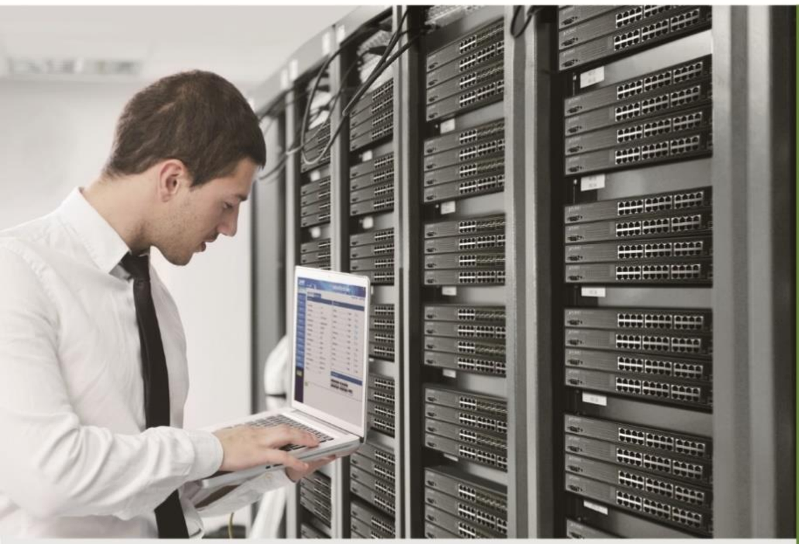
# User's Manual

## Industrial Outdoor LoRaWAN 5G NR Cellular Gateway

► LCG-350W-NR



www.PLANET.com.tw

## Copyright

## 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 and/or changes to 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.

## CE Compliance Statement

This device meets the RED 2014/53/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 it is used at a safe distance of 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

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.

## Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

## Revision

User's Manual of PLANET Industrial LoRaWAN Gateway
Model: LCG-350W-NR
Rev.: 1.0 (Nov. 2024)
Part No. EM-LCG-350W-NR

# Table of Contents

# Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial Outdoor LoRaWAN 5G NR Cellular Gateway, LCG-350W-NR. The description of this model is as follows:

| | |
|---|---|
| **LCG-350W-NR** | Industrial Outdoor LoRaWAN 5G NR Cellular Gateway |

"LoRaWAN Gateway" mentioned in the manual refers to the above model

## 1.1 Package Contents

The package should contain the following:

| | | |
|---|---|---|
| LoRaWAN Gateway x 1 | QR Code Sheet | Wall Bracket and Base x 1 |
| | | |
| RJ45 | Wall-mounted Kit x 1 | Pole Clamp x 1 |
| | | |
| Wired Waterproof Kit x 1 | Power Cord | Waterproof Rubber Stopper |
| | | |

Note

If any of the above items are missing, please contact your dealer immediately.

## 1.2 Overview

### Connecting to 5G NR and LoRa Network with Excellent LoRaWAN Cellular Gateway

PLANET LCG-350W-NR is an Industrial-grade Outdoor 5G NR Cellular LoRaWAN Gateway with reliable connectivity for IoT deployments. It is able to provide ultra-fast broadband access with 5G cellular network.

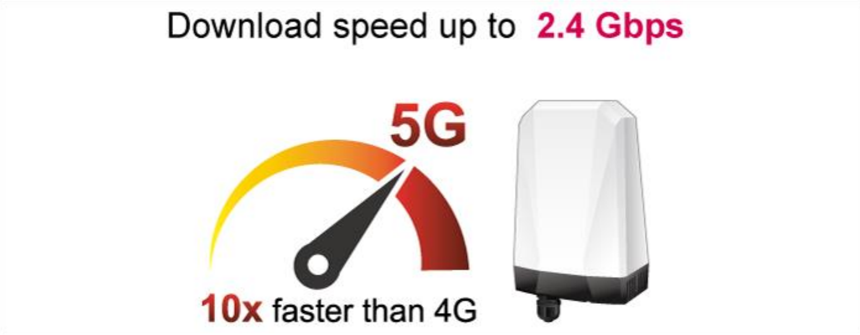
The LCG-350W-NR offers seamless wireless connectivity through compliance with IEEE 802.11b/g/n standards and is optimized for diverse LoRa applications with support for multiple frequency bands. Thus, the LCG-350W-NR is perfect for diverse regional applications. It provides secure wired network access via a 10/100BASE-T Ethernet interface with PoE+ and built-in electromagnetic isolation protection.

The LCG-350W-NR is built to endure harsh conditions, featuring an IP67 rating for dust and water resistance and operating in a wide temperature range. It includes integrated power protection, an MQTT broker for IoT data communication, strong VPN security, and compatibility with remote management systems. The LCG-350W-NR is the ideal choice for secure, reliable, and flexible networking in any scenario.

### Ultra-fast 4G/5G Network*

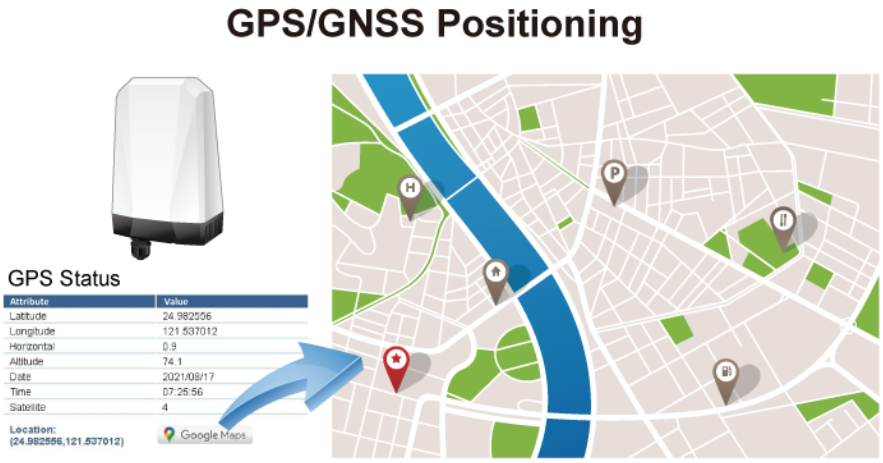
The LCG-350W-NR supports 5G NR DL (downlink) speeds higher than 3.6 Gbps and 4G LTE DL speeds of up to 2 Gbps. Its wide spectrum bandwidth accelerates internet speeds and reduces network latency for premium and time-sensitive connectivity services. It also supports multi-band connectivity including LTE FDD/TDD, WCDMA and GSM for a wide range of applications.

*The real 5G NR/4G LTE data rate is dependent on local service provider.



## GPS Included

The LCG-350W-NR is equipped with global positioning system feature. It adopts the 5G-NR technology that incorporates multiple global navigation systems (BDS/GPS/GLONASS/GALILEO/QZSS/SBAS). It helps to position location of cellular gateway 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.


GPS/GNSS Positioning

GPS Status

| Attribute | Value |
|---|---|
| Latitude | 24.982556 |
| Longitude | 121.537012 |
| Horizontal | 0.9 |
| Altitude | 74.1 |
| Date | 2021/08/17 |
| Time | 07:25:56 |
| Satellite | 4 |

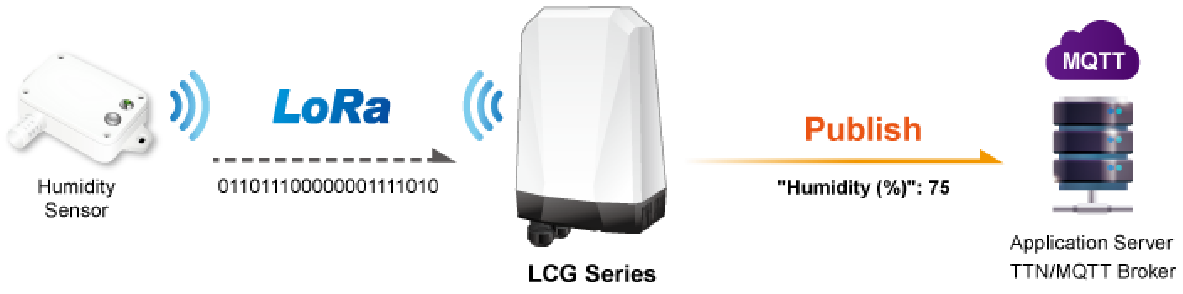
Location: (24.982556,121.537012)

## LoRaWAN Compatibility

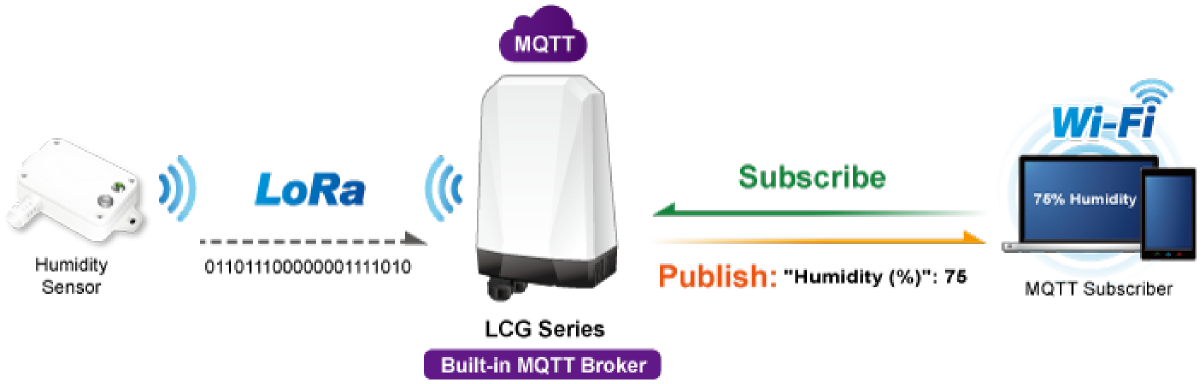
The LCG-350W-NR is LoRaWAN-compatible, ensuring smooth operation with LoRa sensors. LoRaWAN is a low-power, wide area networking protocol built on top of the LoRa radio modulation technique. LoRaWAN networks and devices such as sensor and gateway allow public or private network to connect multiple applications such as IoT, M2M, smart city, sensor network, and industrial automation applications in the same space.

## Enhanced IoT Efficiency with LCG-300 Series

The LCG-300/350 series gateways support the expanding LoRa IoT ecosystem by converting sensor data into easily readable JSON format. This feature allows sensor data to be read without the need for external applications to parse the data, thus significantly simplifying the data integration process and reducing the time required to deploy IoT solutions.

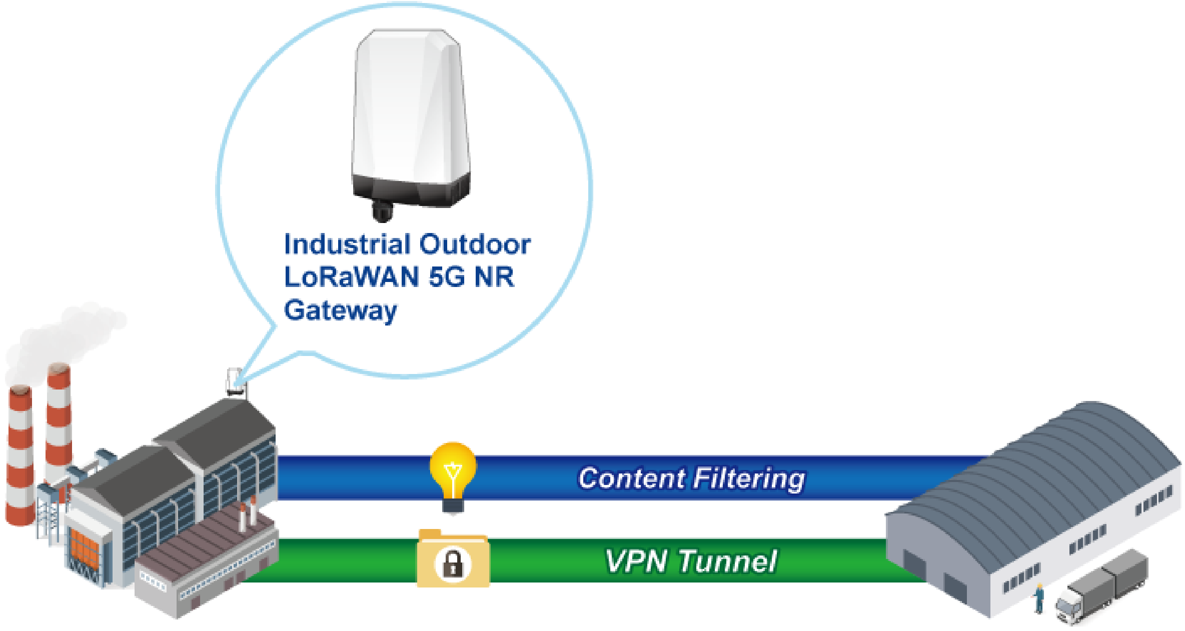


Additionally, the built-in MQTT broker in the LCG-300 series facilitates data parsing and collection, enabling users to obtain data quickly and conveniently. This is possible both through the internal MQTT broker and an external MQTT broker. This functionality helps reduce the costs associated with building network servers and minimizes the complexity of the network architecture.



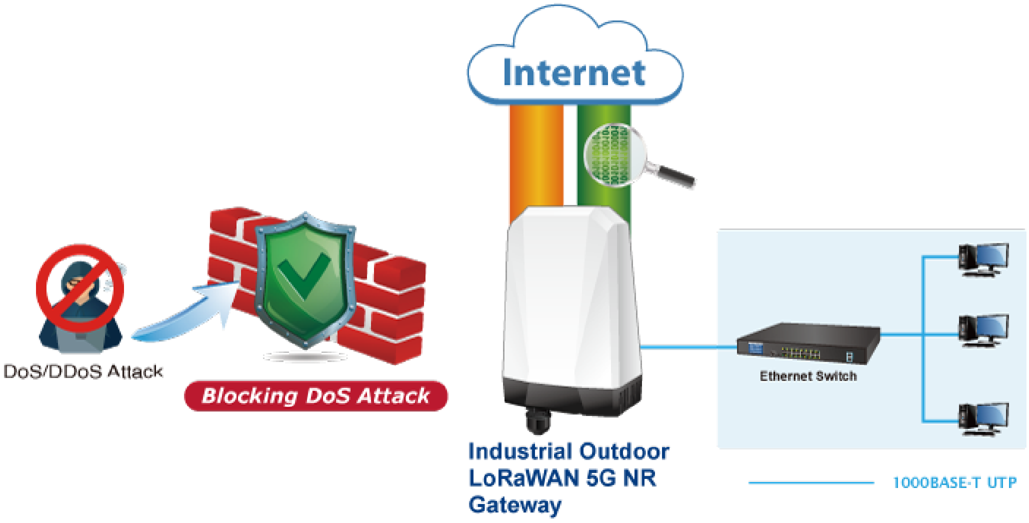
### Ideal High-Availability VPN Security Router Solution for Industrial Environment

The LCG-350W-NR provides complete data security and privacy for accessing and exchanging the most sensitive data, built-in IPSec VPN function with DES/3DES/AES encryption and MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication, and GRE, SSL, PPTP and L2TP server mechanism. The full VPN capability in the LCG-350W-NR makes the connection more secure, flexible, and capable.



### Excellent Ability in Threat Defense

The LCG-350W-NR has built-in SPI (stateful packet inspection) firewall and DoS/DDoS attack mitigation functions to provide high efficiency and extensive protection for your network. Thus, virtual server and DMZ functions can let you set up servers in the Intranet and still provide services to the Internet users.



### Cybersecurity Network Solution to Minimize Security Risks

The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the LCG-350W-NR is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the LCG-350W-NR offers an easy-to-use, platform-independent management and configuration facility. The LCG-350W-NR supports SNMP, allowing it to be managed via any management software based on the standard SNMP protocol.

### Maximizing Work Efficiency with PLANET SD-WAN Gateway

PLANET LCG-350W-NR incorporated in SD-WAN (software-defined wide area network) function can greatly increase WAN optimization for managing multiple WAN. With SD-WAN, users can connect any application across all available network connections at every site. It improves application performance and provides a high-quality user experience for increasing business productivity and reducing IT costs.

# 1.3 Features

### Key Features

- Supports global 5G NR (NSA/SA) and 4G LTE with a Nano-SIM card slot for reliable cellular access.
- Compliant with IEEE 802.11b/g/n standards for wireless connectivity.
- Supports EU868, IN865, RU864, US915, AU915, KR920 and AS923 frequency bands for various regional applications.
- 8 programmable parallel paths for better data processing
- 10/100BASE-T Ethernet LAN interface with 802.11at PoE+ support and built-in 1.5KV electromagnetic isolation protection
- Built-in reverse phase, overvoltage, and lightning protection
- Supports both 100-277V AC input and 802.11at PoE+ power.
- Integrated MQTT broker for efficient IoT data communication
- Supports SSL VPN and robust hybrid VPN protocols (IPSec/PPTP/L2TP over IPSec) for secure data transmission.
- Features Stateful Packet Inspection (SPI) firewall and content filtering to block DoS/DDOS attacks and manage port range forwarding.
- Compatible with Planet NMS controller system and CloudViewerPro app for easy remote management and monitoring.
- Operates in -40°C to 75°C; IP67-rated for dust and water resistance.

### Hardware

- 1 x 10/100BASE-T RJ45 LAN port with 802.3at PoE+
- 2 x 5G NR antennas
- 1 x Nano-SIM card slot
- 1 x LoRa antenna
- 1 x Wi-Fi antenna
- 1 x GPS antenna
- 1 x reset button

### Cellular Interface

- Supports multi-band connectivity with 5G NR (NSA/SA), LTE-FDD, LTE-TDD, and WCDMA.
- Built-in SIM and broadband backup for network redundancy
- Four detachable antennas for 5G NR connection
- LED indicators for signal strength and connection status

### LoRa Interface

- Supports EU868, IN865, RU864, US915, AU915, KR920 and AS923.
- 8 programmable parallel demodulation paths

## RF Interface Characteristics

- Features 2.4GHz (802.11b/g/n) band for configuration.
- 2T2R MIMO technology for simple wireless connection

## IP Routing Feature

- Static route
- Dynamic route
- OSPF

## Firewall Security

- Cybersecurity
- Stateful Packet Inspection (SPI) firewall
- Blocks DoS/DDoS attack
- Content filtering
- MAC filtering and IP filtering
- NAT ALG (Application Layer Gateway)
- Blocks SYN/ICMP flooding

## VPN Features

- IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server and SSL Server/Client (Open VPN)
- Max. Connection Tunnel Entries: 30 VPN tunnels,
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512

## Networking

- DHCP server/NTP client for LAN
- Protocols: TCP/IP, UDP, ARP, IPv4, IPv6
- Port forwarding; QoS; DMZ; IGMP; UPnP; SNMPv1,v2c, v3
- MAC address clone
- DDNS: PLANET DDNS, Easy DDNS, DynDNS and No-IP
- MQTT Broker

## Others

- Setup wizard
- Dashboard for real-time system overview
- Supported access by HTTP or HTTPS
- Auto reboot
- PLANET NMS System and Smart Discovery Utility for deployment management
- Planet CloudViewerPro app for real-time monitoring

## 1.4 Product Specifications

| **Product** | **LCG-350W-NR** |
|---|---|
| **Hardware Specifications** | |
| **Ethernet** | 1 10/100BASE-T RJ-45 Ethernet |
| **Cellular Antenna** | 2 x 3 dBi internal antennas |
| **SIM Interface** | 1 Nano-SIM card slot |
| **LoRa Antenna** | 2 dBi internal antennas with SMA connectors for LoRa |
| **Reset Button** | < 5 sec: System reboot<br>> 5 sec: Factory default |
| **Enclosure** | IP67 rating |
| **Installation** | Wall hanging, pole mounting |
| **LED Indicators** | PWR (**Blue**)<br>Internet (**Blue**)<br>LoRa (**Blue**)<br>4G/5G (**Blue**)<br>Wi-Fi (**Blue**) |
| **Dimensions (W x D x H)** | 150 x 100 x 240 mm |
| **Weight** | 1045g |
| **Power Requirements** | 48V DC IN, 0.5A, IEEE 802.3at PoE+ or<br>100~277V AC IN, 0.5A |
| **Power Consumption** | Max. 2.4 watts/8.19 BTU (No Loading)<br>Max. 3.3 watts/11.26 BTU (Full loading) |
| **LoRaWAN** | |
| **Frequency Band** | Suffixes<br>868: supported EU868, IN865, RU864<br>915: supported US915, AU915, KR920, AS923 |
| **Receiving Sensitivity** | -140dBm |
| **Output Power** | 26±1dBm |
| **Multi Band Support** | |
| **5G Sub6 Band** | LCG-350W-NR-EU:<br>n1/n3/n5/n7/n8/n20/n28/n38/n40/n41/n75/n76/n77/n78<br>LCG-350W-NR-NA:<br>n2/n5/n12/n14/n25/n30/n41/n48/n66/n70/n71/n77 |

| | |
|---|---|
| **LTE Band** | LCG-350W-NR-EU:<br>LTE FDD: B1/B3/B5/B7/B8/B20/B28/B32<br>LTE TDD: B38/B40/B41/B42/B43<br>LCG-350W-NR-NA:<br>LTE FDD: B2/B4/B5/B12/B13/B29/B30/B66/B71<br>LTE TDD: B41/B46(LAA)/B48 |
| **WCDMA** | LCG-350W-NR-EU: B1/B5/B8 |
| **GNSS** | BDS/GPS/GLONASS/GALILEO/QZSS/SBAS |
| **Data Transmission Throughput** | 3.4Gbps (DL)/350Mbps (UL) for 5G NR<br>2Gbps (DL)/150Mbps (UL) for LTE Cat20<br>42Mbps (DL)/5.76Mbps (UL) for HSPA+ |
| **Wireless** | |
| **Standard** | IEEE 802.11b/g/n 2.4GHz |
| **Band Mode** | 2.4G Only |
| **Frequency Range** | 2.4GHz<br>FCC: 2.412~2.462GHz<br>ETSI: 2.412GHz~2.472GHz |
| **Operating Channels** | 2.4GHz<br>FCC: 1~11<br>ETSI: 1~13 |
| **Channel Width** | 20/40MHz |
| **Data Transmission Rates** | Transmit: 150 Mbps* for 2.4 GHz<br>Receive: 150 Mbps* for 2.4 GHz<br><br>***The estimated transmission distance is based on the theory. The actual distance may vary in different environments.** |
| **Transmission Power** | 11b: 26dBm ± 1dBm @11Mbps<br>11g: 24dBm ± 1.5dBm @54Mbps<br>11g/n:<br>20dBm ± 1.5dBm @MCS7, HT20<br>17dBm@MCS7,HT40 |
| **Encryption Security** | WEP (64/128-bit) encryption security<br>WPA / WPA2 (TKIP/AES)<br>WPA-PSK / WPA2-PSK (TKIP/AES)<br>WPA3 personal<br>802.1x Authenticator |
| **Wireless Advanced** | Wi-Fi Multimedia (WMM)<br>Auto channel selection |

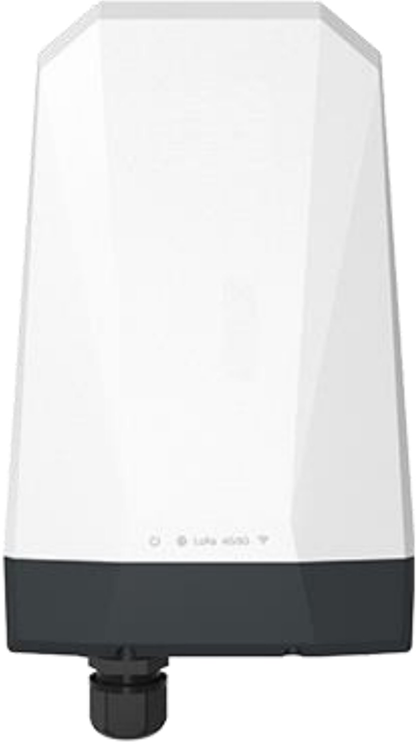
| | |
|---|---|
| | Wireless output power management<br>MAC address filtering |
| **Max. SSID** | 4 |
| **Max. Wireless Clients** | 64 (32 is suggested, depending on usage) |
| **Security Service** | |
| **Firewall Security** | Cybersecurity<br>SSL (HTTPS) Inspection<br>Stateful Packet Inspection (SPI)<br>Blocks DoS/DDoS attack |
| **NAT** | Port forwarding<br>DMZ Host<br>UPnP |
| **Content Filtering** | MAC filtering<br>IP filtering<br>Web filtering |
| **Bandwidth Management** | QoS (Quality of Service) |
| **Networking** | |
| **Operation Mode** | Routing mode |
| **Routing Protocol** | Static Route, Dynamic Route (RIP), OSPF |
| **VLAN** | 802.1q Tag-based, Port-based, Multi-VLAN |
| **Multicast** | IGMP Proxy |
| **NAT Throughput** | Max. 99Mbps |
| **Outbound Load Balancing** | Supported algorithms: Weight |
| **Protocol** | IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, PPPoE, SNMPv1/v2c/v3, |
| **Advanced Functions** | |
| **VPN Function** | IPSec/Remote Server (Net-to-Net, Host-to-Net)<br>GRE<br>PPTP Server<br>L2TP Server<br>SSL Server/Client (Open VPN) |
| **VPN Tunnels** | Max. 30 |
| **VPN Throughput** | Max. 50Mbps |
| **Encryption Methods** | DES, 3DES, AES or AES-128/192/256 encryption |
| **Authentication Methods** | MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm |
| **Management** | |
| **Basic Management Interfaces** | Web browser |

| | |
|---|---|
| | SNMP v1, v2c<br>PLANET Smart Discovery utility and NMS controller supported<br>PLANET CloudViewerPro app |
| **Secure Management Interfaces** | SSHv2, TLSv1.2/1.3, SNMP v3 |
| **System Log** | System Event Log |
| **Others** | Setup wizard<br>Dashboard<br>System status/service<br>Statistics<br>Connection status<br>Auto reboot<br>Diagnostics |
| **Standards Conformance** | |
| **Regulatory Compliance** | CE |
| **Electrostatic Discharge (ESD) Immunity Test** | IEC 61000-4-2, Level 4 |
| **Surge Immunity Test** | IEC 61000-4-5, Level 4 |
| **Electrical Fast Transient (EFT) Burst Immunity Test** | IEC 61000-4-4, Level 4 |
| **Environment** | |
| **Operating** | Temperature: -40 ~ 75 degrees C<br>Relative humidity: 5 ~ 90% (non-condensing) |
| **Storage** | Temperature: -40 ~ 85 degrees C<br>Relative humidity: 5 ~ 90% (non-condensing) |

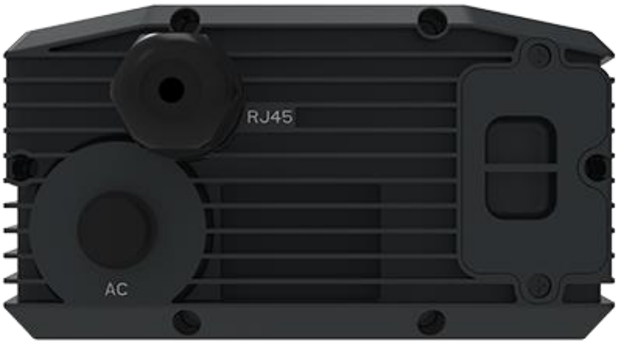
# Chapter 2. Hardware Introduction

## 2.1 Physical Descriptions

### Front View



### Bottom View



**LED Definition:**

- **System**

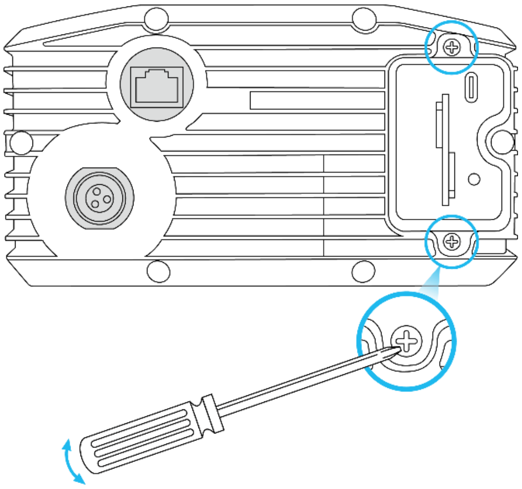
| LED | Color | Function |
|---|---|---|
| **PWR** | **Blue** | Light to indicate that power is active |
| **Internet** | **Blue** | Light to indicate that the port is successfully established |
| **Wi-Fi** | **Blue** | Light to indicate that Wi-Fi is active |
| **5G NR/ 4G LTE** | **Blue** | Light to indicate that the establishment of a LTE/5G signal for the cellular connection is successful |
| **LoRa** | **Blue** | Light to indicate that LoRa signal is active |

## 2.2 Hardware Installation

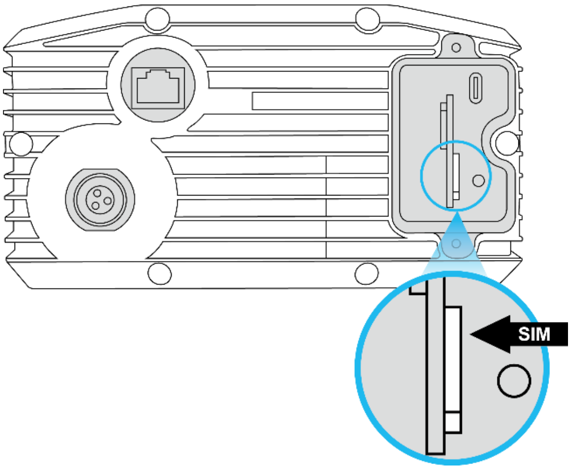
Follow the simple steps below to quickly install your **LoRaWAN Gateway**.

### 2.2.1 SIM Card Installation

A. Unscrew the two screws on the device's cover to remove it.

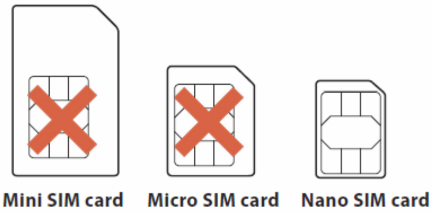


B. Insert the SIM card according to the instructions on the SIM card interface.



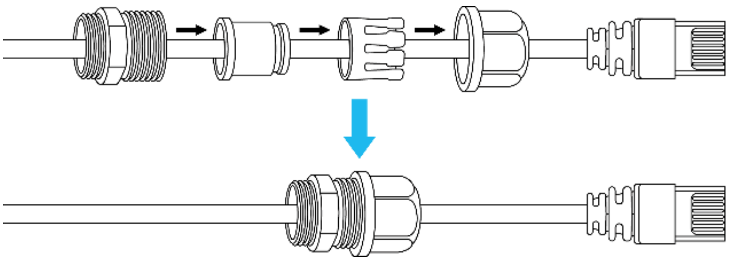
C. Reattach the device's cover and tighten the screws securely.

- **A mini SIM card with 5G NR and 4G LTE subscription**



## 2.2.2 Wiring the Ethernet Cable Installation

As shown in the picture, put the network cable through the waterproof connector, and tighten the connector. Plug the cable into the device's LAN port, and secure the waterproof connector to the device.



Plug the other end of the network cable into the PoE port of the PoE switch to finish the installation.

Note

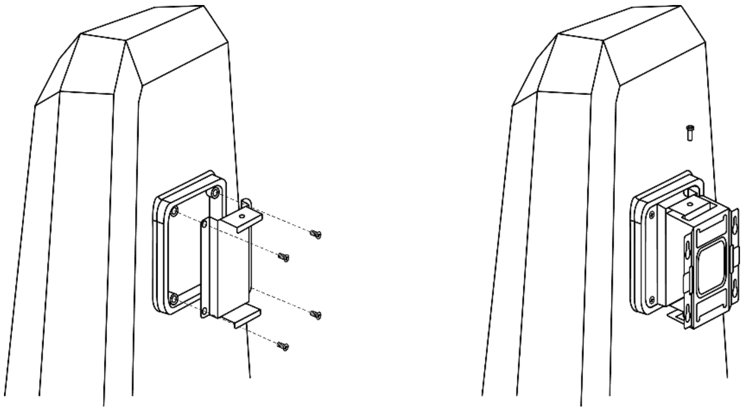
Please make sure that the waterproof connector is securely fastened with **LoRaWAN Gateway** to prevent internal water seepage.

## 2.2.3 Wall Hanging and Pole Mounting Installation

**Wall hanging**

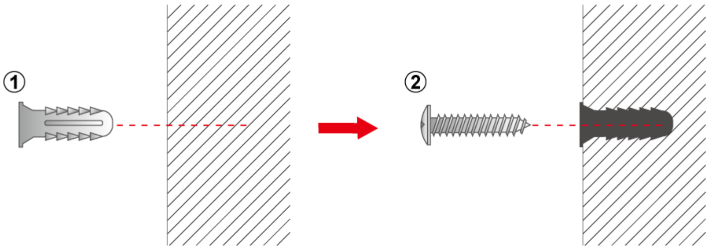
**Step 1:** Lock the base to the device.

**Step 2**: Connect the wall bracket to the base and fasten the screws.

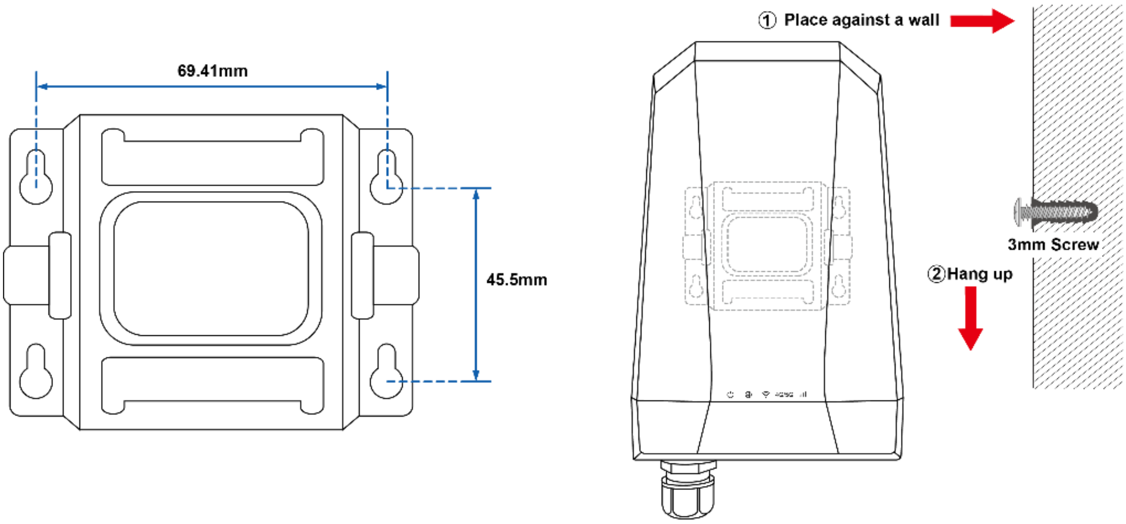


**Step 3**: Drill 4 holes with a **3mm** diameter on the wall. The horizontal and vertical distances between the 2 holes are **69.5mm** and **45mm**, respectively.

**Step 4**: Place four anchors inside the hole by hammering them. Then screw the four screws leaving a space of 2mm apart as shown in the circled diagram below.



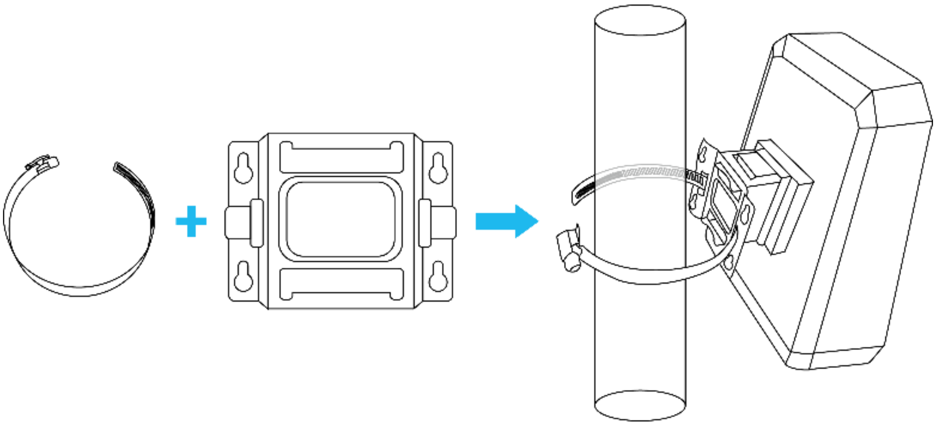
**Step 5:** The switch, shown in the picture below, can now be hung on the wall.



- **Pole mounting**

To install the base and wall bracket, refer to **Step 1** and **Step 2** in Device Installation (Wall Hanging).

**Step 3**: The pole clamp goes through the hole of the wall bracket, and is wrapped around the pole. To finish the installation, fasten the clamp.



# Chapter 3. Preparation

Before getting into the device's web UI, user has to check the network setting and configure PC's IP address.

## 3.1 Requirements

User is able to confirm the following items before configuration:

1. Please confirm the network is working properly; it is strongly suggested to test your network connection by connecting your computer directly to ISP.
2. Suggested operating systems: Windows 7 / 8 / 10 / 11.
3. Recommended web browsers: Microsoft Edge / Mozilla Firefox / Google Chrome.

## 3.2 Setting TCP/IP on your PC

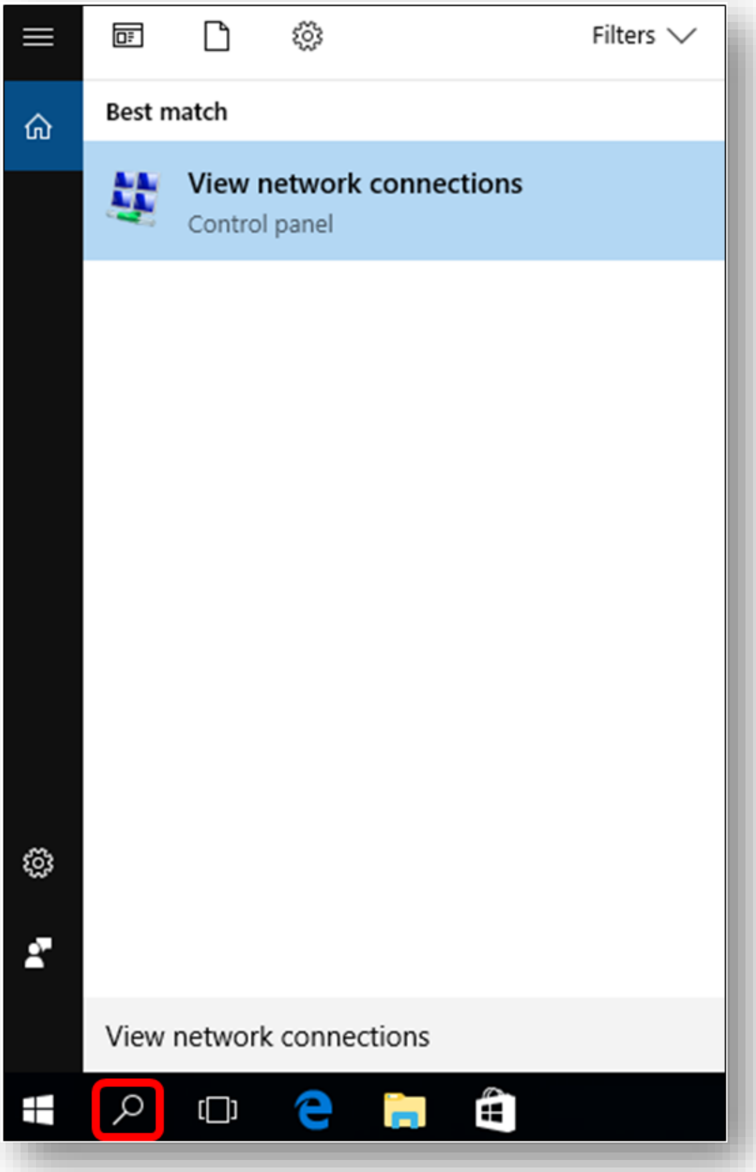
The default IP address of the LoRaWAN Gateway is 192.168.1.1, and the DHCP Server is enabled. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN LoRaWAN Gateway.
Please refer to the following to set the IP address of the connected PC.

1. Select "**Use the following IP address**" and "**Obtain DNS server address automatically**", and then click the “**OK**” button.

