EG9012

KONE Connection 210 (North America)

For 3G/4G Networks

User Guide

About This Document

This document provides hardware and software information of the Robustel EG9012 Gateway, including introduction, installation, configuration and operation.

Trademarks and Permissions

 are trademarks of Guangzhou Robustel Technologies Co., Limited. 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 use of this document.

Technical Support

Tel: +86-20-29019902
Fax: +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.

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada statement

❶ This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:
   1) this device may not cause interference, and
   2) this device must accept any interference, including interference that may cause undesired operation of the device.

❶ Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:
   1) l'appareil ne doit pas produire de brouillage, et
   2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

❷ This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter, except tested built-in radios.

❷ Cet appareil et son antenne ne doivent pas être situés ou fonctionner en conjonction avec une autre antenne ou un autre émetteur, exception faites des radios intégrées qui ont été testées.

❸ The County Code Selection feature is disabled for products marketed in the US/ Canada.

❸ La fonction de sélection de l'indicatif du pays est désactivée pour les produits commercialisés aux États-Unis et au Canada.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EC	Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)	
2012/19/EU	Directive 2012/19/EU the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE)	

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

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

Table 3: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

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

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

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

Document History

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

Date	Firmware Version	Doc Version	Change Description
25 April, 2017	0.10.2	v.1.0.0	Initial release
2 June, 2017	0.11.2	v.1.1.0	Updated: 1. Product picture 2. Input Voltage 3. Power Consumption 4. Packing list 5. Operating temperature 6. LED Indicator 7. 4.1 Generate diagnose file about APN 8. 4.3.1 ISP APN, dial up number

Contents

Chapter 1 Product Concept

1.1 Key Features

Robustel EG9012 is an industrial gateway designed for elevator monitoring and provides fast, reliable and stable Internet connectivity.

EG9012 is a powerful Elevator gateway developed from **RobustOS**, a Robustel self-developed and Linux-based operating system which designed to be used in Robustel hardware gateways. The RobustOS includes basic networking features and protocols providing users with a custom experience. Meanwhile, Robustel offers a **Software Development Kit** (SDK) to partners and customers to allow additional customization by using C or Python or Java, also provides rich **APPs** to satisfy fragmented IoT market.

- Supports 3G/4G cellular network
- Various interfaces: RS232/RS485/Console/USB/Ethernet/FXS
- Emergency call and respond via voice interface
- Modbus gateway serial protocol Support
- RS485 interface supports BACnet protocol
- Event output via Email, SMS
- Auto reboot via SMS/Incoming Call/Timing
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/PPTP/L2TP/DMVPN Support
- Support IBM IoT (Bluemix Internet of Things) devices management platform
- Support KMC (KONE Monitoring Centre) elevators monitoring platform
- Management and upgrading via SMS/Web/CLI/SNMP/RobustLink Cloud
- Robust industrial design (9 to 26V DC, desktop or DIN rail mounting)

1.2 Package Contents

Before installing your EG9012 Gateway, verify the kit contents as following.
Note: The following pictures are for illustration purposes only, not based on their actual sizes.

- 1 x Robustel EG9012 KONE Connection 210 (North America)

- 35 mm DIN rail mounting kit

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

1.3 Specifications

Cellular Interface

- Standards: W-CDMA/FDD-LTE/TDD-LTE
- W-CDMA: max. 14.4Mbps/5.76Mbps (DL/UL)
- FDD-LTE: max. 100/50 Mbps (DL/UL)
- TDD-LTE: max. 100/50 Mbps (DL/UL)
- SIM: 1 (3V & 1.8V)
- Antenna interface: SMA female (ANT1+ANT2)

Ethernet Interface

- Number of ports: 2 x 10/100 Mbps (LAN1+LAN2)
- Magnet isolation protection: 1.5KV

Serial Interfaces

- Number of ports: 2 x RS-232, 1 x RS-485
- Baud rate: 300bps to 57600bps
- RS-232: Tx, Rx, GND
- RS-485: A (Data+), B (Data-)

- Interface: 3.81mm connector

Audio Interface

- Physical Connector: 3.81mm 3-PIN terminal block
- Interface type: FXS
- Interface Standard: ITU Q.512 (SLIC), ITU K.20 (overcurrent and overvoltage protection)
- Subscriber line interface circuit (SLIC)

Ring voltage: 40~90 Vpk configurable
Ring frequency: 20~25 Hz
Ring waveform: sinusoidal
Maximum ringer load: 5 ringer equivalence numbers (RENs)
On-hook/off-hook characteristics:
On-hook voltage (tip/ring): -46~-56V;
Off-hook current: 18~20 mA
Terminating impedance: configurable

System

- LED indicators: PWR, DEV1, DEV2, NET, RSSI, KMC, ERR
- Built-in RTC, Watchdog, Timer
- Expansion: 1 x USB 2.0 host up to 480 Mbps

Software

- Network protocols: PPP, TCP, UDP, DHCP, ICMP, NAT,

DMZ, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, SNTP, Telnet, SNMP etc.

- Firewall: SPI, anti-DoS, Filter, Access Control
- Serial port: TCP client/server, UDP, Modbus RTU/ASCII to Modbus TCP, Virtual COM (COM port redirector), BACnet

Power Supply and Consumption

- Power supply interface: 2-PIN 3.81mm terminal block
- Input voltage: 9 to 26 VDC (Overvoltage Protection)
- Power consumption: 900mA(MAX)@9V, 600mA(MAX)@12V, 400mA(MAX)@26V

Physical Characteristics

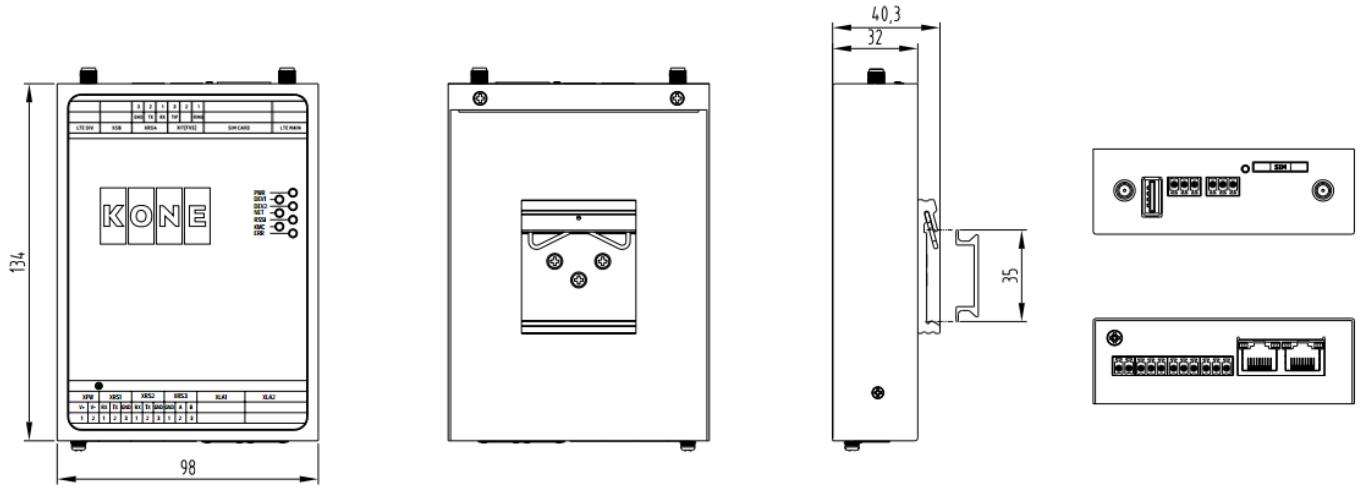
- Housing & weight: Metal, 300g
- Dimension: (L x W x H): 134mm x 98mm x 32mm
- Installation: 35mm DIN rail
- Normal Operating Temperature: -30~+70°C,
- Extended Operating Temperature: -40~-30°C, +70~+85°C
- Humidity: 5~95%RH

1.4 Ordering Information

Model No.	Description	Frequency	Operating Environment
EG9012-4LB	Elevator Gateway, 4G	4G:B2/4/5/13/17 3G:B2/5	Normal Operating Temperature: -30~+70°C

	module		Extended Operating Temperature: -40~-30°C, +70~+85°C Humidity: 5~95%RH

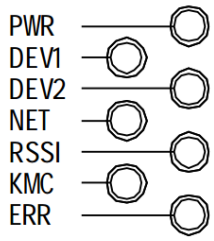
1.5 Dimensions



Front View　　Rear View　　Side View　　Top&Bottom View

Chapter 2 Hardware Installation

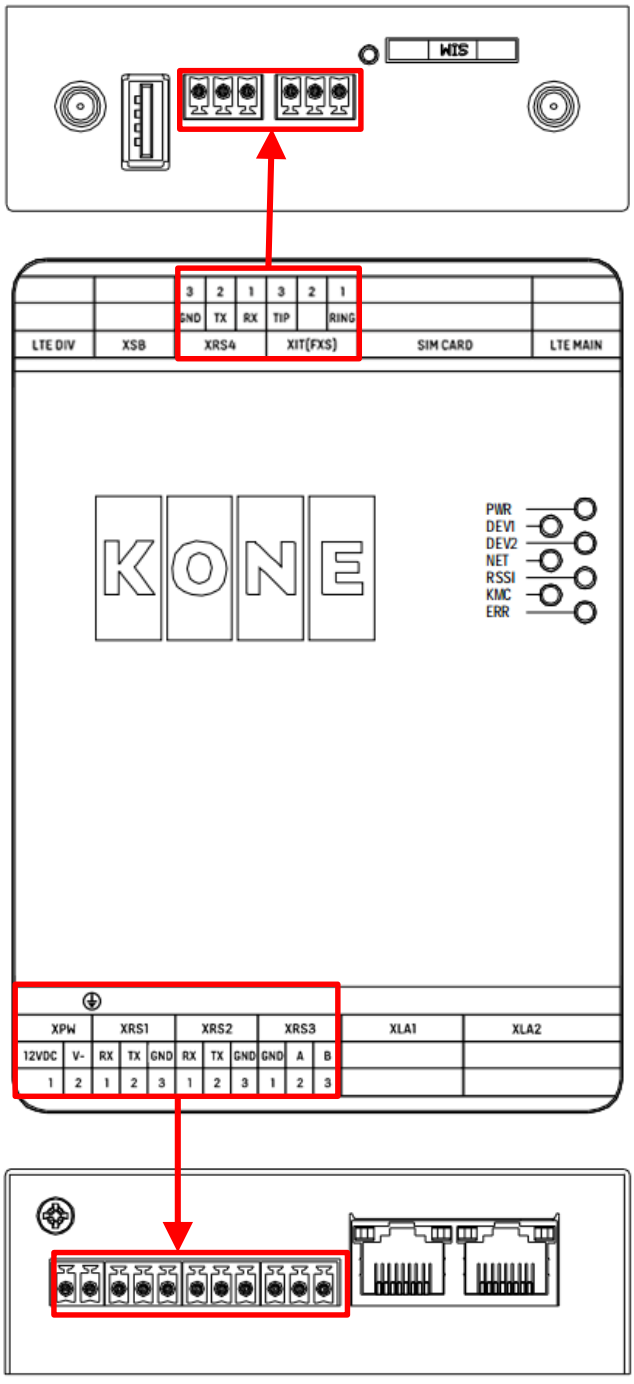
2.1 LED Indicators



Name	Color	Status	Description
PWR	Green	On	Gateway is powered on
DEV1	Green	On	Connected to controller1
DEV2	Green	On	Connected to controller2
NET	Green	Always On	Connected to 4G network
		Blinking every 100ms	Connected to 3G network
RSSI	Green	Blinking every 1s	Signal level: 0-9 (Low Signal)
		Blinking every 100ms	Signal level: 10-19 (Medium Signal)
		Always on	Signal level: 20-31 (High Signal)
		Off	No signal
KMC	Green	Blinking	Registering the KMC Platform
		On	Connected to the KMC Platform
		Off	Disconnected to the KMC Platform
ERR	Green	On	Gateway in fault

2.2 PIN Assignment

There are terminal block PIN relationship tables on the front view of the EG9012, as the following figure showed.



Top View

Front View

Bottom View

XRS4 (Debug)		
PIN	**Function**	**Direction**
1	RX	Device→ EG9012
2	TX	EG9012→Device
3	GND	--

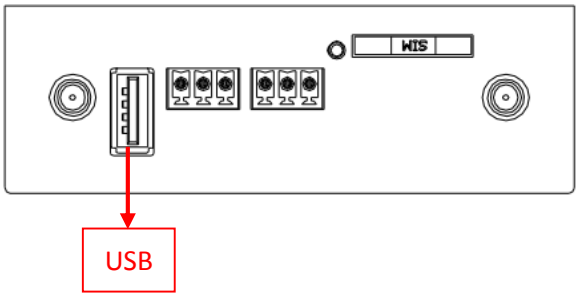
XIT (FXS)		
PIN	**Function**	**Direction**
1	RING	Device→ EG9012
2	--	
3	TIP	EG9012→Device

XPW (Power supply interface)		
PIN	**Function**	**Direction**
1	V+	Adapter→ EG9012
2	V-	EG9012→Adapter

XRS1/XRS2 (RS232 serial port)		
PIN	**Function**	**Direction**
1	RX	Device→ EG9012
2	TX	EG9012→Device
3	GND	--

XRS3 (RS485 serial port)		
PIN	**Function**	**Direction**
1	GND	--
2	A	--
3	B	--

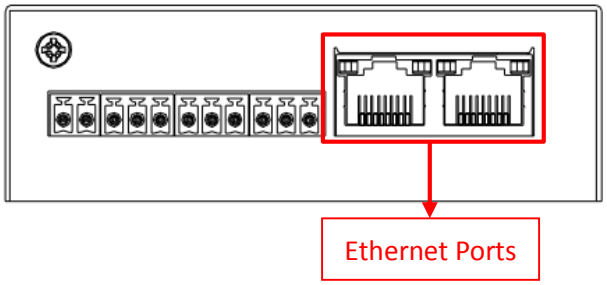
2.3 USB Interface



Top View

Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the router's USB interface, such as a U disk or a hard disk. If there have a supported configuration file or a EG9012 firmware in this USB storage device, the EG9012 router will automatically update the configuration file or the firmware. For more details, see **3.11 Interface > USB**.

2.4 Ethernet Ports



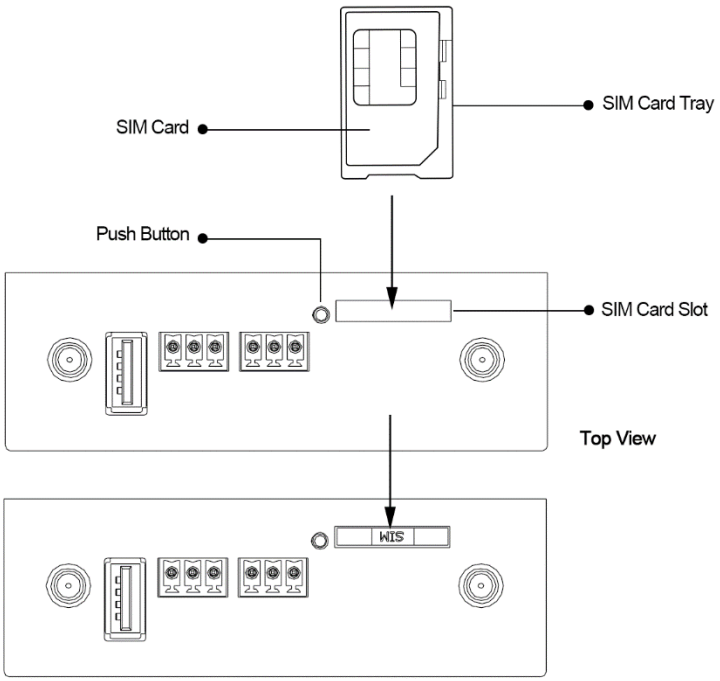
Bottom View

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

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

2.5 Insert or Remove SIM Card

Be sure to insert a SIM card before you use the gateway.



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

- **Inserting SIM Card**

1. Power off the gateway.
2. Use a pointed stick to press the Push Button, and then take out the SIM Card Tray.
3. Place the SIM card on the tray, and insert them to the slot until you hear “a cracking sound”.

- **Removing SIM card**

1. Power off the gateway.
2. Press the Push Button, and the tray with SIM card will pop up to be pulled out.

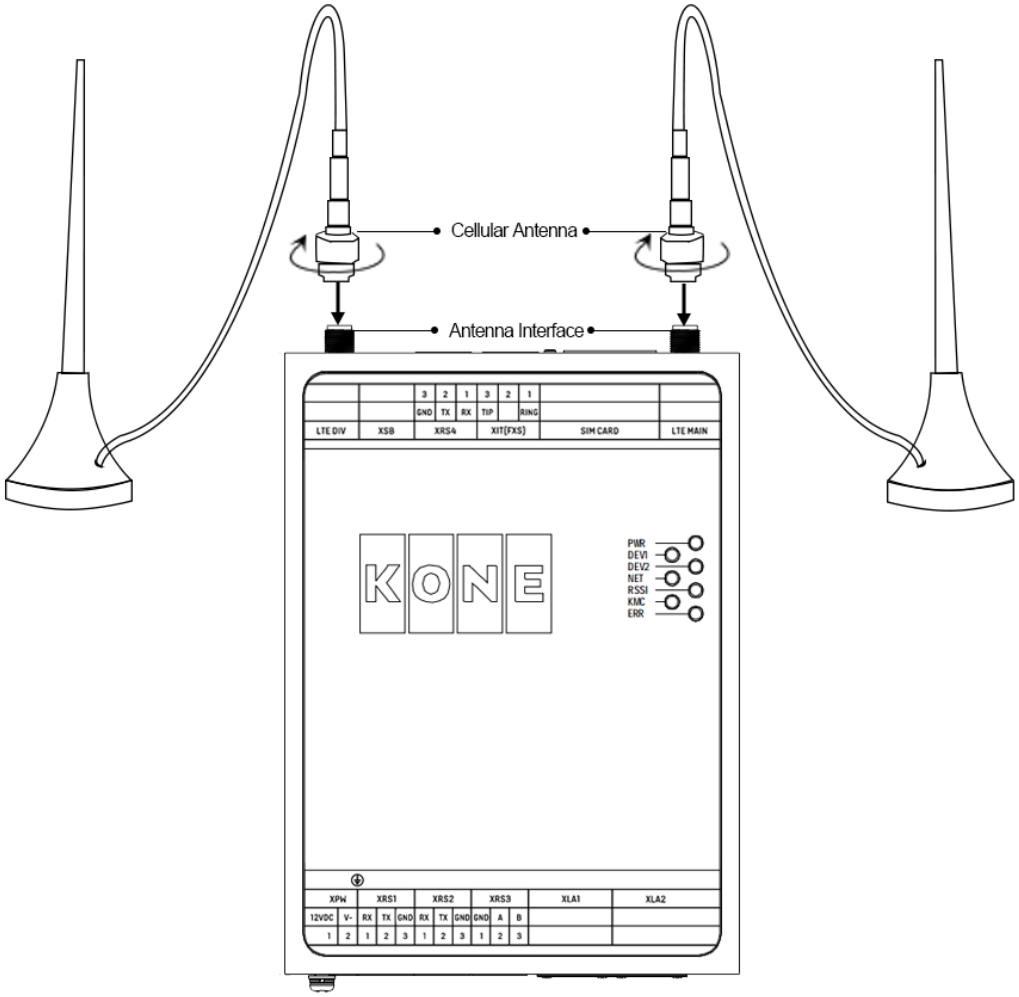
Note:

1. *Don’t touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
2. *Don’t bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
3. *Make sure to disconnect the power source from your gateway before inserting and removing your SIM card.*

2.6 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the gateway's 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.

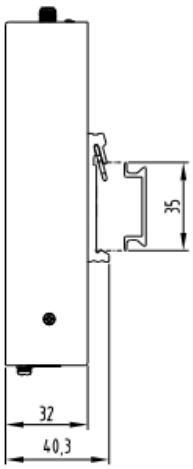


2.7 Mount the Gateway

The gateway can be mounted a 35 mm DIN rail.

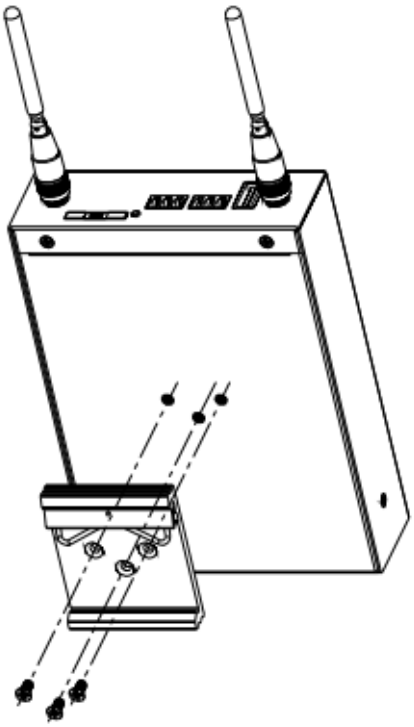
DIN rail size (measured in mm)

Din Rail



Use 3 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.

