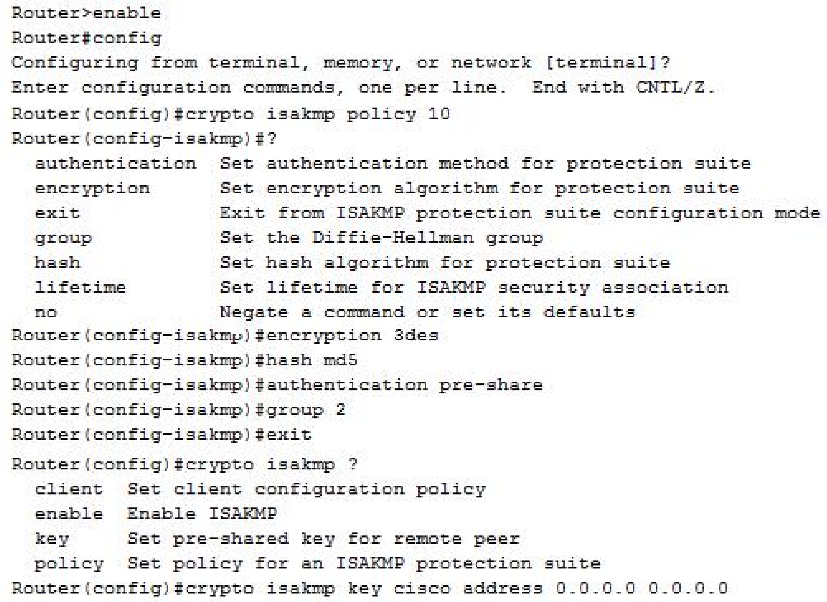
5.2.1 IPsec VPN

The configuration of server and client is as follows. (The IKE and SA parameters must be consistent between the server and the client.)

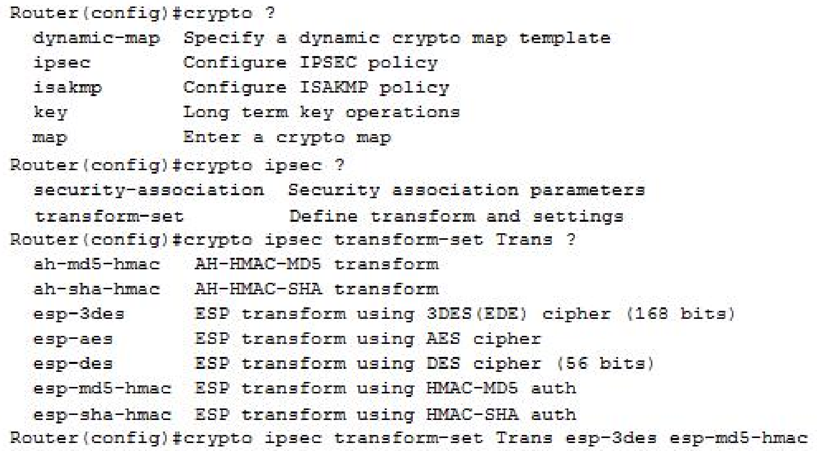


IPsec VPN_Server:

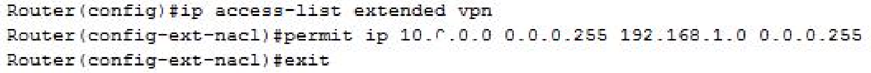
Cisco 2811:



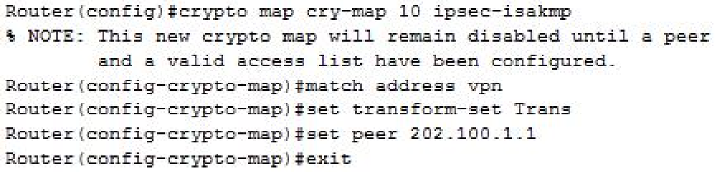
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set 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
```



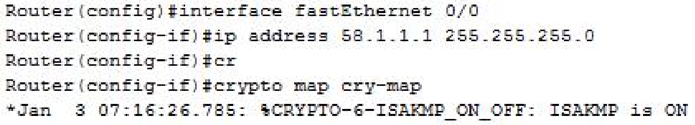
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association 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
```