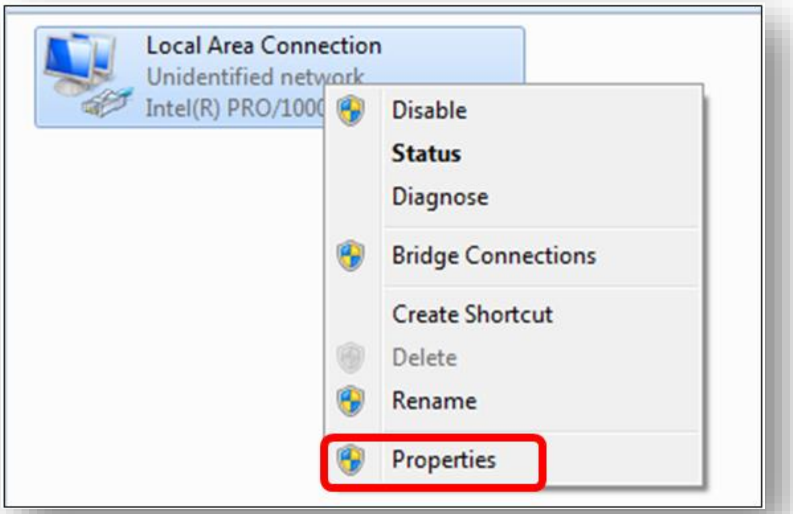
## Windows 10

**If you are using Windows 10, please refer to the following:**

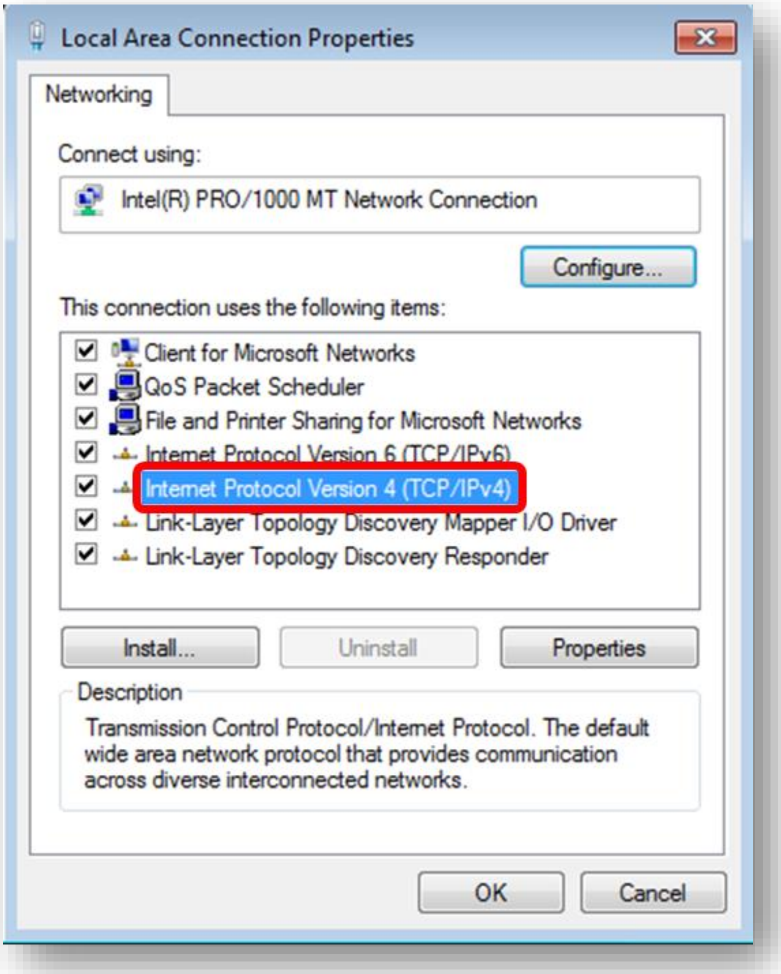
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



2. Right-click on the Local Area Connection and select Properties.



3. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

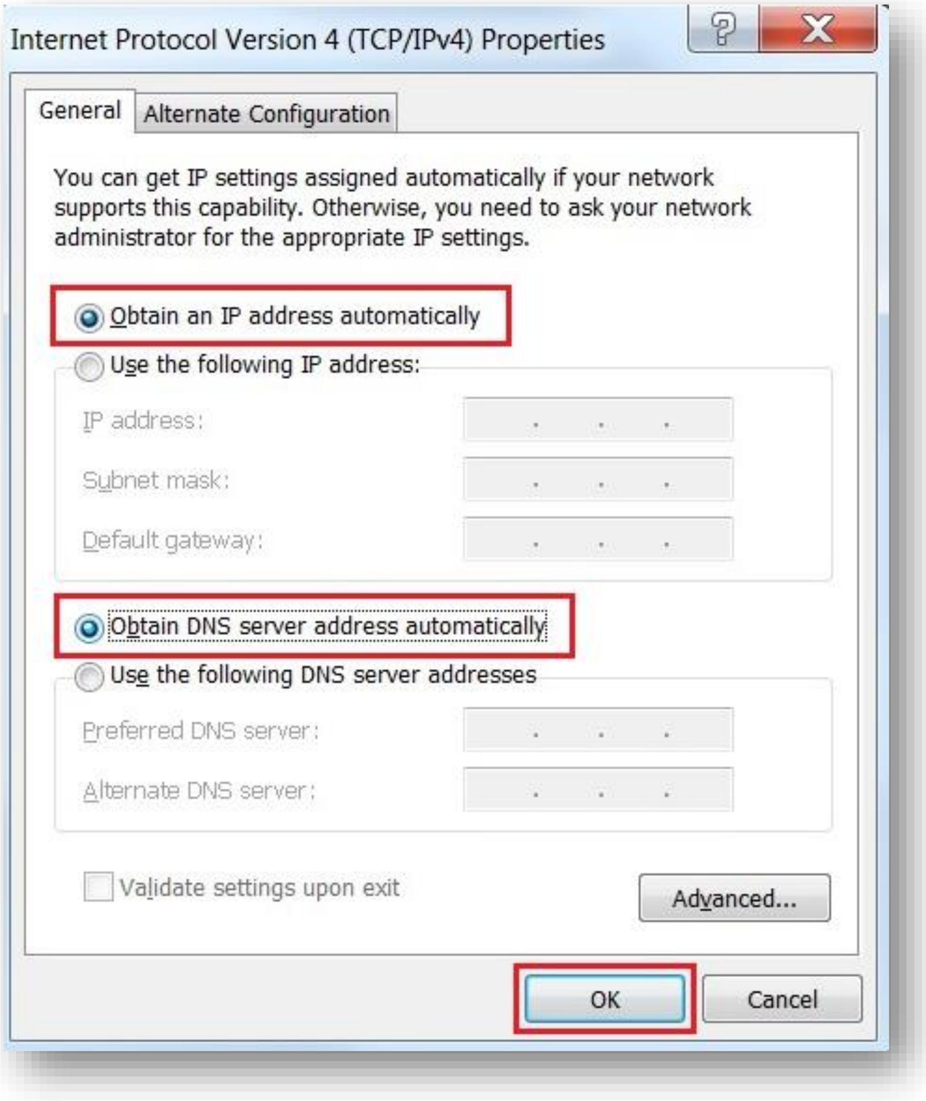
This connection uses the following items:

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

Description

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

4. Select "**Use the following IP address**" and "**Obtain DNS server address automatically**", and then click the "**OK**" button.



Internet Protocol Version 4 (TCP/IPv4) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

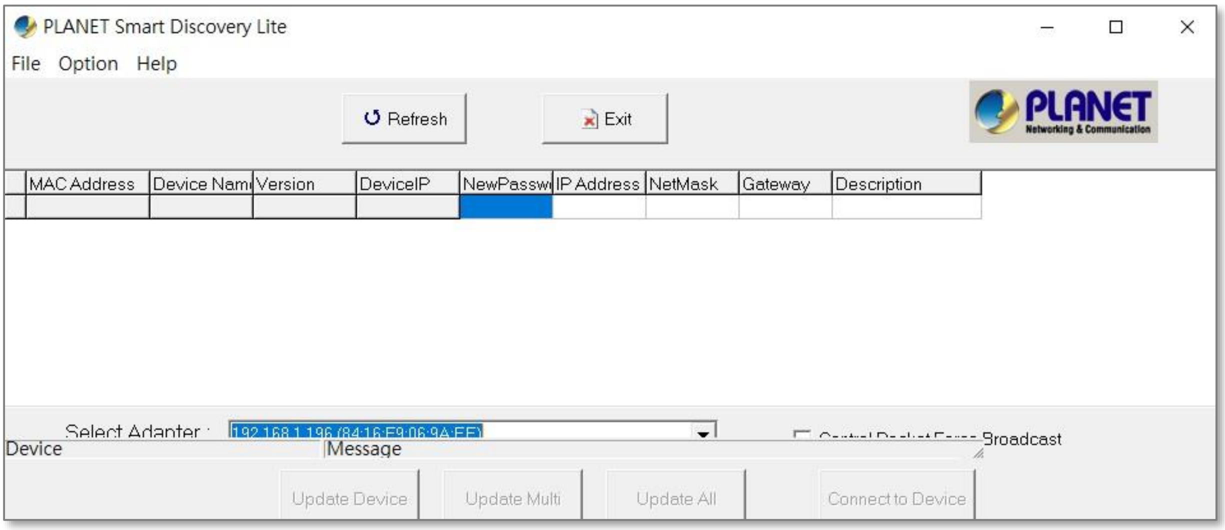
□ Validate settings upon exit

## 3.3 Planet Smart Discovery Utility

For easily listing the LoRaWAN Gateway in your Ethernet environment, the search tool -- Planet Smart Discovery Utility -- is an ideal solution.

The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Download the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

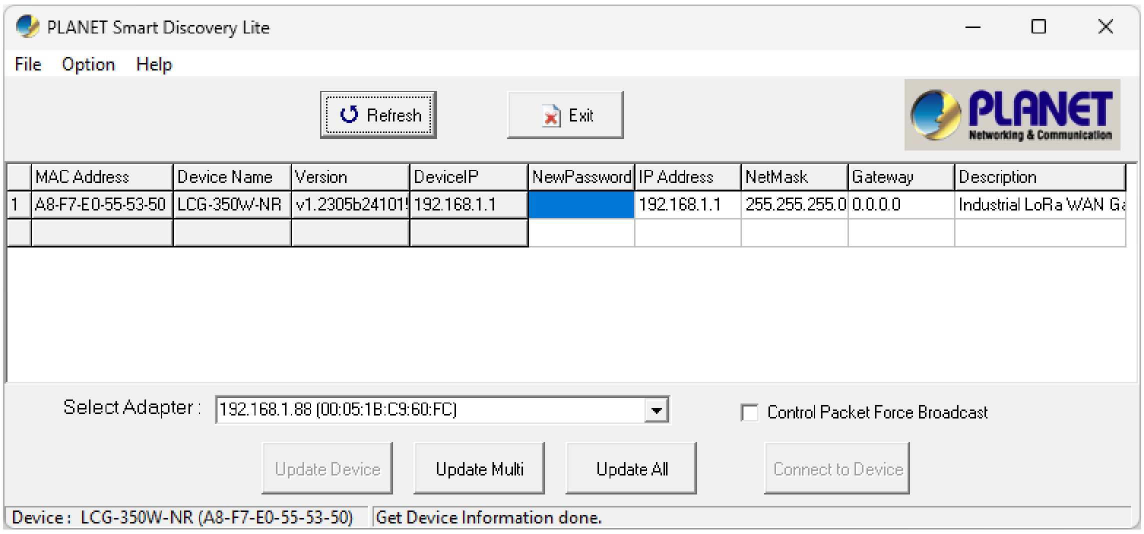


Select Adapter : 192.168.1.196 (84:16:F9:06:9A:EE)

**Figure 3-1-6:** Planet Smart Discovery Utility Screen

If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

3. Press the **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:


PLANET Smart Discovery Lite
File
Option
Help
Refresh
Exit
PLANET Networking & Communication
☐ Control Packet Force Broadcast
Update Device
Update Multi
Update All
Connect to Device

| | MAC Address | Device Name | Version | DeviceIP | NewPassword | IP Address | NetMask | Gateway | Description |
|---|---|---|---|---|---|---|---|---|---|
| 1 | A8-F7-E0-55-53-50 | LCG-350W-NR | v1.2305b24101 | 192.168.1.1 | | 192.168.1.1 | 255.255.255.0 | 0.0.0.0 | Industrial LoRa WAN Ga |

Select Adapter : 192.168.1.88 (00:05:1B:C9:60:FC)

Device : LCG-350W-NR (A8-F7-E0-55-53-50) | Get Device Information done.

**Figure 3-1-7:** Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

2. After setup is completed, press the "**Update Device**", "**Update Multi**" or "**Update All**" button to take effect. The functions of the 3 buttons above are shown below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

   The same functions mentioned above also can be found in "**Option**" tools bar.

3. To click the "**Control Packet Force Broadcast**" function, it allows you to assign a new setting value to the device under a different IP subnet address.

4. Press the "**Connect to Device**" button and the Web login screen appears.

Press the "**Exit**" button to shut down the Planet Smart Discovery Utility.

# Chapter 4. Web-based Management

This chapter provides setup details of the device's Web-based Interface.

## 4.1 Introduction

The device can be configured with your Web browser. Before configuring, please make sure your PC is under the same IP segment with the device.

## 4.2 Logging in to the LoRaWAN Gateway

Refer to the steps below to configure the LoRaWAN Gateway:

**Step 1.** Connect the IT administrator's PC and LoRaWAN Gateway's LAN port to the same hub / switch, and then launch a browser to link the management interface address which is set to **http://192.168.1.1** by default.

Note

The DHCP server of the LoRaWAN Gateway is enabled. Therefore, the LAN PC will get an IP from the VPN LoRaWAN Gateway. If user needs to set an IP address of LAN PC manually, please set the IP address within the range of 192.168.1.2 to 192.168.1.254 (inclusive), and assign the subnet mask of 255.255.255.0.

**Step 2.** The browser prompts you for the login credentials.

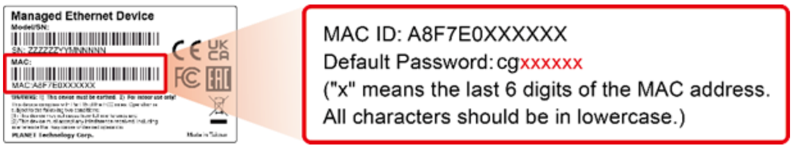
Default IP address: **192.168.1.1**

Default user name: **admin**

Default password: **cg + the last 6 characters of the MAC ID in lowercase**

Default SSID (2.4G): **PLANET_2.4G**

Find the MAC ID on your device label. The default password is "cg" followed by the last six lowercase characters of the MAC ID.



MAC ID: A8F7E0XXXXXX
Default Password: cgxxxxxx
("x" means the last 6 digits of the MAC address.
All characters should be in lowercase.)

**Figure 4-2-1:** MAC ID Label

Note

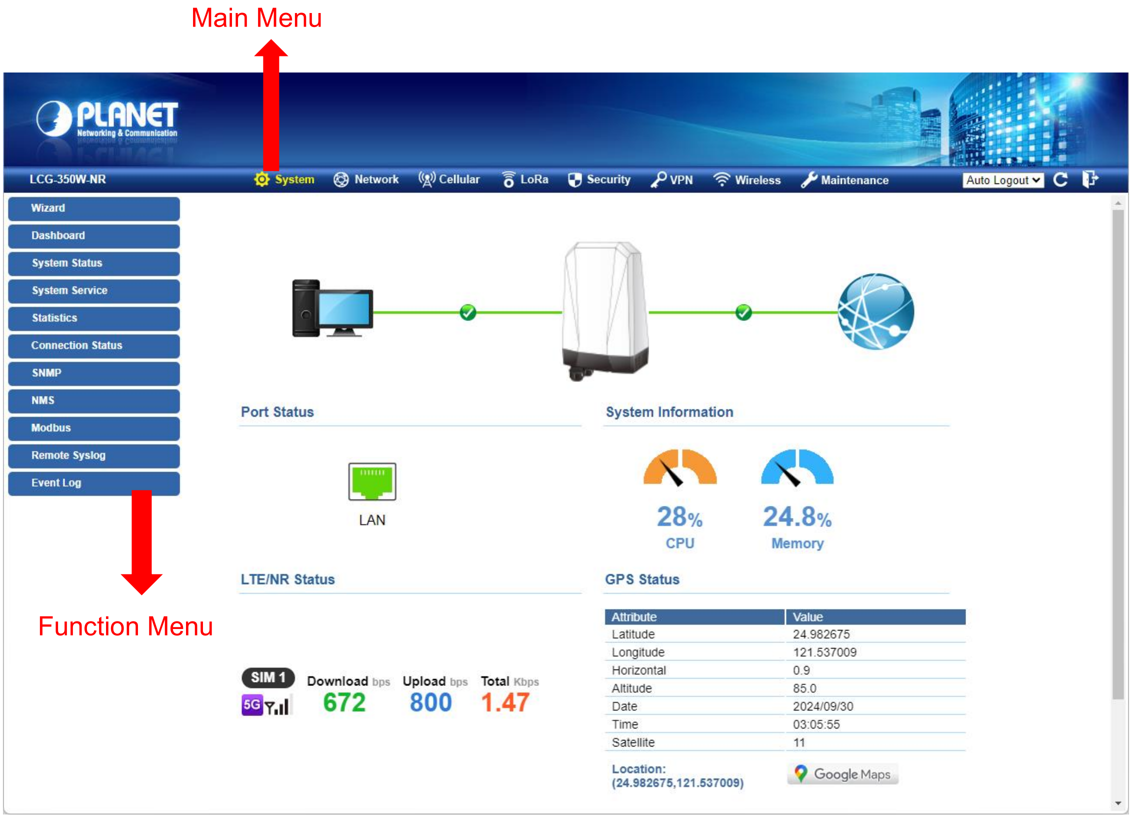
If you have already changed the password web login, please use this new pa to log in and skip **step 2.**

Note

Administrators are strongly suggested to change the default admin and password to ensure system security.

## 4.3 Main Web Page

After a successful login, the main web page appears. The main web page displays the web panel, main menu, function menu, and the main information in the center.



28% CPU

24.8% Memory

Download bps 672

Upload bps 800

Total Kbps 1.47

| Attribute | Value |
|---|---|
| Latitude | 24.982675 |
| Longitude | 121.537009 |
| Horizontal | 0.9 |
| Altitude | 85.0 |
| Date | 2024/09/30 |
| Time | 03:05:55 |
| Satellite | 11 |

Location:
(24.982675,121.537009)

**Figure 4-3-1:** Main Web Page

### ■ Main Menu

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown below:

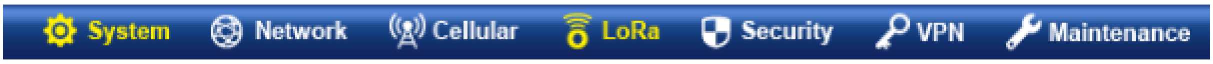


**Figure 4-3-2:** Function Menu

| Object | Description |
|---|---|
| **System** | Provides System information of the LoRaWAN Gateway |
| **Network** | Provides WAN, LAN and network configuration of the LoRaWAN Gateway |
| **Cellular** | Provides cellular configuration of the router |
| **LoRa** | Provides LoRa configuration of the LoRaWAN Gateway |
| **Security** | Provides Firewall and security configuration of the LoRaWAN Gateway |
| **VPN** | Provides VPN configuration of the LoRaWAN Gateway |
| **Wireless** | Provides wireless configuration of the LoRaWAN Gateway |
| **Maintenance** | Provides firmware upgrade and setting file restore/backup configuration of the LoRaWAN Gateway |

**Figure 4-3-3:** Function Button

| Object | Description |
|---|---|
| ↻ | Click the "**Refresh button**" to refresh the current web page. |
| 🚪 | Click the "**Logout button**" to log out of the web UI of the LoRaWAN Gateway |

## 4.4 System

Use the system menu items to display and configure basic administrative details of the LoRaWAN Gateway. The system menu shown in Figure 4-4-1 provides the following features to configure and monitor system.

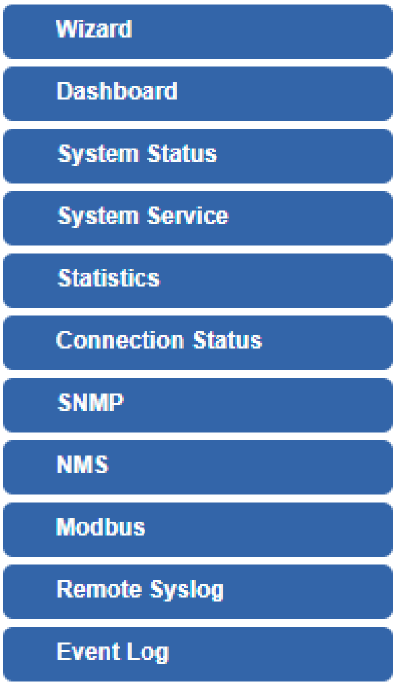


**Figure 4-4-1:** System Menu

| Object | Description |
|---|---|
| **Wizard** | The Wizard will guide the user to configuring the LoRaWAN Gateway easily and quickly. |
| **Dashboard** | The overview of system information includes connection, port, and system status. |
| **System Status** | Display the status of the system, Device Information, LAN and WAN. |
| **System Service** | Display the status of the system, Secured Service and Server Service |
| **Statistics** | Display statistics information of network traffic of LAN and WAN. |
| **Connection Status** | Display the DHCP client table and the ARP table |
| **SNMP** | Display SNMP system information |
| **NMS** | Enable/Disable NMS on LoRaWAN Gateway |
| **Modbus** | Configure Modbus on LoRaWAN Gateway |
| **Remote Syslog** | Enable Captive Portal on LoRaWAN Gateway |
| **Event Log** | Display Event Log information |

## 4.4.1 Setup Wizard

The wizard will guide the user to configuring the LoRaWAN Gateway easily and quickly. There are different procedures in different operation modes. According to the operation mode you switch to, please follow the instructions below to configure the LoRaWAN Gateway via **Setup Wizard** as shown in Figure 4-4-2.

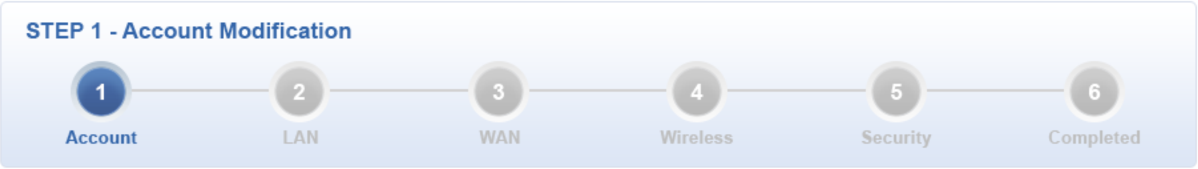
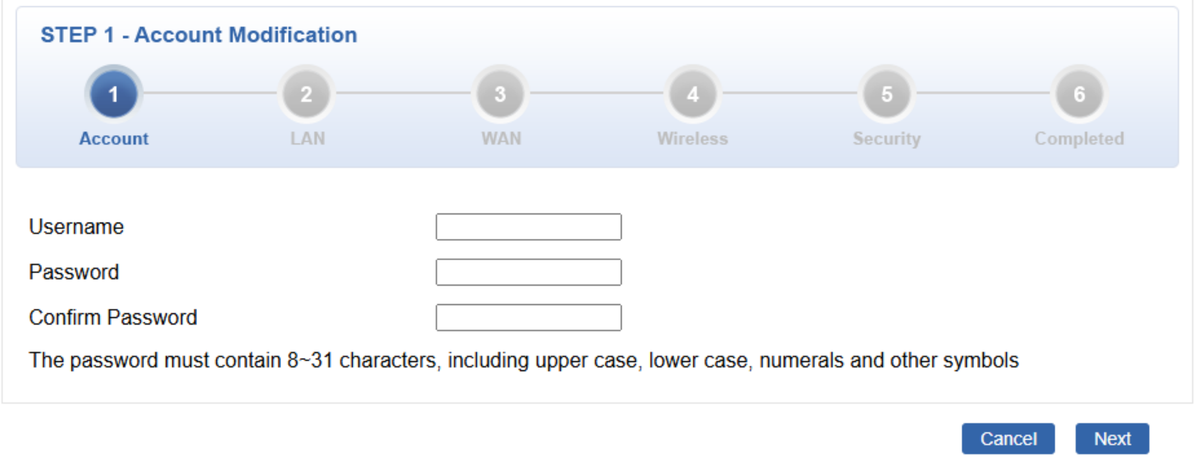


**Figure 4-4-2:** Setup Wizard

### Step 1: Account Modification

Set up the Username and Password for the Account Modification as shown in Figure 4-4-3.



Username

Password

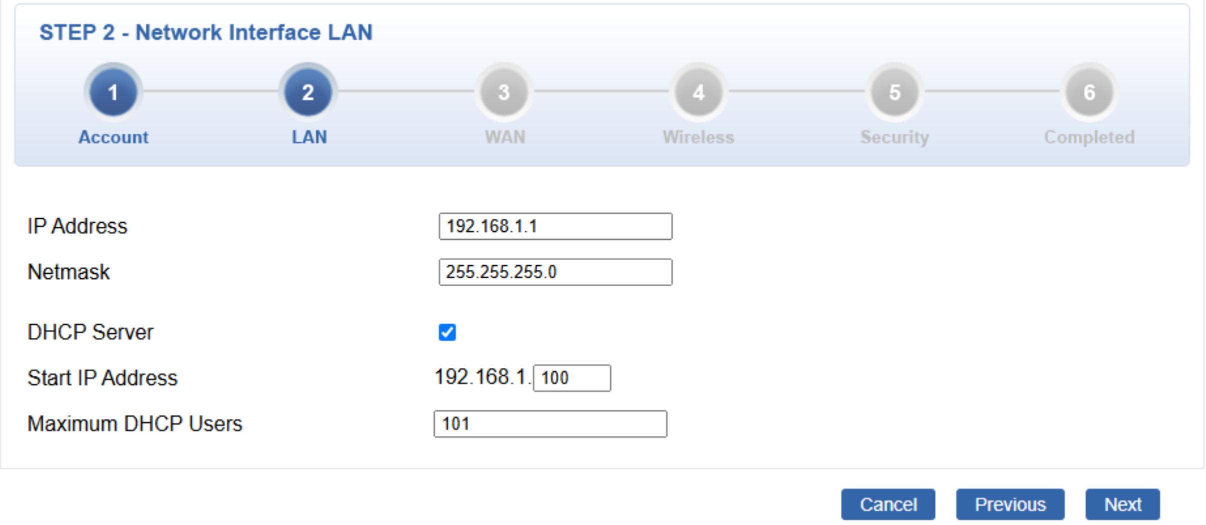
Confirm Password

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols

**Figure 4-4-3:** Account Modification

## Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 4-4-4.



STEP 2 - Network Interface LAN

IP Address: 192.168.1.1

Netmask: 255.255.255.0

DHCP Server: ☑

Start IP Address: 192.168.1. 100

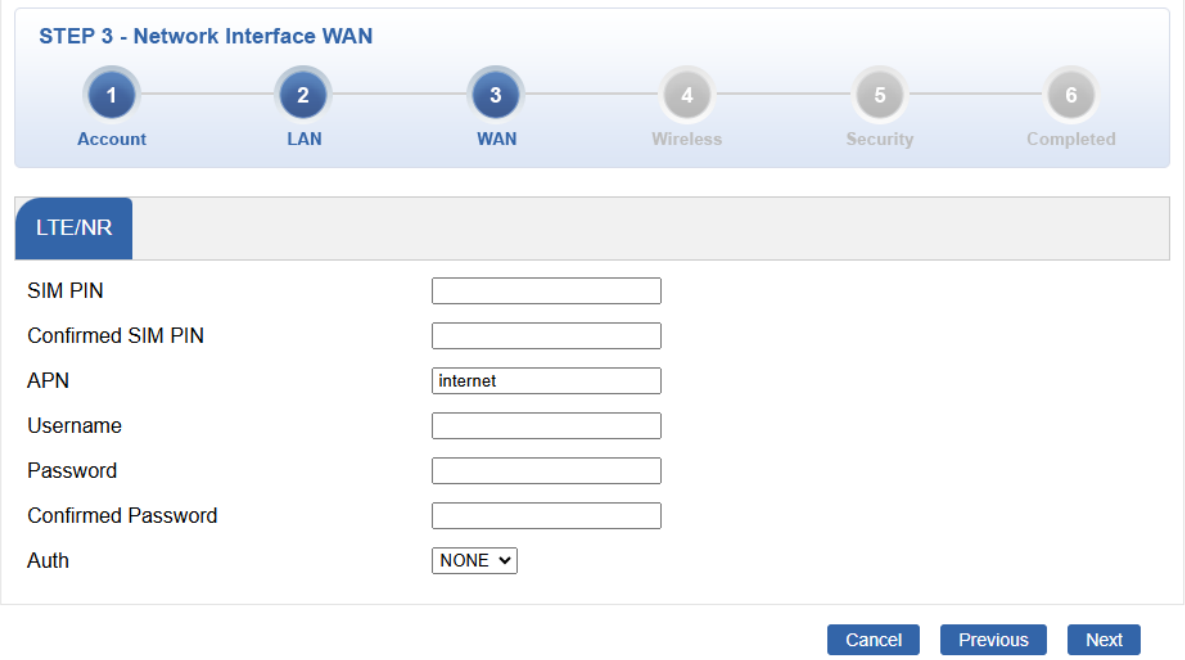
Maximum DHCP Users: 101

**Figure 4-4-4:** Setup Wizard – LAN Configuration

| Object | Description |
|---|---|
| **IP Address** | Enter the IP address of your LoRaWAN Gateway. The default is 192.168.1.1. |
| **Subnet Mask** | An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask. |
| **DHCP Server** | By default, the DHCP Server is enabled.<br>If user needs to disable the function, please uncheck the box. |
| **Start IP Address** | By default, the start IP address is 192.168.1.100.<br>Please do not set it to the same IP address of the LoRaWAN Gateway |
| **Maximum DHCP Users** | By default, the maximum number of DHCP clients is 101, which means the LoRaWAN Gateway will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100. |
| **Next** | Press this button to do the next step. |
| **Cancel** | Press this button to undo any changes made locally and revert to previously saved values. |

## Step 3: WAN

The LoRaWAN Gateway supports LTE/NR access modes on the WAN side shown below:

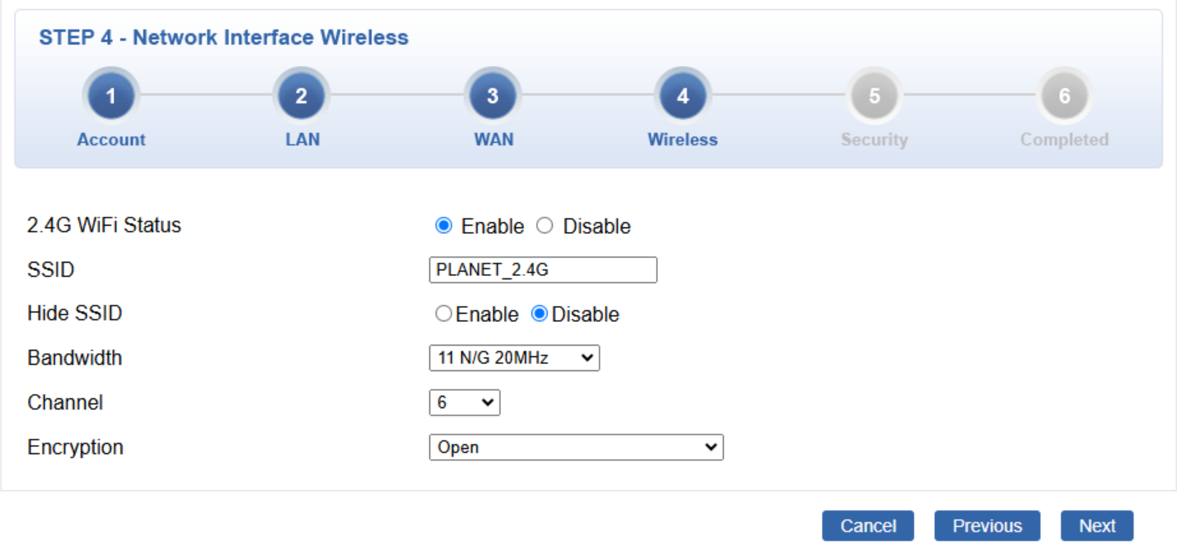


| | |
|---|---|
| SIM PIN | |
| Confirmed SIM PIN | |
| APN | internet |
| Username | |
| Password | |
| Confirmed Password | |
| Auth | NONE |

**Figure 4-4-5:** Setup Wizard – WAN Configuration

## Step 4: Wireless Setting

Set up the Wireless Settings as shown below



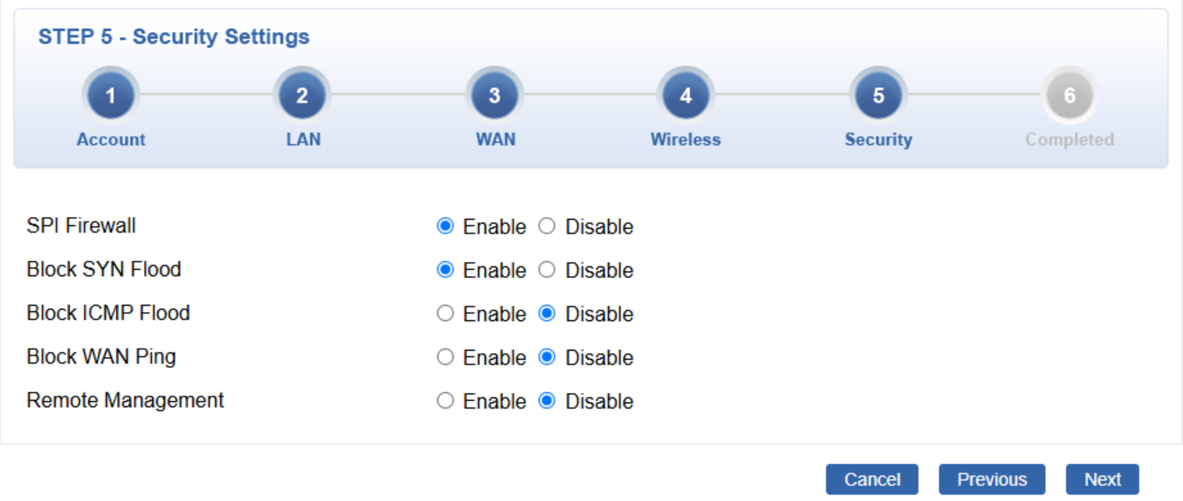
| | |
|---|---|
| 2.4G WiFi Status | ● Enable ○ Disable |
| SSID | PLANET_2.4G |
| Hide SSID | ○Enable ●Disable |
| Bandwidth | 11 N/G 20MHz |
| Channel | 6 |
| Encryption | Open |

**Figure 4-4-6:** Setup Wizard – Wireless Setting

| Object | Description |
|---|---|
| **2.4G Wireless Status** | Allows user to enable or disable 2.4G Wi-Fi |
| **Wireless Name (SSID)** | It is the wireless network name. The default 2.4G SSID is "PLANET_2.4G". |
| **Hide SSID** | Allows user to enable or disable SSID |
| **Bandwidth** | Select the operating channel width, "**20MHz**" or "**40MHz**" |
| **Channel** | It shows the channel of the CPE. Default 2.4GHz is channel 6. |
| **Encryption** | Select the wireless encryption. The default is "**Open**" |

## Step 5: Security Setting

Set up the Wireless Settings as shown in Figure 4-4-7.



SPI Firewall ● Enable ○ Disable

Block SYN Flood ● Enable ○ Disable

Block ICMP Flood ○ Enable ● Disable

Block WAN Ping ○ Enable ● Disable

Remote Management ○ Enable ● Disable

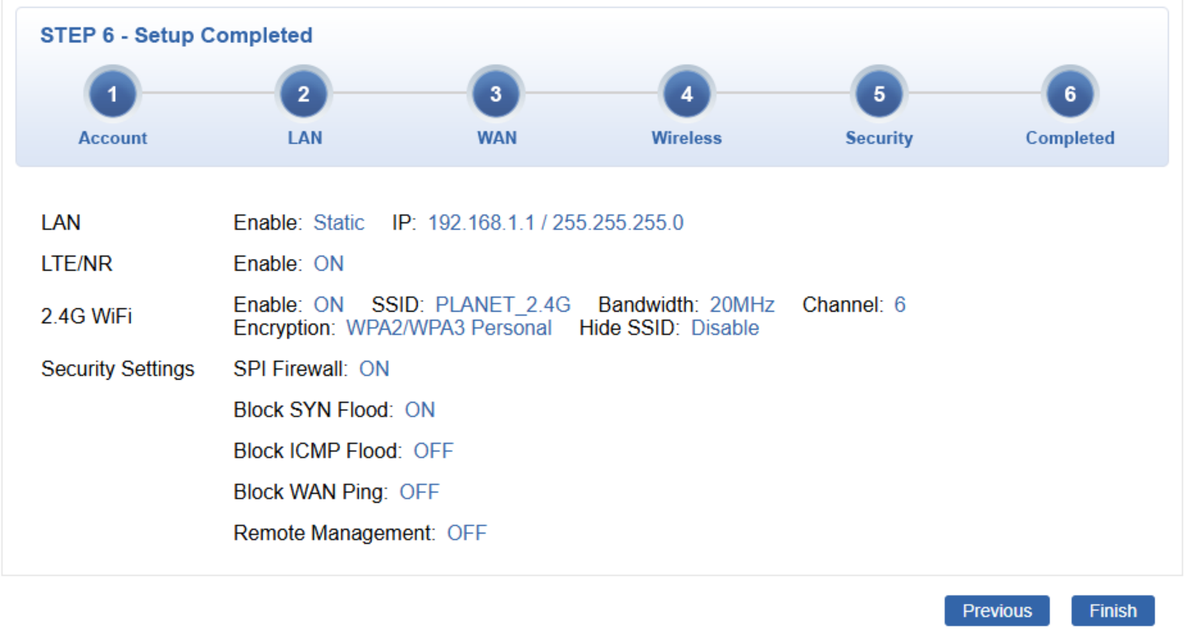
**Figure 4-4-7:** Setup Wizard –Security Setting

| Object | Description |
|---|---|
| **SPI Firewall** | The SPI Firewall prevents attack and improper access to network resources.<br>The default configuration is enabled. |
| **Block SYN Flood** | SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on.<br>The default configuration is enabled. |

| | |
|---|---|
| **Block ICMP Flood** | ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.<br>The default configuration is disabled. |
| **Block WAN Ping** | Enable the function to allow the Ping access from the Internet network.<br>The default configuration is disabled. |
| **Remote Management** | Enable the function to allow the web server access of the LoRaWAN Gateway from the Internet network.<br>The default configuration is disabled. |

## Step 6: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in Figure 4-4-8.


STEP 6 - Setup Completed

LAN — Enable: Static IP: 192.168.1.1 / 255.255.255.0

LTE/NR — Enable: ON

2.4G WiFi — Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHz Channel: 6
Encryption: WPA2/WPA3 Personal Hide SSID: Disable

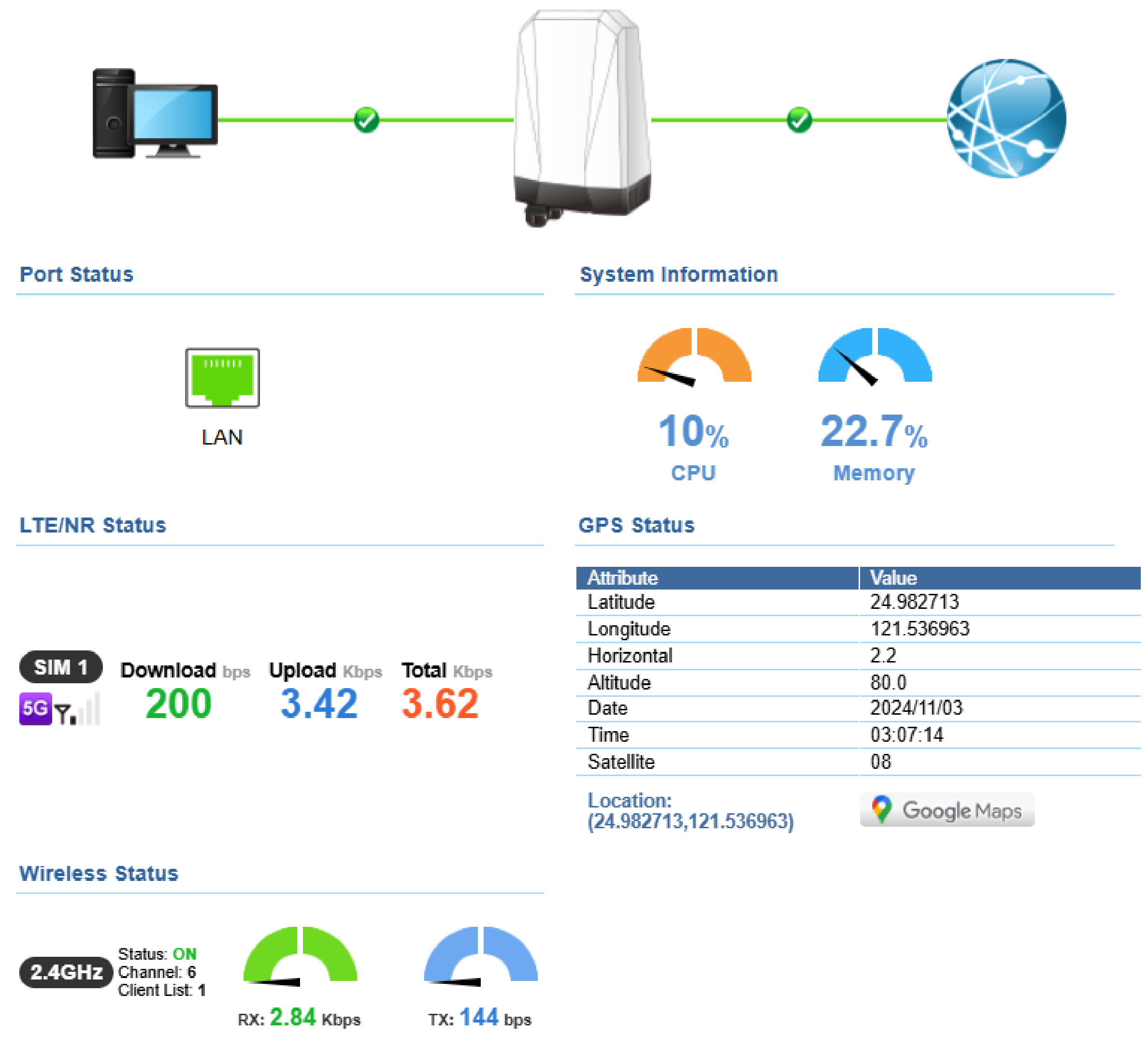
Security Settings — SPI Firewall: ON
Block SYN Flood: ON
Block ICMP Flood: OFF
Block WAN Ping: OFF
Remote Management: OFF

**Figure 4-4-8:** Setup Wizard – Setup Completed

| Object | Description |
|---|---|
| **Finish** | Press this button to save and apply changes. |
| **Previous** | Press this button for the previous step. |

## 4.4.2 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 4-4-12.



Port Status

LAN

System Information

10% CPU

22.7% Memory

LTE/NR Status

SIM 1

5G

Download bps 200

Upload Kbps 3.42

Total Kbps 3.62

GPS Status

| Attribute | Value |
|---|---|
| Latitude | 24.982713 |
| Longitude | 121.536963 |
| Horizontal | 2.2 |
| Altitude | 80.0 |
| Date | 2024/11/03 |
| Time | 03:07:14 |
| Satellite | 08 |

Location:
(24.982713,121.536963)

Google Maps

Wireless Status

2.4GHz

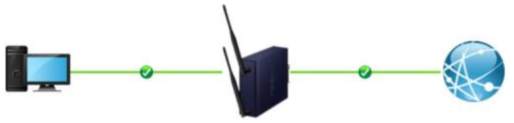
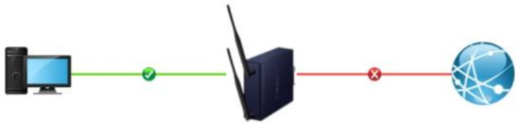
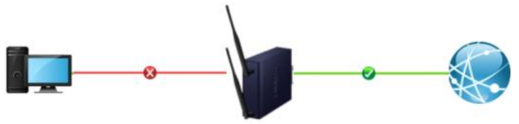
Status: ON
Channel: 6
Client List: 1