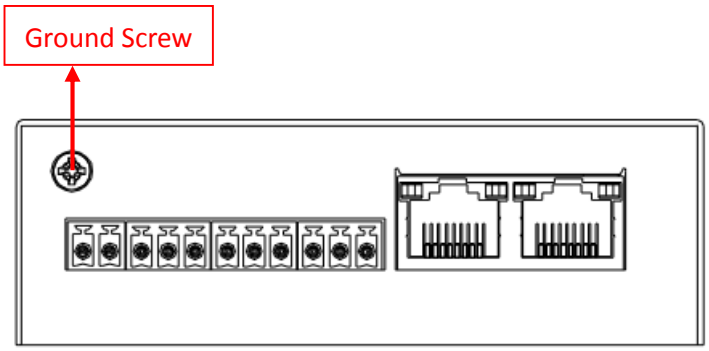
Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.



2.8 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.

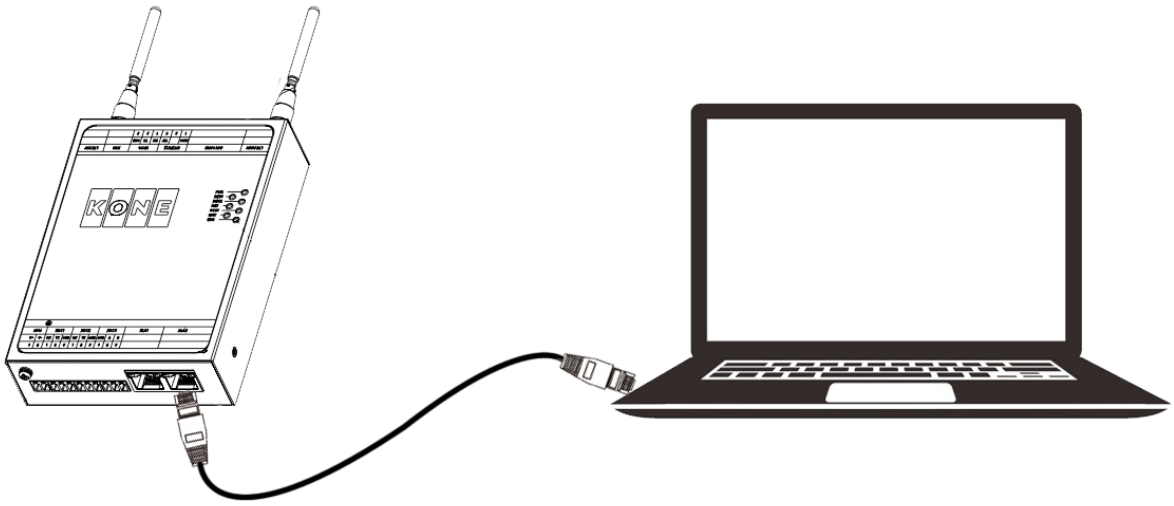
Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.



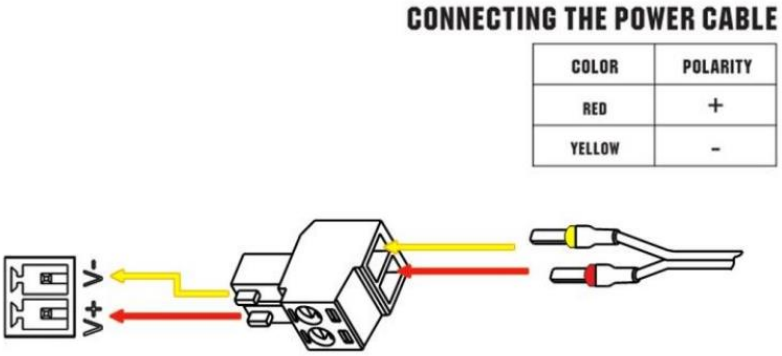
Bottom View

2.9 Connect the Gateway to a Computer

Connect an Ethernet cable to LAN1 or LAN2 at the bottom of the EG9012, and connect the other end of the cable to your computer.



2.10 Power Supply



EG9012 Gateway supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly.

Note: The range of power voltage is 9 to 26V DC.

Chapter 3 Initial Configuration

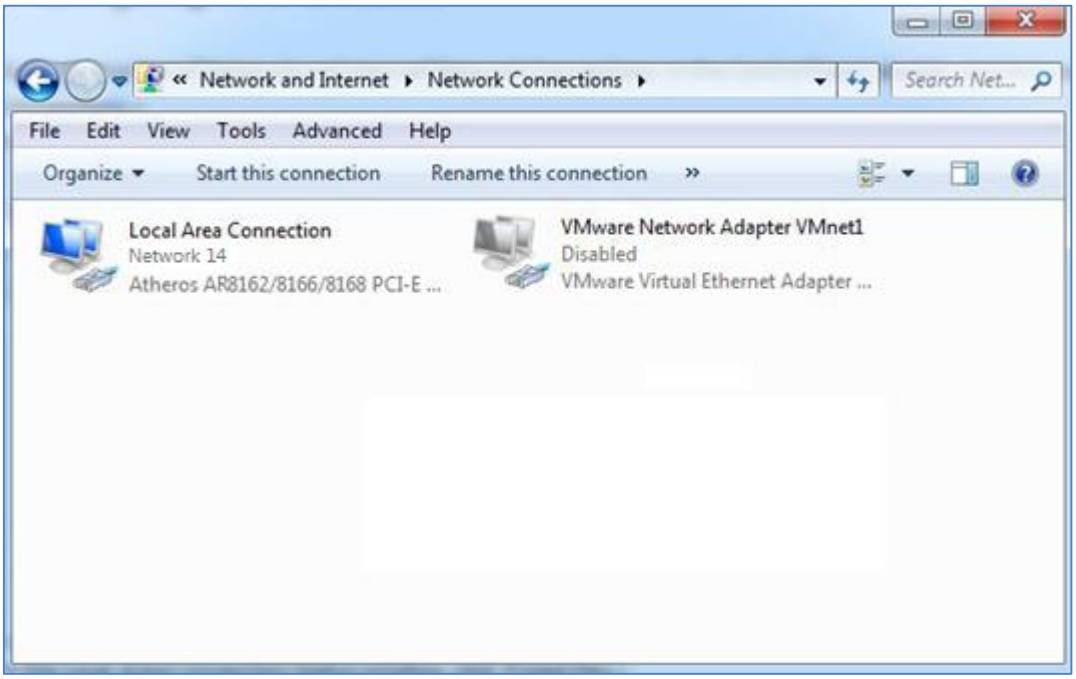
The gateway can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface 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.

3.1 Configure the PC

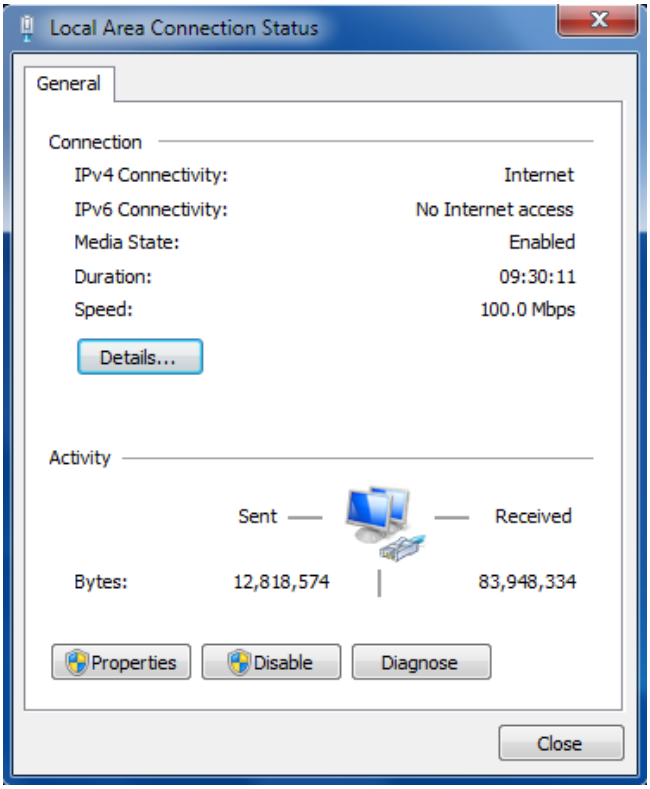
There are two methods to get IP address for the PC, one is to obtain an IP address automatically from "Local Area Connection", and another is to configure a static IP address manually within the same subnet of the gateway. Please refer to the steps below.

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

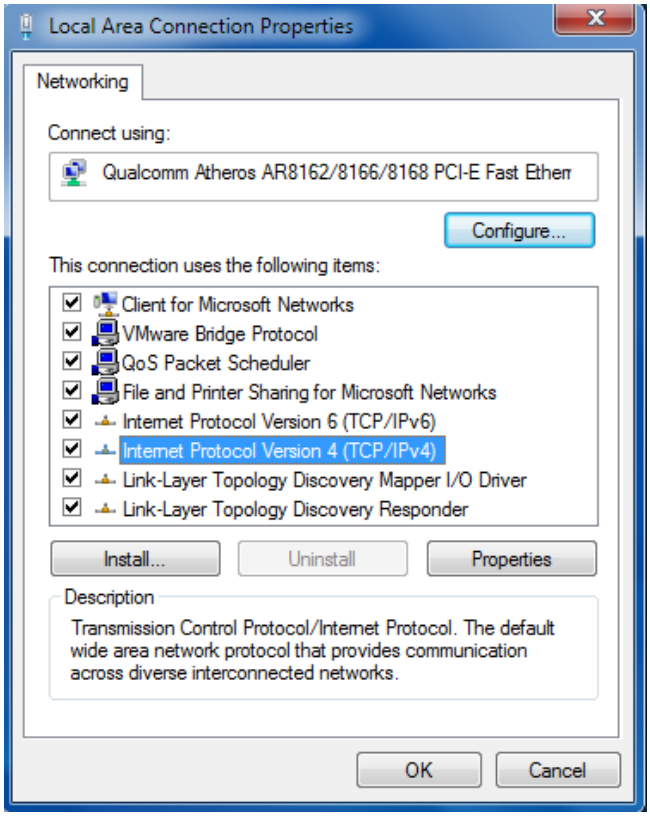
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



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

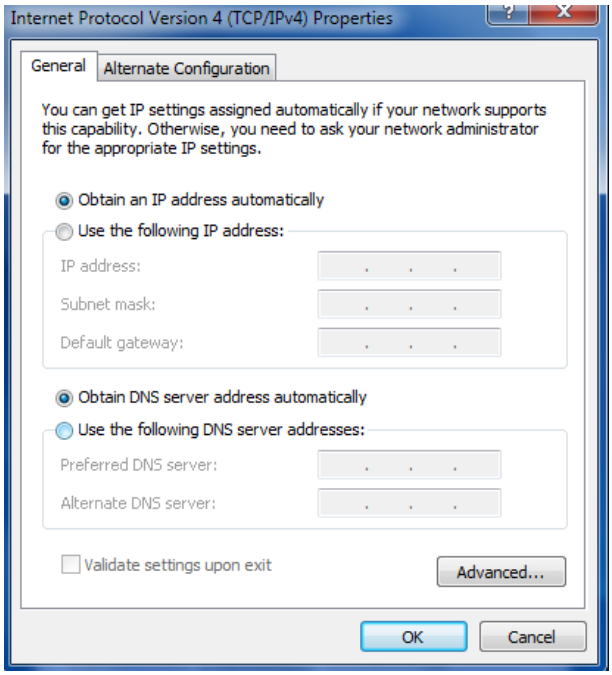


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



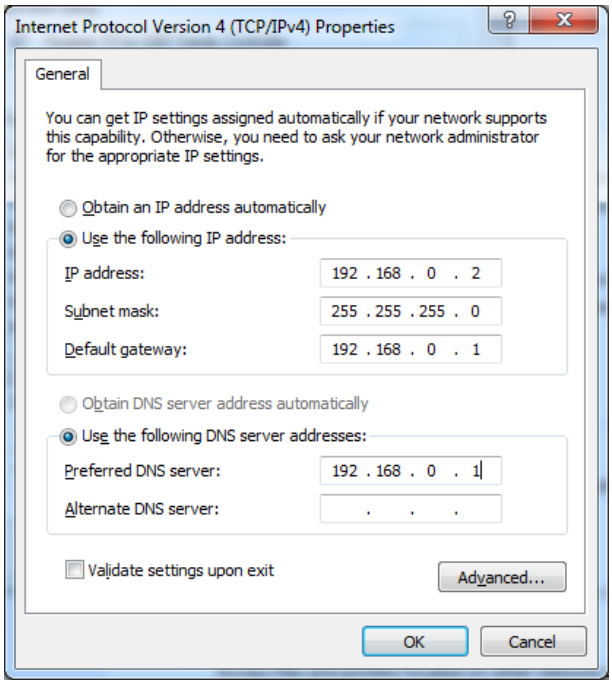
4. Two ways for configuring the IP address of PC

Obtain an IP address automatically:



Use the following IP address:

(Configured a static IP address manually within the same subnet of EG9012 Gateway)



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

3.2 Factory Default Settings

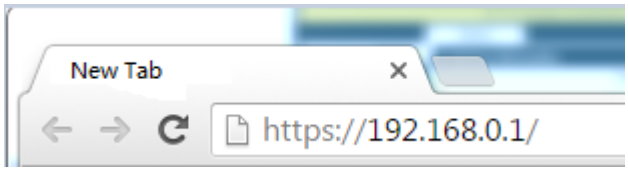
Before configuring your gateway, you need to know the following default settings.

Item	Description
Username	kone
Password	kone
LAN1	192.168.0.1/255.255.255.0, LAN mode
LAN2	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 EG9012 Gateway is 192.168.0.1, though the actual address may vary.



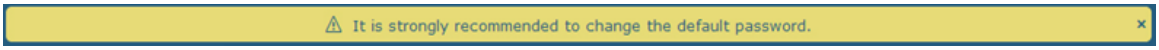
3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password is “kone”.

   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 EG9012 Gateway's web interface is displayed, for example.

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



It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **0 System > 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.

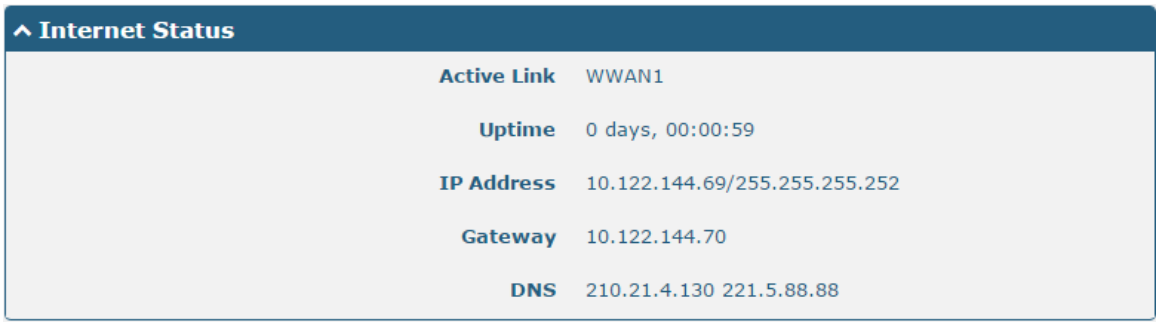
3.5 Status

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

System Information

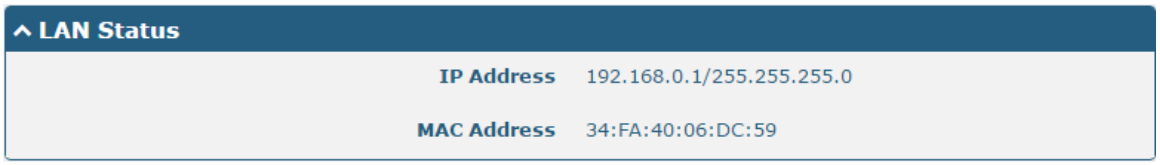
System Information	
Item	**Description**
Device Model	Show the model name of your device.
System Uptime	Show the current amount of time the gateway has been connected.
System Time	Show the current system time.
Firmware Version	Show the firmware version running on the gateway.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.

Internet Status



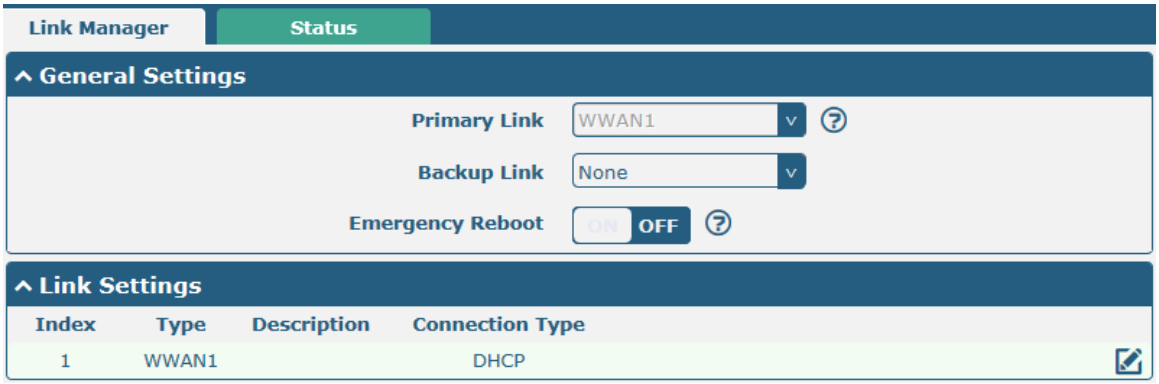
Internet Status	
Item	**Description**
Active Link	Show the current active link.
Uptime	Show the current amount of time the link has been connected.
IP Address	Show the IP address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current primary DNS server and secondary server.

LAN Status



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

3.6 Interface > Link Manager



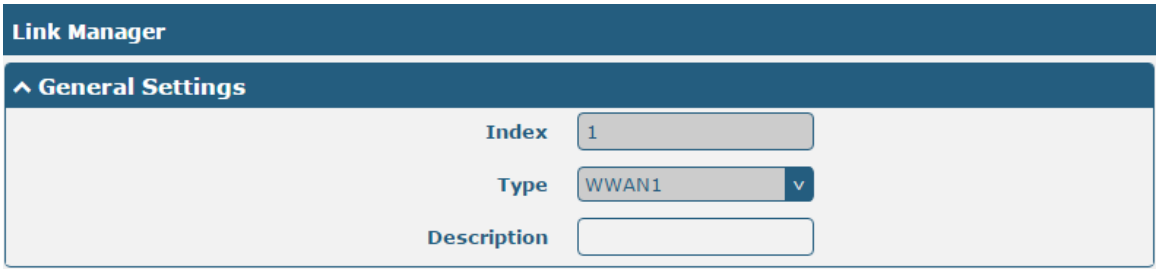
General Settings @ Link Manager		
Item	**Description**	**Default**
Link	It's no need to configure link manually in this part, we recommend to remain the default setting of system.	WWAN1
Emergency Reboot	Enable to reboot the whole system if no links available.	OFF

Note: Click for help.

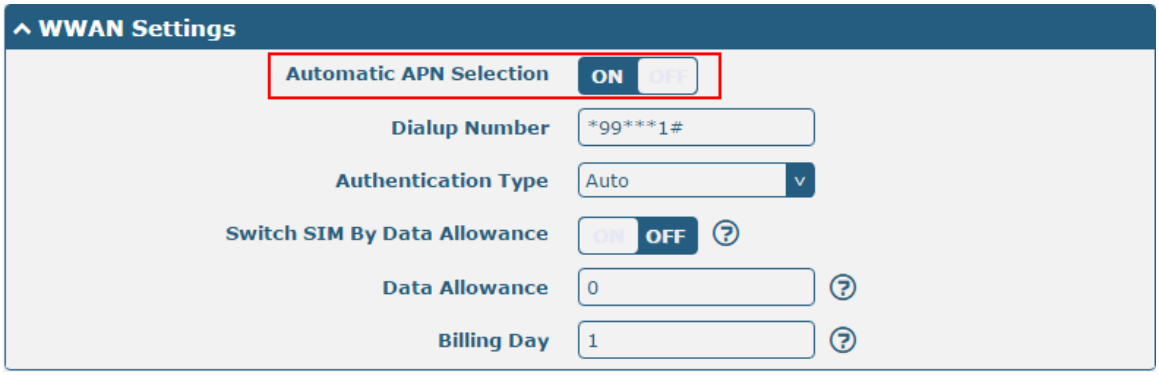
Link Settings allows you to configure the parameters of Cellular link connection. It is recommended to enable Ping detection to keep the gateway always online. The Ping detection increases the reliability and also costs the data traffic.