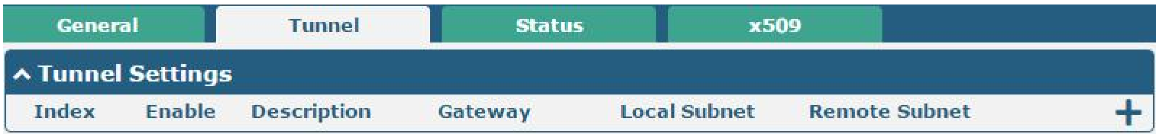
```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1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

IPsec VPN_Client:

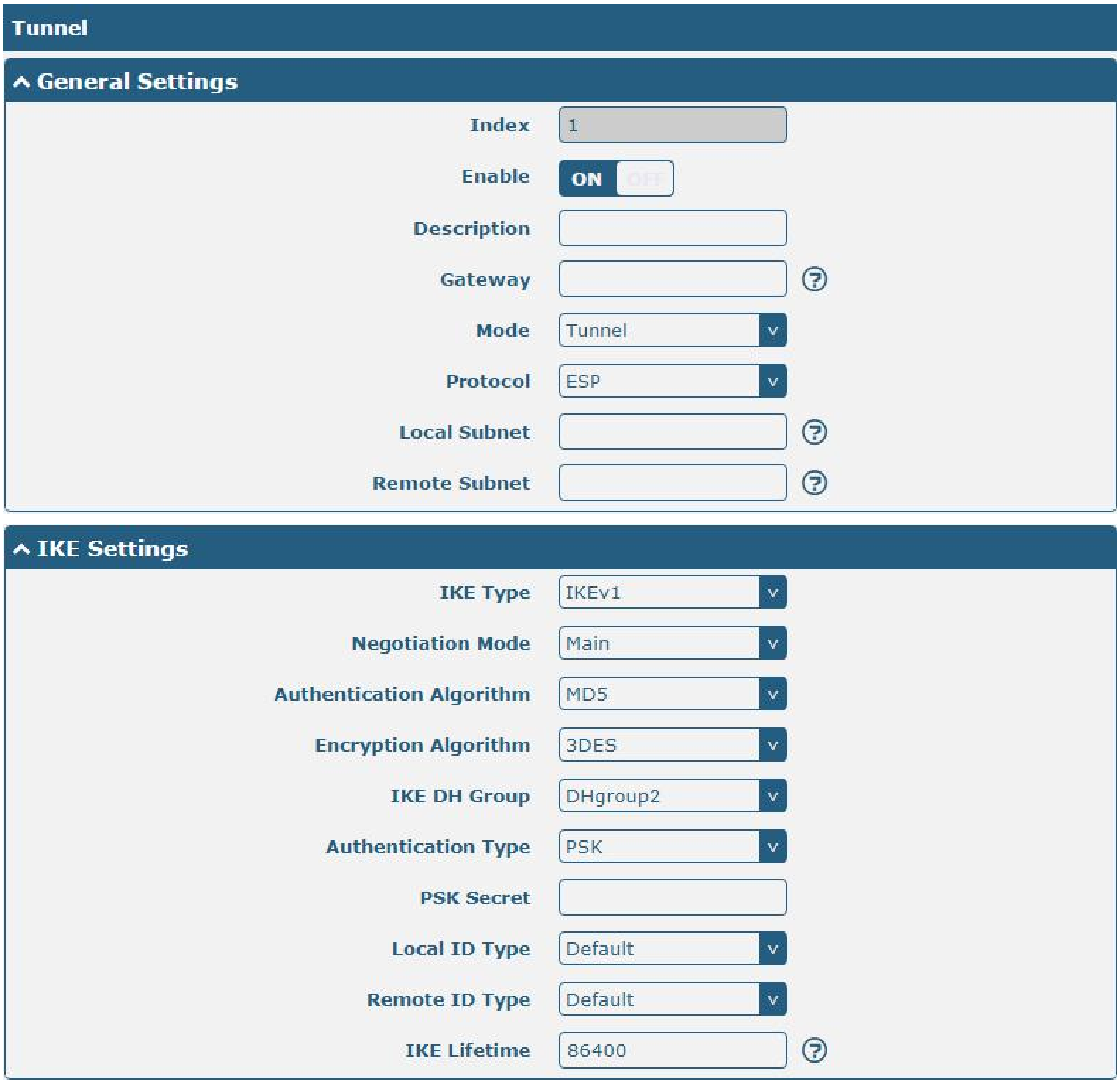
The window is displayed as below by clicking **VPN > IPsec > Tunnel**.



^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

Click + button and set the parameters of IPsec Client as below.



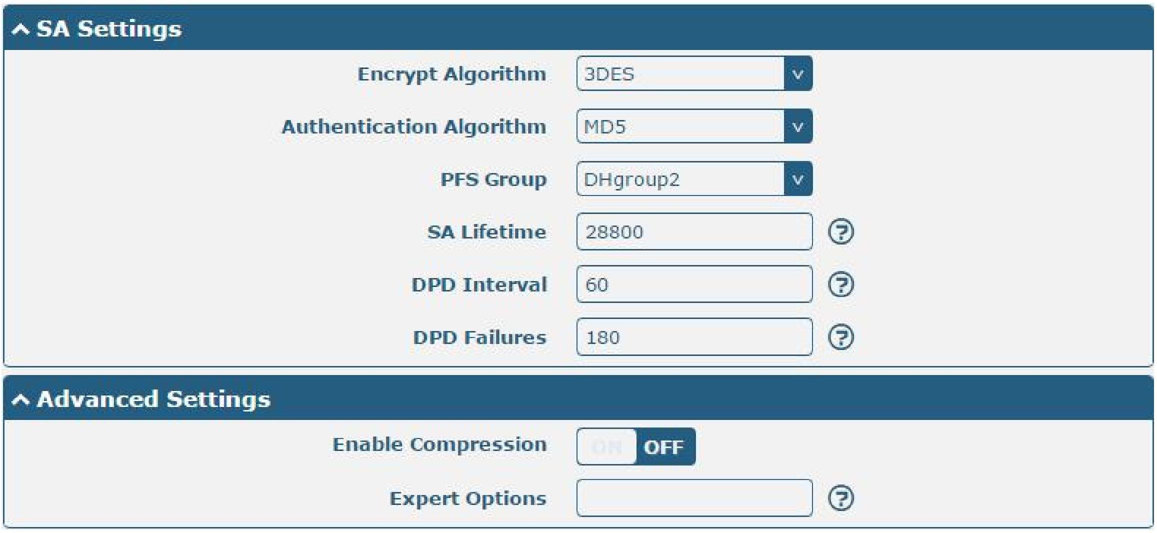
Tunnel

^ General Settings

Index	1	
Enable	ON OFF	
Description		
Gateway		?
Mode	Tunnel	
Protocol	ESP	
Local Subnet		?
Remote Subnet		?