RX: 2.84 Kbps

TX: 144 bps

**Figure 4-4-12:** Dashboard

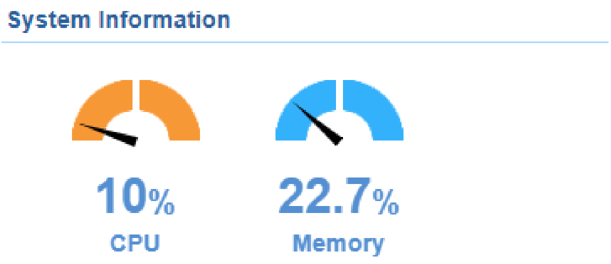
### WAN/LAN Connection Status

| Object | Description |
|---|---|
|  | The status means WAN is connected to Internet and LAN is connected. |
|  | The status means WAN is disconnected to Internet and LAN is connected. |
|  | The status means WAN is connected to Internet and LAN is disconnected. |

### Port Status

| Object | Description |
|---|---|
| 🟩 | Ethernet port is in use. |
| ⬛ | Ethernet port is not in use. |

### System Information



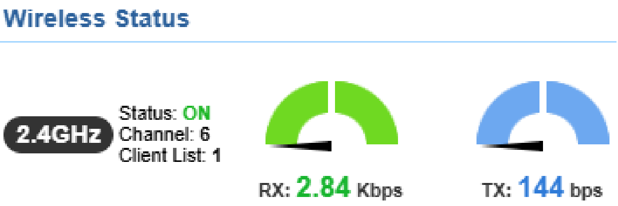
System Information

10% CPU

22.7% Memory

| Object | Description |
|---|---|
| **CPU** | Display the CPU loading |
| **Memory** | Display the memory usage |

### Wireless Status

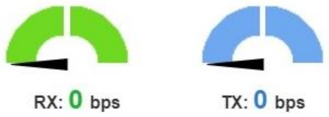
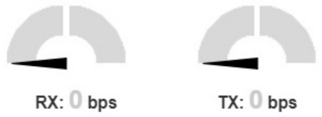


Wireless Status

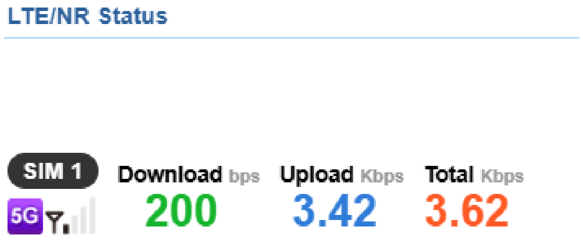
2.4GHz
Status: ON
Channel: 6
Client List: 1

RX: 2.84 Kbps

TX: 144 bps

| Object | Description |
|---|---|
|  | Wireless is in use. |
|  | Wireless is not in use. |

### LTE/NR Status



LTE/NR Status

SIM 1
5G

Download bps
200

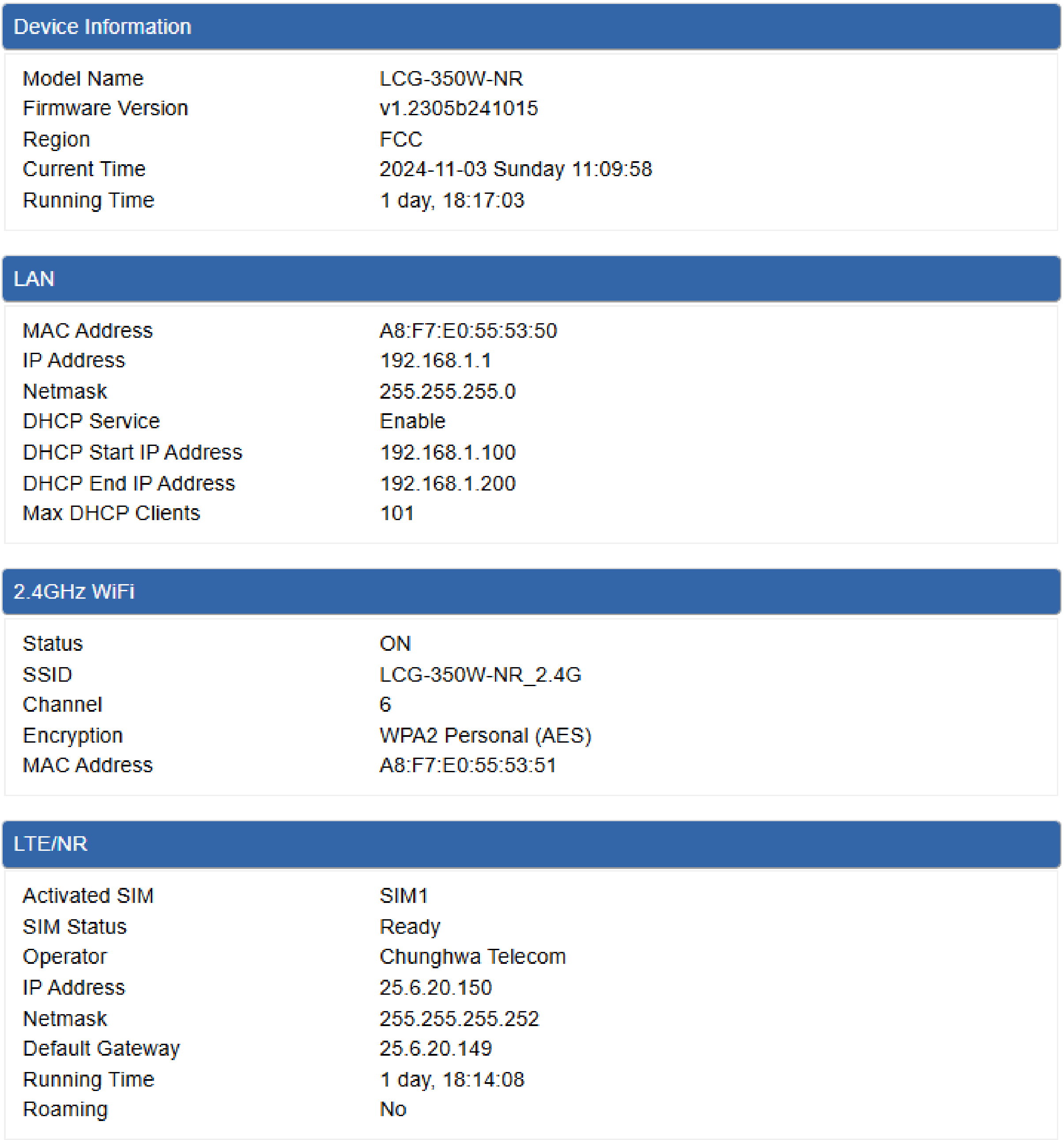
Upload Kbps
3.42

Total Kbps
3.62

| Object | Description |
|---|---|
| **SIM** | SIM signal<br>■ 5G 5G signal<br>■ 4G 4G signal<br>■ 3G 3G signal |
| **Download** | Download data rate of SIM |
| **Upload** | Upload data rate of SIM |
| **Total** | Total data rate of SIM |

## 4.4.3 System Status

This page displays system status information as shown in Figure 4-4-13.



Device Information

| | |
|---|---|
| Model Name | LCG-350W-NR |
| Firmware Version | v1.2305b241015 |
| Region | FCC |
| Current Time | 2024-11-03 Sunday 11:09:58 |
| Running Time | 1 day, 18:17:03 |

LAN

| | |
|---|---|
| MAC Address | A8:F7:E0:55:53:50 |
| IP Address | 192.168.1.1 |
| Netmask | 255.255.255.0 |
| DHCP Service | Enable |
| DHCP Start IP Address | 192.168.1.100 |
| DHCP End IP Address | 192.168.1.200 |
| Max DHCP Clients | 101 |

2.4GHz WiFi

| | |
|---|---|
| Status | ON |
| SSID | LCG-350W-NR_2.4G |
| Channel | 6 |
| Encryption | WPA2 Personal (AES) |
| MAC Address | A8:F7:E0:55:53:51 |

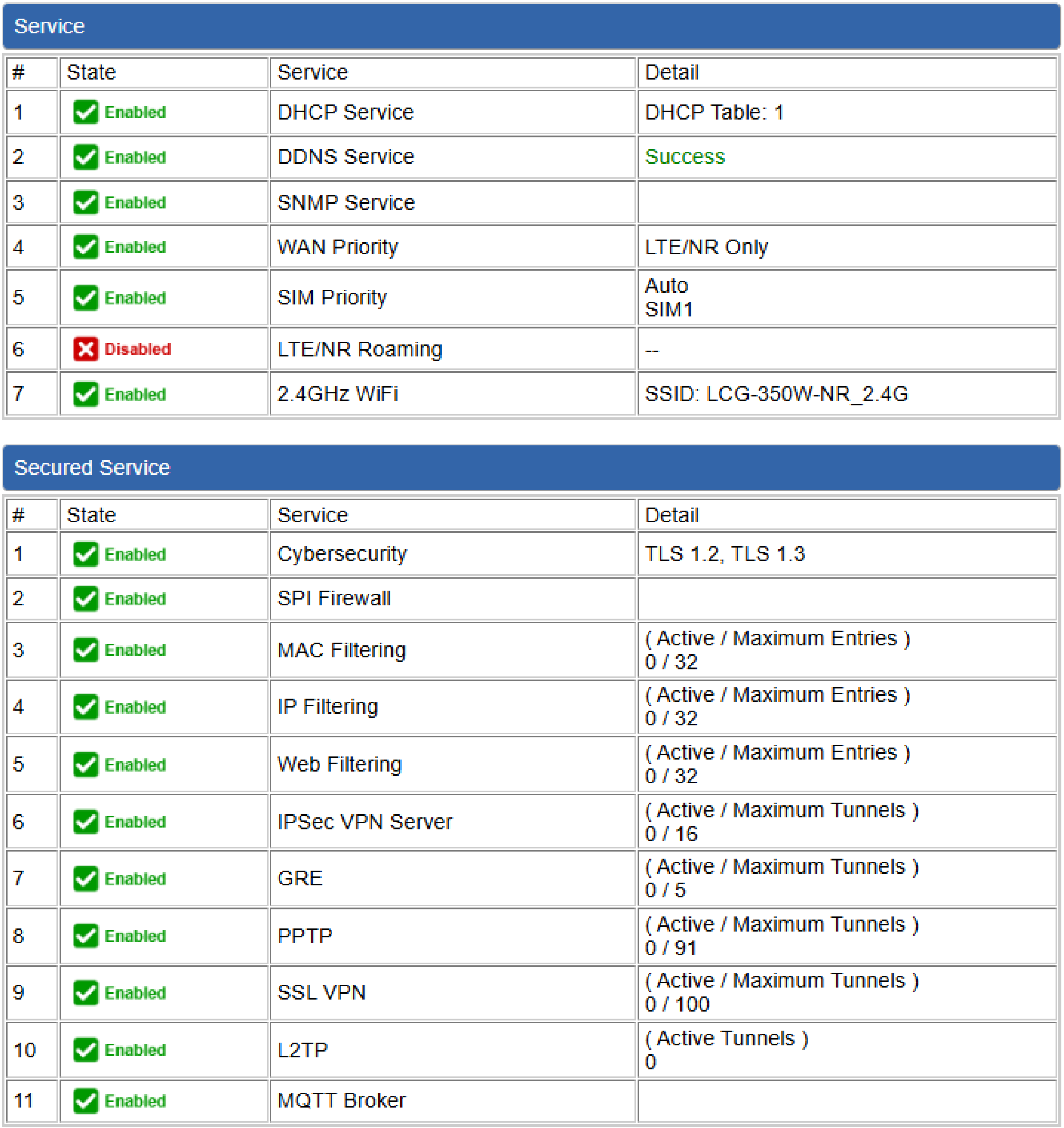
LTE/NR

| | |
|---|---|
| Activated SIM | SIM1 |
| SIM Status | Ready |
| Operator | Chunghwa Telecom |
| IP Address | 25.6.20.150 |
| Netmask | 255.255.255.252 |
| Default Gateway | 25.6.20.149 |
| Running Time | 1 day, 18:14:08 |
| Roaming | No |

**Figure 4-4-13:** System Status

## 4.4.4 System Service

This page displays system service information as shown in Figure 4-4-14.



Service

| # | State | Service | Detail |
|---|---|---|---|
| 1 | ✓ Enabled | DHCP Service | DHCP Table: 1 |
| 2 | ✓ Enabled | DDNS Service | Success |
| 3 | ✓ Enabled | SNMP Service | |
| 4 | ✓ Enabled | WAN Priority | LTE/NR Only |
| 5 | ✓ Enabled | SIM Priority | Auto<br>SIM1 |
| 6 | ✗ Disabled | LTE/NR Roaming | -- |
| 7 | ✓ Enabled | 2.4GHz WiFi | SSID: LCG-350W-NR_2.4G |

Secured Service

| # | State | Service | Detail |
|---|---|---|---|
| 1 | ✓ Enabled | Cybersecurity | TLS 1.2, TLS 1.3 |
| 2 | ✓ Enabled | SPI Firewall | |
| 3 | ✓ Enabled | MAC Filtering | ( Active / Maximum Entries )<br>0 / 32 |
| 4 | ✓ Enabled | IP Filtering | ( Active / Maximum Entries )<br>0 / 32 |
| 5 | ✓ Enabled | Web Filtering | ( Active / Maximum Entries )<br>0 / 32 |
| 6 | ✓ Enabled | IPSec VPN Server | ( Active / Maximum Tunnels )<br>0 / 16 |
| 7 | ✓ Enabled | GRE | ( Active / Maximum Tunnels )<br>0 / 5 |
| 8 | ✓ Enabled | PPTP | ( Active / Maximum Tunnels )<br>0 / 91 |
| 9 | ✓ Enabled | SSL VPN | ( Active / Maximum Tunnels )<br>0 / 100 |
| 10 | ✓ Enabled | L2TP | ( Active Tunnels )<br>0 |
| 11 | ✓ Enabled | MQTT Broker | |

**Figure 4-4-14:** System Service

## 4.4.5 Statistics

This page displays the number of packets that pass through the LoRaWAN Gateway on the LAN. The statistics are shown in Figure 4-4-15.

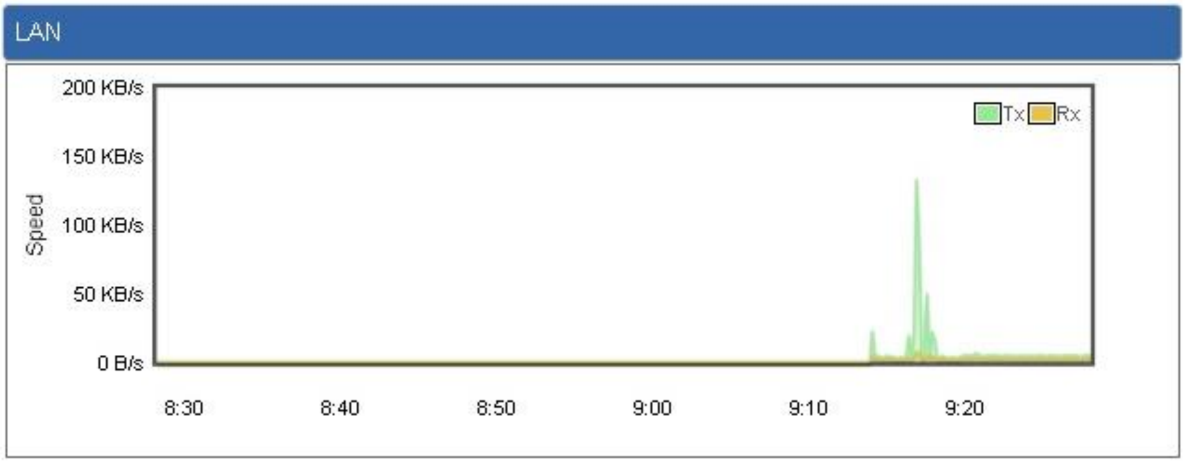
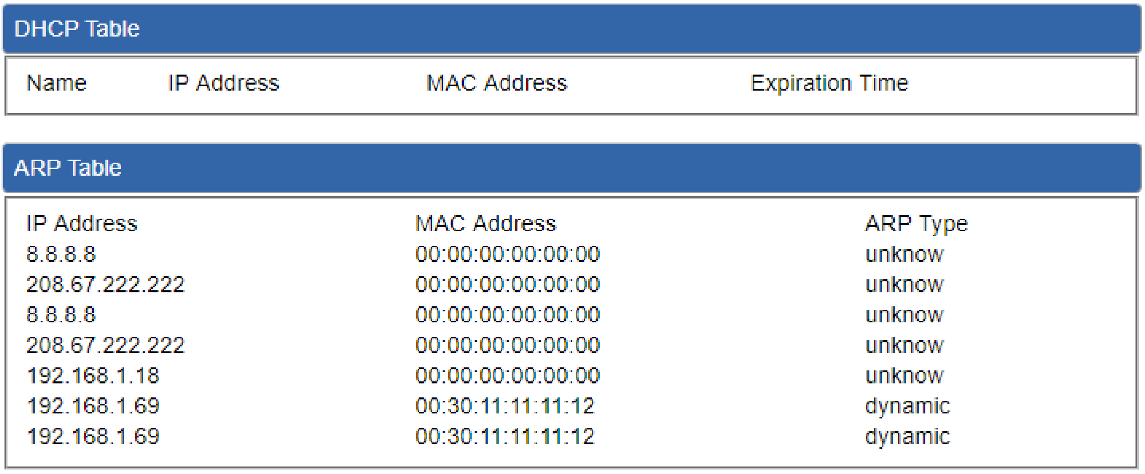


**Figure 4-4-15:** Statistics

## 4.4.6 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in Figure 4-4-16.



DHCP Table

| Name | IP Address | MAC Address | Expiration Time |
|---|---|---|---|

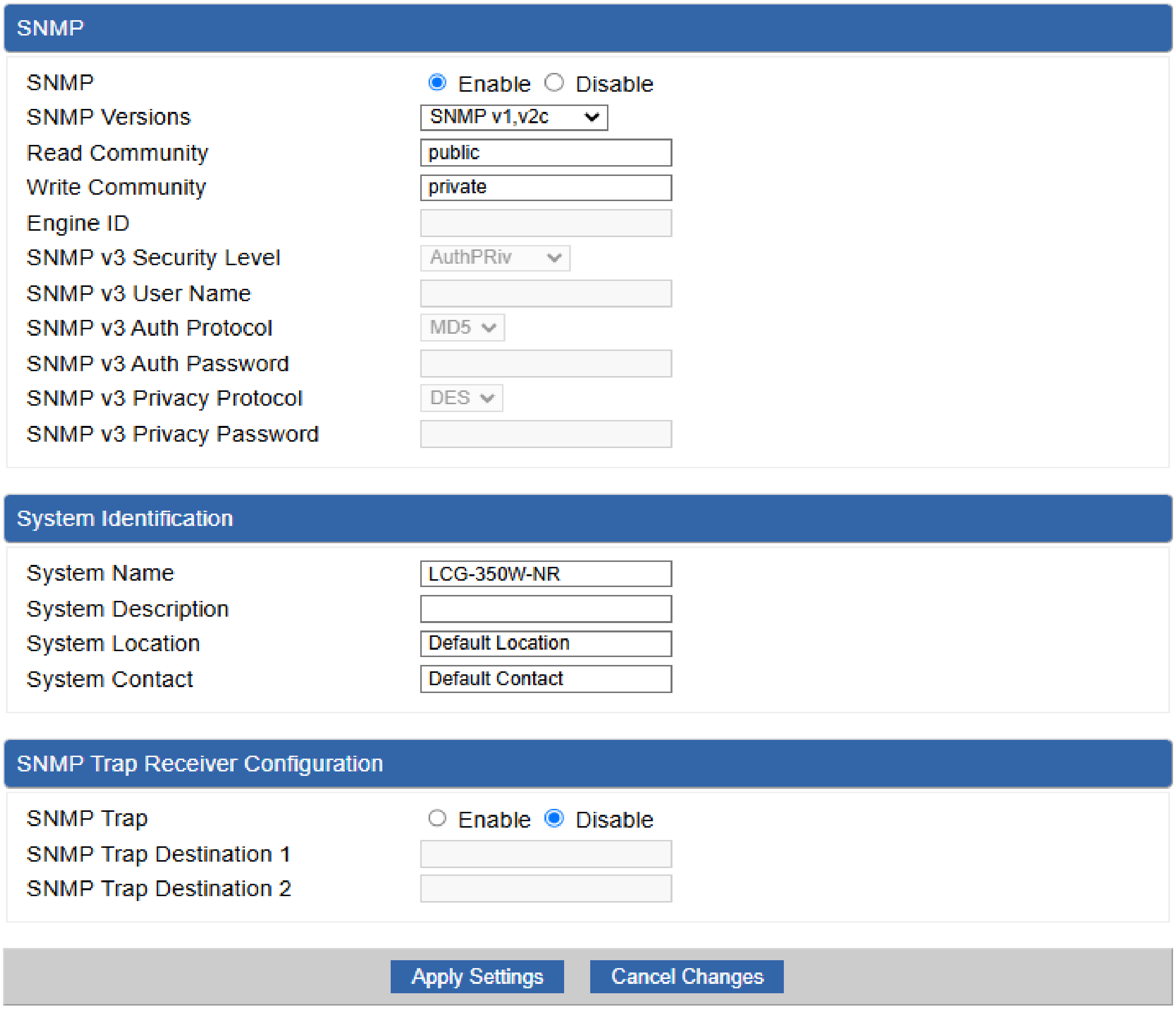
ARP Table

| IP Address | MAC Address | ARP Type |
|---|---|---|
| 8.8.8.8 | 00:00:00:00:00:00 | unknow |
| 208.67.222.222 | 00:00:00:00:00:00 | unknow |
| 8.8.8.8 | 00:00:00:00:00:00 | unknow |
| 208.67.222.222 | 00:00:00:00:00:00 | unknow |
| 192.168.1.18 | 00:00:00:00:00:00 | unknow |
| 192.168.1.69 | 00:30:11:11:11:12 | dynamic |
| 192.168.1.69 | 00:30:11:11:11:12 | dynamic |

**Figure 4-4-16:** Connection Status

## 4.4.7 SNMP

This page provides SNMP setting as shown in Figure 4-4-21.



SNMP

| | |
|---|---|
| SNMP | ● Enable ○ Disable |
| SNMP Versions | SNMP v1,v2c |
| Read Community | public |
| Write Community | private |
| Engine ID | |
| SNMP v3 Security Level | AuthPRiv |
| SNMP v3 User Name | |
| SNMP v3 Auth Protocol | MD5 |
| SNMP v3 Auth Password | |
| SNMP v3 Privacy Protocol | DES |
| SNMP v3 Privacy Password | |

System Identification

| | |
|---|---|
| System Name | LCG-350W-NR |
| System Description | |
| System Location | Default Location |
| System Contact | Default Contact |

SNMP Trap Receiver Configuration

| | |
|---|---|
| SNMP Trap | ○ Enable ● Disable |
| SNMP Trap Destination 1 | |
| SNMP Trap Destination 2 | |

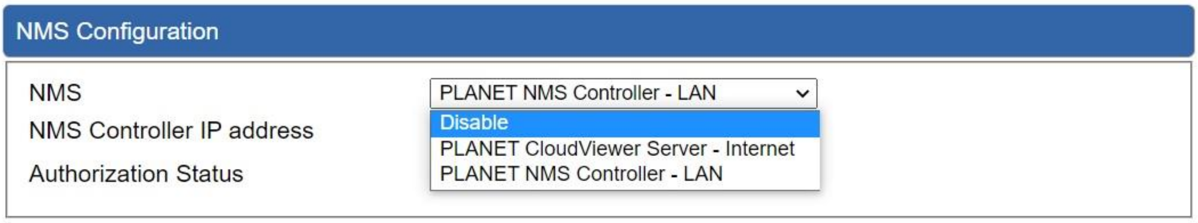
**Figure 4-4-21:** SNMP

| Object | Description |
|---|---|
| **Enable SNMP** | Disable or enable the SNMP function.<br>The default configuration is enabled. |
| **Read/Write Community** | Allows entering characters for SNMP Read/Write Community of the LoRaWAN Gateway |
| **System Name** | Allows entering characters for system name of the LoRaWAN Gateway |
| **System Location** | Allows entering characters for system location of the LoRaWAN Gateway |
| **System Contact** | Allows entering characters for system contact of the LoRaWAN Gateway |
| **Apply Settings** | Press this button to save and apply changes. |
| **Cancel Changes** | Press this button to undo any changes made locally and revert to previously saved values. |

## 4.4.8 NMS

The LCG-300 series can support both NMS controller and CloudViewer Sever for remote management. PLANET's NMS Controller is a Network Management System that can monitor all kinds of deployed network devices, such as managed switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The CloudViewer is a free networking service just for PLANET Products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudViewer app, user can easily check network status, device information, Port and PoE status from Internet. Other services are not included.

NMS Configuration is shown in Figure 4-4-22.



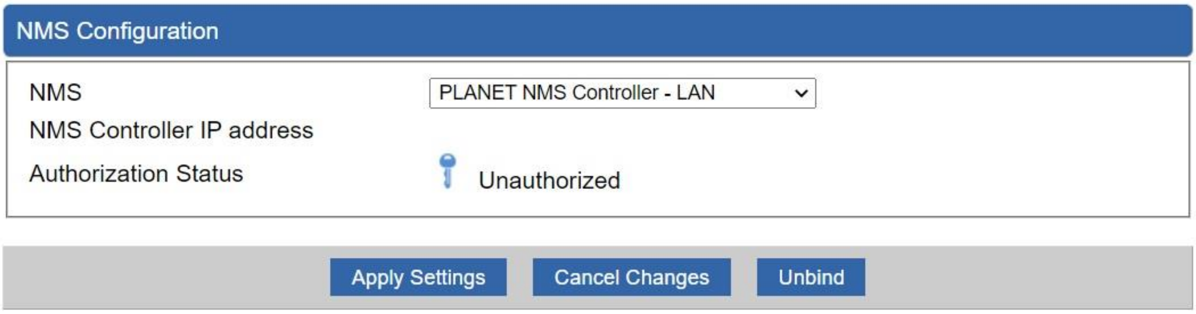
NMS Configuration

| | |
|---|---|
| NMS | PLANET NMS Controller - LAN |
| NMS Controller IP address | |
| Authorization Status | |

Disable
PLANET CloudViewer Server - Internet
PLANET NMS Controller - LAN

**Figure 4-4-22** NMS Configuration Page

LAN Configuration is shown in Figure 4-4-23.



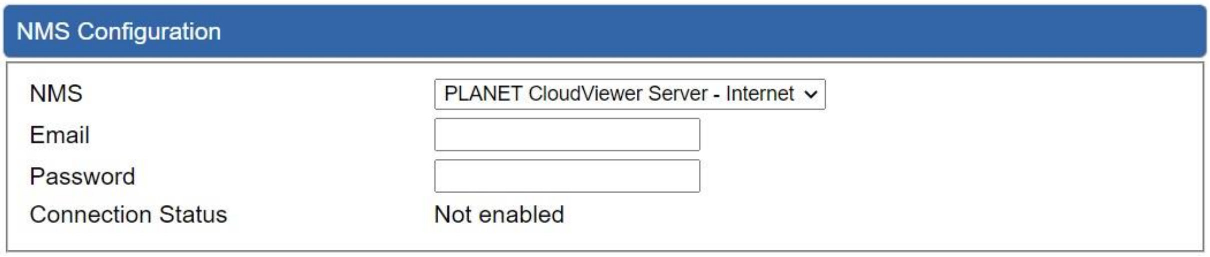
NMS Configuration

| | |
|---|---|
| NMS | PLANET NMS Controller - LAN |
| NMS Controller IP address | |
| Authorization Status | Unauthorized |

**Figure 4-4-23** NMS Controller – LAN Configuration Page

| Object | Description |
|---|---|
| **NMS Controller IP address** | The IP address of NMS Controller |
| **Authorization Status** | Indicates the authorization status of the switch to NMS Controller |

The CloudViewer Server – Internet configuration – is shown in Figure 4-4-24.



NMS Configuration

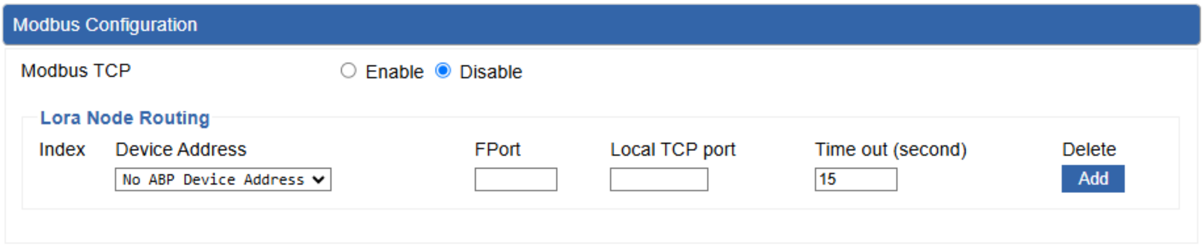
| | |
|---|---|
| NMS | PLANET CloudViewer Server - Internet |
| Email | |
| Password | |
| Connection Status | Not enabled |

**Figure 4-4-24** CloudViewer Server – Internet Configuration Page

| Object | Description |
|---|---|
| **Email** | The email registered on CloudViewer Server |
| **Password** | The password of your CloudViewer account |
| **Connection Status** | Indicates the status of connecting CloudViewer Server |

### 4.4.9 Modbus

This page provides Modbus setting as shown in Figure 4-4-25.



Modbus Configuration

Modbus TCP ○ Enable ● Disable

Lora Node Routing

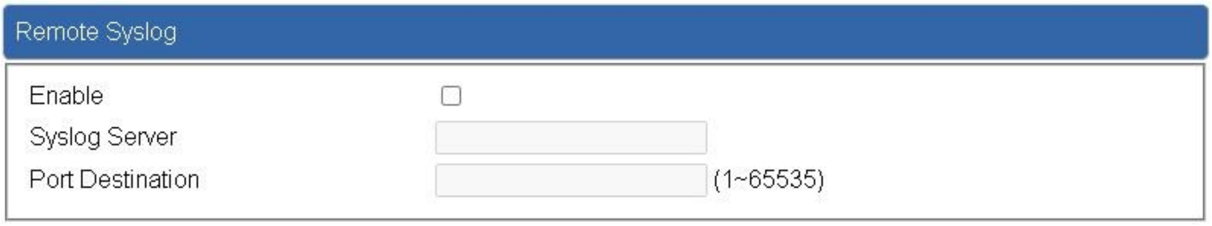
| Index | Device Address | FPort | Local TCP port | Time out (second) | Delete |
|---|---|---|---|---|---|
| | No ABP Device Address | | | 15 | Add |

**Figure 4-4-25:** Modbus

| Object | Description |
|---|---|
| **Enable** | Enable/disable Modbus function. |
| **Device Access** | The device address of the LoRaWAN sensor. |
| **FPort** | The port field in the data packet (Frame Port) |
| **Local TCP port** | The port is used for the TCP connection that corresponds to the specific FPort. |
| **Time out** | The timeout duration for waiting on a TCP connection response.<br>The default is 15. |
| **Add** | Add the rule of LoRa Node routing. |
| **Delete** | Delete the rule of LoRa Node routing. |

## 4.4.10 Remote Syslog

This page provides remote syslog setting as shown in Figure 4-4-26.



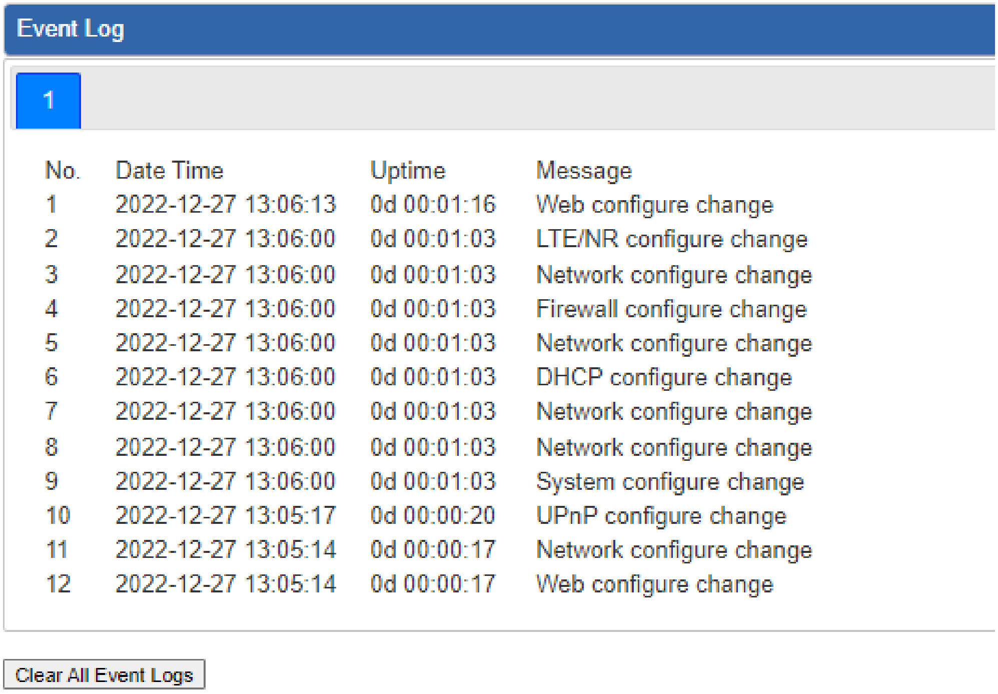
| | | |
|---|---|---|
| Enable | □ | |
| Syslog Server | | |
| Port Destination | | (1~65535) |

**Figure 4-4-26:** Remote Syslog

| Object | Description |
|---|---|
| **Enable** | Controls whether remote syslog is enabled |
| **Syslog Server IP** | Indicates the IPv4 host address of syslog server |
| **Port Destination** | Configure port for remote syslog |

## 4.4.11 Event Log

This page provides Event Log as shown below.



| No. | Date Time | Uptime | Message |
|---|---|---|---|
| 1 | 2022-12-27 13:06:13 | 0d 00:01:16 | Web configure change |
| 2 | 2022-12-27 13:06:00 | 0d 00:01:03 | LTE/NR configure change |
| 3 | 2022-12-27 13:06:00 | 0d 00:01:03 | Network configure change |
| 4 | 2022-12-27 13:06:00 | 0d 00:01:03 | Firewall configure change |
| 5 | 2022-12-27 13:06:00 | 0d 00:01:03 | Network configure change |
| 6 | 2022-12-27 13:06:00 | 0d 00:01:03 | DHCP configure change |
| 7 | 2022-12-27 13:06:00 | 0d 00:01:03 | Network configure change |
| 8 | 2022-12-27 13:06:00 | 0d 00:01:03 | Network configure change |
| 9 | 2022-12-27 13:06:00 | 0d 00:01:03 | System configure change |
| 10 | 2022-12-27 13:05:17 | 0d 00:00:20 | UPnP configure change |
| 11 | 2022-12-27 13:05:14 | 0d 00:00:17 | Network configure change |
| 12 | 2022-12-27 13:05:14 | 0d 00:00:17 | Web configure change |

**Figure 4-4-27:** Remote Syslog

## 4.5 Network

The Network function provides LAN and network configurations of the LoRaWAN Gateway as shown in Figure 4-5-1.

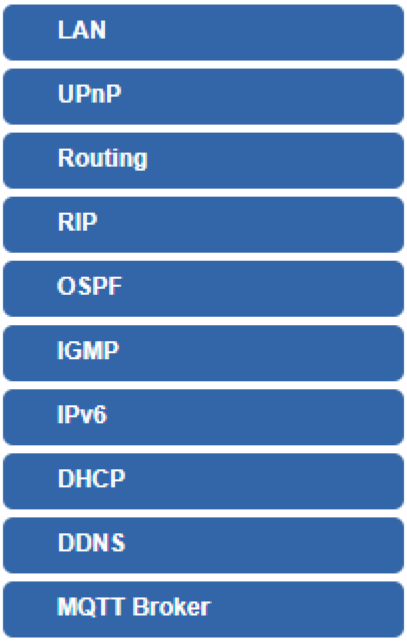
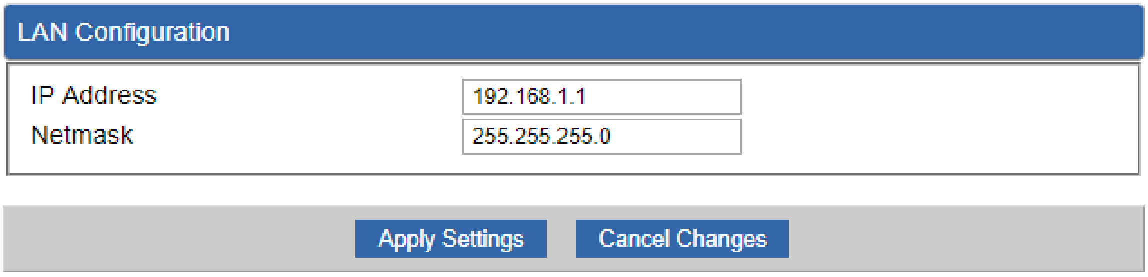


**Figure 4-5-1:** Network Menu

| Object | Description |
|---|---|
| **LAN** | Allows setting LAN interface. |
| **UPnP** | Disable or enable the UPnP function.<br>The default configuration is disabled. |
| **Routing** | Allows setting Route. |
| **RIP** | Disable or enable the RIP function.<br>The default configuration is disabled. |
| **OSPF** | Disable or enable the OSPF function.<br>The default configuration is disabled. |
| **IGMP** | Disable or enable the IGMP function.<br>The default configuration is disabled. |
| **IPv6** | Allows setting IPv6 WAN interface. |
| **DHCP** | Allows setting DHCP Server. |
| **DDNS** | Allows setting DDNS and PLANET DDNS. |
| **MAC Address Clone** | Allows setting WAN MAC Address Clone. |

## 4.5.1 LAN Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your LoRaWAN Gateway as shown in Figure 4-5-4. Here you may change the settings for IP address, subnet mask, DHCP, etc.



LAN Configuration

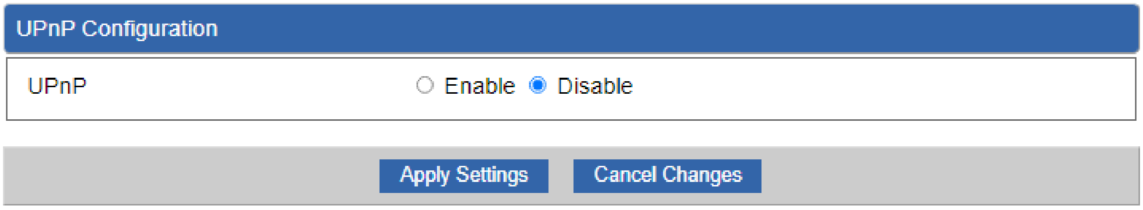
IP Address: 192.168.1.1
Netmask: 255.255.255.0

**Figure 4-5-4:** LAN Setup

| Object | Description |
|---|---|
| **IP Address** | The LAN IP address of the LoRaWAN Gateway and default is **192.168.1.1**. |
| **Net Mask** | Default is **255.255.255.0**. |

## 4.5.2 UPnP

Please refer to the following sections for the details as shown below.



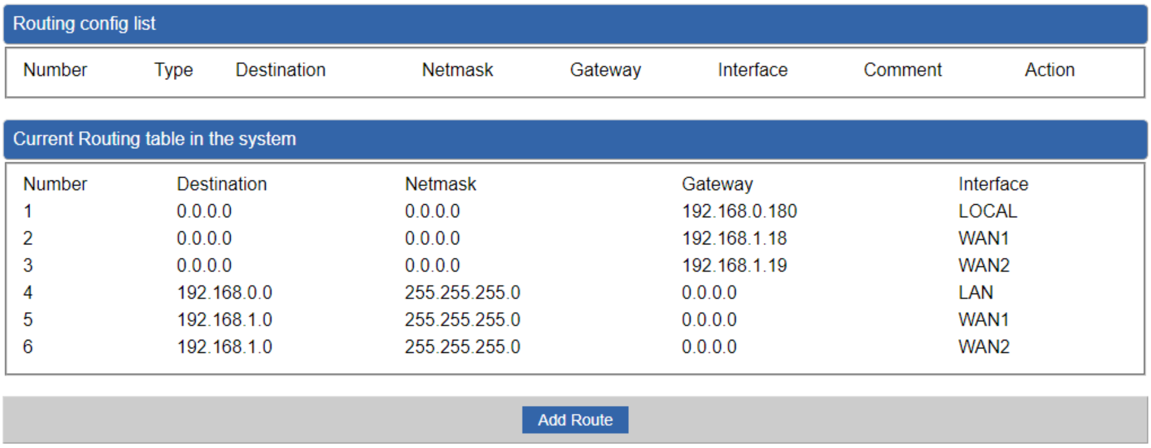
UPnP Configuration

UPnP: ○ Enable ● Disable

Figure: VLAN Configuration

### 4.5.3 Routing

Please refer to the following sections for the details as shown in Figures 4-5-6 and 4-5-7.



