PLANET
Networking & Communication

User's Manual

Industrial 4G LTE Cellular Gateway with 4-port 10/100TX

► ICG-2420-LTE / ICG-2420G-LTE Series

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Caution:

To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Compliance Statement

This device meets the RED directive 2014/53/EU of EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm from your body.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

PLANET ICG-2420(G)-LTE Series User's Manual

Model: ICG-2420-LTE and ICG-2420G-LTE Series

Revision: 1.0 (September, 2017)

Part No: EM-ICG-2420(G)-LTE Series_v1.0

Manufacture: PLANET Technology Corp.
Manufacture address: 10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan R.O.C.

TABLE OF CONTENTS

1. INTRODUCTION

Thank you for purchasing PLANET Industrial 4G LTE Cellular Gateway. Please refer to the table list below for the models used in Europe and the U.S.:

Model Name	4G LTE		GPS
	FDD	TDD	
ICG-2420-LTE-EU	B1/B3/B5/B7/B8/B20	B38/B40/B41	-
ICG-2420G-LTE-EU			■
ICG-2420-LTE-US	B2/B4/B12		-
ICG-2420G-LTE-US			■

"**Cellular Gateway**" is used as an alternative name in this user's manual.

1.1 Packet Contents

Open the box of the **Cellular Gateway** and carefully unpack it. The box should contain the following items:

ICG-2420-LTE/ICG-2420G-LTE	**Quick Installation Guide**
	
4G LTE Antennas (2dBi) x 2	**1.5m RJ45 UTP Cable**
	
Antenna Dust Caps	**GPS Antenna** (ICG-24240G Series)
 ICG-2420-LTE x 2 ICG-2420G-LTE x 3	

If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Description

Making Network Connection Easy with 4G LTE Cellular Gateway

PLANET ICG-2420(G)-LTE series is a reliable, secure and high-bandwidth communications industrial- grade cellular gateway for demanding mobile applications, and **M2M** (machine-to-machine) and **IoT** deployments. It features **4G LTE** (Long Term Evolution), **four Ethernet** ports (3 LAN and 1 WAN), **serial ports**, **DI** and **DO** interfaces and **VPN** technology bundled in a compact yet rugged aluminum case. It establishes a fast cellular connection between Ethernet and serial port equipped devices.

High-performance 4G LTE

The ICG-2420(G)-LTE series supports LTE 2x1 DL MIMO technology which can reach a download (DL) speed of up to **150Mbps** and an upload (UL) speed of **50Mbps**. The Cellular Gateway also supports multi-band connectivity including LTE FDD/TDD, WCDMA and GSM for a wide range of applications.

Dual SIM Design

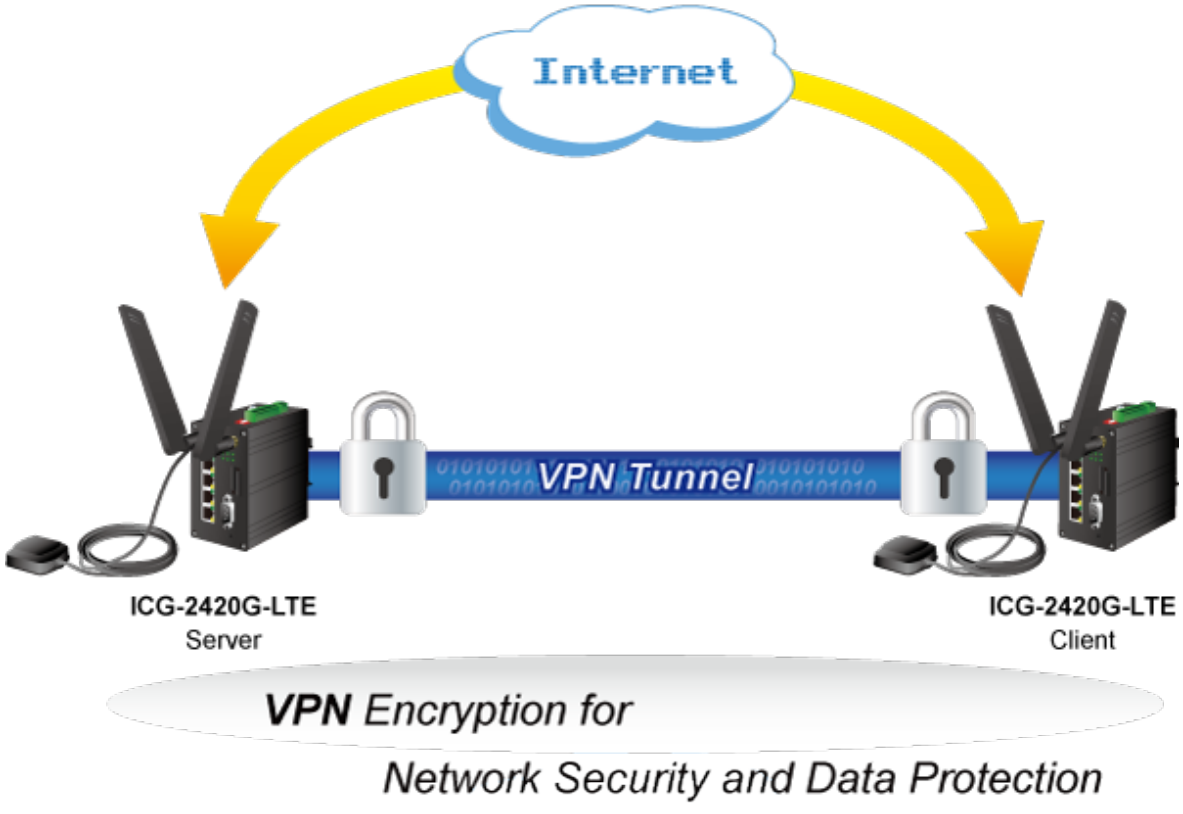
To enhance reliability, the ICG-2420(G)-LTE series is equipped with dual SIM slots that support failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications. It provides a more flexible and easier way for users to create an instant network sharing service via 4G LTE whenever in public places like transportation, outdoor event, etc.

GPS Included (For ICG-2420G-LTE)

The ICG-2420G-LTE is equipped with one convenient feature and that is GPS (Global Positioning System). It is a positioning system based on a network of satellites that continuously transmit necessary data. More signals transmitted from more satellites can triangulate its location on the ground, meaning any location can be easily tracked anytime.

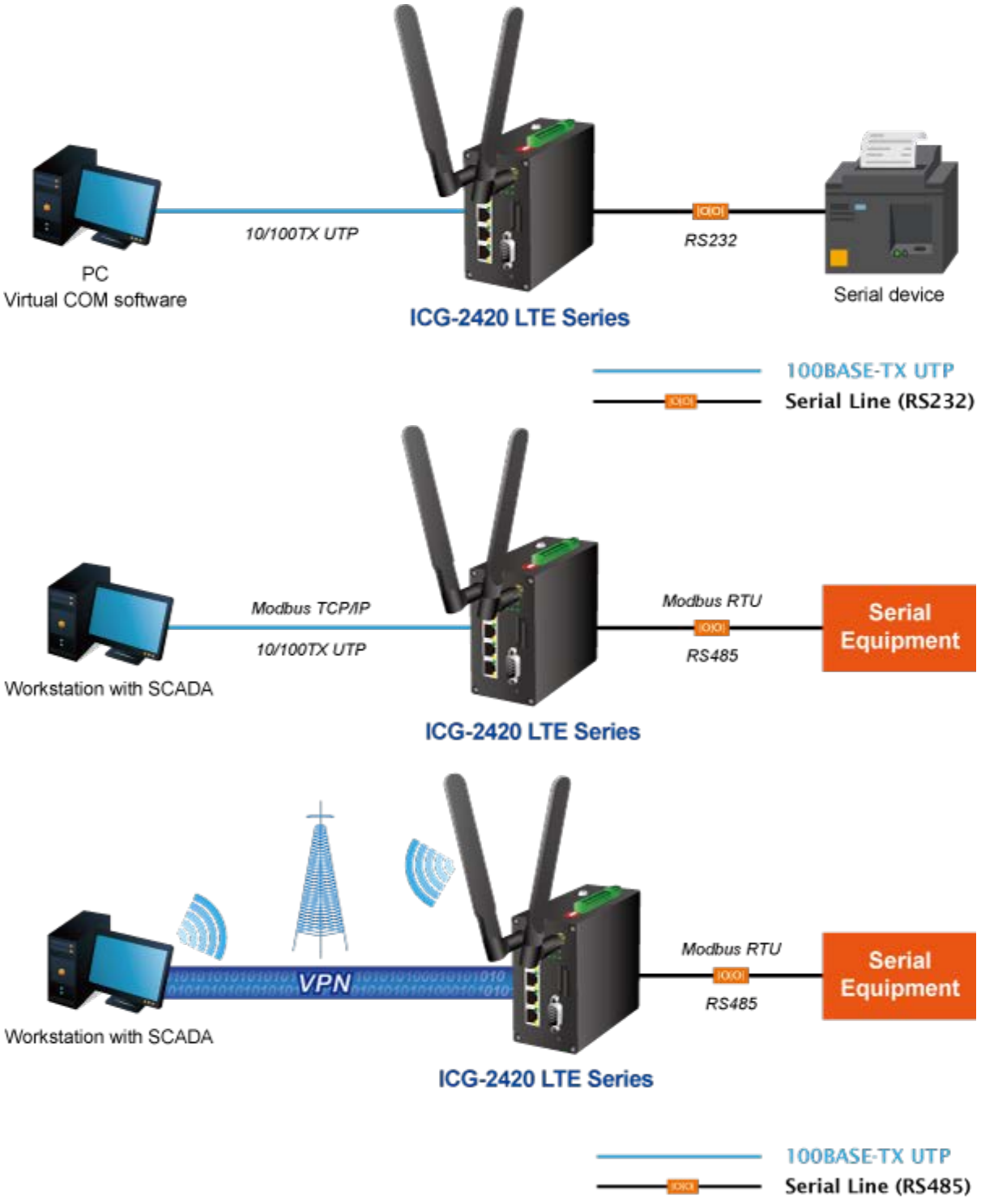
Cost-effective VPN Solution

The ICG-2420(G)-LTE series provides a complete data security and privacy feature for access and exchange of sensitive data. The full VPN capability of the ICG-2420(G)-LTE series including built-in **OpenVPN** and **IPSec VPN** functions with DES/3DES/AES encryption and MD5/SHA-1 authentication makes the shared connection more secure and flexible. The IPSec VPN also makes the private tunnel over Internet more secure for enterprises doing business transactions.



Remote Manageable Solution for Ethernet to RS232/RS485 Applications

PLANET ICG-2420(G)-LTE series' serial RS232/RS485 interface can be converted over the Fast Ethernet networking. It can operate as a virtual server or client where IP-based serial equipment can be managed. The ICG-2420(G)-LTE series helps save the network administrator's valuable time in detecting and locating network problems, rather than visual inspection of cabling and equipment.



Superior Management Functions

For networking management features, the ICG-2420(G)-LTE series provides such functions as DHCP server, DMZ and Port Forwarding, as well as full secure functions including Network Address Translation (NAT), and IP/URL/MAC filtering. The ICG-2420(G)-LTE series has 4G and WAN connection failover characteristics, which can automatically switch over to the redundant, stable WAN connection to keep users always online without missing any fascinating moments.

User-friendly and Secure Management

For efficient management, the ICG-2420(G)-LTE series is equipped with console, web and SNMP management interfaces. With the built-in web-based management interface, the ICG-2420(G)-LTE series offers an easy-to-use, platform independent management and configuration facility. The ICG-2420(G)-LTE series supports SNMP and it can be managed via any management software based on the standard SNMP v1 or v2 Protocol. Moreover, the ICG-2420(G)-LTE series offers the remotely secure management by supporting **SSHv2** and **SNMP v3** connection where the packet content can be encrypted at each session.

IPv6/IPv4 Dual Stack Capability

The ICG-2420(G)-LTE series supports both IPv4 and IPv6 Protocols. As more network devices are growing and the needs for larger addressing and higher security become critical, the ICG-2420(G)-LTE series is the best solution for applications of 4G LTE and serial communication to connect with the IPv6 network

1.3 How to Use This Manual

This User Manual is structured as follows:

Section 2, INSTALLATION

The section explains the functions of the Cellular Gateway and how to physically install the Cellular Gateway.

Section 3, CELLULAR GATEWAY MANAGEMENT

The section contains the information about the software function of the Cellular Gateway.

Section 4, WEB CONFIGURATION

The section explains how to manage the Cellular Gateway by Web interface.

Section 5, CELLULAR GATEWAY OPERATION

The chapter explains how to do the Cellular Gateway operation of the Cellular Gateway.

Section 6, TROUBLESHOOTING

The chapter explains how to troubleshoot the Cellular Gateway.

Appendix A

The section contains cable information of the Cellular Gateway.

1.4 Product Features

- **Physical Port**
  - **3 10/100BASE-TX** RJ45 LAN ports, auto-negotiation, auto MDI/MDI-X
  - **1 10/100BASE-TX** RJ45 WAN port, auto-negotiation, auto MDI/MDI-X
  - **2** 4G LTE 2dBi antennas
  - **2** SIM card slots
  - **1 GPS** antenna (ICG-2420G-LTE Series)
  - 3 console interfaces (2 RS232 and 1 RS485)
    - COM1 (RS232 for management and setup
    - COM2 (RS232 for remote serial device)
    - COM3 (RS485 for remote serial device)
  - One DIP switch to improve the communication of RS485 networks

- **Cellular Interfaces**
  - Supports multi-band connectivity with FDD LTE/ TDD LTE/ WCDMA/ GSM/ LTE Cat4
  - Built-in dual SIM for network redundancy
  - Two detachable antennas for protection against radio interference
  - LED indicators for connection and data transmission status

- **Industrial Case and Installation**
  - IP40 aluminum case
  - DIN-rail design
  - Power requirement: 10~32V DC
  - Supports EFT protection for 2000V DC power and 6000V DC Ethernet ESD protection
  - -20 to 70 degrees C operating temperature

- **Digital Input and Digital Output (Alarm)**
  - 2 digital input (DI)
  - 1 digital output (alarm)
  - Integrates sensors into auto alarm system
  - Transfers alarm via SNMP trap

- **Advanced Features**
  - Supports demilitarized zone (DMZ).
  - Supports OpenVPN
  - Supports IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256)
  - Supports Modbus TCP (Only functions with COM3 RS485)
  - Supports Port Forwarding
  - Supports Dynamic DNS and PLANET DDNS
  - Supports WAN connection types: DHCP client, static IP and PPPoE client
  - Secures network connection
    - IP filter
    - URL filter
    - MAC filter

➢ **Management**

- IPv4 and IPv6 dual stack management
- Cellular Gateway management interfaces
  - Console/Telnet Command Line interface
  - Web management
  - SNMP v1, v2c, and v3
  - SSHv2 secure access
- **IPv6** IP address/DNS management
- System Maintenance
  - Firmware upload via HTTP
  - Reset button for system reboot or reset to factory default
  - Dual images
- SNTP (Simple Network Time Protocol)
- TR069
- System log
- Remote system log
- SNMP trap for interface Link Up and Link Down notification
- Configuration backup and restore

1.5 Product Specifications

Product	ICG-2420-LTE	ICG-2420G-LTE
Hardware Specifications		
Copper Ports	3 LAN 10/100BASE-TX RJ45 auto-MDI/MDI-X ports 1 WAN 10/100BASE-TX RJ45 auto-MDI/MDI-X port	
Serial Interface	3 serial interfaces (2 RS232 and 1 RS485) COM1 (RS232 for management and setup) (115200, N, 8, 1) COM2 (RS232 TXD/RXD for remote serial device) COM3 (RS485 D+/D- for remote serial device)	
SIM Interface	2 SIM card slots with mini SIM card tray	
Cellular Antenna	2 2dBi external antennas with SMA connectors for LTE	
GPS Antenna	-	1 28dB gain external antennas with SMA connectors - 2m
DI & DO Interfaces	■ 2 Digital Input (DI): Level 0: 0V~3V (±0.1V) Level 1: 10V~30V (±0.1V) ■ 1 Digital Output (alarm): Open collector to 50V DC, 500mA (max.)	
Connector	Removable 3-pin terminal block for power input Removable 11-pin terminal block for DI/DO and serial interface	
Switch Architecture	Store-and-Forward	
Address Table	1K entries, automatic source address learning and aging	
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex	
Reset Button	< 5 sec: System reboot > 10 sec: Factory default	
Surge Protection	2KV DC	
ESD Protection	6KV DC	
Enclosure	IP40 aluminum case	
Installation	DIN rail kit	
LED	System: SYS (Green) Ethernet Interfaces (Port1-3 and WAN Port): LNK/ACT (Green) 100 (Orange) 10 (off) LTE SIM and Signal : VPN (Green) SIM1 and SIM2 (Green) Cellular signal: High and low (Green)	
Dimensions (W x D x H)	60 x 106 x 110 mm	

Weight	452g	457g
Power Requirements – DC	10~32V DC, 1A	
Power Consumption	7 watts/24 BTU	
Multi Band Supports		
EU Model	■ FDD LTE B1/B3/B5/B7/B8/B20 (2100/1800/850/2600/900/800) ■ TDD LTE B38/B40/B41 (2600/2300/2500) ■ WCDMA B1/B5/B8 (2100/850/900) ■ GSM/EDGE B3/B8 (1800/900)	
US Model	■ FDD LTE B2/B4/B12 (1900/AWS1700/700) ■ WCDMA B2/B4/B5 (1900/AWS1700/850)	
LTE Data Rate	20MHz bandwidth: 150Mbps (DL), 50Mbps (UL)	
Advanced Functions		
VPN	Tunnel Number ■ OpenVPN: 10 ■ IPSec 12: IPSec: Encryption Algorithm: 3DES/AES128/AES196/AES256 Integrity Algorithm: MD5/SHA1/SHA256	
WAN Connection Types	DHCP Client Static IP PPPoE Client	
Secure Network	IP filter URL filter MAC filter	
Others	Supports demilitarized zone (DMZ) Supports Modbus TCP (only functions with COM3 RS485) Supports Port Forwarding Supports Dynamic DNS and PLANET DDNS	
Management		
Basic Management Interfaces	Console; Telnet; Web browser; SNMP v1, v2c, TR069	
Secure Management Interfaces	SSHv2, SNMP v3	
SNMP MIBs	RFC 1213 MIB-II RFC 1643 Ethernet MIB RFC 2665 Ether-Like MIB RFC 4293 IP MIB	
Standards Conformance		
Regulatory Compliance	FCC Part 15 Class A, CE	
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3x flow control and back pressure	

	RFC 768 UDP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP
Environment	
Operating	Temperature: -20 ~ 70 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
Storage	Temperature: -40 ~ 85 degrees C Relative Humidity: 5 ~ 95% (non-condensing)

2. INSTALLATION

This section describes the hardware features and installation of the Industrial Cellular Gateway on the desktop or mounting. For easier management and control of the Industrial Cellular Gateway, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Industrial Cellular Gateway, please read this chapter completely.

2.1 Hardware Description

2.1.1 Cellular Gateway Front Panel

The front panel provides the monitoring of the Cellular Gateway's simple interfaces. Figure 2-1 & 2-2 shows the front panel of the Industrial Cellular Gateway.

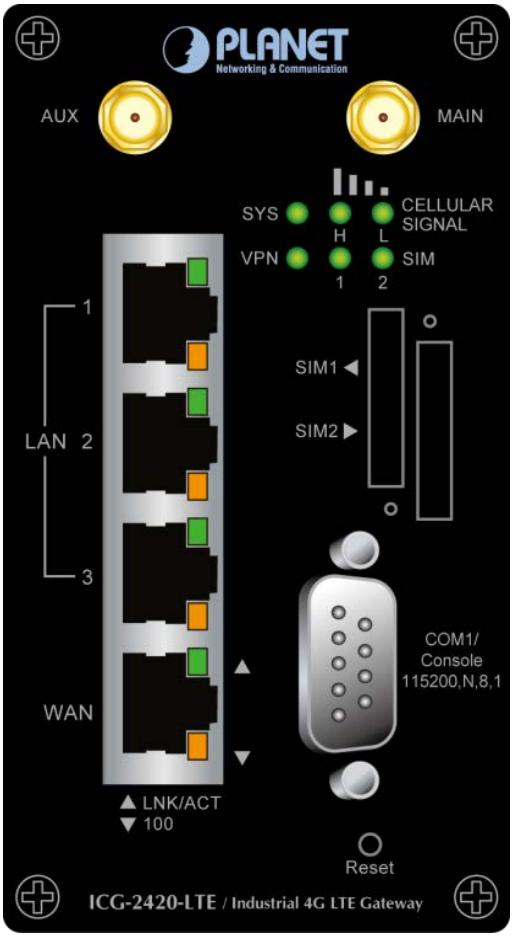


Figure 2-1 ICG-2420-LTE Front Panel

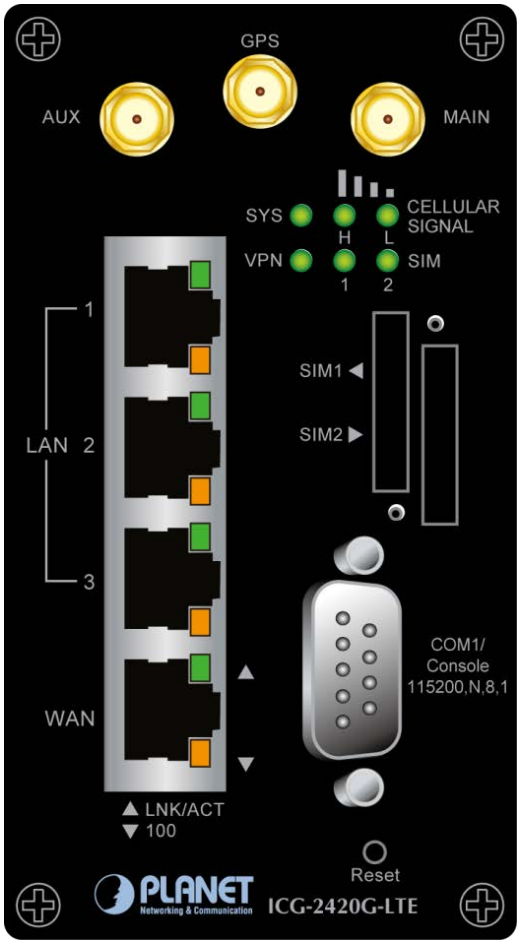


Figure 2-2 ICG-2420G-LTE Front Panel

■ **Reset Button**

On the front of the ICG-2420(G)-LTE series, the reset button is designed to reboot the Industrial Cellular Gateway without turning off and on the power. The following is the summary table of the reset button functions:

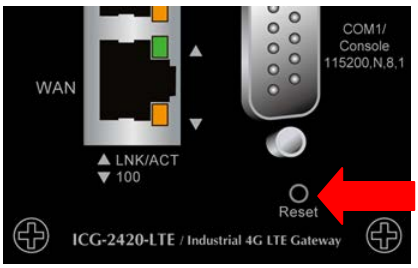


Figure 2-3 Rest Button of ICG-2420(G)-LTE Series

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Industrial Cellular Gateway.
> 10 sec: Factory Default	Reset the Industrial Cellular Gateway to Factory Default configuration. Industrial Cellular Gateway will then reboot and load the default settings shown below: ◦ Default username: **admin** ◦ Default password: **admin** ◦ Default IP address: **192.168.1.1** ◦ Subnet mask: **255.255.255.0**

2.1.2 LED Indications

The front panel LEDs indicate instant status of port links, data activity and system power; it helps monitor and troubleshoot when needed.

■ **System**

LED	Color	Function	
SYS	**Green**	**Lights**	Indicates the system is working on properly.
		Slow Blinking	Indicates the system is booting.
		Off	Indicates the system is down.
VPN	**Green**	**Lights**	Indicates the VPN is connected.
		Slow Blinking	Indicates the WAN is connected.
		Off	Indicates the WAN is not connected.
Cellular Signal (L)	**Green**	**Lights**	Indicates the signal is low.
Cellular Signal (H)	**Green**	**Lights**	Indicates the signal is normal or high.
SIM1 & 2	**Green**	**Lights**	Indicates SIM1 or SIM2 is connecting successfully.
		Slow Blinking	Indicates SIM1 or SIM2 is trying to connect.
		Fast Blinking	Indicates SIM1 or SIM2 fails to connect or no SIM card inserted.

■ **10/100BASE-TX LAN Port Interfaces (Port-1 to Port-3)**

LED	Color	Function	
Ethernet	Green	Lights	Indicates that the link is successfully established.
		Blinking	Indicates that the port is actively sending or receiving data.
	Orange	Lights	Indicates that the port is operating at 100Mbps.
		Off	Indicates that the port is operating at 10Mbps.

■ **10/100BASE-TX WAN Port Interfaces**

LED	Color	Function	
Ethernet	Green	Lights	Indicates that the link is successfully established.
		Blinking	Indicates that the port is actively sending or receiving data.
	Orange	Lights	Indicates that the port is operating at 100Mbps.
		Off	Indicates that the port is operating at 10Mbps.

2.1.3 Cellular Gateway Upper Panel

The upper panel of the Industrial Cellular Gateway consists of two terminal block connectors. Figure 2-4 shows the upper panel of the Cellular Gateway.

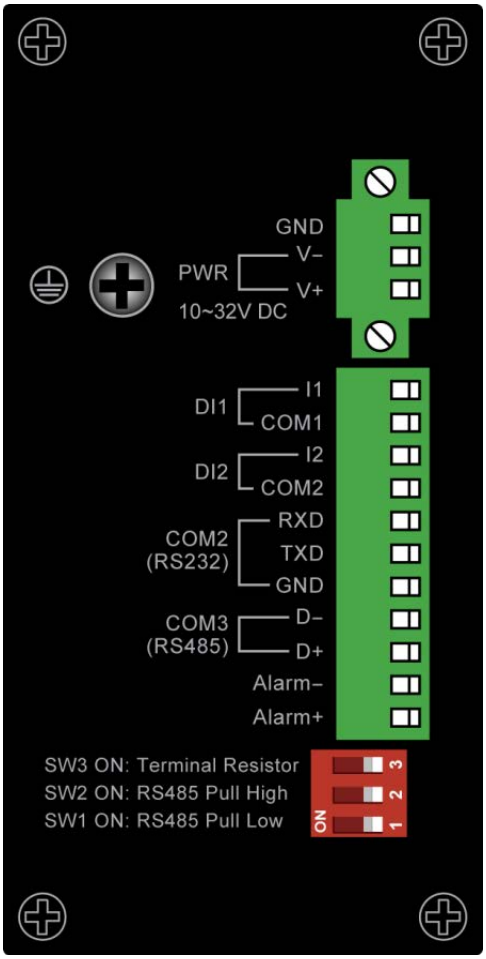


Figure 2-4: ICG-2420(G)-LTE Series Upper Panel

2.1.4 Wiring the Power Inputs

The 3-contact terminal block connector on the top panel of Industrial Cellular Gateway is used for one DC power input. The power input range is from 10 to 32V DC. Please follow the steps below to insert the power wire.

1. Please read the above description of upper panel carefully before inserting positive/negative DC power wires into the 3-contact terminal block connector.

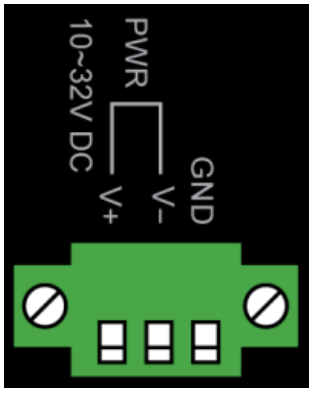


Figure 2-5: Wiring the Power Inputs

2. Tighten the wire-clamp screws for preventing the wires from loosening.

2.1.5 Wiring the Digital Input/Output (Alarm)

The 11-contact terminal block connector on the top panel of ICG-2420(G)-LTE Series is used for Digital Input and Digital Output (Alarm). Please follow the steps below to insert wire.

1. The ICG-2420(G)-LTE Series offers two DI sets and one DO set.

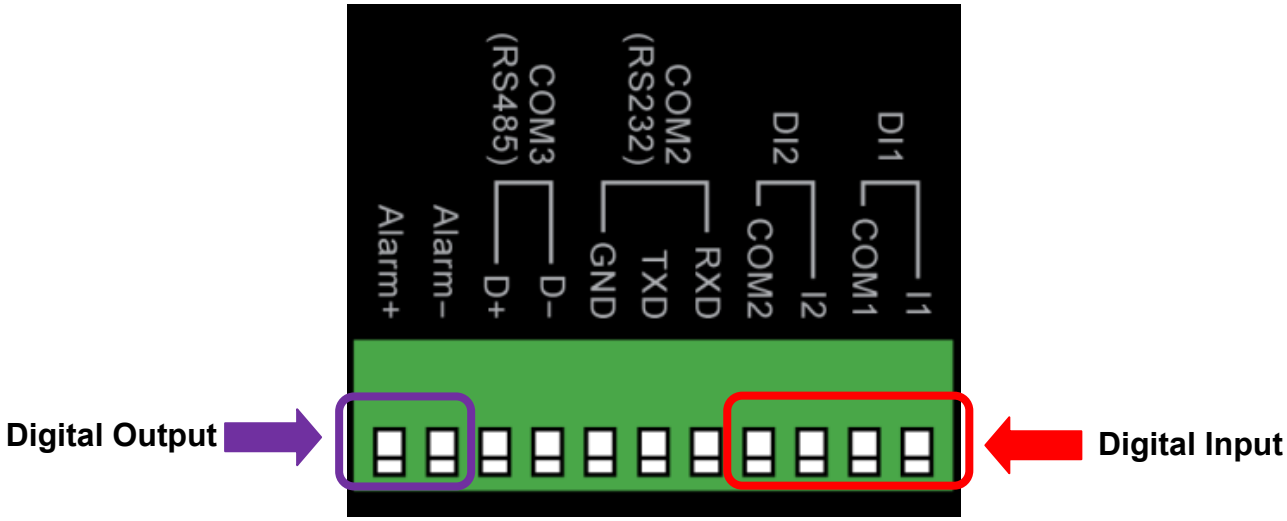


Figure 2-6 Wiring the DI/DO Inputs

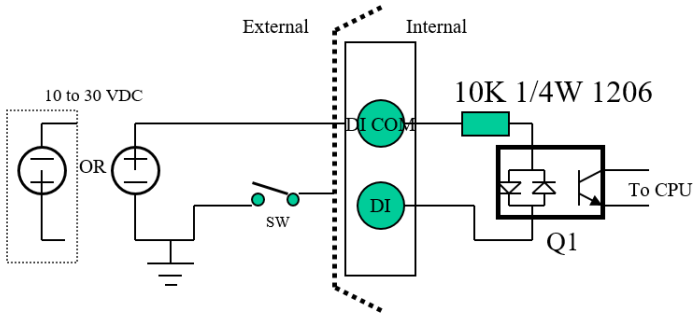
2. Tighten the wire-clamp screws for preventing the wires from loosening.

3. There are two Digital Input sets for you to monitor two different devices.

4. There is one Digital Output set (Alarm) for you to sense ICG-2420(G)-LTE Series VPN/WAN disconnection or issue a high or low signal to external device.

(1) Digital Input DI1 & DI2

Note: Q1 is a b-idirectional component.



Wet Contact

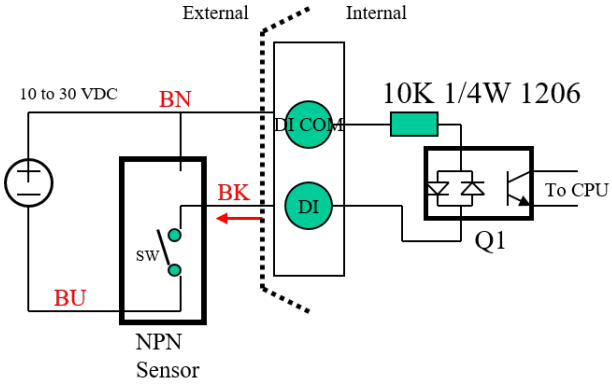
- Logic Level 1 : 10 to 30 VDC (Q1 On)
- Logic Level 0 : 0 to 3 VDC (Q1 Off)

Digital Input

- Wet Contact (Level from DI to DI COM)
  - Logic Level 1 : 10 to 30 VDC (Q1 on)
  - Logic Level 0 : 0 to 3 VDC (Q1 off)
- Wet Contact (Alarm trigger*):
  - Alarm ON* : Q1 On (SW Close)
  - Alarm Off* : Q1 off (SW Open)

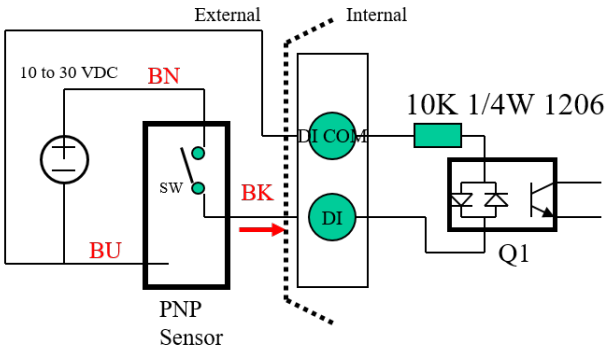
* Refer to the Alarm function on web management

* Q1 is bi-directional part



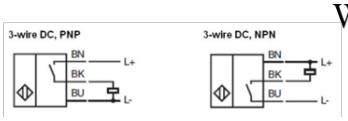
Wet Contact

- Alarm trigger* : Q1 turn on
- Alarm un-trigger* : Q1 turn off



Wet Contact

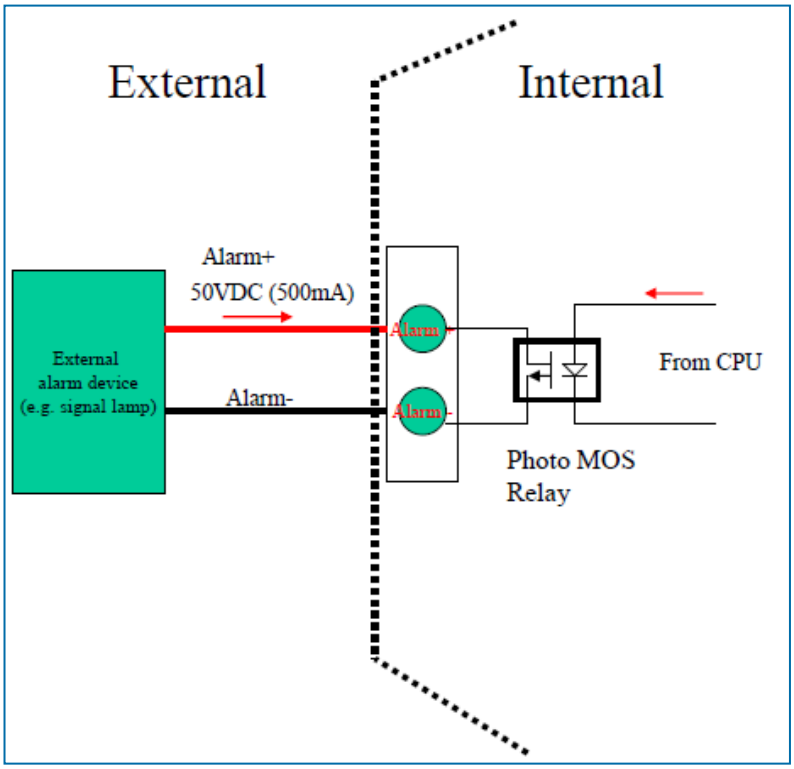
- Alarm trigger* : Q1 turn on
- Alarm un-trigger* : Q1 turn off



(2) Digital Output – Alarm Contacts

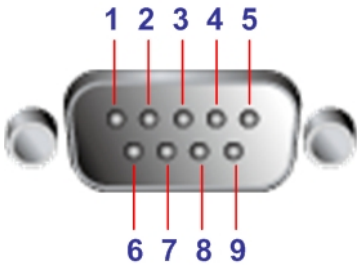
Relay output with current capacity of 500mA/50VDC (maximum).