^ IKE Settings

IKE Type	IKEv1	
Negotiation Mode	Main	
Authentication Algorithm	MD5	
Encryption Algorithm	3DES	
IKE DH Group	DHgroup2	
Authentication Type	PSK	
PSK Secret		
Local ID Type	Default	
Remote ID Type	Default	
IKE Lifetime	86400	?



^ SA Settings

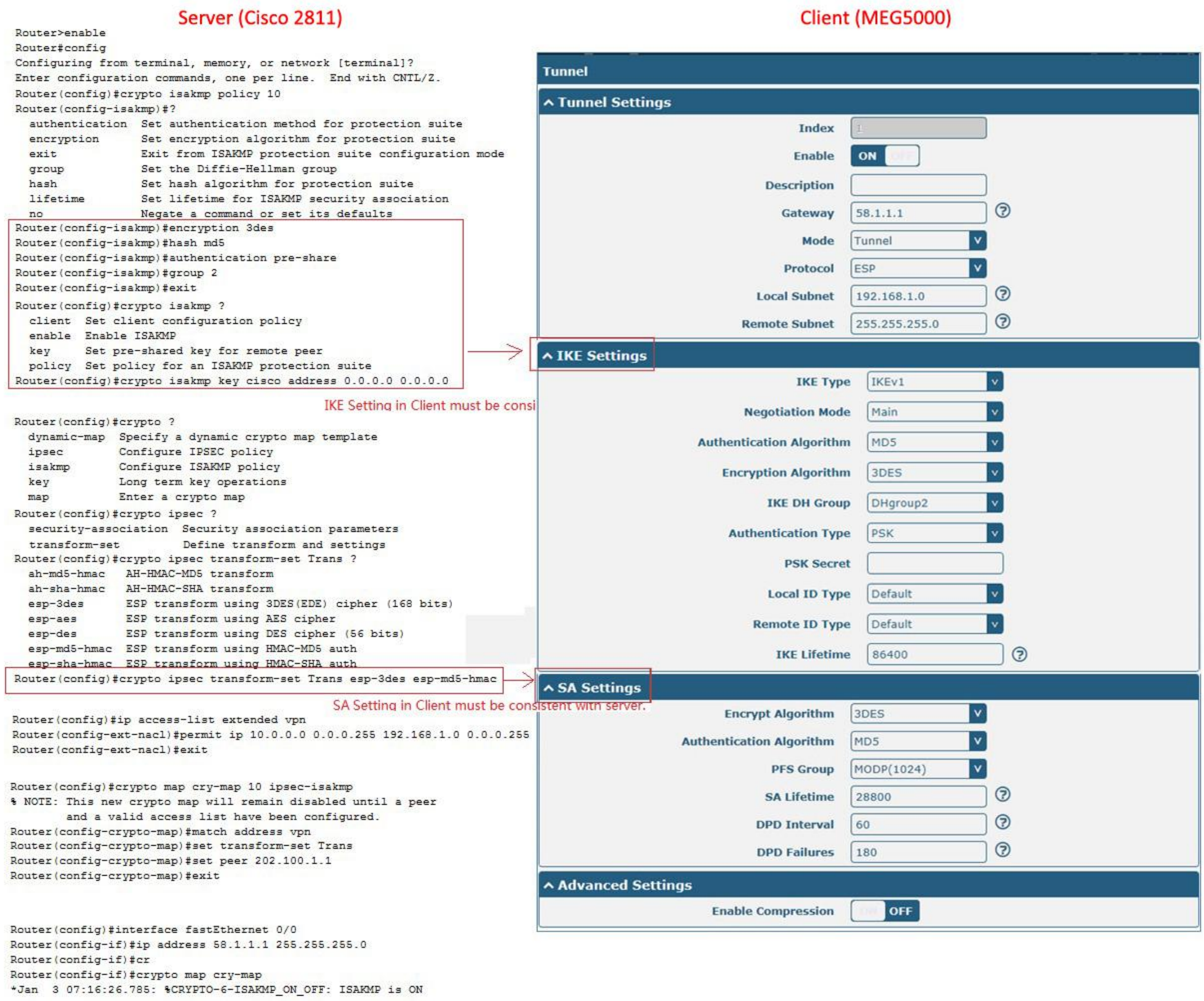
Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

^ Advanced Settings

Enable Compression	ON OFF
Expert Options	

When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between server and client is as below.



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 consi