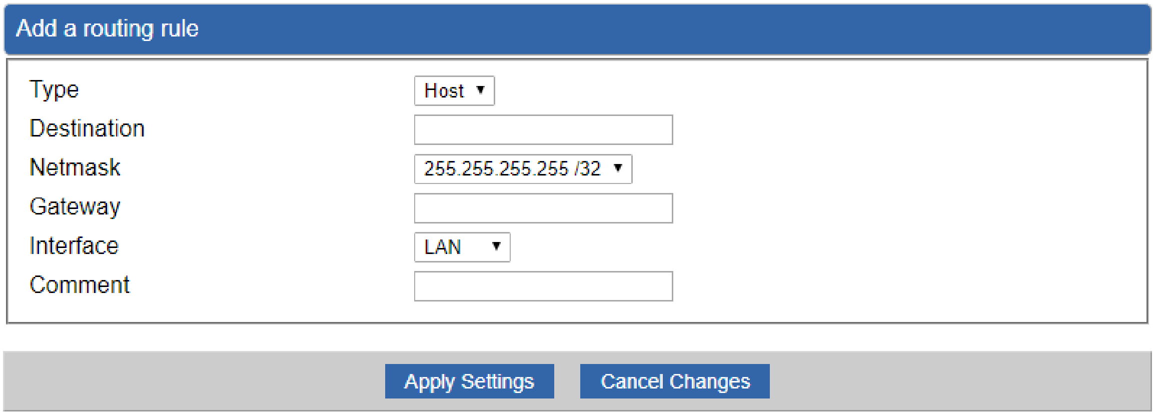
Routing config list

| Number | Type | Destination | Netmask | Gateway | Interface | Comment | Action |
|---|---|---|---|---|---|---|---|

Current Routing table in the system

| Number | Destination | Netmask | Gateway | Interface |
|---|---|---|---|---|
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.0.180 | LOCAL |
| 2 | 0.0.0.0 | 0.0.0.0 | 192.168.1.18 | WAN1 |
| 3 | 0.0.0.0 | 0.0.0.0 | 192.168.1.19 | WAN2 |
| 4 | 192.168.0.0 | 255.255.255.0 | 0.0.0.0 | LAN |
| 5 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | WAN1 |
| 6 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | WAN2 |

**Figure 4-5-6:** Routing table



Add a routing rule

| | |
|---|---|
| Type | Host ▾ |
| Destination | |
| Netmask | 255.255.255.255 /32 ▾ |
| Gateway | |
| Interface | LAN ▾ |
| Comment | |

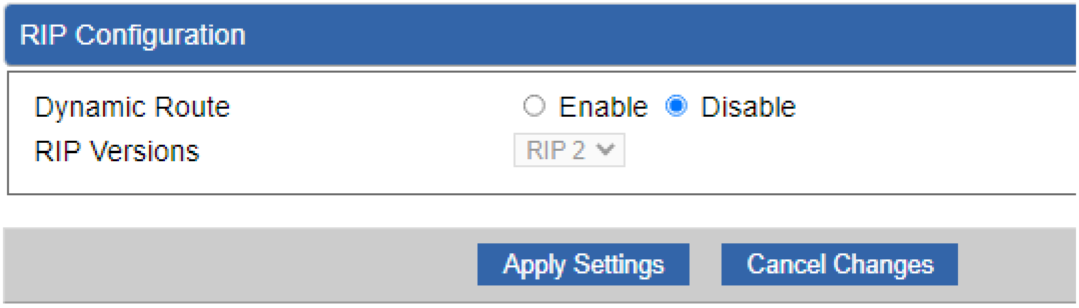
**Figure 4-5-7:** Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote LoRaWAN Gateway (or other network gateway) that the local LoRaWAN Gateway is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.

| Object | Description |
|---|---|
| **Type** | There are two types: Host and Net.<br>When the Net type is selected, user does not need to input the Gateway. |
| **Destination** | The network or host IP address desired to access. |
| **Net Mask** | The subnet mask of destination IP. |
| **Gateway** | The gateway is the router or host's IP address to which packet was sent. It must be the same network segment with the WAN or LAN port. |
| **Interface** | Select the interface that the IP packet must use to transmit out of the router when this route is used. |
| **Comment** | Enter any words for recognition. |

## 4.5.4 RIP

Please refer to the following sections for the details as shown below.



RIP Configuration

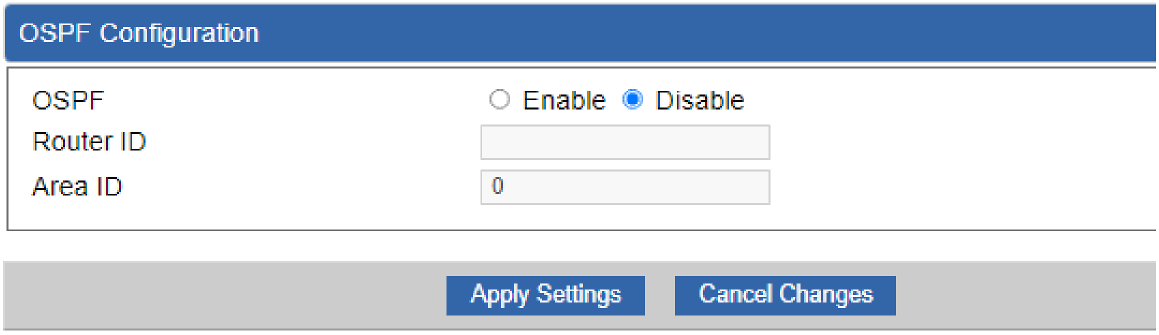
Dynamic Route ○ Enable ● Disable

RIP Versions RIP 2

**Figure:** OSPF Configuration table

## 4.5.5 OSPF

Please refer to the following sections for the details as shown below.



OSPF Configuration

OSPF ○ Enable ● Disable

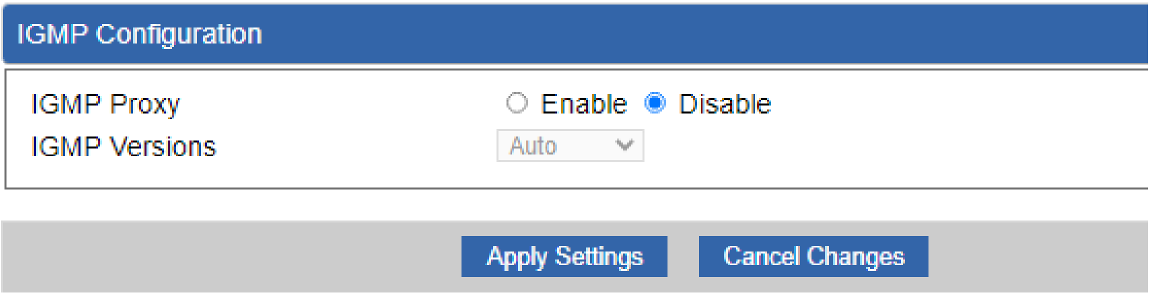
Router ID

Area ID 0

**Figure:** Routing table

## 4.5.6 IGMP

Please refer to the following sections for the details as shown below.



IGMP Configuration

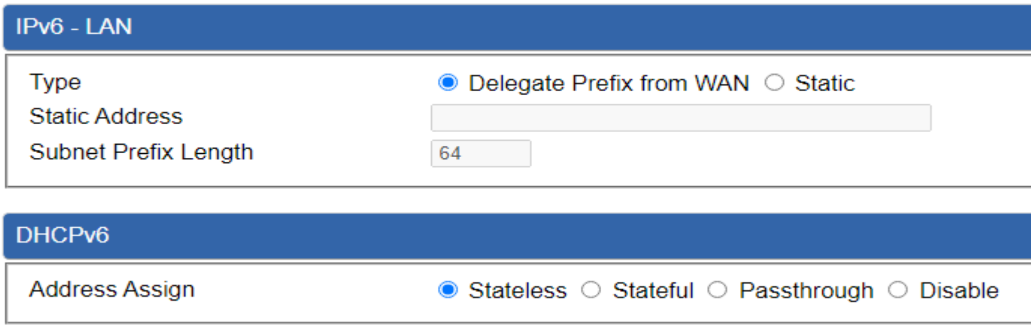
IGMP Proxy ○ Enable ● Disable

IGMP Versions Auto

**Figure:** Routing table

## 4.5.7 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in Figure 4-33. It allows you to enable IPv6 function and set up the parameters of the router's WAN. In this setting you may change WAN connection type and other settings.



IPv6 - LAN

| | |
|---|---|
| Type | ● Delegate Prefix from WAN ○ Static |
| Static Address | |
| Subnet Prefix Length | 64 |

DHCPv6

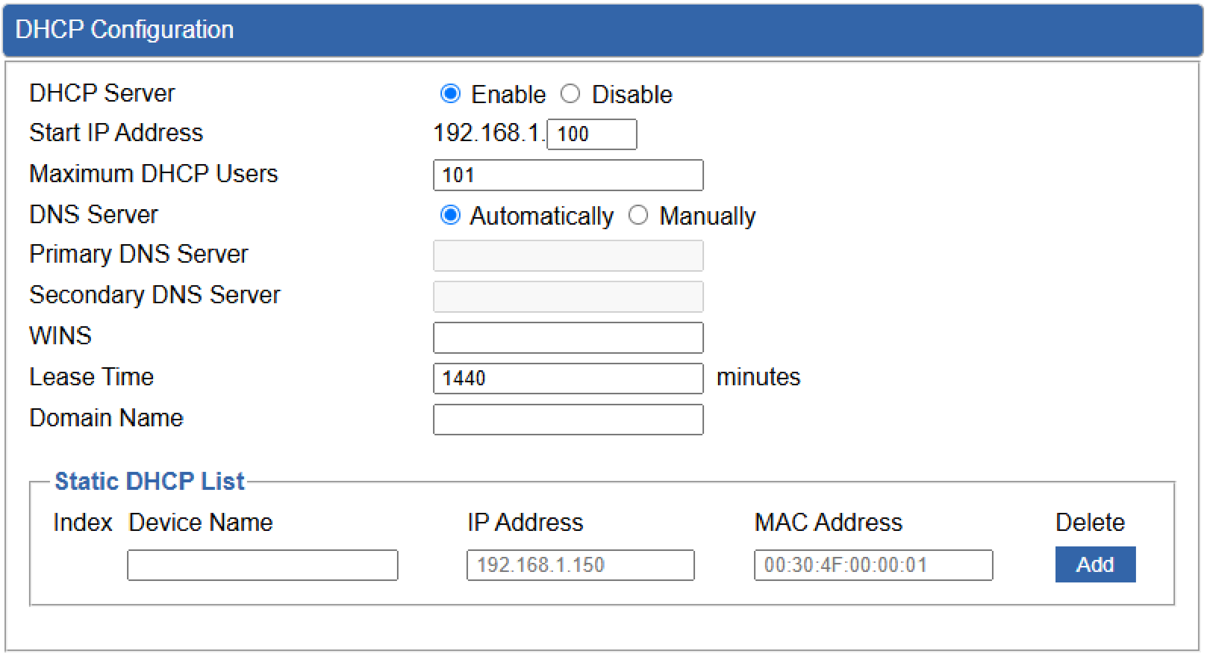
| | |
|---|---|
| Address Assign | ● Stateless ○ Stateful ○ Passthrough ○ Disable |

**Figure 4-33:** IPv6 WAN setup

| Object | Description |
|---|---|
| **Connection Type** | Select IPv6 WAN type either by using DHCP or Static. |
| **IPv6 Address** | Enter the WAN IPv6 address. |
| **Subnet Prefix Length** | Enter the subnet prefix length. |
| **Default Gateway** | Enter the default gateway of the WAN port. |

## 4.5.8 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network, it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown in Figure 4-5-9.



DHCP Configuration

| | |
|---|---|
| DHCP Server | ● Enable ○ Disable |
| Start IP Address | 192.168.1. 100 |
| Maximum DHCP Users | 101 |
| DNS Server | ● Automatically ○ Manually |
| Primary DNS Server | |
| Secondary DNS Server | |
| WINS | |
| Lease Time | 1440 minutes |
| Domain Name | |

Static DHCP List

| Index | Device Name | IP Address | MAC Address | Delete |
|---|---|---|---|---|
| | | 192.168.1.150 | 00:30:4F:00:00:01 | Add |

**Figure 4-5-9:** DHCP

| Object | Description |
|---|---|
| **DHCP Service** | By default, the DHCP Server is enabled, meaning the LoRaWAN Gateway will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable. |
| **Start IP Address** | By default, the start IP address is 192.168.1.100.<br>Please do not set it to the same IP address of the LoRaWAN Gateway |
| **Maximum DHCP Users** | By default, the maximum number of DHCP clients is 101, meaning the LoRaWAN Gateway will provide DHCP clients with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100. |
| **Set DNS** | By default, it is set as Automatically, and the DNS server is the LoRaWAN Gateway's LAN IP address. |

| Object | Description |
|---|---|
| | If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server. |
| **Primary/Secondary DNS Server** | Input a specific DNS server. |
| **WINS** | Input a WINS server if needed. |
| **Lease Time** | Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the LoRaWAN Gateway<br>Default is 1440 minutes. |
| **Domain Name** | Input a domain name for the LoRaWAN Gateway<br>Default is Planet. |

### 4.5.9 DDNS

The LoRaWAN Gateway offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS (**http://www.planetddns.com**)** and set up the domain name of your choice.

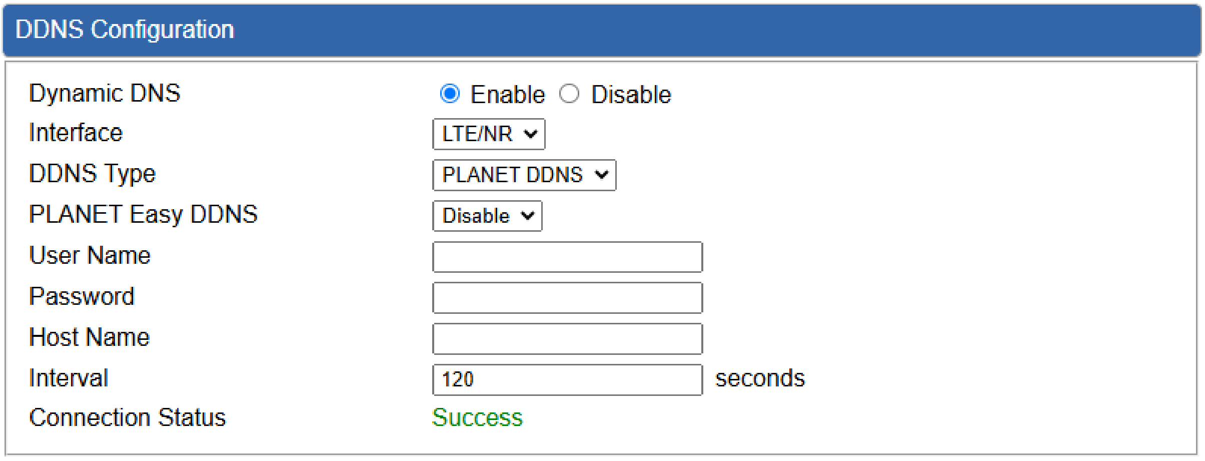
PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in Figure 4-5-10.

**PLANET DDNS**

For example, you've just installed a PLANET IP camera with dynamic IP like 210.66.155.93 in the network. You can name this device as “Mycam1” and register a domain as Mycam1.planetddns.com at PLANET DDNS (http://www.planetddns.com). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

**PLANET Easy DDNS**

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your LoRaWAN Gateway, and check the DDNS menu and just enable it. You don’t need to go to http://www.planetddns.com to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the LoRaWAN Gateway’s MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)



DDNS Configuration

| | |
|---|---|
| Dynamic DNS | ● Enable ○ Disable |
| Interface | LTE/NR |
| DDNS Type | PLANET DDNS |
| PLANET Easy DDNS | Disable |
| User Name | |
| Password | |
| Host Name | |
| Interval | 120 seconds |
| Connection Status | Success |

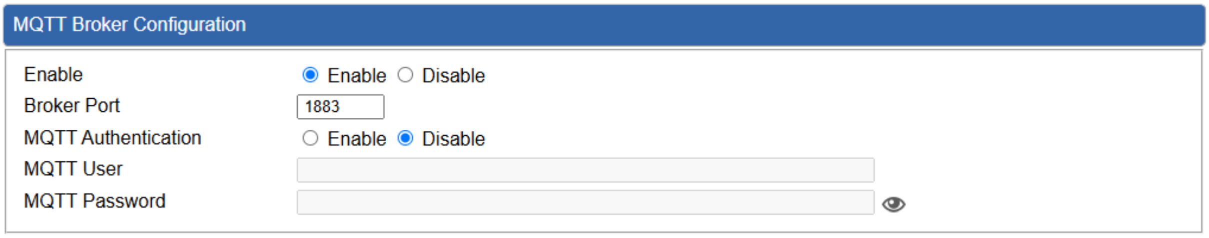
**Figure 4-5-10:** PLANET DDNS

| Object | Description |
|---|---|
| **DDNS Service** | By default, the DDNS service is disabled.<br>If user needs to enable the function, please set it as enable. |
| **Interface** | User is able to select the interface for DDNS service.<br>By default, the interface is WAN 1. |
| **DDNS Type** | There are three options:<br>1. PLANET DDNS: Activate PLANET DDNS service.<br>2. DynDNS: Activate DynDNS service.<br>3. NOIP: Activate NOIP service.<br>Note that please first register with the DDNS service and set up the domain name of your choice to begin using it. |
| **Easy DDNS** | When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS.<br>When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account. |
| **User Name** | The user name is used to log in to DDNS service. |
| **Password** | The password is used to log in to DDNS service. |
| **Host Name** | The host name as registered with your DDNS provider. |
| **Interval** | Set the update interval of the DDNS function. |
| **Update Status** | Show the connection status of the DDNS function. |

## 4.5.10 MQTT Broker

The MQTT Broker serves as the central hub in an MQTT (Message Queuing Telemetry Transport) system, managing message exchanges between clients. Its main functions include receiving messages from publishers, filtering them, and routing them to subscribers based on topic filters. This architecture is commonly used in IoT (Internet of Things) applications, where devices need to exchange data in a lightweight, efficient, and reliable manner. Common applications include smart homes, remote monitoring, and industrial automation.

The MQTT Broker settings for the LoRaWAN Gateway are shown in Figure 4-5-11.



MQTT Broker Configuration

Enable: ● Enable ○ Disable
Broker Port: 1883
MQTT Authentication: ○ Enable ● Disable
MQTT User:
MQTT Password:

**Figure 4-5-11: MQTT Broker settings**

| Object | Description |
|---|---|
| **Broker Port** | The port of MQTT broker server |
| **MQTT Authentication** | Enable or disable the local MQTT Broker Authentication |
| **MQTT User** | The user name for MQTT broker |
| **MQTT Password** | The password for MQTT broker |

## 4.6 Cellular

The Cellular menu provides LTE/NR related functions as shown in Figure 4-6-1. Please refer to the following sections for the details.

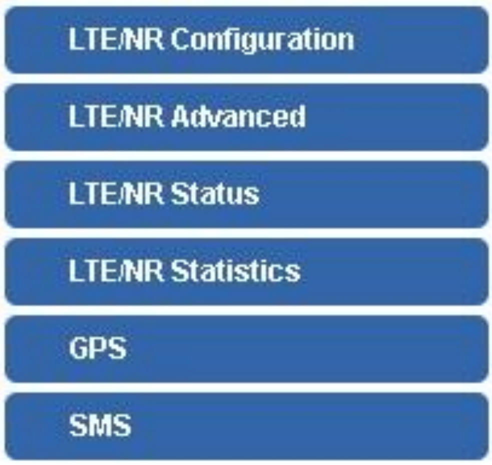
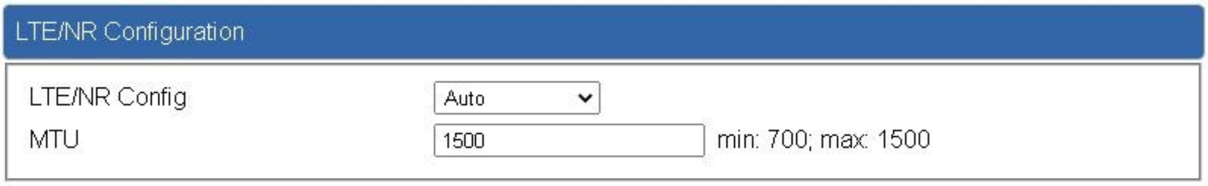


**Figure 4-6-1:** Cellular menu

| Object | Description |
|---|---|
| **LTE/NR Configuration** | Allows setting LTE/NR configuration. |
| **LTE/NR Advanced** | Allows setting SIM configuration. |
| **LTE/NR Status** | Displays the status of cellular. |
| **LTE/NR Statistics** | Displays the statistics of cellular. |
| **GPS** | Displays the location of cellular gateway. |
| **SMS** | Allows setting SMS configuration for alarm notification. |

### 4.6.1 LTE/NR Configuration

This page provides LTE/NR configuration as shown in Figure 4-6-2.



LTE/NR Configuration

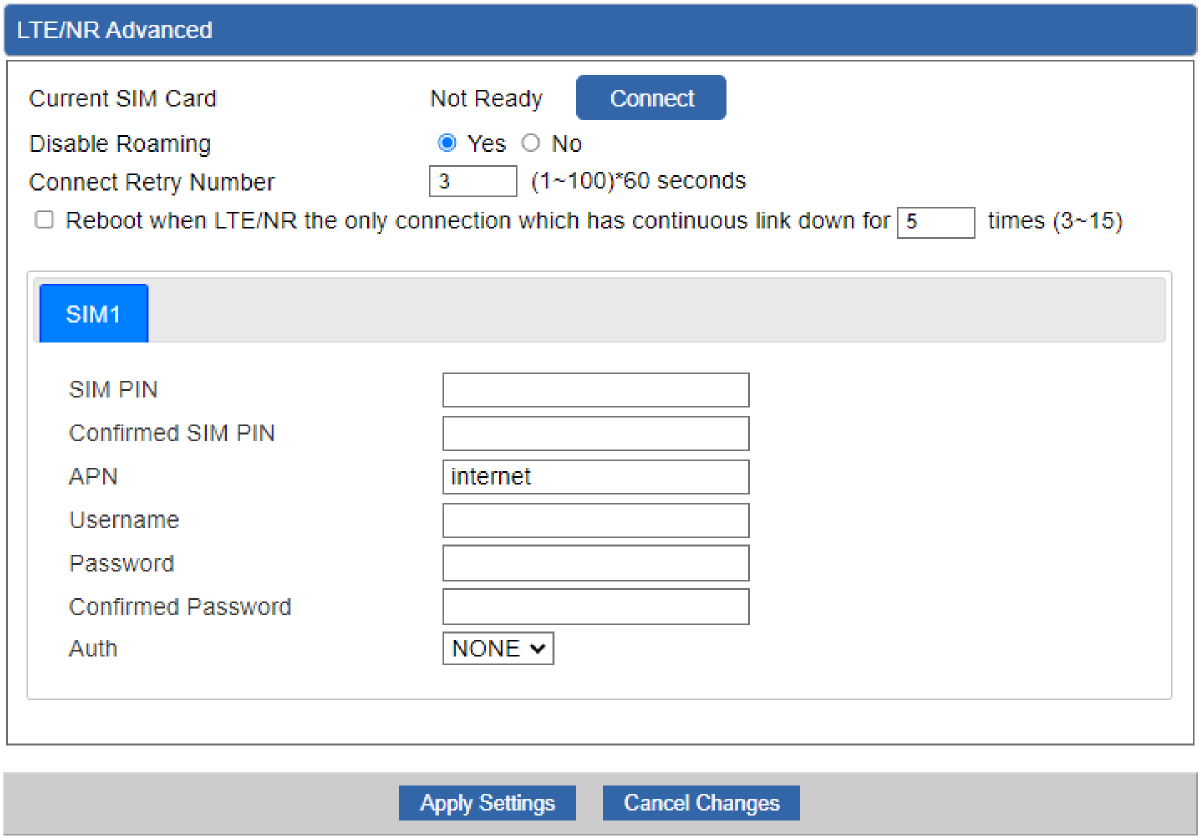
| | | |
|---|---|---|
| LTE/NR Config | Auto | |
| MTU | 1500 | min: 700; max: 1500 |

**Figure 4-6-2:** LTE/NR configuration

| Object | Description |
|---|---|
| **LTE/NR Config** | Indicates what kind of LTE will be used. Possible modes are:<br>■ **Auto**: Automatically connect the possible band.<br>■ **4G&5G Only**: Connect to 4G or 5G network only.<br>■ **5G Only**: Connect to 5G network only.<br>■ **4G Only**: Connect to 4G network only.<br>■ **3G Only**: Connect to 3G network only. |
| **MTU (Maximum transfer unit)** | Default is **1500**. |

### 4.6.2 LTE/NR Advanced

This page provides LTE/NR advanced configuration as shown in Figure 4-6-3.



LTE/NR Advanced

| | |
|---|---|
| Current SIM Card | Not Ready Connect |
| Disable Roaming | ● Yes ○ No |
| Connect Retry Number | 3 (1~100)*60 seconds |

□ Reboot when LTE/NR the only connection which has continuous link down for 5 times (3~15)

SIM1

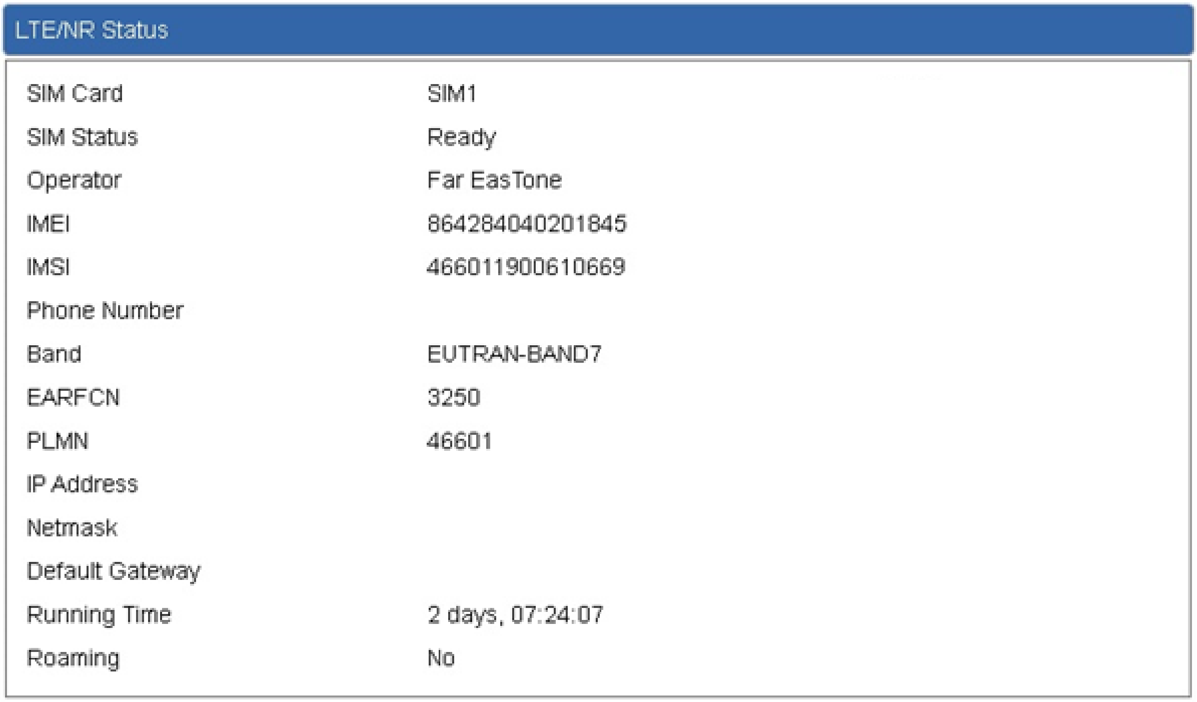
| | |
|---|---|
| SIM PIN | |
| Confirmed SIM PIN | |
| APN | internet |
| Username | |
| Password | |
| Confirmed Password | |
| Auth | NONE |

**Figure 4-6-3:** LTE/NR advanced

| Object | Description |
|---|---|
| **Current SIM Card** | Displays which SIM slot is using. |
| **Disable Roaming** | ■ **Disable:** SIM gets connection even it is in roaming state.<br>■ **Enable:** SIM would not get connection when in roaming state. |
| **SIM PIN** | ■ Configure PIN code to unlock SIM PIN. |
| **Confirmed SIM PIN** | ■ Confirm PIN code. |
| **APN** | ■ APN can be input by user or the system.. |
| **Username** | ■ The username can be input by user or the system. |
| **Password** | ■ The password can be input by user or the system. |
| **Confirm Password** | ■ Fill in your changed password. |
| **Auth** | Configure authentication<br>■ **None**<br>■ **PAP**<br>■ **CHAP** |

## 4.6.3 LTE/NR Status

This page displays LTE/NR status as shown in Figure 4-6-4.



LTE/NR Status

| | |
|---|---|
| SIM Card | SIM1 |
| SIM Status | Ready |
| Operator | Far EasTone |
| IMEI | 864284040201845 |
| IMSI | 466011900610669 |
| Phone Number | |
| Band | EUTRAN-BAND7 |
| EARFCN | 3250 |
| PLMN | 46601 |
| IP Address | |
| Netmask | |
| Default Gateway | |
| Running Time | 2 days, 07:24:07 |
| Roaming | No |

**Figure 4-6-4:** LTE/NR status

## 4.6.4 LTE/NR Statistics

This page displays LTE/NR status as shown in Figure 4-6-5.

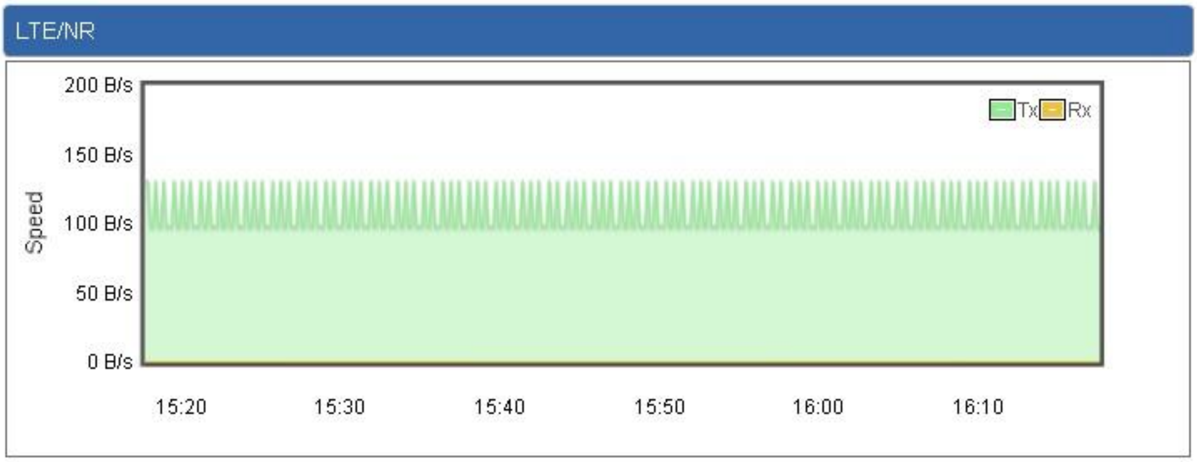
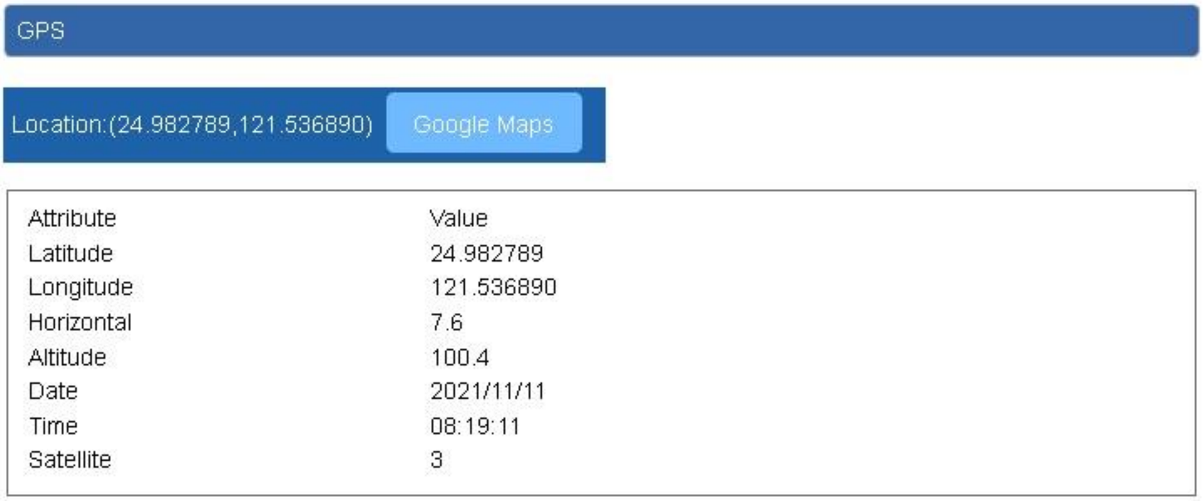


**Figure 4-6-5:** LTE/NR statistics

## 4.6.5 GPS

This page displays GPS status as shown in Figure 4-6-6.



GPS

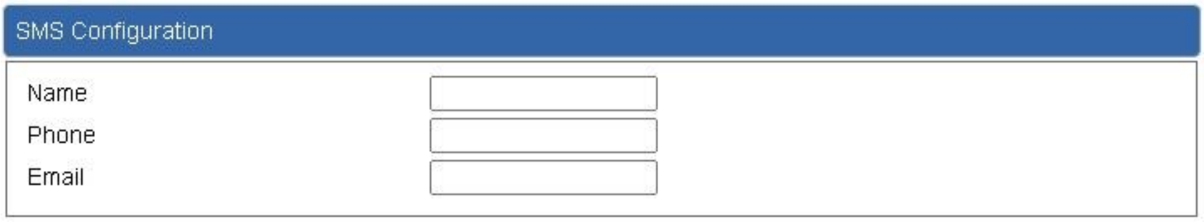
Location:(24.982789,121.536890)

| Attribute | Value |
|---|---|
| Latitude | 24.982789 |
| Longitude | 121.536890 |
| Horizontal | 7.6 |
| Altitude | 100.4 |
| Date | 2021/11/11 |
| Time | 08:19:11 |
| Satellite | 3 |

**Figure 4-6-6:** GPS

## 4.6.6 SMS

This page provides SMS configuration as shown in Figure 4-6-7.



SMS Configuration

| | |
|---|---|
| Name | |
| Phone | |
| Email | |

**Figure 4-6-7:** SMS

| Object | Description |
|---|---|
| **Name** | Configure user’s name |
| **Phone** | Configure user’s phone number |
| **Email** | Configure user’s email |

## 4.7 LoRa

The LoRa menu provides LoRa functions as shown in Figure 4-7-1. Please refer to the following sections for details.

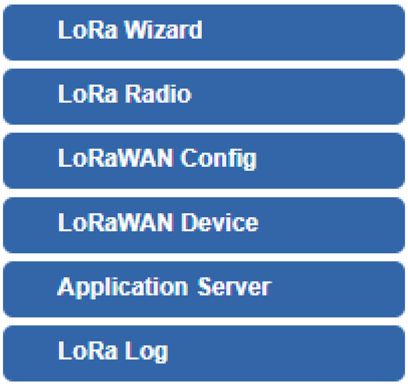


**Figure 4-7-1:** LoRa menu

| Object | Description |
|---|---|
| **LoRa Wizard** | Allows quick setup of LoRa Radio, LoRaWAN, and Application Server configurations. |
| **LoRa Radio** | Allows configuration of LoRa Radio settings. |
| **LoRaWAN Configuration** | Allows setup of data routing and network service configurations. |
| **LoRaWAN Device** | Allows configuring ABP decryption settings for LoRaWAN devices. |
| **Application Server** | Allows setting MQTT configuration. |
| **LoRa Log** | Displays LoRa log |

## 4.7.1 LoRa Wizard

The Wizard will guide the user to configuring the LoRa and LoRaWAN Configuration easily and quickly. There are different procedures in different operation modes. According to the operation mode you switch to, please follow the instructions below to configure the LoRa Configuration via **LoRa Wizard** as shown in Figure 4-7-2.

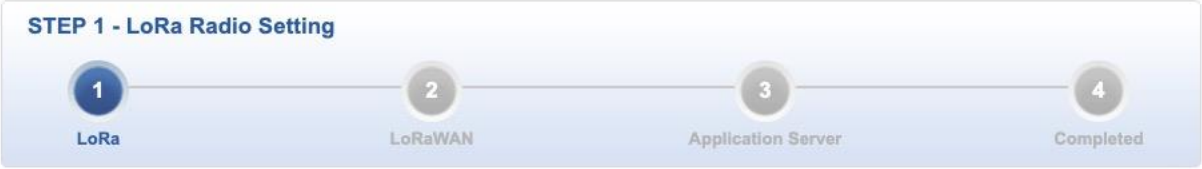
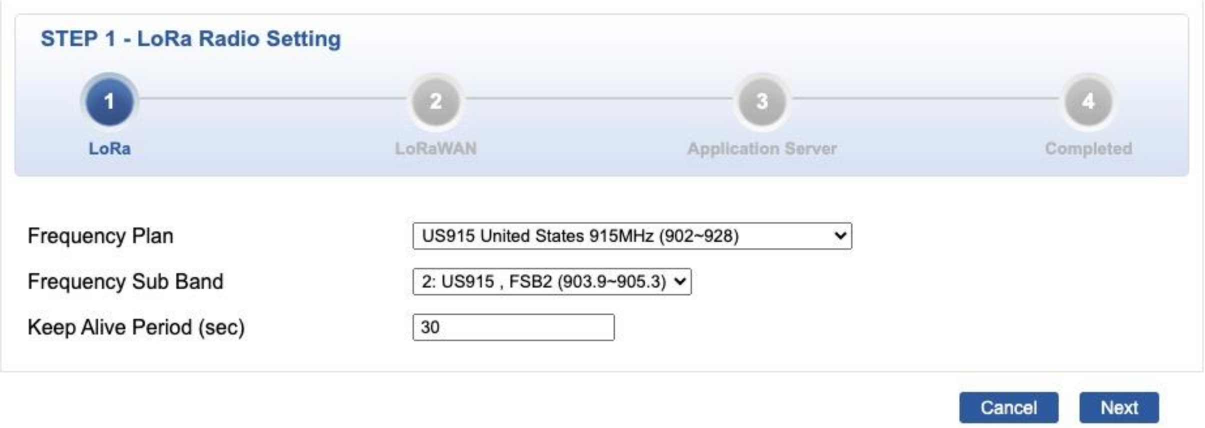


**Figure 4-7-2:** LoRa Wizard

### Step 1: LoRa Radio Setting

Set up the frequency plan to match the end node so as to receive the LoRaWAN packets from the LoRaWAN sensor, as shown in Figure 4-7-3.



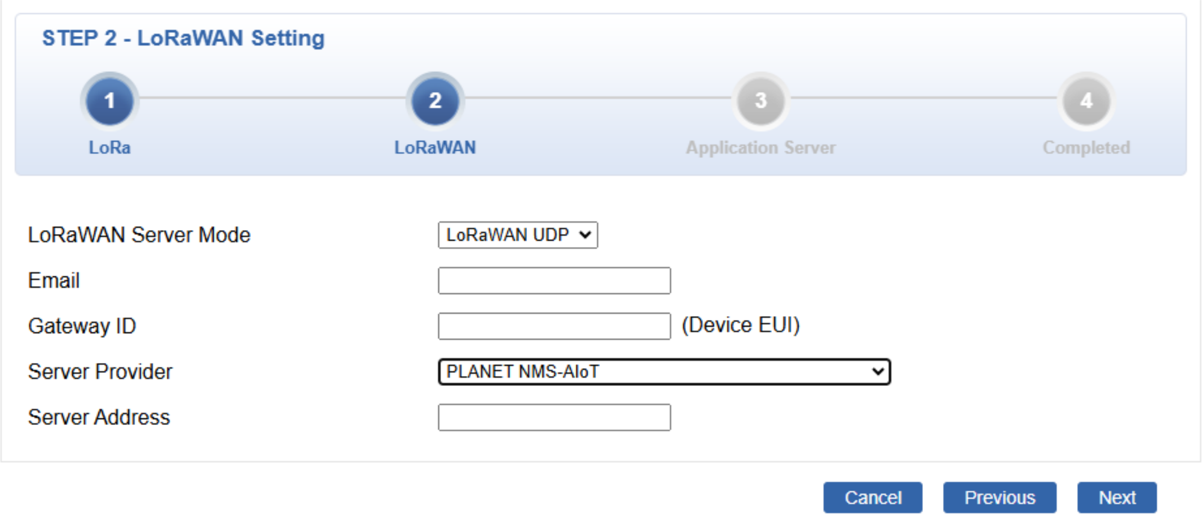
Frequency Plan: US915 United States 915MHz (902~928)
Frequency Sub Band: 2: US915 , FSB2 (903.9~905.3)
Keep Alive Period (sec): 30

**Figure 4-7-3:** LoRa Radio Setting

| Object | Description |
|---|---|
| **Frequency Plan** | Set the frequency plan to match the end node so as to receive the LoRaWAN packets from the LoRaWAN sensor.<br>EU: 863~870MHz (IN865/EU868/RU864)<br>US: 902~928MHz (US915/AU915/KR920/AS923) |
| **Keep Alive Period (sec)** | After the configured length of time, the Gateway will issue a Pull request to the specified IP address to confirm its connection is still active. |

## Step 2: LoRaWAN Setting

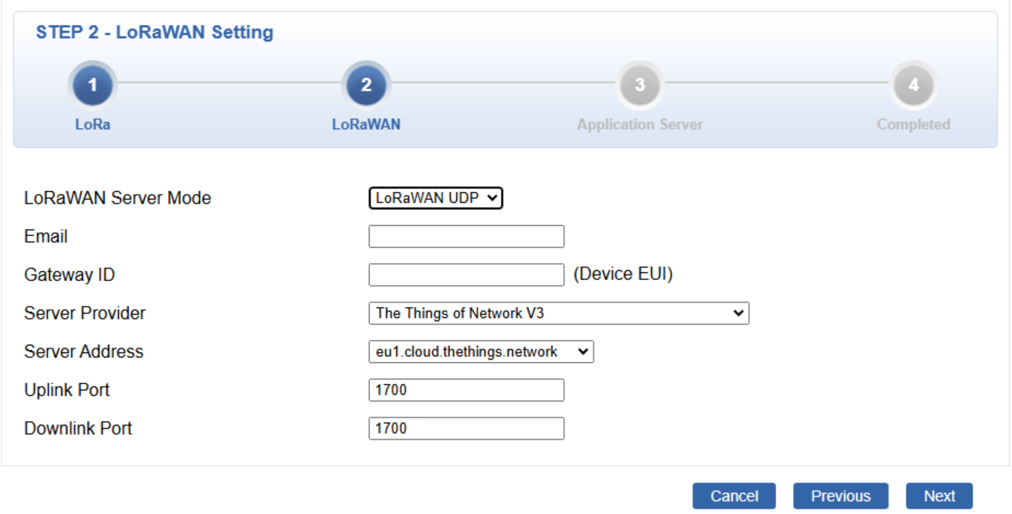
Set up the data routing and network service configurations, as shown in Figure 4-7-4.