Pin	Description
Alarm -	Alarm negative signal output
Alarm +	Alarm positive signal output



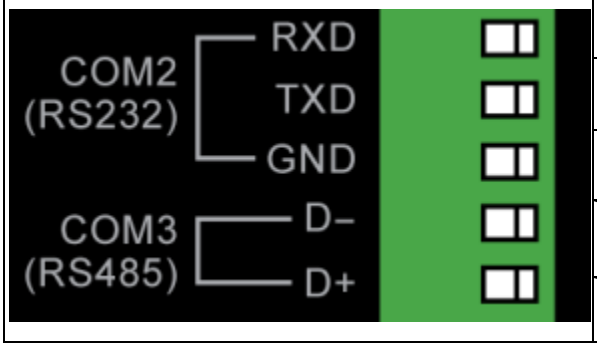
2.1.6 DB9 and Terminal Block Pin Define

◆ **COM1** Pin Define:



DB9-PIN	RS-232
1	NA
2	RXD
3	TXD
4	NA
5	GND
6	NA
7	RTS
8	CTS
9	NA

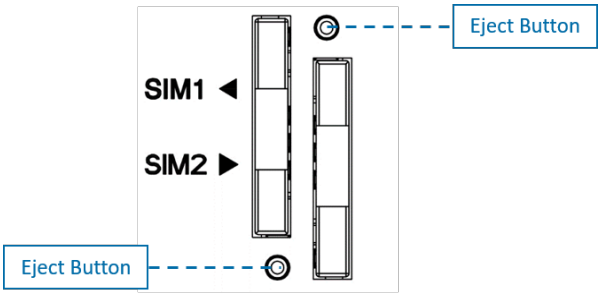
◆ **COM2**(**RS232**) and **COM3**(**RS485**) Pin Define:



3-wire for RS232 (COM2)	2-wire for RS485 (COM3)
RXD	
TXD	
GND	
	Data B(-)
	Data A(+)

2.1.7 Dual SIM Cards Installation

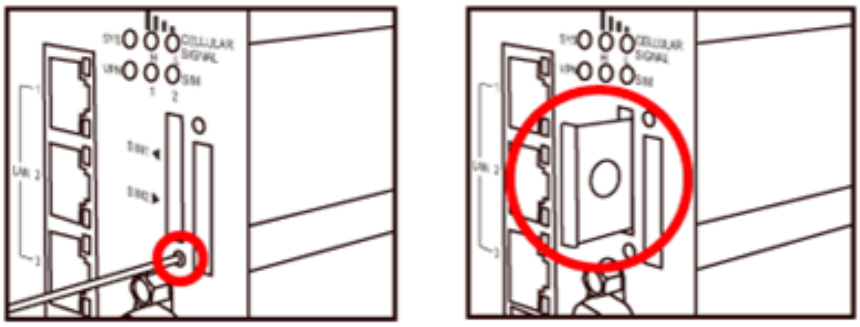
1. SIM1/SIM2 Card Drawers and Eject Buttons



2. Insert and Remove SIM1/SIM2 Card

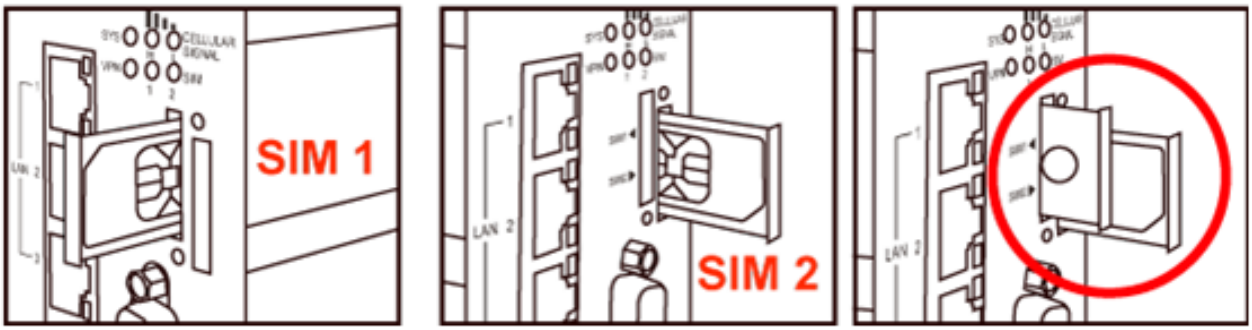
(1) Before inserting or removing the SIM card, ensure that the power has been turned off and the power connector has been removed from Cellular Gateway.

(2) Press the button with a paper clip or suitable tool to eject the SIM card from the drawer.



(3) Insert the SIM card with the contacts facing up and align it properly into the drawer. Make sure your direction of SIM Card and put it into the tray.

(4) Slide the drawer back and locks it in place.



Note

Please make sure the direction first. When pulling into the SIM tray without putting the correct direction, the tray will be stuck inside.

Please turn off Cellular Gateway before taking the SIM card.

2.1.8 DIP Switch

A built-in 120 ohm terminal resistor can be activated by DIP switch. Pull High or Pull Low resistor adjustments are also available. It improves the communication on RS485 networks for a specific application.

	Description
	Switch 1 and 2 set the pull high/low resistor Switch 3 enables or disables the terminal resistor

Pull High (510 ohm) / Pull Low (510 ohm) Bias Resistor	SW 1 (Pull Low)	SW 2 (Pull High)
Enable	ON	ON
Disable (Default)	OFF	OFF

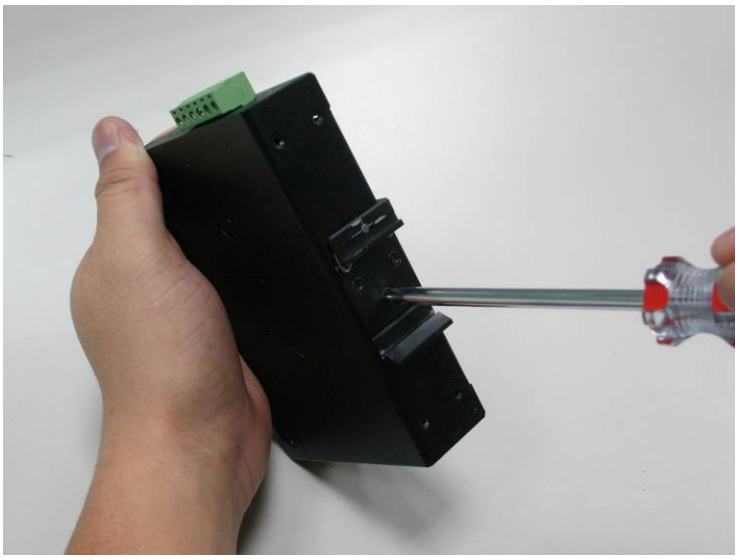
Terminal Resistor (120 ohm)	SW 3
Enable	ON
Disable (Default)	OFF

2.2 Mounting Installation

This section describes how to install your Industrial Cellular Gateway and make connections to the Industrial Cellular Gateway. Please read the following topics and perform the procedures in the order being presented. To install your Industrial Cellular Gateway on a desktop or shelf, simply complete the following steps.

2.2.1 DIN-rail Mounting

The DIN-rail is screwed on the Industrial Cellular Gateway when out of factory. Please refer to the following figures to screw the DIN-rail on the Industrial Cellular Gateway. To hang the Industrial Cellular Gateway, follow the steps below:



Step 1: Screw the DIN-rail on the Industrial Cellular Gateway.

Step 2: Place the bottom of DIN-rail lightly into the track.

Step 3: Check whether the DIN-rail is tightly on the track.

Step 4: Please refer to the following procedures to remove the Industrial Cellular Gateway from the track.

Step 5: Lightly pull out the bottom of DIN-rail to remove it from the track.

3. CELLULAR GATEWAY MANAGEMENT

This chapter explains the methods that you can use to configure management access to the Industrial Cellular Gateway. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Web Management Access
- SNMP Access
- Standards, Protocols and Related Reading

3.1 Requirements

- **Workstations** running Windows 2000/XP, 2003, Vista/7/8, 2008, MAC OS9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols.
- **Workstation** is installed with **Ethernet NIC** (Network Interface Card).
- Ethernet Port connection
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- The above Workstation is installed with **Web browser** and **Java runtime environment** plug-in.

It is recommended to use Internet Explore 8.0 or above to access Industrial Cellular Gateway.

3.2 Management Access Overview

The Industrial Cellular Gateway gives you the flexibility to access and manage it using any or all of the following methods:

- **Web browser** interface
- An external **SNMP-based network management application**

The Web browser interfaces are embedded in the Industrial Cellular Gateway software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the two management methods.

Method	Advantages	Disadvantages
Web Browser	• Ideal for configuring the Cellular Gateway remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need to only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with Cellular Gateway functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need to only know the community name)

Table 3-1 Comparison of Management Methods

3.3 Web Management

The Industrial Cellular Gateway offers management features that allow users to manage the Industrial Cellular Gateway from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After you set up your IP address for the cellular gateway, you can access the Industrial Cellular Gateway's Web interface applications directly in your Web browser by entering the IP address of the Industrial Cellular Gateway.

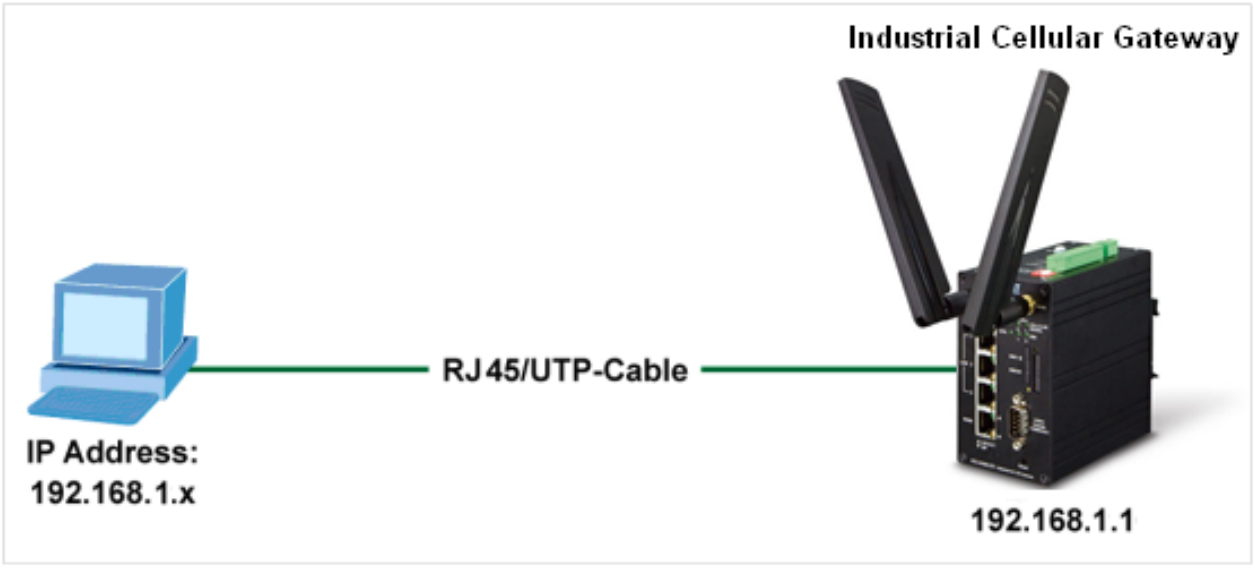


Figure 3-1-1 Web Management

You can then use your Web browser to list and manage the Industrial Cellular Gateway configuration parameters from one central location. Web Management requires either **Microsoft Internet Explorer 8.0** or later, **Google Chrome**, **Safari** or **Mozilla Firefox 1.5** or later.

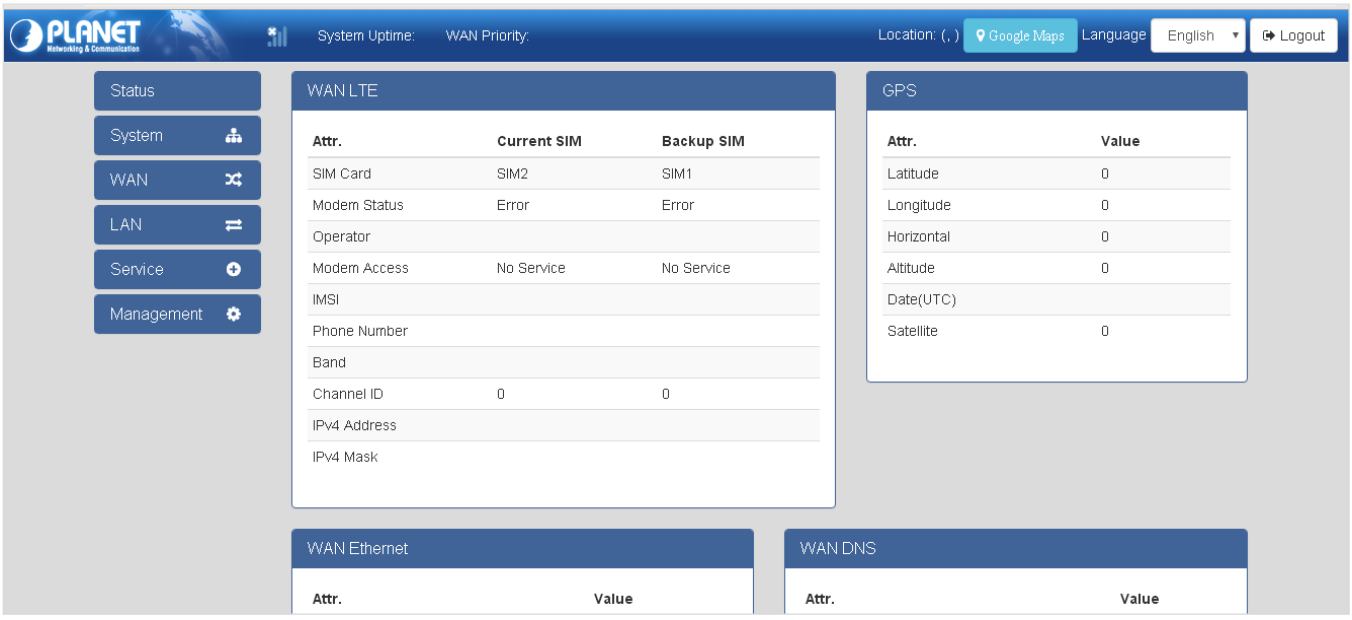


Figure 3-1-4 Web Main Screen of Industrial Cellular Gateway

3.4 SNMP-based Network Management

You can use an external SNMP-based application to configure and manage the Industrial Cellular Gateway, such as SNMPc Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the cellular gateway and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default get and set community strings for the Industrial Cellular Gateway are public.

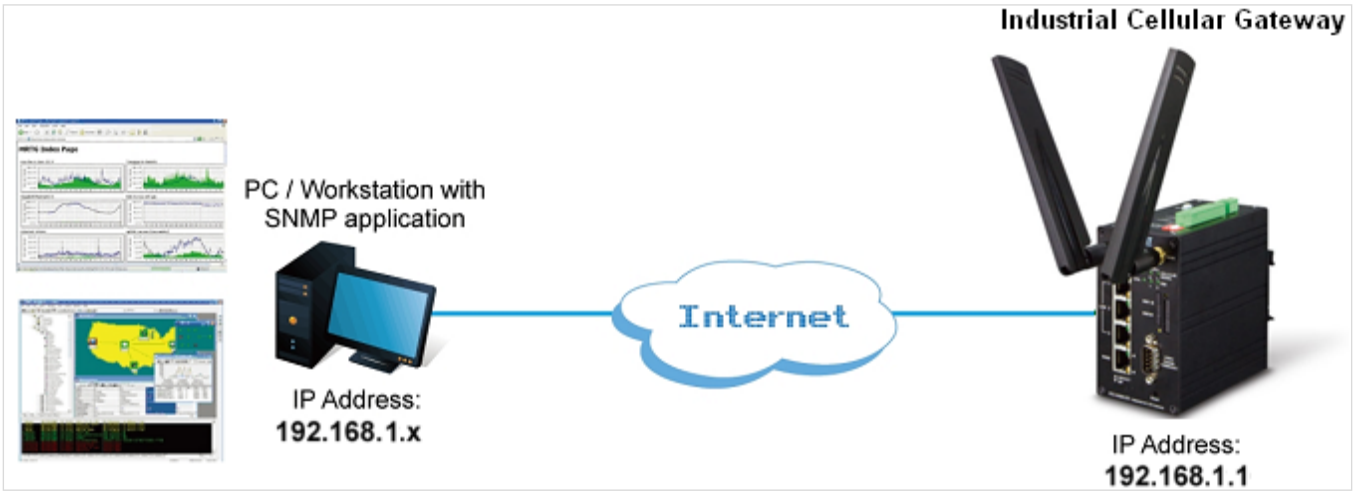


Figure 3-1-5 SNMP Management

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management.

About Web-based Management

The Industrial Cellular Gateway offers management features that allow users to manage the Industrial Cellular Gateway from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-based Management supports Internet Explorer 8.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note

By default, IE8.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Industrial Cellular Gateway can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address as the Industrial Cellular Gateway.

For example, the default IP address of the Industrial Cellular Gateway is ***192.168.1.1***, then the manager PC should be set to **192.168.1.x** (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Industrial Cellular Gateway to 192.168.2.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set to 192.168.2.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

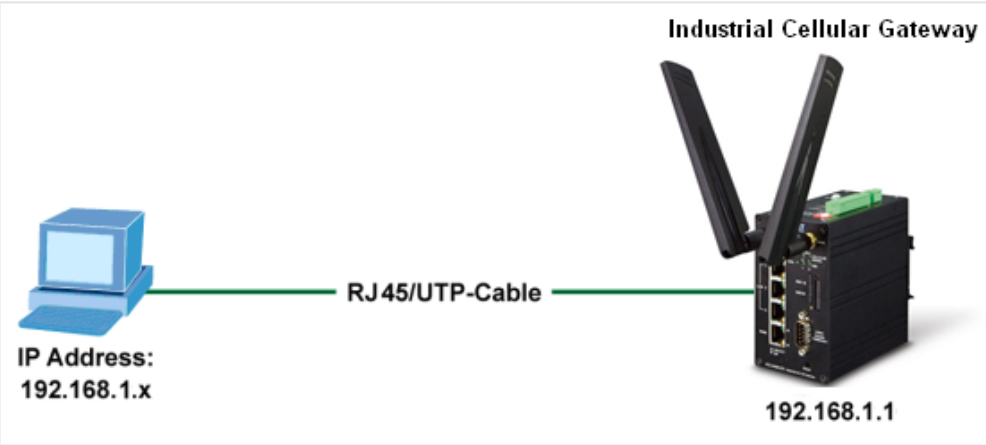


Figure 4-1-1 Web Management

- **Logging on to the Cellular Gateway**

1. Use Internet Explorer 8.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP address is as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username and password you have changed via console) to login the main screen of Industrial Cellular Gateway. The login screen in Figure 4-1-2 appears.

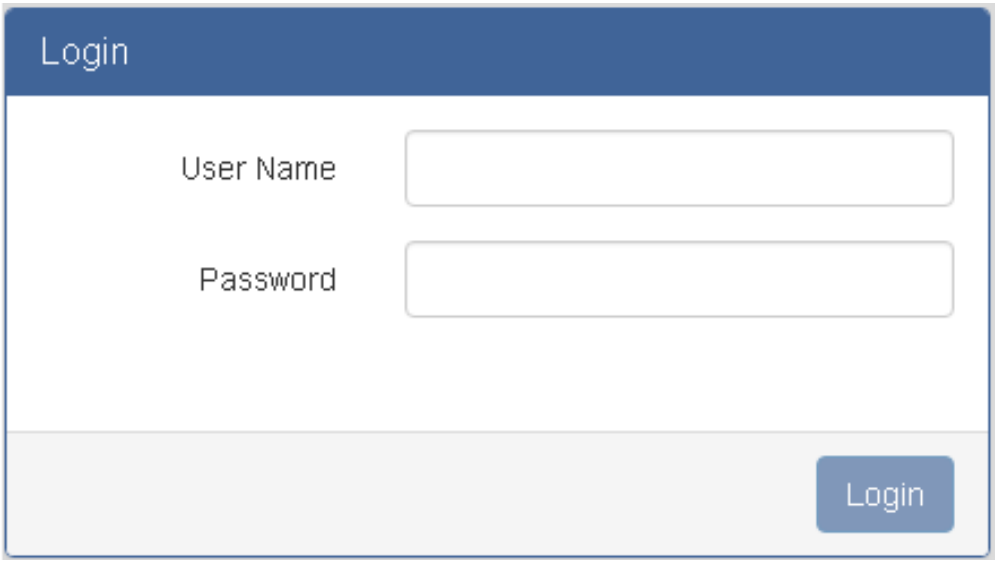


Figure 4-1-2 Login screen

Default User Name: **admin**
Default Password: **admin**

After entering the username and password, the main screen appears as Figure 4-1-3.

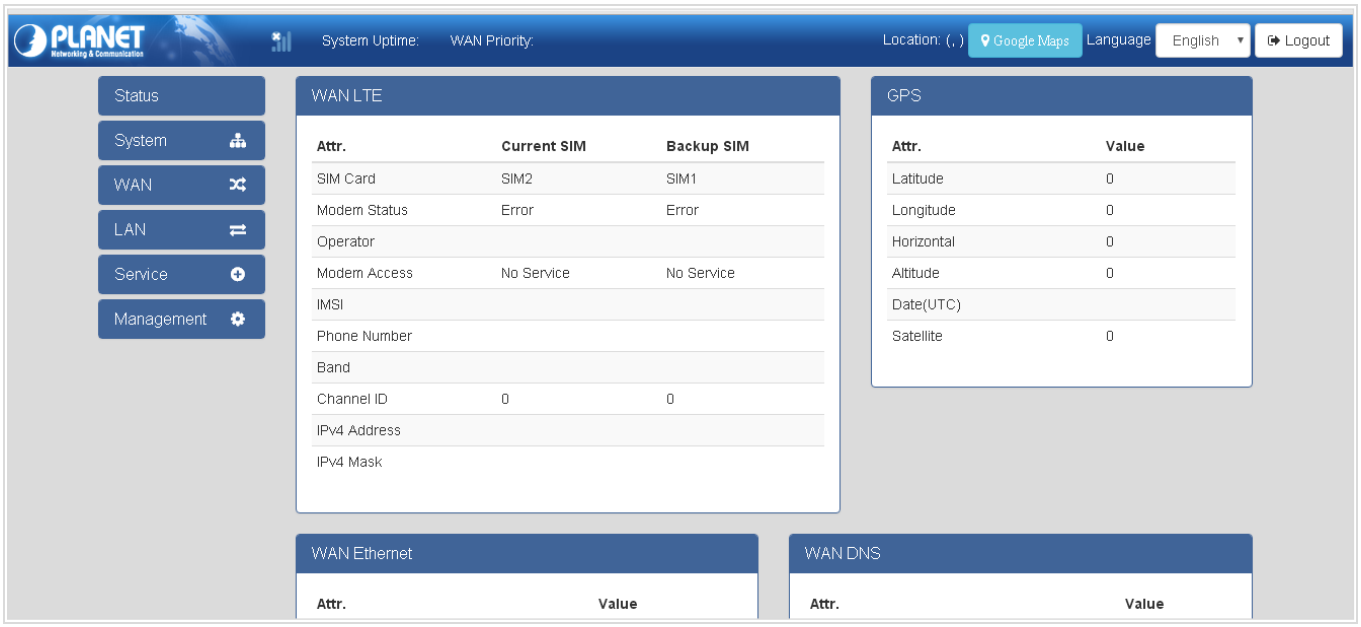


Figure 4-1-3 Default Main Page

Now, you can use the Web management interface to continue the cellular gateway management or manage the Industrial Cellular Gateway by Web interface. The Cellular Gateway Menu on the left of the web page lets you access all the commands and statistics the Industrial Cellular Gateway provides.

It is recommended to use Internet Explore 8.0 or above to access Industrial Cellular Gateway.

For security reason, please change and memorize the new password after this first setup. Only accept command in lowercase letter under Web interface.

4.1 Main Web Page

The Industrial Cellular Gateway provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Industrial Cellular Gateway using the Web browser of your choice. This chapter describes how to use the Industrial Cellular Gateway's Web browser interface to configure and manage it.

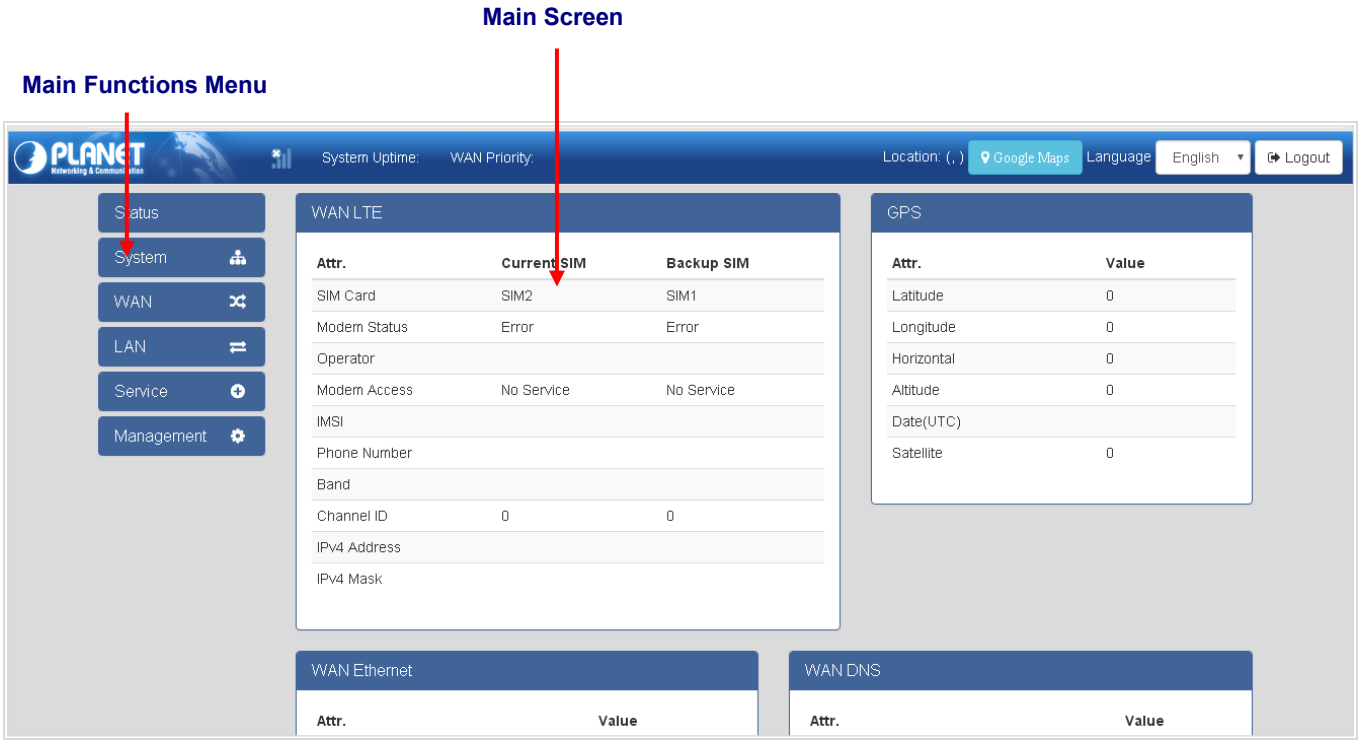


Figure 4-1-4 Main Page

Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the Industrial Cellular Gateway, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Industrial Cellular Gateway by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

Figure 4-1-5 Industrial Cellular Gateway Main Functions Menu

Buttons

: Click to log out the Industrial Cellular Gateway.

: Click to display the current location from the Google Maps

4.1.1 GPS Button

This GPS button allows you to know the cellular gateway's current position. The Latitude and longitude will also show on the right-top banner of web interface. The screen in Figure 4-1-6 appears.

Figure 4-1-6 GPS Button Screenshot

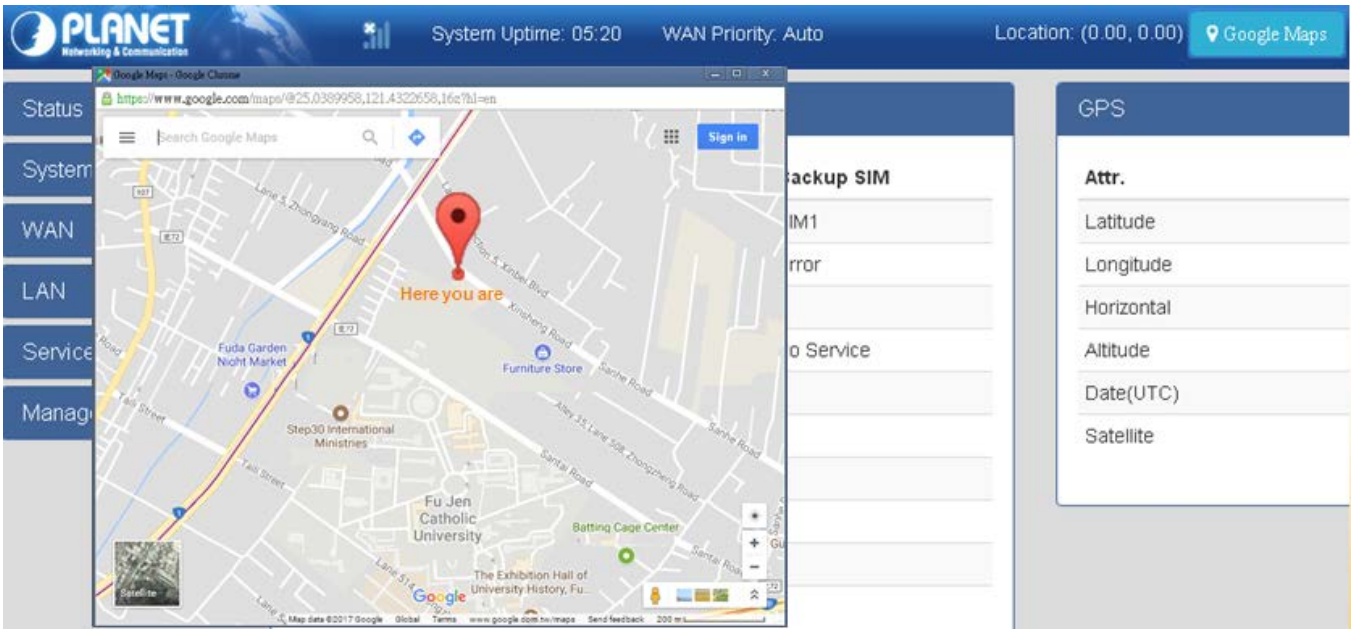


Figure 4-1-7 GPS Google Map Screenshot

4.2 Status

When you enter the web browser in the beginning, the interface displays the status of cellular gateway to make you know about Cellular Attribute, Dual SIM information, the current connectivity of WAN Ethernet and LAN Ethernet. If the cellular gateway with GPS function, The screens in Figure 4-2-1 appear.

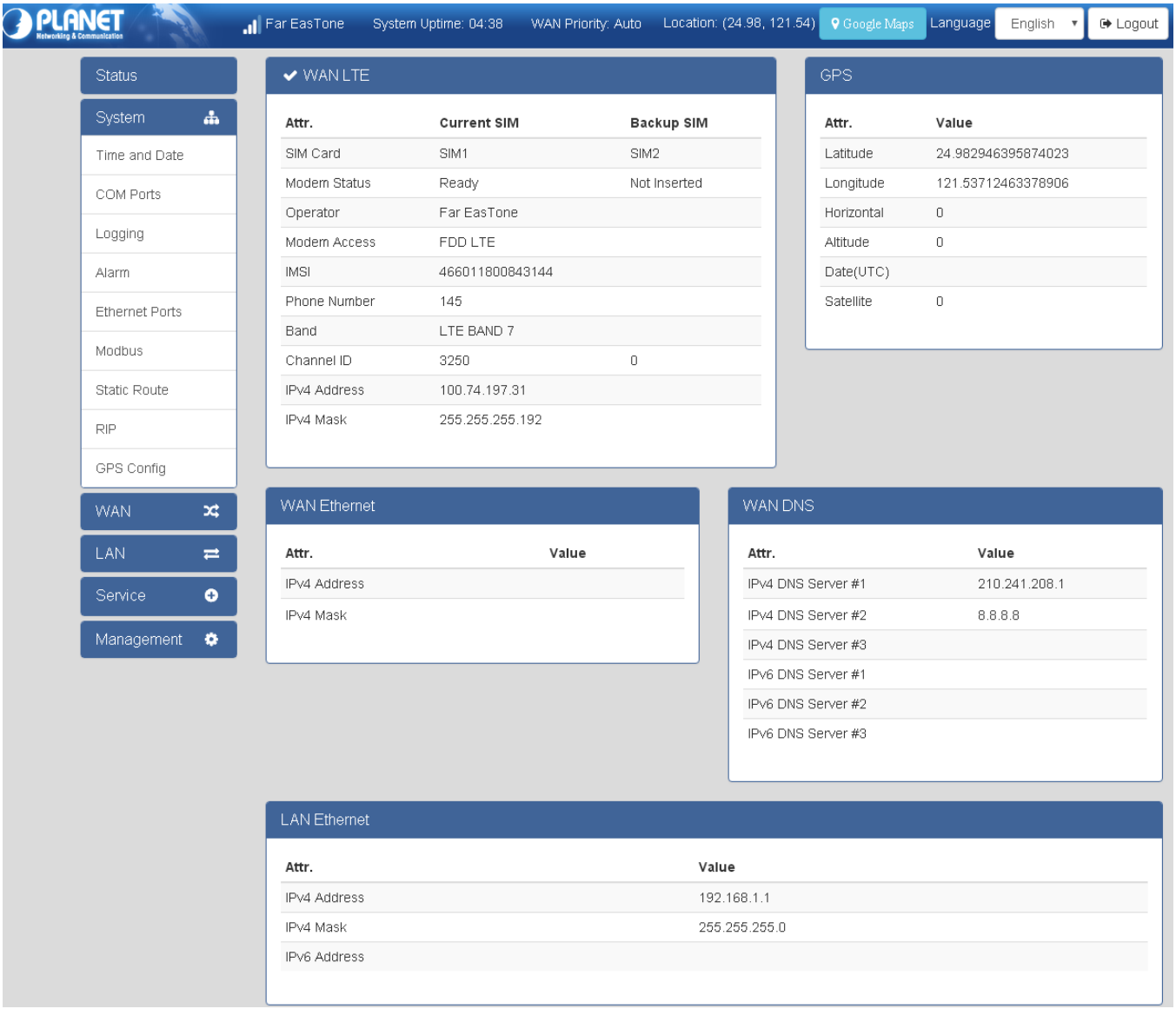


Figure 4-2-1 Status Page Screenshot

The page includes the following fields:

Object – WAN LTE	Description
• **SIM Card**	Show the number of SIM card
• **Modem Status**	Display the status of modem.
• **Operator**	Display the name of carrier.
• **Modem Access**	Display the cellular gateway to access protocol type
• **IMSI**	Display the IMSI number of the current SIM cards.