```
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 (MEG5000)

Tunnel

^ Tunnel Settings

Index	1
Enable	ON OFF
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0
Remote Subnet	255.255.255.0

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

^ SA Settings

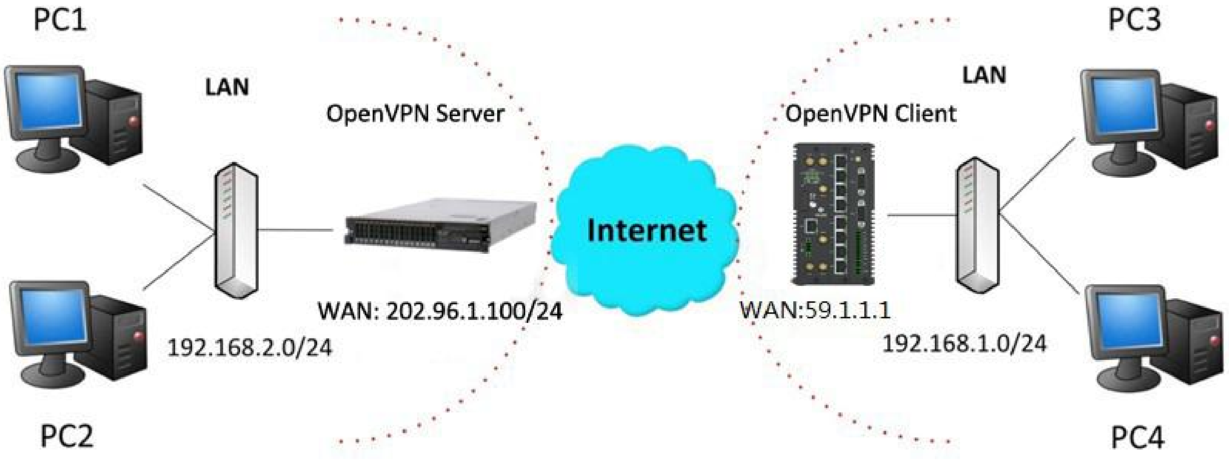
Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

^ Advanced Settings

Enable Compression	ON OFF

5.2.2 OpenVPN

OpenVPN supports two modes, including Client and P2P. Here takes Client as an example.



OpenVPN_Server:

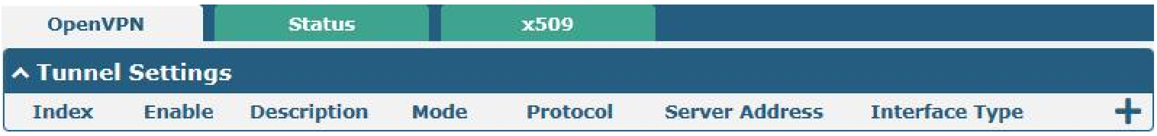
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Note: For more configuration details, please contact your technical support engineer.

OpenVPN_Client:

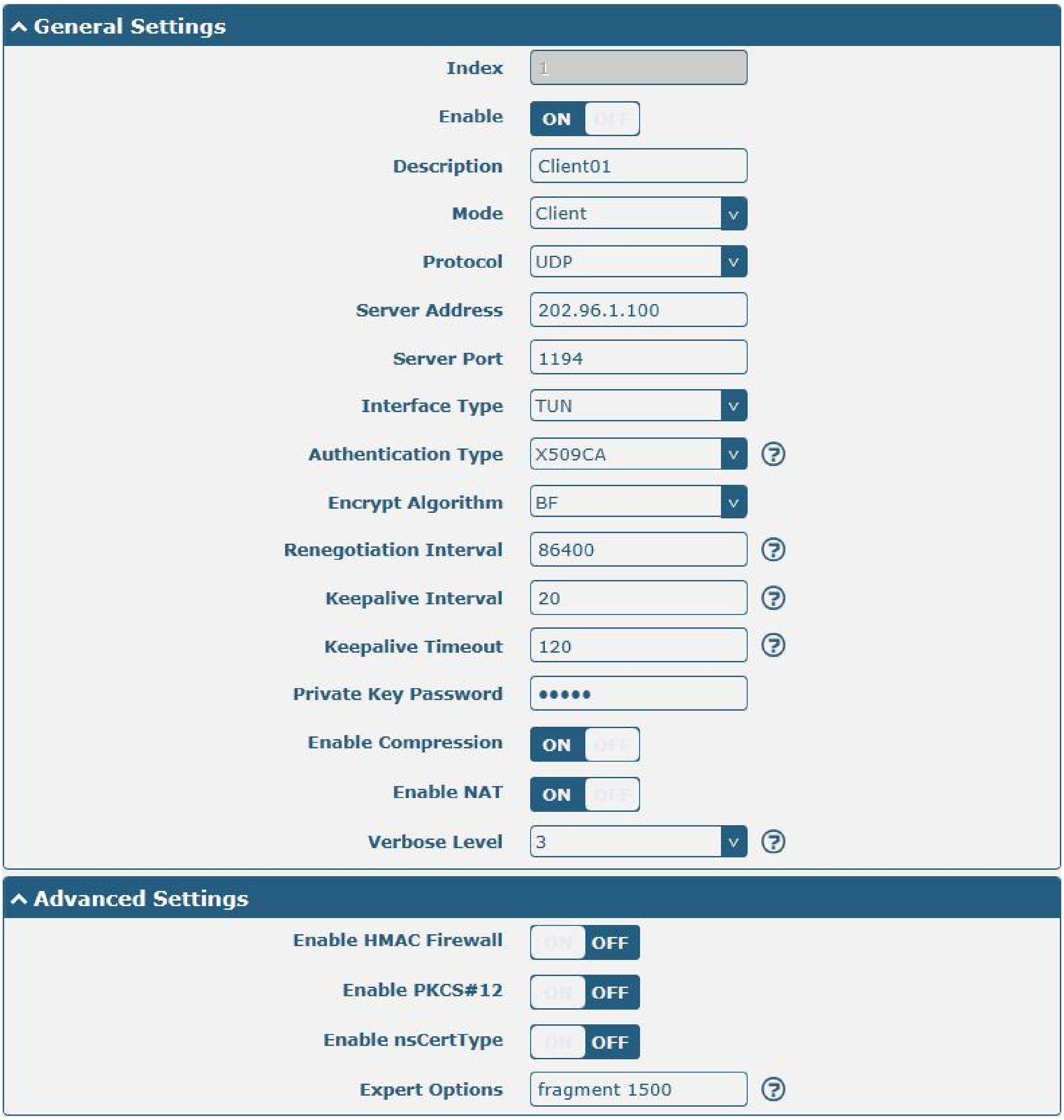
Click **VPN > OpenVPN > OpenVPN** as below.