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

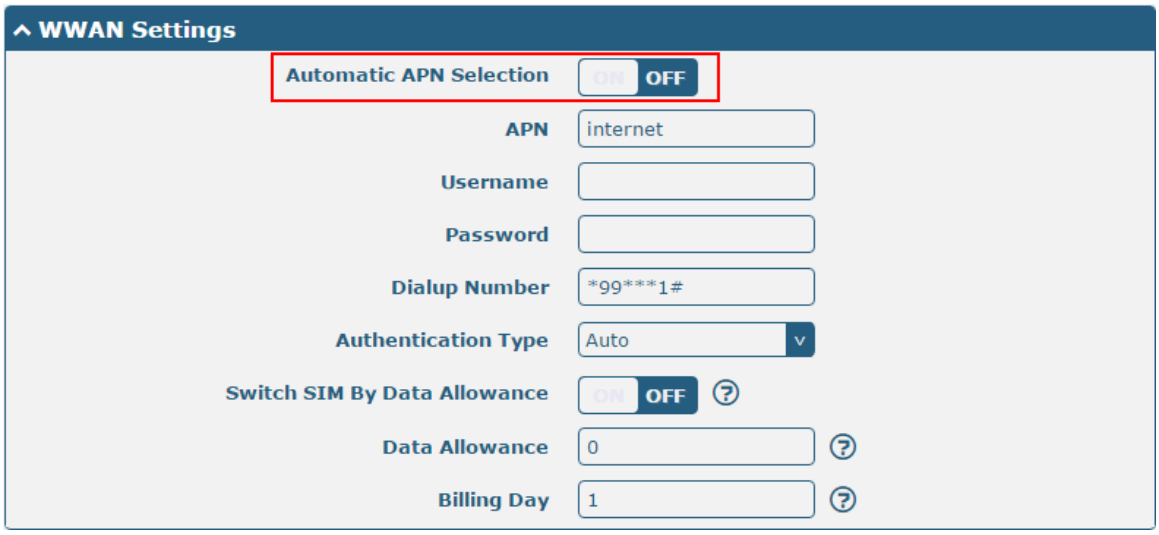
WWAN1

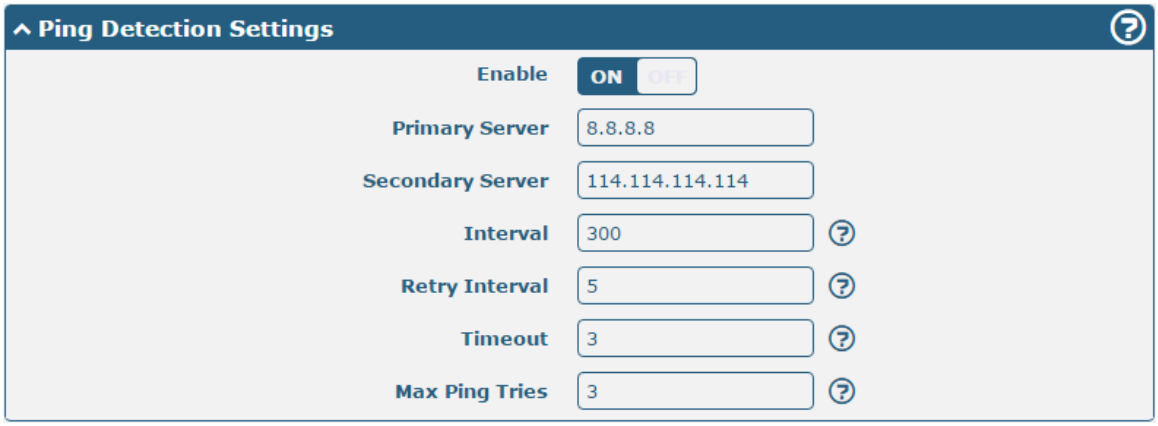


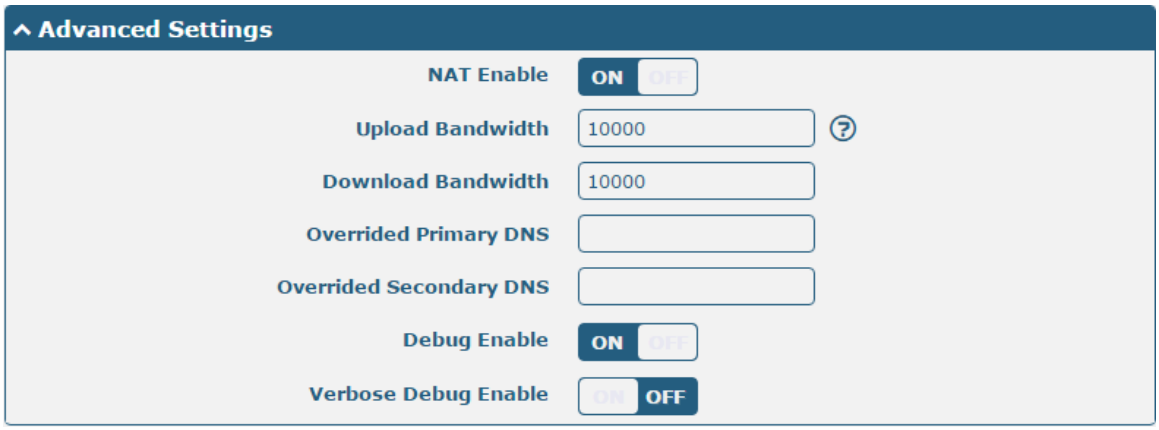
The window is displayed as below when enabling the "Automatic APN Selection" option.



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





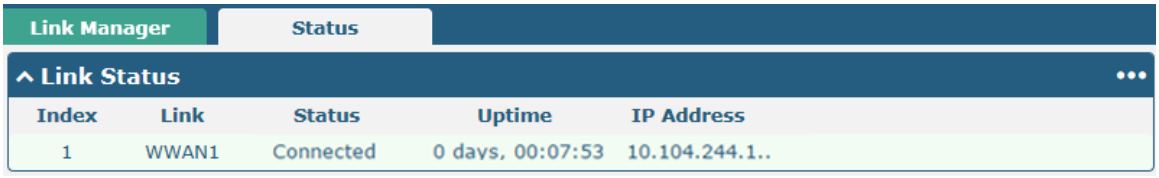


Link Settings (WWAN)		
Item	**Description**	**Default**
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the "Automatic 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
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 keepalive policy of EG9012 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

Link Settings (WWAN)		
Item	**Description**	**Default**
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

Status

This page allows you to view the status of link connection and clear the monthly data usage statistics.



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.

Click the **Clear** button to clear SIM 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**.

3.7 Interface > LAN

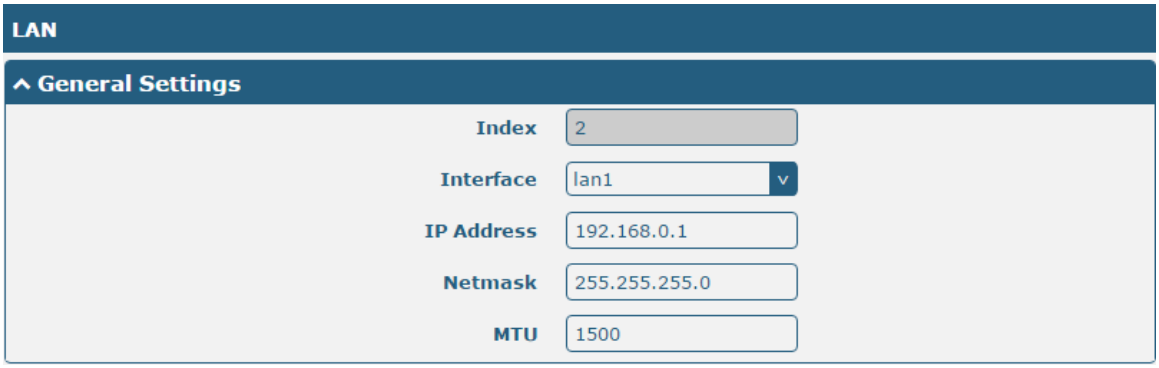
This section allows you to set the related parameters for LAN port. There are two LAN ports on EG9012 Gateway, including ETH11 and ETH2. ETH11 and ETH2 can freely choose from lan0~lan1, but at least one ETH port must be assigned as lan0. The default settings of ETH1 are lan0, and their default IP are 192.168.0.1/255.255.255.0. For more details, see **3.8 Interface > Ethernet**.

LAN

By default, there is a lan0 in the list. To begin adding lan1, please configure one of ETH0 and ETH1 as lan1 first in **Ethernet > Ports > Port Settings**. Otherwise, the operation will be prompted as "List is full".

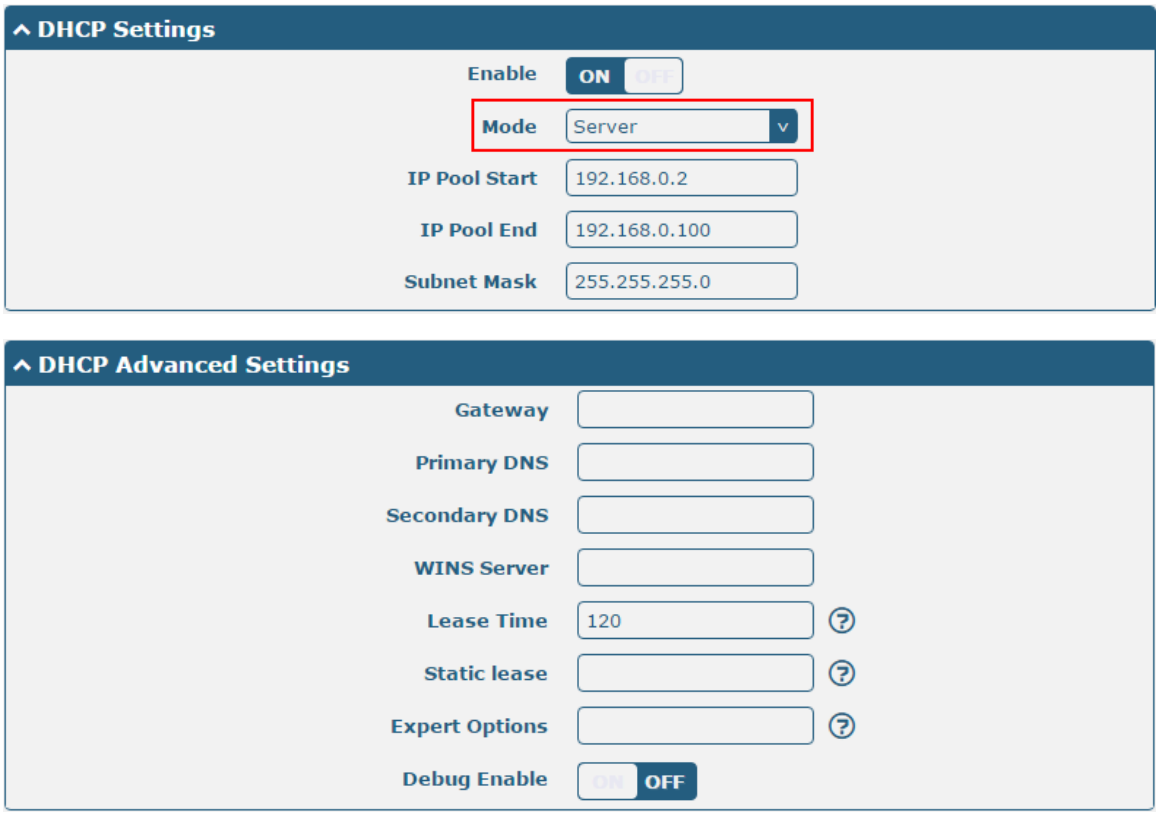
Note: Lan0 cannot be deleted.

You may click to edit the configuration of the LAN port, or click to delete the current LAN port. Now, click to add a new LAN port. The maximum count is 2.

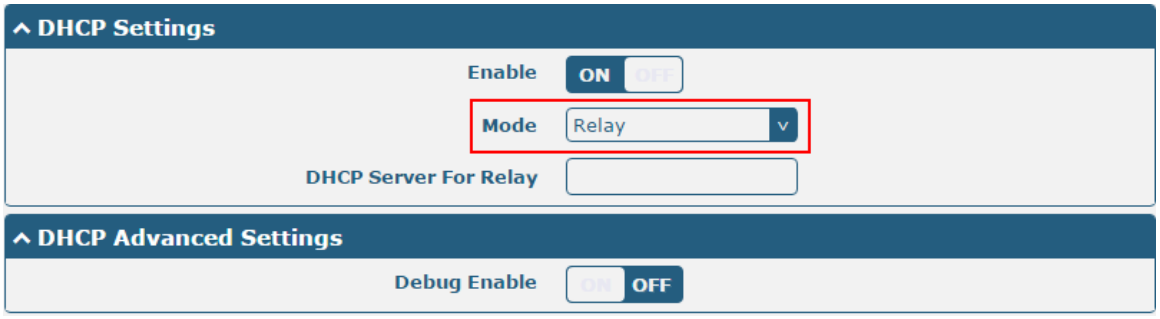


General Settings @ LAN		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Interface	Lan1 is available only if it was selected by one of ETH0 and ETH1 in **Ethernet > Ports > Port Settings**, and so on.	--
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

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



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

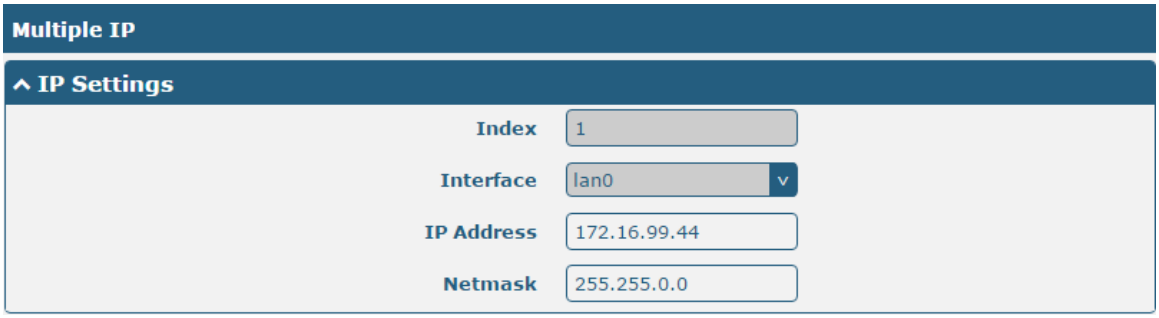


LAN		
Item	**Description**	**Default**
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. • Server: Lease IP address to DHCP clients which have been connected to LAN port • Relay: Gateway can be a DHCP Relay, which will provide 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

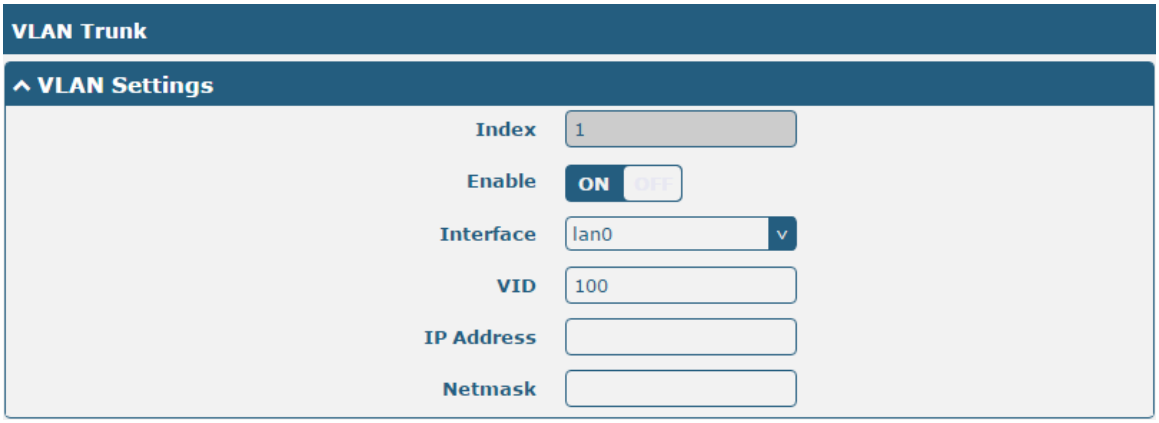
You may click + to add a multiple IP to the LAN port, or click ✕ to delete the multiple IP of the LAN port. Now, click to edit the multiple IP of the LAN port.



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

VLAN Trunk

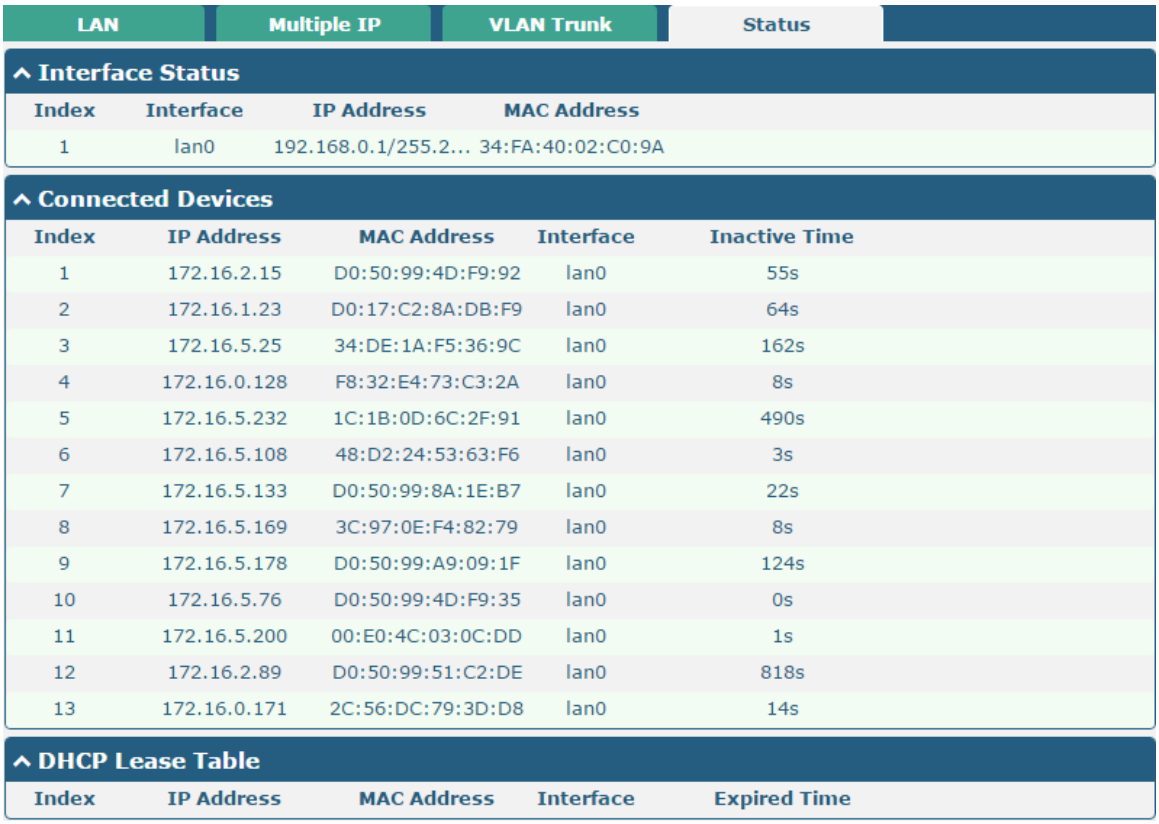
Click + to add a VLAN. The maximum count is 8.