• **Phone Number**	Display the phone number of the current SIM or Backup SIM.
• **Band**	Display current connected Band.
• **Channel ID**	Display current connected channel ID.
• **IPv4 Address**	LTE obtain IPv4 address.
• **IPv4 Mask**	LTE IPv4 mask.

Object – WAN Ethernet	Description
• **IPv4 Address**	Ethernet WAN obtain IPv4 Address.
• **IPv4 Mask**	Ethernet WAN obtain IPv4 Mask.

Object – LAN Ethernet	Description
• **IPv4 Address**	Ethernet LAN is assigned IPv4 Address.
• **IPv4 Mask**	Ethernet LAN is assigned IPv4 Mask.
• **IPv6 Address**	Ethernet LAN is assigned IPv6 Address.

Object – WAN DNS	Description
• **IPv4 DNS Server #1**	Display the address of IPv4 DNS Server #1.
• **IPv4 DNS Server #2**	Display the address of IPv4 DNS Server #2.
• **IPv4 DNS Server #3**	Display the address of IPv4 DNS Server #3.
• **IPv6 DNS Server #1**	Display the address of IPv6 DNS Server #1.
• **IPv6 DNS Server #2**	Display the address of IPv6 DNS Server #2.
• **IPv6 DNS Server #3**	Display the address of IPv6 DNS Server #3.

Object – WAN GPS	Description
• **Latitude**	Display the latitude information of location.
• **Longitude**	Display the longitude information of location.
• **Horizontal**	Display the horizontal information of location.
• **Altitude**	Display the altitude information of location.
• **Date (UTC)**	Display the date information of location.
• **Satellite**	Display the satellite information of location.

4.3 System

4.3.1 Time and Date

Configure SNTP on this page. **SNTP** is an acronym for **Simple Network Time Protocol**, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers and set GMT Time zone or you can set the time manually. The SNTP Configuration screens in Figure 4-3-1 appear.

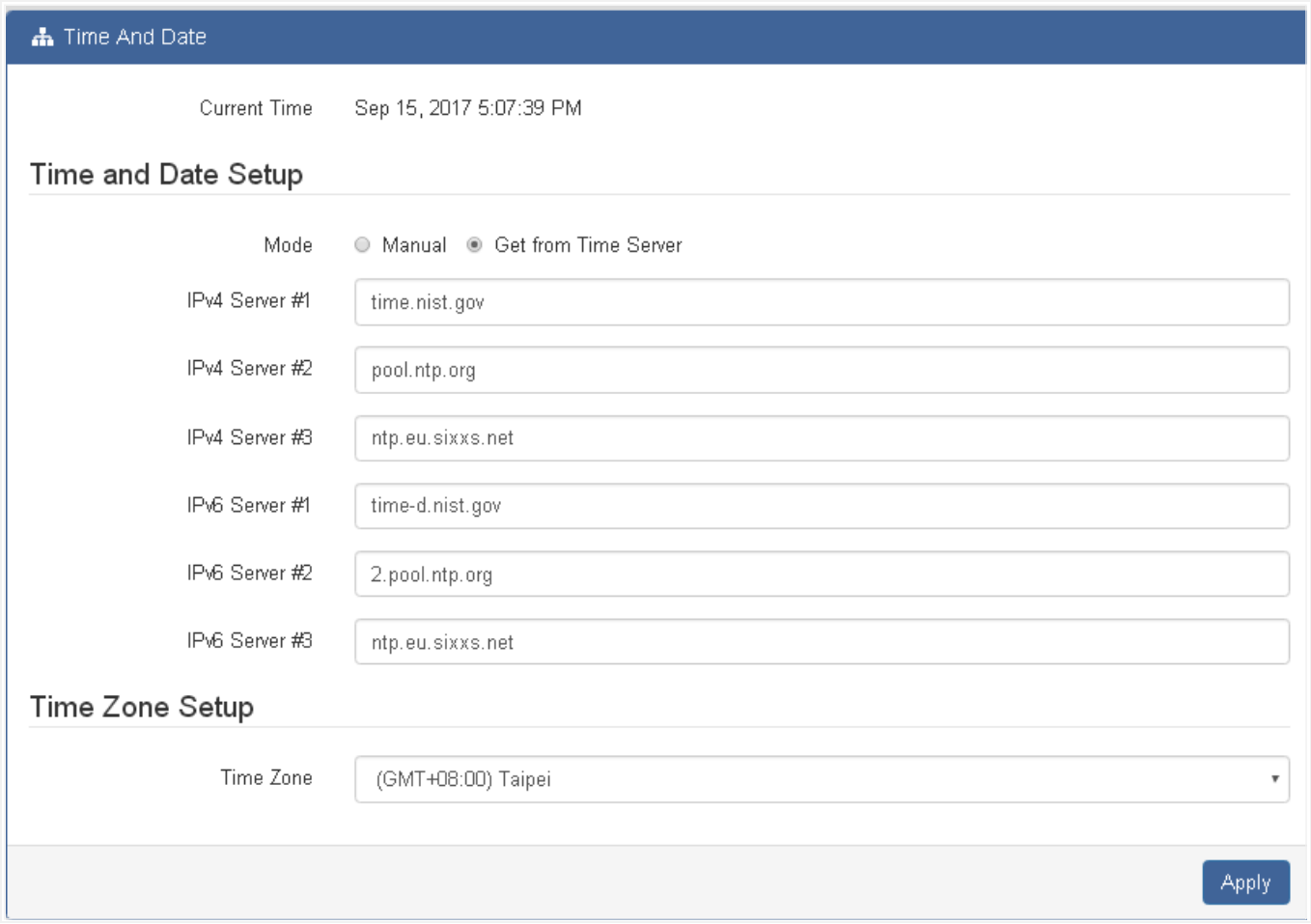


Figure 4-3-1 Time and Date Page Screenshot

The page includes the following fields:

Object	Description
• **Current Time**	Display the current time
• **Mode**	Allows to choose which way to get time; Manual or Time Server
• **IPv4 Server #1**	Type the IPv4 address of the SNTP server # 1
• **IPv4 Server #2**	Type the IPv4 address of the SNTP server # 2
• **IPv4 Server #3**	Type the IPv4 address of the SNTP server # 3
• **IPv6 Server #1**	Type the IPv6 address of the SNTP server # 1
• **IPv6 Server #2**	Type the IPv6 address of the SNTP server # 2
• **IPv6 Server #3**	Type the IPv6 address of the SNTP server # 3
• **Time Zone**	Allows to select the time zone according to the current location of cellular gateway.

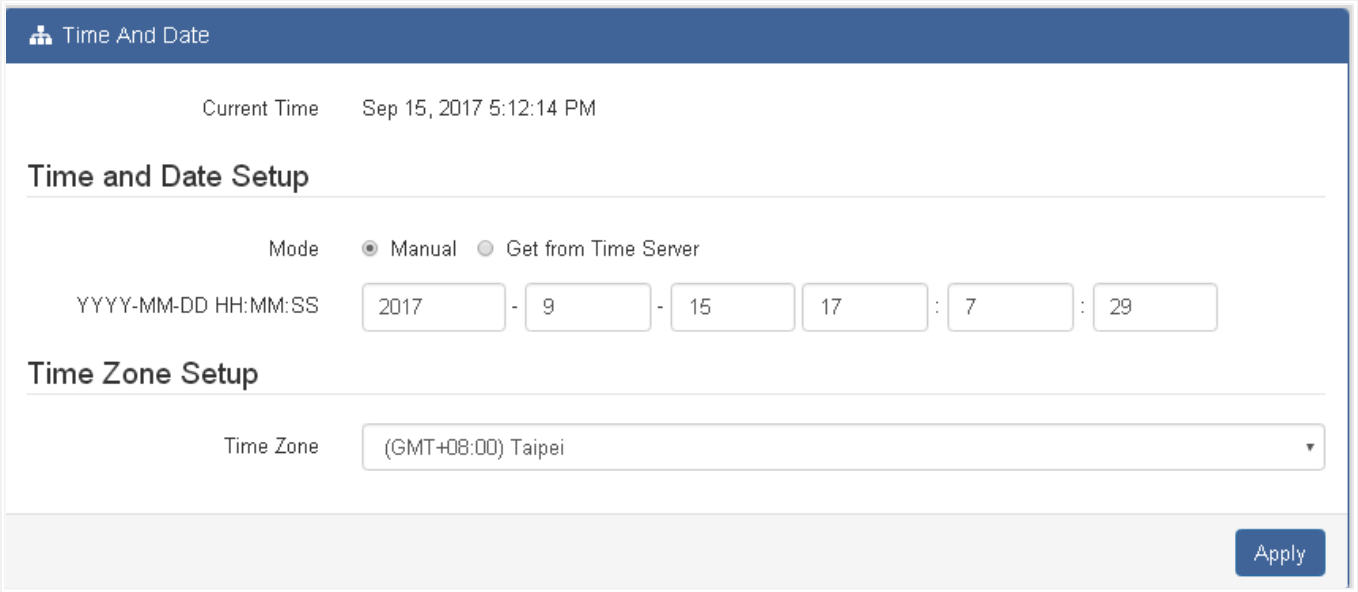


Figure 4-3-2 Time and Date Manual Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	Allows to choose which way to get time; Manual or Time Server
• **YYYY-MM-DD HH:MM:SS**	Allows to adjust the time manually
• **Time Zone**	Allows to select the time zone according to the current location of cellular gateway.

Buttons

Apply: Click to apply changes

4.3.2 COM Ports

This section provides you to configure the COM port settings and remotely manage the device through the virtual COM setting. For the remote management, the managed device should be connected to the cellular gateway by serial interface either RS232 or RS485. The screens in Figure 4-3-3 appear.

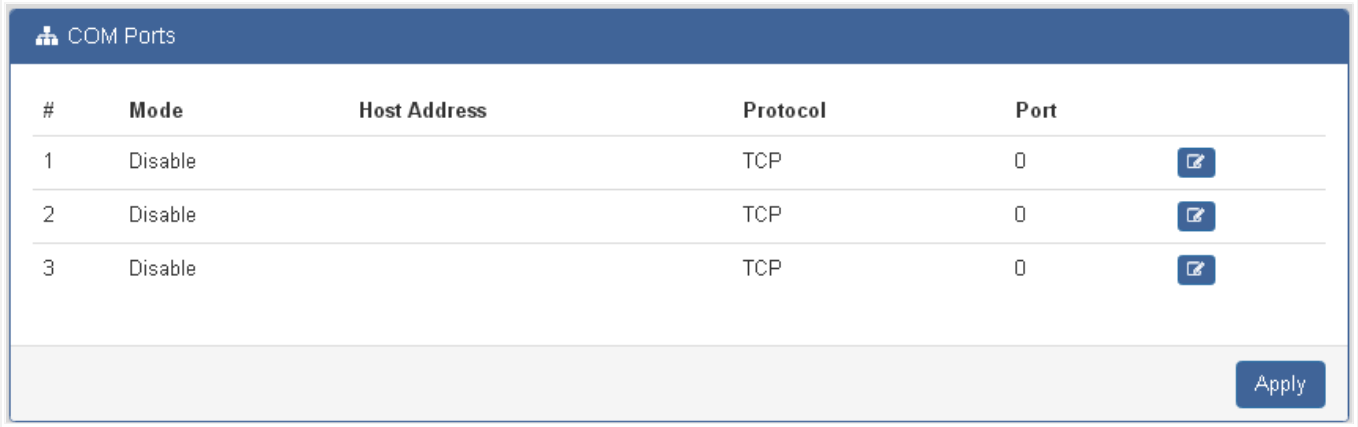
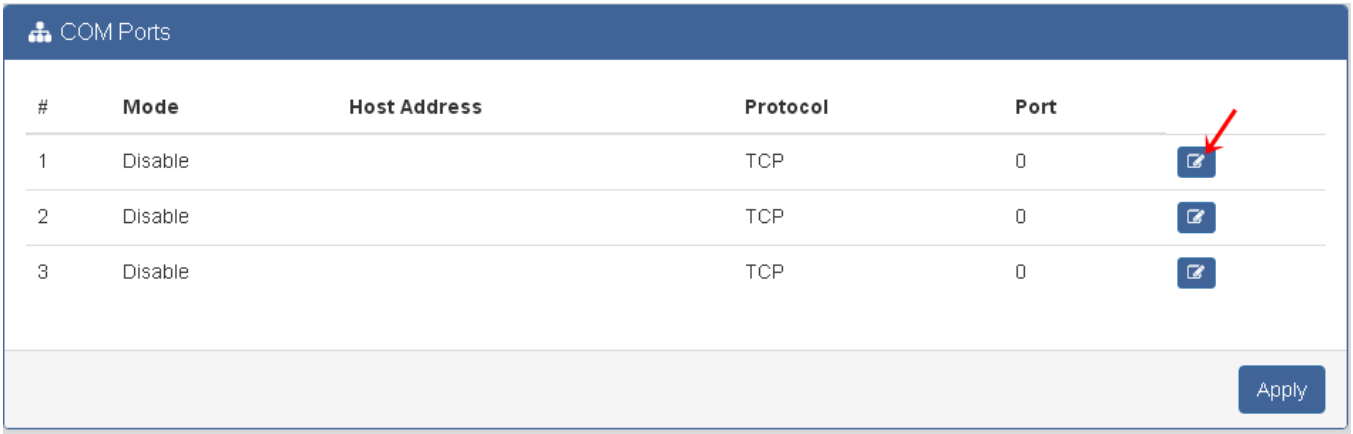


Figure 4-3-3 COM Port Setting Page Screenshot

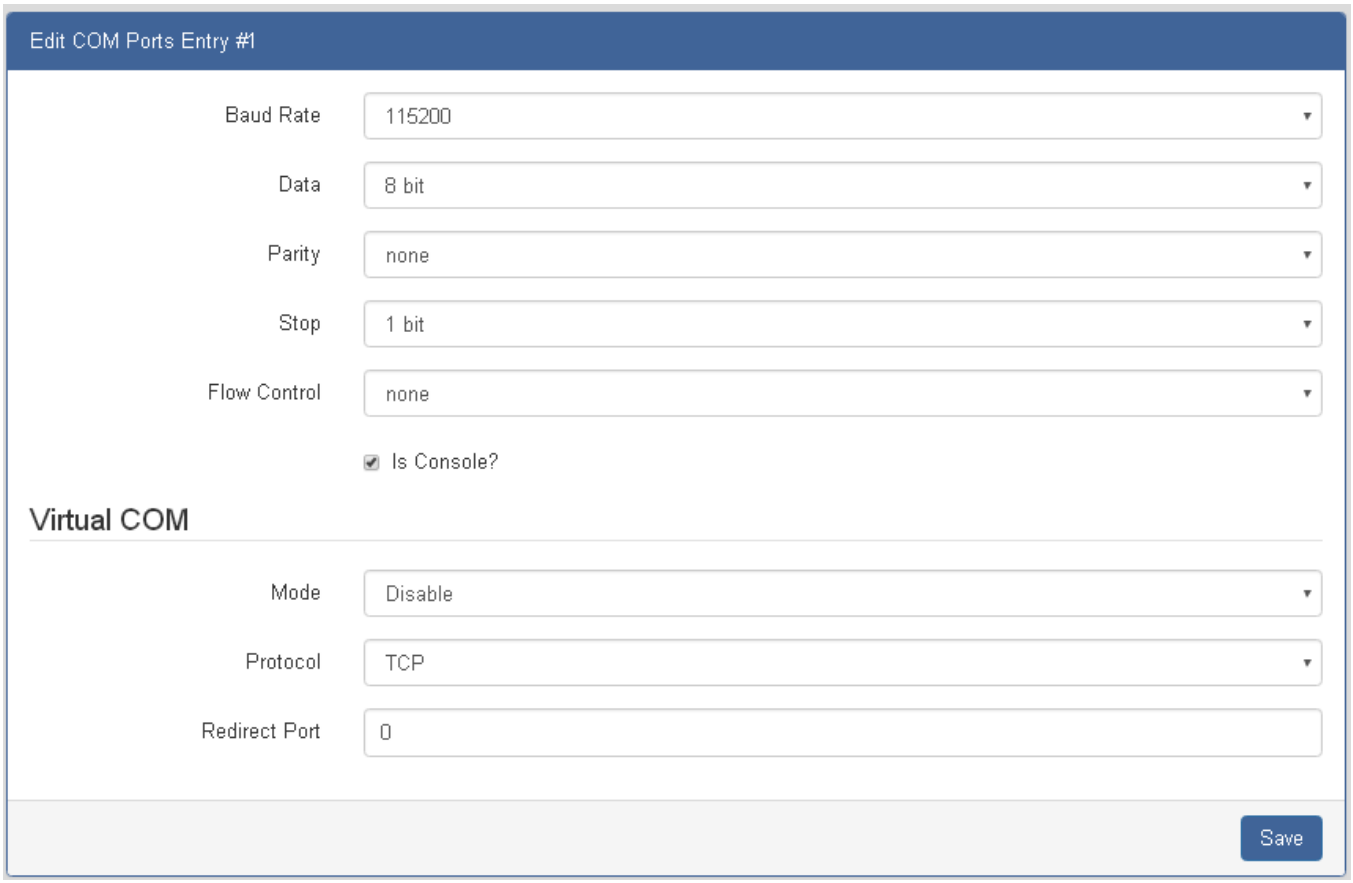
Note

The COM 1 and COM 2 are RS232 interface, and the COM 3 is RS485 interface.

(1) The default is Disable. You can click edit button to configure your settings.



(2) Set up the configuration and Virtual COM. After configuring, click Save to confirm your settings.

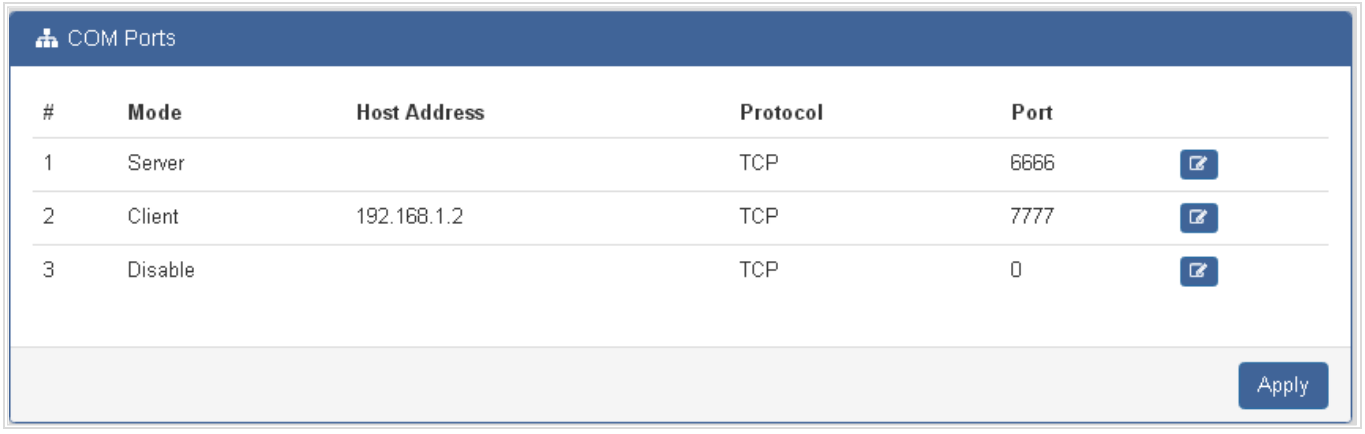


(3) The "is console" is the command-line interface (CLI) management option for cellular gateway. You can assign the COM port to be a management port by this option.

Note

Suggest to enable at least 1 COM port as your console port and the default console port is COM 1.

(4) The interface shows the setting information and click Apply to configure.



The page includes the following fields:

Object	Description
• **Baud Rate**	Select from the current Baud Rate.
• **Data**	Select from 7 bit or 8 bit.
• **Parity**	Select from the information of Parity.
• **Stop**	Select from 1 bit or 2 bit.
• **Flow Control**	Select from none, Xon/Xoff or hardware.
• **Mode**	Select from Disable, Server or Client.
• **Protocol**	Select from TCP or UDP.
• **Host Address**	The host address is only available on client mode. Specify what the domain name or IP address (IPv4 or IPv6) to be connected.
• **Redirect Port**	■ Server Mode: This network package of mobile router is on this port. ■ Client Mode: The network package of remote device is on the remote host.

Buttons

: Click to apply changes.

: Click to save changes.

4.3.3 Logging

The cellular gateway log information is provided here. The System Log screen in Figure 4-3-4 appears.

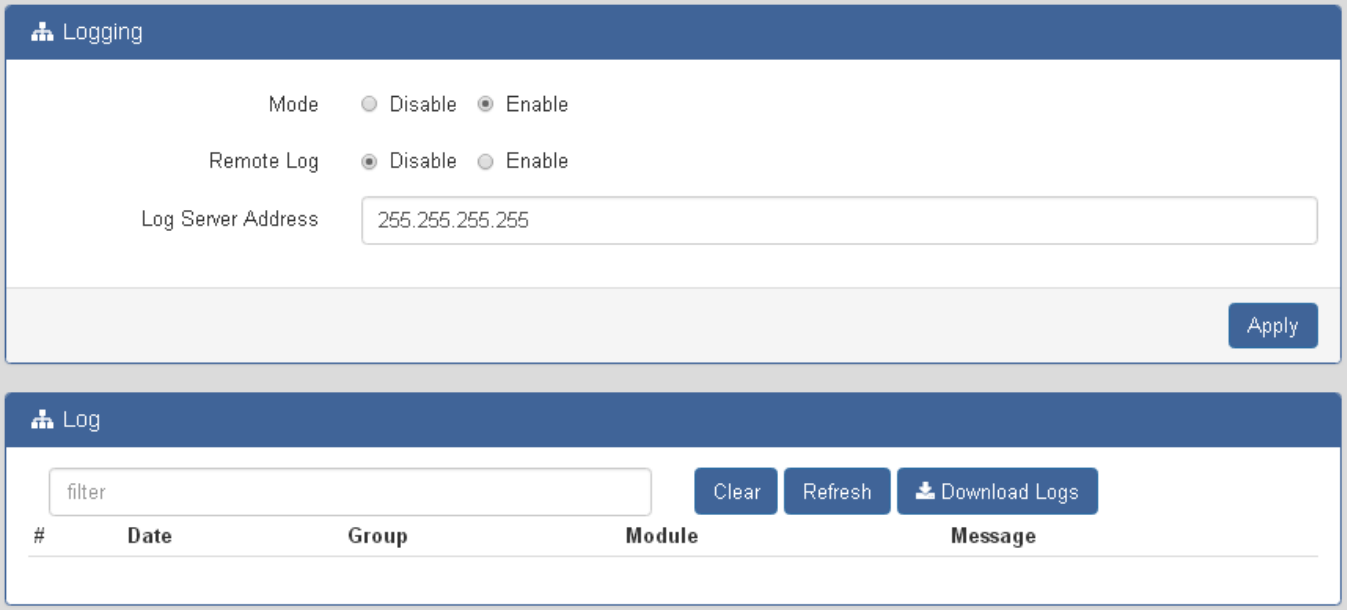


Figure 4-3-4 Logging Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	■ **Enabled**: Enable syslog mode operation. ■ **Disabled**: Disable syslog mode operation.
• **Remote Log**	■ **Enabled**: Enable remote syslog mode operation. ■ **Disabled**: Disable remote syslog mode operation.
• **Log Server Address**	Indicates the IPv4 host address of syslog server.

Buttons

Clear : Click to clear the logs.

Refresh : Click to refresh the logs.

Download Logs : Click to download the logs.

4.3.4 Alarm

The cellular gateway alarm configuation is provided here. The alarm screen in Figure 4-3-5 appears.

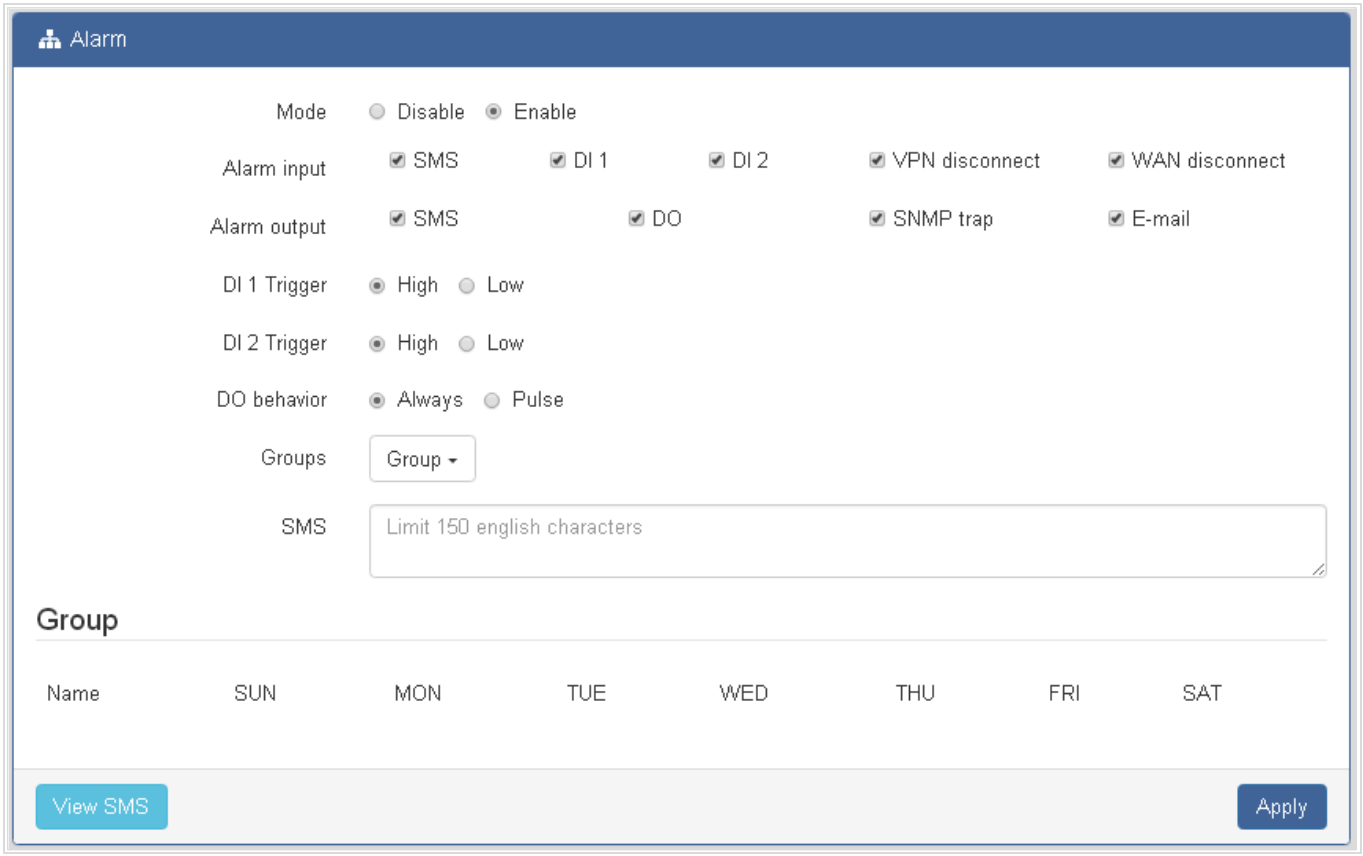


Figure 4-3-5 Alarm Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the Alarm configuration. The default is Enable.
• **Alarm Input**	Select from SMS, DI 1, DI 2, VPN disconnect and WAN disconnect as input to trigger alarm. ■ **SMS:** It means team members on selected week day can send SMS to the phone number of using SIM card to trigger alarm. ■ **DI 1/2:** IO high to trigger alarm. ■ **VPN disconnect:** All tunnels get disconnected and then trigger alarm. ■ **WAN disconnect:** All WAN connections get disconnected and then trigger alarm.
• **Alarm Output**	Select from SMS, DO and SNMP trap as alarm output.
• **DI 1 Trigger** • **D1 2 Trigger**	Select from High or Low. The default is High Trigger. ■ **High:** SW is On to trigger. ■ **Low:** SW is OFF to trigge.
• **DO behavior**	■ **Always:** Pull DO high. ■ **Pulse:** High and Low continuously.

• **Groups**	Create your groups and edit your information of groups.
• **SMS**	Write your messages limited to 150 English characters.

Buttons

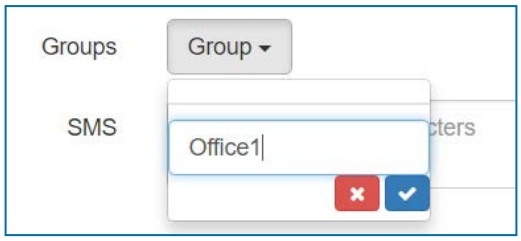
Apply: Click to apply changes.

View SMS: Click to view the incoming SMS.

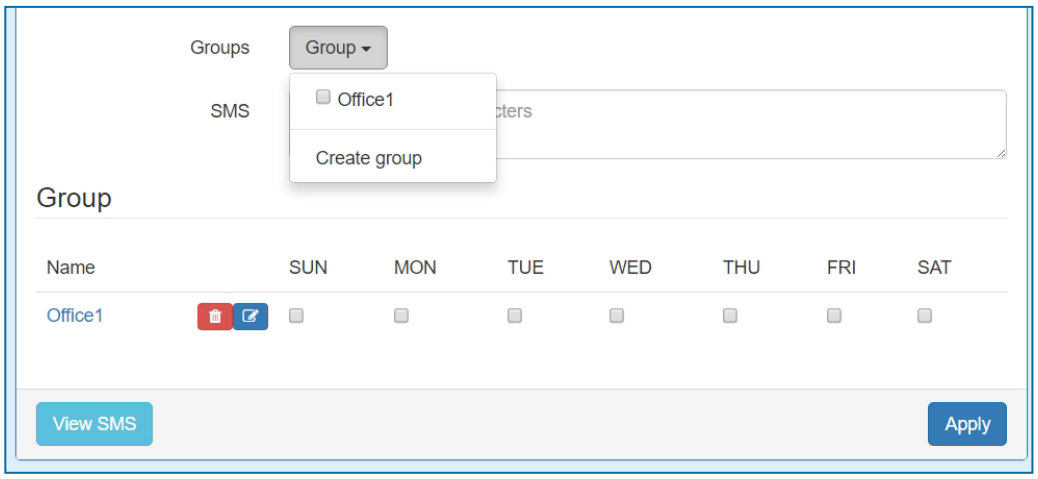
4.3.4.1 Example of Creating Group and Add Users

(1) How to create your group

■ Name a group

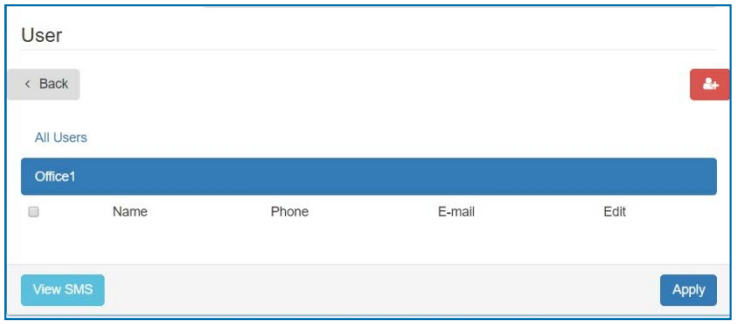


■ Show your group name from the list of groups.

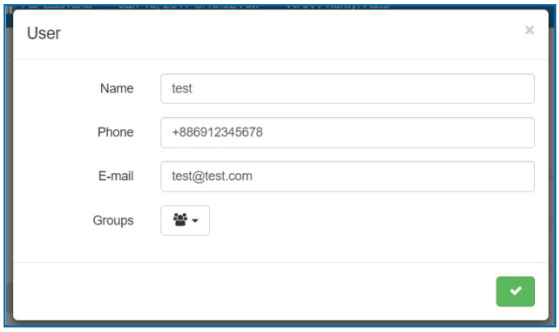


(2) How to edit your group

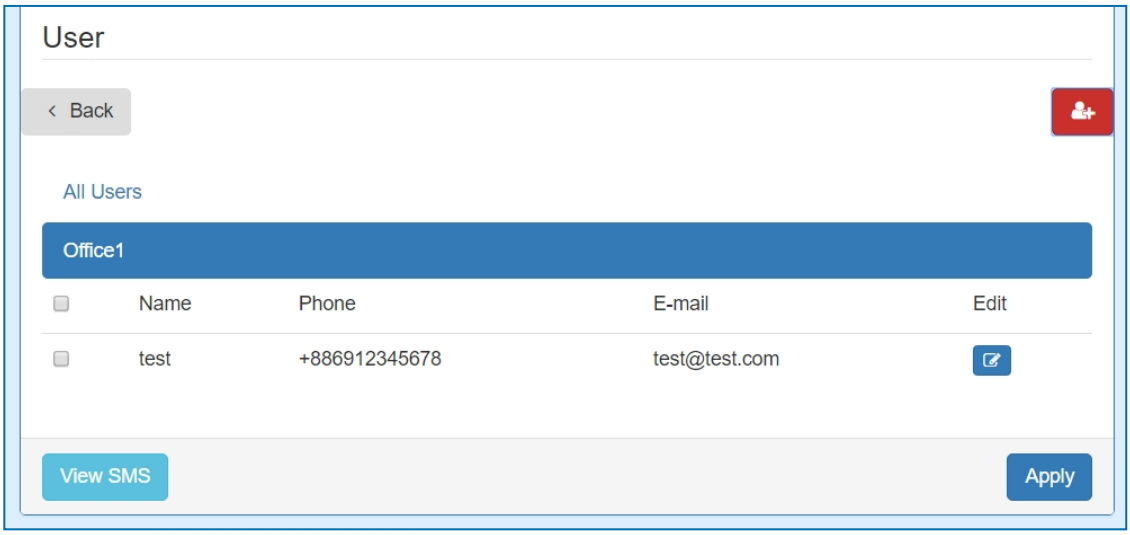
■ Select your group and click  to edit your group information, including Name, Phone and E-mail.



- After filling in your information, click  to submit your settings.