STEP 2 - LoRaWAN Setting

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | PLANET NMS-AIoT |
| Server Address | |

**Figure 4-7-4:** LoRaWAN UDP setting – PLANET NMS-AIoT

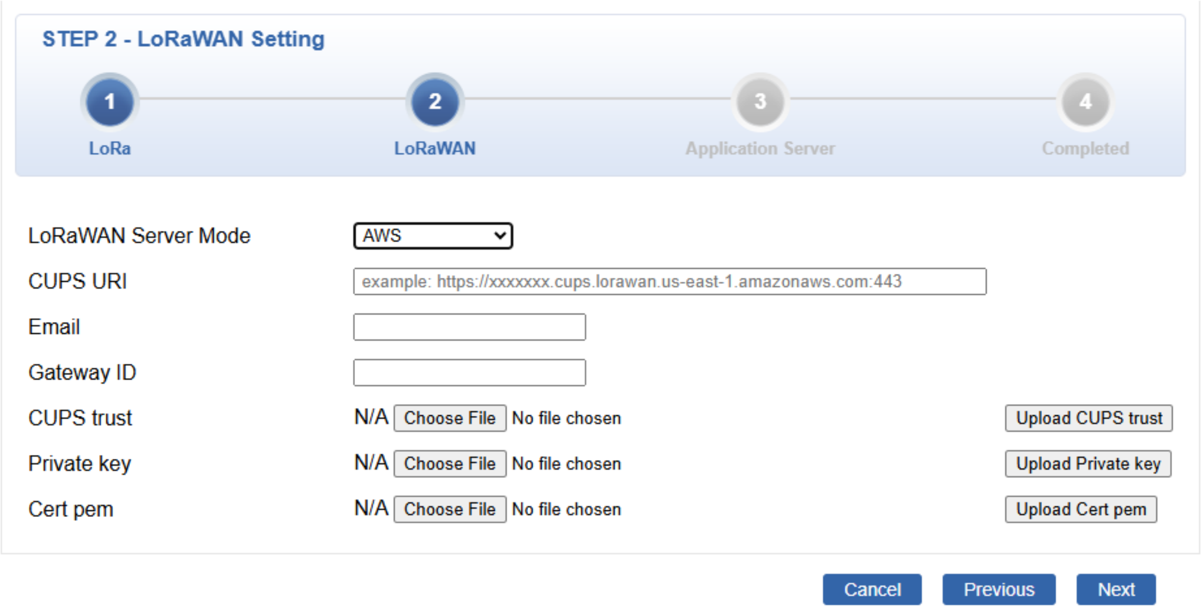
LoRaWAN Server Mode: **LoRaWAN UDP**


STEP 2 - LoRaWAN Setting

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | The Things of Network V3 |
| Server Address | eu1.cloud.thethings.network |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

**Figure 4-7-5:** LoRaWAN UDP setting – The Things of Network

LoRaWAN Server Mode: **AWS** (AWS IoT Core for LoRaWAN using CUPS)



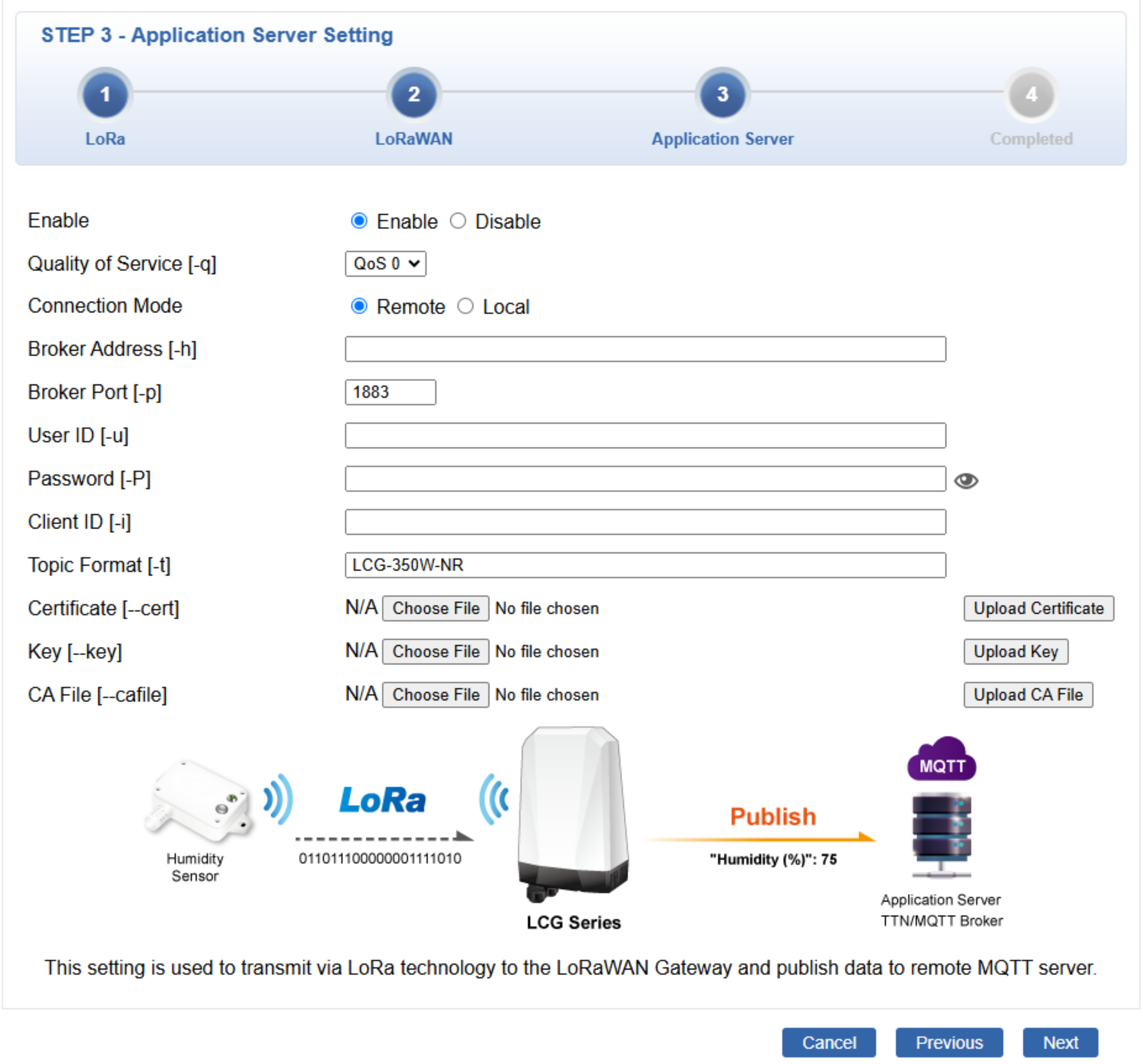
| | |
|---|---|
| LoRaWAN Server Mode | AWS |
| CUPS URI | example: https://xxxxxxx.cups.lorawan.us-east-1.amazonaws.com:443 |
| Email | |
| Gateway ID | |
| CUPS trust | N/A Choose File No file chosen Upload CUPS trust |
| Private key | N/A Choose File No file chosen Upload Private key |
| Cert pem | N/A Choose File No file chosen Upload Cert pem |

**Figure 4-7-6:** LoRaWAN setting - AWS

| Object | Description |
|---|---|
| **LoRaWAN Server Mode** | The service of LoRaWAN |
| **Email** | The registered email of LoRaWAN server |
| **Gateway ID** | The unique identity of the base station, which the server can distinguish different LoRaWAN base station |
| **Service Provider** | The service provider of LoRaWAN server |
| **Server Address** | The IP address of LoRaWAN server |
| **Server Uplink Port** | LoRaWAN data service center program uplink port. Value range is 0-65535 and the default value is 1700. |
| **Server Downlink Port** | LoRaWAN data service center program downlink port. Value range is 0-65535 and the default value is 1700 |

## Step 3: Application Server

This page provides Application Server (MQTT) Configuration as shown in Figure 4-7-7 and Figure 4-7-8.



STEP 3 - Application Server Setting

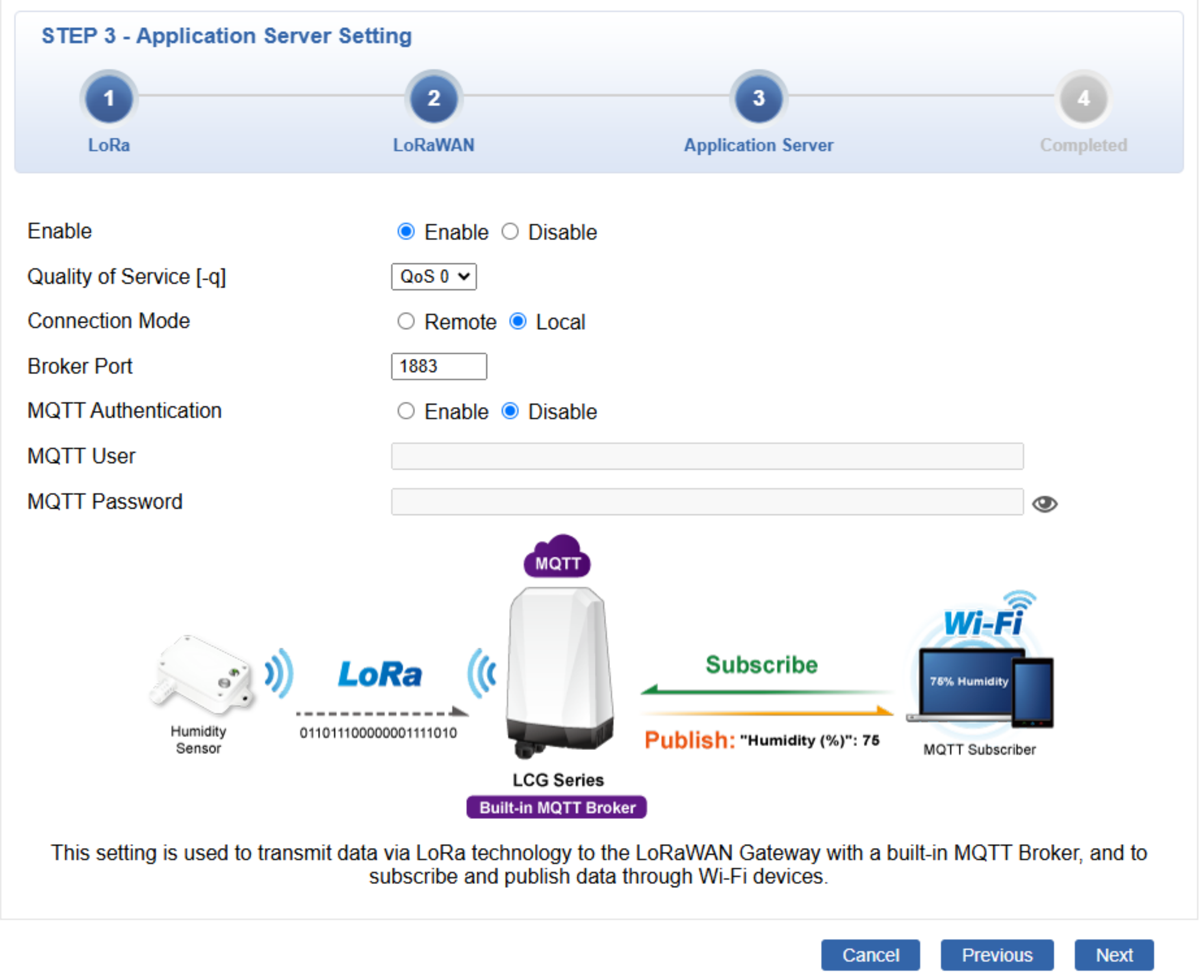
| | |
|---|---|
| Enable | ● Enable ○ Disable |
| Quality of Service [-q] | QoS 0 |
| Connection Mode | ● Remote ○ Local |
| Broker Address [-h] | |
| Broker Port [-p] | 1883 |
| User ID [-u] | |
| Password [-P] | |
| Client ID [-i] | |
| Topic Format [-t] | LCG-350W-NR |
| Certificate [--cert] | N/A Choose File No file chosen Upload Certificate |
| Key [--key] | N/A Choose File No file chosen Upload Key |
| CA File [--cafile] | N/A Choose File No file chosen Upload CA File |

This setting is used to transmit via LoRa technology to the LoRaWAN Gateway and publish data to remote MQTT server.

**Figure 4-7-7:** Application Server Configuration - MQTT Client

| Object | Description |
|---|---|
| **Enable** | Enable or disable MQTT service |
| **Quality of Service** | The level of quality of service |
| **Connection Mode** | The MQTT Broker server configuration |
| **Broker Address** | The IP address of MQTT broker server |
| **Broker Port** | The port of MQTT broker server |

| Object | Description |
|---|---|
| **User ID** | The user ID for MQTT broker |
| **Password** | The password for MQTT broker |
| **Client ID** | The client identifier for MQTT broker |
| **Certificate** | The certificates for MQTT SSL authentication |
| **Key** | The key for MQTT SSL authentication |
| **CA File** | The CA file for MQTT SSL authentication |



| | |
|---|---|
| Enable | ● Enable ○ Disable |
| Quality of Service [-q] | QoS 0 |
| Connection Mode | ○ Remote ● Local |
| Broker Port | 1883 |
| MQTT Authentication | ○ Enable ● Disable |
| MQTT User | |
| MQTT Password | |

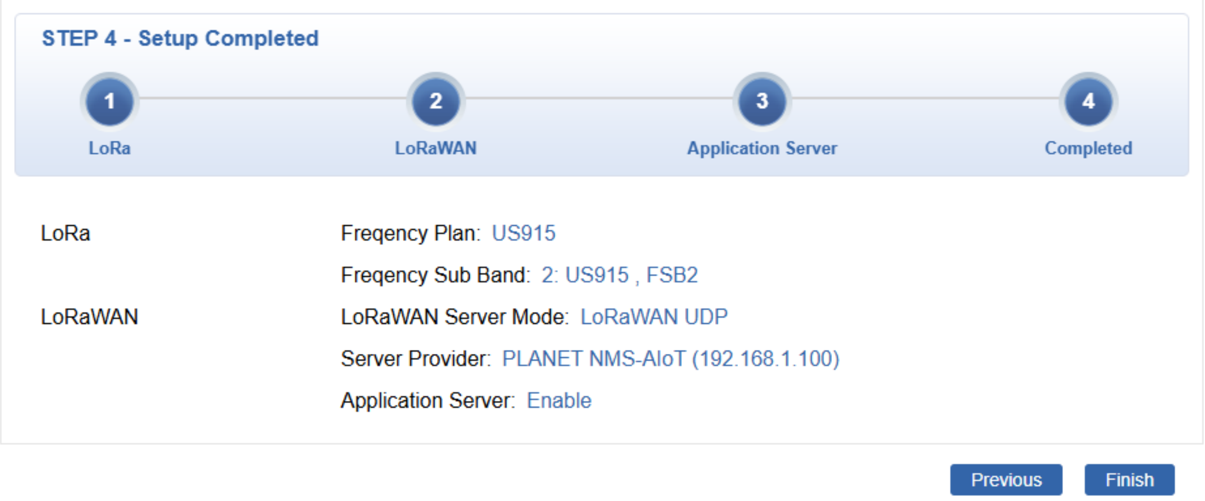
This setting is used to transmit data via LoRa technology to the LoRaWAN Gateway with a built-in MQTT Broker, and to subscribe and publish data through Wi-Fi devices.

**Figure 4-7-8:** Application Server Configuration – MQTT Broker

| Object | Description |
|---|---|
| **Enable** | Enable or disable MQTT service |
| **Quality of Service** | The level of quality of service |
| **Connection Mode** | The MQTT Broker server configuration |
| **Broker Port** | The port of MQTT broker server |
| **MQTT Authentication** | Enable or disable the local MQTT Broker Authentication |
| **MQTT User** | The user name for MQTT broker |
| **MQTT Password** | The password for MQTT broker |

## Step 4: Setup Completed

The page will show the summary of LoRa, LoRaWAN and Application server settings as shown in Figure 4-4-11.



LoRa Freqency Plan: US915

Freqency Sub Band: 2: US915 , FSB2

LoRaWAN LoRaWAN Server Mode: LoRaWAN UDP

Server Provider: PLANET NMS-AIoT (192.168.1.100)

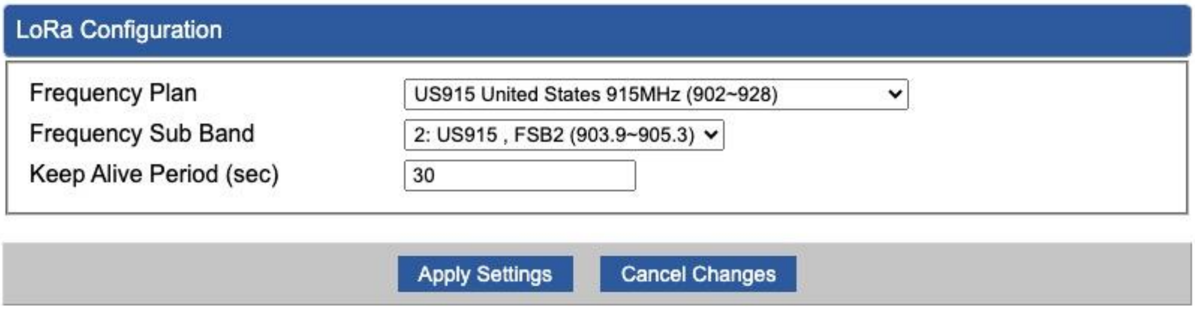
Application Server: Enable

**Figure 4-7-9:** Setup Completed

| Object | Description |
|---|---|
| **Finish** | Press this button to save and apply changes. |
| **Previous** | Press this button for the previous step. |

## 4.7.2 LoRa Radio

This page provides LoRa Radio configuration as shown in Figure 4-7-10.



LoRa Configuration

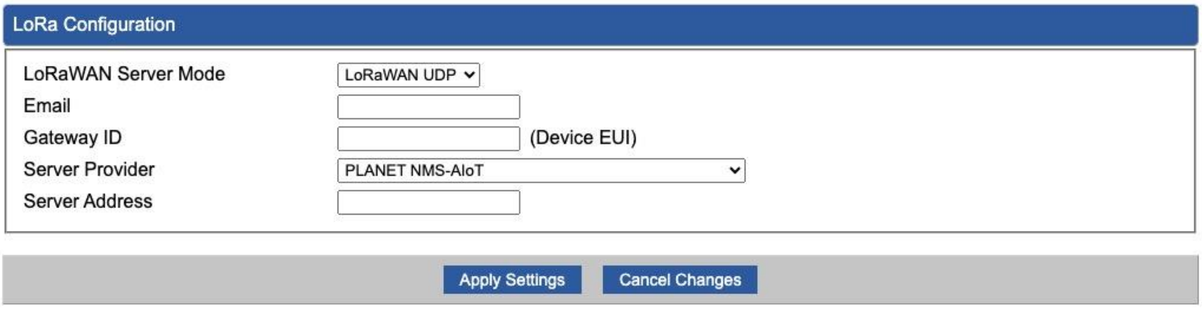
| | |
|---|---|
| Frequency Plan | US915 United States 915MHz (902~928) |
| Frequency Sub Band | 2: US915 , FSB2 (903.9~905.3) |
| Keep Alive Period (sec) | 30 |

**Figure 4-7-10:** LoRa Radio configuration

| Object | Description |
|---|---|
| **Keep Alive Period (sec)** | After the configured length of time, the Gateway will issue a Pull request to the specified IP address to confirm its connection is still active. |
| **Frequency Plan** | Set the frequency plan to match the end node so as to receive the LoRaWAN packets from the LoRaWAN sensor.<br>EU: 863~870MHz (IN865/EU868/RU864)<br>US: 902~928MHz (US915/AU915/KR920/AS923) |

### 4.7.3 LoRaWAN Configuration

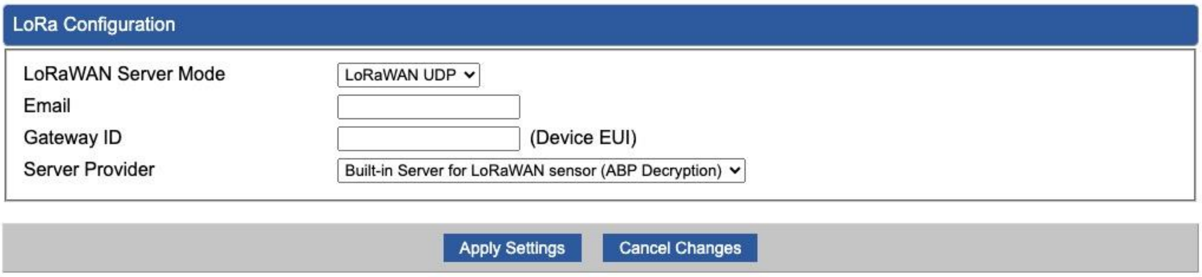
This page provides LoRaWAN configuration as shown in Figure 4-7-11.



LoRa Configuration

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | PLANET NMS-AIoT |
| Server Address | |

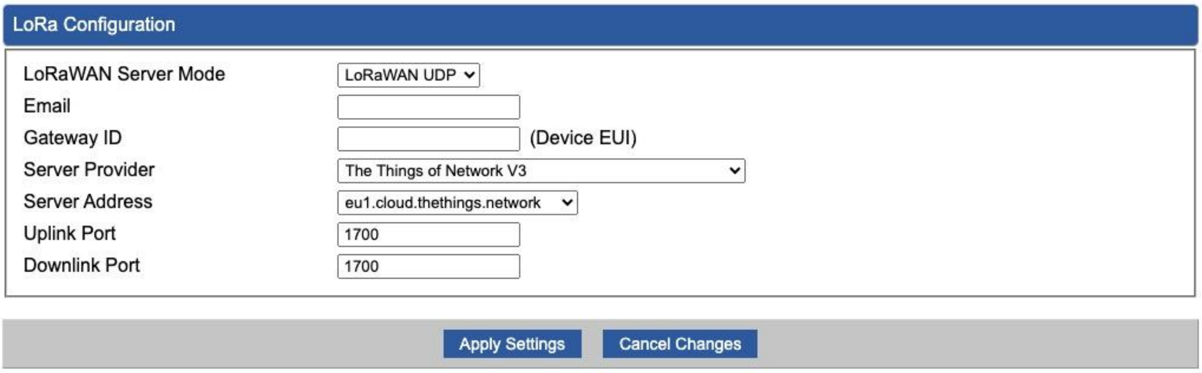
**Figure 4-7-11:** LoRaWAN UDP setting – PLANET NMS-AIoT



LoRa Configuration

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | Built-in Server for LoRaWAN sensor (ABP Decryption) |

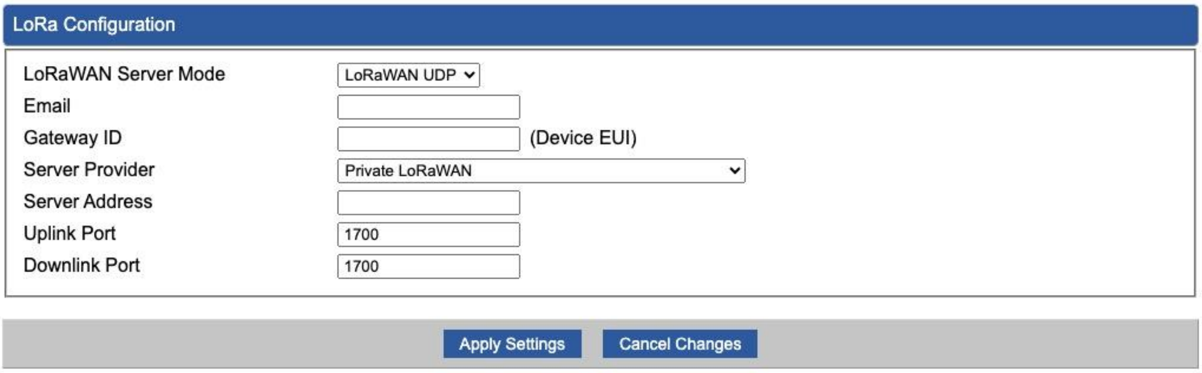
**Figure 4-7-12:** LoRaWAN UDP setting – Built-in Server for LoRaWAN Sensor



LoRa Configuration

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | The Things of Network V3 |
| Server Address | eu1.cloud.thethings.network |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

**Figure 4-7-13:** LoRaWAN UDP setting – The Thing of Network



LoRa Configuration

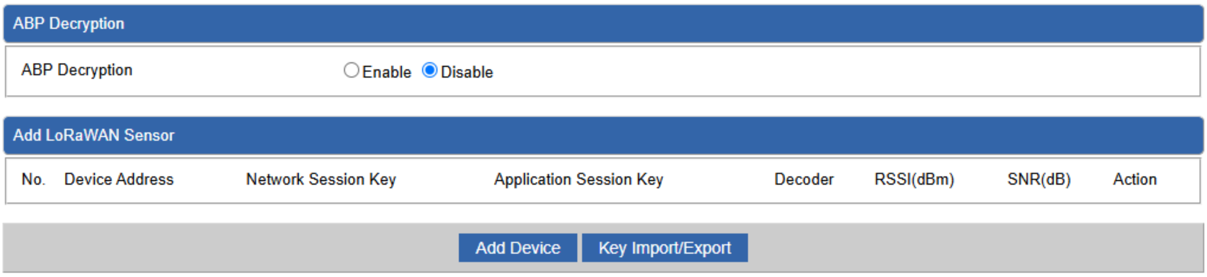
| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | (Device EUI) |
| Server Provider | Private LoRaWAN |
| Server Address | |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

**Figure 4-7-14:** LoRaWAN UDP setting – Private LoRaWAN

| Object | Description |
|---|---|
| **LoRaWAN Server Mode** | The service of LoRaWAN |
| **Email** | The registered email of LoRaWAN server |
| **Gateway ID** | The unique identity of the base station, allowing the server to distinguish between LoRaWAN base stations |
| **Service Provider** | The service provider of LoRaWAN server<br>1. PLANET NMS-AIoT<br>2. Built-in Server for LoRaWAN Sensor<br>3. The Thing of Network<br>4. Private LoRaWAN |
| **Server Address** | The IP address of LoRaWAN server |
| **Server Uplink Port** | LoRaWAN data service center program uplink port. Value range is 0-65535 and the default value is 1700. |
| **Server Downlink Port** | LoRaWAN data service center program downlink port. Value range is 0-65535 and the default value is 1700 |

### 4.7.4 LoRaWAN Device

This page provides ABP Decryption configuration as shown in Figure 4-7-15.



ABP Decryption

ABP Decryption ○ Enable ● Disable

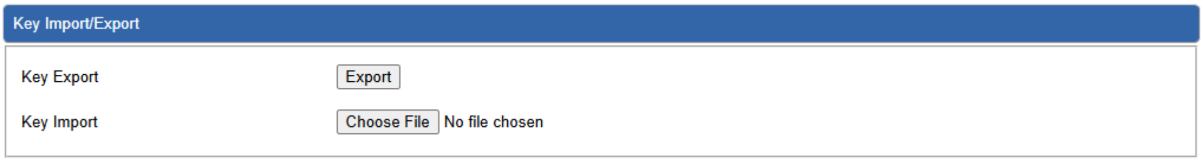
Add LoRaWAN Sensor

| No. | Device Address | Network Session Key | Application Session Key | Decoder | RSSI(dBm) | SNR(dB) | Action |
|---|---|---|---|---|---|---|---|

**Figure 4-7-15:** ABP Decryption

| Object | Description |
|---|---|
| **No.** | The number of ABP Decryption devices |
| **Dev ADDR** | The Dev ADDR of devices |
| **APP Session Key** | The APP session key of devices |
| **Network Session Key** | The network session Key of devices |
| **Decoder** | The decoder way |
| **Action** | The action status of sensor or node |

The feature of Key Import and Export as shown in Figure 4-7-16.



Key Import/Export

Key Export Export

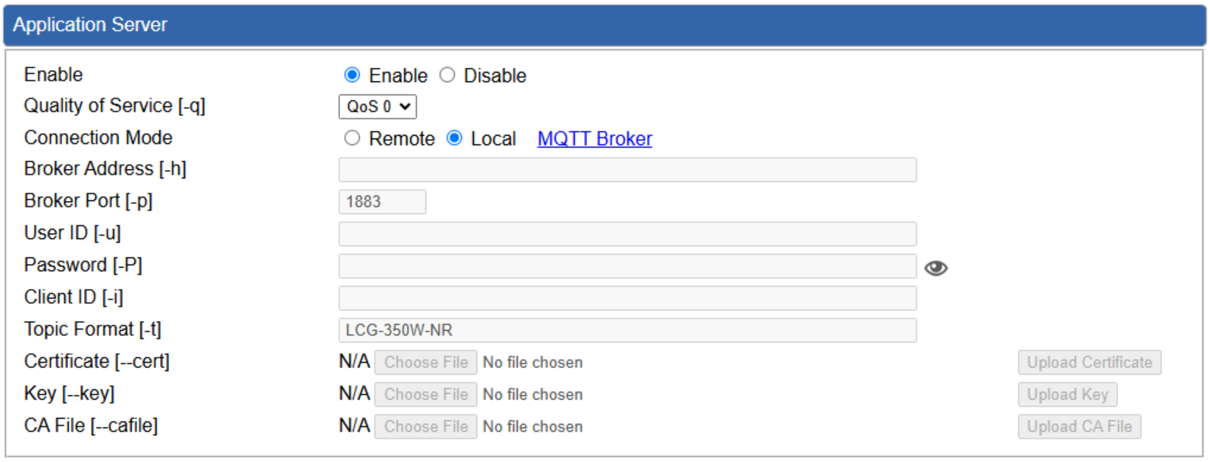
Key Import Choose File No file chosen

**Figure 4-7-16:** Key Import/Export Page

| Object | Description |
|---|---|
| **Key Export** | Press the Export button to save setting file to PC. |
| **Key Import** | Press the Choose File button to select the setting file, and then press the Import button to upload setting file from PC. |

## 4.7.5 Application Server

This page provides MQTT server Configuration as shown in Figure 4-7-17.



Application Server

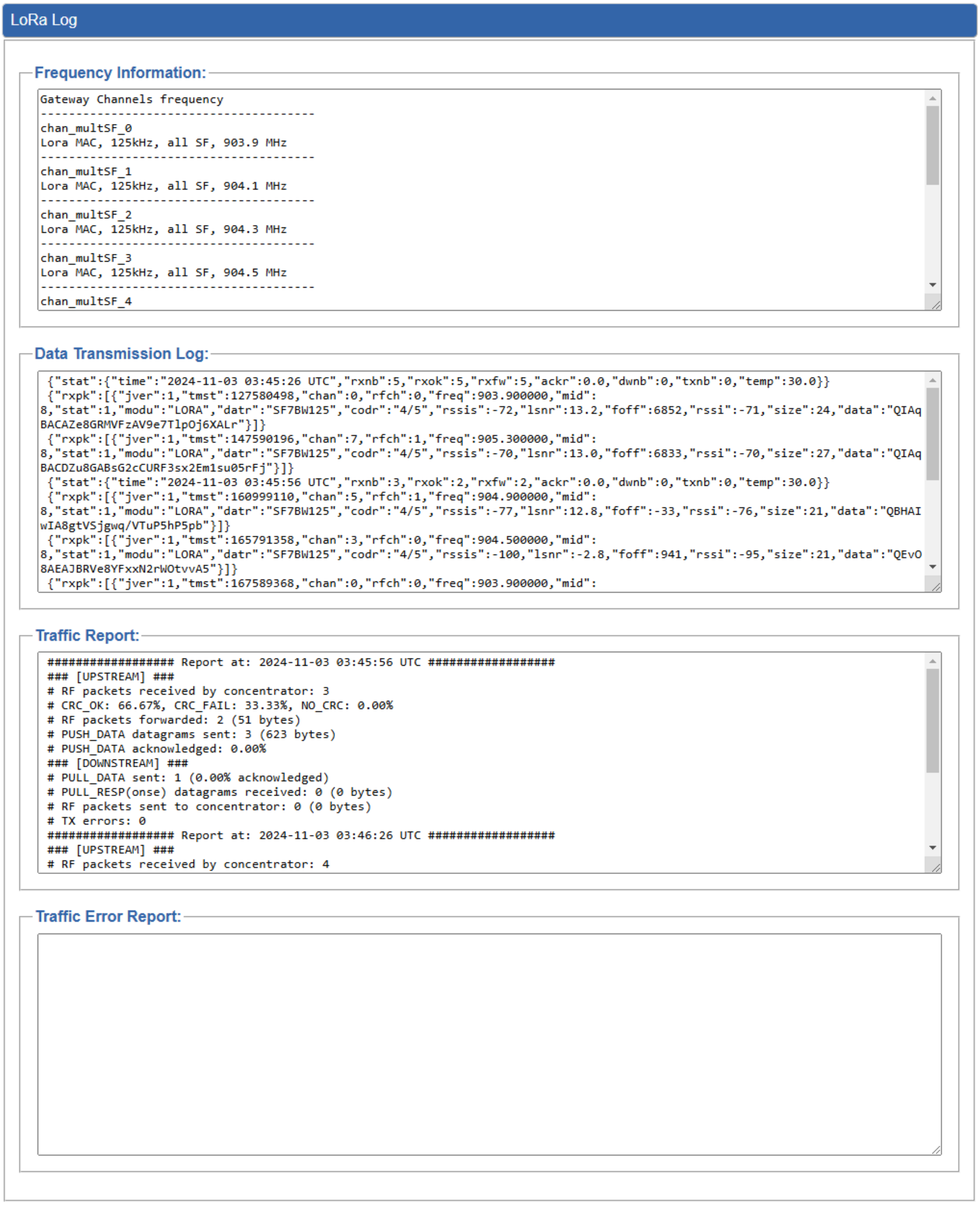
| | |
|---|---|
| Enable | ● Enable ○ Disable |
| Quality of Service [-q] | QoS 0 |
| Connection Mode | ○ Remote ● Local MQTT Broker |
| Broker Address [-h] | |
| Broker Port [-p] | 1883 |
| User ID [-u] | |
| Password [-P] | |
| Client ID [-i] | |
| Topic Format [-t] | LCG-350W-NR |
| Certificate [--cert] | N/A Choose File No file chosen Upload Certificate |
| Key [--key] | N/A Choose File No file chosen Upload Key |
| CA File [--cafile] | N/A Choose File No file chosen Upload CA File |

**Figure 4-7-17:** Application Server Configuration

| Object | Description |
|---|---|
| **Enable** | Enable or disable MQTT service |
| **Quality of Service** | The level of quality of service |
| **Connection Mode** | The MQTT Broker server configuration |
| **MQTT Broker** | The local MQTT Broker server configuration |
| **Broker Address** | The IP address of MQTT broker server |
| **Broker Port** | The port of MQTT broker server |
| **User ID** | The user ID for MQTT broker |
| **Password** | The password for MQTT broker |
| **Client ID** | The client identifier for MQTT broker |
| **Certificate** | The certificates for MQTT SSL authentication |
| **Key** | The key for MQTT SSL authentication |
| **CA File** | The CA file for MQTT SSL authentication |

## 4.7.6 LoRa Log

This page shows the frequency for LoRa radio and traffic as shown in Figure 4-7-18.



LoRa Log

Frequency Information:

```
Gateway Channels frequency
---------------------------------------
chan_multSF_0
Lora MAC, 125kHz, all SF, 903.9 MHz
---------------------------------------
chan_multSF_1
Lora MAC, 125kHz, all SF, 904.1 MHz
---------------------------------------
chan_multSF_2
Lora MAC, 125kHz, all SF, 904.3 MHz
---------------------------------------
chan_multSF_3
Lora MAC, 125kHz, all SF, 904.5 MHz
---------------------------------------
chan_multSF_4
```

Data Transmission Log:

```
 {"stat":{"time":"2024-11-03 03:45:26 UTC","rxnb":5,"rxok":5,"rxfw":5,"ackr":0.0,"dwnb":0,"txnb":0,"temp":30.0}}
 {"rxpk":[{"jver":1,"tmst":127580498,"chan":0,"rfch":0,"freq":903.900000,"mid":
8,"stat":1,"modu":"LORA","datr":"SF7BW125","codr":"4/5","rssis":-72,"lsnr":13.2,"foff":6852,"rssi":-71,"size":24,"data":"QIAq
BACAZe8GRMVFzAV9e7Tlp0j6XALr"}]}
 {"rxpk":[{"jver":1,"tmst":147590196,"chan":7,"rfch":1,"freq":905.300000,"mid":
8,"stat":1,"modu":"LORA","datr":"SF7BW125","codr":"4/5","rssis":-70,"lsnr":13.0,"foff":6833,"rssi":-70,"size":27,"data":"QIAq
BACDZu8GABsG2cCURF3sx2Em1su05rFj"}]}
 {"stat":{"time":"2024-11-03 03:45:56 UTC","rxnb":3,"rxok":2,"rxfw":2,"ackr":0.0,"dwnb":0,"txnb":0,"temp":30.0}}
 {"rxpk":[{"jver":1,"tmst":160999110,"chan":5,"rfch":1,"freq":904.900000,"mid":
8,"stat":1,"modu":"LORA","datr":"SF7BW125","codr":"4/5","rssis":-77,"lsnr":12.8,"foff":-33,"rssi":-76,"size":21,"data":"QBHAI
wIA8gtVSjgwq/VTuP5hP5pb"}]}
 {"rxpk":[{"jver":1,"tmst":165791358,"chan":3,"rfch":0,"freq":904.500000,"mid":
8,"stat":1,"modu":"LORA","datr":"SF7BW125","codr":"4/5","rssis":-100,"lsnr":-2.8,"foff":941,"rssi":-95,"size":21,"data":"QEvO
8AEAJBRVe8YFxxN2rWOtvvA5"}]}
 {"rxpk":[{"jver":1,"tmst":167589368,"chan":0,"rfch":0,"freq":903.900000,"mid":
```

Traffic Report:

```
 ################## Report at: 2024-11-03 03:45:56 UTC ##################
 ### [UPSTREAM] ###
 # RF packets received by concentrator: 3
 # CRC_OK: 66.67%, CRC_FAIL: 33.33%, NO_CRC: 0.00%
 # RF packets forwarded: 2 (51 bytes)
 # PUSH_DATA datagrams sent: 3 (623 bytes)
 # PUSH_DATA acknowledged: 0.00%
 ### [DOWNSTREAM] ###
 # PULL_DATA sent: 1 (0.00% acknowledged)
 # PULL_RESP(onse) datagrams received: 0 (0 bytes)
 # RF packets sent to concentrator: 0 (0 bytes)
 # TX errors: 0
 ################## Report at: 2024-11-03 03:46:26 UTC ##################
 ### [UPSTREAM] ###
 # RF packets received by concentrator: 4
```

Traffic Error Report:

**Figure 4-7-18:** LoRa Radio and Traffic

## 4.8 Security

The security menu provides Firewall, Access Filtering and other functions as shown in Figure 4-8-1. Please refer to the following sections for the details.

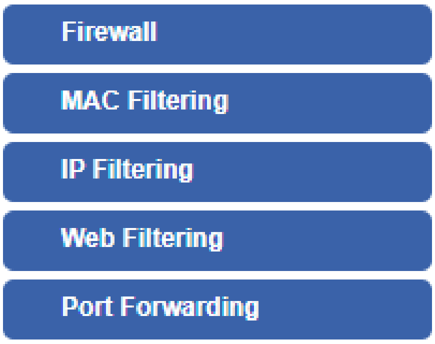
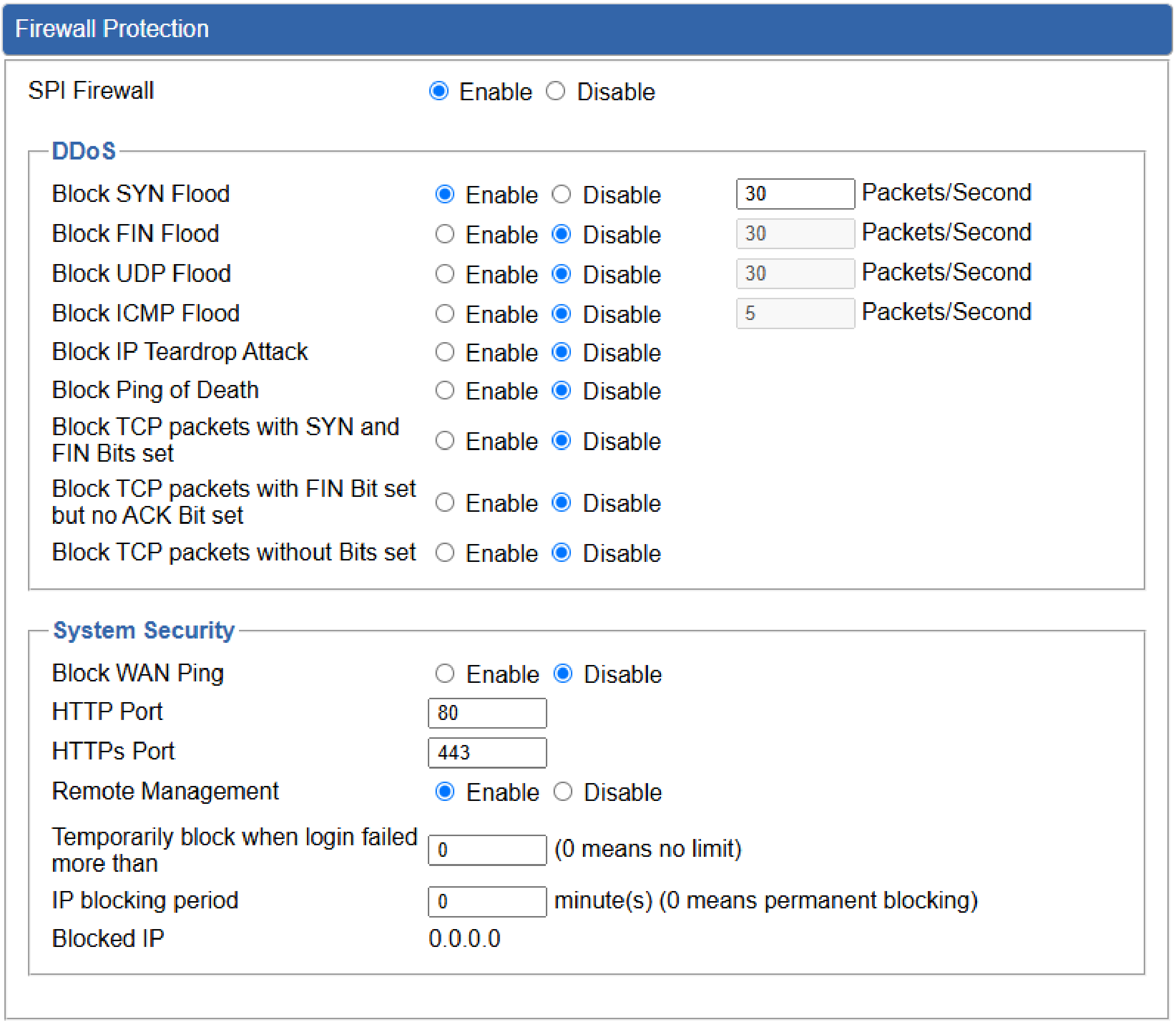


**Figure 4-8-1:** Security menu

| Object | Description |
|---|---|
| **Firewall** | Allows setting DoS (Denial of Service) protection as enable. |
| **MAC Filtering** | Allows setting MAC Filtering. |
| **IP Filtering** | Allows setting IP Filtering. |
| **Web Filtering** | Allows setting Web Filtering. |
| **Port Range Forwarding** | Allows setting Port Forwarding. |

## 4.8.1 Firewall

The LoRaWAN Gateway can prevent specific DoS attacks as shown in Figure 4-8-2.