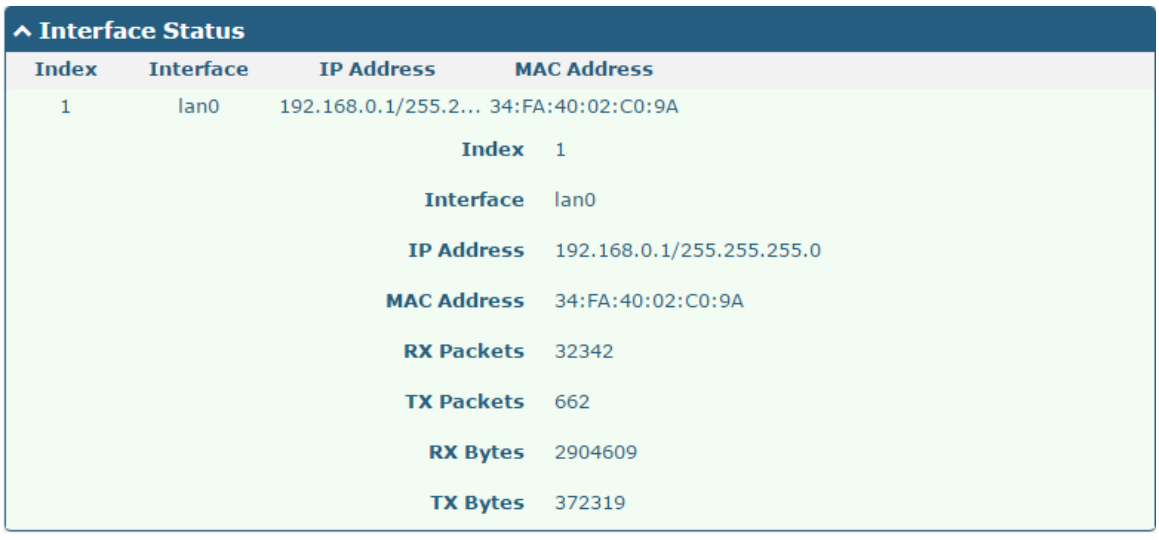
VLAN Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this VLAN. Enable to make gateway can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0", "lan1", "lan2" or "lan3" depends on your ETH1~ETH4's corresponding LAN port.	lan0
VID	Set the tag ID of VLAN and digits from 1 to 4094.	100
IP Address	Set the IP address of VLAN port.	Null
Netmask	Set the Netmask of VLAN port.	Null

Status

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

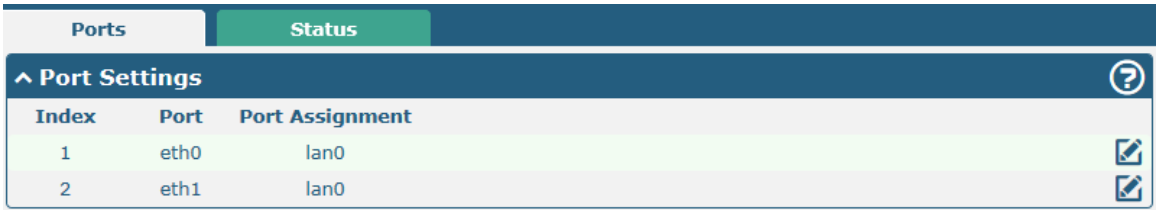


Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

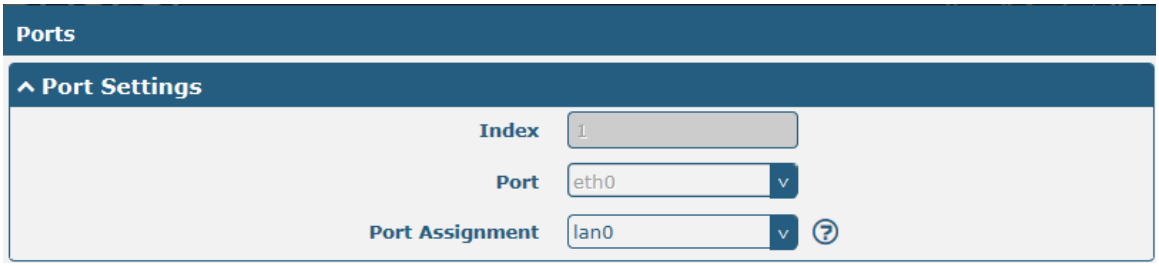


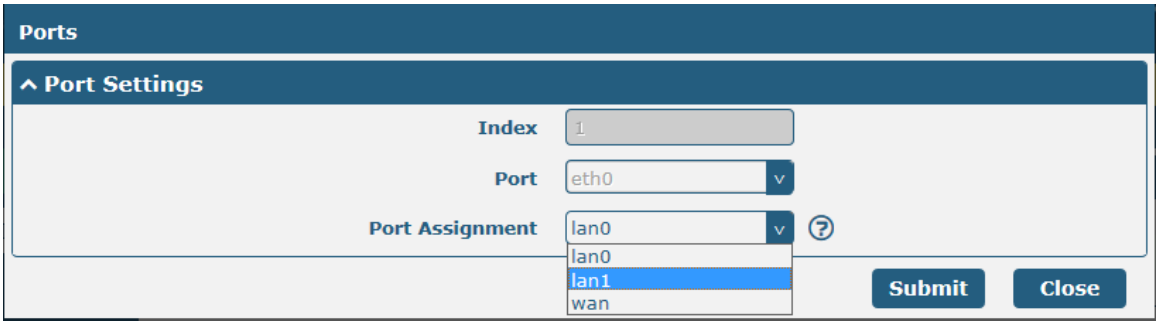
3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on EG9012 Gateway, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from lan0~lan1, but at least one LAN port must be assigned as lan0. In another word, ETH0+ETH1 can be configured as lan0+lan0, lan0+lan1, or lan1+lan0. Both of ETH0 and ETH1 default to lan0, and their default IP are 192.168.0.1/255.255.255.0.



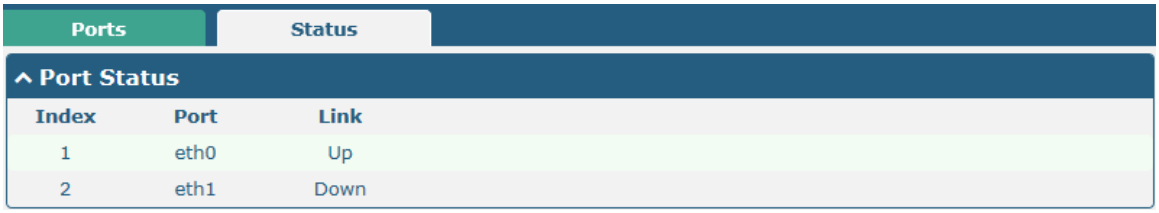
Click button of eth0 to configure its parameters. The port assignment can be changed by selecting from the drop down list.



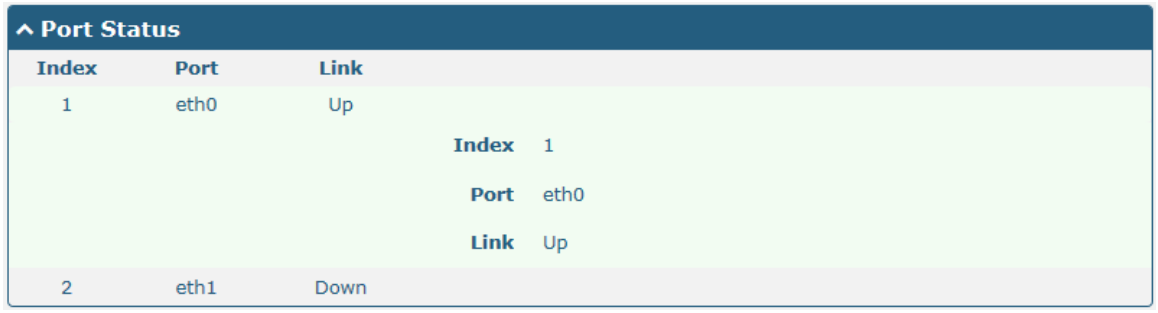


Port Settings		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Choose the Ethernet port's type to lan0 or lan1.	lan0

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

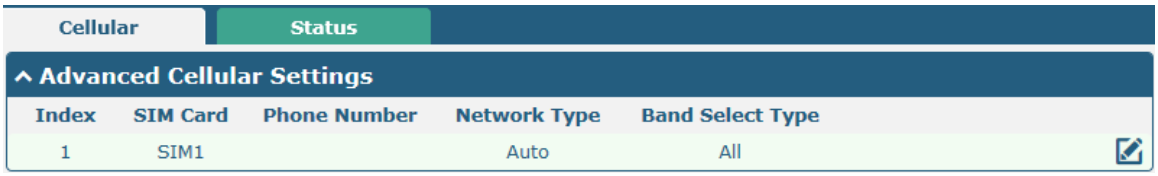


Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.

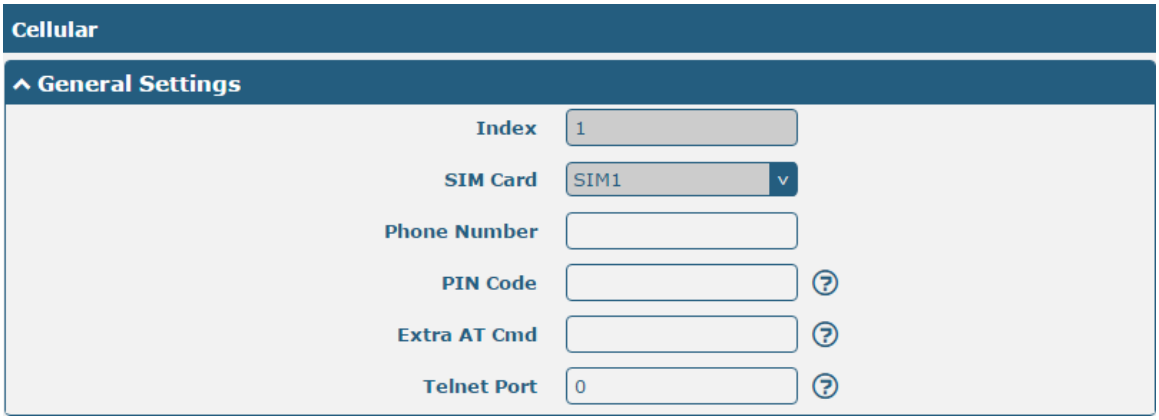


3.9 Interface > Cellular

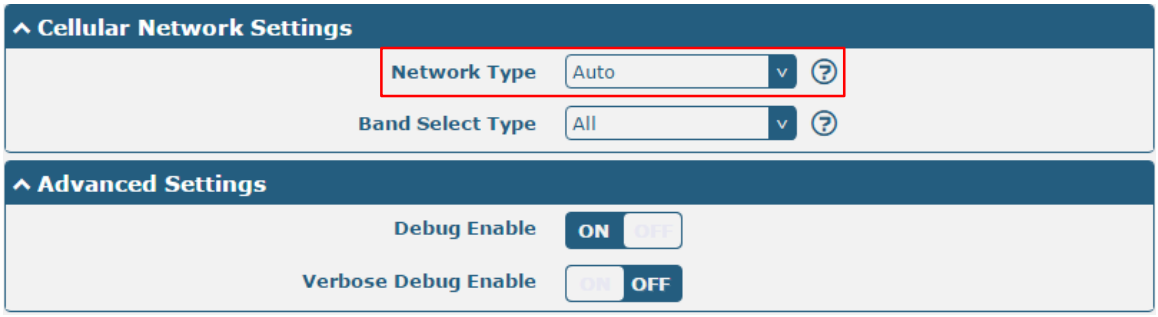
This section allows you to set the related parameters of Cellular.



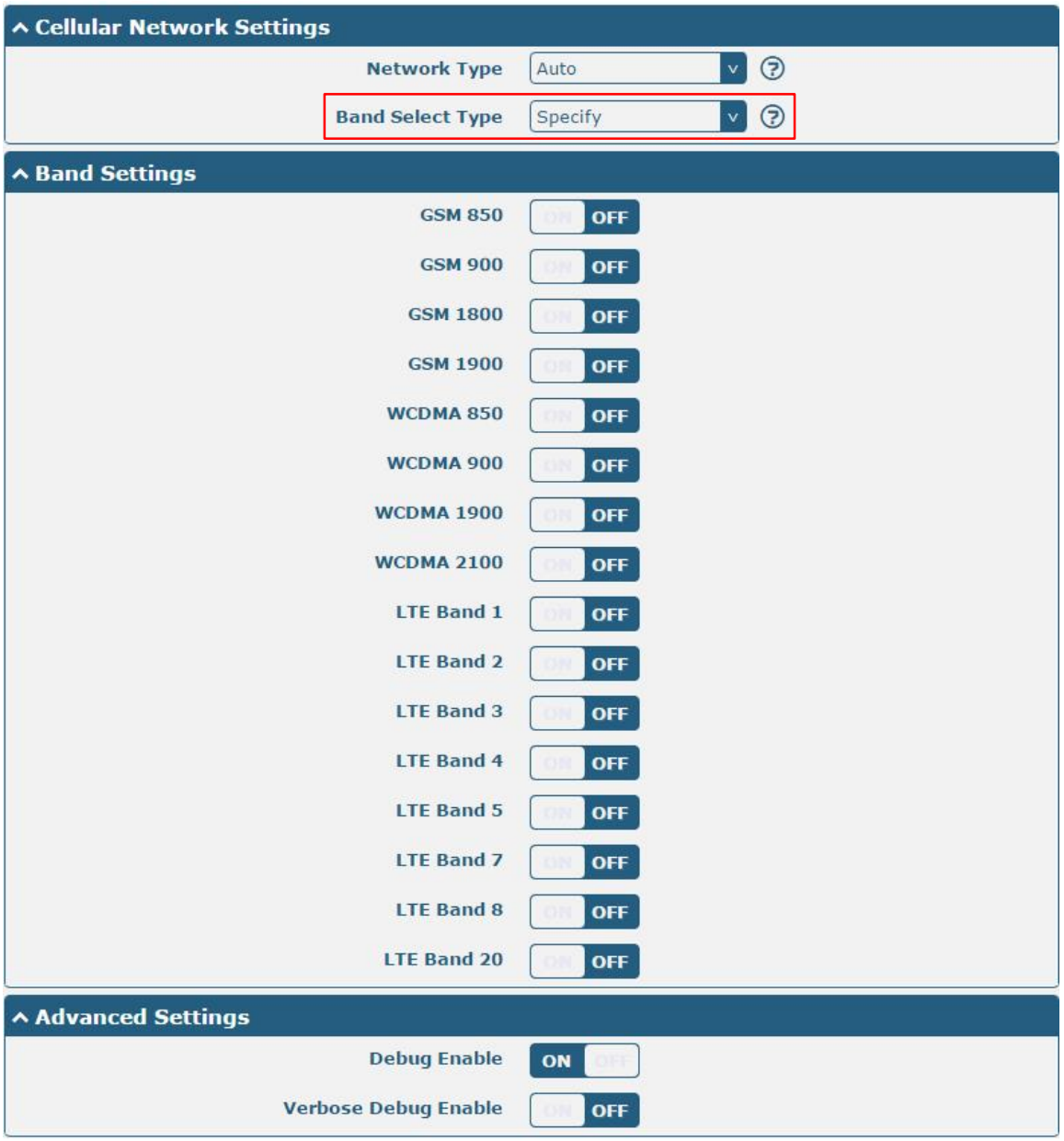
Click of SIM 1 to edit the parameters.



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

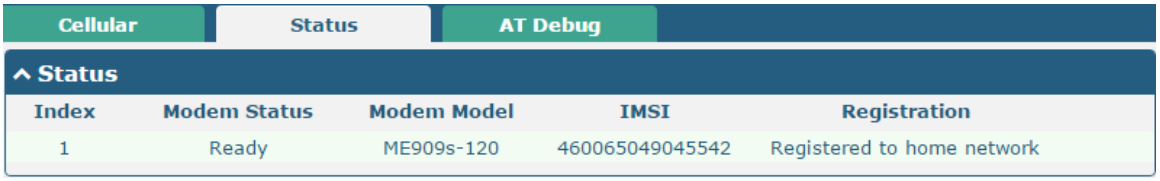


The window is displayed as below when choosing "Specify" as the band select type.



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		
Network Type	Select from “Auto”, “3G Only”, “3G First”, “4G Only”, “4G First”. • Auto: Connect to the best signal network automatically • 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.



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

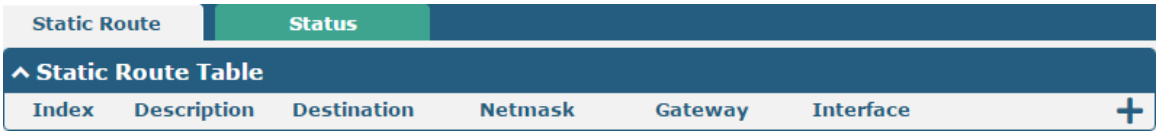
Status	
Item	**Description**
Index	Indicate the ordinal of the list.
Gateway Status	Show the status of the radio module.
Gateway Model	Show the model of the radio module.
Current SIM	Show the SIM card that your gateway is using.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the signal strength detected by the mobile.
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.

Status	
Item	**Description**
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

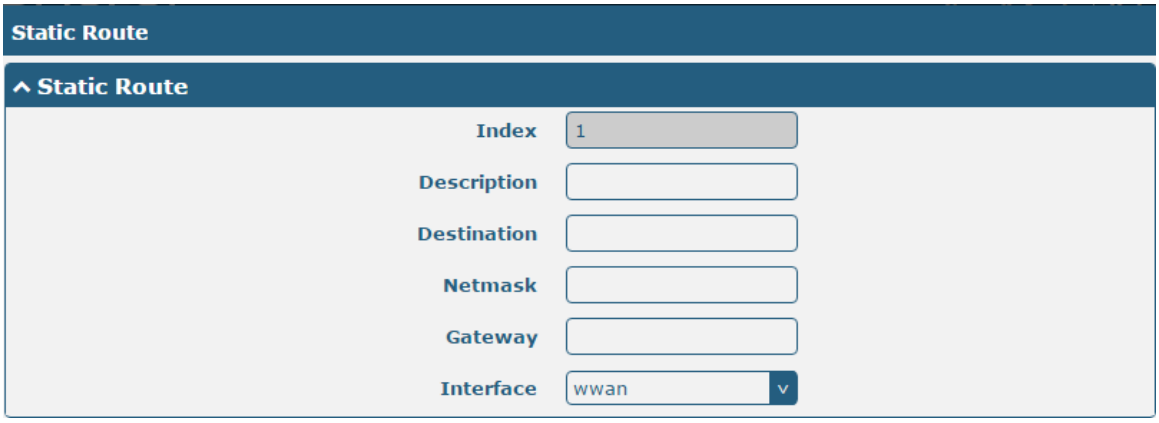
3.10 Network > Route

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.

Static Route



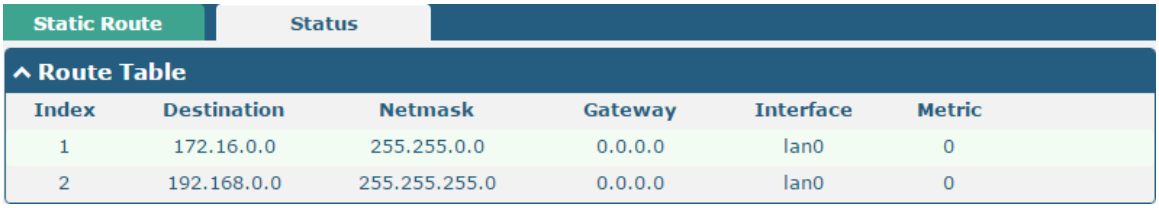
Click + to add static routes. The maximum count is 20.



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

Status

This window allows you to view the status of route.

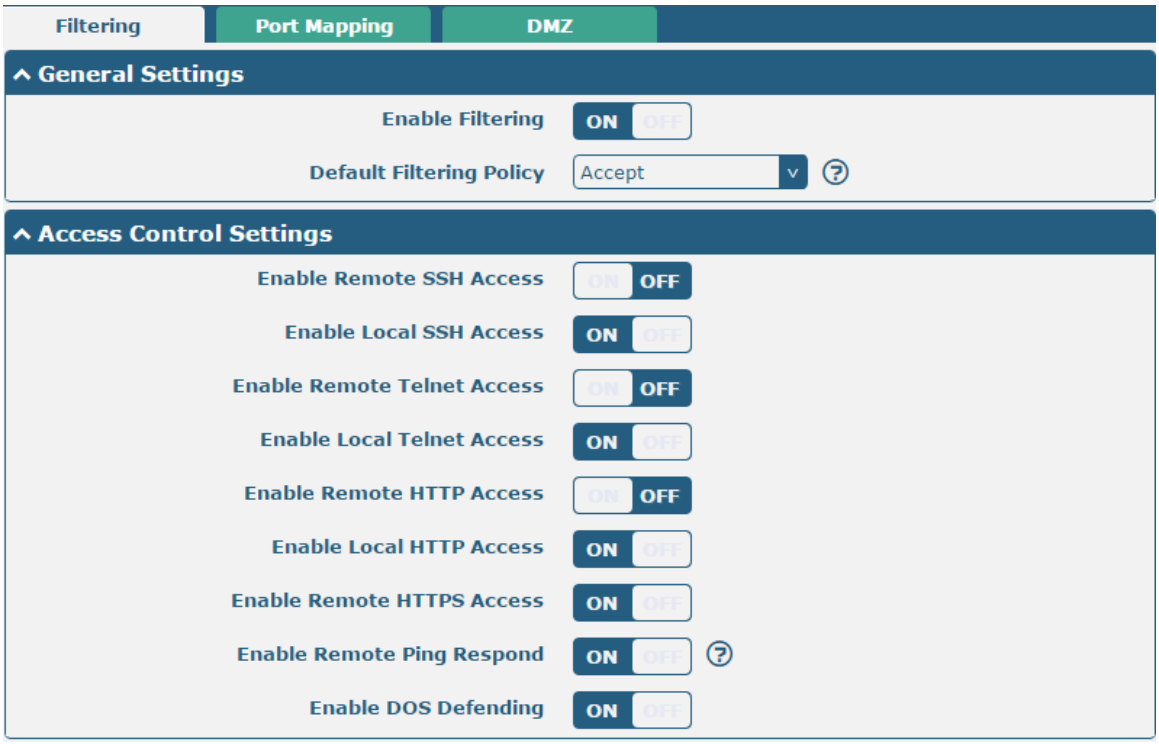


3.11 Network > Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ.

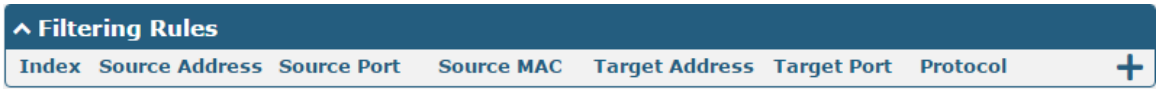
Filtering

The filtering rules can be used to either accept or block certain users or ports from accessing your gateway.