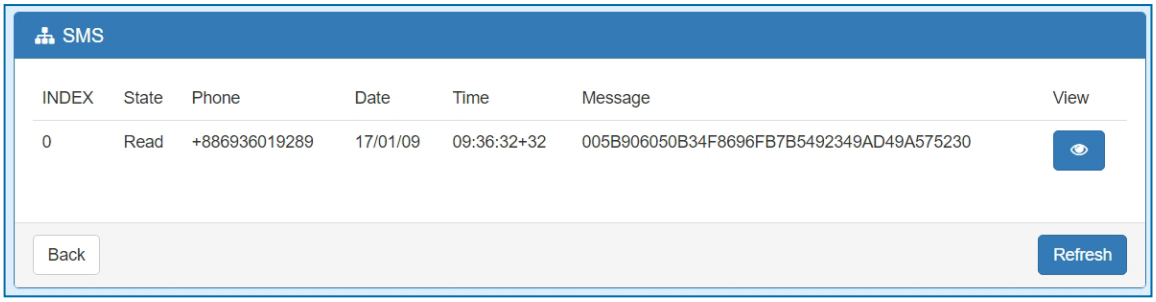


- After submitting your setting, the interface shows the information that you edited.



(3) How to View SMS

- View SMS to view the information, including the state, phone, and date and time.
- Click  to review your all messages.



4.3.5 Ethernet Ports

This page displays current port configurations. Ports can also be configured here. The Port Configuration screen in Figure 4-3-6 appears.

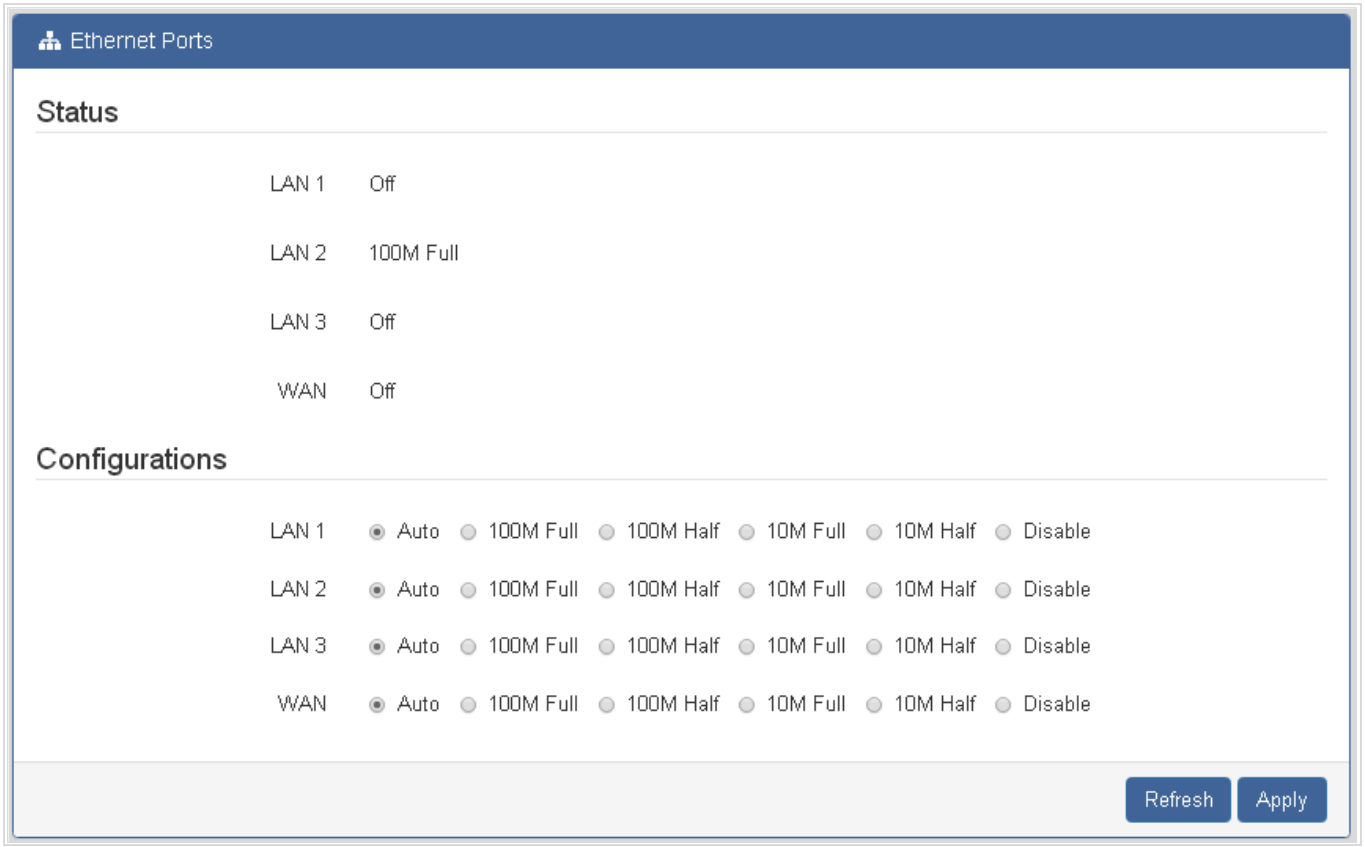


Figure 4-3-6 Ethernet Ports Page Screenshot

The page includes the following fields:

Object	Description
• **Status**	Provides the current link speed of the port.
• **Configurations**	Select any available link speed for the given port. ■ **Auto** - Setup Auto negotiation for copper interface. ■ **10Mbps Half** - Force sets 10Mbps/Half-Duplex mode. ■ **10Mbps Full** - Force sets 10Mbps/Full-Duplex mode. ■ **100Mbps Half** - Force sets 100Mbps/Half-Duplex mode. ■ **100Mbps Full** - Force sets 100Mbps/Full-Duplex mode. ■ **Disable** – Shut down the port manually.

Buttons

Apply: Click to apply changes.

Refresh: Click to refresh the status logs.

4.3.6 Modbus

The cellular gateway Modbus configuation is provided here. The Modbus screen in Figure 4-3-7 appears.

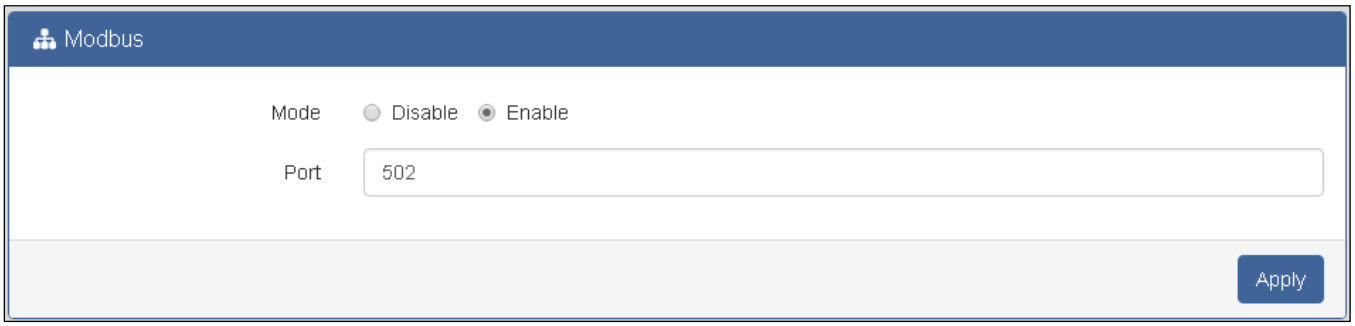


Figure 4-3-7 Modbus Setup Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the Modbus configuration. The default is Enable.
• **Port**	The listening port of Modbus TCP.

Buttons

Apply: Click to apply changes.

4.3.7 Static Route

The cellular gateway static route configuation is provided here. The static route screen in Figure 4-3-8 appears.

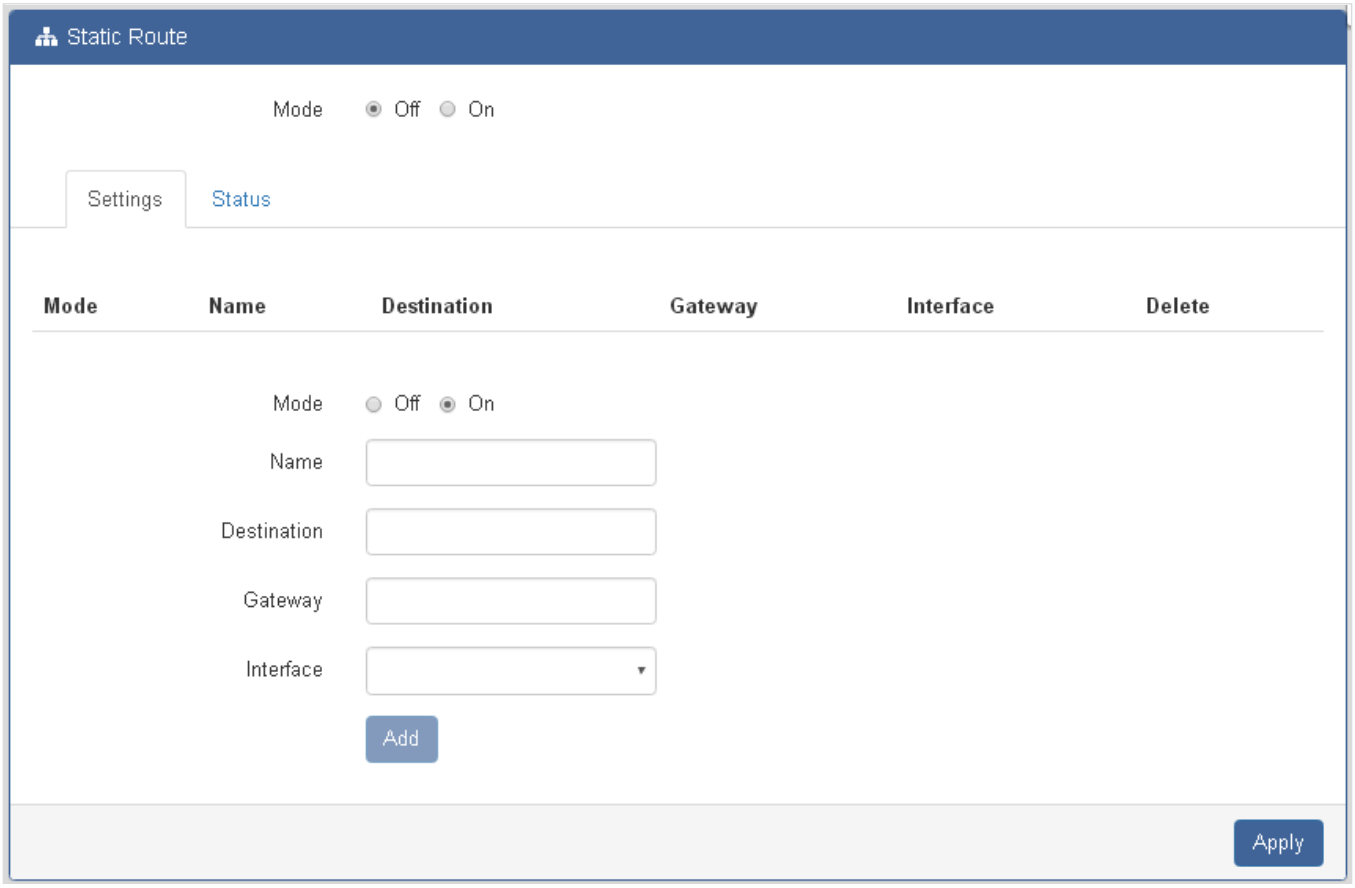


Figure 4-3-8 Static Route Setup Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	The setting is for full network. Select from Off or On.
• **Mode**	The setting is for the specific network. Select from Off or On.
• **Name**	Set up each name for running host or network.
• **Destination**	Fill in the destination of a specific subnet or IP from network.
• **Gateway**	Fill in the gateway address of your router.
• **Interface**	Select the interface from LAN or Ethernet.

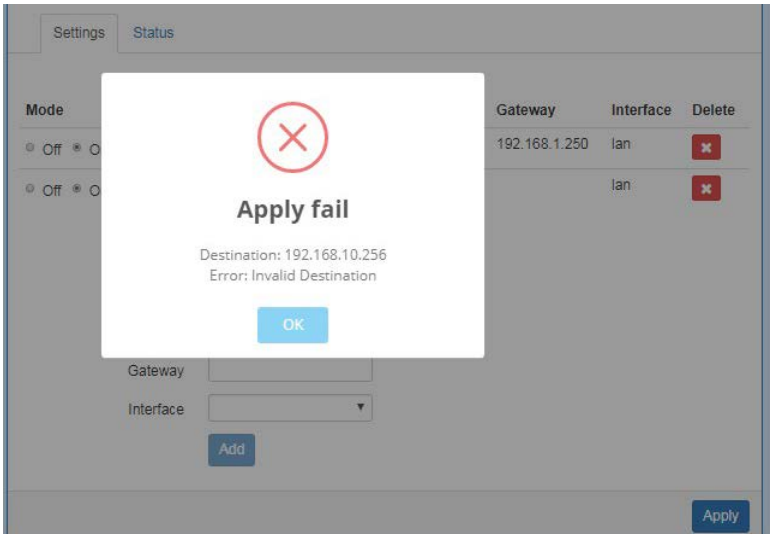
Buttons

Apply: Click to apply changes.

Note:

- The destination field is required to fill in. The format of destination is IPv4 or IPv6.
- The address of gateway or the type of interface can be chosen one or both to fill in the field.
- There are two fail situations when you fill in the incorrect type for the field.

(1) Input the invalid format of destination. The interface is shown in Apply fail to notice.



(2) Input the IP address of destination/gateway from IPv4 and IPv6 at the same time. The interface is shown in Apply fail to notice. You should select either IPv4 or IPv6 as the address of destination/gateway.

The status tab shows the information from the settings of static route. The static route screen in Figure 4-3-9 appears.

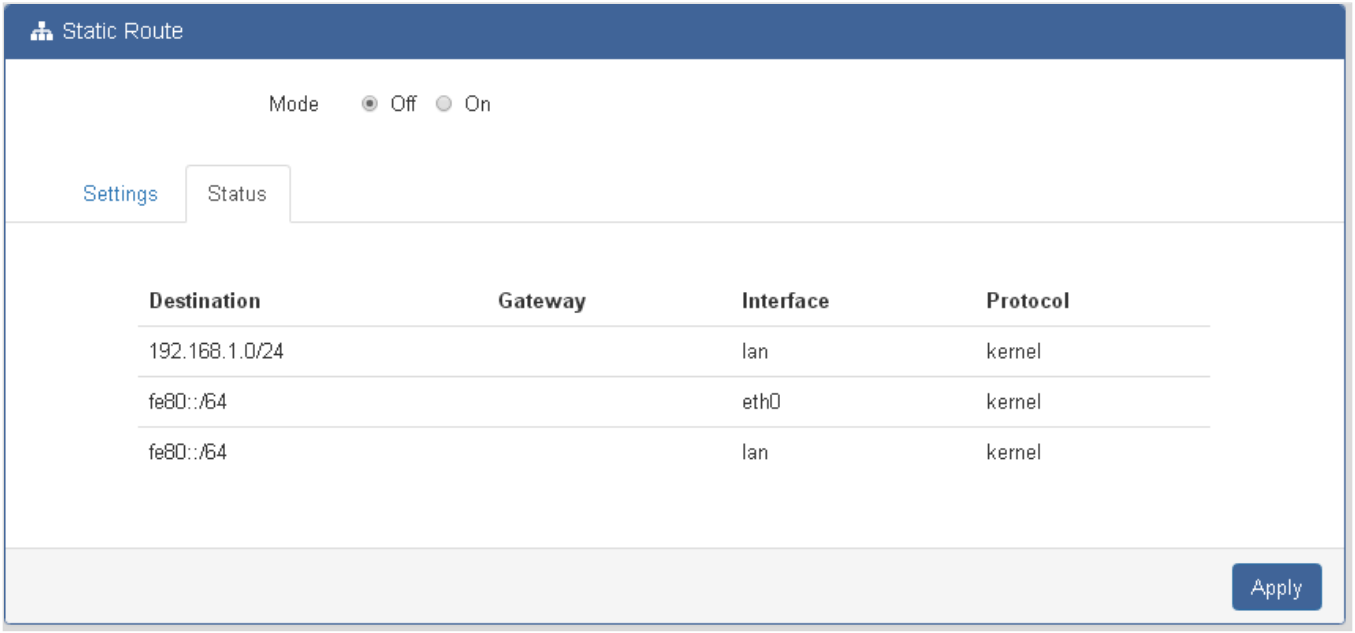


Figure 4-3-9 Static Route Status Page Screenshot

4.2.8 RIP

The cellular gateway RIP configuation is provided here. The RIP screen in Figure 4-3-10 appears.

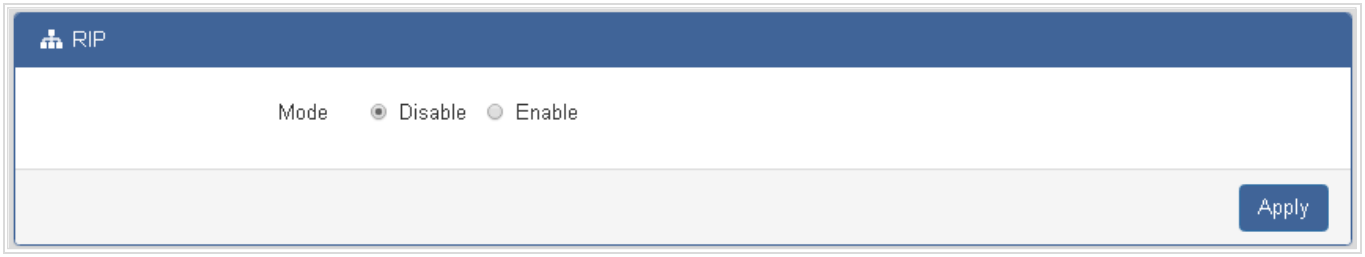


Figure 4-3-10 RIP Setup Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the Modbus configuration. The default is Disable.

Buttons

Apply: Click to apply changes.

4.2.9 GPS Config

The cellular gateway GPS configuation is provided here. The GPS Config screen in Figure 4-3-11 appears.

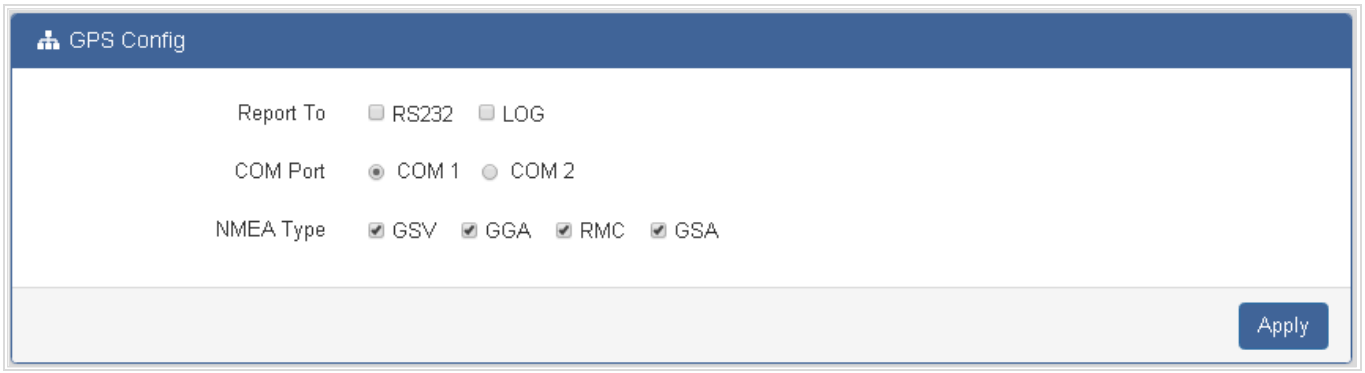


Figure 4-3-11 GPS Config Page Screenshot

The page includes the following fields:

Object	Description
• **Report To**	Indicates where to send the message.
• **COM Port**	Select which COM Port for reporting to.
• **NMEA Type**	Select NMEA Type.

Buttons

Apply: Click to apply changes.

4.4 WAN

4.4.1 Priority

The cellular gateway WAN Priority configuation is provided here. The Priority Config screen in Figure 4-4-1 appears.

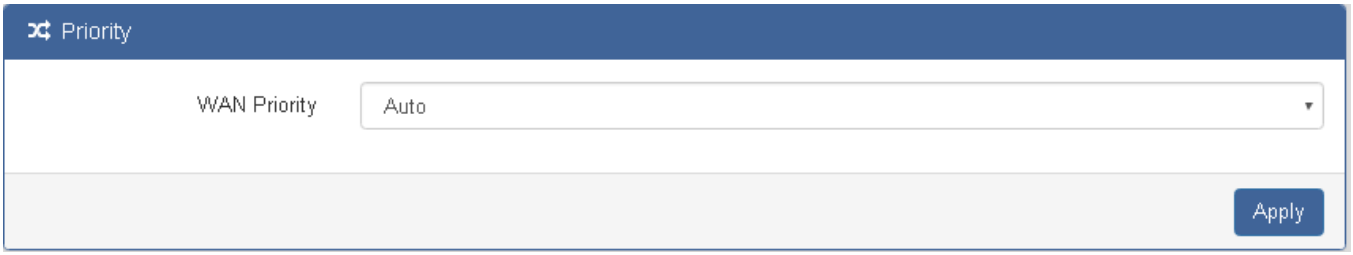


Figure 4-4-1 Priority Setup Page Screenshot

The page includes the following fields:

Object	Description
• **WAN Priority**	■ Auto: WAN Ethernet is first priority and second priority is LTE. The default is Auto. ■ LTE Only: The priority is only LTE. ■ ETH Only: The priority is only Ethernet.

Buttons

Apply: Click to apply changes.

4.4.2 LTE Config

The cellular gateway LTE configuation is provided here. The LTE Config screen in Figure 4-4-2 appears.

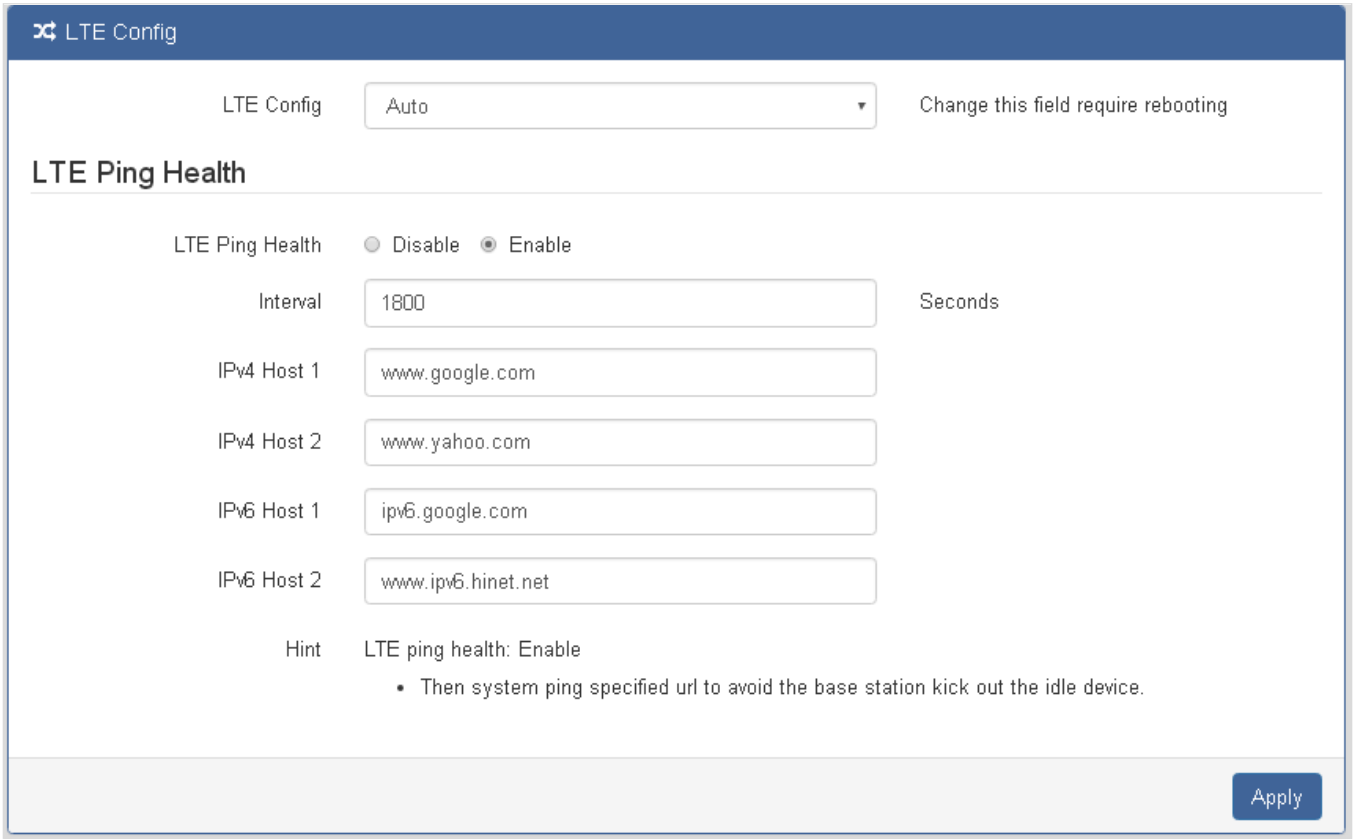


Figure 4-4-2 LTE Config Setup Page Screenshot

The page includes the following fields:

Object – LTE Config	Description
• **LTE Config**	Indicates what kind of LTE will be used. Possible modes are: ■ **Auto**: Automatically connect the possible band. ■ **4G Only**: Connect to 4G network only. ■ **3G Only**: Connect to 3G network only. ■ **2G Only**: Connect to 2G network only.
Object – LTE Ping Health	**Description**
• **LTE Ping Health**	**Disable or Enable** the LTE Ping Health configuration. The default is Enable.
• **Interval**	Input the interval seconds of ping.
• **IPv4 Host 1**	Input the address of IPv4 Host 1.
• **IPv4 Host 2**	Input the address of IPv4 Host 2.
• **IPv6 Host 1**	Input the address of IPv6 Host 1.

• **IPv6 Host 2**	Input the address of IPv6 Host 2.

Buttons

: Click to apply changes.

4.4.3 Dual SIM

The cellular gateway Dual SIM configuation is provided here. The Dual SIM screen in Figure 4-4-3 appears.

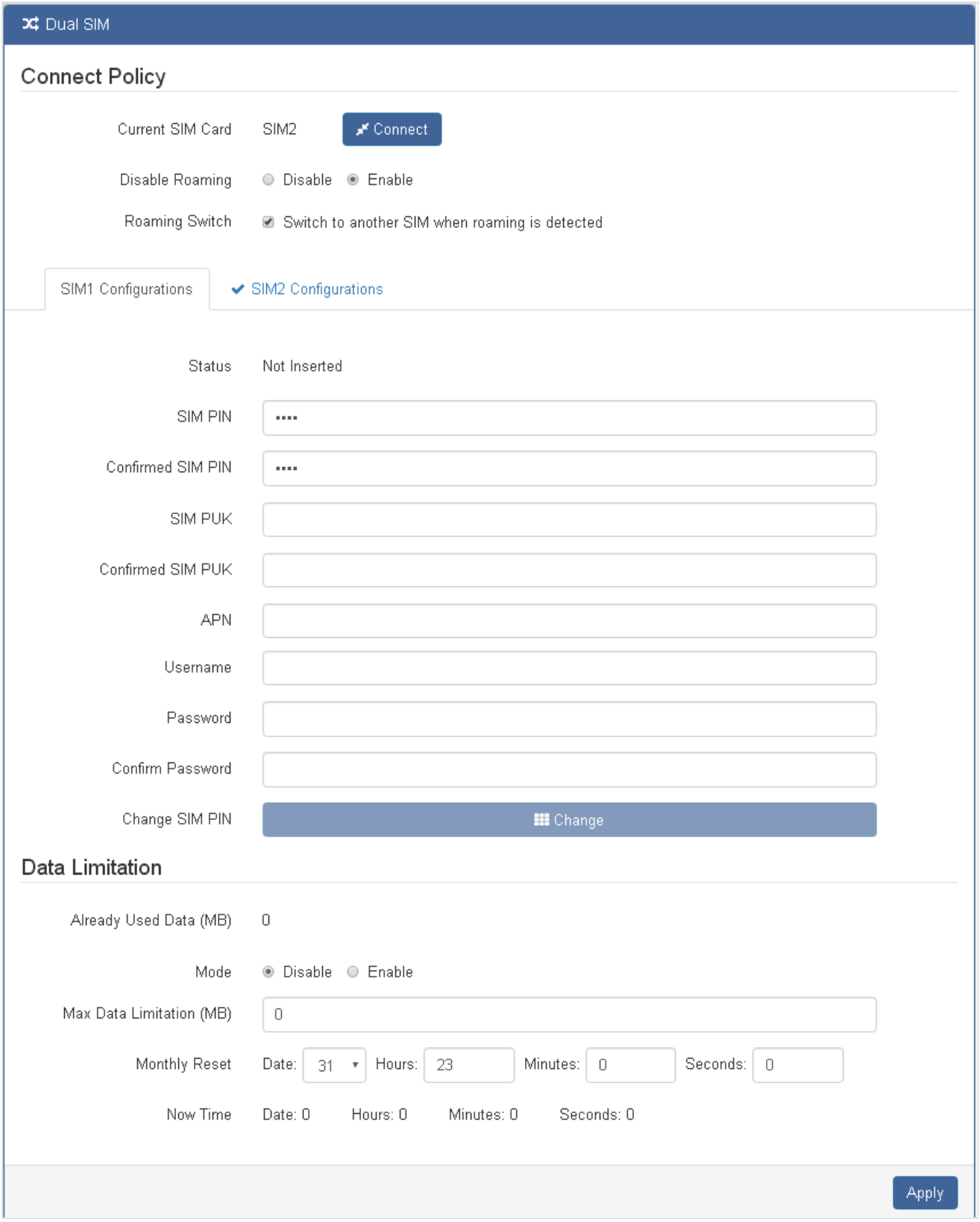


Figure 4-4-3 Dual SIM Setup Page Screenshot

The page includes the following fields:

Object – Connect Policy	Description
• Current SIM Card	Display which SIM slot is using.
• Status of SIM Card Connectivity	■ **Connect:** After manually disconnecting, user can only click the Connect button to get connection or reboot the device to make it automatically connect. ■ **Disconnect:** If there is one SIM slot get connection, the Disconnect button appears. After manually clicking Disconnect, the system would not automatically get connection until next reboot.
• Disable Roaming	■ **Disable:** SIM gets connection even it is in roaming state. ■ **Enable:** SIM would not get connection when in roaming state.
• Roaming Switch	Switch to another SIM when roaming is detected. System will switch SIM slot when current SIM is in roaming state and another SIM slot is in READY state.
Object – SIM1/2 Config	**Description**
• Status	Display the status of Dual SIM.
• SIM PIN	Configure PIN code to unlock SIM PIN.
• Confirmed SIM PIN	Confirm PIN code.
• SIM PUK	Fill in PUK to unlock SIM Card after typing more than 3 times.
• Confirmed SIM PUK	Confirm SIM PUK.
• APN	APN can be input by user or the system will search from internal database if APN is blank.
• Username	The username can be input by user or the system will search from internal database if the username is blank.
• Password	The password can be input by user or the system will search from internal database if the password is blank.
• Confirm Password	Fill in your changed password.
• Change SIM PIN	Change your old SIM PIN code into new SIM PIN code.
Object – Data Limitation	**Description**
• Mode	**Disable or Enable** the Modbus configuration. The default is Disable.
• Already Used Data (MB)	Display current used throughput.
• Max Data Limitation (MB)	Configure max throughput.
• Monthly Reset	Set up the reset time during the month.
• Now Time	Show the current time of system.

- **SIM PIN:** If you have configured SIM PIN code into SIM card, please type SIM PIN code in Dual SIM configuration to make unlock successfully.
- **SIM PUK:** If you have typed wrong SIM PIN code and retried more than 3 times, the SIM Card will become the blocked mode. In this case, you have to type PUK and new SIM code to unlock SIM Card.

Buttons

Apply: Click to apply changes.

4.4.4 Ethernet

The cellular gateway Ethernet configuation is provided here. The Ethernet screen in Figure 4-4-4 appears.

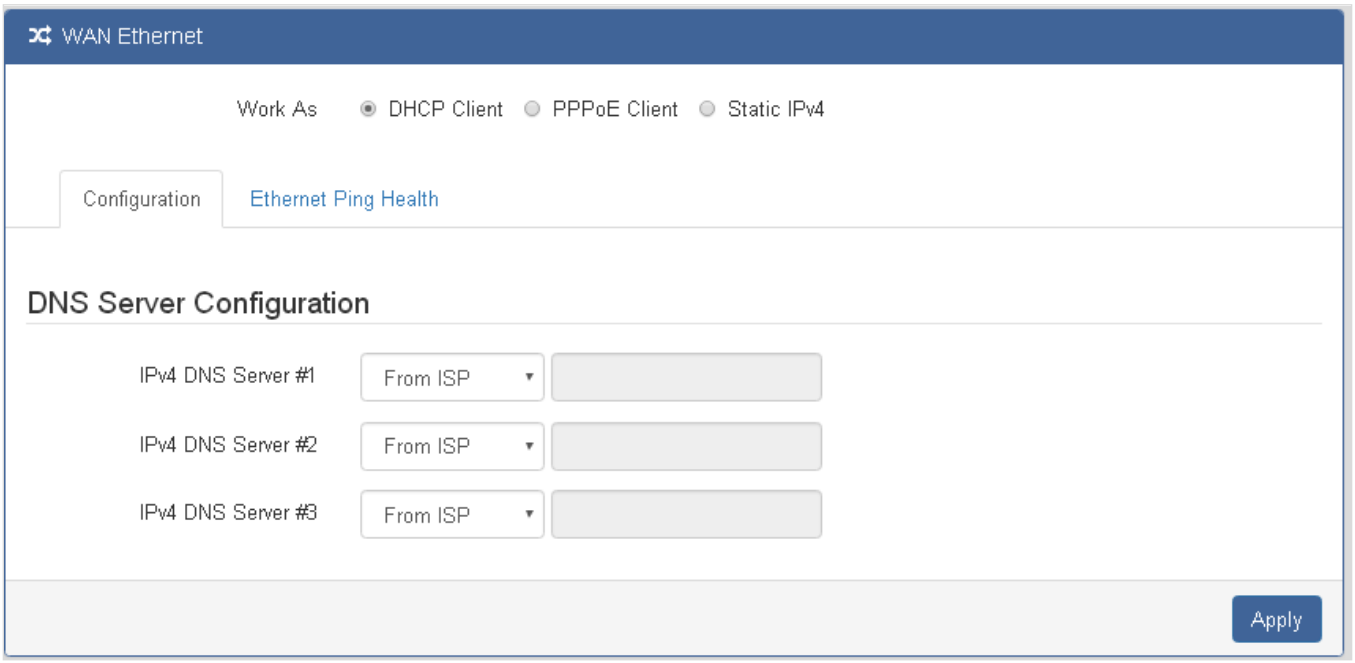


Figure 4-4-4 Ethernet Setup Page Screenshot

The page includes the following fields:

Object	Description
• **Work As**	There are three options to obtain the IP of WAN Ethernet. ■ **DHCP Client:** DHCP server-assigned IP address, netmask, gateway, and DNS. ■ **PPPoE Client:** Your ISP will provide you with a username and password. This option is typically used for DSL services. ■ **Static IPv4:** User-defined IP address, netmask, and gateway address.
• **IPv4 DNS Server #1** **IPv4 DNS Server #2** **IPv4 DNS Server #3**	Each setting of DNS Server has three options, including From ISP, User Defined and None. **From ISP**: the IPv4 DNS server IP is obtained from ISP. **User Defined**: the IPv4 DNS server IP is input by user.