Tunnel Settings

Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

Click + to configure the Client01 as below.



General Settings

Index	1
Enable	ON
Description	Client01
Mode	Client
Protocol	UDP
Server Address	202.96.1.100
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Private Key Password	•••••
Enable Compression	ON
Enable NAT	ON
Verbose Level	3

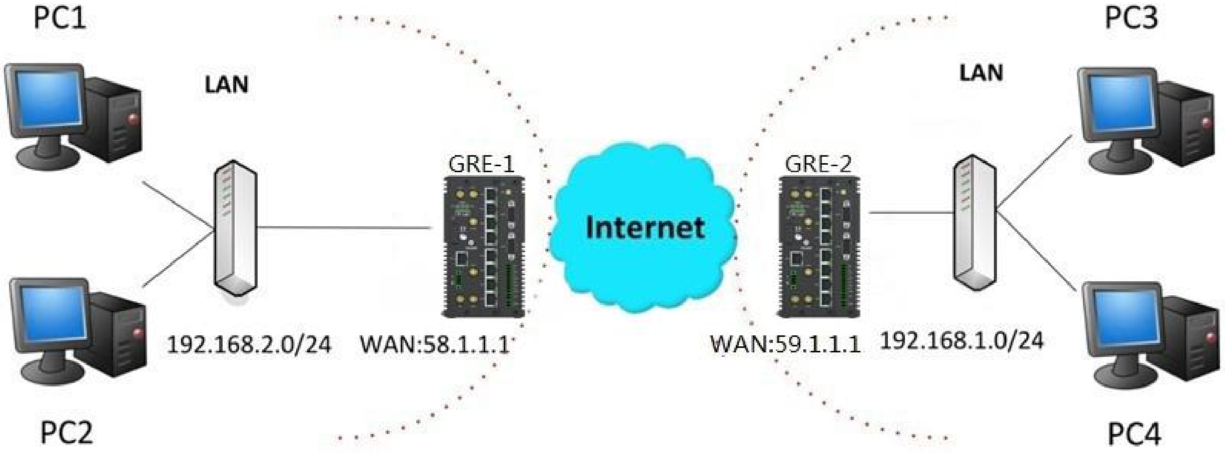
Advanced Settings

Enable HMAC Firewall	OFF
Enable PKCS#12	OFF
Enable nsCertType	OFF
Expert Options	fragment 1500

When finished, click **Submit > Save & Apply** for the configuration to take effect.

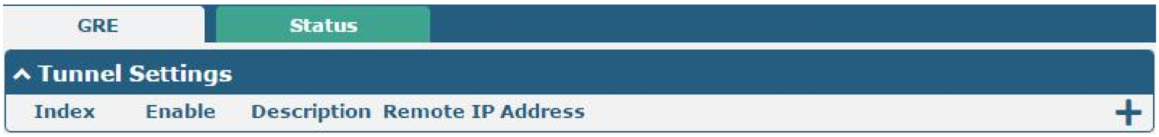
5.2.3 GRE VPN

The configuration of two points is as follows.