Firewall Protection

| | | |
|---|---|---|
| SPI Firewall | ● Enable ○ Disable | |

**DDoS**

| | | |
|---|---|---|
| Block SYN Flood | ● Enable ○ Disable | 30 Packets/Second |
| Block FIN Flood | ○ Enable ● Disable | 30 Packets/Second |
| Block UDP Flood | ○ Enable ● Disable | 30 Packets/Second |
| Block ICMP Flood | ○ Enable ● Disable | 5 Packets/Second |
| Block IP Teardrop Attack | ○ Enable ● Disable | |
| Block Ping of Death | ○ Enable ● Disable | |
| Block TCP packets with SYN and FIN Bits set | ○ Enable ● Disable | |
| Block TCP packets with FIN Bit set but no ACK Bit set | ○ Enable ● Disable | |
| Block TCP packets without Bits set | ○ Enable ● Disable | |

**System Security**

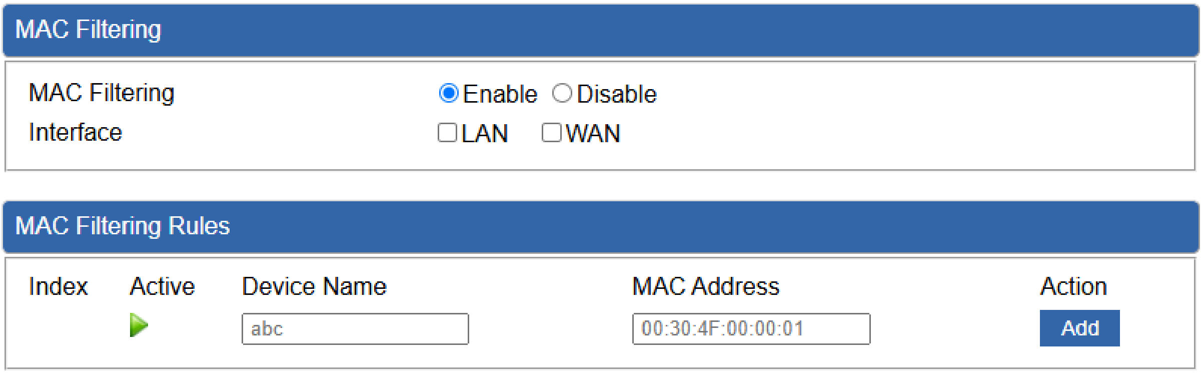
| | |
|---|---|
| Block WAN Ping | ○ Enable ● Disable |
| HTTP Port | 80 |
| HTTPs Port | 443 |
| Remote Management | ● Enable ○ Disable |
| Temporarily block when login failed more than | 0 (0 means no limit) |
| IP blocking period | 0 minute(s) (0 means permanent blocking) |
| Blocked IP | 0.0.0.0 |

**Figure 4-7-2:** Firewall

| Object | Description |
|---|---|
| **SPI Firewall** | The SPI Firewall prevents attack and improper access to network resources.<br>The default configuration is enabled. |
| **Block SYN Flood** | SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on.<br>The default configuration is enabled. |
| **Block FIN Flood** | If the function is enabled, when the number of the current FIN packets is beyond the set value, the LoRaWAN Gateway will start the blocking function immediately.<br>The default configuration is disabled. |
| **Block UDP Flood** | If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the LoRaWAN Gateway will start the blocking function immediately.<br>The default configuration is disabled. |
| **Block ICMP Flood** | ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.<br>The default configuration is disabled. |
| **IP TearDrop** | If the function is enabled, the LoRaWAN Gateway will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes. |
| **Ping Of Death** | If the function is enabled, the LoRaWAN Gateway will block Ping of Death attack that aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size causing the target machine to freeze or crash. |
| **Block WAN Ping** | Enable the function to allow the Ping access from the Internet network.<br>The default configuration is disabled. |
| **Remote Management** | Enable the function to allow the web server access of the LoRaWAN Gateway from the Internet network.<br>The default configuration is disabled. |

## 4.8.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the LoRaWAN Gateway Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-8-3.



MAC Filtering

MAC Filtering ● Enable ○ Disable
Interface □ LAN □ WAN

MAC Filtering Rules

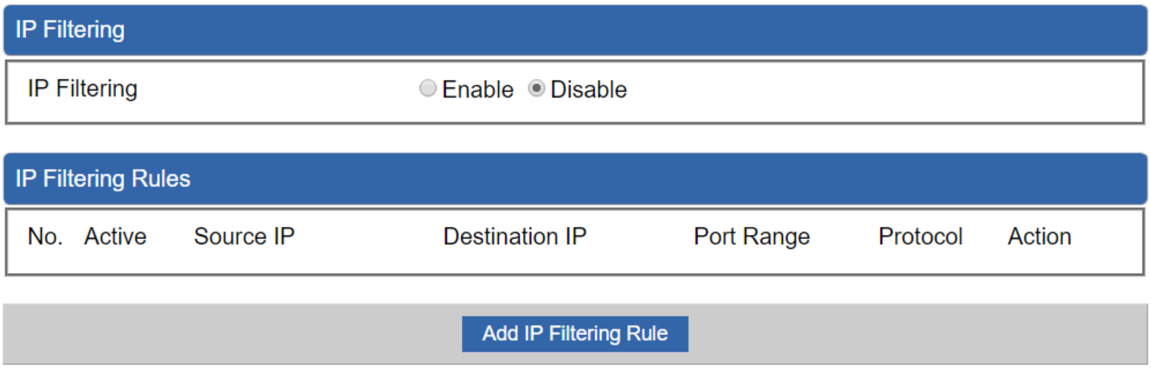
| Index | Active | Device Name | MAC Address | Action |
|---|---|---|---|---|
| | ▶ | abc | 00:30:4F:00:00:01 | Add |

**Figure 4-8-3:** MAC Filtering

| Object | Description |
|---|---|
| **Enable MAC Filtering** | Set the function as enable or disable.<br>When the function is enabled, the LoRaWAN Gateway will block traffic of the MAC address on the list. |
| **Interface** | Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa. |
| **MAC Address** | Input a MAC address you want to control, such as A8:F7:E0:00:06:62. |
| **Add** | When you input a MAC address, please click the "Add" button to add it into the list. |
| **Remove** | If you want to remove a MAC address from the list, please click on the MAC address, and then click the "Remove" button to remove it. |
| **Remove All** | If you want to remove all MAC addresses from the list, please click the "Remove All" button to remove all. |

## 4.8.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in Figure 4-8-4. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.



IP Filtering

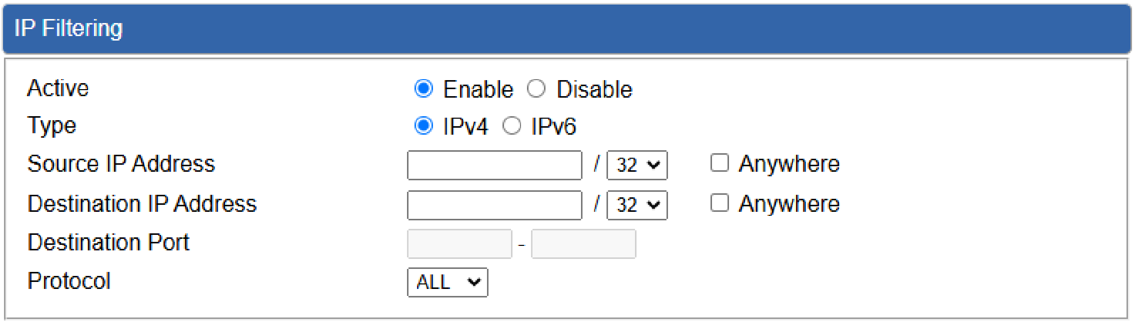
IP Filtering ○ Enable ● Disable

IP Filtering Rules

| No. | Active | Source IP | Destination IP | Port Range | Protocol | Action |
|---|---|---|---|---|---|---|

**Figure 4-8-4:** IP Filtering

| Object | Description |
|---|---|
| **IP Filtering** | Set the function as enable or disable. |
| **Add IP Filtering Rule** | Go to the Add Filtering Rule page to add a new rule. |



IP Filtering

Active ● Enable ○ Disable
Type ● IPv4 ○ IPv6
Source IP Address / 32 □ Anywhere
Destination IP Address / 32 □ Anywhere
Destination Port -
Protocol ALL

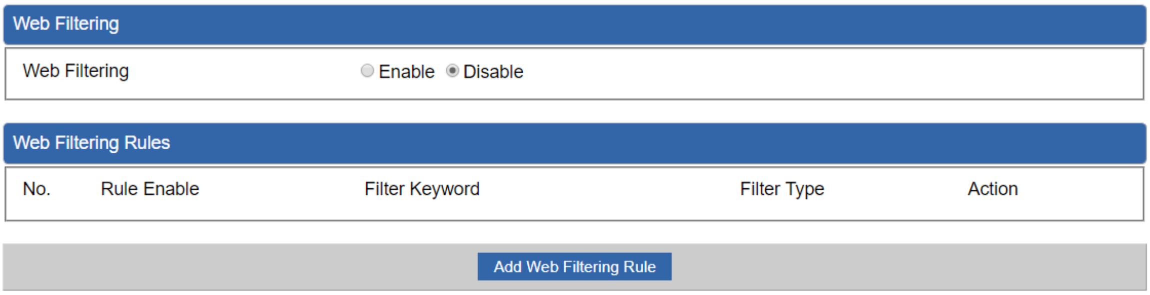
**Figure 4-7-5:** IP Filter Rule Setting

| Object | Description |
|---|---|
| **Enable** | Set the rule as enable or disable. |
| **Source IP Address** | Input the IP address of LAN user (such as PC or laptop) which you want to control. |
| **Anywhere (of source IP Address)** | Check the box if you want to control all LAN users. |
| **Destination IP Address** | Input the IP address of web site which you want to block. |
| **Anywhere (of destination IP Address)** | Check the box if you want to control all web sites, meaning the LAN user can't visit any web site. |

| Object | Description |
|---|---|
| **Destination Port** | Input the port of destination IP Address which you want to block.<br>Leave it as blank if you want to block all ports of the web site. |
| **Protocol** | Select the protocol type (TCP, UDP or all).<br>If you are unsure, please leave it to the default all protocol. |

## 4.8.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-8-6. Block those URLs which contain keywords listed below.


Web Filtering

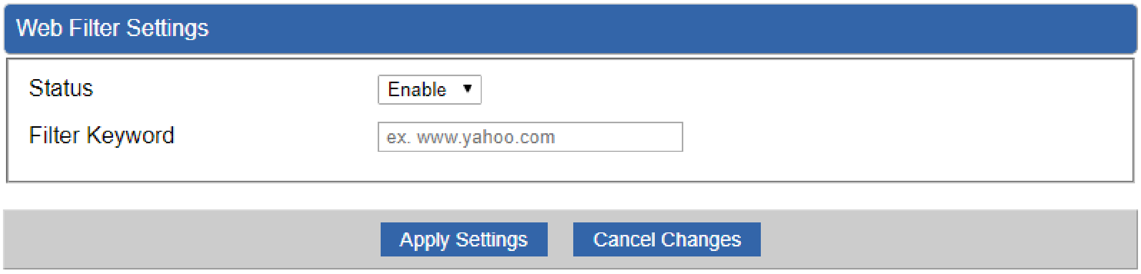
Web Filtering ○ Enable ● Disable

Web Filtering Rules

| No. | Rule Enable | Filter Keyword | Filter Type | Action |
|---|---|---|---|---|

**Figure 4-8-6:** Web Filtering

| Object | Description |
|---|---|
| **Web Filtering** | Set the function as enable or disable. |
| **Add Web Filtering Rule** | Go to the Add Web Filtering Rule page to add a new rule. |


Web Filter Settings

Status: Enable ▼

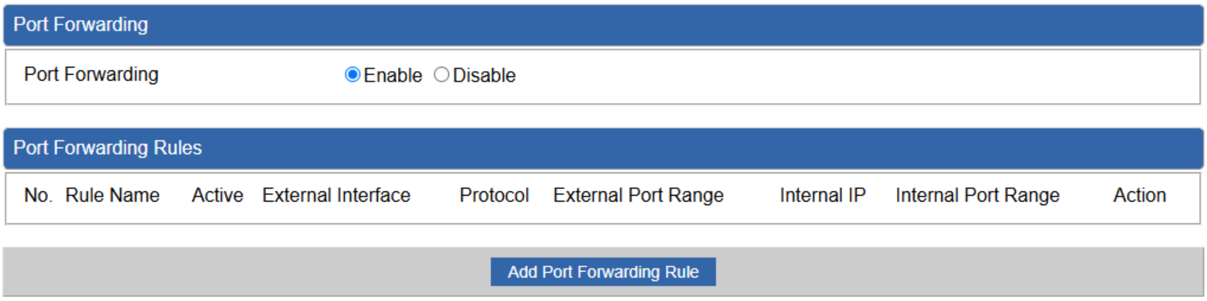
Filter Keyword: ex. www.yahoo.com

**Figure 4-8-7** Web Filtering Rule Setting

| Object | Description |
|---|---|
| **Status** | Set the rule as enable or disable. |
| **Filter Keyword** | Input the URL address that you want to filter, such as<br>www.yahoo.com. |

### 4.8.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in Figure 4-8-8. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your LoRaWAN Gateway's NAT firewall.



Port Forwarding

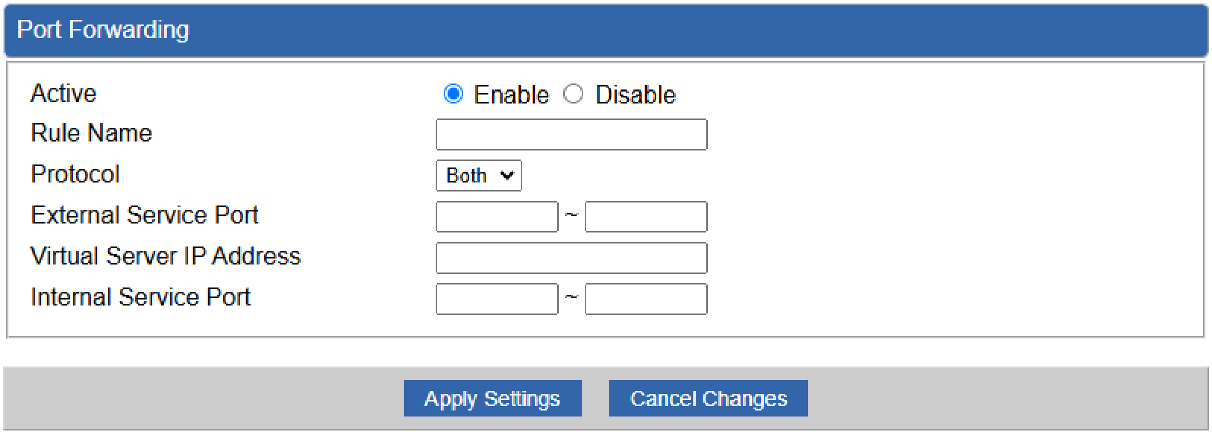
Port Forwarding ● Enable ○ Disable

Port Forwarding Rules

| No. | Rule Name | Active | External Interface | Protocol | External Port Range | Internal IP | Internal Port Range | Action |
|---|---|---|---|---|---|---|---|---|

**Figure 4-8-8:** Port Forwarding

| Object | Description |
|---|---|
| **Port Forwarding** | Set the function as enable or disable. |
| **Add Port Forwarding Rule** | Go to the Add Port Forwarding Rule page to add a new rule. |



Port Forwarding

Active ● Enable ○ Disable

Rule Name

Protocol Both

External Service Port ~

Virtual Server IP Address

Internal Service Port ~

**Figure 4-8-9:** Port Forwarding Rule Setting

| Object | Description |
|---|---|
| **Rule Name** | Enter any words for recognition. |
| **Protocol** | Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols. |
| **External Service Port** | Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields. |
| **Virtual Server IP Address** | Enter the local IP address. |
| **Internal Service Port** | Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields. |

## 4.9 VPN

To obtain a private and secure network link, the LoRaWAN Gateway is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secure options for enterprises to adopt in comparison to other methods.

The VPN menu provides the following features as shown in Figure 4-9-1

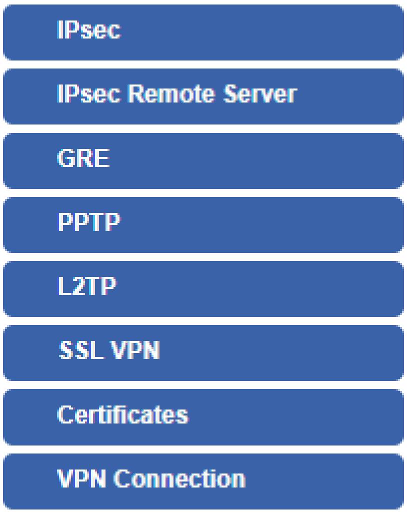


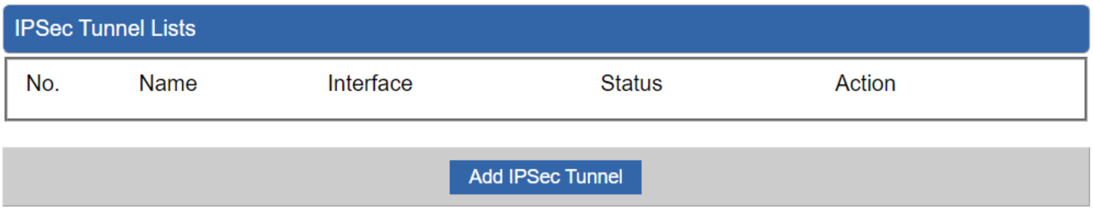
**Figure 4-9-1:** VPN Menu

| Object | Description |
|---|---|
| **IPsec** | Allows setting IPsec function. |
| **IPsec Remote Server** | Disable or enable the IPsec Remote Server function.<br>The default configuration is disabled. |
| **GRE** | Allows setting GRE function. |
| **PPTP** | Allows setting PPTP function. |
| **L2TP** | Allows setting L2TP function. |
| **SSL VPN** | Allows setting SSL VPN function. |
| **Certificates** | Download System CA Certificate |
| **VPN Connection** | Allows checking VPN Connection Status. |

## 4.9.1 IPSec

**IPSec** (IP Security) is a generic standardized VPN solution. IPSec must be implemented in the IP stack which is part of the kernel. Since IPSec is a standardized protocol it is compatible to most vendors that implement IPSec. It allows users to have an encrypted network session by standard **IKE** (Internet Key Exchange). We strongly encourage you to use IPSec only if you need to because of interoperability purposes. When IPSec lifetime is specified, the device can randomly refresh and identify forged IKE's during the IPSec lifetime.

This page will allow you to modify the user name and passwords as shown in Figure 4-9-2.

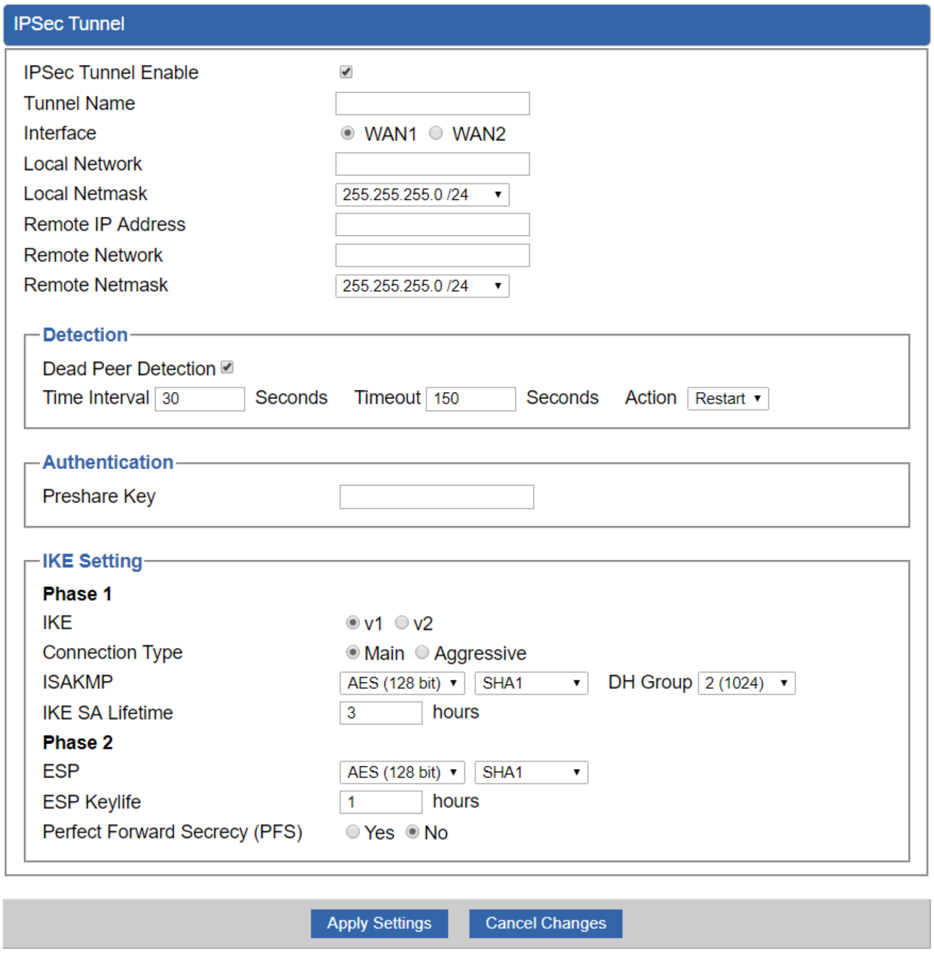


IPSec Tunnel Lists

| No. | Name | Interface | Status | Action |
|---|---|---|---|---|

**Figure 4-9-2:** IPSec

| Object | Description |
|---|---|
| **Add IPSec Tunnel** | Go to the Add IPSec Tunnel page to add a new tunnel. |



IPSec Tunnel

IPSec Tunnel Enable ☑
Tunnel Name
Interface ● WAN1 ○ WAN2
Local Network
Local Netmask 255.255.255.0 /24
Remote IP Address
Remote Network
Remote Netmask 255.255.255.0 /24

Detection
Dead Peer Detection ☑
Time Interval 30 Seconds Timeout 150 Seconds Action Restart

Authentication
Preshare Key

IKE Setting
**Phase 1**
IKE ● v1 ○ v2
Connection Type ● Main ○ Aggressive
ISAKMP AES (128 bit) SHA1 DH Group 2 (1024)
IKE SA Lifetime 3 hours
**Phase 2**
ESP AES (128 bit) SHA1
ESP Keylife 1 hours
Perfect Forward Secrecy (PFS) ○ Yes ● No

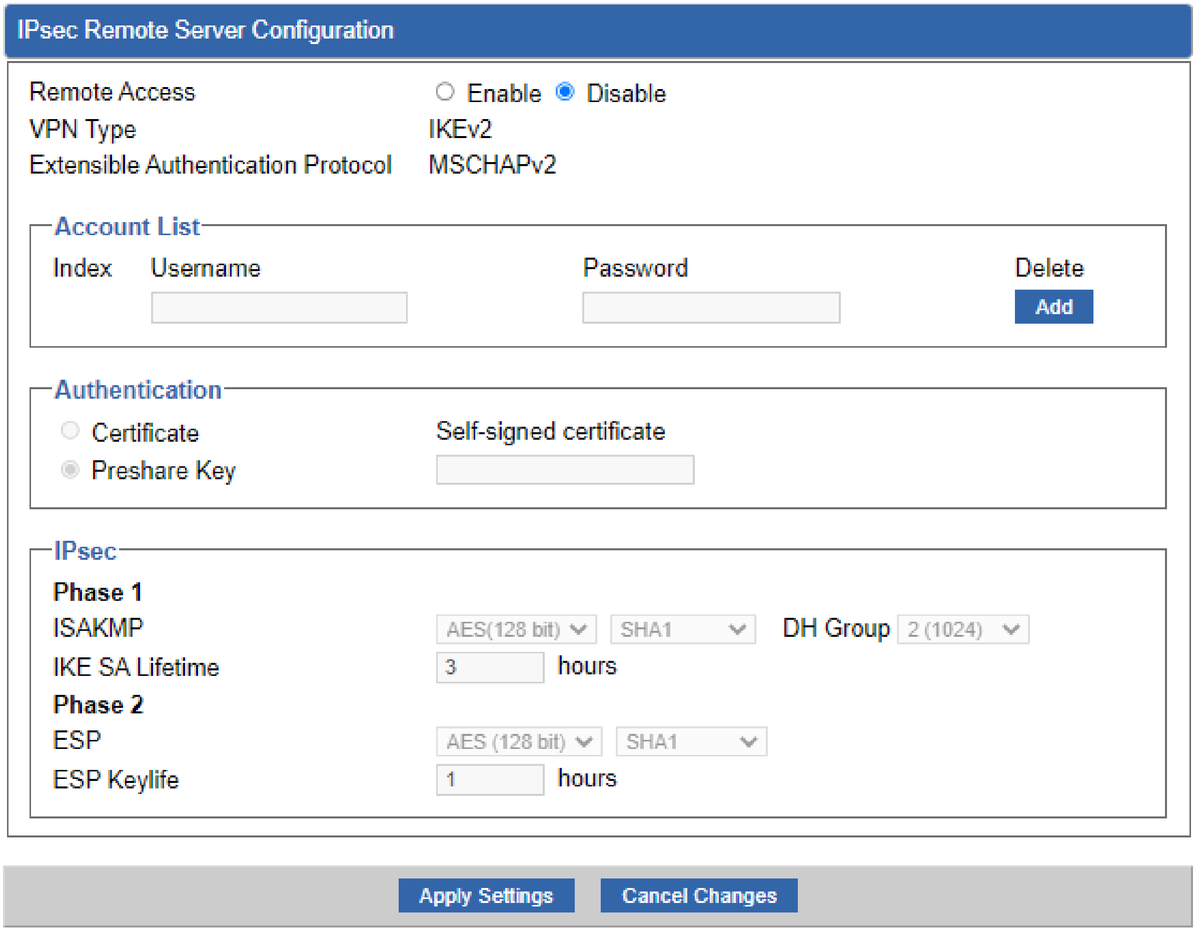
**Figure 4-9-3:** IPSec Tunnel

| Object | Description |
|---|---|
| **IPSec Tunnel Enable** | Check the box to enable the function. |
| **Tunnel Name** | Enter any words for recognition. |
| **Interface** | This is only available for host-to-host connections and specifies to which interface the host is connecting.<br>1. WAN 1.<br>2. WAN 2. |
| **Local Network** | The local subnet in CIDR notation. For instance, "192.168.1.0”. |
| **Local Netmask** | The netmask of this LoRaWAN Gateway |
| **Remote IP Address** | Input the IP address of the remote host. For instance, "210.66.1.10”. |
| **Remote Network** | The remote subnet in CIDR notation. For instance, "210.66.1.0”. |
| **Remote Netmask** | The netmask of the remote host. |
| **Dead Peer Detection** | Set up the detection time of **DPD** (Dead Peer Detection).<br>By default, the DPD detection’s gap is 30 seconds, over 150 seconds to think that is the broken line.<br>When VPN detects opposite party reaction time, the function will take one of the actions: “Hold” stand for the system will retain IPSec SA, "Clear" stand for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPSec SA and reset VPN tunnel. |
| **Preshare Key** | Enter a pass phrase to be used to authenticate the other side of the tunnel. Should be the same as the remote host. |
| **IKE** | Select the IKE (Internet Key Exchange) version. |
| **Connection Type** | 1. Main.<br>2. Aggressive. |

| | |
|---|---|
| **ISAKMP** | It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.<br>1. **AES**: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.<br>2. **3DES**: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.<br>3. **SHA1**: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.<br>4. **SHA2**: Either 256, 384 or 512 can be chosen<br>5. **MD5 Algorithm**: MD5 processes a variably long message into a fixed-length output of 128 bits.<br>6. **DH Group**: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen. |
| **IKE SA Lifetime** | You can specify how long IKE packets are valid. |
| **ESP** | It offers AES, 3 DES, SHA 1, SHA2, and MD5.<br>1. **AES**: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.<br>2. **3DES**: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.<br>3. **SHA1:** The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.<br>4. **SHA2**: Either 256, 384 or 512 can be chosen.<br>5. **MD5 Algorithm**: MD5 processes a variably long message into a fixed-length output of 128 bits. |
| **ESP Keylife** | You can specify how long ESP packets are valid. |
| **Perfect Forward Secrecy (PFS)** | Set the function as enable or disable. |

### 4.9.2 IPsec Remote Server

This section assists you in setting the IPsec Remote Server Configuration as shown below.



IPsec Remote Server Configuration

Remote Access ○ Enable ● Disable

VPN Type IKEv2

Extensible Authentication Protocol MSCHAPv2

Account List

| Index | Username | Password | Delete |
|---|---|---|---|
| | | | Add |

Authentication

○ Certificate Self-signed certificate

● Preshare Key

IPsec

**Phase 1**

ISAKMP AES(128 bit) SHA1 DH Group 2 (1024)

IKE SA Lifetime 3 hours

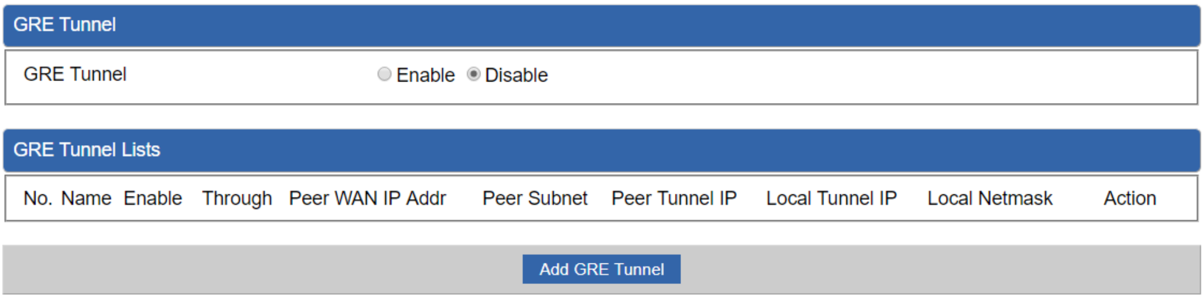
**Phase 2**

ESP AES (128 bit) SHA1

ESP Keylife 1 hours

### 4.9.3 GRE

This section assists you in setting the GRE Tunnel as shown in Figure 4-9-4.



GRE Tunnel

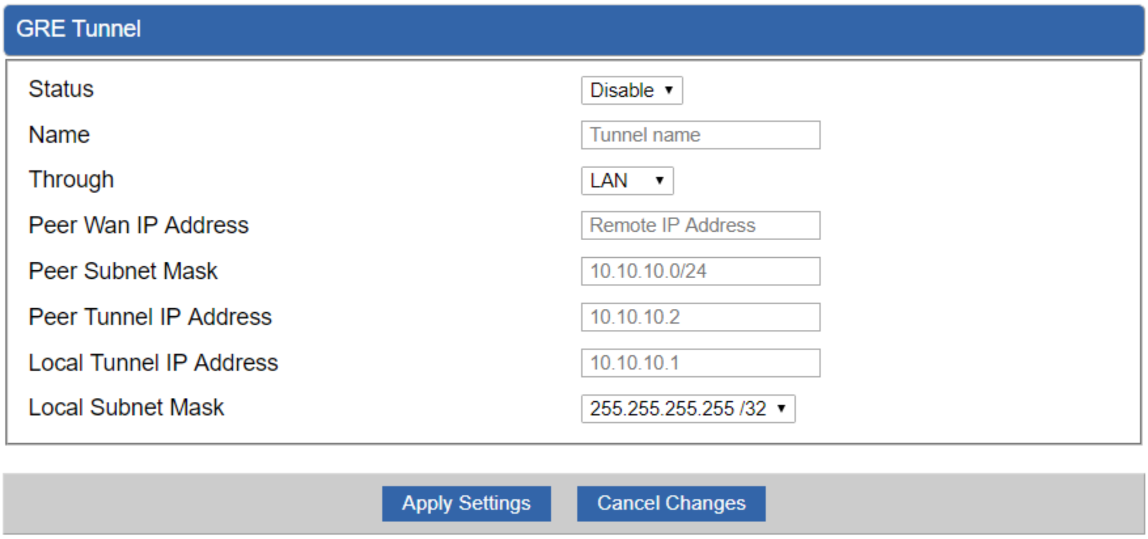
GRE Tunnel ○ Enable ● Disable

GRE Tunnel Lists

| No. | Name | Enable | Through | Peer WAN IP Addr | Peer Subnet | Peer Tunnel IP | Local Tunnel IP | Local Netmask | Action |
|---|---|---|---|---|---|---|---|---|---|

**Figure 4-9-4:** GRE

| Object | Description |
|---|---|
| **GRE Tunnel** | Set the function as enable or disable. |
| **Add GRE Tunnel** | Go to the Add GRE Tunnel page to add a new tunnel. |


GRE Tunnel

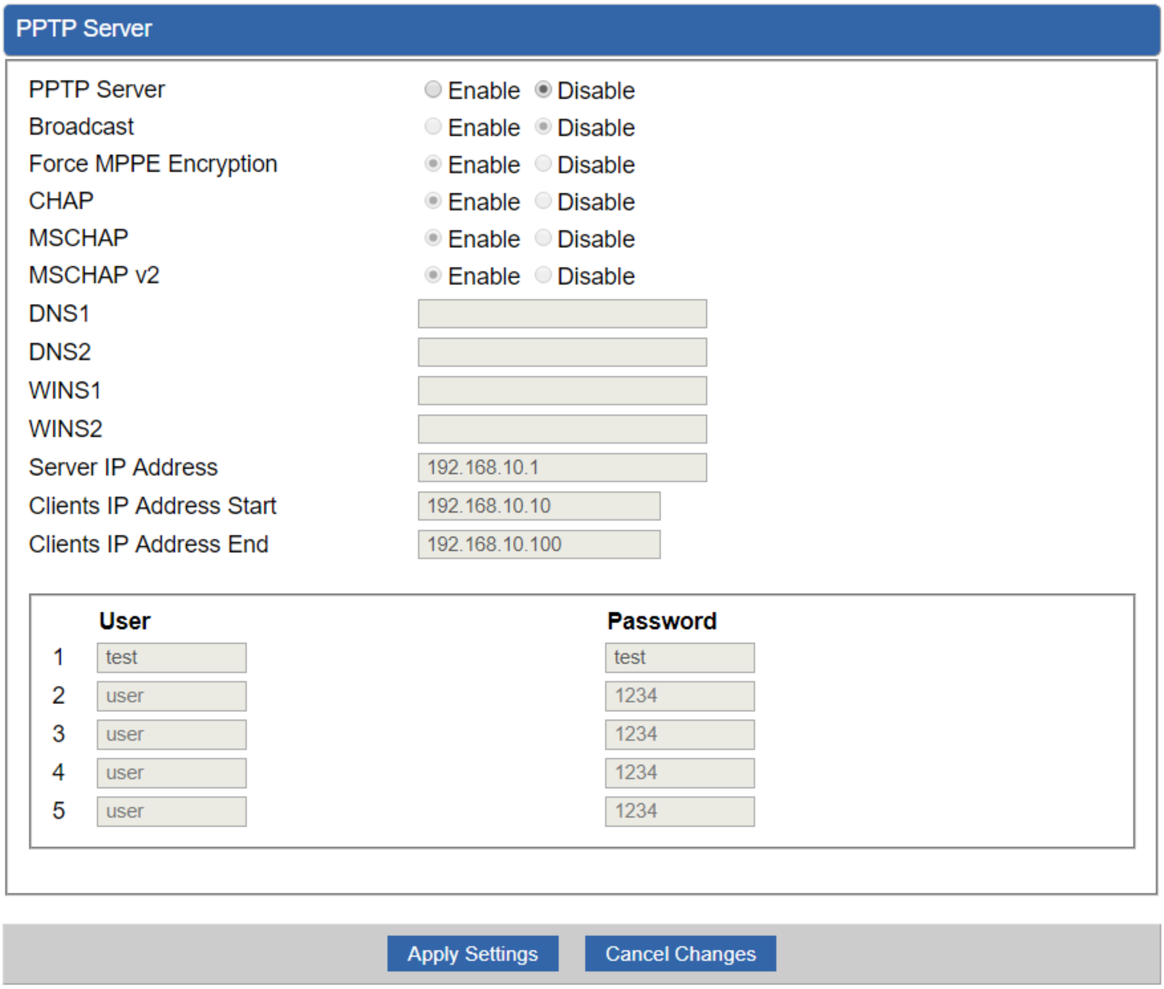
| | |
|---|---|
| Status | Disable ▾ |
| Name | Tunnel name |
| Through | LAN ▾ |
| Peer Wan IP Address | Remote IP Address |
| Peer Subnet Mask | 10.10.10.0/24 |
| Peer Tunnel IP Address | 10.10.10.2 |
| Local Tunnel IP Address | 10.10.10.1 |
| Local Subnet Mask | 255.255.255.255 /32 ▾ |

**Figure 4-9-5:** GRE Tunnel

| Object | Description |
|---|---|
| **Active** | Check the box to enable the function. |
| **Tunnel Name** | Enter any words for recognition. |
| **Through** | This is only available for host-to-host connections and specifies to which interface the host is connecting.<br>1. LAN.<br>2. WAN 1.<br>3. WAN 2. |
| **Peer WAN IP Address** | Input the IP address of the remote host. For instance, "210.66.1.10”. |
| **Peer Netmask** | The remote subnet in CIDR notation. For instance, "210.66.1.0/24”. |
| **Peer Tunnel IP Address** | Input the Tunnel IP address of remote host. |
| **Local Tunnel IP Address** | Input the Tunnel IP address of remote host. |
| **Local Netmask** | Input the Tunnel IP address of the LoRaWAN Gateway |

## 4.9.4 PPTP Server

Use the IP address and the scope option needs to match the far end of the PPTP server; its goal is to use the PPTP channel technology, and establish Site-to-Site VPN where the channel can have equally good results from different methods with IPSec. The PPTP server is shown in Figure 4-9-6.



PPTP Server

| | |
|---|---|
| PPTP Server | ○ Enable ● Disable |
| Broadcast | ○ Enable ● Disable |
| Force MPPE Encryption | ● Enable ○ Disable |
| CHAP | ● Enable ○ Disable |
| MSCHAP | ● Enable ○ Disable |
| MSCHAP v2 | ● Enable ○ Disable |
| DNS1 | |
| DNS2 | |
| WINS1 | |
| WINS2 | |
| Server IP Address | 192.168.10.1 |
| Clients IP Address Start | 192.168.10.10 |
| Clients IP Address End | 192.168.10.100 |

| | User | Password |
|---|---|---|
| 1 | test | test |
| 2 | user | 1234 |
| 3 | user | 1234 |
| 4 | user | 1234 |
| 5 | user | 1234 |

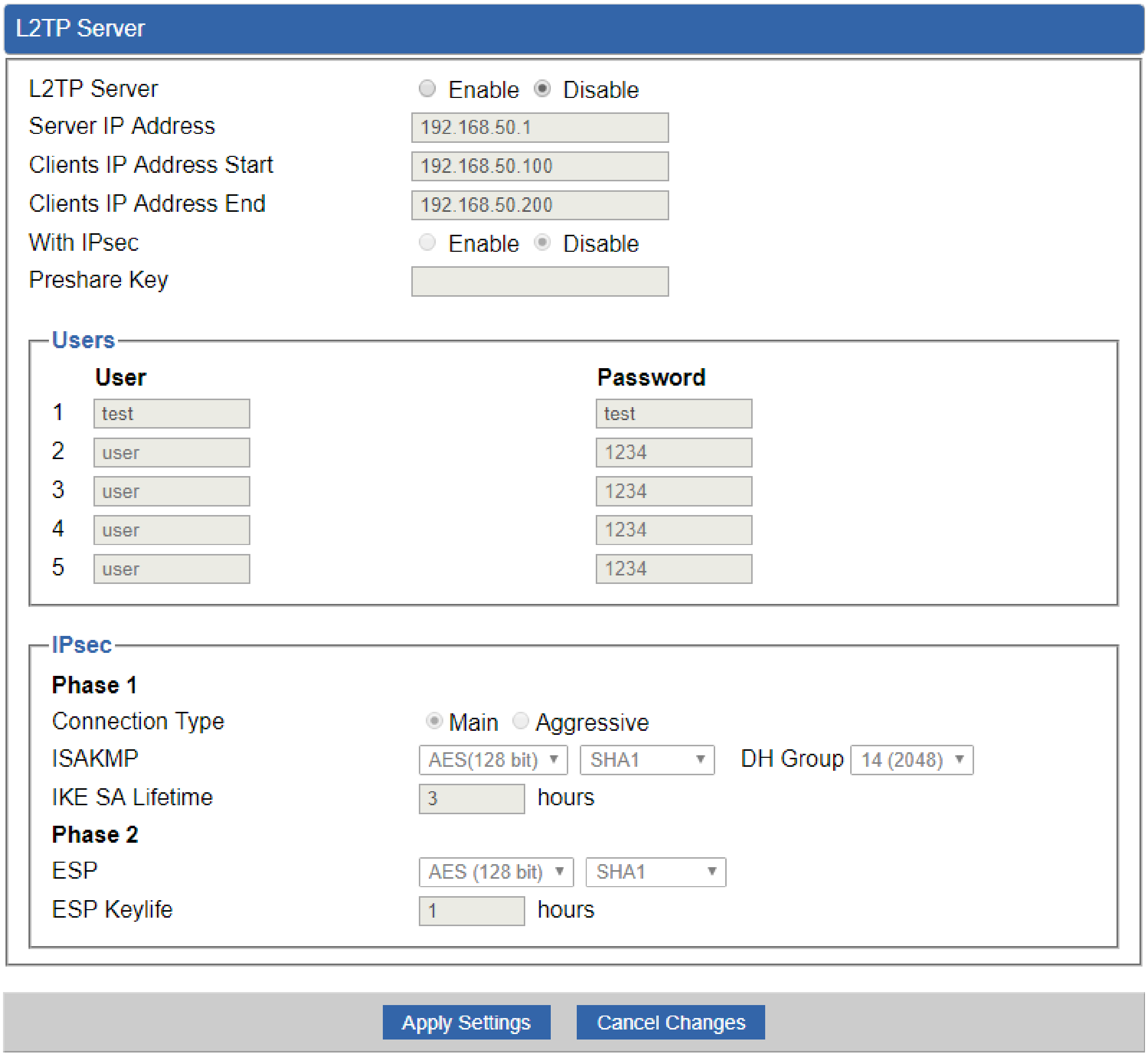
**Figure 4-9-6:** PPTP Server

| Object | Description |
|---|---|
| **PPTP Server** | Set the function as enable or disable. |
| **Broadcast** | Enter any words for recognition. |
| **Force MPPE Encryption** | Set the encryption as enable or disable. |
| **CHAP** | Set the authentication as enable or disable. |
| **MSCHAP** | Set the authentication as enable or disable. |

| | |
|---|---|
| **MSCHAP v2** | Set the authentication as enable or disable. |
| **DNS** | When the PPTP client connects to the PPTP server, it will assign the DNS server IP address to client. |
| **WINS** | When the PPTP client connects to the PPTP server, it will assign the WINS server IP address to client. |
| **Server IP Address** | Input the IP address of the PPTP Server. For instance, "192.168.10.1”. |
| **Clients IP Address (Start/End)** | When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.10.10”, the end IP address is "192.168.10.100”. |
| **User and Password** | Create the username and password for the VPN client. |

## 4.9.5 L2TP Server

This section assists you in setting the L2TP Server as shown in Figure 4-9-7.