The cellular gateway Ethernet Ping Health configuation is provided here. The Ethernet Ping Health screen in Figure 4-4-5 appears.

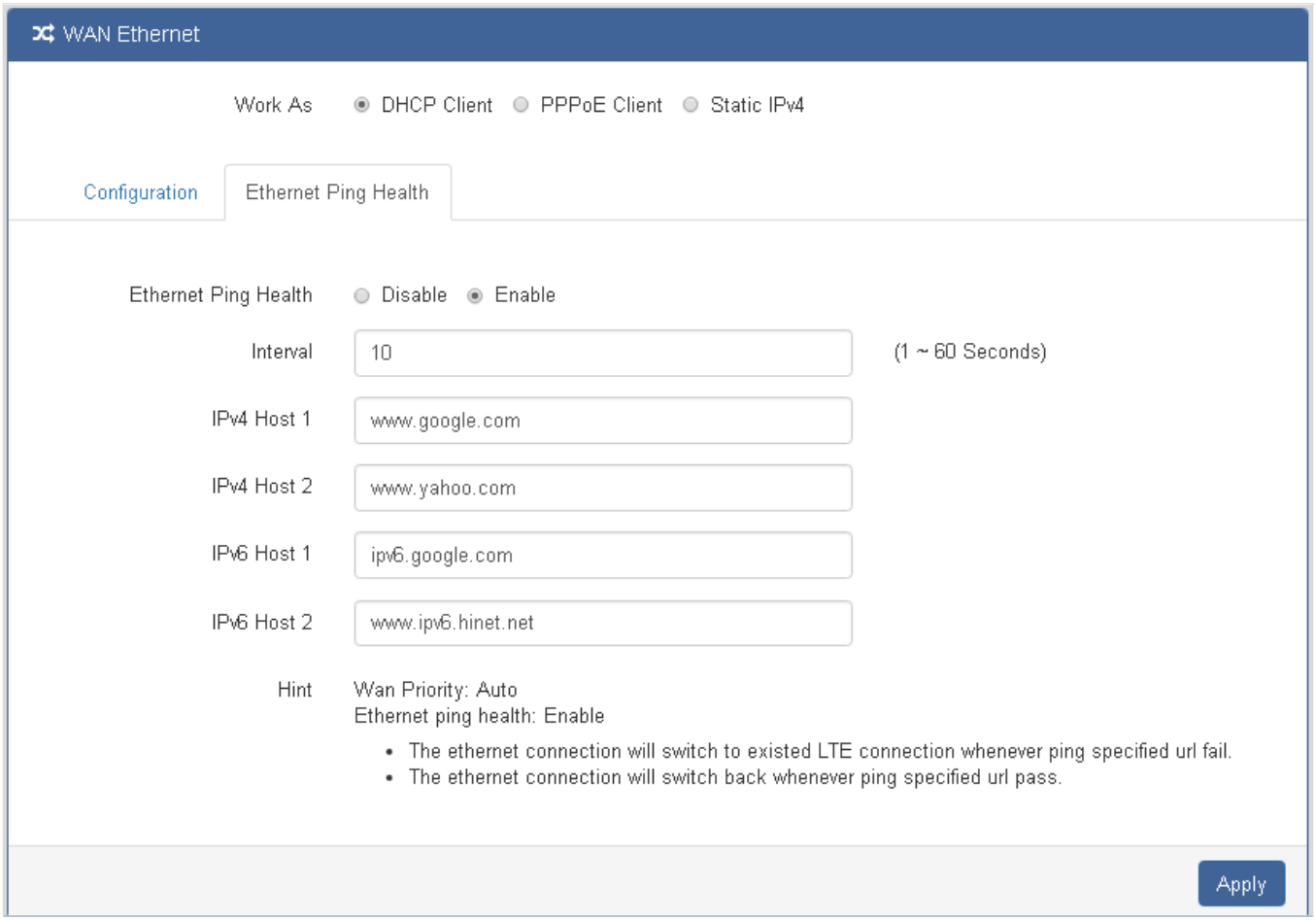


Figure 4-4-5 Ethernet Ping Health Page Screenshot

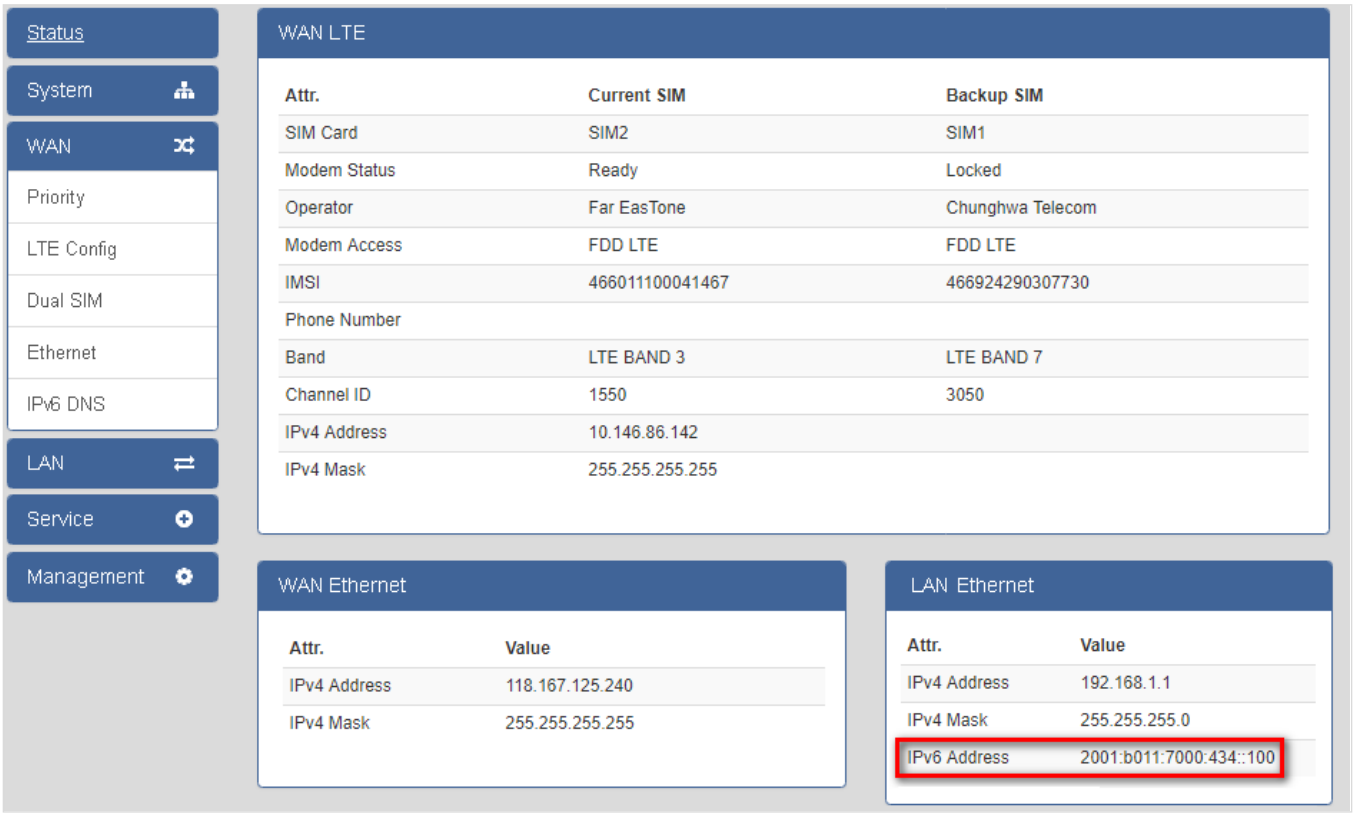
The page includes the following fields:

Object	Description
• **LTE Ping Health**	**Disable or Enable** the LTE Ping Health configuration. The default is Enable.
• **Interval**	Input the interval seconds of ping.
• **IPv4 Host 1**	Input the address of IPv4 Host 1.
• **IPv4 Host 2**	Input the address of IPv4 Host 2.
• **IPv6 Host 1**	Input the address of IPv6 Host 1.
• **IPv6 Host 2**	Input the address of IPv6 Host 2.

Buttons

Apply: Click to apply changes.

In addition, you can check which WAN is actually using from "**Status**" page. For IPv6 address, the status will be displayed on LAN Etherent Interface when IPv6 is using as WAN connection.



4.4.5 IPv6 DNS

The cellular gateway IPv6 DNS configuation is provided here. The IPv6 DNS screen in Figure 4-4-6 appears.

Figure 4-4-6 IPv6 DNS Page Screenshot

The page includes the following fields:

Object	Description
• **IPv6 DNS Server #1** **IPv6 DNS Server #2** **IPv6 DNS Server #3**	Each setting of DNS Server has three options, including From ISP, User Defined and None. **From ISP**: the IPv4 DNS server IP is obtained from ISP. **User Defined**: the IPv4 DNS server IP is input by user.

Buttons

Apply: Click to apply changes.

4.5 LAN

4.5.1 IPv4

The cellular gateway IPv4 configuation is provided here. The IPv4 screen in Figure 4-5-1 appears.

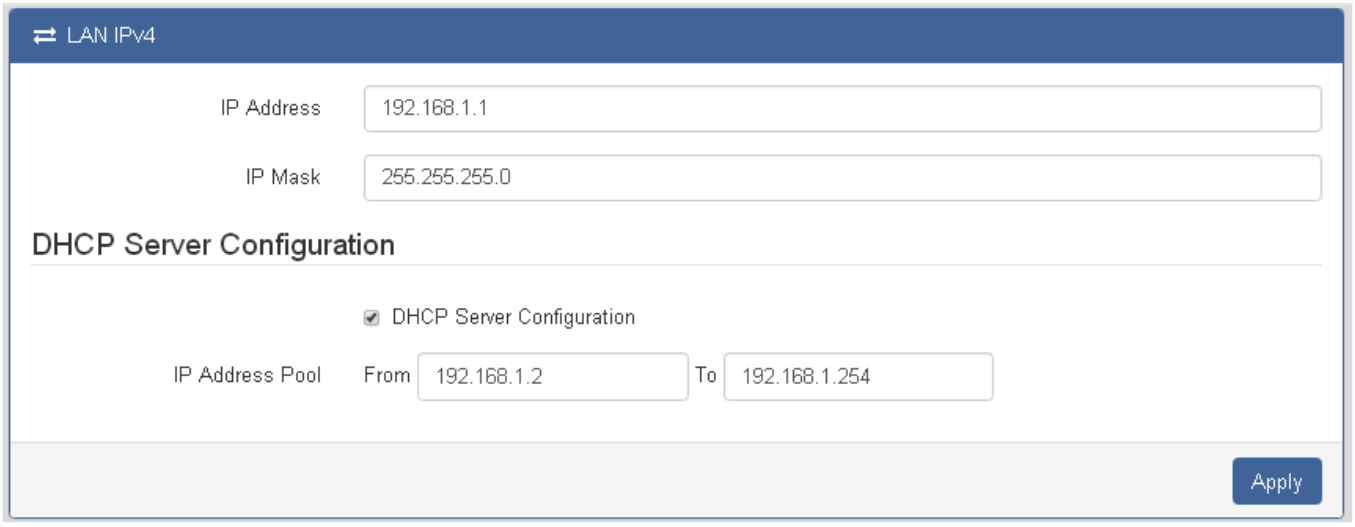


Figure 4-5-1 IPv4 Page Screenshot

The page includes the following fields:

Object	Description
• **LAN IPv4**	■ IP Address:192.168.1.1 ■ IP Mask:255.255.255.0 Both of them are default, you can change them according to your local IP Address and IP Mask.
• **DHCP Server Configuration**	Turn on/off DHCP Server Configuration. Enable to make router lease IP address to DHCP clients which are connected to LAN.
• **IP Address Pool**	Define the beginning and the end of the pool of IP addresses which will lease to DHCP clients.

Buttons

Apply: Click to apply changes.

4.5.3 IPv6

The cellular gateway IPv6 configuration is provided here. The IPv6 screen in Figure 4-5-2 appears.

Figure 4-5-2 IPv6 Page Screenshot

The page includes the following fields:

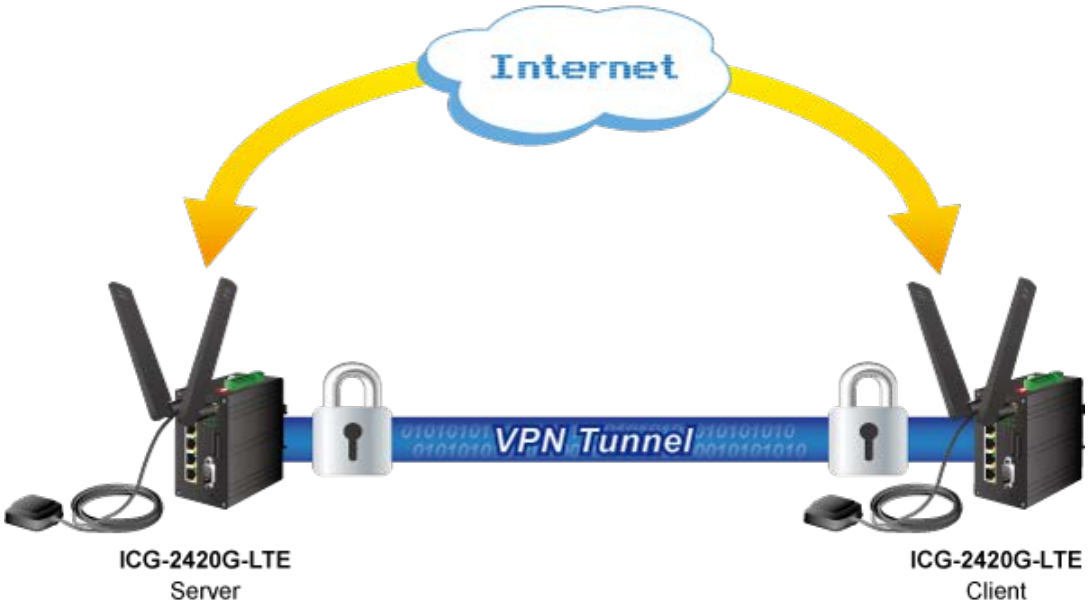
Object	Description
• **Type**	**Delegate Prefix from WAN:** Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router. **Static:** Select this option to configure a fixed IPv6 address for the mobile router's LAN IPv6 address.
• **Address Assign Setup**	Select how you obtain an IPv6 address: ■ **Stateless**: The mobile router uses IPv6 stateless auto configuration. RADVD (Router Advertisement Daemon) is enabled to have the mobile router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 clients. ■ **Stateful**: The mobile router uses IPv6 stateful auto configuration. The LAN IPv6 clients can obtain IPv6 addresses through DHCPv6.

Buttons

Apply: Click to apply changes.

4.6 Service

4.6.1 Open VPN



The cellular gateway Open VPN status is provided here. The Open VPN screen in Figure 4-6-1 appears.

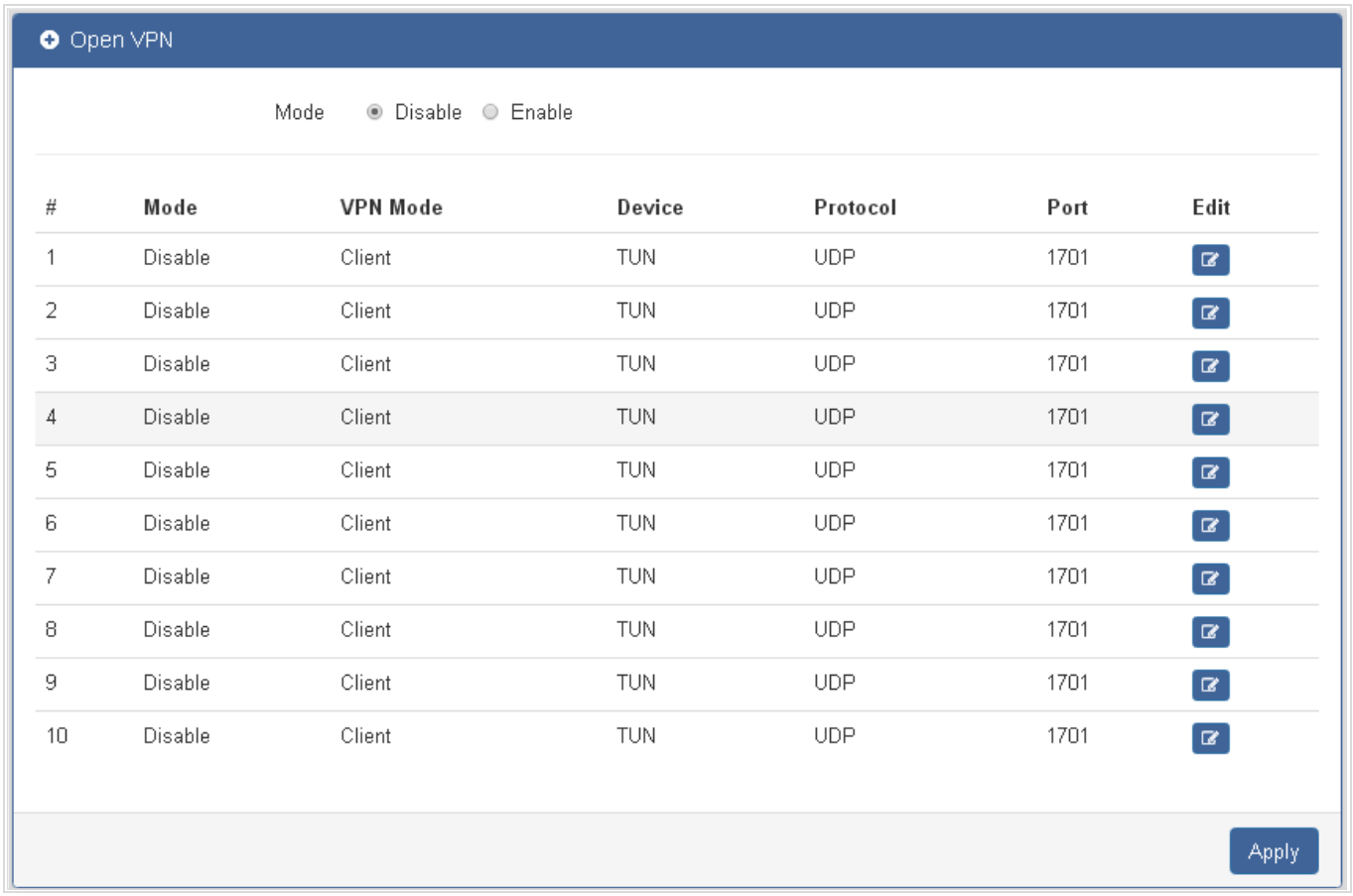


Figure 4-6-1 Open VPN Page Screenshot

The page includes the following fields:

Object	Description
• #	No. of group
• Mode	Shows the current mode.
• VPN Mode	Shows the current VPN mode.
• Device	Shows the current Device.
• Protocol	Shows the current Protocol.
• Port	Shows the current Port.
• Edit	Allows to configure the advance's Open VPN configuation

Buttons

: Click to apply changes.

4.6.1.1 Edit Open VPN Connection

The cellular gateway Open VPN configuation is provided here. The Open VPN screen in Figure 4-6-2 appears. There are three VPN Modes: Server, Client and Customer, which will show in Figure 4-6-3, Figure 4-6-4 and Figure 4-6-5 below.

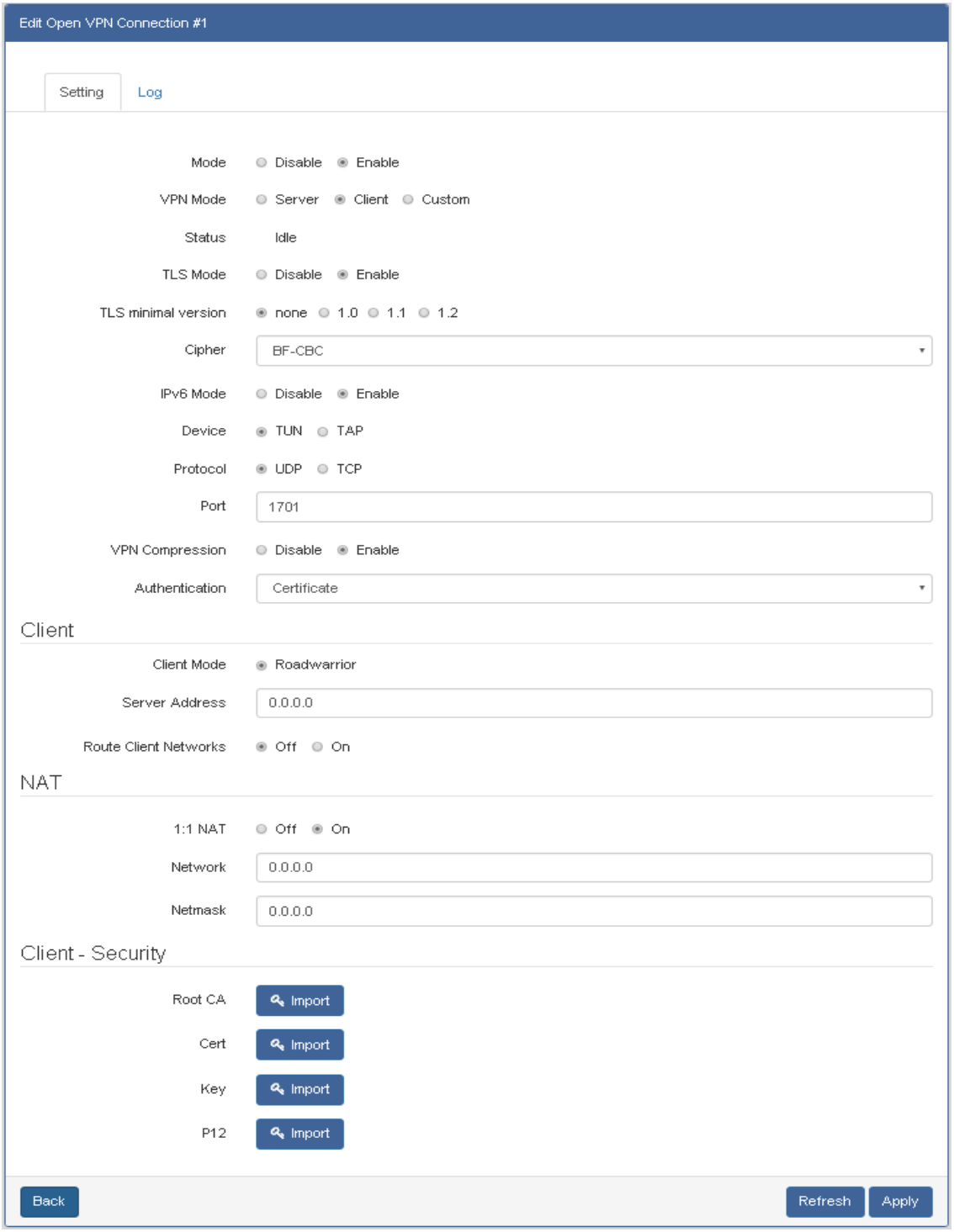


Figure 4-6-2 Open VPN Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the Open VPN configuration. The default is Disable.
• **VPN Mode**	■ Server: Tick to enable OpenVPN server tunnel. ■ Client: Tick to enable OpenVPN client tunnel. The default is Client. ■ Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advanced options to be compatible with other servers.
• **Status**	Display the status of OpenVPN.
• **TLS Mode**	Select from Disable or Enable for data security. The default is Disable.
• **Cipher**	The OpenVPN format of data transmission.
• **IPv6 Mode**	Select from Disable or Enable. The default is Disable.
• **Device**	Select from TUN or TAP. The default is TUN.
• **Protocol**	Select from UDP or TCP Client which depends on the application. The default is UDP.
• **Port**	Enter the listening port of remote side OpenVPN server.
• **VPN Compression**	Select Disable or Enable to compress the data stream. The default is Disable.
• **Authentication**	Select from two different kinds of authentication ways: Certificate or pkcs#12 Certificate. ■ The pkcs#12 option is only available on the VPN client mode.

4.6.1.2 Edit Open VPN Connection – Server Mode

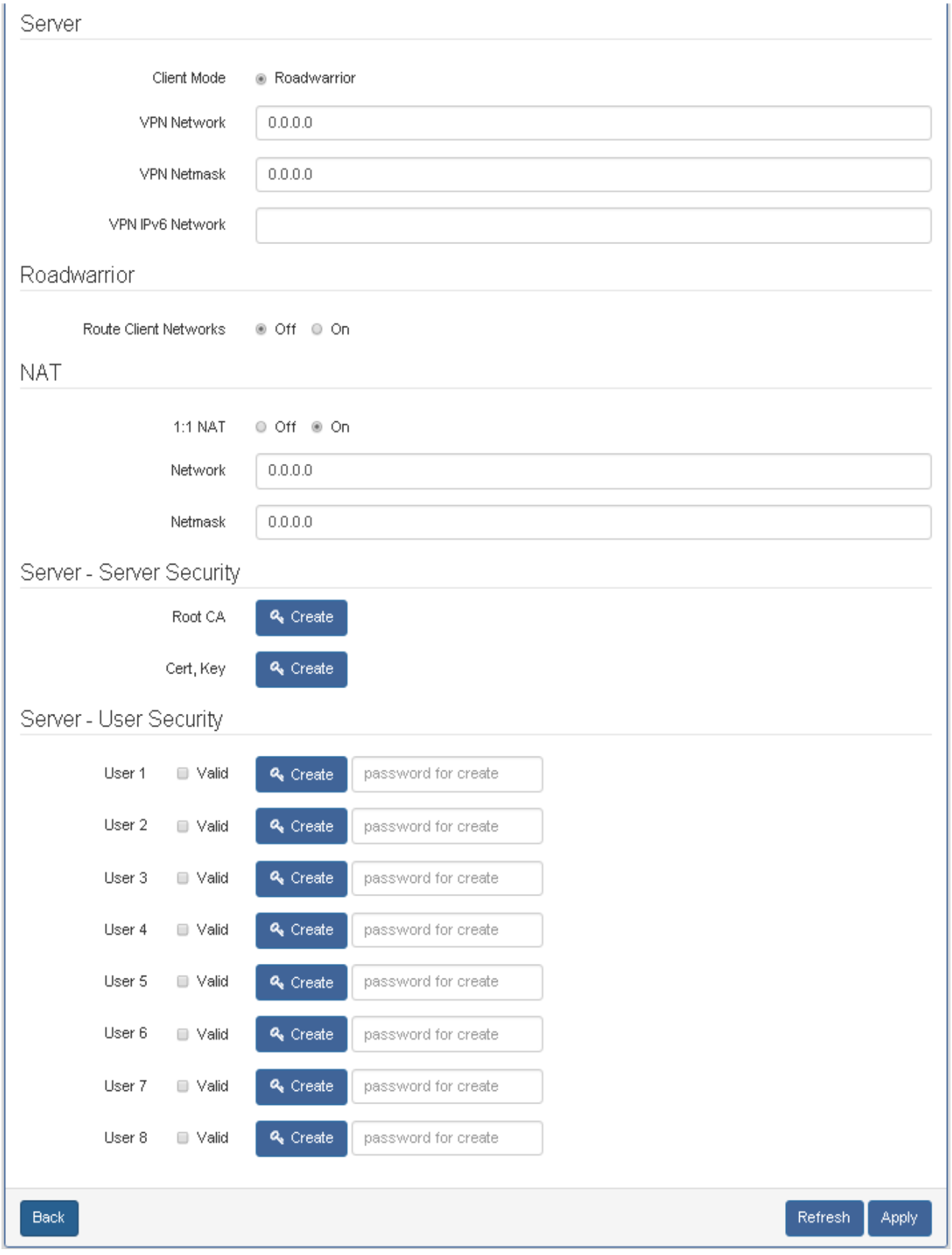


Figure 4-6-3 Open VPN - Server Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Client Mode**	Only support the Roadwarrior mode.
• **VPN Network**	The network ID for OpenVPN virtual network.
• **VPN Netmask**	The netmask for OpenVPN virtual network.
• **Roadwarrior: Route Client Networks**	Select from Off or On. The OpenVPN server will route the client traffic or not. User should fill in the client IP and netmask when this option is enabled.
• **1:1 NAT**	■ Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. ■ Select from Off or On. The default is Off. When two routers' LAN Subnets are the same and create OpenVPN tunnels, this function is turned on.
• **Root CA**	Create Root CA key.
• **Cert, Key and DH**	Create Cert, Key and DH key.
• **User 1 - User 8**	According to your requirement, you can create different kinds of user security keys from User 1 to User 8.

4.6.1.3 Edit Open VPN Connection – Client Mode

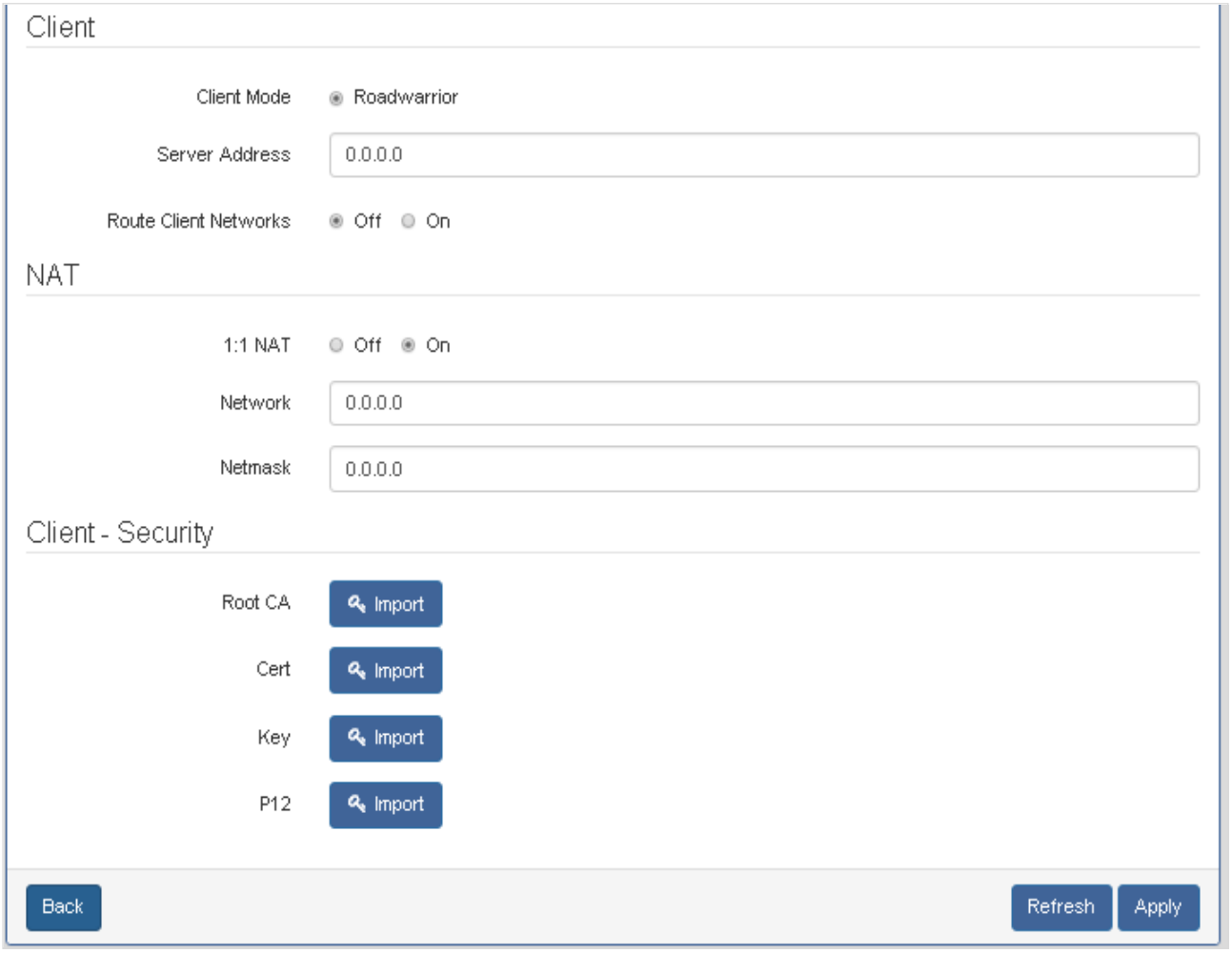


Figure 4-6-4 Open VPN - Client Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Client Mode**	Only support the Roadwarrior mode.
• **Server Address**	Fill in WAN IP of OpenVPN server.
• **Route Client Networks**	Select from Off or On. This setting needs to match the server side. When enabled, the mobile router will auto apply the properly routing rules.
• **1:1 NAT**	■ Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment. ■ Select from Off or On. The default is Off. When two routers' LAN Subnets are the same and create OpenVPN tunnels, this function is turned on.
• **Root CA**	The Certificate Authority file of OpenVPN server could be downloaded from OpenVPN server.
• **Cert**	The certification file is for OpenVPN client, which could be downloaded from OpenVPN

	server.
• **Key**	The private key file is for OpenVPN client, which could be downloaded from OpenVPN server.
• **P12**	The PKCS#12 file is for OpenVPN client, which could be downloaded from OpenVPN server.

4.6.1.4 Edit Open VPN Connection – Custom Mode

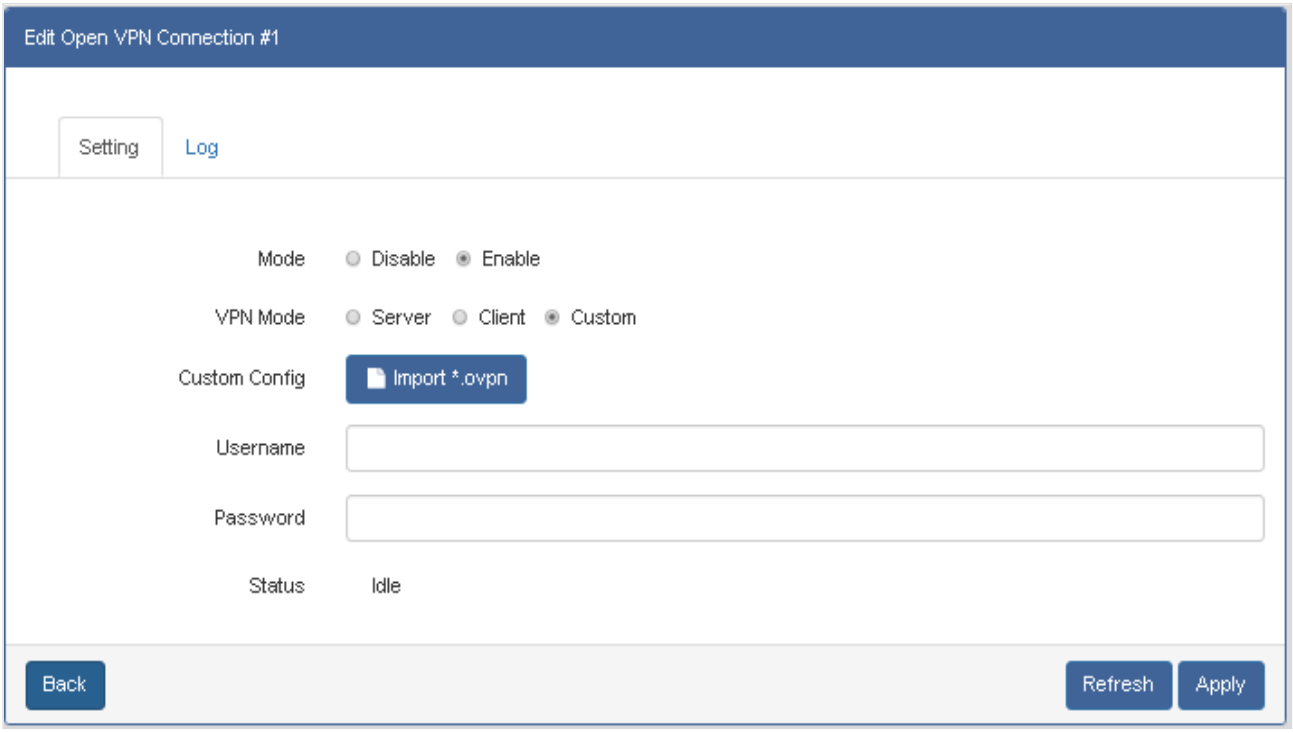


Figure 4-6-5 Open VPN - Custom Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the Open VPN configuration. The default is Disable.
• **VPN Mode**	■ Server: Tick to enable OpenVPN server tunnel. ■ Client: Tick to enable OpenVPN client tunnel. The default is Client. Custom: This option allows user to use the .ovpn configuration file to quickly set up VPN tunnel with third-party server or use the OpenVPN advanced options to be compatible with other servers.
• **Custom Config**	Allows to inport third party of VPN Server's .opvn file.
• **Username**	Fill in the username if the imported file has already set up the username.
• **Password**	Fill in the password if the imported file has already set up the password.
• **Status**	Display the connection status of OpenVPN, such as IP address and the connected time.