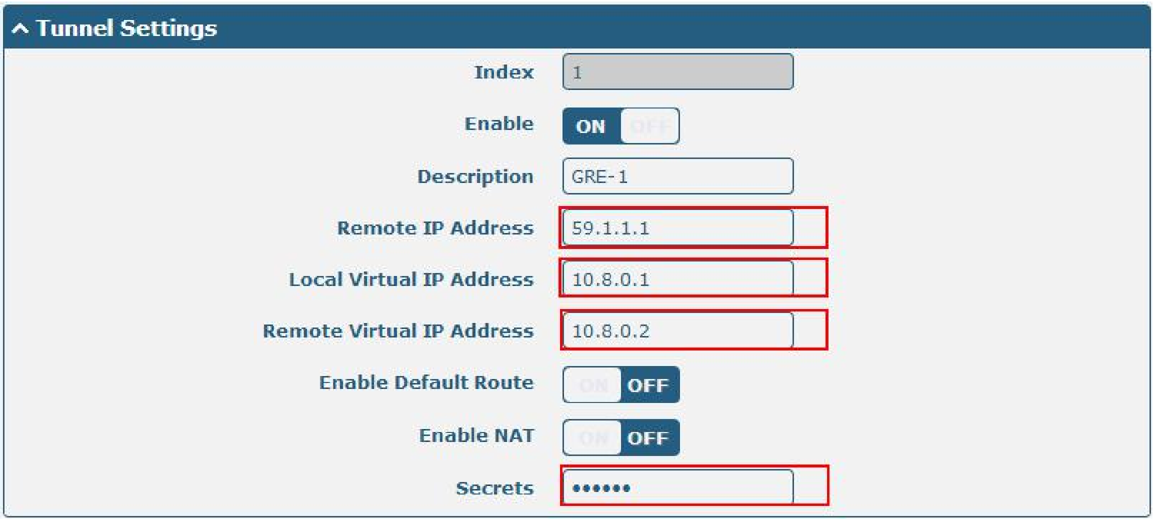


GRE-1:

The window is displayed as below by clicking **VPN > GRE > GRE**.



Click + button and set the parameters of GRE-1 as below.



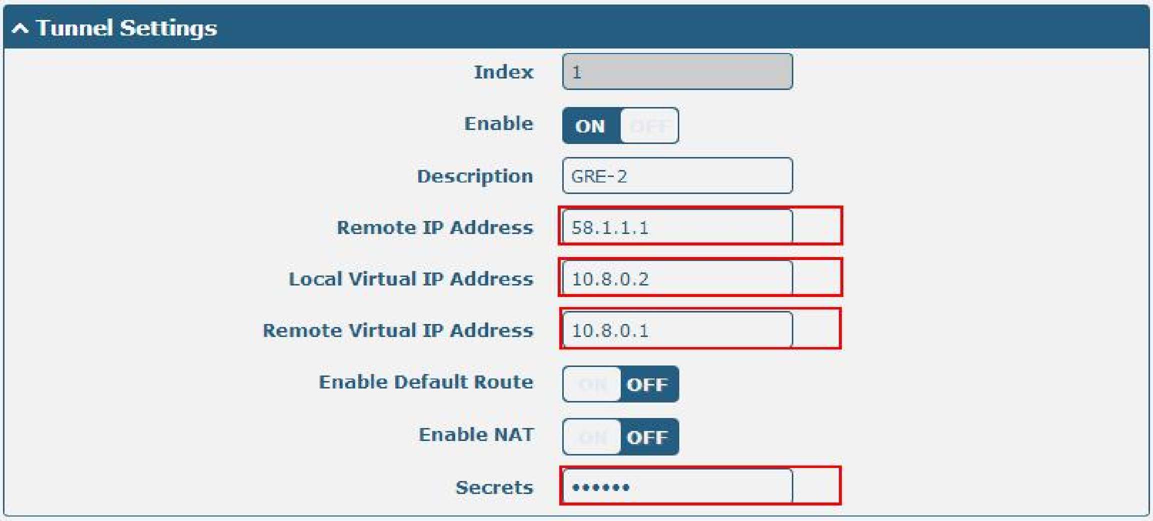
^ Tunnel Settings

Index	1
Enable	ON
Description	GRE-1
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••

When finished, click **Submit > Save & Apply** for the configuration to take effect.

GRE-2:

Click + button and set the parameters of GRE-2 as below.