L2TP Server

| | |
|---|---|
| L2TP Server | ○ Enable ● Disable |
| Server IP Address | 192.168.50.1 |
| Clients IP Address Start | 192.168.50.100 |
| Clients IP Address End | 192.168.50.200 |
| With IPsec | ○ Enable ● Disable |
| Preshare Key | |

Users

| | User | Password |
|---|---|---|
| 1 | test | test |
| 2 | user | 1234 |
| 3 | user | 1234 |
| 4 | user | 1234 |
| 5 | user | 1234 |

IPsec

**Phase 1**

| | |
|---|---|
| Connection Type | ● Main ○ Aggressive |
| ISAKMP | AES(128 bit) SHA1 DH Group 14 (2048) |
| IKE SA Lifetime | 3 hours |

**Phase 2**

| | |
|---|---|
| ESP | AES (128 bit) SHA1 |
| ESP Keylife | 1 hours |

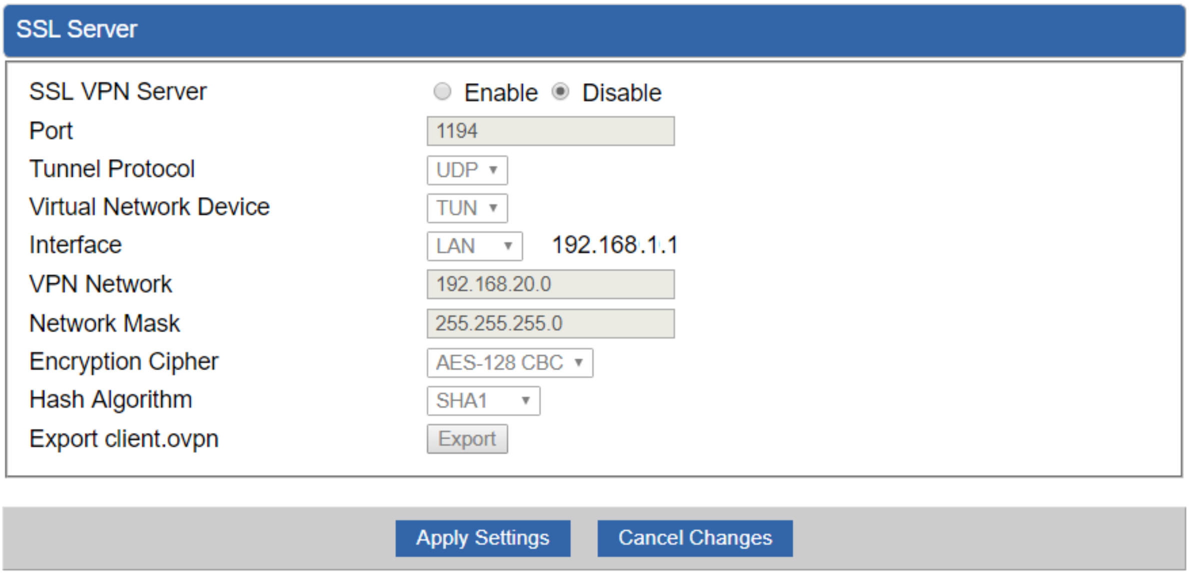
**Figure 4-9-7:** L2TP Server

| Object | Description |
|---|---|
| **L2TP Server** | Set the function as enable or disable. |
| **Server IP Address** | Input the IP address of the L2TP Server. For instance, "192.168.50.1”. |
| **Clients IP Address (Start/End)** | When the VPN connection is established, the VPN client will get IP address from the VPN Server. Please set the range of IP Address. For instance, the start IP address is "192.168.50.100”, the end IP address is "192.168.50.200”. |
| **With IPsec** | Set the function as enable to make the L2TP work with IPsec encryption. |
| **Preshare Key** | Enter a pass phrase. |

| Object | Description |
|---|---|
| **User and Password** | Create the username and password for the VPN client. |
| **Connection Type** | 1. Main.<br>2. Aggressive. |
| **ISAKMP** | It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.<br>1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.<br>2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.<br>3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.<br>4. SHA2: Either 256, 384 or 512 can be chosen.<br>5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits.<br>6. DH Group: Either 1, 2, 5, 14, 15, 16, 17, or 18 can be chosen. |
| **IKE SA Lifetime** | You can specify how long IKE packets are valid. |
| **ESP** | It offers AES, 3 DES, SHA 1, SHA2, and MD5.<br>1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.<br>2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.<br>3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.<br>4. SHA2: Either 256, 384 or 512 can be chosen.<br>5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. |
| **ESP Keylife** | You can specify how long ESP packets are valid. |

## 4.9.6 SSL VPN

This section assists you in setting the SSL Server as shown in Figure 4-9-8.



SSL Server

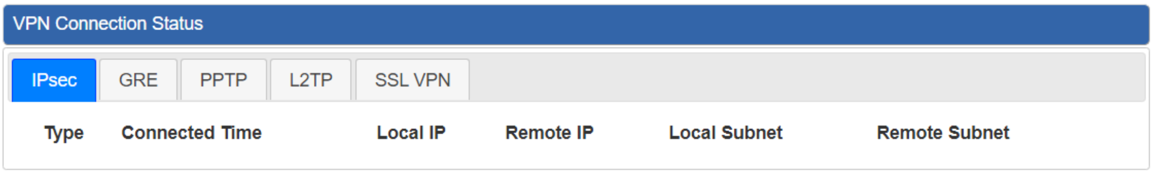
| | |
|---|---|
| SSL VPN Server | ○ Enable ● Disable |
| Port | 1194 |
| Tunnel Protocol | UDP ▾ |
| Virtual Network Device | TUN ▾ |
| Interface | LAN ▾ 192.168.1.1 |
| VPN Network | 192.168.20.0 |
| Network Mask | 255.255.255.0 |
| Encryption Cipher | AES-128 CBC ▾ |
| Hash Algorithm | SHA1 ▾ |
| Export client.ovpn | Export |

**Figure 4-9-8:** SSL Server

| Object | Description |
|---|---|
| **SSL VPN Server** | Set the function as enable or disable. |
| **Port** | Set a port for the SSL Service. Default port is 1194. |
| **Tunnel Protocol** | Set the protocol as TCP or UDP. |
| **Virtual Network Device** | Set the Virtual Network Device as TUN or TAP. |
| **Interface** | User is able to select the interface for SSL service using. |
| **VPN Network** | The VPN subnet in CIDR notation. For instance, "192.168.20.0”. |
| **Network Mask** | The netmask of the VPN. |
| **Encryption Cipher** | There are four encryption types: None, AES-128 CBC, AES-192 CBC or AES-256 CBC. |
| **Hash Algorithm** | There are five types of Hash Algorithm: None, SHA1, SHA1, SHA512 or MD5. |
| **Export client.ovpn** | Export a configuration for the SSL client. User is able to upload it to VPN client (such as Open VPN software). |

### 4.9.7 VPN Connection

This page shows the VPN connection status as shown in Figure 4-9-9.



VPN Connection Status

| Type | Connected Time | Local IP | Remote IP | Local Subnet | Remote Subnet |
|---|---|---|---|---|---|

**Figure 4-9-9:** VPN Connection Status

| Object | Description |
|---|---|
| **VPN Connection Status** | Click the IPSec/GRE/…/SSL VPN bookmark to check the current connection status. |

## 4.10Wireless

The Wireless menu provides the following features as shown in Figure 4-10-1

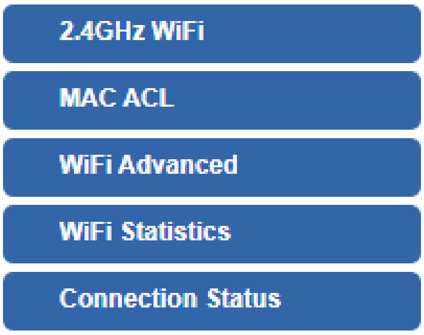
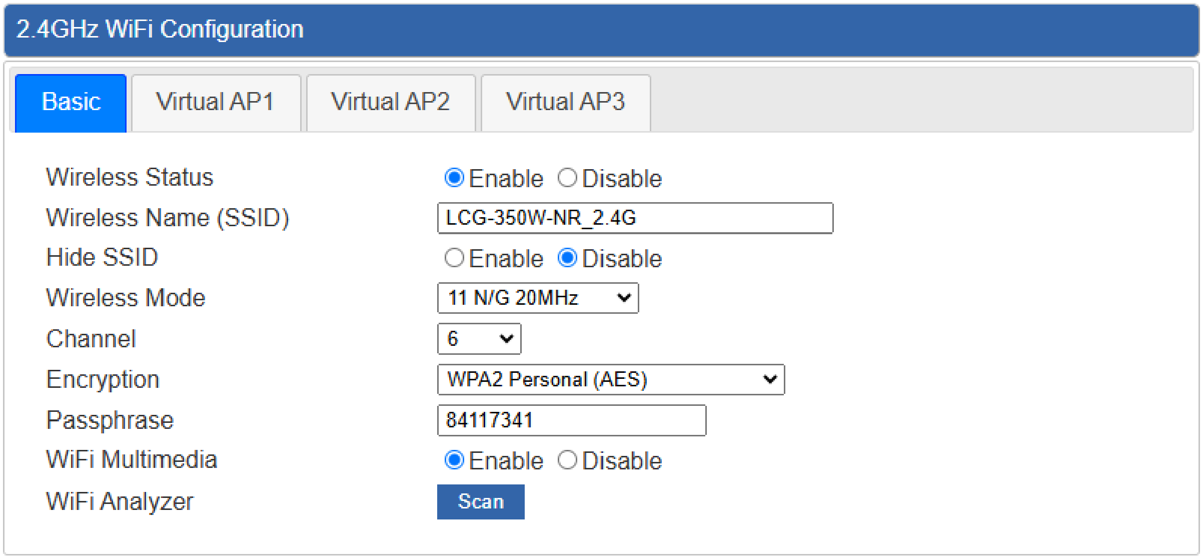


**Figure 4-10-1:** Wireless Menu

| Object | Description |
|---|---|
| **2.4G Wi-Fi** | Allow to configure 2.4G Wi-Fi. |
| **MAC ACL** | Allow configure MAC ACL. |
| **Wi-Fi Advanced** | Allow to configure advanced setting of Wi-Fi. |
| **Wi-Fi Statistics** | Display the statistics of Wi-Fi traffic. |
| **Connection Status** | Display the connection status. |

## 4.10.1 2.4G Wi-Fi

This page allows the user to define 2.4G Wi-Fi as shown in Figure 4-10-2.



2.4GHz WiFi Configuration

| | |
|---|---|
| Wireless Status | ● Enable ○ Disable |
| Wireless Name (SSID) | LCG-350W-NR_2.4G |
| Hide SSID | ○ Enable ● Disable |
| Wireless Mode | 11 N/G 20MHz |
| Channel | 6 |
| Encryption | WPA2 Personal (AES) |
| Passphrase | 84117341 |
| WiFi Multimedia | ● Enable ○ Disable |
| WiFi Analyzer | Scan |

**Figure 4-10-2:** 2.4G Wi-Fi

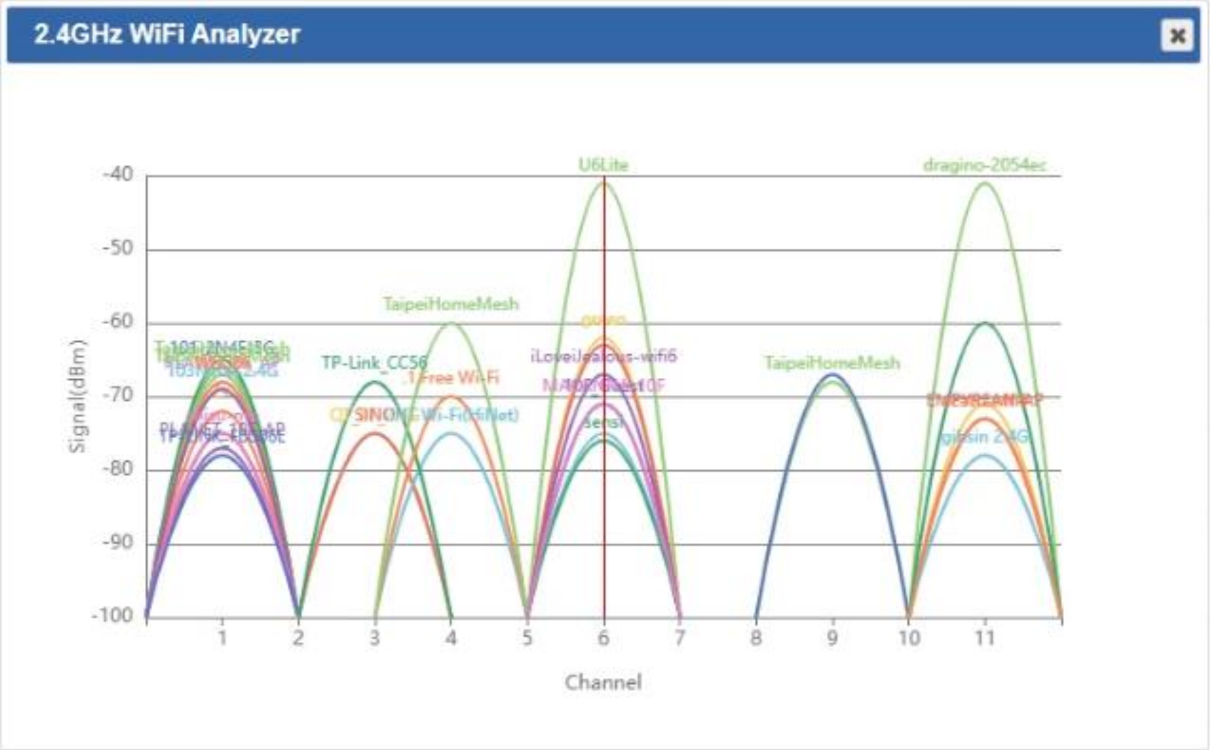
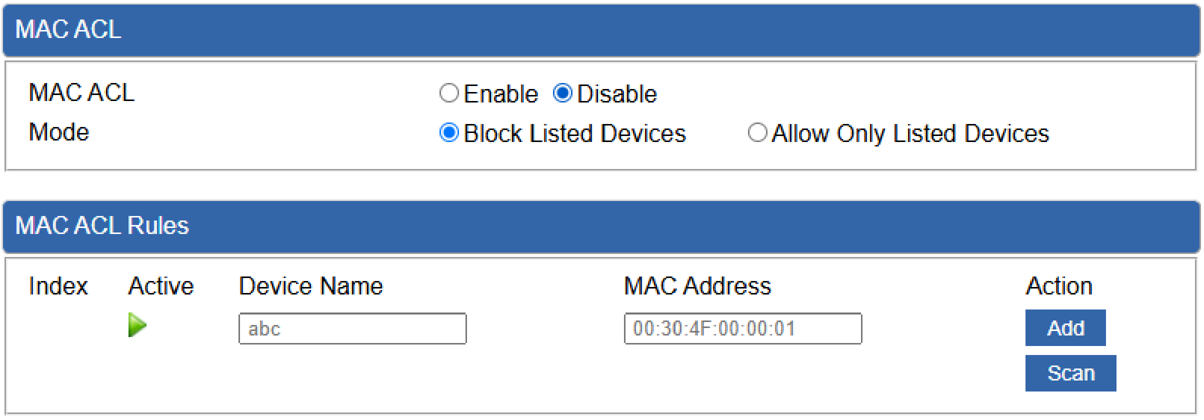


**Figure 4-10-3:** 2.4G Wi-Fi Analyzer

| Object | Description |
|---|---|
| **Wireless Status** | Allows user to enable or disable 2.4G WiFi |
| **Wireless Name (SSID)** | It is the wireless network name. The default 2.4G SSID is “PLANET_2.4G” |
| **Hide SSID** | Allows user to enable or disable SSID |
| **Bandwidth** | Select the operating channel width, “**20MHz**” or “**40MHz**” |
| **Channel** | It shows the channel of the CPE. Default 2.4GHz is channel 6. |
| **Encryption** | Select the wireless encryption. The default is “**Open**” |
| **WiFi Multimedia** | Enable/Disable WMM (Wi-Fi Multimedia ) function |

## 4.10.2 MAC ACL

This page provides MAC ACL configuration as shown in Figure 4-10-4.



MAC ACL

| | |
|---|---|
| MAC ACL | ○ Enable ● Disable |
| Mode | ● Block Listed Devices ○ Allow Only Listed Devices |

MAC ACL Rules

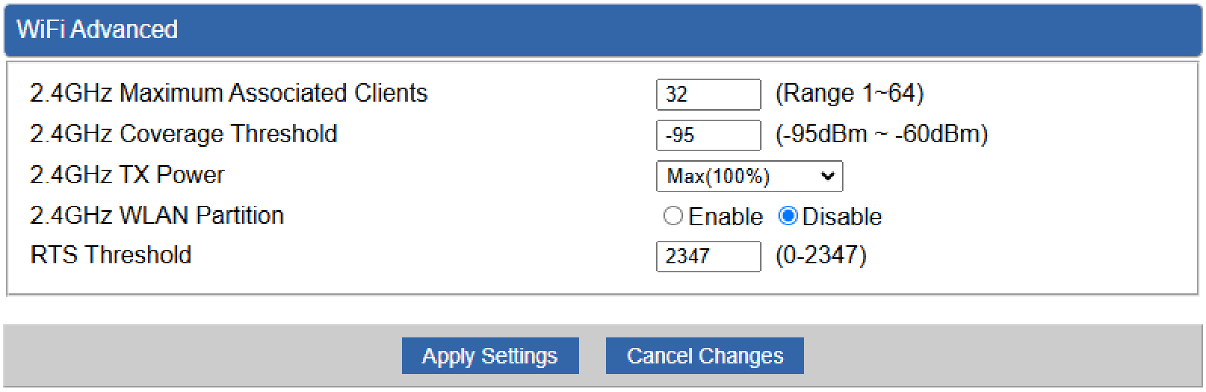
| Index | Active | Device Name | MAC Address | Action |
|---|---|---|---|---|
| | ▶ | abc | 00:30:4F:00:00:01 | Add<br>Scan |

**Figure 4-10-4:** MAC ACL

| Object | Description |
|---|---|
| **Mode** | Enables the rule to allow or deny client access to the network. |
| **Active** | Allows the devices to pass in the rule |
| **Device Name** | Set an allowed device name |
| **MAC Address** | Set an allowed device MAC address |
| **Add** | Press the "**Add**" button to add end-device that is scanned from wireless network and mark them |
| **Scan** | Connect to client list |

## 4.10.3 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi as shown in Figure 4-10-5.



WiFi Advanced

|  |  |
|---|---|
| 2.4GHz Maximum Associated Clients | 32 (Range 1~64) |
| 2.4GHz Coverage Threshold | -95 (-95dBm ~ -60dBm) |
| 2.4GHz TX Power | Max(100%) |
| 2.4GHz WLAN Partition | ○ Enable ● Disable |
| RTS Threshold | 2347 (0-2347) |

**Figure 4-10-5:** Wi-Fi advanced

| Object | Description |
|---|---|
| **2.4G Mode** | 11N: Select 802.11B/G or 802.11N/G |
| **2.4GHz Maximum Associated Clients** | The maximum users are 64 |
| **2.4G Coverage Threshold** | The coverage threshold is to limit the weak signal of clients occupying session. The default is -95dBm |
| **2.4G TX Power** | The range of transmit power is **Max (100%)**, **Efficient (75%)**, **Enhanced (50%), Standard (25%)** or **Min (15%)**. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power |

## 4.10.4 Wi-Fi Statistics

This page displays Wi-Fi statistics as shown in Figure 4-10-6.

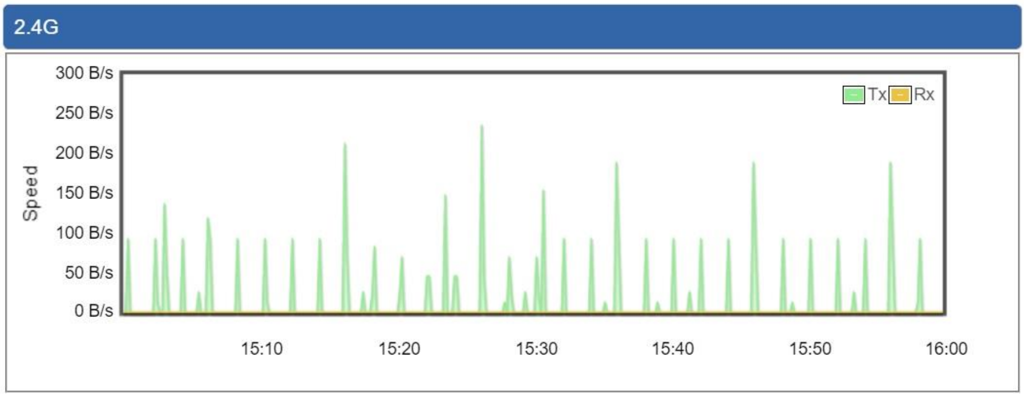
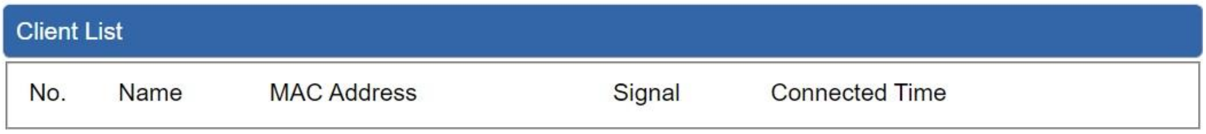


**Figure 4-10-6:** Wi-Fi Statistics

### 4.10.5 Connection Status

This page shows the host names and MAC address of all the clients in your network as shown in Figure 4-10-7.



| | | | | |
|---|---|---|---|---|
| No. | Name | MAC Address | Signal | Connected Time |

Figure 4-10-7: Connection status

| Object | Description |
|---|---|
| **Name** | Display the host name of connected clients. |
| **MAC Address** | Display the MAC address of connected clients. |
| **Signal** | Display the connected signal of connected clients. |
| **Connected Time** | Display the connected time of connected clients. |

# 4.11 Maintenance

The Maintenance menu provides the following features for managing the system as shown in Figure 4-11-1

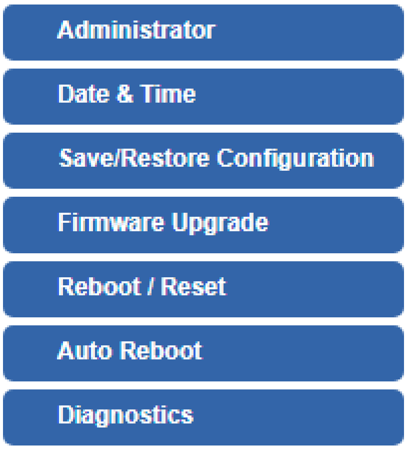
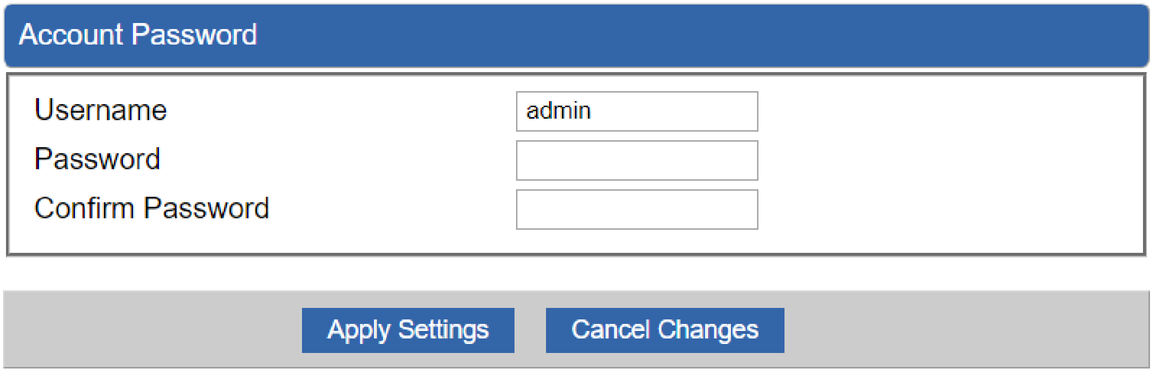


**Figure 4-11-1:** Maintenance Menu

| Object | Description |
|---|---|
| **Administrator** | Allows changing the login username and password. |
| **Date & Time** | Allows setting Date & Time function. |
| **Save/Restore Configuration** | Export the LoRaWAN Gateway's configuration to local or USB sticker.<br>Restore the LoRaWAN Gateway's configuration from local or USB sticker. |
| **Firmware Upgrade** | Upgrade the firmware from local or USB storage. |
| **Reboot / Reset** | Reboot or reset the system. |
| **Auto Reboot** | Allows setting auto-reboot schedule. |
| **Diagnostics** | Allows you to issue ICMP PING packets to troubleshoot IP. |

### 4.11.1 Administrator

To ensure the LoRaWAN Gateway's security is secure, you will be asked for your password when you access the LoRaWAN Gateway's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords as shown in Figure 4-11-2.



Account Password

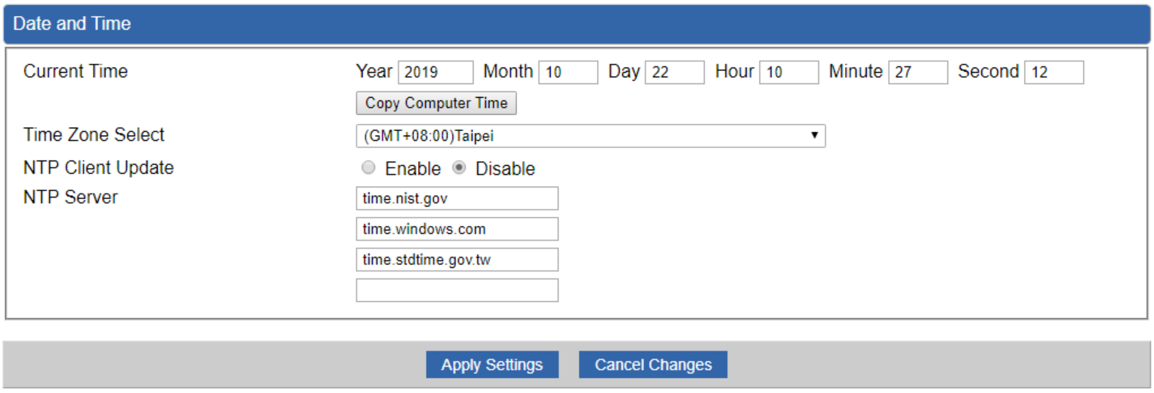
| | |
|---|---|
| Username | admin |
| Password | |
| Confirm Password | |

**Figure 4-11-2:** Account and Password

| Object | Description |
|---|---|
| **Username** | Input a new username. |
| **Password** | Input a new password. |
| **Confirm Password** | Input password again. |

### 4.11.2 Date and Time

This section assists you in setting the system time of the LoRaWAN Gateway. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown in Figure 4-11-3.



Date and Time

Current Time: Year 2019 Month 10 Day 22 Hour 10 Minute 27 Second 12

Time Zone Select: (GMT+08:00)Taipei

NTP Client Update: ○ Enable ● Disable

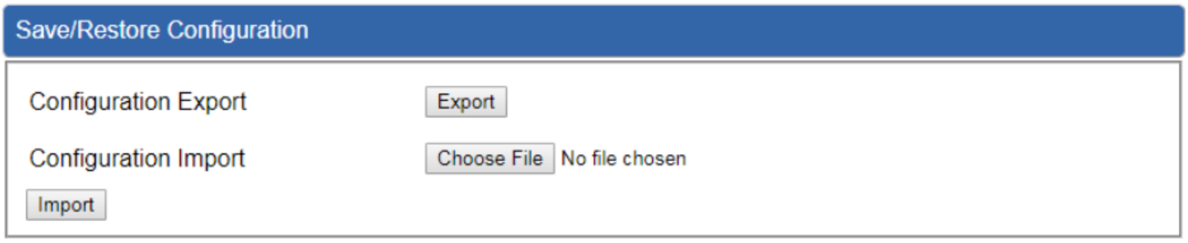
NTP Server: time.nist.gov<br>time.windows.com<br>time.stdtime.gov.tw

**Figure 4-11-3:** Date and Time

| Object | Description |
|---|---|
| **Current Time** | Show the current time.<br>User is able to set time and date manually. |
| **Time Zone Select** | Select the time zone of the country you are currently in. The LoRaWAN Gateway will set its time based on your selection. |
| **NTP Client Update** | Once this function is enabled, LoRaWAN Gateway will automatically update current time from NTP server. |
| **NTP Server** | User may use the default NTP sever or input NTP server manually. |

## 4.11.3 Saving/Restoring Configuration

This page shows the status of the configuration. You may save the setting file to either USB storage or PC and load the setting file from USB storage or PC as Figure 4-11-4 is shown below:



Save/Restore Configuration

Configuration Export
Configuration Import

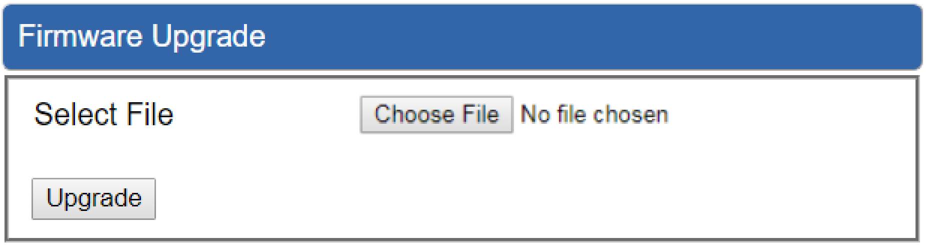
**Figure 4-11-4:** Saving/Restoring Configuration

- **Save Setting to PC**

| Object | Description |
|---|---|
| **Configuration Export** | Press the Export button to save setting file to PC. |
| **Configuration Import** | Press the Choose File button to select the setting file, and then press the Import button to upload setting file from PC. |

## 4.11.4 Upgrading Firmware

This page provides the firmware upgrade function as shown in Figure 4-11-5



Firmware Upgrade

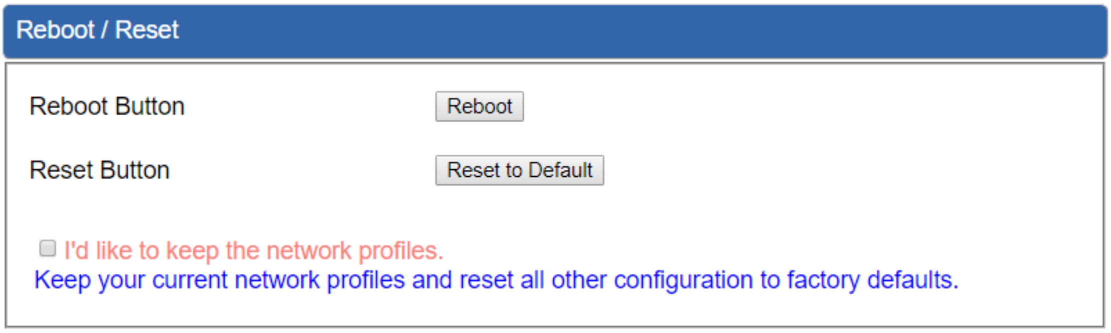
Select File

**Figure 4-11-5:** Firmware Upgrade

| Object | Description |
|---|---|
| **Choose File** | Press the button to select the firmware. |
| **Upgrade** | Press the button to upgrade firmware to system. |

### 4.11.5 Reboot / Reset

This page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in the Web interface as Figure 4-11-6 is shown below:



Reboot / Reset

Reboot Button

Reset Button

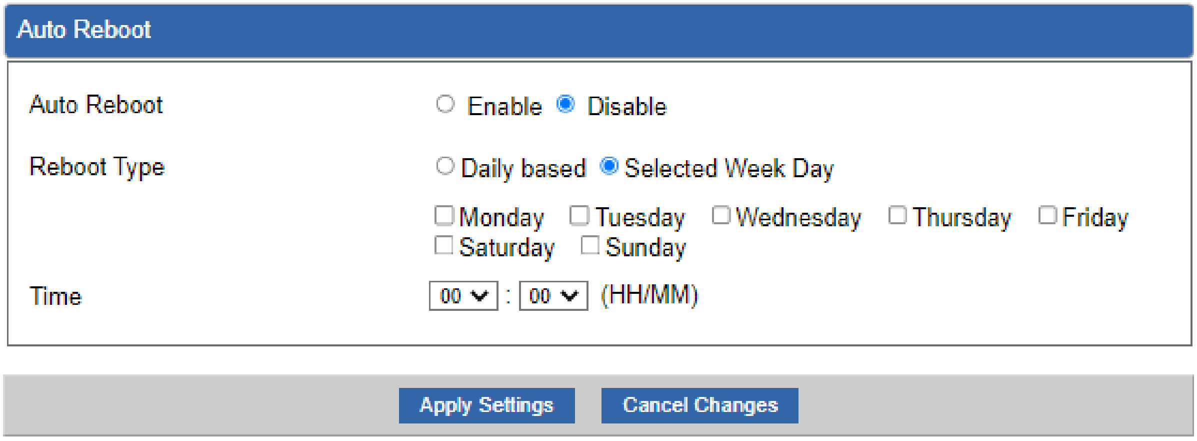
□ I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

**Figure 4-11-6:** Reboot and Reset

| Object | Description |
|---|---|
| **Reboot** | Press the button to reboot system. |
| **Reset** | Press the button to restore all settings to factory default settings. |
| **I'd like to keep the network profiles.** | Check the box and then press the Reset to Default button to keep the current network profiles and reset all other configurations to factory defaults. |

### 4.11.6 Auto Reboot

This page provides the Auto Reboot function as shown below



Auto Reboot

Auto Reboot ○ Enable ● Disable

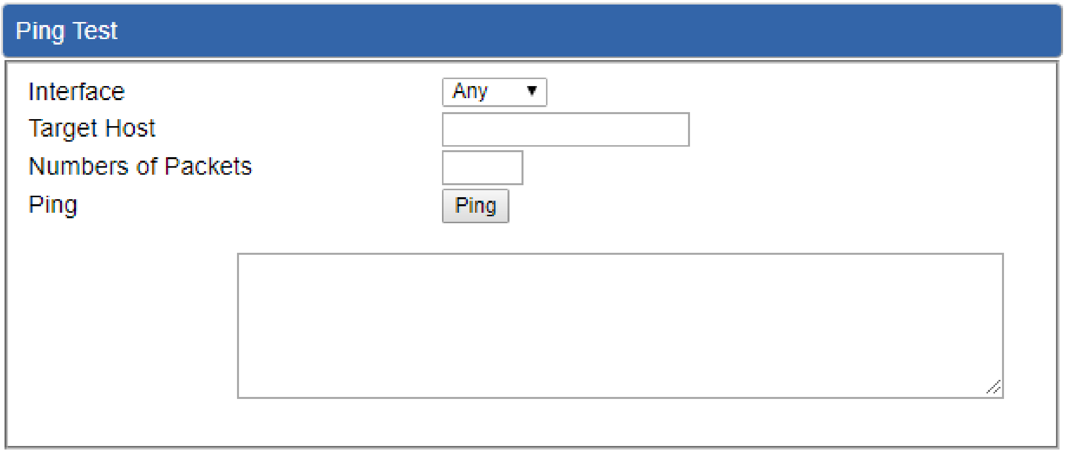
Reboot Type ○ Daily based ● Selected Week Day

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Time 00 : 00 (HH/MM)

## 4.11.7 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “Ping”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs as shown in Figure 4-11-7



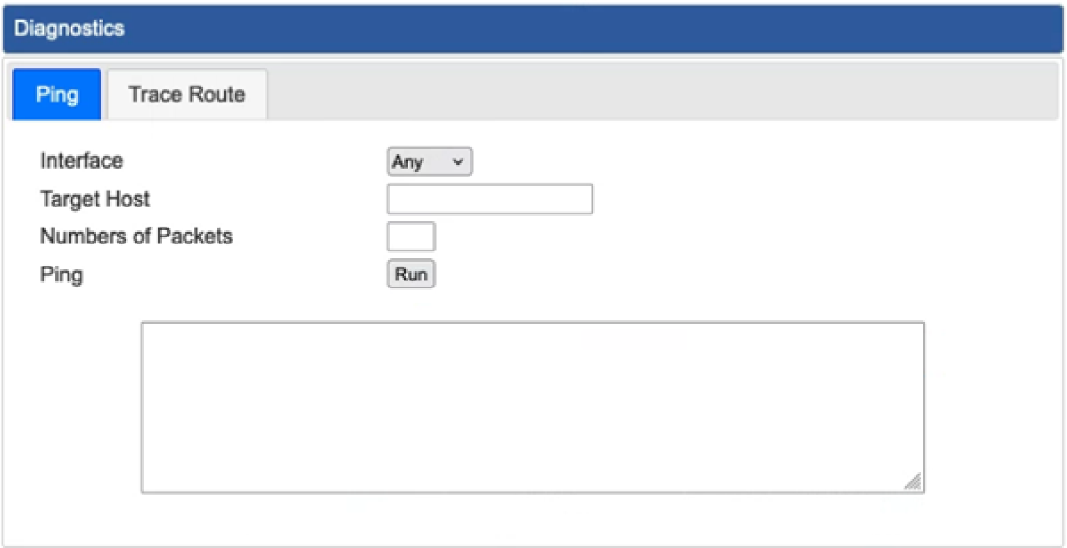


**Figure 4-11-7:** Diagnostics

| Object | Description |
|---|---|
| **Interface** | Select an interface of the LoRaWAN Gateway |
| **Target Host** | The destination IP Address or domain. |
| **Number of Packets** | Set the number of packets that will be transmitted; the maximum is 100. |
| **Ping** | The time of ping. |

Note

Be sure the target IP address is within the same network subnet of the LoRaWAN Gateway, or you have to set up the correct gateway IP address.

# Appendix A:

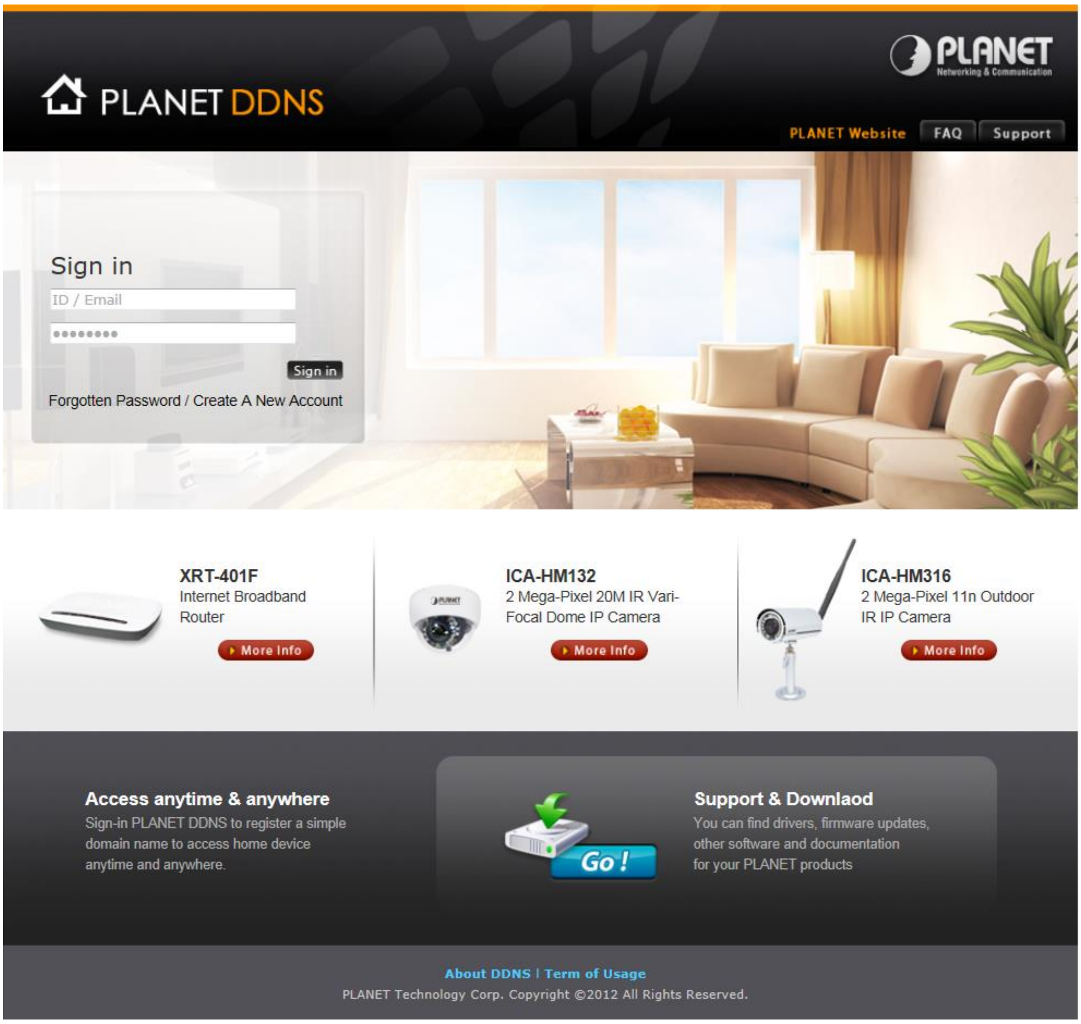
# Appendix A: DDNS Application

**Configuring PLANET DDNS steps:**

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at http://planetddns.com

Step 2: Enable DDNS option through accessing web page of the device.