Buttons

: Click to apply changes.

: Click to go back to previous configuration page.

: Click to refresh the status.

4.6.2 IPSec

Internet Protocol Security (**IPsec**) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

4.6.2.1 General Setting

The cellular gateway IPSec configuation is provided here. The IPSec – General Setting screen in Figure 4-6-6 appears.

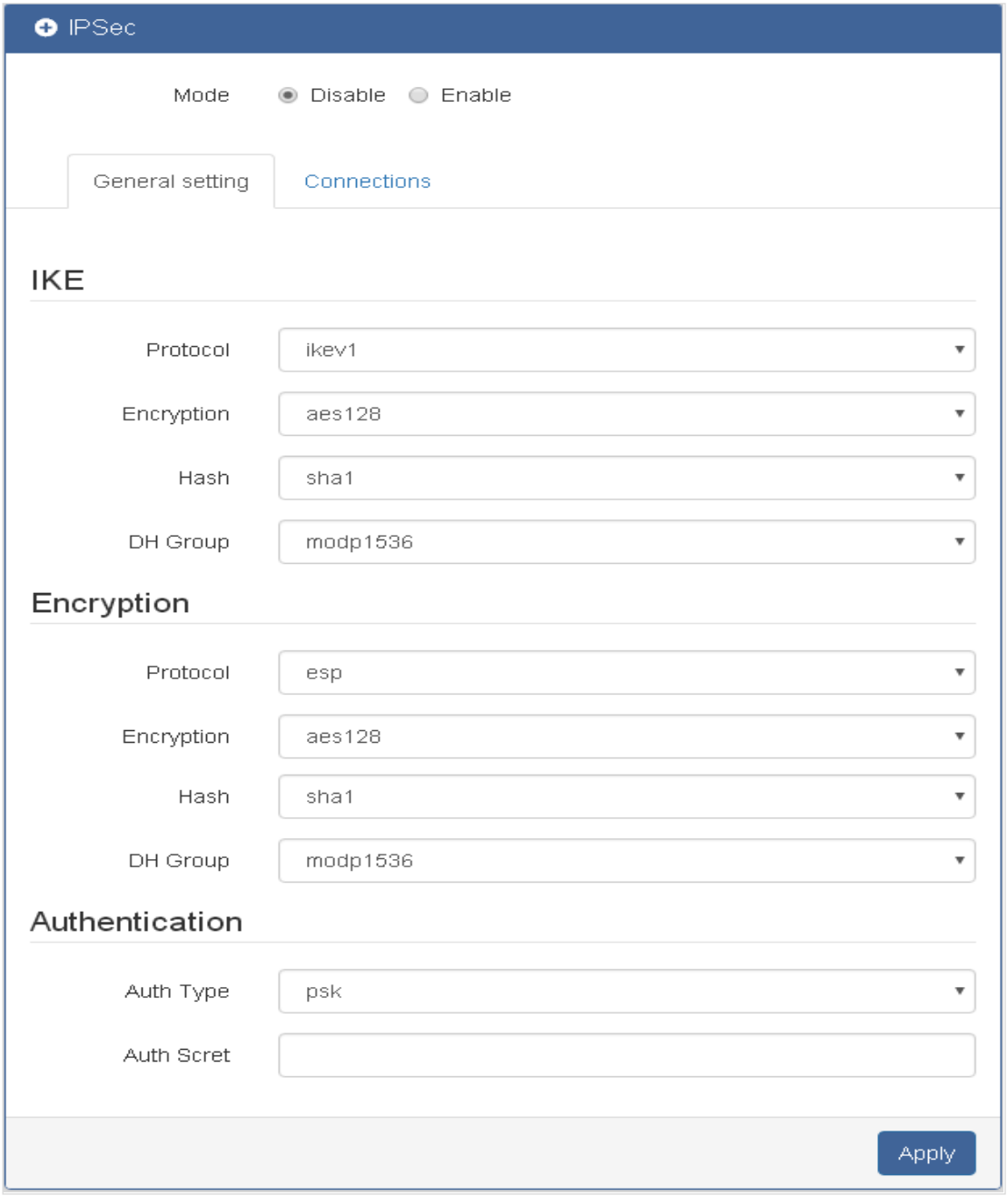


Figure 4-6-6 IPSec – General Setting Configuration Page Screenshot

The page includes the following fields:

Object	Description
• Mode	**Disable or Enable** the IPSec configuration. The default is Disable.
Object - IKE	**Description**
• Protocol	Select from ikev1 or ikev2.
• Encryption	Select from aes128 (default), aes192, aes256 or 3des.
• Hash	Select from sha1 (default), md5 or sha256.
• DH Group	Select from modp1536 (default)、modp768、modp1024、modp2048、modp3072、modp4096、modp6144 or modp8192.
Object - Encryption	**Description**
• Protocol	Select from esp or aes128.
• Encryption	Select from aes128 (default), aes192, aes256 or 3des.
• Hash	Select from sha1 (default), md5 or sha256.
• DH Group	Select from modp1536 (default), modp768, modp1024, modp2048, modp3072, modp4096, modp6144 or modp8192.
Object - Authentication	**Description**
• Auth Type	Select from psk or rsa.
• Auth Scret	The password is for psk authentication type.

Buttons

Apply: Click to apply changes.

4.6.2.2 Connections

The cellular gateway IPSec configuation is provided here. The IPSec – Connections screen in Figure 4-6-7 appears.

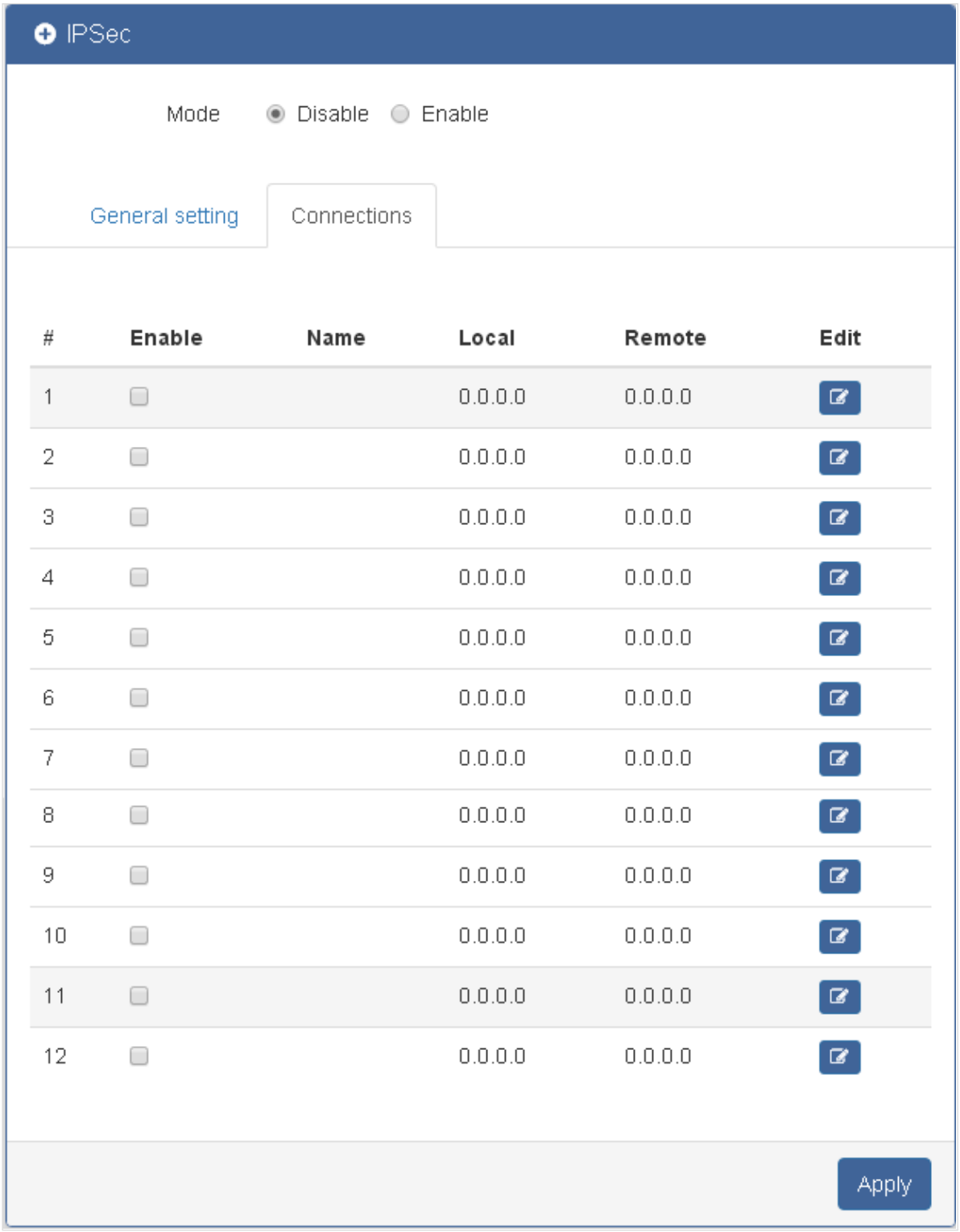


Figure 4-6-7 IPSec – Connections Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **#**	No. of group
• **Enable**	Tick to Enable IPSec Connections group.

• **Name**	Shows the current Name of connection.
• **Local**	Shows the current Local IP Address.
• **Remote**	Shows the current Remote IP Address.
• **Edit**	Allows to configure the advance's IPSec - Connections configuration

Buttons

Apply: Click to apply changes.

4.6.2.3 Edit IPSec Connections

The cellular gateway IPSec configuration is provided here. The Edit IPSec Connections screen in Figure 4-6-8 appears.

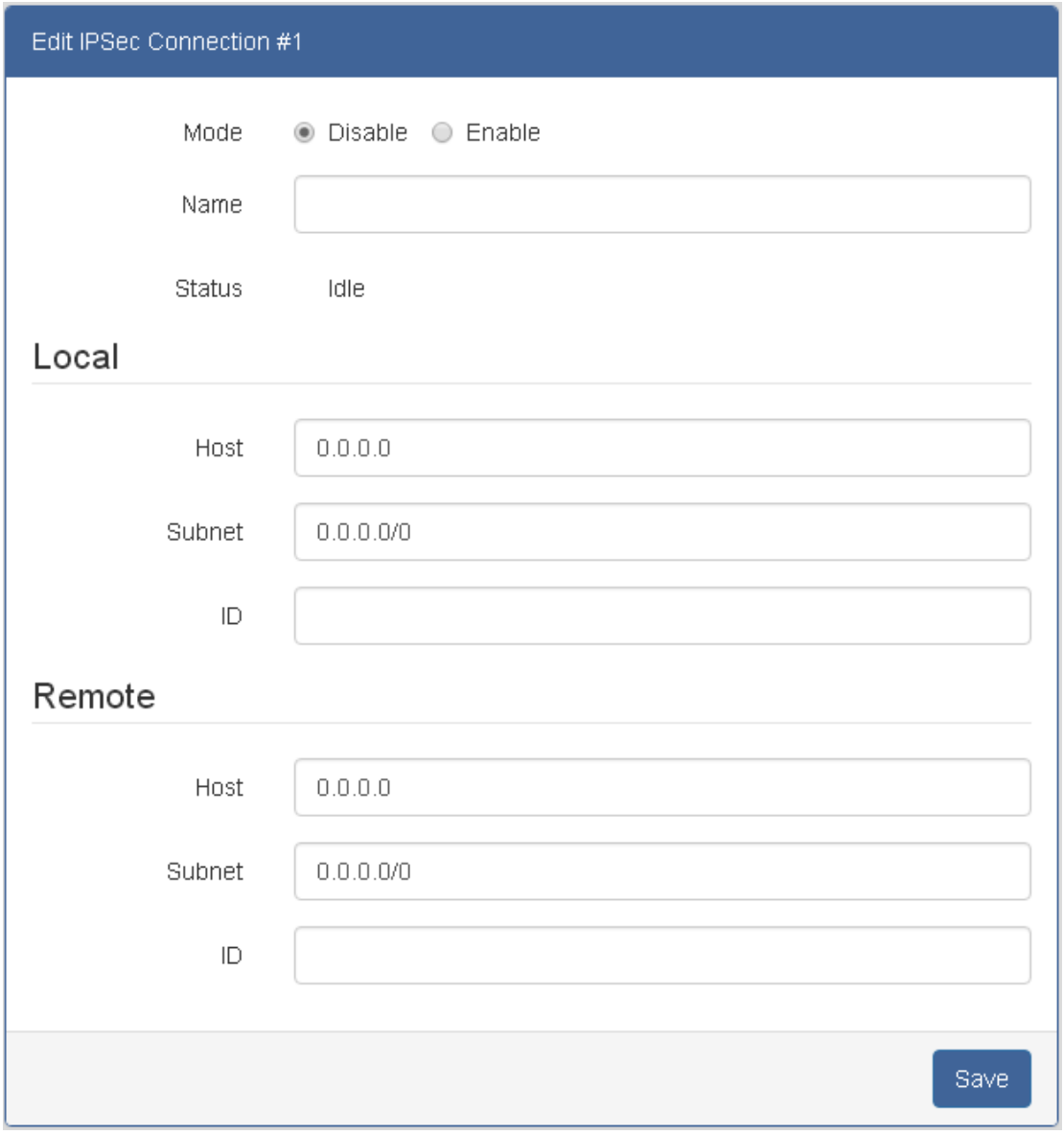


Figure 4-6-8 Edit IPSec Connections Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IPSec Connections configuration. The default is Disable.
• **Name**	Fill in the name of IPSec Tunnel.
• **Status**	Display the connection status of IPSec.
Object – Local	**Description**
• **Host**	Fill in the WAN IP of mobile router.
• **Subnet**	Fill in the subnet for the LAN of mobile router.
• **ID**	The connection ID of IPSec local side.
Object – Remote	**Description**
• **Host**	Fill in the granted remote IP. If no limitation, keep it blank.
• **Subnet**	Fill in the granted remote subnet. If no limitation, keep it blank.
• **ID**	The connection ID of IPSec Remote side.

Buttons

: Click to save changes.

4.6.2.4 Setting X.509 Certificates

The cellular gateway IPSec configuration is provided here. The X.509 Certificates screen in Figure 4-6-9 appears.

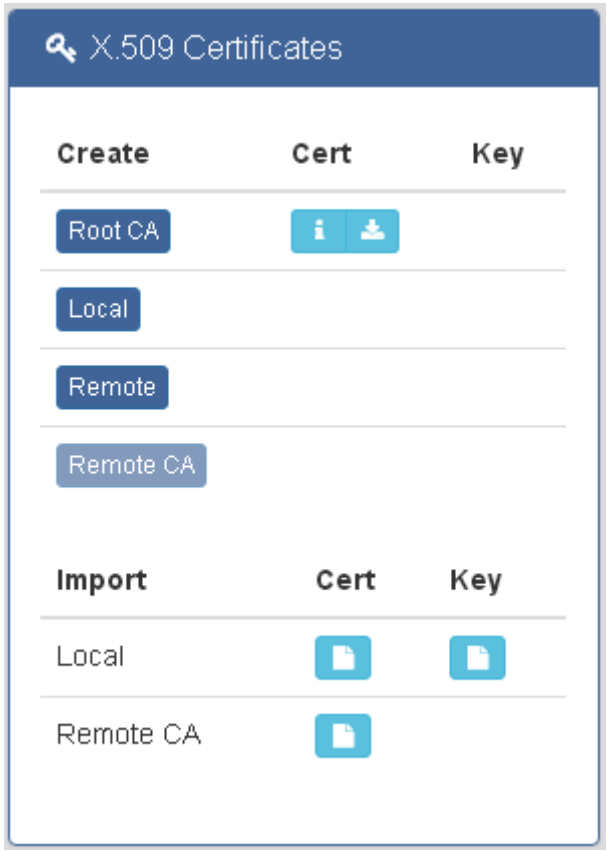


Figure 4-6-8 X.509 Certificates Configuration Page Screenshot

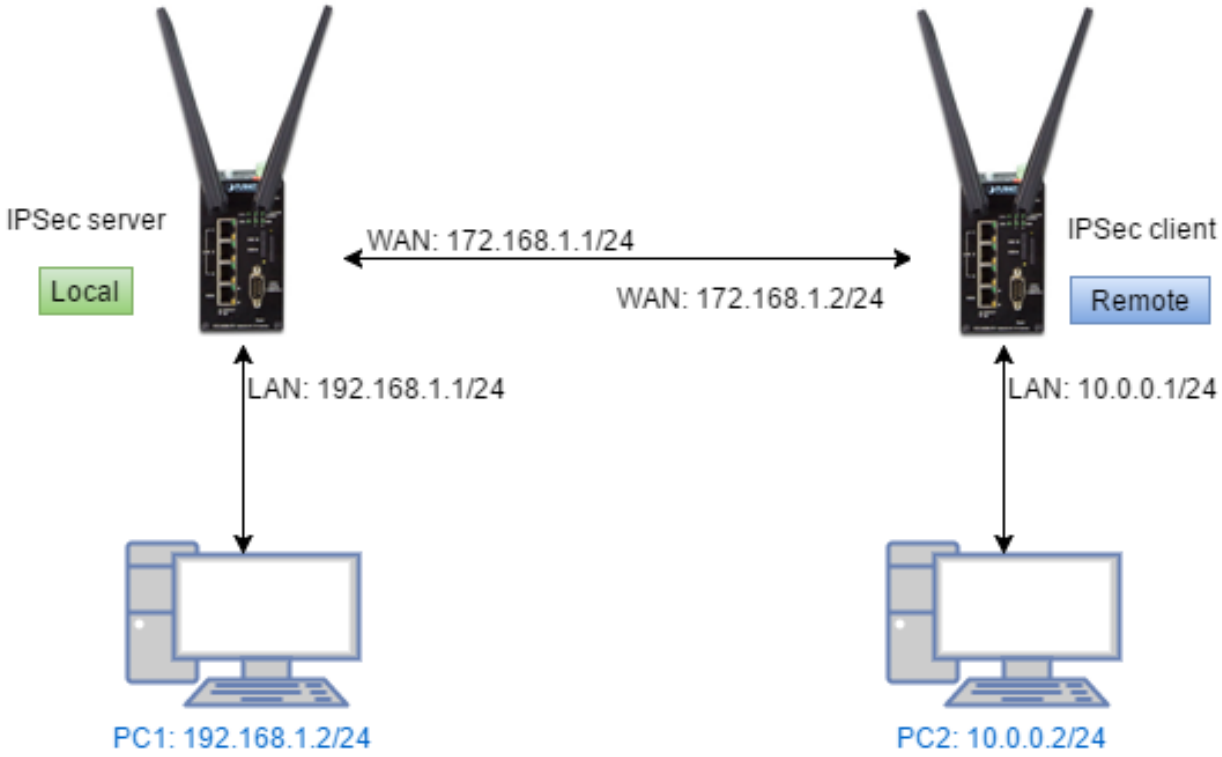
The interface shows the setting items of X.509 Certificates.

- You need to create the IPSec Security Keys by clicking the Create button, including Root CA, Local, Remote and Remote CA. For example, to create Root CA file, click the Root CA button.
- For the IPSec connection, the client should set up properly Root CA, Local, Remote and Remote CA key and cert files. The files could be downloaded by clicking the Download button after the file generated.

You can import the files of local and remote CA from the server.

4.6.2.5 Example of IPSec Net-to-Net configuration

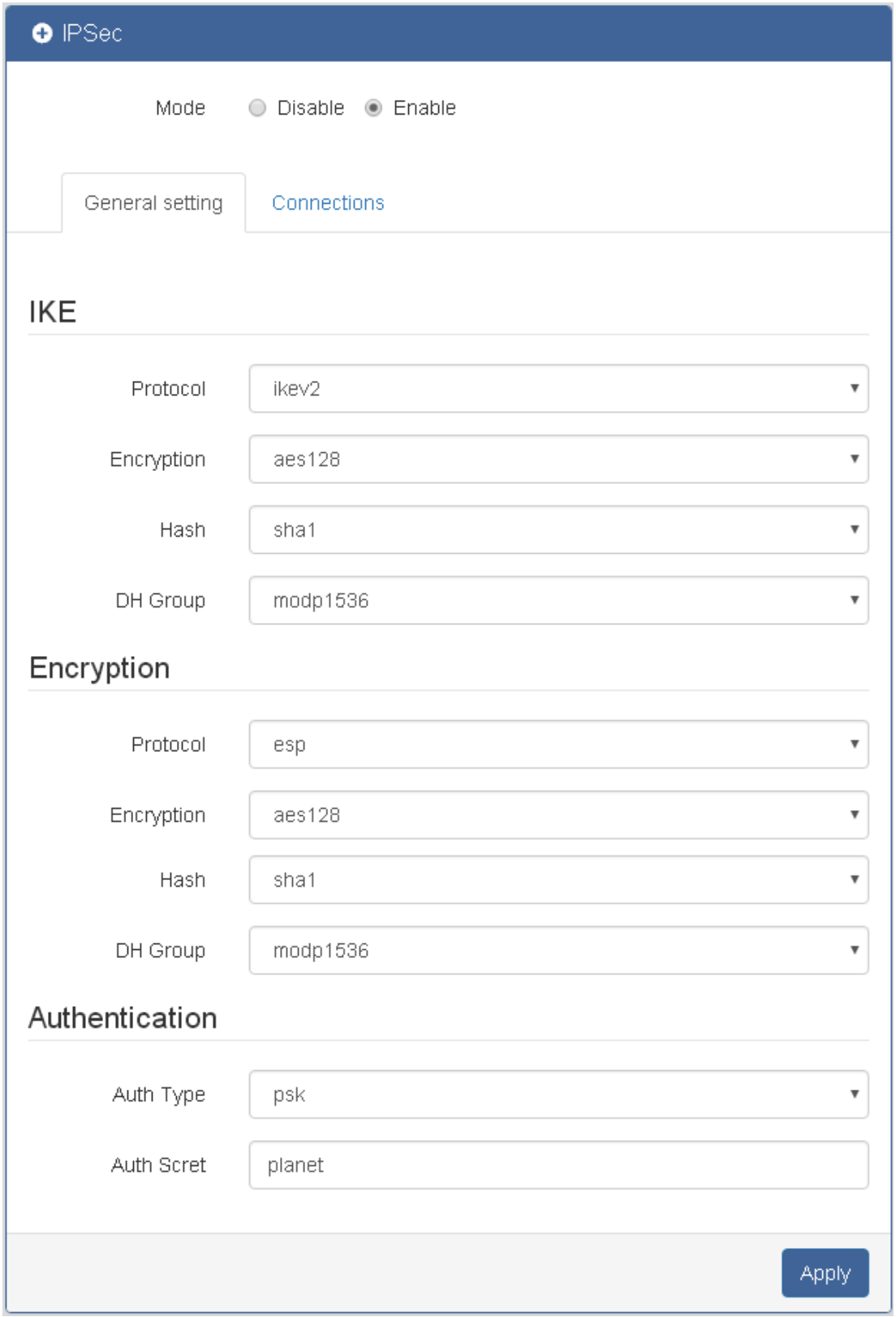
In this case, the IPSec VPN tunnel uses the two LAN side subnet clouds and makes them communicate each other. There are two settings for the Cellular Gateway IPSec feature.



General setting

The first part is the general setting. It provides the IPSec basic setting and authentication configuration. The psk (Pre-shared key) is as an authentication option to simplify the progress.

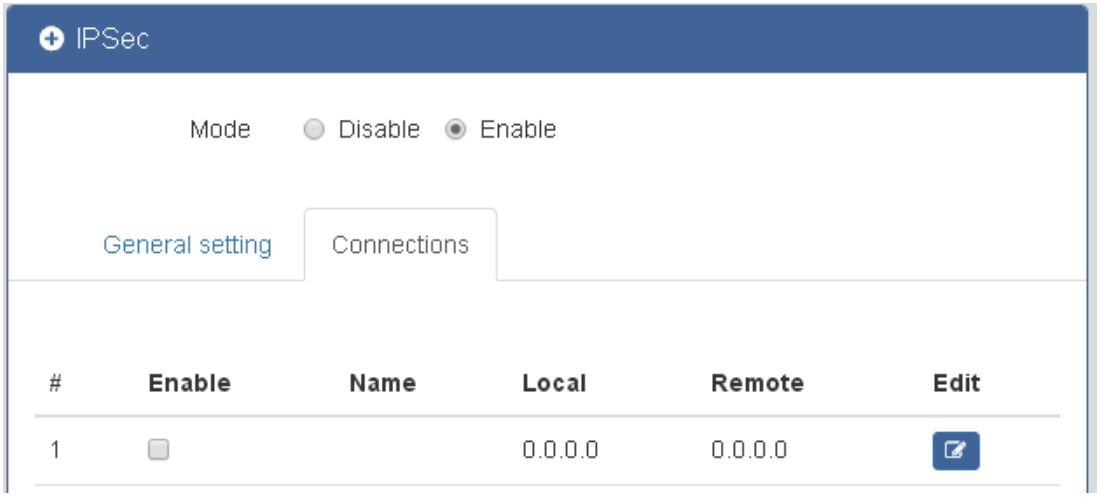
The general setting for the local and remote sides should be used the same setting.



Connections Setting

The second part is the connection setting. You can configure the local and the remote side settings for each connection.

For the Net-to-Net scenario, you can configure the information of **Host**, **Subnet** and **ID** for the local and remote side. In this case, the #1 connection is edited from connections tab for setting up the Net-to-Net configuration.



■ Local Side

First, fill out the local Host and Subnet fields by the network information of IPSec server.

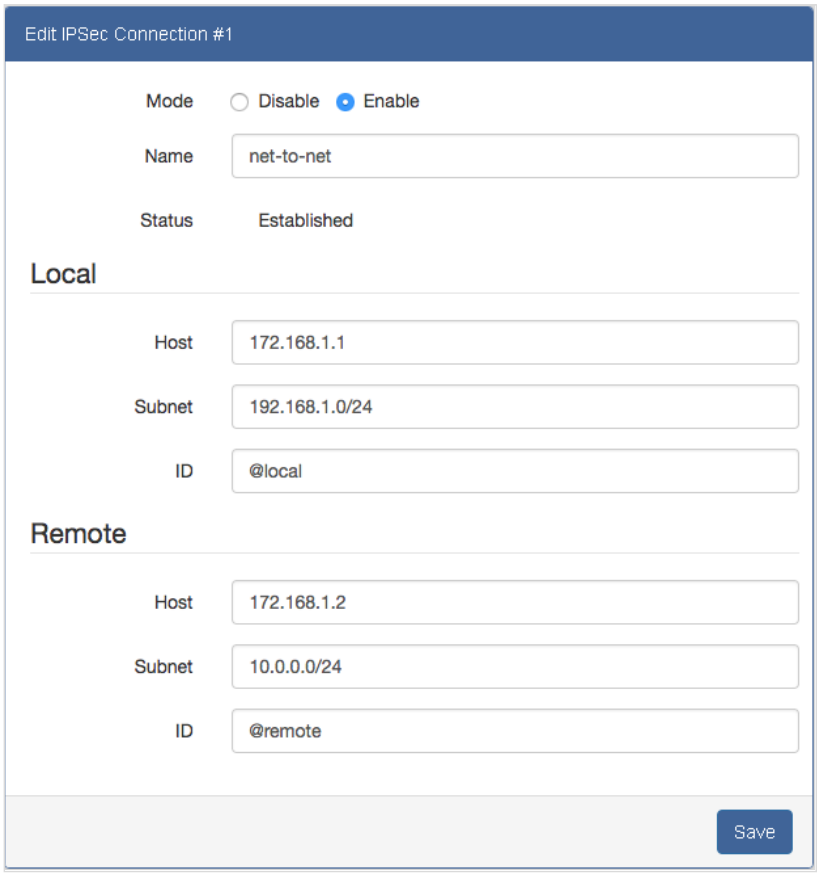
And, use the network information of IPSec client to fill out the remote setting.

Then, specify the ID for both sides.

In this case, the IDs for the local and remote side are named as @local and @remote respectively.

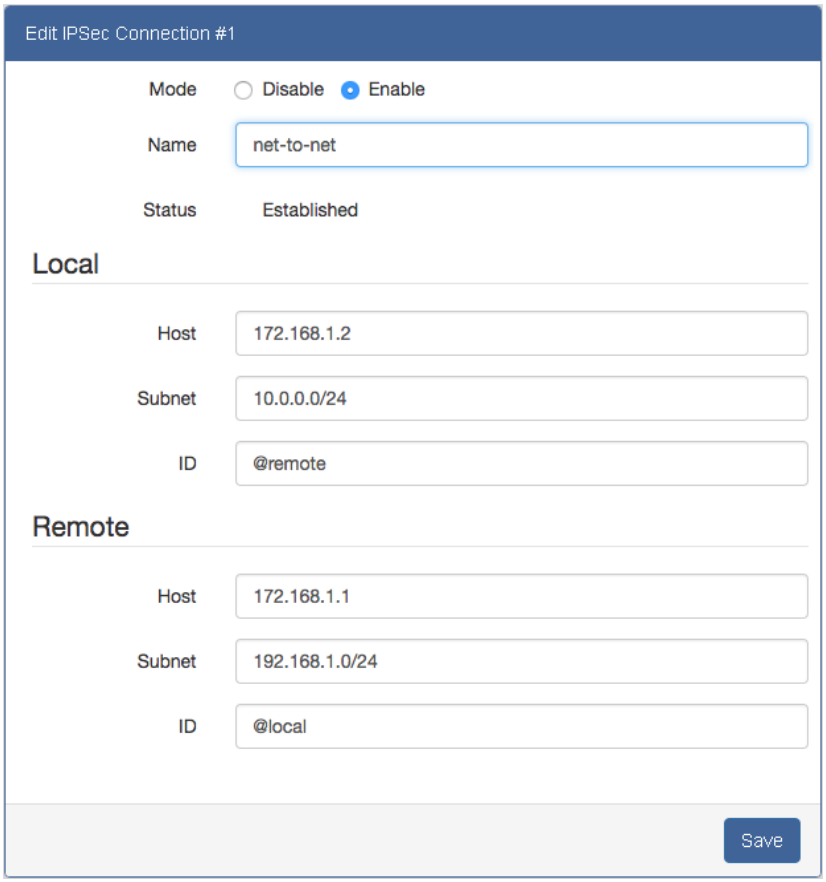
Note

The ID should be started with @ symbol. The above settings will make the traffic between 192.168.1.0/24 and 10.0.0.0/24. They can be forwarded by IPSec tunnel.



■ Remote Side

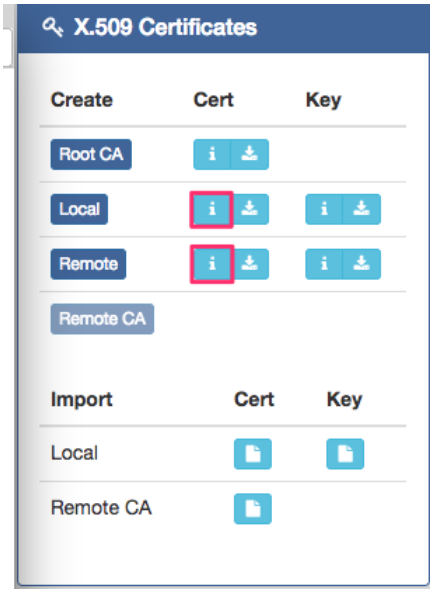
The setting for remote side is similar to Local Side. Just swap the local settings with the remote setting.

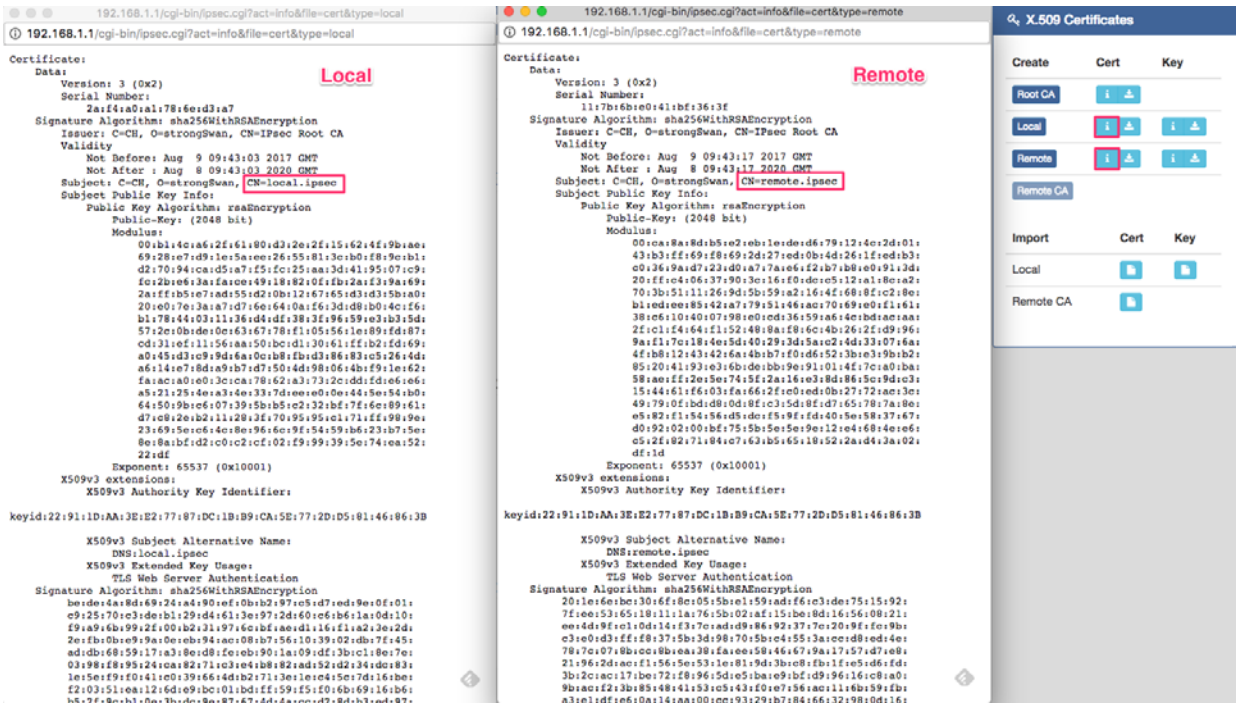


Net-to-Net (Pre-shared key)

When the **rsa** authentication is used, there will have some differences with psk. In the **rsa** authentication, the **id** of connections is corresponded with the certificate **CN** field for the both sides.