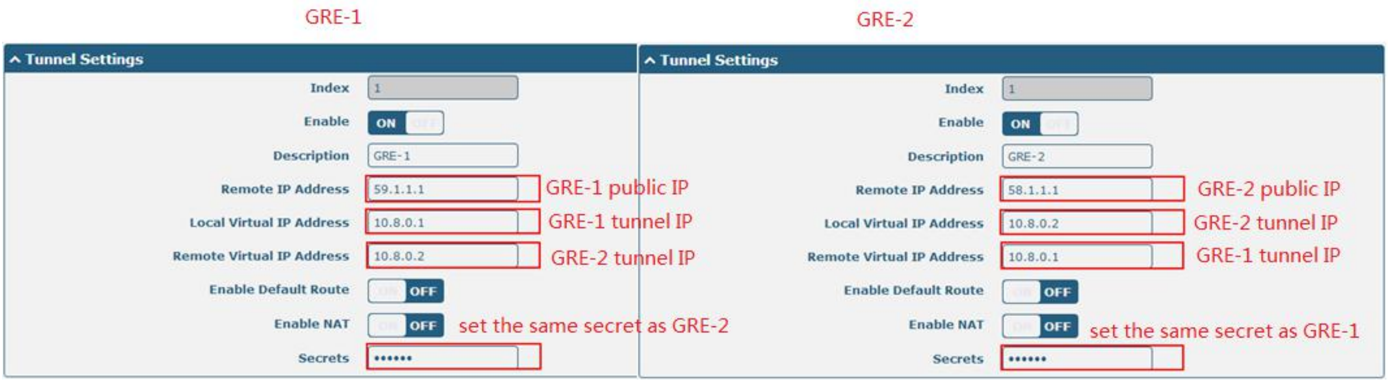


^ Tunnel Settings

Index	1
Enable	ON
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Remote Virtual IP Address	10.8.0.1
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••

When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between GRE-1 and GRE-2 is as below.

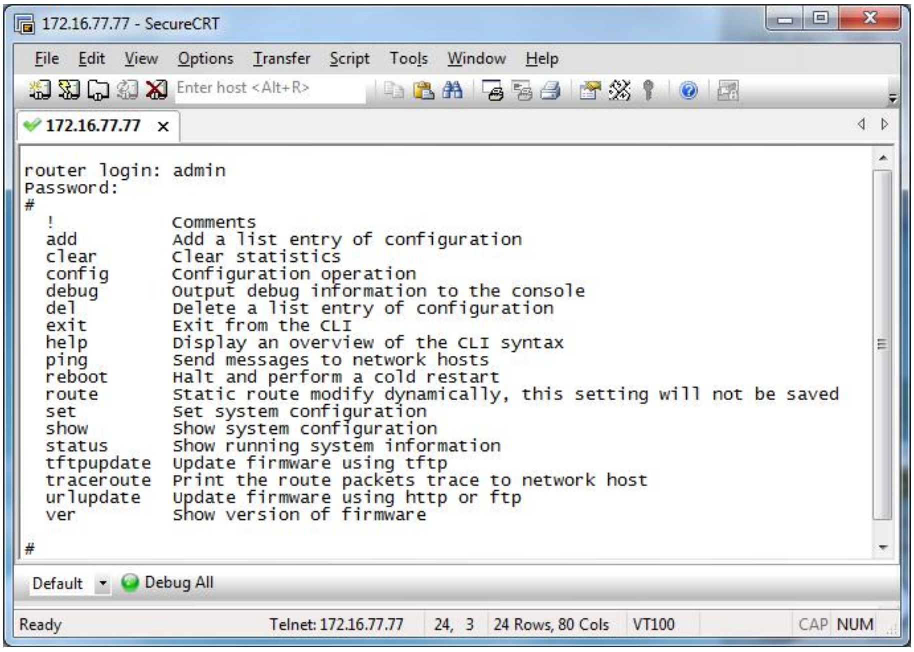


	GRE-1		GRE-2	
Index	1		1	
Enable	ON		ON	
Description	GRE-1		GRE-2	
Remote IP Address	59.1.1.1	GRE-1 public IP	58.1.1.1	GRE-2 public IP
Local Virtual IP Address	10.8.0.1	GRE-1 tunnel IP	10.8.0.2	GRE-2 tunnel IP
Remote Virtual IP Address	10.8.0.2	GRE-2 tunnel IP	10.8.0.1	GRE-1 tunnel IP
Enable Default Route	OFF		OFF	
Enable NAT	OFF	set the same secret as GRE-2	OFF	set the same secret as GRE-1
Secrets	••••••		••••••	

Chapter 6 Introductions for CLI

6.1 What Is CLI

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. Users can connect to the gateway through SSH or telnet to configure CLI commands. After establishing a Telnet or SSH connection with the gateway, enter the login account and password (default admin/admin) to enter the gateway configuration mode, as shown below.



```
router login: admin
Password:
#
  !           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

#
```

Route login:

Gateway 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

6.2 How to Configure the CLI

Following is a table 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 your setting finished, you should enter those commands to make your setting take effect on the device. **Note:** Commit and save_and_apply plays the same role.

6.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function
Set	Set *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	Add *parameters*	