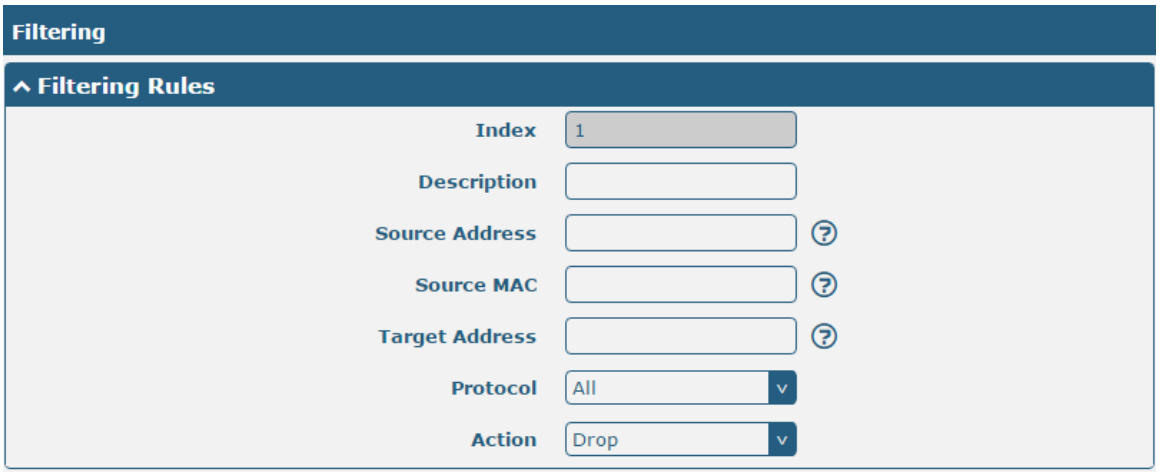


Filtering		
Item	**Description**	**Default**
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. Cannot be changed when filtering rules table is not empty. • Accept: Gateway will accept all the 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

Filtering		
Item	**Description**	**Default**
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



Click + to add a filtering rule. The maximum count is 20.

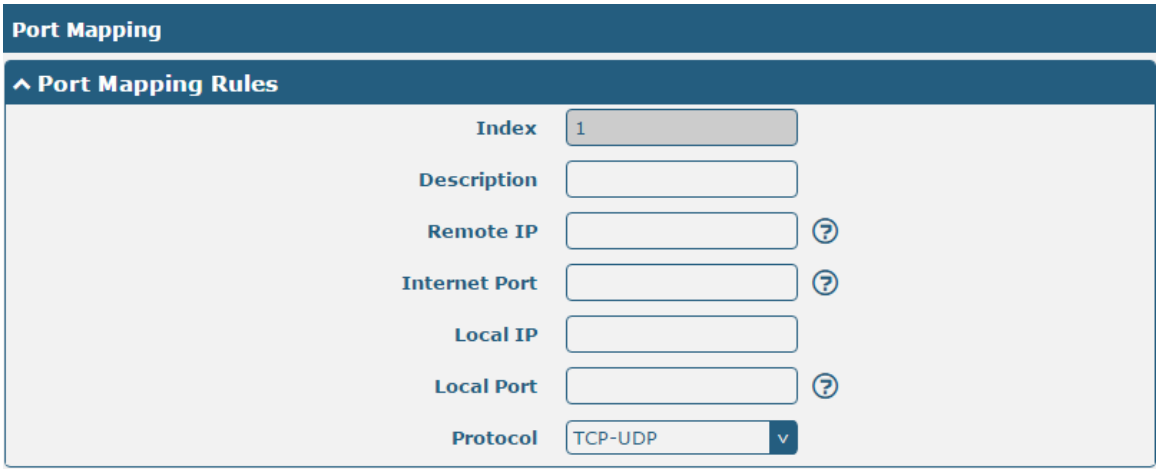


Filtering Rules		
Item	**Description**	**Default**
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	Null

Filtering Rules		
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

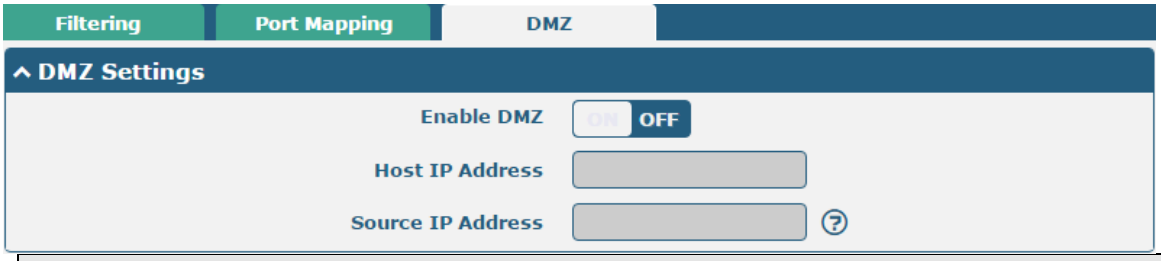
Port Mapping

Click + to add port mapping rules. The maximum rule count is 40.



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

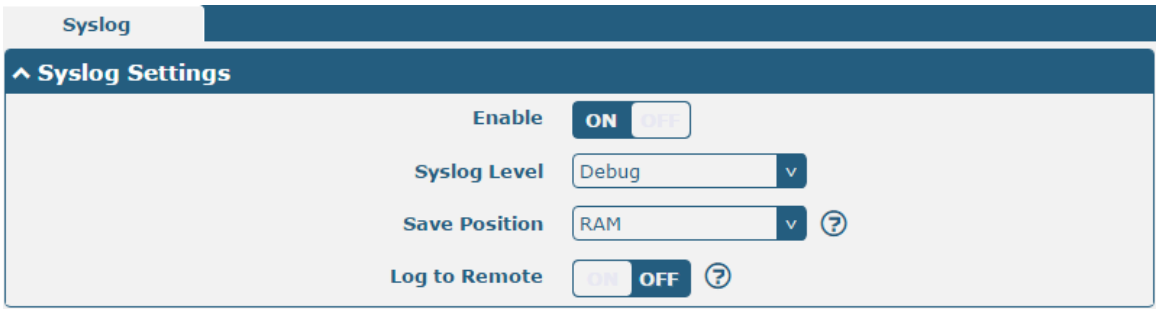
DMZ



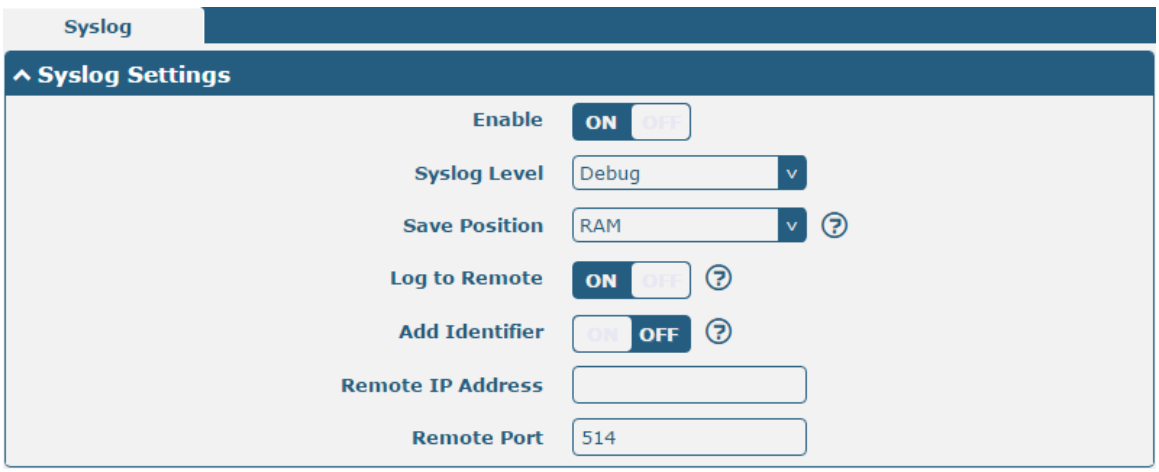
DMZ Settings		
Item	**Description**	**Default**
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null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

3.12 Services > Syslog

This section allows you to set the syslog parameters. The system log of EG9012 Gateway can be saved in the local, also supports to be sent to remote log server and specified application debugging. By default, the "Log to Remote" option is disabled.



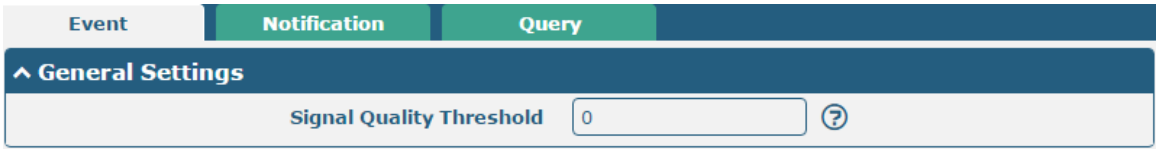
The window is displayed as below when enabling the "Log to Remote" option.



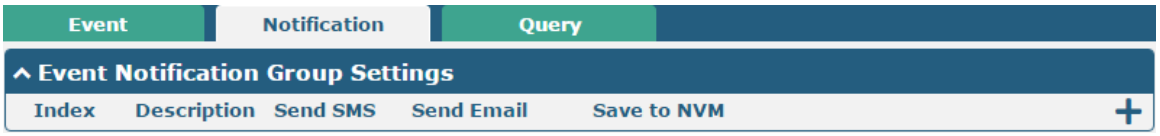
Syslog Settings		
Item	**Description**	**Default**
Enable	Click the toggle button to enable/disable the Syslog settings option.	OFF
Syslog Level	Select from “Debug”, “Info”, “Notice”, “Warning” or “Error”, which from low to high. The lower level will output more syslog in details.	Notice
Save Position	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 (Non-Volatile Memory) 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

3.13 Services > Event

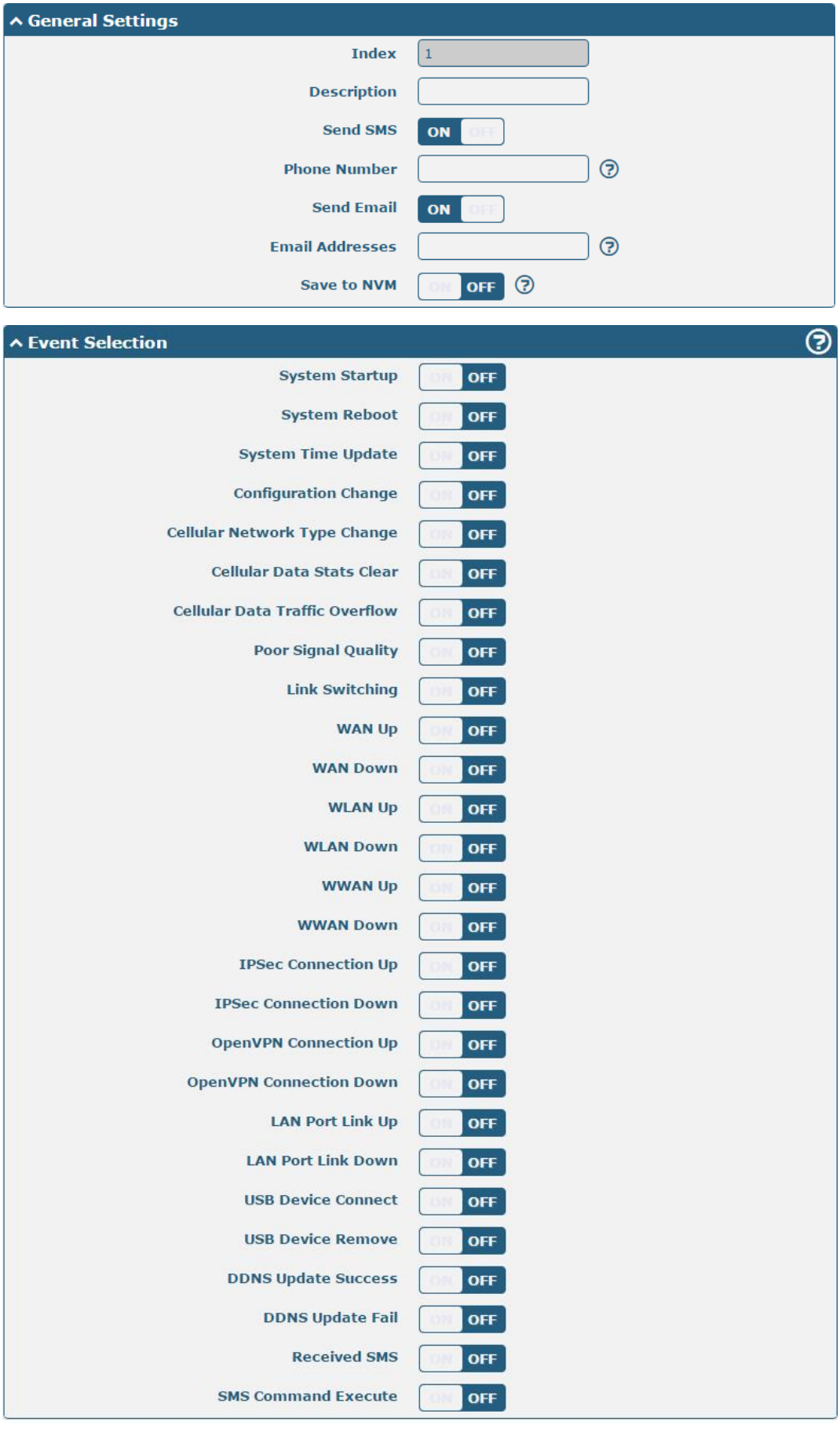
This section allows you to set the event parameters. Event feature provides an ability to send alerts by SMS or Email when certain system events occur.



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

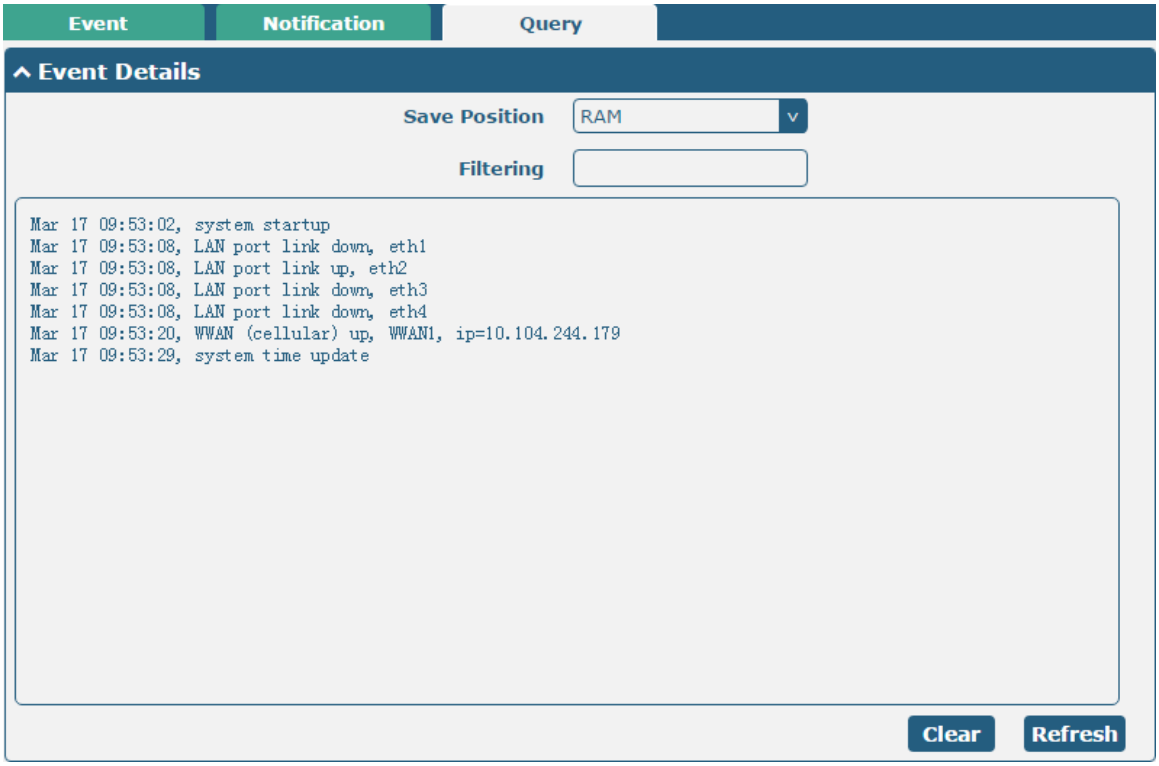


Click + button to add an Event parameters.



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.

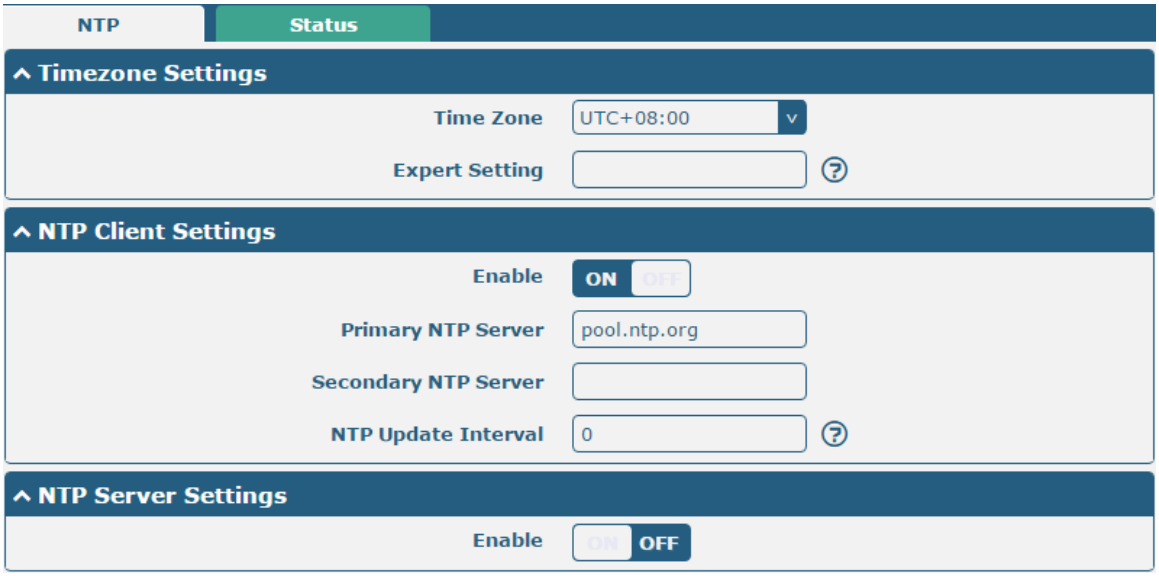


Event Details		
Item	**Description**	**Default**
Save Position	Select the events' save position from "RAM" or "NVM". • RAM: Random-access memory	RAM

	• NVM: Non-Volatile Memory	
Filter Message	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

3.14 Services > NTP

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

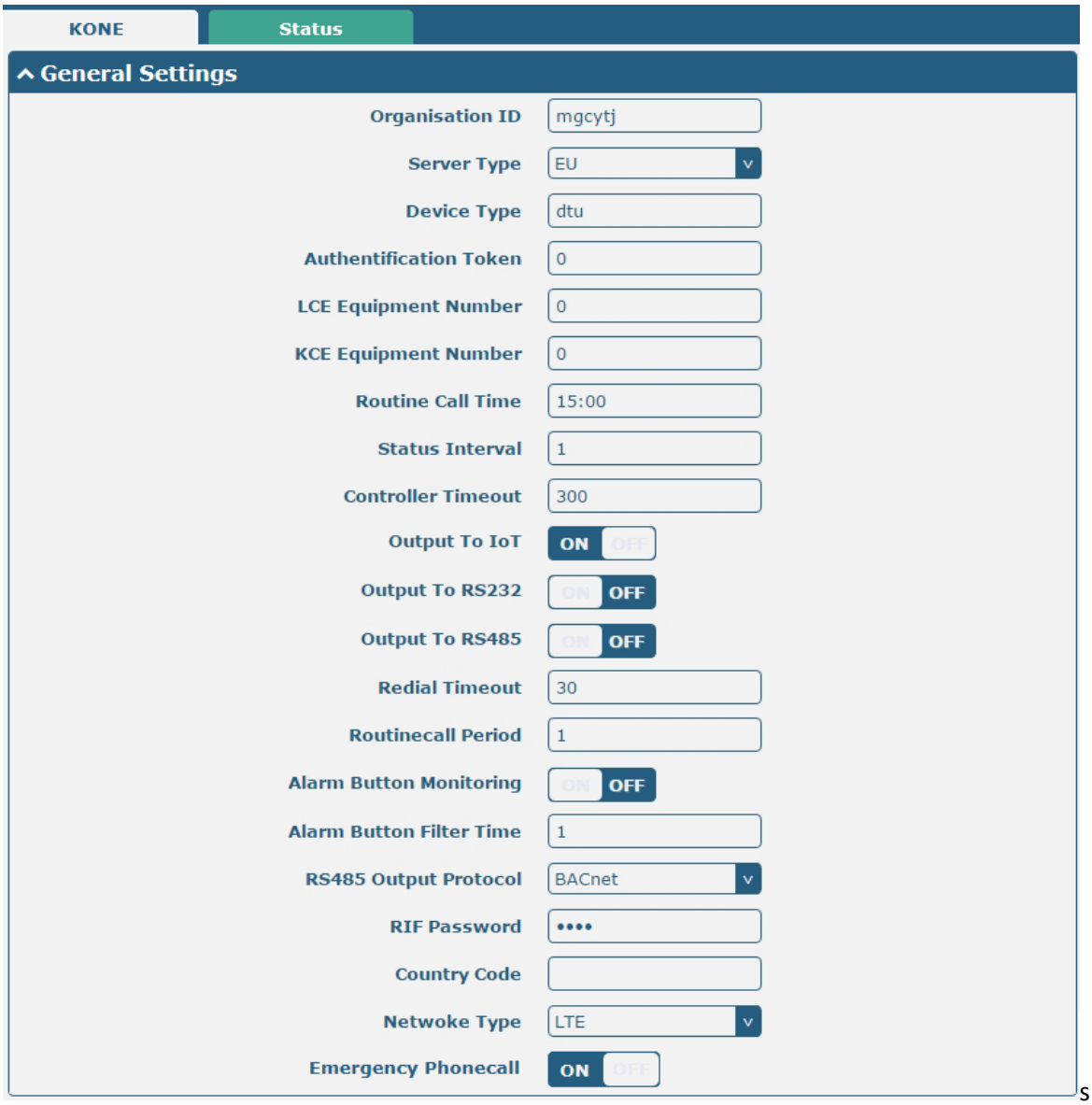


NTP		
Item	**Description**	**Default**
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client 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.