For the Cellular Gateway IPSec certificate generation, it generates the local and remote side certificates with **@local.ipsec** and **@remote.ipsec**. (The certificate information can be queried by the information button.)





Import Certificate

For the IPSec remote side, it requires the certificates from local side to authenticate the IPSec connection. Thus, you need to download the Root CA, remote cert and key from local side. And, import them to the remote side.

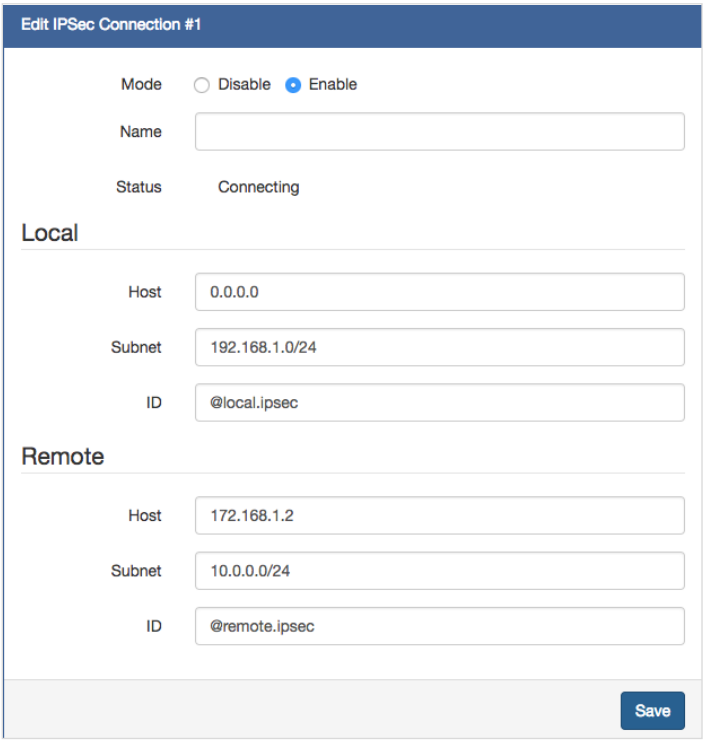
The mapping is shown below:

1. Root CA (Local side) -> Import Remote CA (Remote side)
2. Remote Cert (Local side) -> Import Local Cert (Remote side)
3. Remote Key (Local side) -> Import Local Key (Remote side)

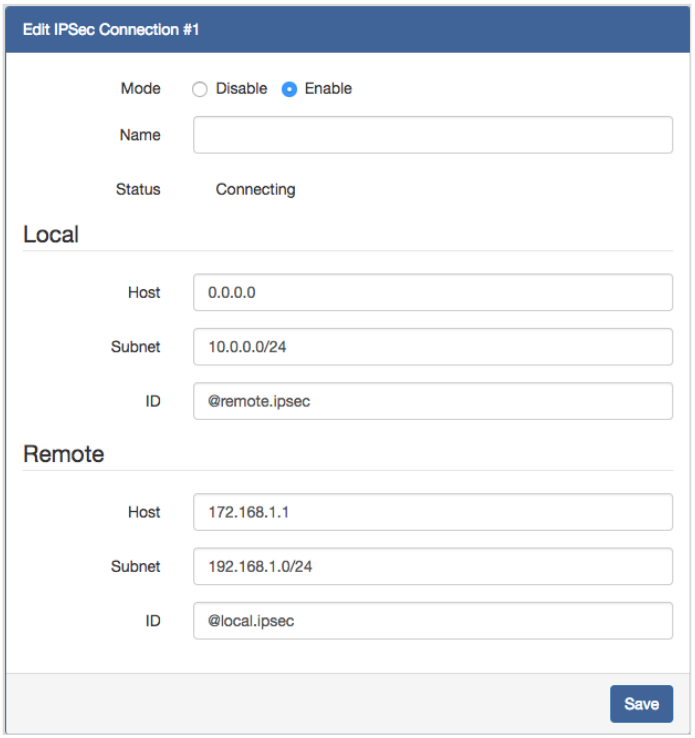
For Connection setting, the mapping of connection IDs is like the following table.

Certificate	IPSec local side	IPSec remote side
Local	@local.ipsec	@remote.ipsec
Remote	@remote.ipsec	@local.ipsec

Local Side



Remote Side



4.6.3 Port Forwarding

Port Forwarding is an application of network address translation (NAT) that redirects a communication request from one address andport number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host. The Port Forwarding screen in Figure 4-6-9 appears.

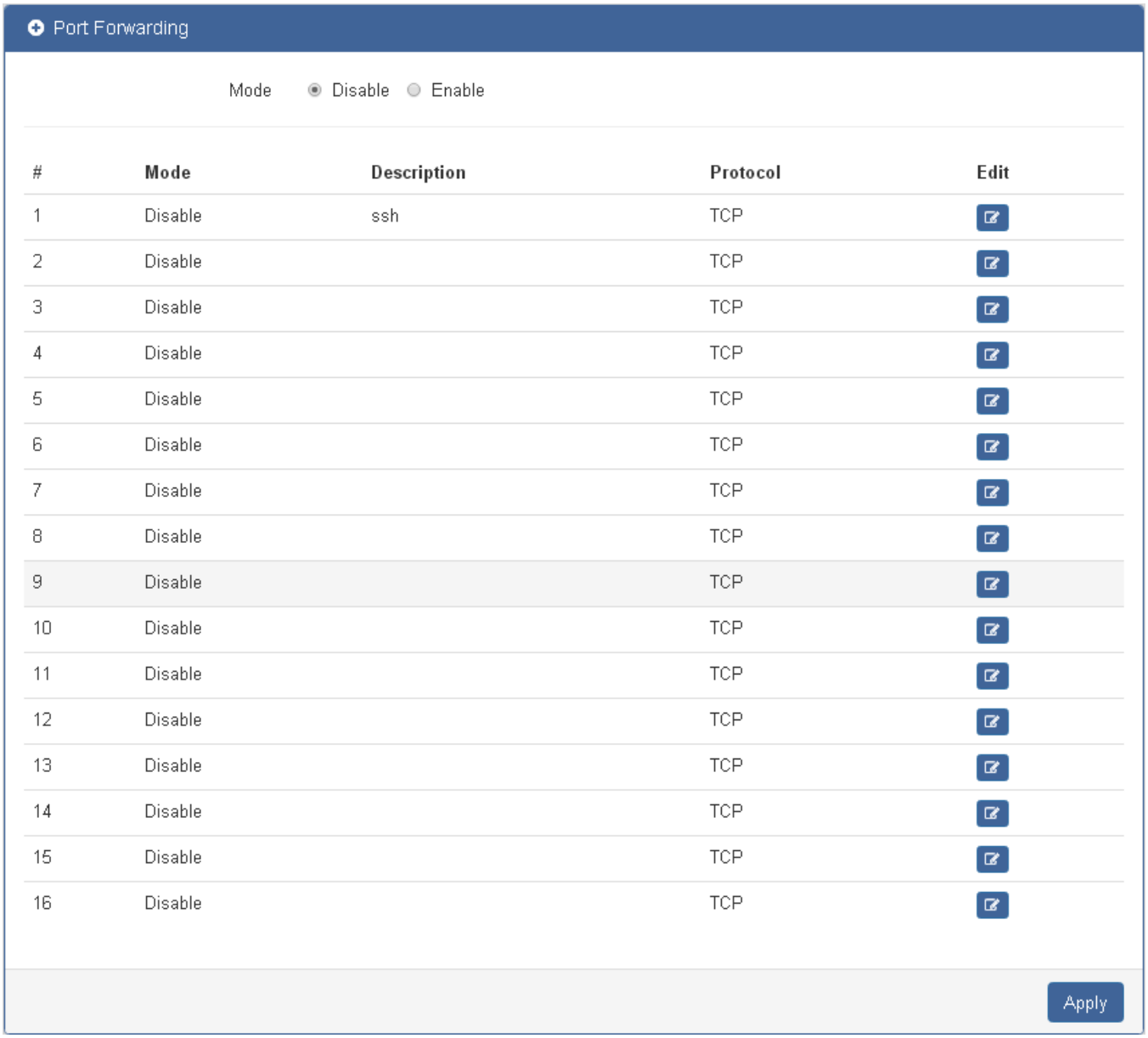


Figure 4-6-9 Port Forwarding Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IPSec Connections configuration. The default is Disable.
• **#**	No. of group
• **Mode**	Shows the current Mode.
• **Description**	Shows the per group description.
• **Protocol**	Shows the current use of protocol.
• **Edit**	Allows to configure the advance's port forwarding configuation

Buttons

Apply: Click to apply changes.

4.6.3.1 Edit Port Forwarding Entry

The cellular gateway Port Forwarding configuation is provided here. The IPSec – Edit Port Forwarding Entry screen in Figure 4-6-10 appears.

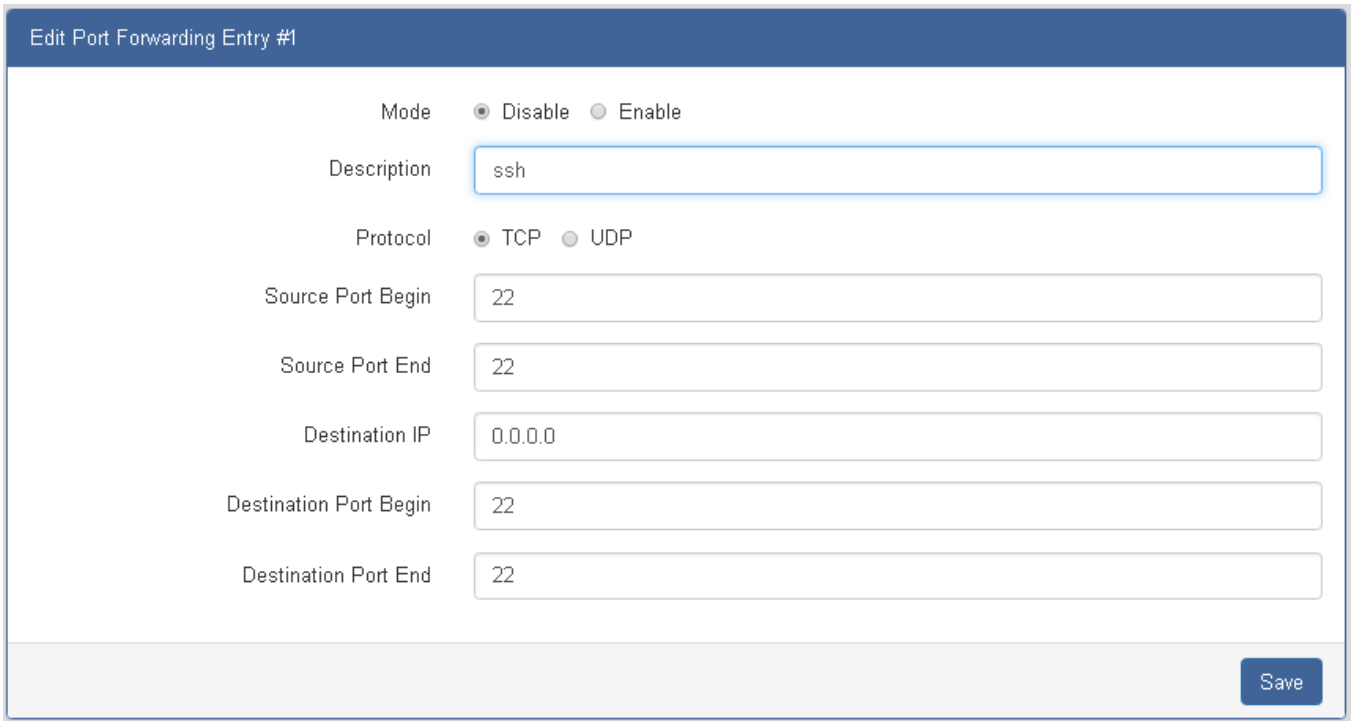


Figure 4-6-10 Edit Port Forwarding Entry Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the port forwarding configuration. The default is Disable.
• **Description**	Describe the name of Port Forwarding.
• **Protocol**	Select from UDP or TCP Client which depends on the application.
• **Source Port Begin**	Fill in the beginning of source port.
• **Source Port End**	Fill in the end of source port.
• **Destination Port Begin**	Fill in the beginning of private destination port.
• **Destination Port End**	Fill in the end of private destination port.
• **Description**	Fill in the current private destination IP.

Buttons

: Click to save changes.

4.6.4 Dynamic DNS

The cellular gateway Dynamic DNS configuation is provided here. The Dynamic DNS screen in Figure 4-6-11 appears.

Figure 4-6-11 Dynamic DNS Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IPSec Connections configuration. The default is Disable.
• **Service Provider**	Select the Service Provider of Dynamic DNS.
• **Host Name**	Fill in your registered Host Name from Service Provider.
• **Token ID**	Fill in your Token ID from Service Provider.
• **Host Secret ID**	Fill in your Secret ID from Service Provider.
• **Username**	Fill in your registered username from Service Provider.
• **Password**	Fill in your registered password from Service Provider.
• **Update Period Time (Sec)**	Fill in "0" to mean 30 days.

Buttons

Apply: Click to apply changes.

4.6.5 DMZ

The cellular gateway DMZ configuation is provided here. The DMZ screen in Figure 4-6-12 appears.

Figure 4-6-12 DMZ Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IPSec Connections configuration. The default is Disable.
• **Host IP Address**	Fill in your Host IP Address.

Buttons

Apply: Click to apply changes.

4.6.6 SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

4.6.6.1 Community

The cellular gateway SNMP configuation is provided here. The SNMP – Community screen in Figure 4-6-13 appears.

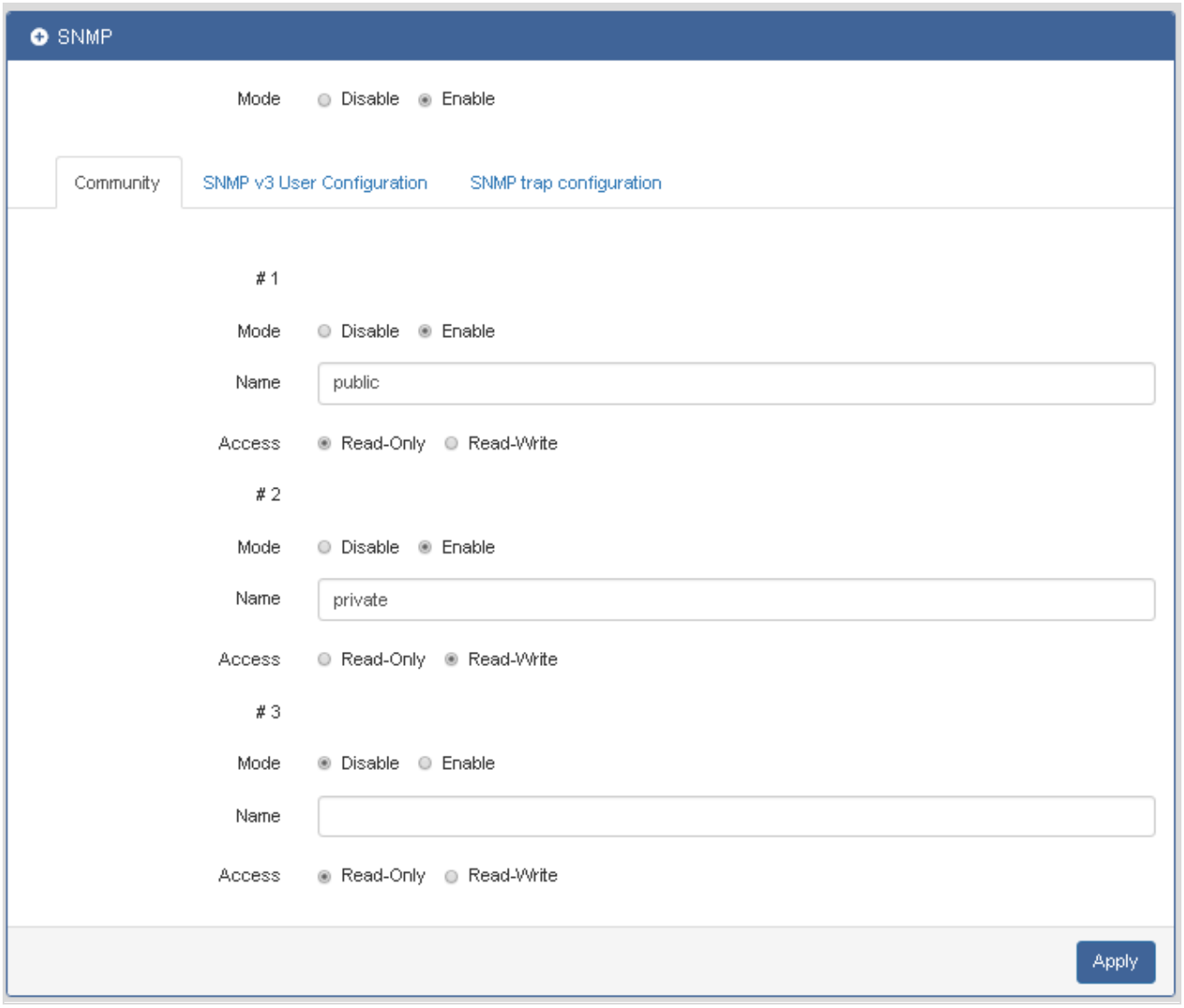


Figure 4-6-13 Community Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the SNMP configuration. The default is Enable.

• **Community**	Configure community setting with three options, including # 1and # 2.
• **Mode**	**Disable or Enable** the # 1 and # 2 configuration. The default is Disable.
• **Name**	Name each community.
• **Access**	Select from Read-Only or Read-Write.

Buttons

Apply: Click to apply changes.

4.6.6.2 SNMPv3 User Configuration

The cellular gateway SNMP configuration is provided here. The SNMP v3 screen in Figure 4-6-14 appears.

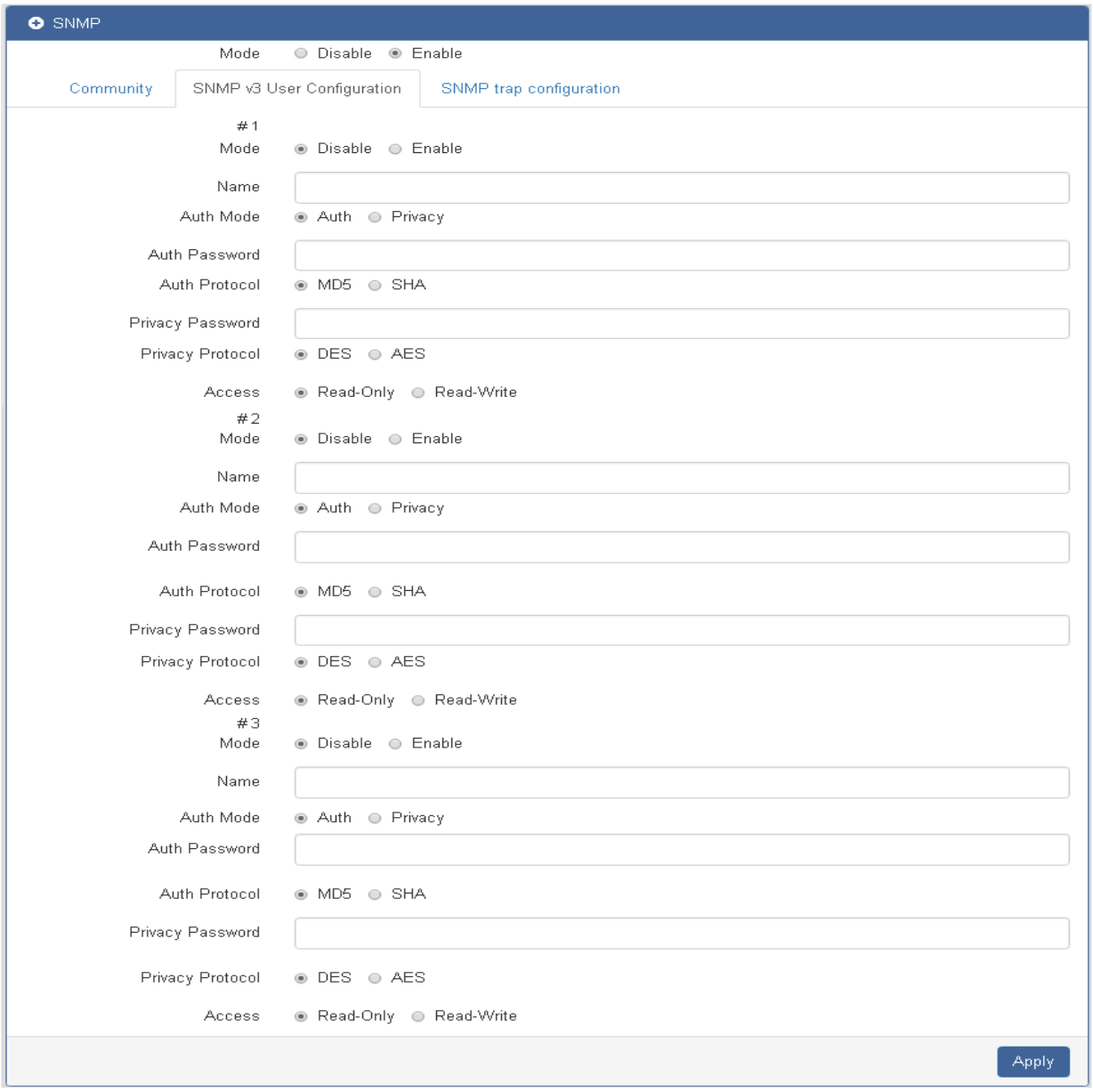


Figure 4-6-14 SNMP v3 Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the SNMP configuration. The default is Enable.
• **Name**	Fill in your name.
• **Auth Mode**	Select from Authentication or Privacy.
• **Authentication Password**	Fill in your authentication password.
• **Authentication Protocol**	Select from MD5 or SHA.
• **Privacy Password**	Fill in your privacy password.
• **Privacy Protocol**	Select from DES or AES.
• **Access**	Select from Read-Only or Read-Write.

Buttons

Apply: Click to apply changes.

4.6.6.3 SNMP Trap Configuration

The cellular gateway SNMP configuation is provided here. The SNMP trap configuration screen in Figure 4-6-15 appears.

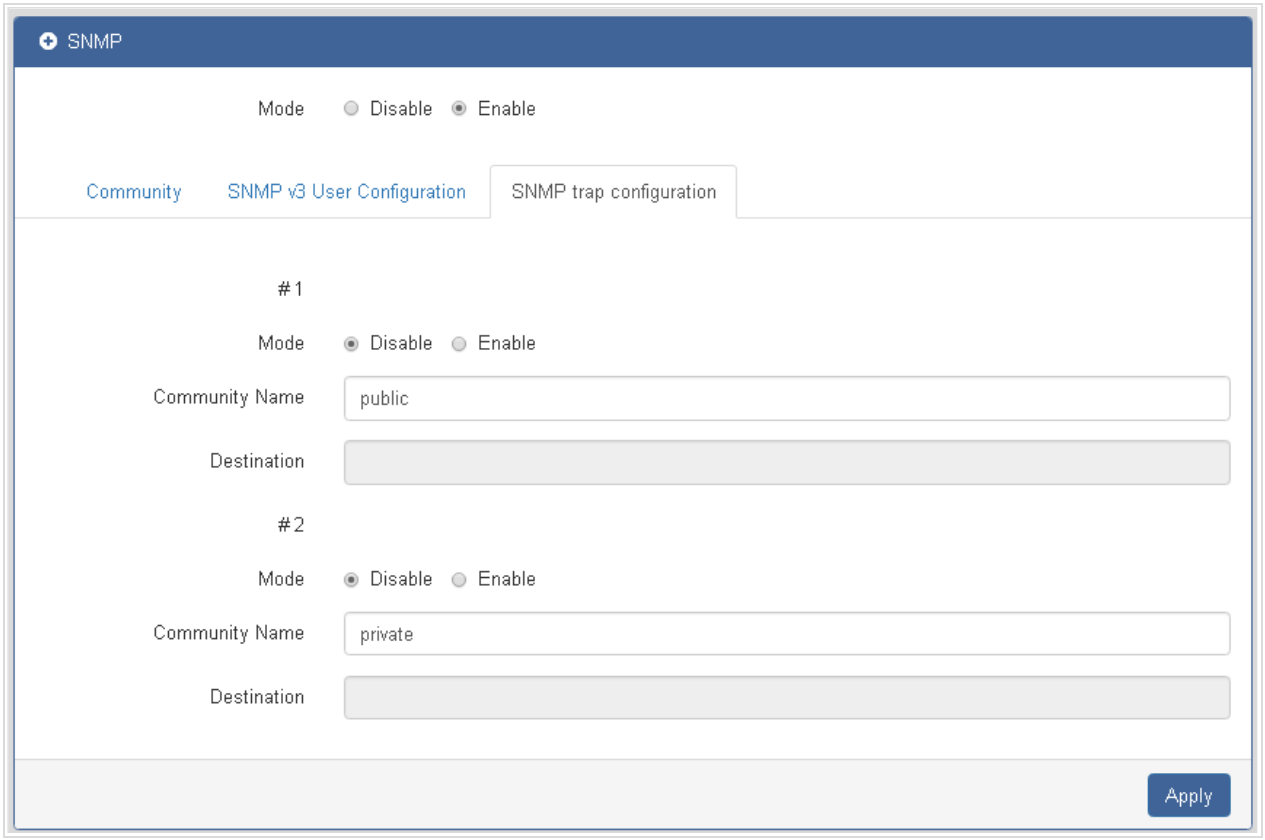


Figure 4-6-15 SNMP Trap Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the SNMP configuration. The default is Enable.
• **Mode**	**Disable or Enable** the # 1 and # 2 configuration. The default is Disable.
• **Community Name**	Fill in your community name.
• **Destination**	The destination (domain name/IP) of remote SNMP trap server.

Buttons

Apply: Click to apply changes.

4.6.7 TR069

TR-069 (Technical Report 069) is a technical specification that defines an application layer protocol for remote management of end-user devices. The cellular gateway TR069 configuation is provided here. The TR069 screen in Figure 4-6-16 appears.

Figure 4-6-16 TR069 Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the SNMP configuration. The default is Disable.
• **ACS URL**	Fill in the URL address of ACS (Auto-Configuration Server).
• **ACS Username**	Fill in the ACS username to authenticate the CPE (this cellular gateway) when connecting to the ACS.
• **ACS Password**	Fill in the ACS password to authenticate the CPE (this cellular gateway) when connecting to the ACS.
• **Periodic Inform**	Select from Disable or Enable. The default is Disable. The CPE reports the status to the ACS when enabling a period of time set.
• **Periodic Inform Interval (Sec)**	Fill in the periodic time. The CPE reports to ACS the status according to your duration in seconds of the interval set.
• **Connection Request Username**	Fill in the connection request username to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.
• **Connection Request Password**	Fill in the connection request password to authenticate the ACS if the ACS attempts to communicate with the CPE connecting.

Buttons

Apply: Click to apply changes.

4.6.8 IP Filter

The cellular gateway IP Filter configuation is provided here. The IP Filter screen in Figure 4-6-17 appears.

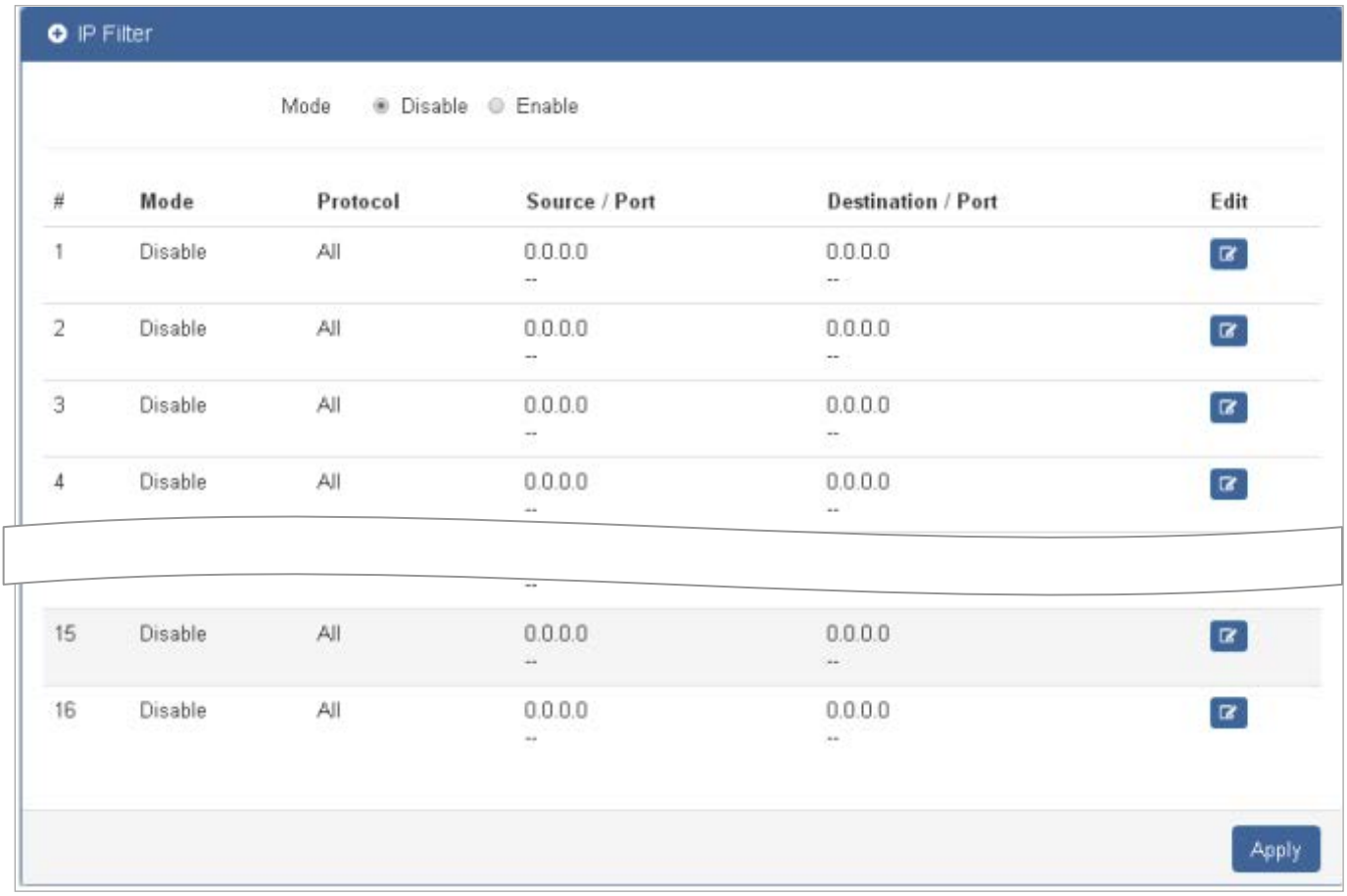


Figure 4-6-17 IP Filter Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IP Filter configuration. The default is Disable.
• **#**	No. of Group
• **Mode**	Shows the current mode.
• **Protocol**	Shows the current setting of protocol.
• **Source / Port**	Shows the current setting of source IP and port.
• **Destination / Port**	Show sthe current setting of destination IP and port.
• **Edit**	Allows to configure the IP Filter configuation

Buttons

Apply: Click to apply changes.

4.6.8.1 Edit IP Filter Black List Entry

The cellular gateway IP Filter configuation is provided here. The Edit IP Filter Black List Entry screen in Figure 4-6-18 appears.
When selecting Enable Mode, the protocol is TCP. The source IP has IPv4 and IPv6 setting formats.
For Source IP, there are three types to input your source IP that depends on your requirement, including single IP, IP with Mask or giving a range of IP. The following table provides some examples.

IP Format	Single IP	IP with Mask	Ranged IP
IPv4	192.168.0.123	192.168.1.0/24 192.168.1.0/255.255.255.	192.168.1.1-192.168.1.123
IPv6	2607:f0d0:1002:51::4	2607:f0d0:1002:51::0/64	2607:f0d0:1002:51::4- 2607:f0d0:1002:51::aaaa

Note

To set up a range of IP, please use "**–**" (hyphen symbol) to mark your ranged IP.

For Source Port, there are two types to input your source port that depends on your requirement, including single port (e.g.1234) or giving a range of ports (e.g.1234:5678).

Note

Setting up a range of source ports, please use "**:**" (colon symbol) to mark your ranged ports.

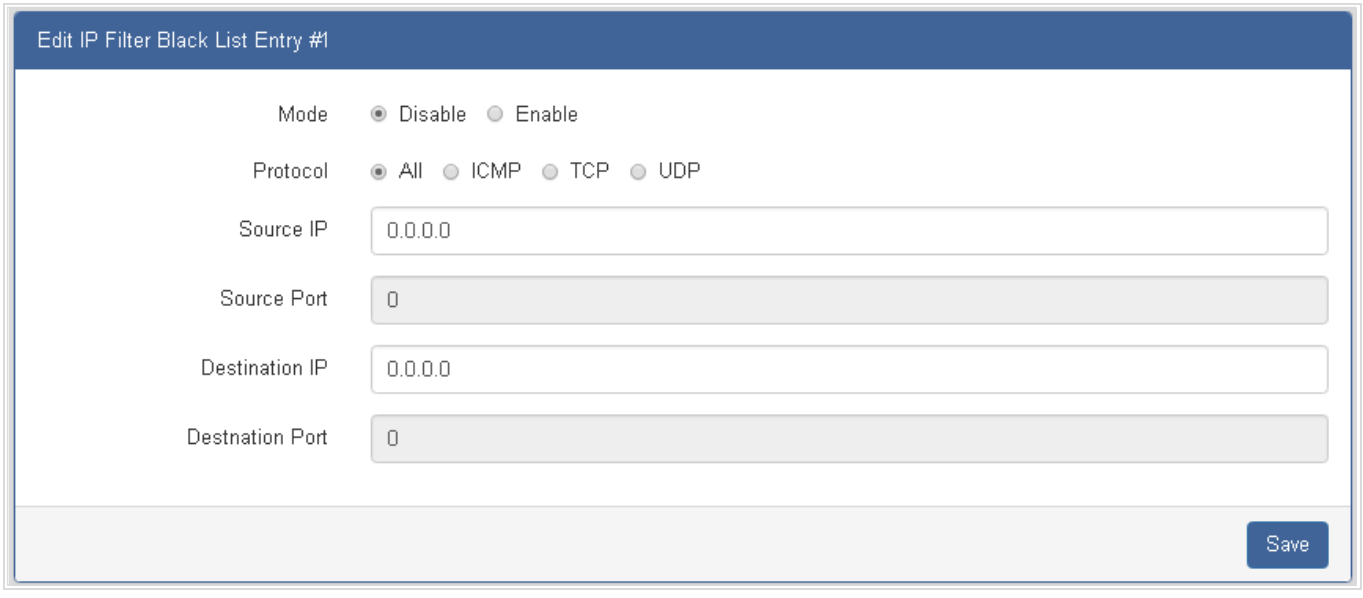


Figure 4-6-18 Edit IP Filter Black List Entry Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IP Filter configuration. The default is Disable.
• **Protocol**	Select from All, ICMP, TCP or UDP.
• **Source IP**	Fill in your source IP address.
• **Source Port**	Fill in your source port.
• **Destination IP**	Fill in your destination IP address.
• **Destination Port**	Fill in your destination port.