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

6.4 CLI Configuration Examples

Quick Start with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the webpage and then read 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 "
kernel_version = 4.1.30
device_model = "MEG5000"
serial_number =11002217110001
uptime = "0 days, 05:17:45"
system_time = "Su Jan 1 05:17:02 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate （space+?）
  firmware    New firmware
# tftpupdate firmware （space+?）
  String    Firmware name
# tftpupdate firmware MEG5000-firmware-sysupgrade-unknown.bin host 192.168.100.99 // enter a new firmware name
  Downloading
MEG5000-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-manager

```
# set
# set (space+?)
    at_over_telnet       AT Over Telnet
    cellular             Cellular
    ddns                 Dynamic DNS
    ethernet             Ethernet
    event                Event Management
    firewall             Firewall
    gre                  GRE
    ipsec                IPsec
    lan                  Local Area Network
    link_manager         Link Manager
    ntp                  NTP
    openvpn              OpenVPN
    reboot               Automatic Reboot
    robustlink           Robustlink
    route                Route
    sms                  SMS
    snmp                 SNMP agent
    ssh                  SSH
    syslog               Syslog
    system               System
    user_management      User Management
    vrrp                 VRRP
    web_server           Web Server
# set link_management
    primary_link         Primary Link
    backup_link          Backup Link
    backup_mode          BackSup Mode
    emergency_reboot     Emergency Reboot
    link                 Link Settings
# set link_management primary_link（space+?）
Enum    Primary Link   （wwan1/wwan2/wan/wlan）
# set link_management primary_link wwan1                   //select “wwan1” as primary link
OK                                                          //setting succeed
set link_manager link 1
    type                 Type
    desc                 Description
    connection_type      Connection Type
    wwan                 WWAN Settings
```

```
   static_addr          Static Address Settings
   pppoe                PPPoE Settings
   ping                 Ping Settings
   mtu                  MTU
   dns1_overrided       Overrided Primary DNS
   dns2_overrided       Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                     Automatic APN Selection
   apn                          APN
   username                     Username
   password                     Password
   dialup_number                Dialup Number
   auth_type                    Authentication Type
   aggressive_reset             Aggressive Reset
   switch_by_data_allowance     Switch SIM By Data Allowance
   data_allowance               Data Allowance
   billing_day                  Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100          // open cellular switch by data traffic
OK                                                         //setting succeed
# set link_manager link 1 wwan billing_day 1               //setting specifies the day of month for billing
OK                                                         //setting succeed
…
# config save_and_apply
OK                                      //save and apply current configuration, make you configuration effect
```

Example 4: Set Ethernet

```
# set Ethernet port_setting 2 port_assignment lan0         // set Table 2 (eth1) to lan0
OK
# config save_and_apply                                    //make you configuration effect
OK
```

Example 5: Set LAN IP address

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
```

```
        netmask = 255.255.255.0
        mtu = 1500
        dhcp {
                enable = true
                mode = server
                relay_server = ""
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                gateway = ""
                primary_dns = ""
                secondary_dns = ""
                wins_server = ""
                lease_time = 120
                expert_options = ""
                debug_enable = false
        }
}
multi_ip {
        id = 1
        interface = lan0
        ip = 172.16.10.66
        netmask = 255.255.0.0
}
#
# set lan
    network          Network Settings
    multi_ip     Multiple IP Address Settings
    vlan             VLAN
# set lan network 1(space+?)
    interface    Interface
    ip           IP Address
    netmask      Netmask
    mtu          MTU
    dhcp         DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.10.66                    //set IP address for lan
OK                                                     //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_apply
OK                                                //save and apply current configuration, make you configuration effect
```

Example 6: CLI for setting Cellular

```
# show cellular all
sim {
        id = 1
        card = sim1
        phone_number = ""
        extra_at_cmd = ""
        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
        band_lte_1700 = false
        band_lte_700 = false
        band_tdd_lte_2600 = false
        band_tdd_lte_1900 = false
        band_tdd_lte_2300 = false
        band_tdd_lte_2500 = false
}
sim {
        id = 2
        card = sim2
        phone_number = ""
        extra_at_cmd = ""
        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
    band_lte_1700 = false
    band_lte_700 = false
    band_tdd_lte_2600 = false
    band_tdd_lte_1900 = false
    band_tdd_lte_2300 = false
    band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet   cellular      ddns          dhcp          dns
event            firewall      ipsec         lan           link_manager
ntp              openvpn       reboot        route         serial_port
sms              snmp          syslog        system        user_management
vrrp
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..2)

# set cellular sim 1(space+?)
   card                   SIM Card
   phone_number           Phone Number
   extra_at_cmd           Extra AT Cmd
   network_type           Network Type
   band_select_type       Band Select Type
   band_gsm_850           GSM 850
   band_gsm_900           GSM 900
   band_gsm_1800          GSM 1800
   band_gsm_1900          GSM 1900
   band_wcdma_850         WCDMA 850
   band_wcdma_900         WCDMA 900
   band_wcdma_1900        WCDMA 1900
   band_wcdma_2100        WCDMA 2100
   band_lte_800           LTE 800 (band 20)
   band_lte_850           LTE 850 (band 5)
   band_lte_900           LTE 900 (band 8)
   band_lte_1800          LTE 1800 (band 3)
   band_lte_1900          LTE 1900 (band 2)
   band_lte_2100          LTE 2100 (band 1)
   band_lte_2600          LTE 2600 (band 7)
   band_lte_1700          LTE 1700 (band 4)
   band_lte_700           LTE 700 (band 17)
   band_tdd_lte_2600      TDD LTE 2600 (band 38)
   band_tdd_lte_1900      TDD LTE 1900 (band 39)
   band_tdd_lte_2300      TDD LTE 2300 (band 40)
   band_tdd_lte_2500      TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                                  //save and apply current configuration, make you configuration effect
```

Chapter 7 Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
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 Identity
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol

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

Abbr.	Description
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.
Add: 501, Building 2, No. 63, Yong'an Avenue,
Huangpu District, Guangzhou, China 510660
Tel: 86-20-82321505
Email: support@robustel.com
Web: www.robustel.com