3.15 Service > KONE (for IBM IoT Platform)

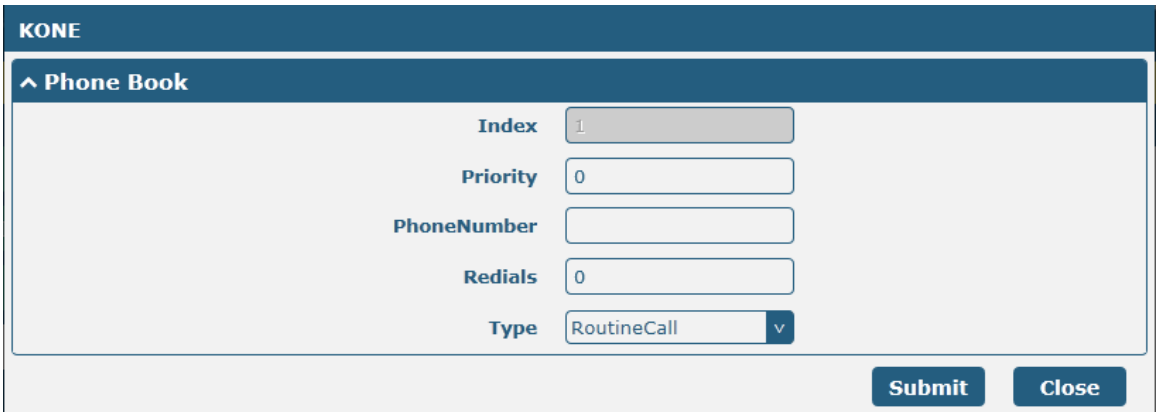
User can configure the related parameters for EG9012 gateway connecting to IBM IoT platform in this section. When EG9012 connected to IBM IoT platform successfully, user can manage and control the gateway on the platform.



s

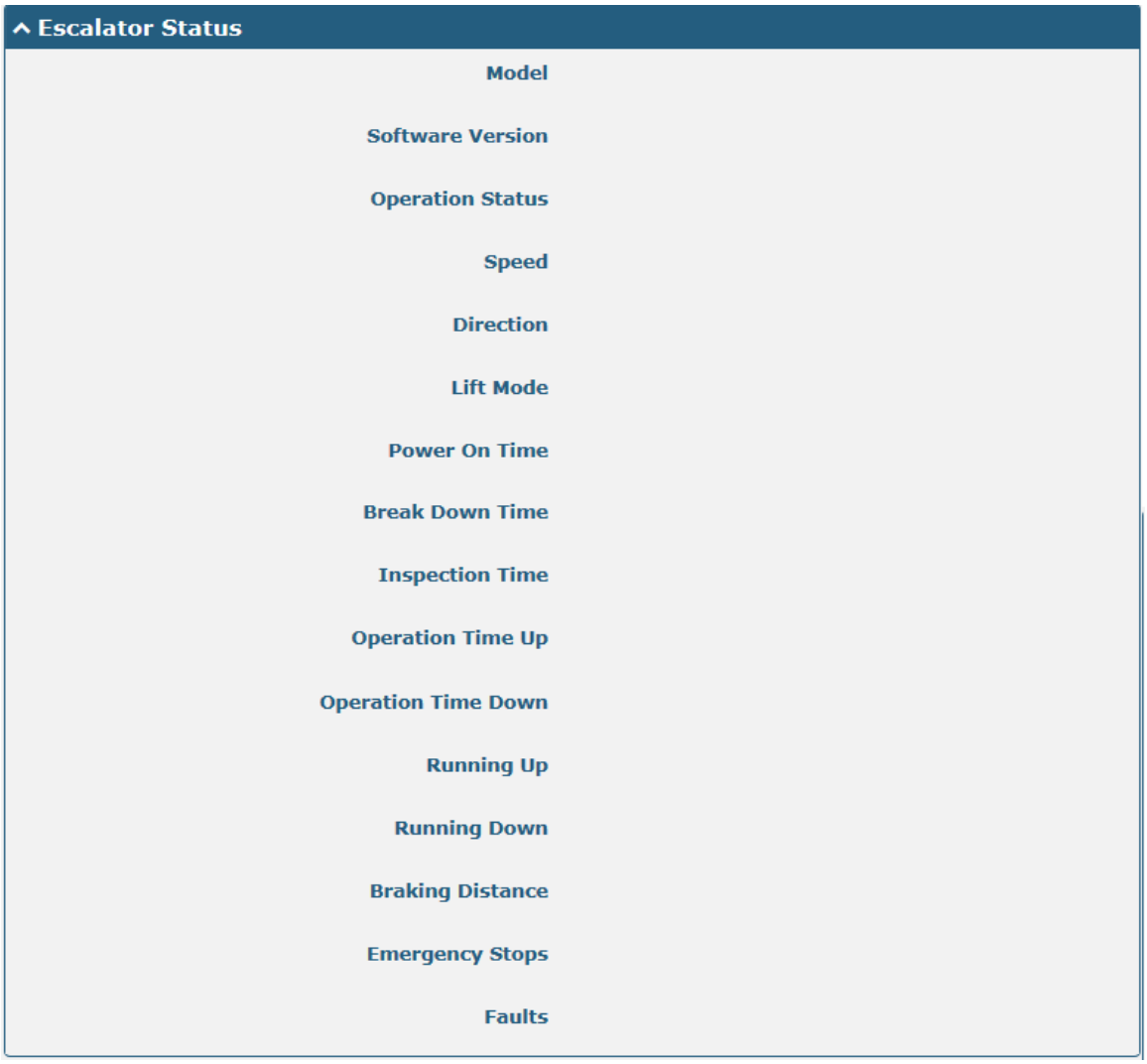
KONE (for IBM IoT Platform)		
Item	**Description**	**Default**
General Settings		
Organisation ID	Enter the organization ID of the server. The KONE project in North America and Europe use the same server, and they server's organization ID default to mgcytj.	mgcytj
Server Type	Choose the server type to EU (Europe & NA) or China.	EU
Device Type	Enter the device type of EG9012.	dtu
Authentification Token	Enter the Authentication token in this item, and the token is assigned from the IBM IoT platform server.	0
LCE Equipment Number	Enter the LCE (Low Cost Electrification) Equipment number. LCE Equipment is the new security controller.	0
KCE Equipment Number	Enter the KCE Equipment number.	0
Routine Call Time	Enter the Routine Call Time.	15:00
Status Interval	Enter the Status Interval, unit: second.	1
Controller Timeout	Set the timeout interval for controller connection, unit: 30.	300
Output To IoT	Enable or disable EG9012 output the running data to IBM IoT platform.	ON
Output To RS232	Enable or disable EG9012 output the running data to the local RS232 serial port.	OFF
Output To RS485	Enable or disable EG9012 output the running data to the local RS485 serial port.	OFF
Redial Timeout	Set the timeout interval for EG9012 redialing, unit: second.	30
Routinecall Period	Set the routine call period, unit: second.	1
Alarm Button Monitoring	Enable or disable the alarm monitor feature.	ON
Alarm Button Filter Time	Set the alarm filter time, unit: second.	1
RS485 Output Protocol	Choose the RS485 output protocol to BACnet or Modbus.	BACnet
RIF Password	Set the RIF Password, the maximum number of characters :	1234
Country Code	Enter the current country code in this item.	Null
Network Type	Choose the network type as LTE or LAN.	LTE
Emergency Phonecall	Enable or disable emergency phone call	ON

Click the + to add a new phone number. Configure the phone book in the following screenshot.



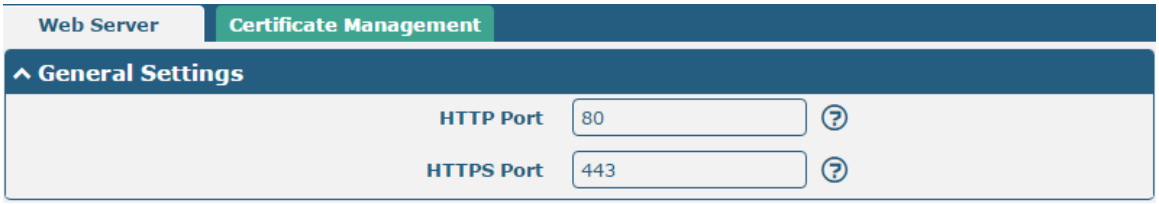
KONE (for IBM IoT Platform)		
Item	**Description**	**Default**
Phone Book		
Index	Show the code of the current phone number.	/
Priority	Set the priority of the current phone number.	0
PhoneNumber	Enter the phone number in this item.	Null
Redials	Set the interval time for redialing.	0
Type	Select from RoutineCall, Failurecall or Alarmcall.	Rountinecall

Check the status of the Elevator and Escalator.



3.16 Services > Web Server

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



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

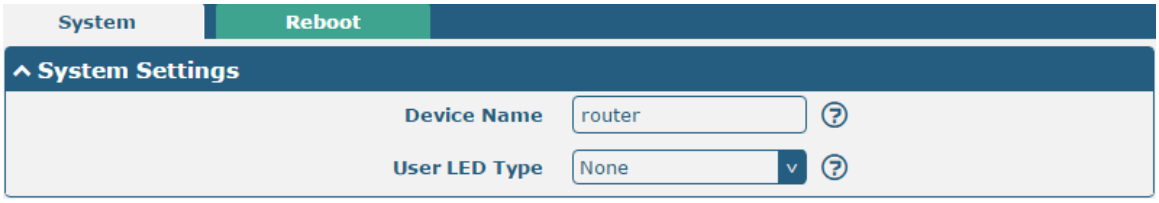
HTTPS Port	Enter the HTTPS port number you want to change in gateway's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the gateway with other HTTPS Port number except 443, only adding that port number then you can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

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

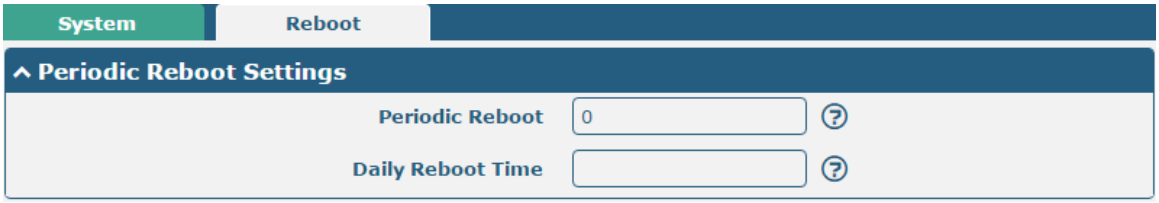
Import Certificate		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". • CA: a digital certificate issued by CA center • Private Key: a private key file	CA
HTTPS Certificate	Click on "Choose File" to locate the certificate file from your computer, and then click "Import"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

3.17 Services > Advanced

This section allows you to set the Advanced and parameters.



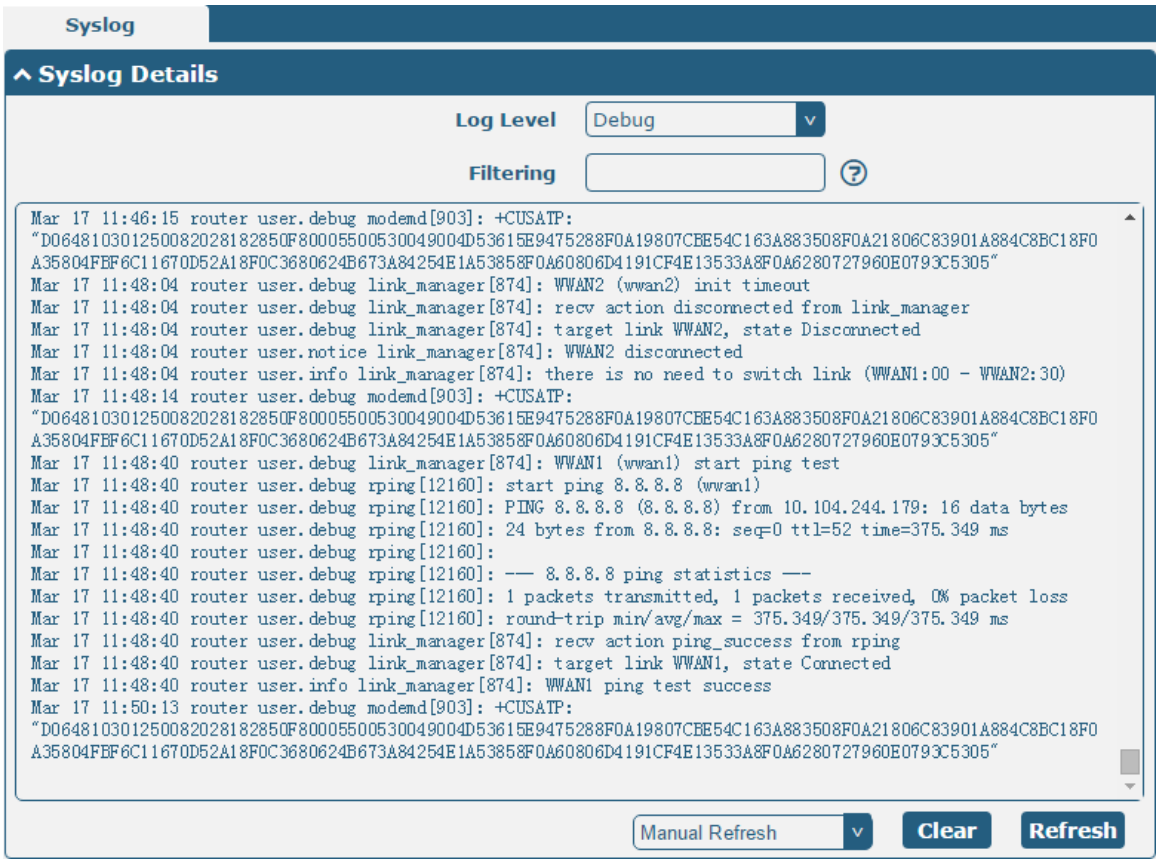
System Settings		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, $, and *.	gateway
User LED Type	This Feature is unavailable in EG9012 Gateway.	None

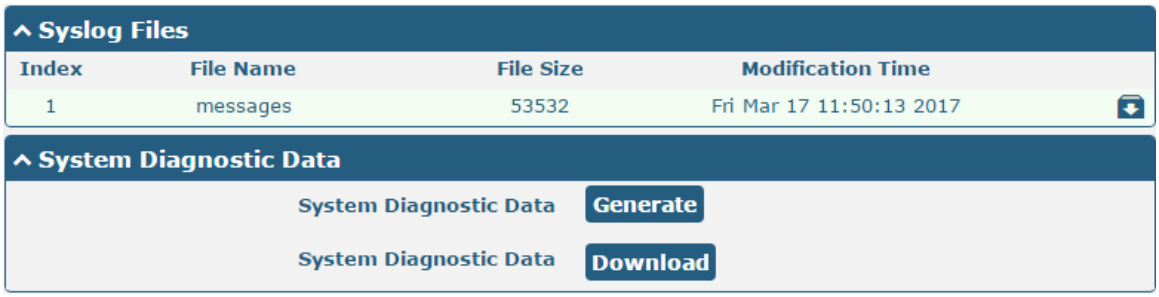


Periodic Reboot Settings		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the gateway. 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the gateway. You should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty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

3.18 System > Debug

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

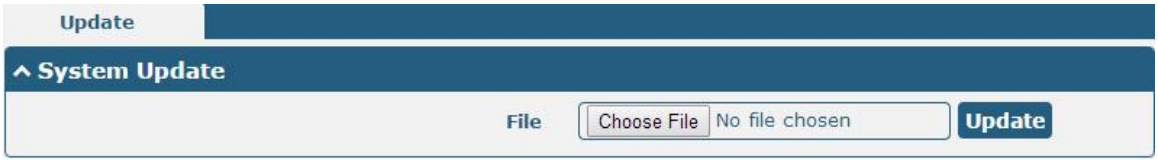




Syslog		
Item	**Description**	**Default**
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Enter the filtering message based on the keywords. Use “&” to separate more than one filter 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.	--

3.19 System > Update

This section allows you to upgrade the firmware of your EG9012. 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.

System Update		
Item	**Description**	**Default**

System Update	Click Choose File button to select the correct firmware in your PC, and then click Update button to update. After updating successfully, you need to click "save and apply", and then reboot the gateway to take effect.	Null

3.20 System > APP Center

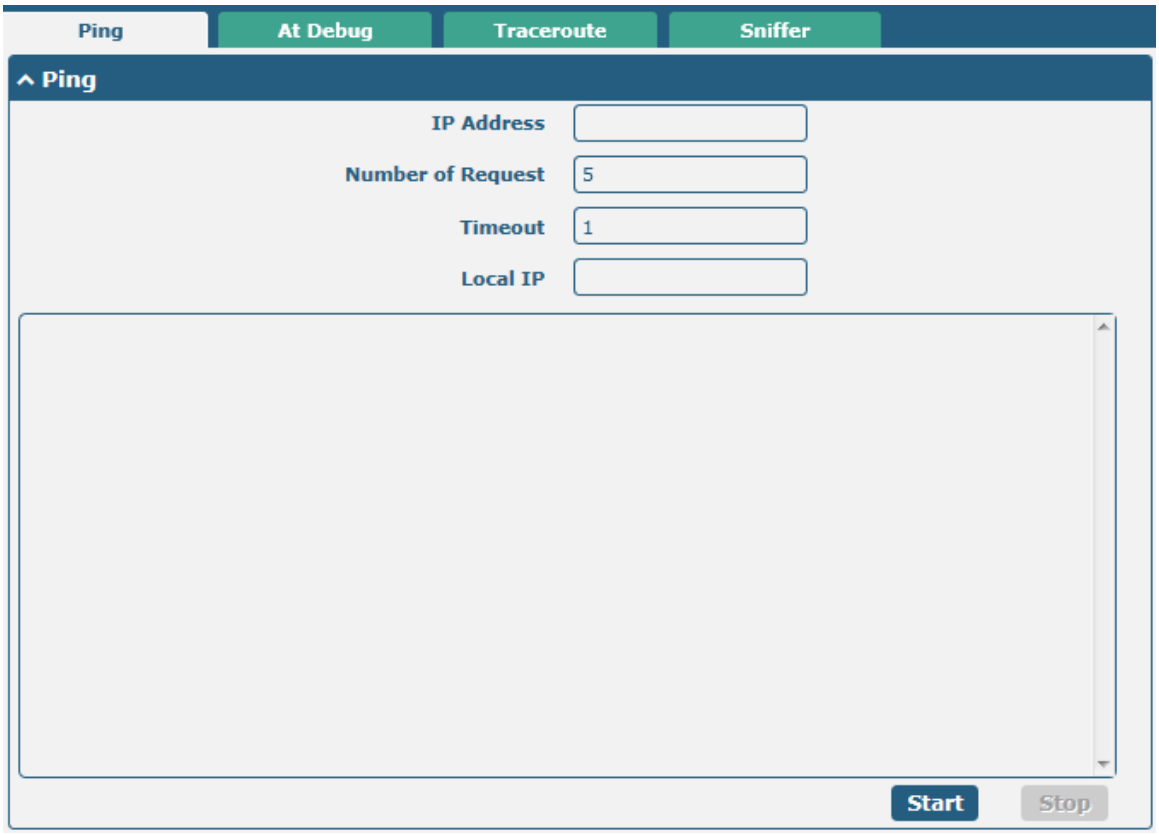
This section allows you to add some required or customized applications to the gateway. Import and install your applications to the APP Center, and reboot the device according to the system prompts. Each installed application will be displayed under the "Services" menu, while other applications related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

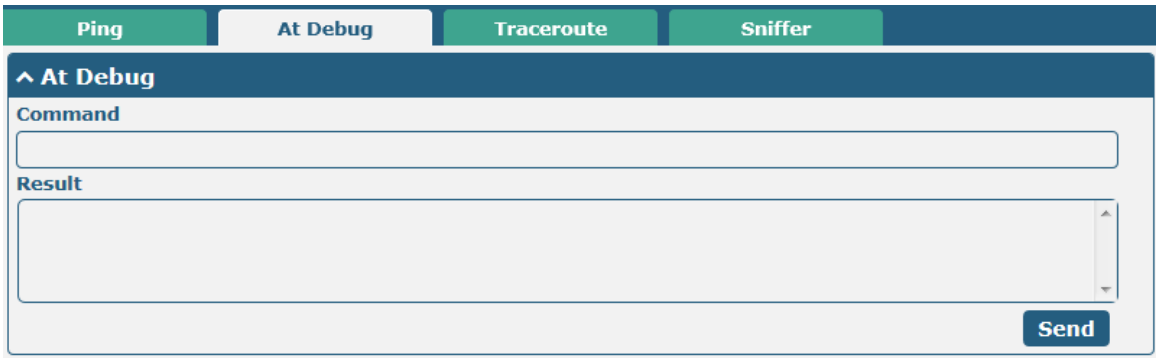
App Center		
Item	**Description**	**Default**
App Install		
File	Click on "Choose File" to locate the App file from your computer, and then click Install to import this file into your gateway. **Note**: File format should be *xxx.rpk*, e.g. *EG9012-robustlink-1.0.0.rpk*.	--
Installed Apps		
Index	Indicate 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