Buttons

Save: Click to save the current changes.

4.6.9 MAC Filter

The cellular gateway MAC Filter configuration is provided here. The MAC Filter screen in Figure 4-6-19 appears.

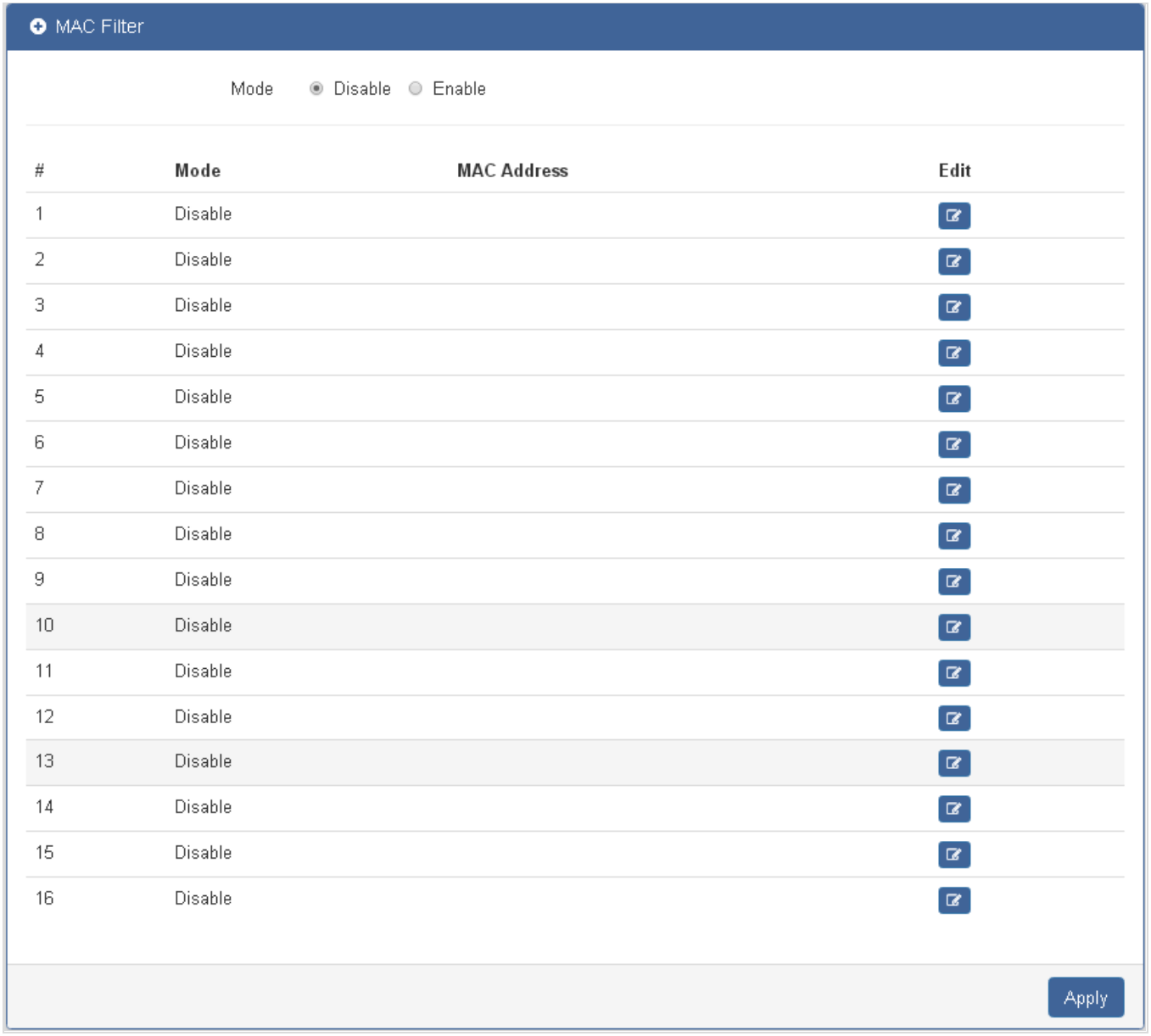


Figure 4-6-19 MAC Filter Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the MAC Filter configuration. The default is Disable.
• **#**	No. of Group
• **Mode**	Shows the current mode.
• **MAC Address**	Shows the current setting of MAC Address.
• **Edit**	Allows to configure the IP Filter configuation

Buttons

Apply: Click to apply changes.

4.6.9.1 Edit MAC Filter Black List Entry

The cellular gateway MAC Filter configuration is provided here. The Edit MAC Filter Black List Entry screen in Figure 4-6-20 appears.

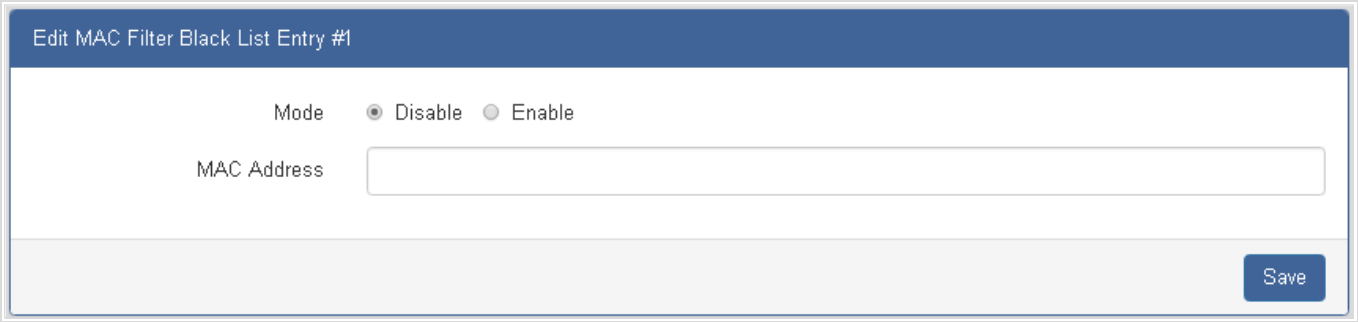


Figure 4-6-20 Edit MAC Filter Black List Entry Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IP Filter configuration. The default is Disable.
• **MAC Address**	Fill in the MAC Address you want to block.

Buttons

Save: Click to save the current changes.

Note

Setting up MAC address, please use "**:**" (colon symbol; e.g. xx : xx : xx: xx) or **–** hyphen symbol to mark (e.g. xx- xx–xx-xx).

4.6.10 URL Filter

The cellular gateway URL Filter configuration is provided here. The URL Filter screen in Figure 4-6-21 appears.

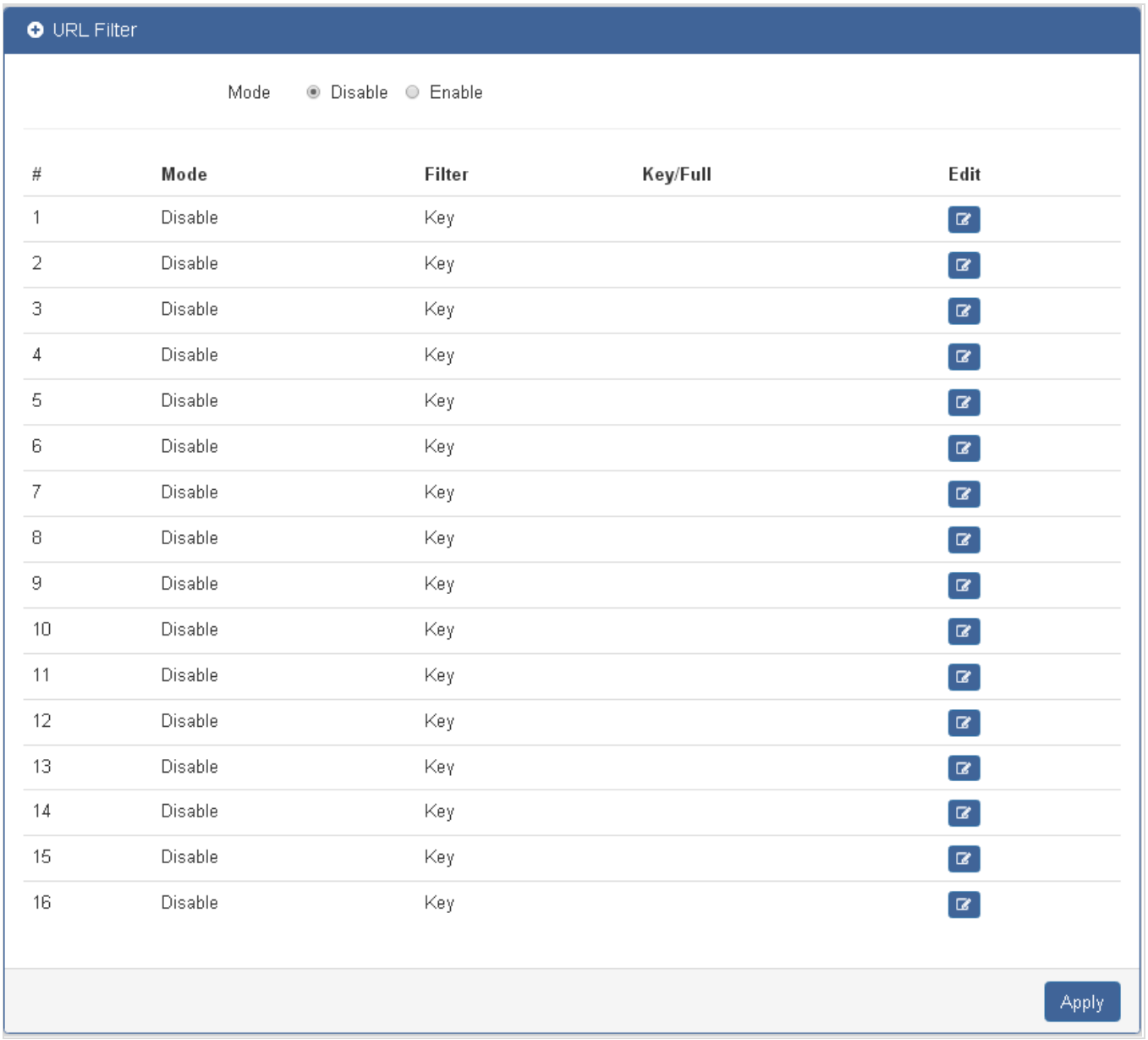


Figure 4-6-21 URL Filter Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the URL Filter configuration. The default is Disable.
• **#**	No. of Group
• **Mode**	Shows the current mode.
• **Filter**	Shows the current setting of Filter.

• **Key/Full**	Shows the current setting of Key/Full.
• **Edit**	Allows to configure the IP Filter configuration

Buttons

Apply: Click to apply changes.

4.6.10.1 Edit URL Filter Black List Entry

The cellular gateway URL Filter configuration is provided here. The Edit URL Filter Black List Entry screen in Figure 4-6-22 appears.

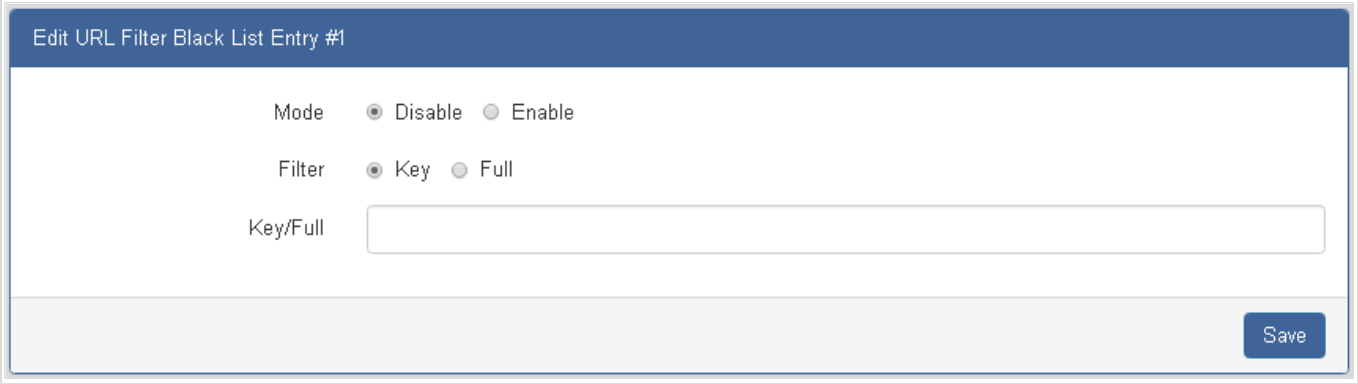


Figure 4-6-22 Edit URL Filter Black List Entry Page Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the IP Filter configuration. The default is Disable.
• **Filter**	Select from Key or Full. The default is Key.
• **Key/Full**	Fill in your Key/Full URL information.

Buttons

Save: Click to save the current changes.

4.6.11 VRRP

The cellular gateway VRRP configuration is provided here. The VRRP screen in Figure 4-6-23 appears.

Figure 4-6-23 VRRP Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the URL Filter configuration. The default is Disable.
• **Group**	Specify which VRRP group of this router belong to (1-255). The default is 1.
• **Priority**	Enter the priority value from 1 to 254. The larger value has higher priority. The default is 100.
• **Virtual IP**	■ Each cellular gateway in the same VRRP group must have the same virtual IP address. The default is 0.0.0.0. ■ This virtual IP address must belong to the same address range as the real IP address of the interface.

Buttons

Apply: Click to apply changes.

4.6.12 MQTT

This section makes you configure MQTT which allows the MQTT client to send the message within specific topic or channel. By default, the cellular gateway does not allow anonymous to read/write the MQTT topic or channel. Thus, you need to create the account with username and password for MQTT client in the web UI. The cellular gateway MQTT configuration is provided here. The MQTT screen in Figure 4-6-24 appears.

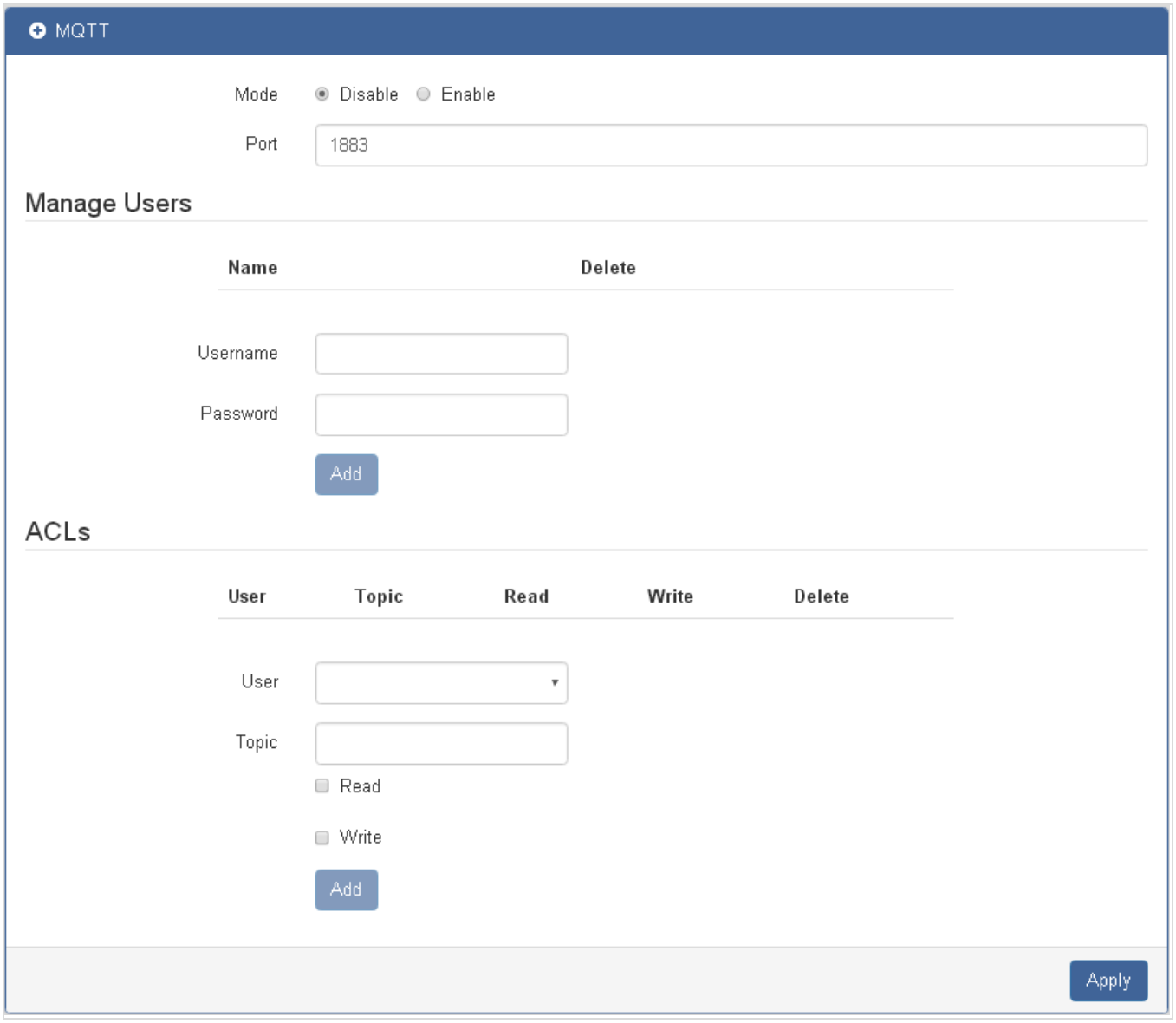


Figure 4-6-24 MQTT Configuration Screenshot

The page includes the following fields:

Object	Description
• **Mode**	**Disable or Enable** the URL Filter configuration. The default is Disable.
• **Port**	Fill in the port number of MQTT application.
• **Manage Users**	Create the users and show all users' names. Allow each user to delete their name.
• **Username**	Fill in the username of manage user.
• **Password**	Fill in the password of manage user.
• **ACLs**	Allow to specify what topic should be limited.
• **User**	Select the users and identify their authority to read or write the MQTT topic/channel.
• **Topic**	Name the topic of MQTT message.

Buttons

Apply: Click to apply changes.

4.7 Management

4.7.1 Identification

The Identification page provides information for the current device information. Identification page helps a cellular gateway administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 4-7-1 appears.

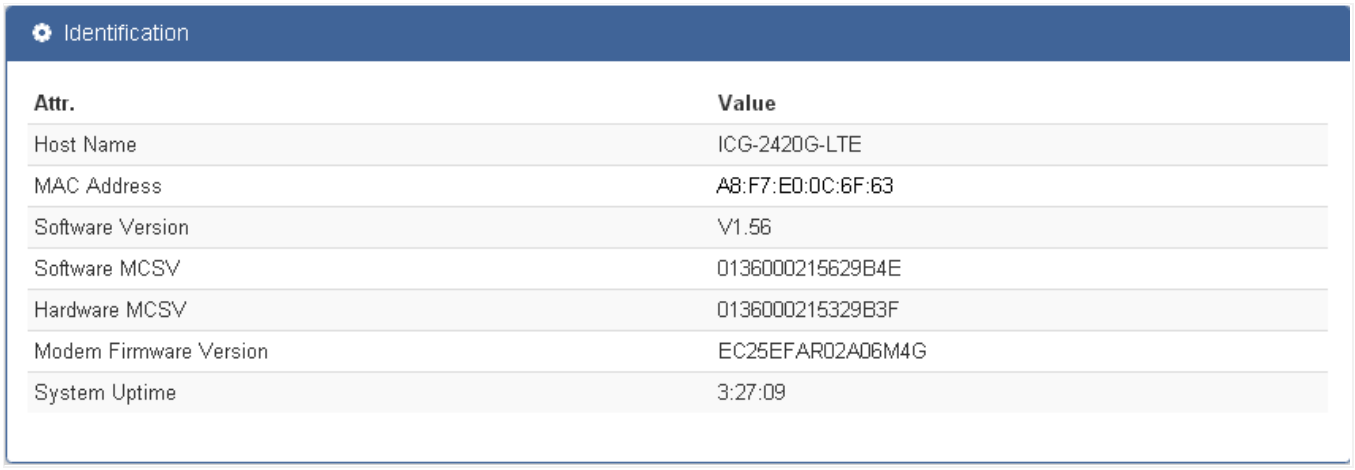


Figure 4-7-1 Identification Page Screenshot

The page includes the following fields:

Object	Description
• **Host Name**	Show the host name of cellular gateway.
• **MAC Address**	Show the MAC address.
• **Software Version**	Show the current software version.
• **Software MCSV**	Show the current software MCSV.
• **Hardware MCSV**	Show the current hardware MCSV.
• **Modem Firmware Version**	Show the current firmware version.
• **System Uptime**	Show the current system uptime.

4.7.2 Administration

The cellular gateway Administration configuration is provided here. The Administration screen in Figure 4-7-2 appears.

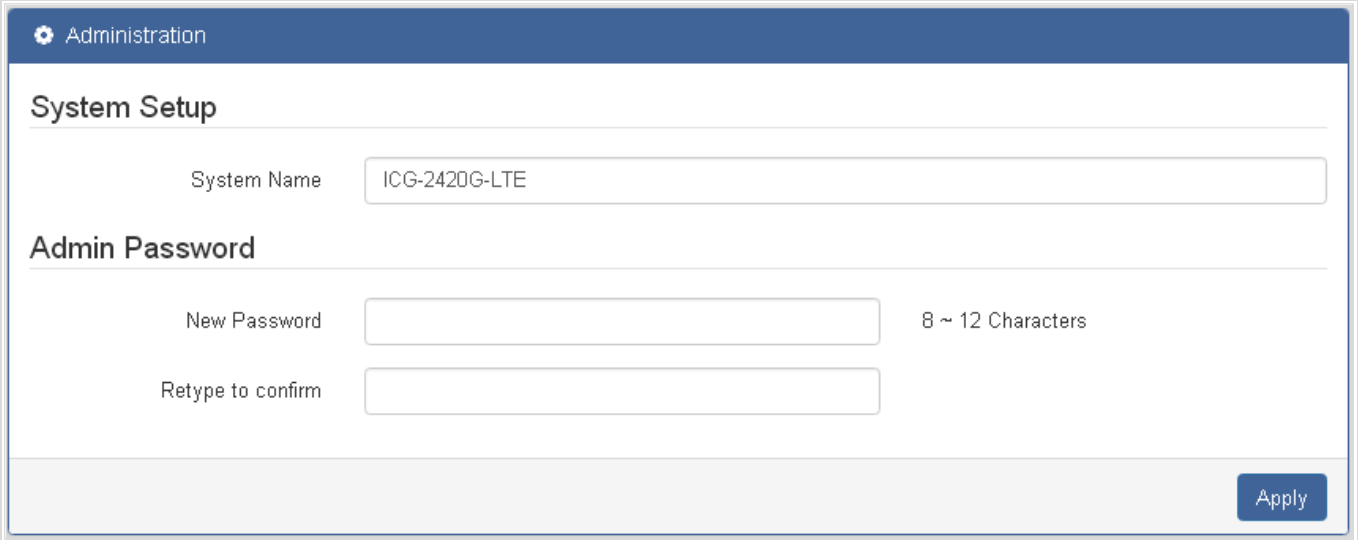


Figure 4-7-2 Administration Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Name**	Allows to change the system name.
• **New Password**	The password of the user. The allowed string length is **8** to **12**.
• **Retype to confirm**	Please enter the user's new password here again to confirm.

Buttons

Apply: Click to apply changes.

4.7.3 Firmware

This page facilitates an update of the firmware controlling the cellular gateway. The Web Firmware Upgrade screen in Figure 4-7-3 appears.

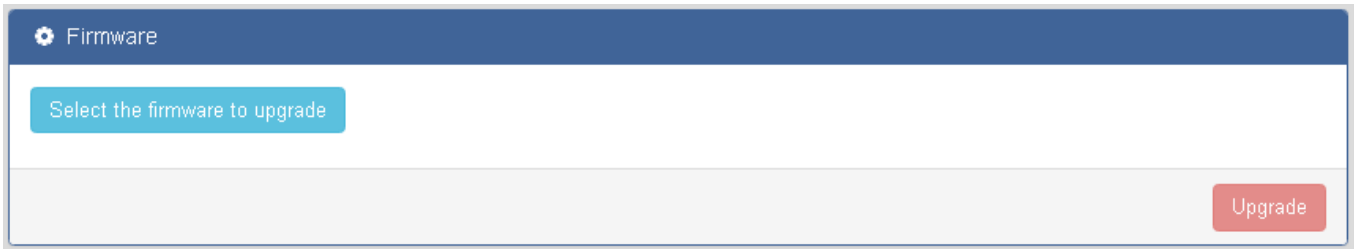


Figure 4-7-3 Firmware Page Screenshot

To open **Firmware Upgrade** screen, perform the following:

1. Click **Management** -> **Firmware**.
2. The Firmware Upgrade screen is displayed as in Figure 4-7-3.
3. Click the "Select the firmware to upgrade "button of the Main page, the system would pop up the file selection menu to choose firmware.
4. Select on the firmware then click "Upgrade", the **Software Upload Progress** would show the file with upload status.
5. Once the software is loaded to the system successfully, the following screen appears. The system will load the new software after reboot.

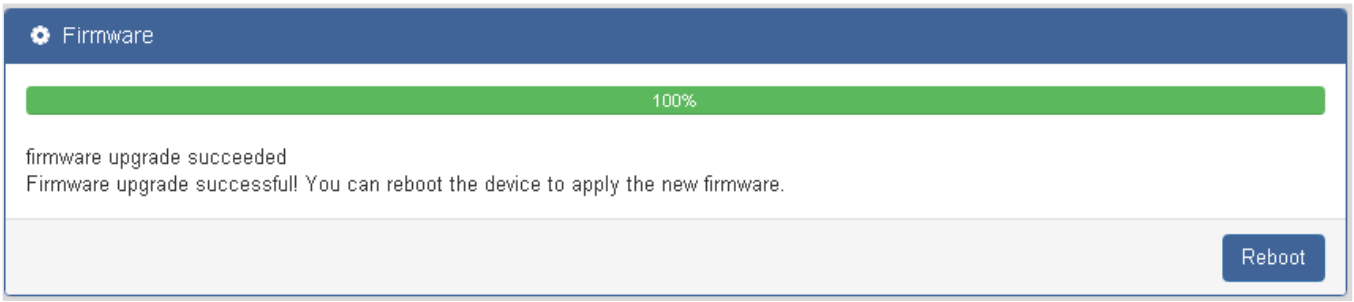


Figure 4-7-4: Software Successfully Loaded Notice Screen

Note

DO NOT Power OFF the Cellular Gateway until the update progress is completed.

4.7.4 Configuation

The cellular gateway stores its configuration in a .tgz files. It also can restore back the configure file to the cellular gateway. The Configuation screen in Figure 4-7-5 appears.

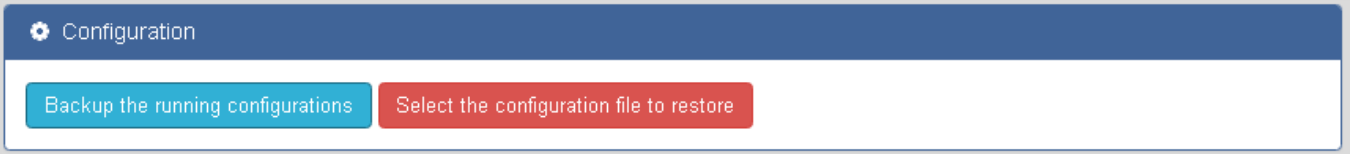


Figure 4-7-5 Configuration Page Screenshot

Buttons

Backup the running configurations: Click to download the current running of file.

Select the configuration file to restore: Click to restore the configure file to the cellular gateway.

4.7.5 Load Factory

You can reset the configuration of the Industrial Cellular Gateway on this page. The Load Factory screen in Figure 4-7-6 appears..

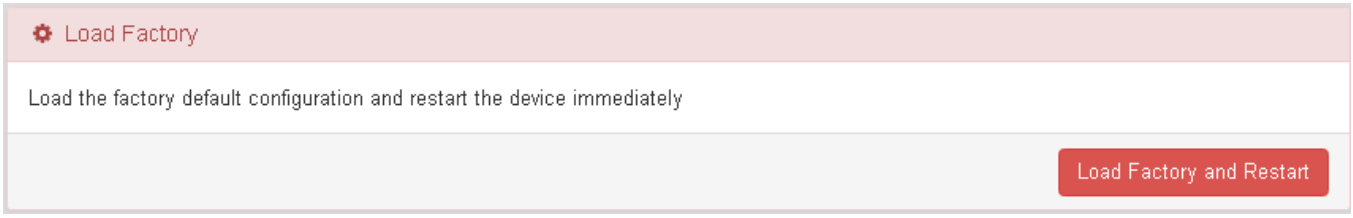


Figure 4-7-6 Configuration Page Screenshot

Buttons

Load Factory and Restart : Click to reset the default and restart the cellular gateway.

4.7.6 Restart

The **Restart** page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in to the Web interface. The restart screen in Figure 4-7-7 appears.

Figure 4-7-7 Restart Page Screenshot

Buttons

Restart : Click to restart the cellular gateway.

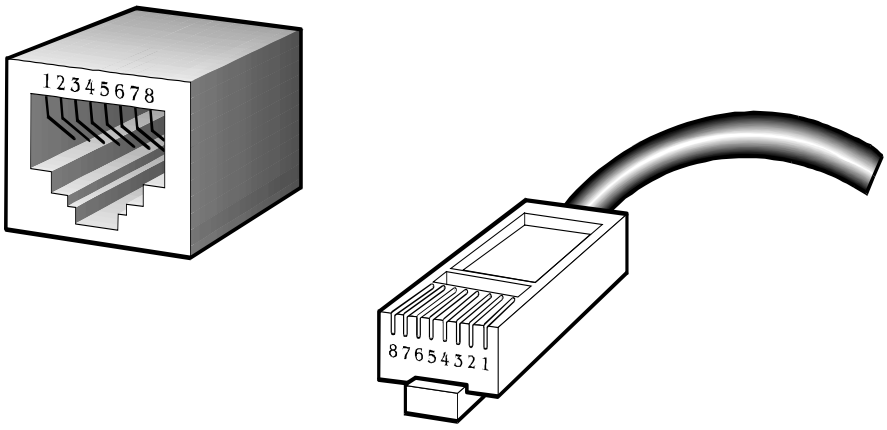
APPENDIX A RJ45 Pin Assignments

A.1 10/100Mbps, 10/100BASE-TX

When connecting your 10/100Mbps Cellular Gateway to another device, a bridge or a hub, a straight-through or crossover cable is necessary. Each port of the Cellular Gateway supports auto-MDI/MDI-X detection. That means you can directly connect the Cellular Gateway to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
Contact	**MDI** **Media Dependent Interface**	**MDI-X** **Media Dependent Interface-Cross**
1	**Tx + (transmit)**	**Rx + (receive)**
2	**Tx - (transmit)**	**Rx - (receive)**
3	**Rx + (receive)**	**Tx + (transmit)**
4, 5	**Not used**	
6	**Rx - (receive)**	**Tx - (transmit)**
7, 8	**Not used**	

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

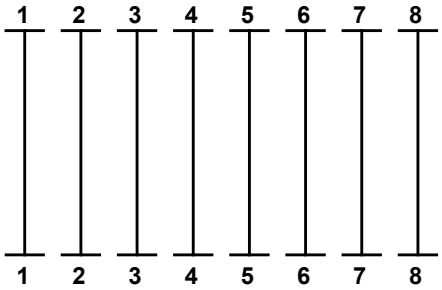
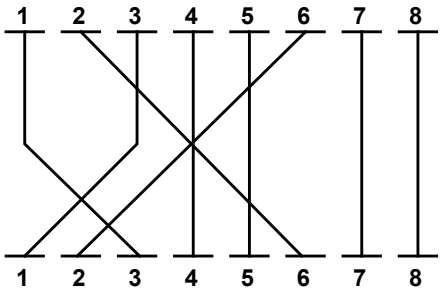
Straight-through Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with the same pin assignment and color as the above table before deploying the cables into your network.

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation,** declares that this **Industrial 4G LTE Cellular Gateway** is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **Industrial 4G LTE Cellular Gateway** tenkina visus svarbiausius 2014/53/EU direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **Industrial 4G LTE Cellular Gateway** lňuje základní požadavky a další příslušná ustanovení směrnice 2014/53/EU.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **Industrial 4G LTE Cellular Gateway** megfelel az 2014/53/EU irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **Industrial 4G LTE Cellular Gateway** overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **Industrial 4G LTE Cellular Gateway** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU
Deutsch	Hiermit erklärt **PLANET Technology Corporation,** dass sich dieses Gerät **Industrial 4G LTE Cellular Gateway** in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 2014/53/EU befindet". (BMWi)	**Nederlands**	Hierbij verklaart , **PLANET Technology orporation,** dat **Industrial 4G LTE Cellular Gateway** in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU
Eestikeeles	Käesolevaga kinnitab **PLANET Technology Corporation,** et see **Industrial 4G LTE Cellular Gateway** vastab Euroopa Nõukogu direktiivi 2014/53/EU põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **Industrial 4G LTE Cellular Gateway** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 2014/53/EU.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **Industrial 4G LTE Cellular Gateway** *ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ* ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU	**Português**	**PLANET Technology Corporation**, declara que este **Industrial 4G LTE Cellular Gateway** está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Español	Por medio de la presente, **PLANET Technology Corporation,** declara que **Industrial 4G LTE Cellular Gateway** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU	**Slovensky**	Výrobca **PLANET Technology Corporation,** týmto deklaruje, že táto **Industrial 4G LTE Cellular Gateway** je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 2014/53/EU.
Français	Par la présente, **PLANET Technology Corporation,** déclare que les appareils du **Industrial 4G LTE Cellular Gateway** sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU	**Slovensko**	**PLANET Technology Corporation**, **s tem potrjuje,** da je ta **Industrial 4G LTE Cellular Gateway** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 2014/53/EU.
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **Industrial 4G LTE Cellular Gateway** conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **Industrial 4G LTE Cellular Gateway** tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo **PLANET Technology Corporation,** apliecina, ka šī **802.11ac Industrial 4G LTE Cellular Gateway** atbilst Direktīvas 2014/53/EU pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **Industrial 4G LTE Cellular Gateway** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.