3.21 System > Tools

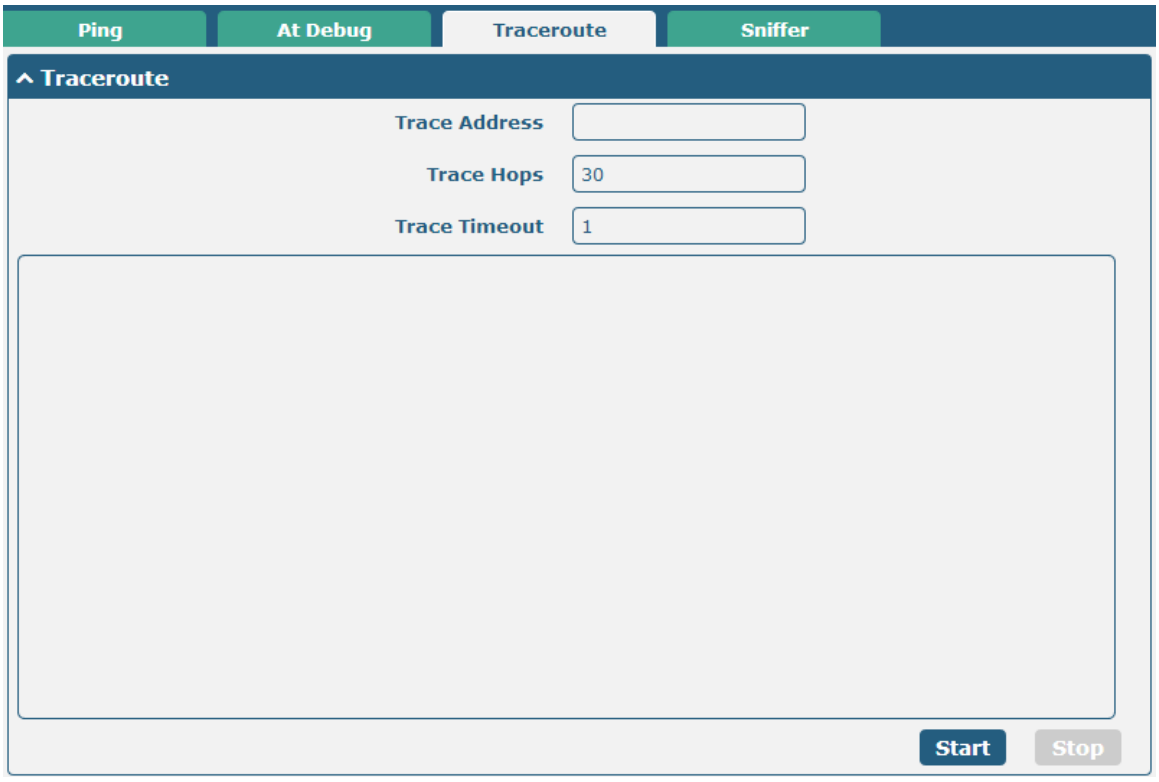
This section provides users three tools: Ping, At Debug, Traceroute and Sniffer.



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.	--

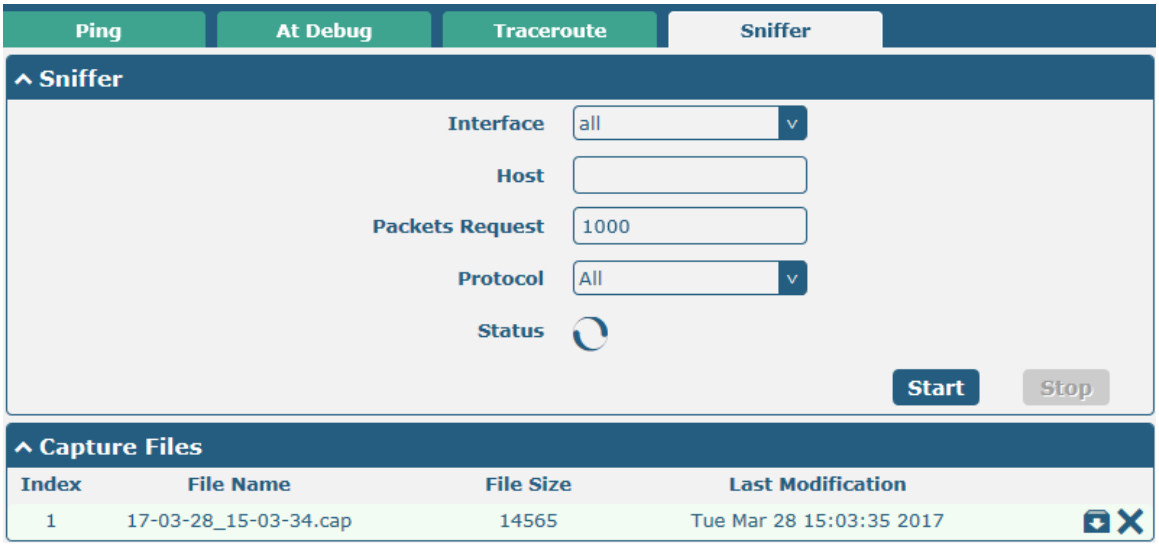


At Debug @ Tools	
Item	Description
Command	Enter a At command in Command box, then click Send button to send the At command to the cellular module.
Result	It will display the AT commands which respond from the cellular module in this box.



Traceroute		
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

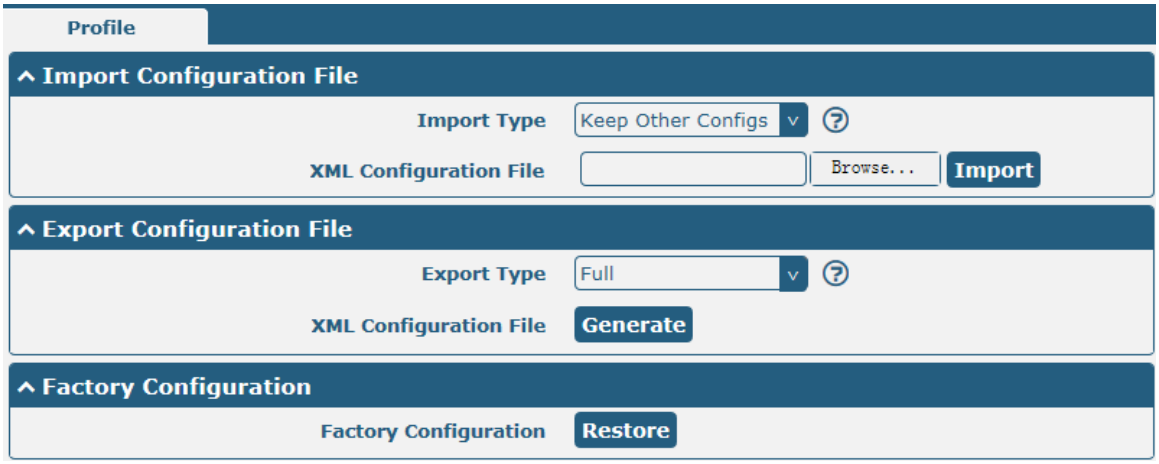
Start	Click this button to start Traceroute request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop Traceroute request.	--



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 that the gateway can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	--
Stop	Click this button to stop the sniffer. Once 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

3.22 System > Profile

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

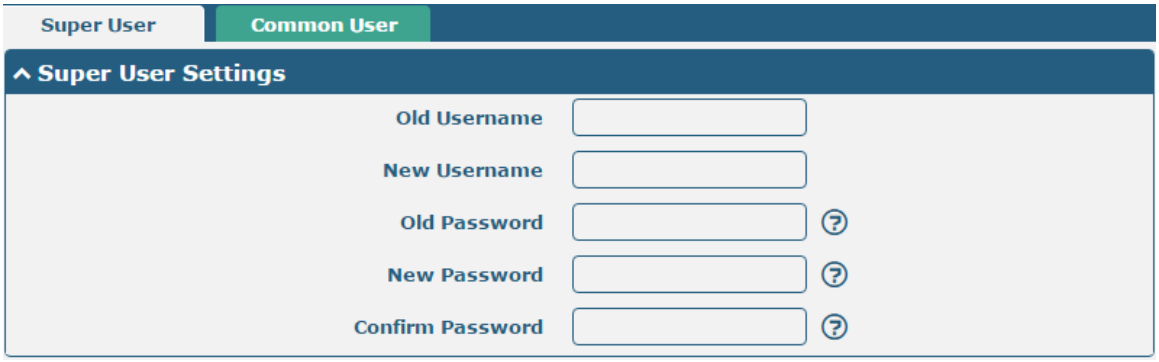


Profile		
Item	**Description**	**Default**
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as "ON" to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as "OFF" to ignore invalid settings.	OFF
XML Configuration File	Click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

3.23 System > 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		
Item	**Description**	**Default**
Old Username	Enter the old username of your gateway. The default is “kone”.	Null
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 “kone”.	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

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

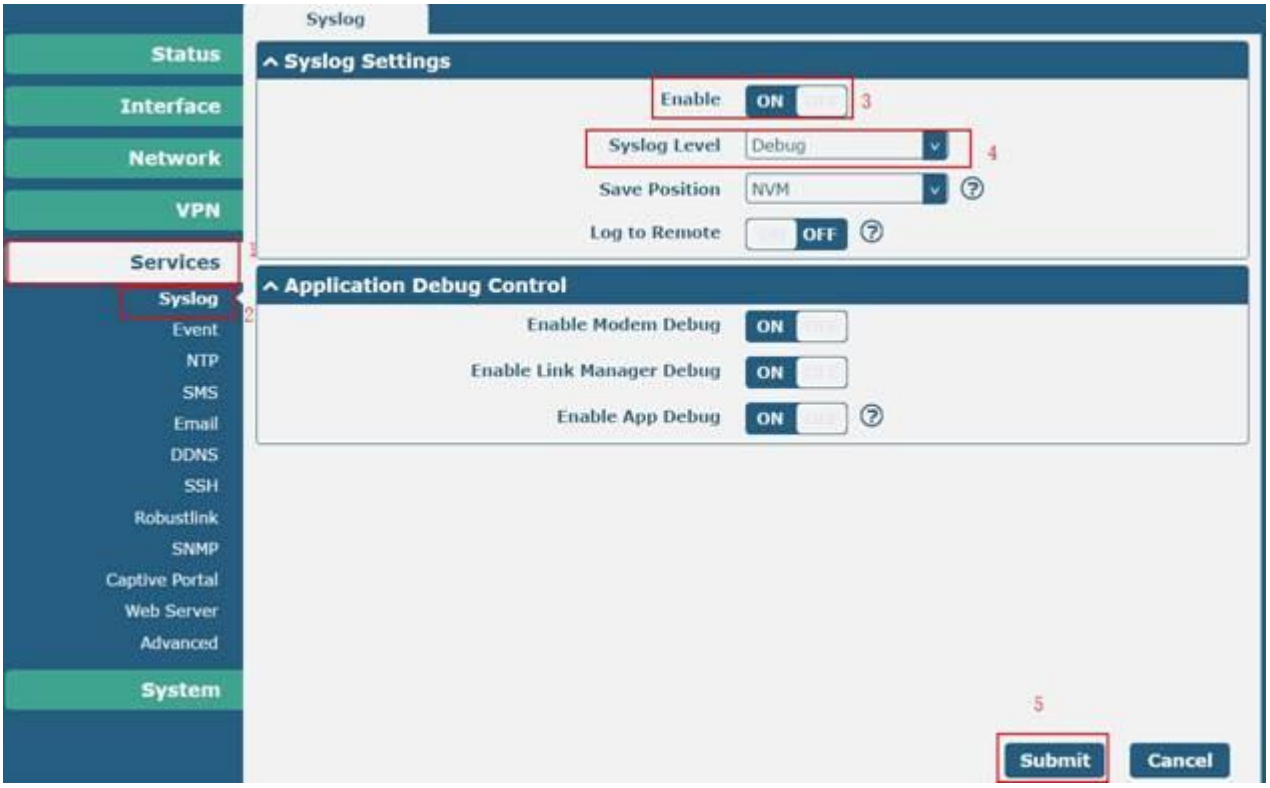
Common User Settings		
Item	**Description**	**Default**

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

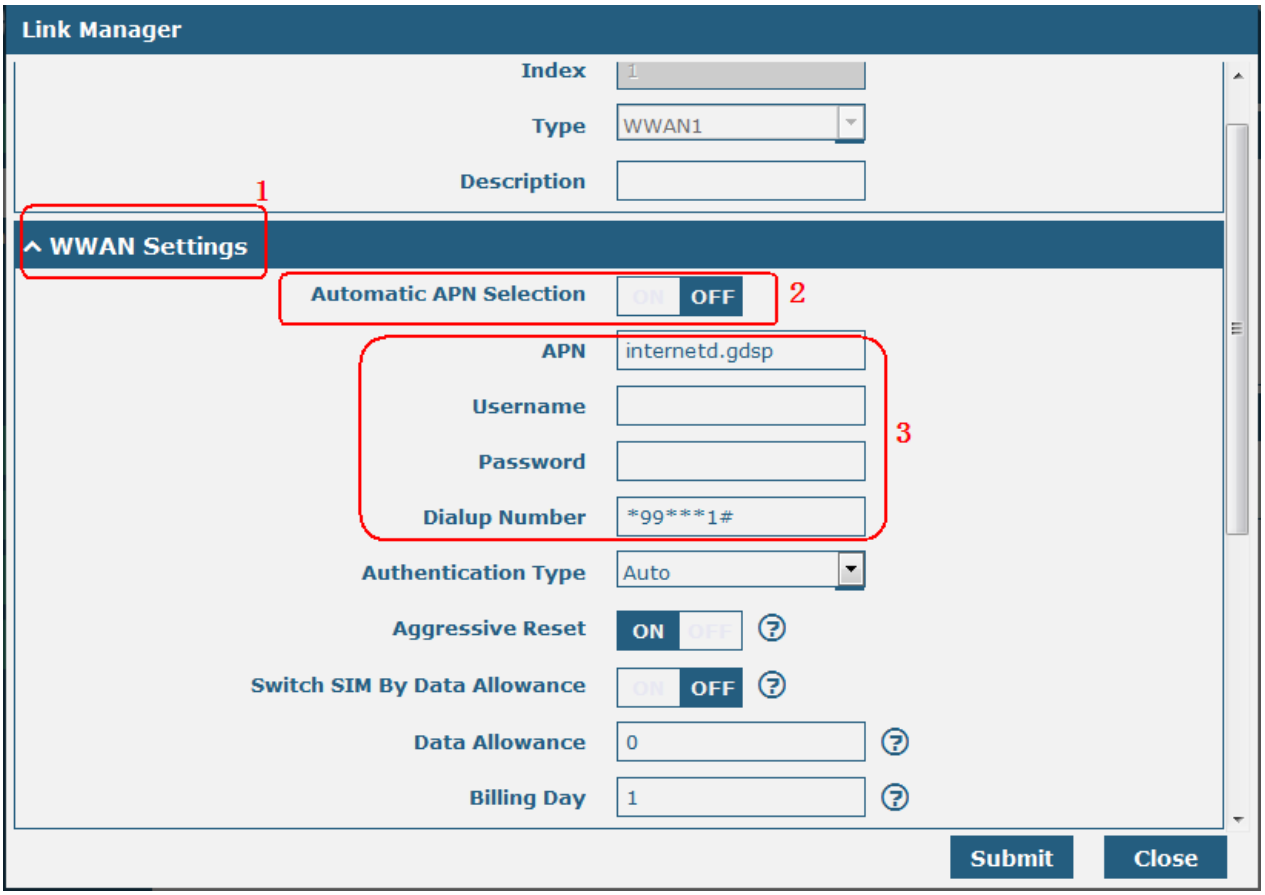
Chapter 4 Configuration Examples

4.1 Generate diagnose file about APN

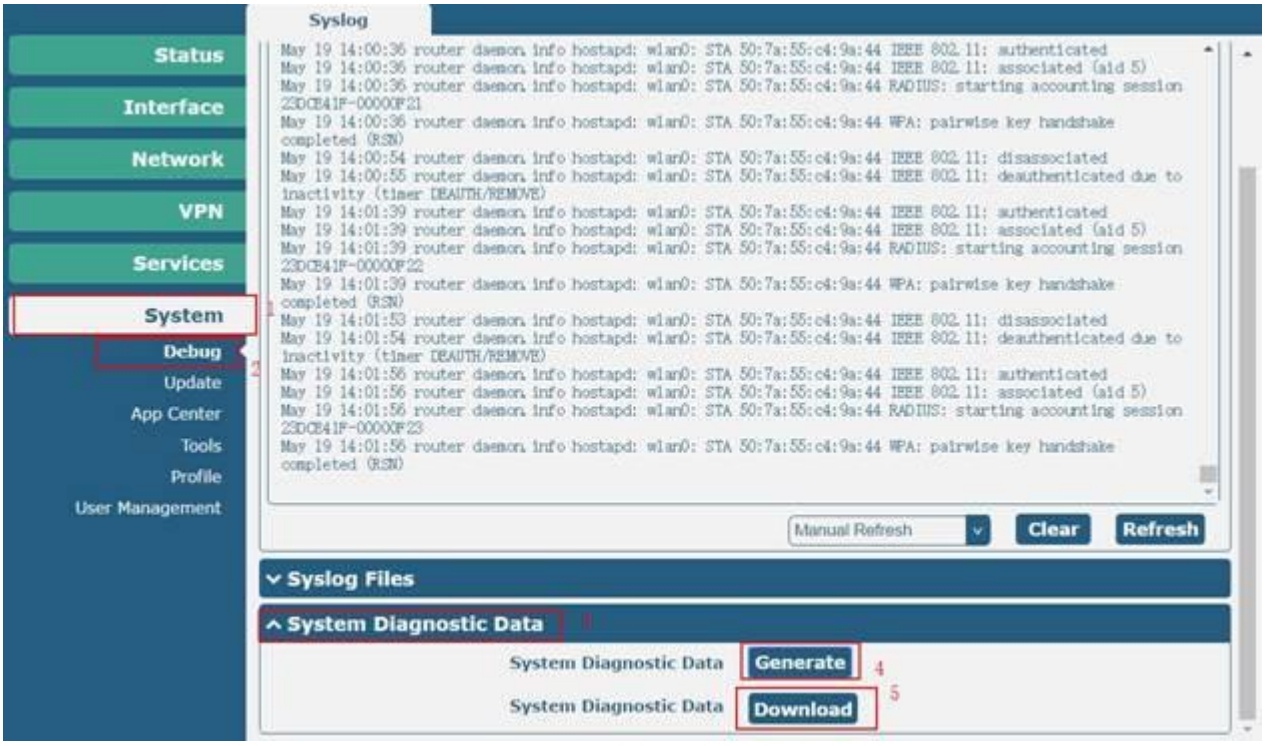
1) Enable syslog feature on router



2) Manually setting APN.



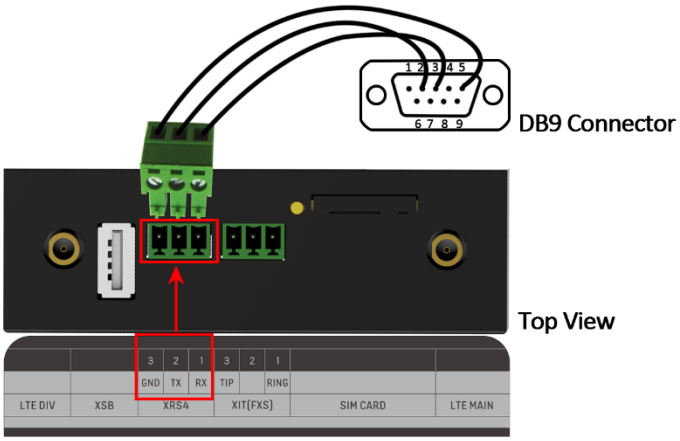
3) Generate diagnose file



4.2 Terminal Block Connection

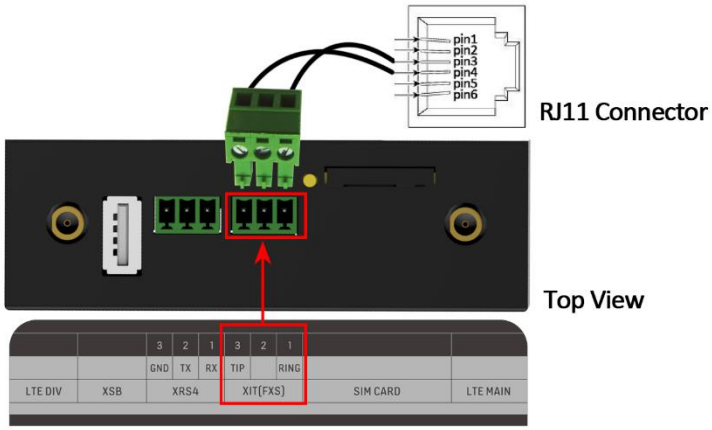
4.2.1 Console Port

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



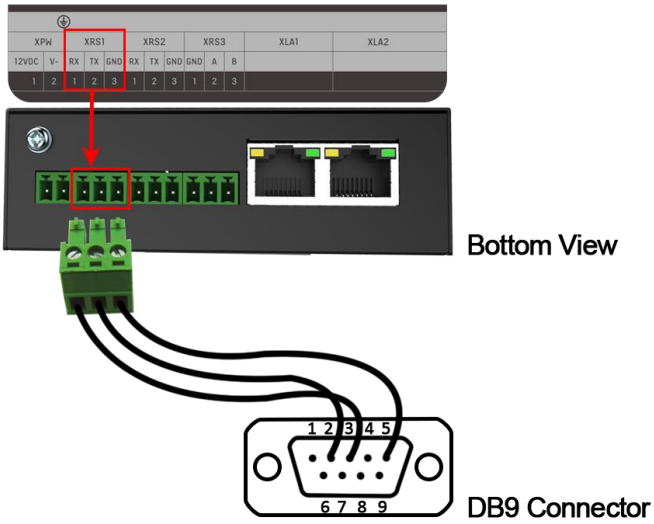
4.2.2 Audio Port

EG9012 supports one FXS port for voice conversation.
Please refer to the connection diagram at the right site.



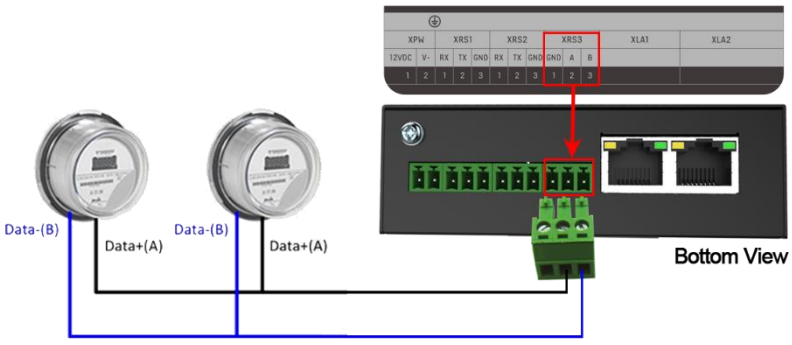
4.2.3 RS232

EG9012 supports two RS232 for serial data communication. Please refer to the connection diagram at the right site.



4.2.4 RS485

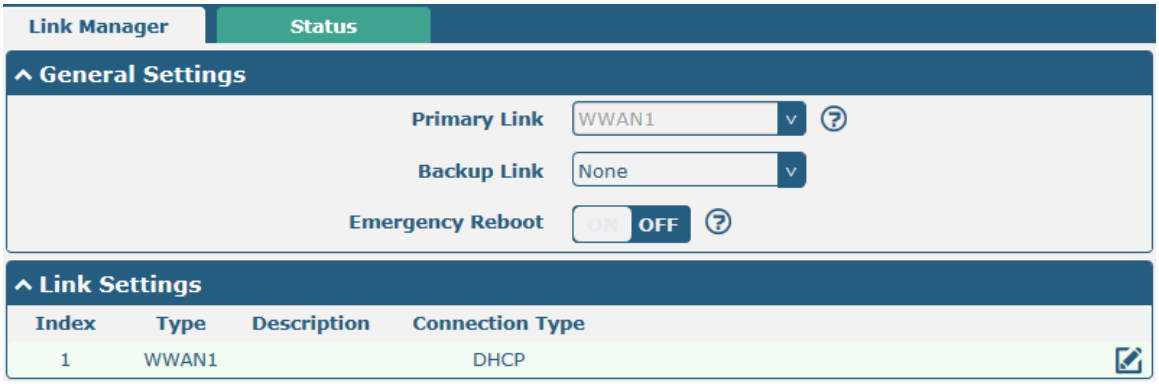
EG9012 supports one RS485 for serial data communication.
Please refer to the connection diagram at the right site.



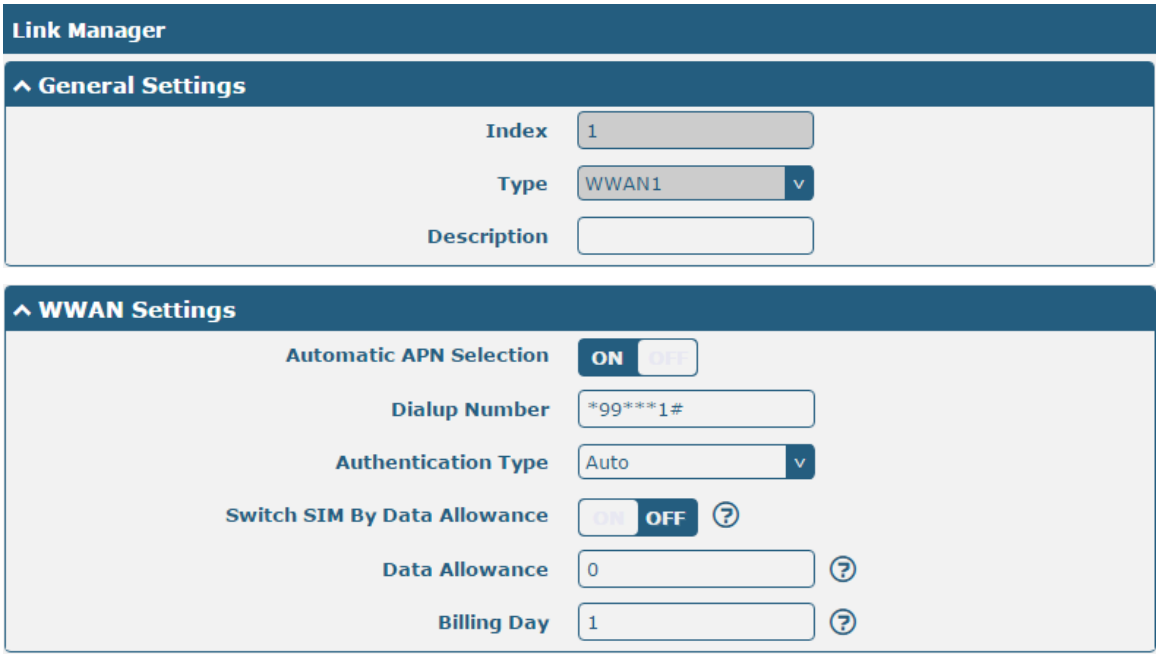
4.3 Cellular Connection

4.3.1 Cellular Dial-Up

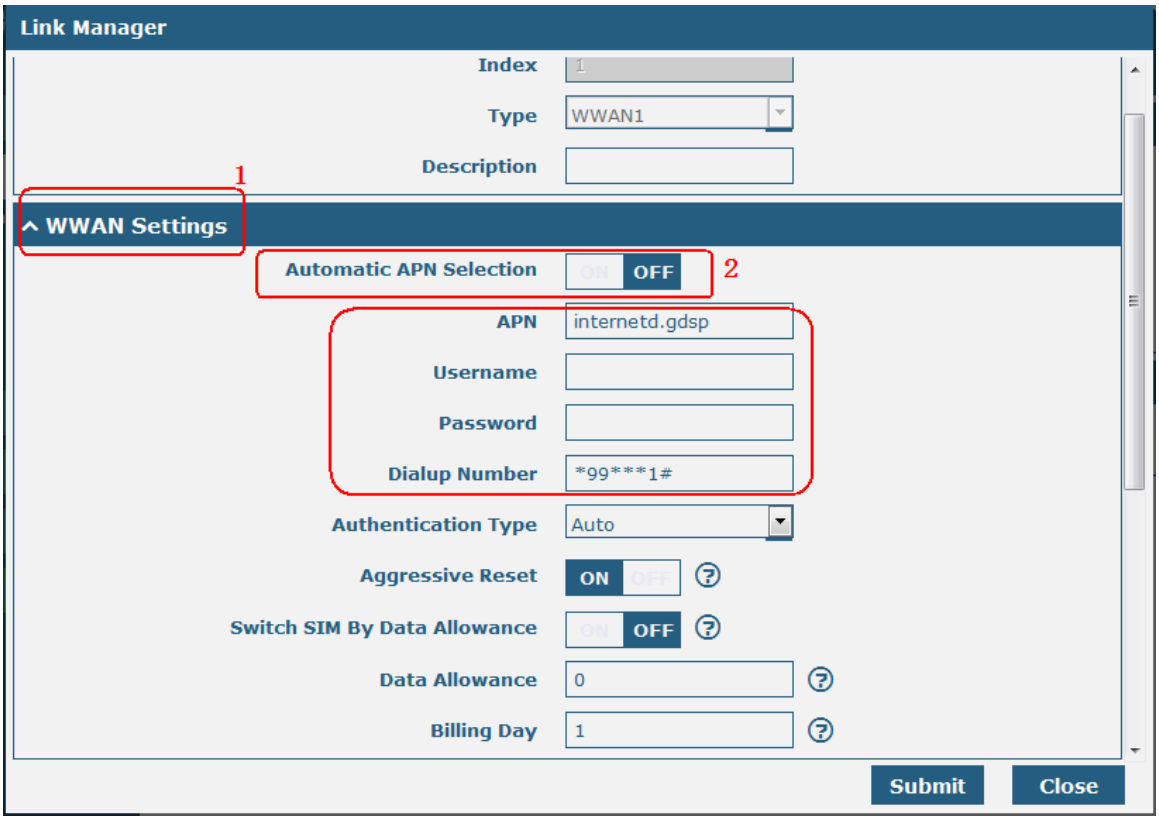
This section shows you how to configure SIM card for Cellular Dial-up. Connect the gateway correctly and insert SIM, then open the configuration page. Under the homepage menu, click **Interface > Link Manager > General Settings**.

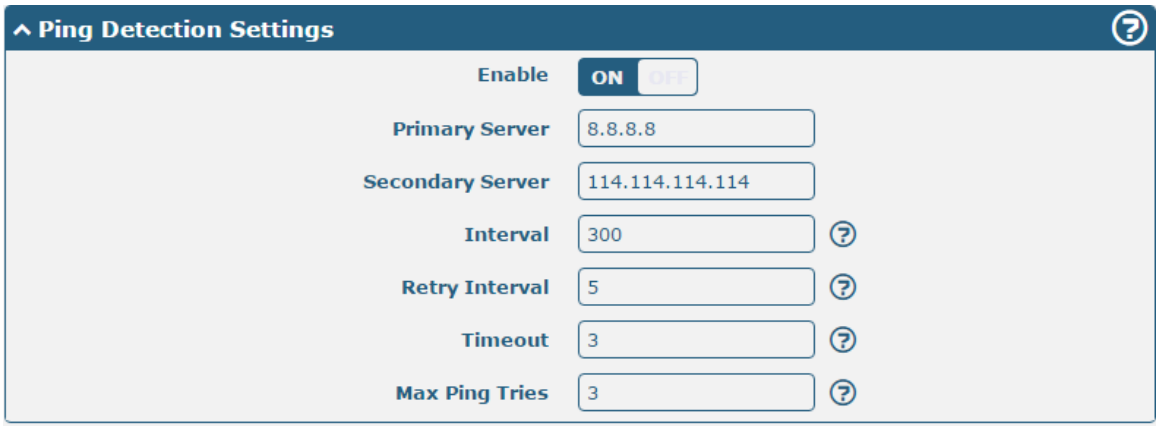


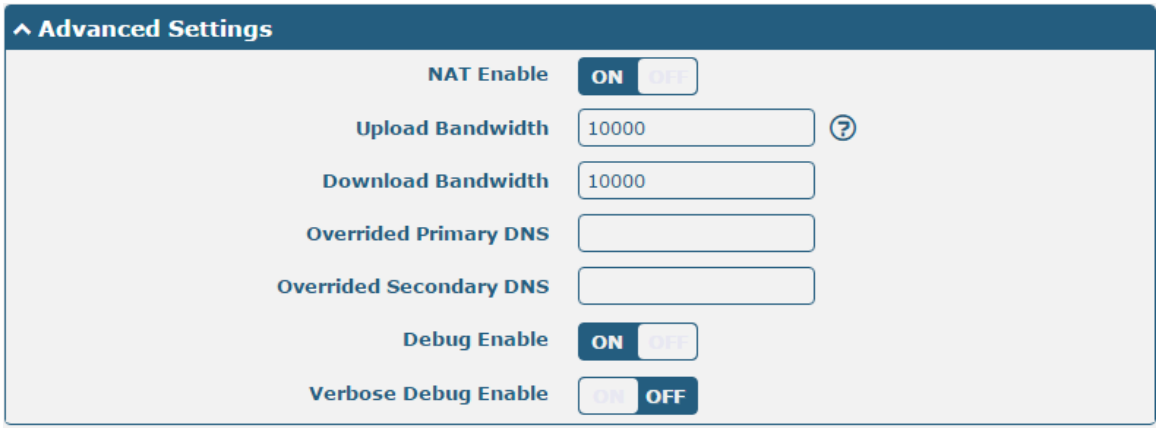
Click the edit button of WWAN1 to set its parameters according to the current ISP.



For AT&T in NA, you should set the APN as following screenshot.

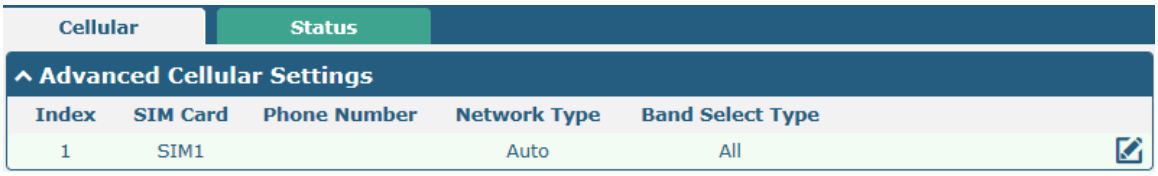




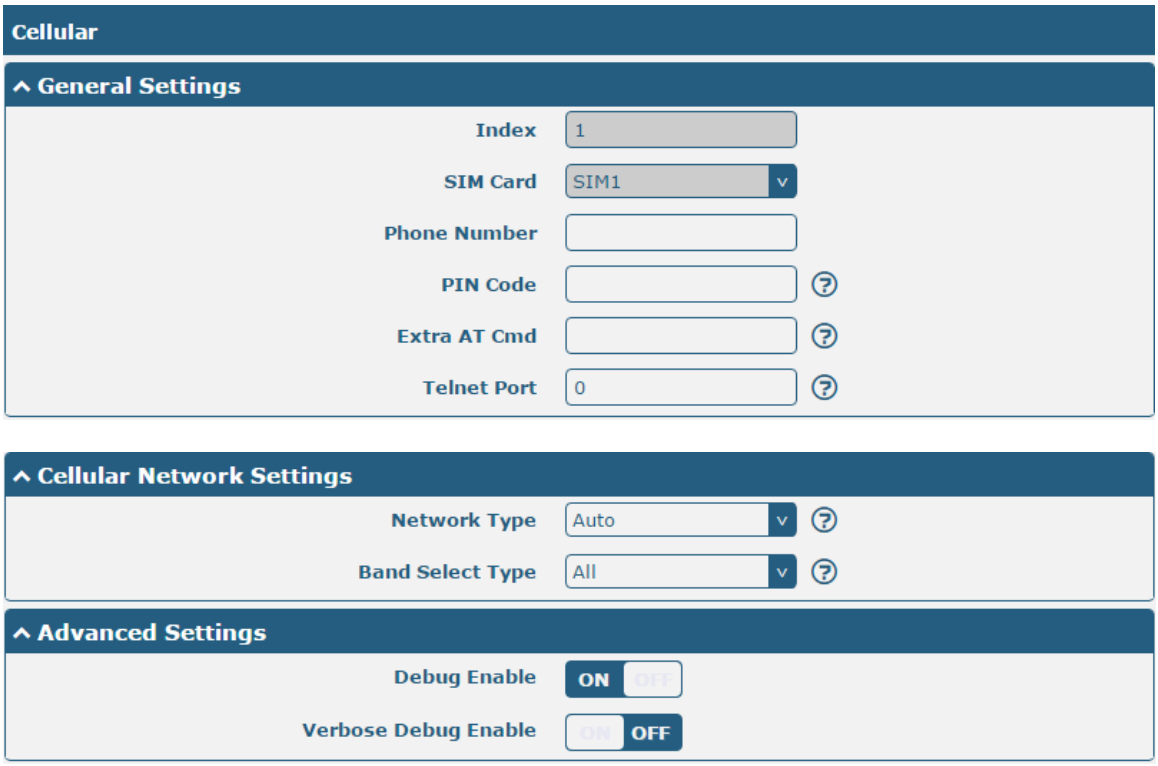


When finished, click **Submit > Save & Apply** for the configuration to take effect.

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



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



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

4.3.2 SMS Remote Control

EG9012 supports remote control via SMS. You can use following commands to get the status of EG9012, and set all the parameters of EG9012. 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--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).

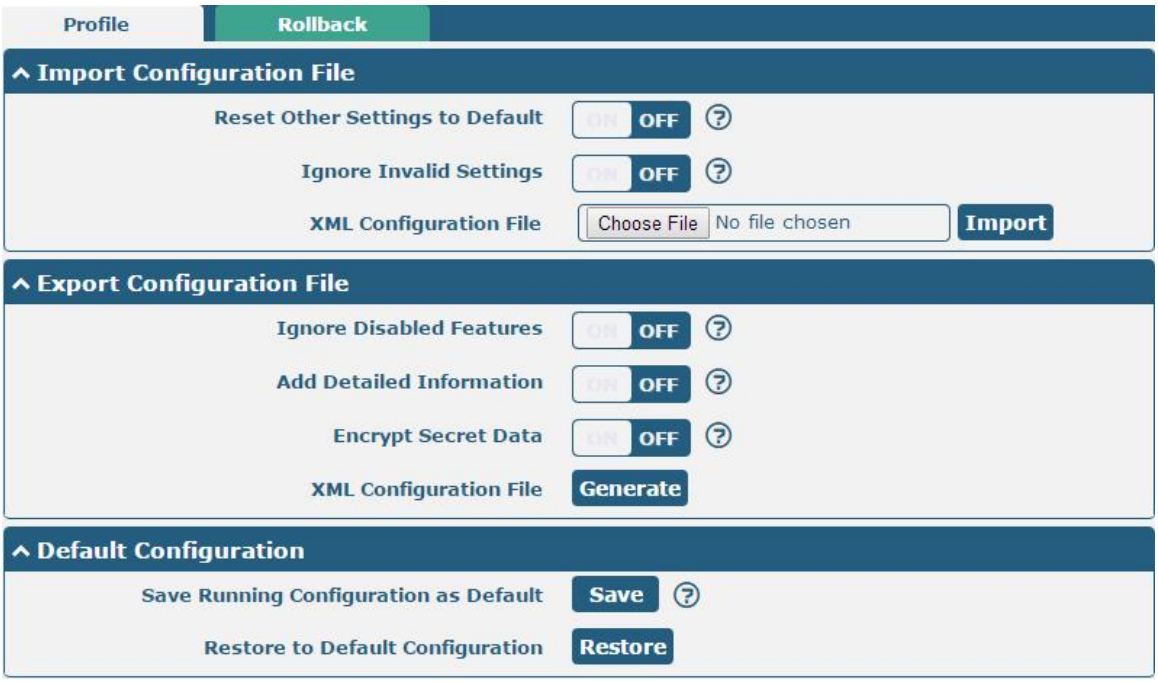
SMS command Explanation:

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 > 172.16.24.24</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

set lan network 1 interface lan0
set lan network 1 ip 172.16.24.24
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.

kone:kone;status system

In this command, username is "kone", password is "kone", and the function of the command is to get the system status.

SMS received:

hardware_version = 1.2
firmware_version = "3.0.0"
kernel_version = 4.1.0

device_model = EG9012
serial_number = 201612221052
uptime = "0 days, 00:39:31"
system_time = "Mon Feb 27 09:52:52 2017"

kone:kone;reboot
In this command, username is “kone”, password is “kone”, and the command is to reboot the Gateway.
SMS received:
OK

kone:kone;set firewall remote_ssh_access false;set firewall remote_telnet_access false
In this command, username is “kone”, password is “kone”, and the command is to disable the remote_ssh and remote_telnet access.
SMS received:
OK
OK

kone:kone; 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 “kone”, password is “kone”, and the commands is to configure the LAN parameter.
SMS received:
OK
OK
OK
OK

Chapter 5 Introductions for CLI

5.1 What Is CLI

The EG9012 command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.

Route login:

Gateway login: kone

Password: kone

#

CLI commands:

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

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

5.2 How to Configure the CLI

Following is a 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.

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
hardware_version = 1.0
firmware_version = "3.0.0"
kernel_version = 4.1.0
device_model = EG9012
serial_number = 201612221052
uptime = "0 days, 00:39:31"
system_time = "Mon Feb 27 09:52:52 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
   firmware    New firmware
# tftpupdate firmware (space+?)
   String    Firmware name
# tftpupdate firmware EG9012-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware
name
Downloading
EG9012-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 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 = 172.16.24.24
        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 172.16.99.22                  //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 4: 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
```

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using “show running ”
Set	Set *parameters*	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.

Chapter 6 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 gateways)
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
IBM	International Business Machines
ID	identification data
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
kbps	kbits per second

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

Abbr.	Description
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel Technologies Co., Ltd.
Address: 3rd Floor, Building F, Kehui Park, No.95 Daguan Road, Guangzhou, China 510660
Tel: 086-20-29019902
Email: info@robustel.com