Step 3: Input all DDNS settings.



XRT-401F
Internet Broadband Router

ICA-HM132
2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera

ICA-HM316
2 Mega-Pixel 11n Outdoor IR IP Camera

Access anytime & anywhere
Sign-in PLANET DDNS to register a simple domain name to access home device anytime and anywhere.

Support & Downlaod
You can find drivers, firmware updates, other software and documentation for your PLANET products

PLANET Technology Corp. Copyright ©2012 All Rights Reserved.

# Appendix B: LoRaWAN Settings

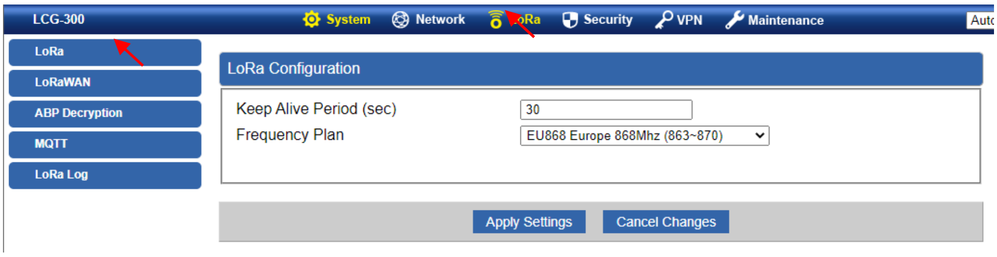
## Setting Up to Connect with TTN (The Things Network)

**The Setting Up of LCG-300 series**

1. LoRa Setting

   a. Open browser and log in to the Web GUI of LCG-300 series.

   b. Click **LoRa** under the main menu and **LoRa** on function menu.

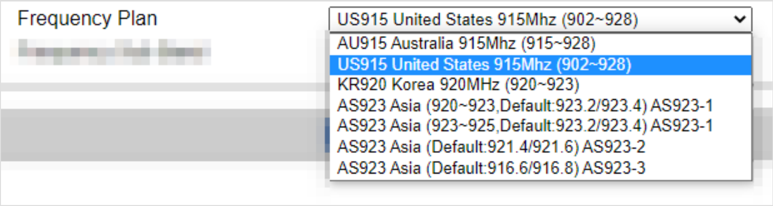
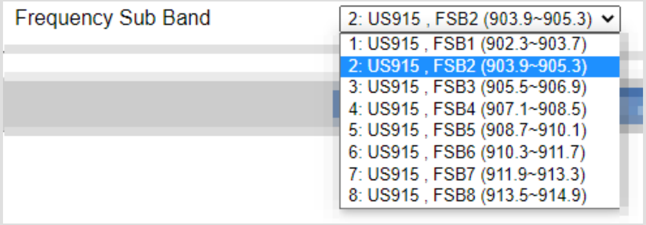
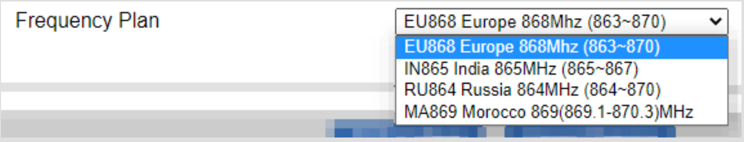


LoRa Configuration

Keep Alive Period (sec): 30

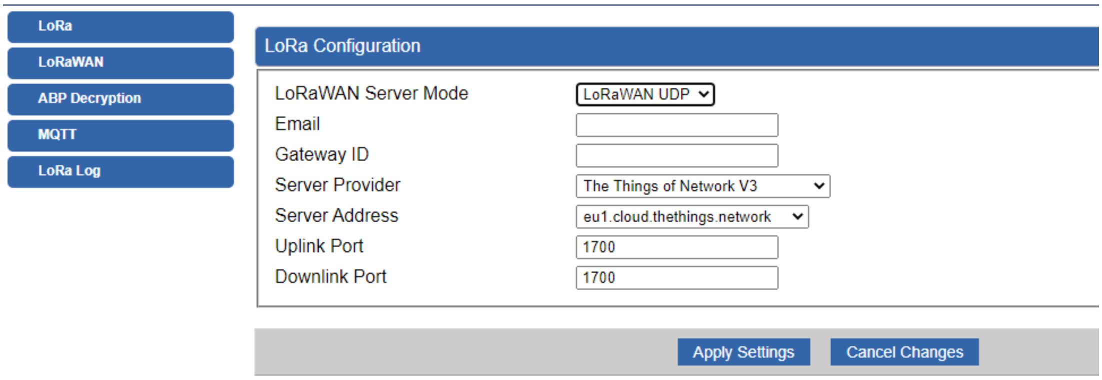
Frequency Plan: EU868 Europe 868Mhz (863~870)

Select the **Frequency Plan** for your local area. Some Frequency Bands support **Frequency Sub Band**. (In this case, select “US915” for frequency band and “US915 and FSB2” for frequency sub-band.)

| | |
|---|---|
| LCG-300<br>series-US | <br>Frequency Plan: US915 United States 915Mhz (902~928)<br>AU915 Australia 915Mhz (915~928)<br>US915 United States 915Mhz (902~928)<br>KR920 Korea 920MHz (920~923)<br>AS923 Asia (920~923,Default:923.2/923.4) AS923-1<br>AS923 Asia (923~925,Default:923.2/923.4) AS923-1<br>AS923 Asia (Default:921.4/921.6) AS923-2<br>AS923 Asia (Default:916.6/916.8) AS923-3<br><br>Frequency Sub Band: 2: US915 , FSB2 (903.9~905.3)<br>1: US915 , FSB1 (902.3~903.7)<br>2: US915 , FSB2 (903.9~905.3)<br>3: US915 , FSB3 (905.5~906.9)<br>4: US915 , FSB4 (907.1~908.5)<br>5: US915 , FSB5 (908.7~910.1)<br>6: US915 , FSB6 (910.3~911.7)<br>7: US915 , FSB7 (911.9~913.3)<br>8: US915 , FSB8 (913.5~914.9) |
| LCG-300<br>series-EU | <br>Frequency Plan: EU868 Europe 868Mhz (863~870)<br>EU868 Europe 868Mhz (863~870)<br>IN865 India 865MHz (865~867)<br>RU864 Russia 864MHz (864~870)<br>MA869 Morocco 869(869.1-870.3)MHz |

2. LoRaWAN Setting

Click **LoRaWAN** and input the related data.



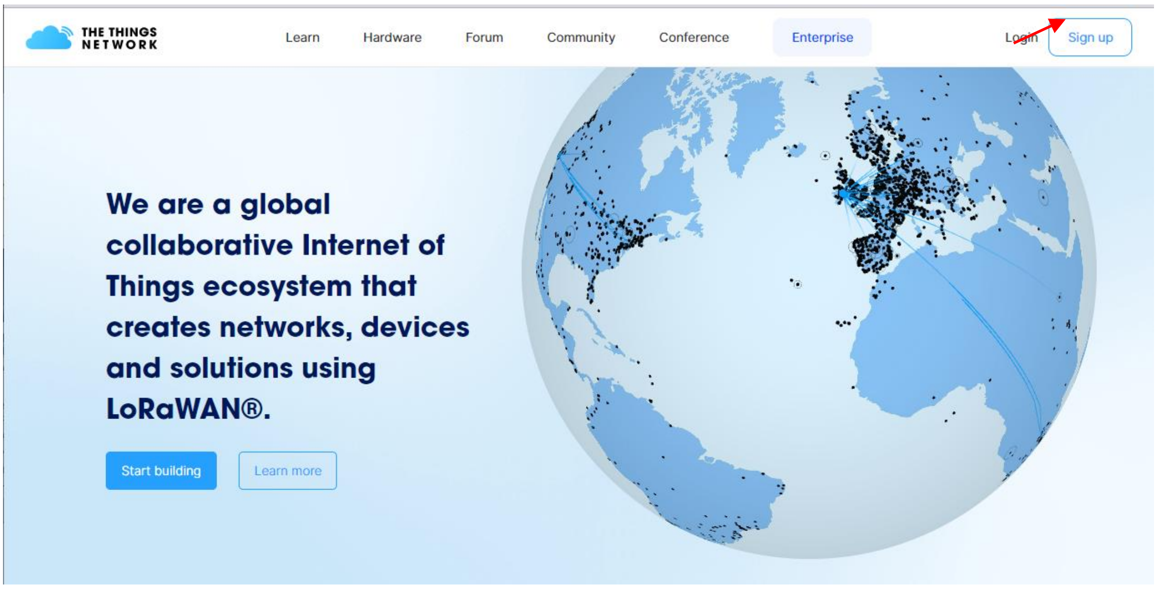
LoRa Configuration

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | |
| Server Provider | The Things of Network V3 |
| Server Address | eu1.cloud.thethings.network |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

| | |
|---|---|
| LoRaWAN Server Mode | **LoRaWAN UDP** |
| Email | kinlin.planet@gmail.com (TTN account) |
| Gateway ID | a8f7e01234567895 |
| Server Provider | The Things of Network V3 |
| Server Address | eu1.cloud.thethings.network<br>nam1.cloud.thethings.network<br>au1.cloud.thethings.network |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

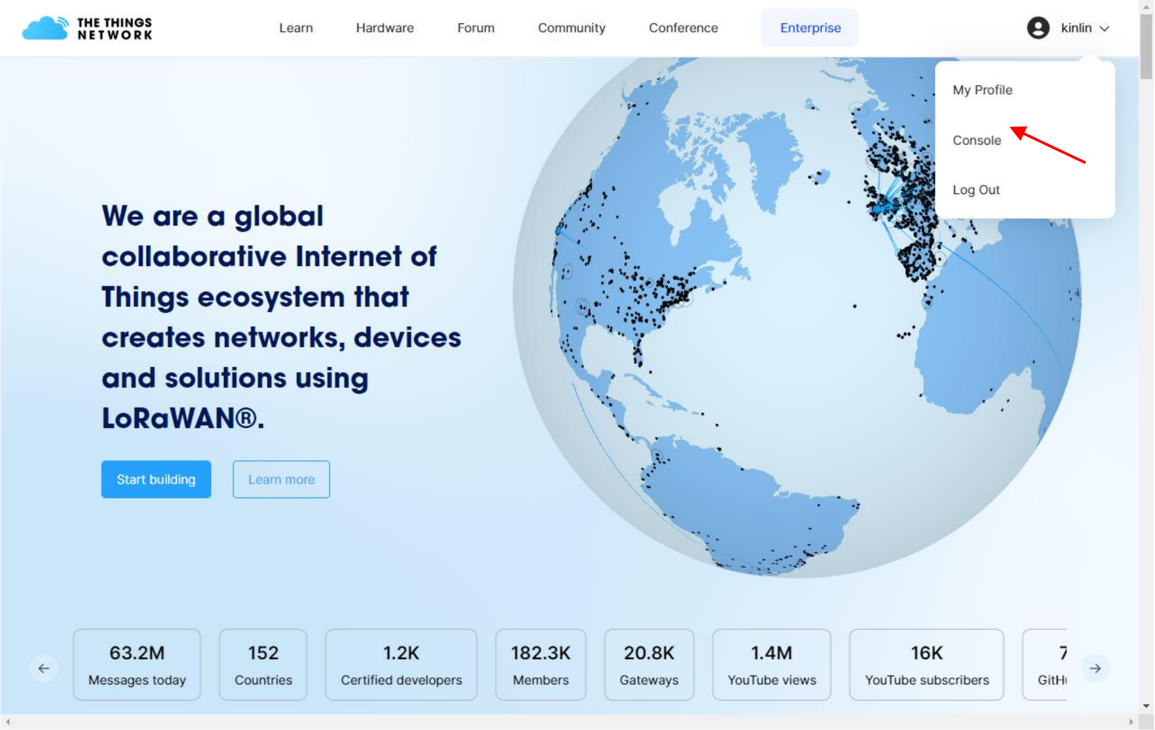
**The Setting Up of the Things Network**

1. Log in to TTN (https://www.thethingsnetwork.org/). Please sign up before logging in.



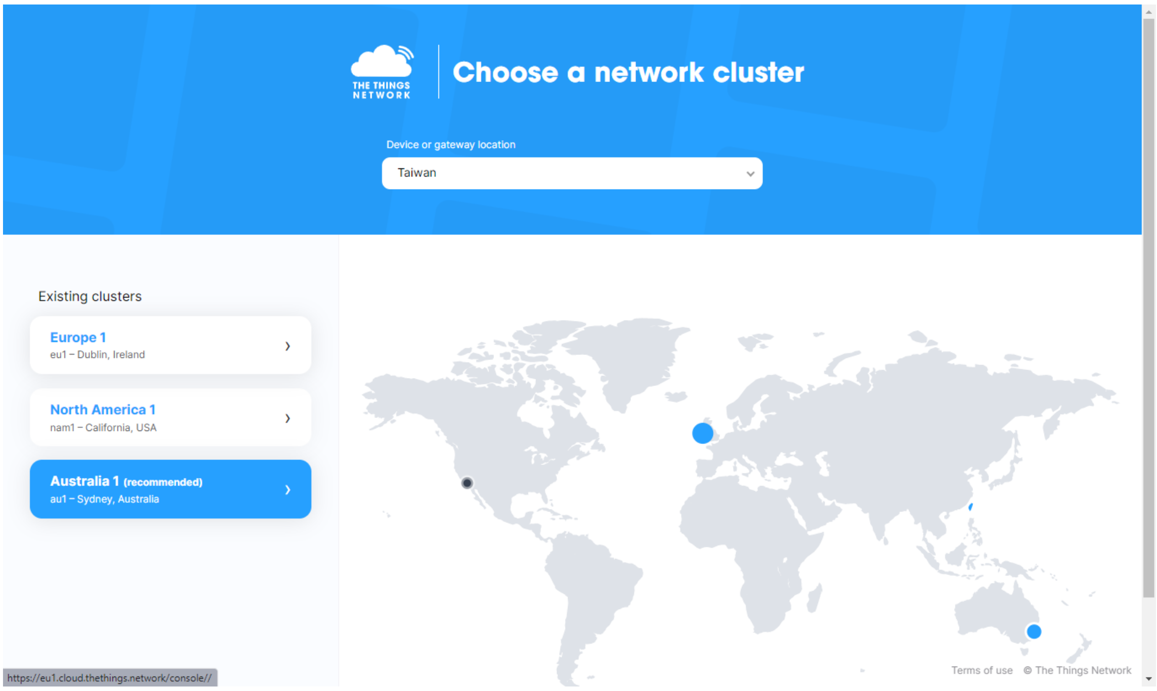
We are a global collaborative Internet of Things ecosystem that creates networks, devices and solutions using LoRaWAN®.

a. After logging in, select “console” under “account” shown in the upper right corner of the page.



b. Select a cluster which is near your location. The cluster will be the **server address** of LoRaWAN in the LCG-300 setting.

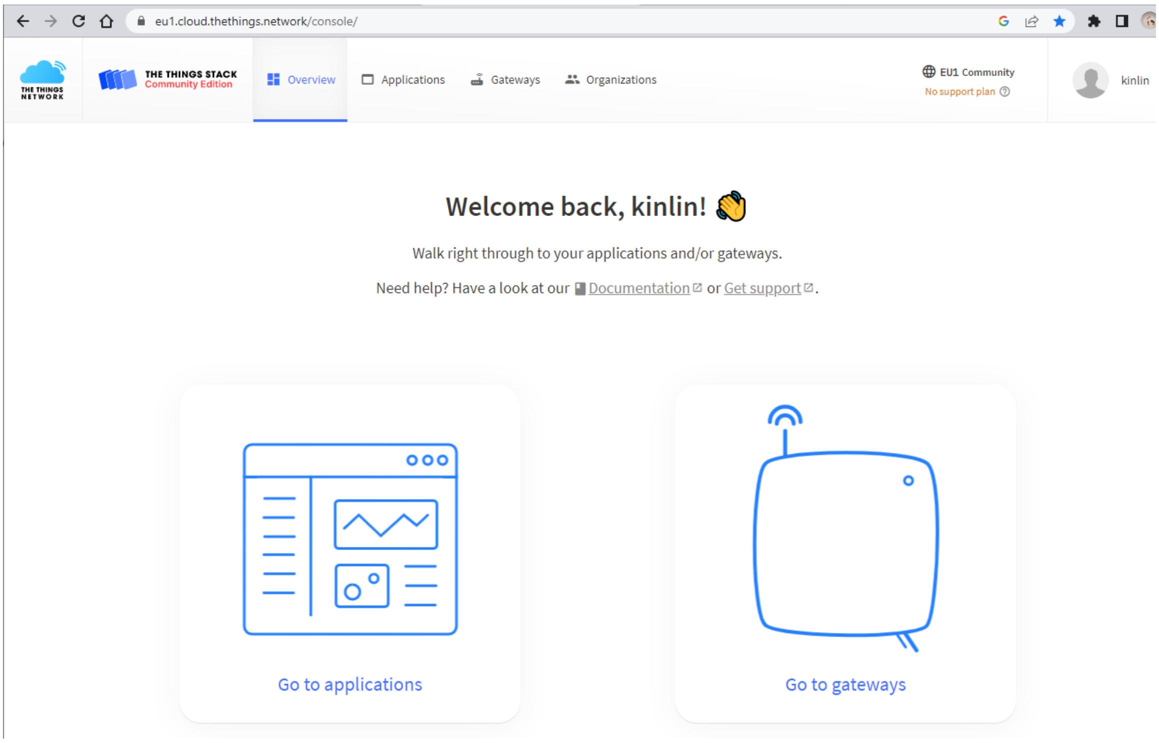
(The test case: Europe 1)



c. The console page

“Go to application” is for setting LoRa node and LoRa sensor.

“Go to gateways” is for setting LoRaWAN gateway.



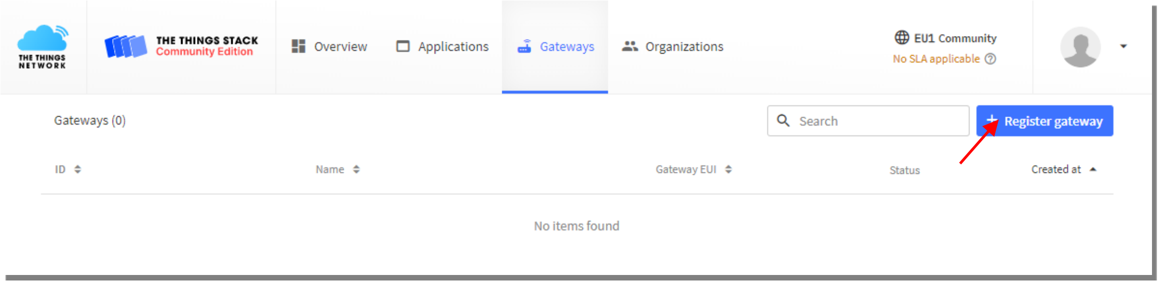
Welcome back, kinlin! 👋

Walk right through to your applications and/or gateways.

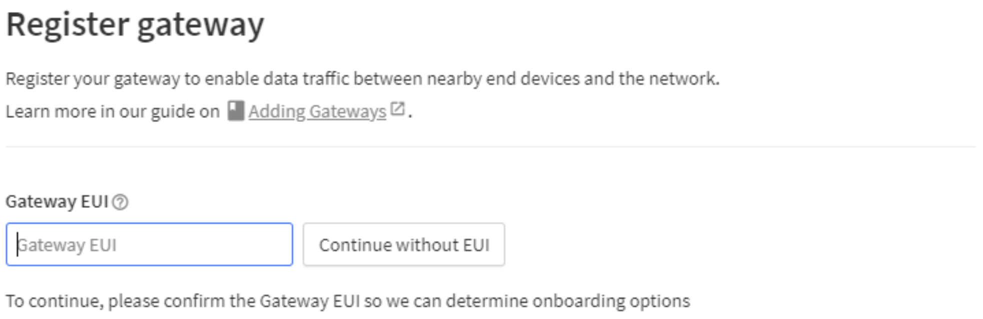
Need help? Have a look at our Documentation or Get support.

Register a gateway

1. Click “Register gateway”.



1. Input Gateway EUI



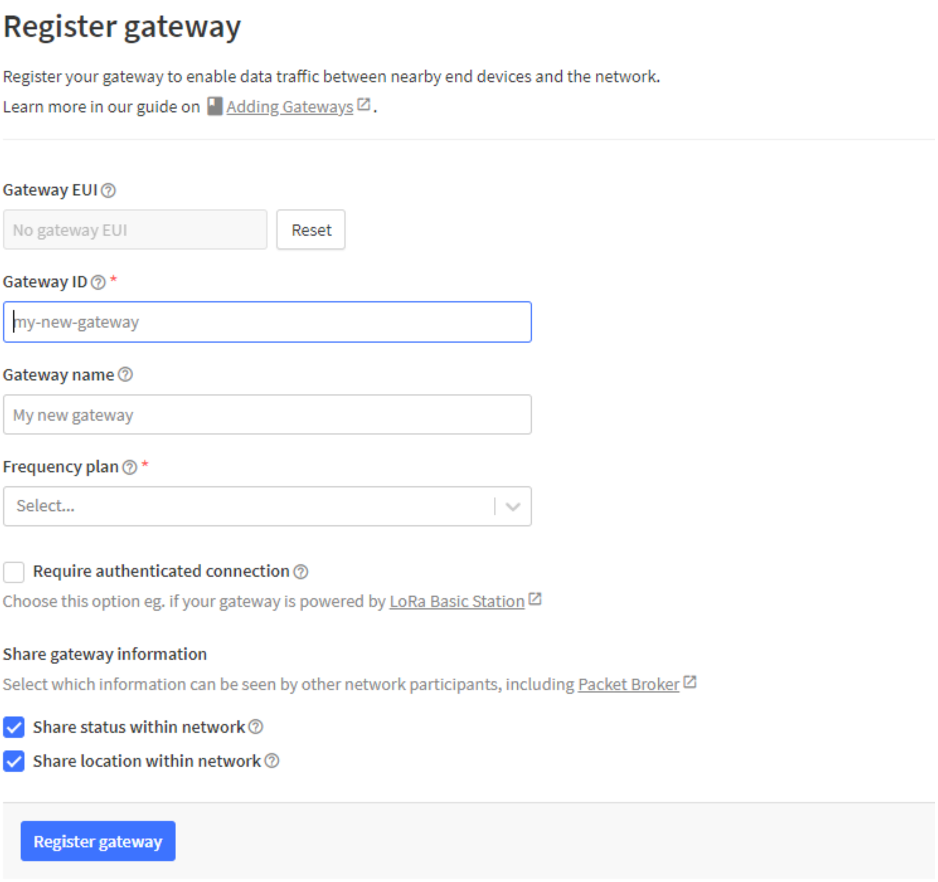
Register gateway

Register your gateway to enable data traffic between nearby end devices and the network.
Learn more in our guide on Adding Gateways.

To continue, please confirm the Gateway EUI so we can determine onboarding options

2. Input General settings

The Gateway ID has to be the same as the Gateway ID of LoRaWAN setting.



## Register gateway

Register your gateway to enable data traffic between nearby end devices and the network.
Learn more in our guide on Adding Gateways.

Gateway EUI: No gateway EUI

Gateway ID *: my-new-gateway

Gateway name: My new gateway

Frequency plan *: Select...

□ Require authenticated connection

Choose this option eg. if your gateway is powered by LoRa Basic Station

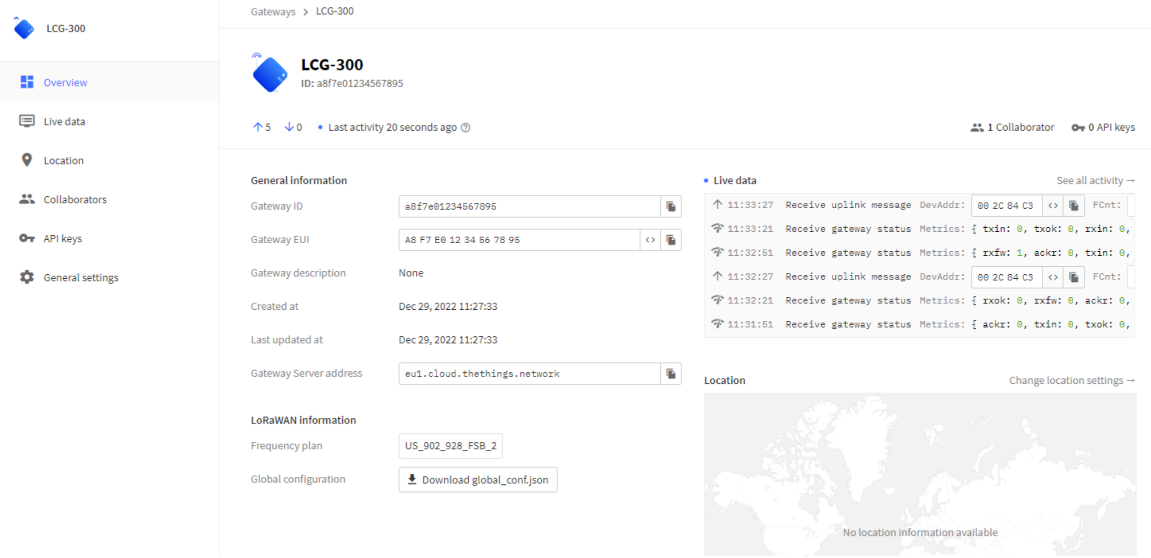
**Share gateway information**

Select which information can be seen by other network participants, including Packet Broker

☑ Share status within network

☑ Share location within network

3. After finishing the setting, TTN will keep updating the information of the gateway.



**LCG-300**
ID: a8f7e01234567895

↑5 ↓0 • Last activity 20 seconds ago

1 Collaborator 0 API keys

**General information**

| | |
|---|---|
| Gateway ID | a8f7e01234567895 |
| Gateway EUI | A8 F7 E0 12 34 56 78 95 |
| Gateway description | None |
| Created at | Dec 29, 2022 11:27:33 |
| Last updated at | Dec 29, 2022 11:27:33 |
| Gateway Server address | eu1.cloud.thethings.network |

**LoRaWAN information**

| | |
|---|---|
| Frequency plan | US_902_928_FSB_2 |
| Global configuration | Download global_conf.json |

• Live data

```
↑ 11:33:27  Receive uplink message  DevAddr: 00 2C 84 C3  FCnt:
  11:33:21  Receive gateway status  Metrics: { txin: 0, txok: 0, rxin: 0,
  11:32:51  Receive gateway status  Metrics: { rxfw: 1, ackr: 0, txin: 0,
↑ 11:32:27  Receive uplink message  DevAddr: 00 2C 84 C3  FCnt:
  11:32:21  Receive gateway status  Metrics: { rxok: 0, rxfw: 0, ackr: 0,
  11:31:51  Receive gateway status  Metrics: { ackr: 0, txin: 0, txok: 0,
```

Location

No location information available

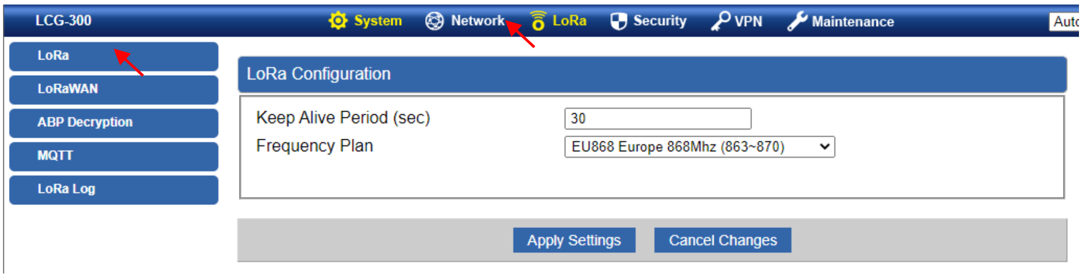
# Setting Up to Connect with Built-in ABP Decoder

**The Setting Up of LCG-300 series**

1. LoRa Setting

   a. Open browser and log in to the Web GUI of LCG-300 series.

   b. Click **LoRa** under the main menu and **LoRa** on the function menu.

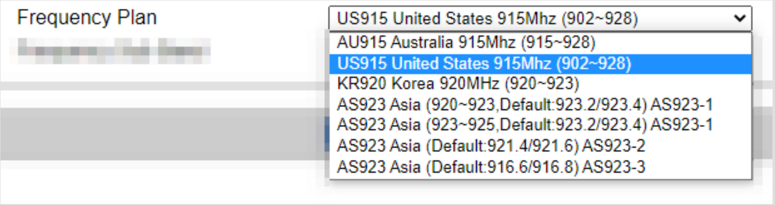
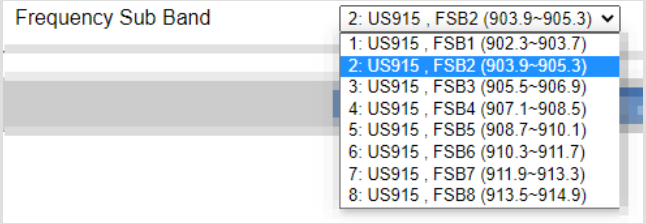
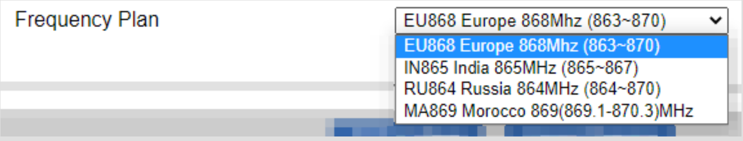


Keep Alive Period (sec): 30

Frequency Plan: EU868 Europe 868Mhz (863~870)

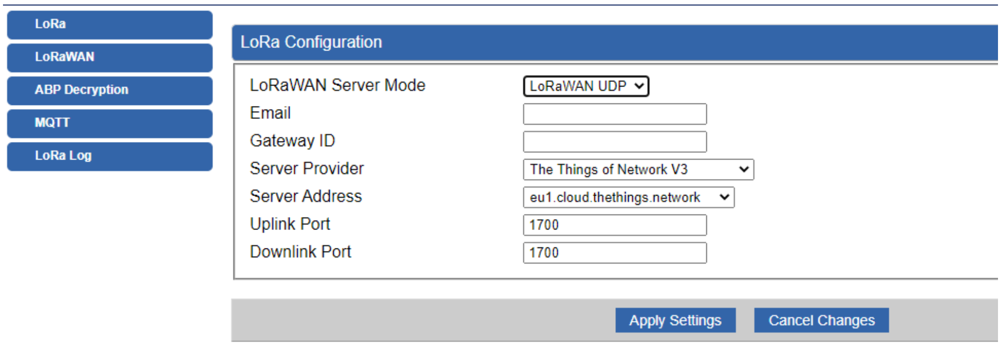
   c. Select the **Frequency Plan** for your local area. Some frequency bands support **Frequency Sub Band**.

   (In this case [LCG-300-US], select "US915" for frequency band and "US915 and FSB2" for frequency sub band.)

| | |
|---|---|
| LCG-300<br>series-US |  Frequency Plan<br>US915 United States 915Mhz (902~928)<br>AU915 Australia 915Mhz (915~928)<br>US915 United States 915Mhz (902~928)<br>KR920 Korea 920MHz (920~923)<br>AS923 Asia (920~923,Default:923.2/923.4) AS923-1<br>AS923 Asia (923~925,Default:923.2/923.4) AS923-1<br>AS923 Asia (Default:921.4/921.6) AS923-2<br>AS923 Asia (Default:916.6/916.8) AS923-3<br> Frequency Sub Band<br>2: US915 , FSB2 (903.9~905.3)<br>1: US915 , FSB1 (902.3~903.7)<br>2: US915 , FSB2 (903.9~905.3)<br>3: US915 , FSB3 (905.5~906.9)<br>4: US915 , FSB4 (907.1~908.5)<br>5: US915 , FSB5 (908.7~910.1)<br>6: US915 , FSB6 (910.3~911.7)<br>7: US915 , FSB7 (911.9~913.3)<br>8: US915 , FSB8 (913.5~914.9) |
| LCG-300<br>series-EU |  Frequency Plan<br>EU868 Europe 868Mhz (863~870)<br>EU868 Europe 868Mhz (863~870)<br>IN865 India 865MHz (865~867)<br>RU864 Russia 864MHz (864~870)<br>MA869 Morocco 869(869.1-870.3)MHz |

2. LoRaWAN Setting

Click **LoRaWAN** and key-in data.

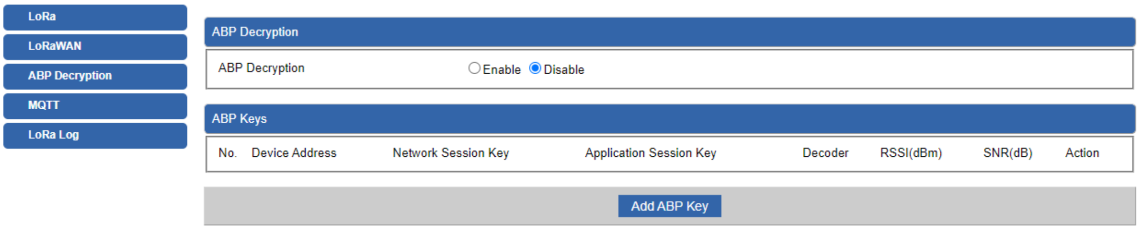


LoRa Configuration

| | |
|---|---|
| LoRaWAN Server Mode | LoRaWAN UDP |
| Email | |
| Gateway ID | |
| Server Provider | The Things of Network V3 |
| Server Address | eu1.cloud.thethings.network |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

| | |
|---|---|
| LoRaWAN Server Mode | **LoRaWAN UDP** |
| Email | kinlin.planet@gmail.com |
| Gateway ID | a8f7e01234567895 |
| Server Provider | **Built-in ABP Decoder** |
| Uplink Port | 1700 |
| Downlink Port | 1700 |

3. ABP Decryption



ABP Decryption

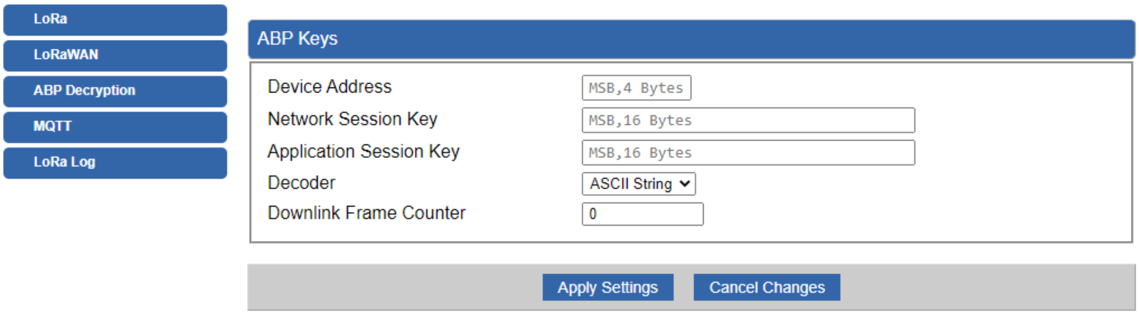
ABP Decryption ○ Enable ● Disable

ABP Keys

| No. | Device Address | Network Session Key | Application Session Key | Decoder | RSSI(dBm) | SNR(dB) | Action |
|---|---|---|---|---|---|---|---|

a. Click Enable.

b. Click the **Add ABP Key** button. Then input data which has to be the same as the settings of LoRa node/sensor.



ABP Keys

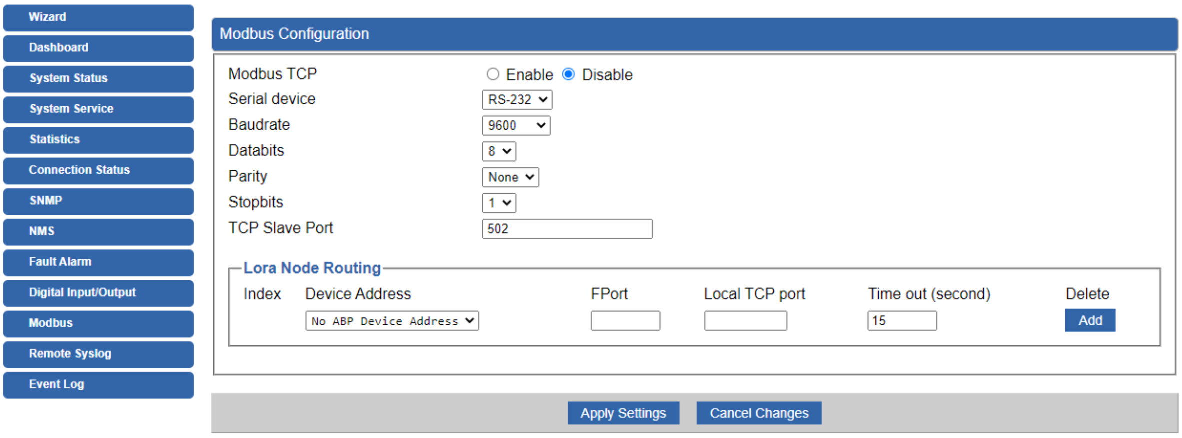
| | |
|---|---|
| Device Address | MSB,4 Bytes |
| Network Session Key | MSB,16 Bytes |
| Application Session Key | MSB,16 Bytes |
| Decoder | ASCII String |
| Downlink Frame Counter | 0 |

| | |
|---|---|
| Device Address | *B0508566 |
| Network Session Key | *A04106056144579AD82F86DF0EF42A2F |
| Application Session Key | *A4A197D52E8BFA3AC3DD4D1F303CF54F |
| Decoder | ACSII String |
| Downlink Frame Counter | *0 |

***The data has to be the same as the LoRa node/sensor.**

4. Modbus configuration

a. Click “**System**” under the main menu and “**Modbus**” on the function menu.



Modbus Configuration

Modbus TCP ○ Enable ● Disable

Serial device RS-232

Baudrate 9600

Databits 8

Parity None

Stopbits 1

TCP Slave Port 502

Lora Node Routing

| Index | Device Address | FPort | Local TCP port | Time out (second) | Delete |
|---|---|---|---|---|---|
| | No ABP Device Address | | | 15 | Add |

b. Click Enable and set “**Serial device**” to be RS-485.

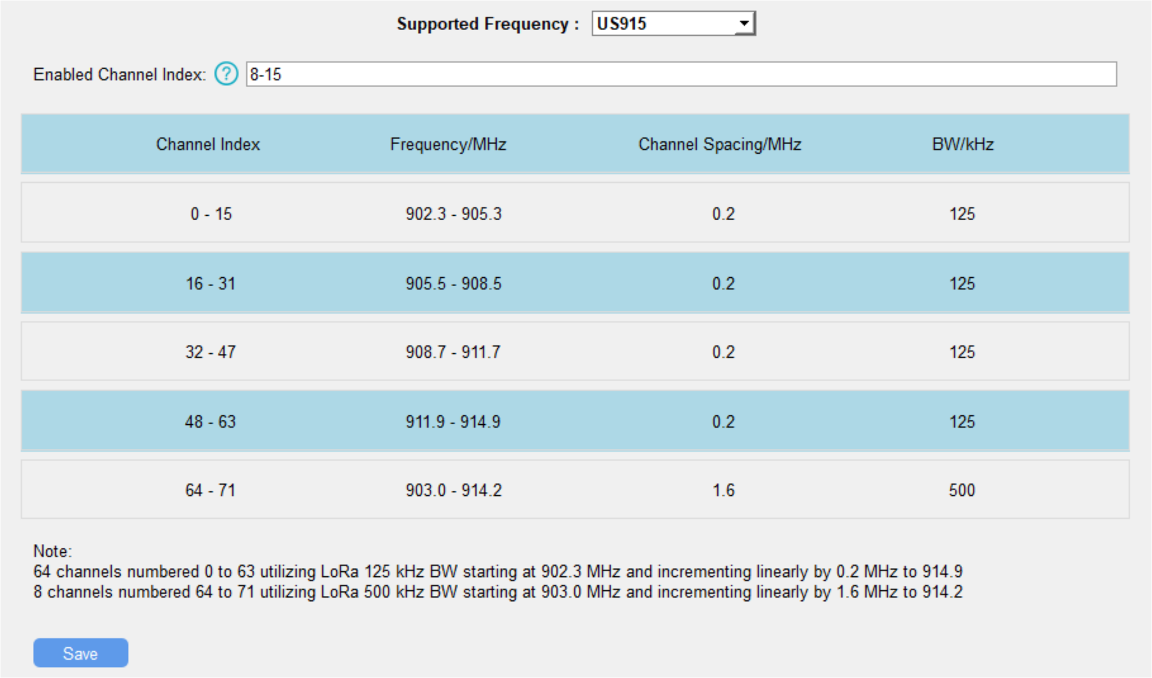
c. Input LoRa devices data in LoRa Node Routing.

| | |
|---|---|
| Device Address | B0508566 |
| FPort | 2 |
| Local TCP port | 503 |
| Time out (second) | 15 (default setting) |

d. Click Apply Settings to save the setting.

### The Setting Up of LoRa Node

1. Launch LoRa node/sensor utility.
2. Go to LoRaWAN Settings, and set frequency of the LoRa node.



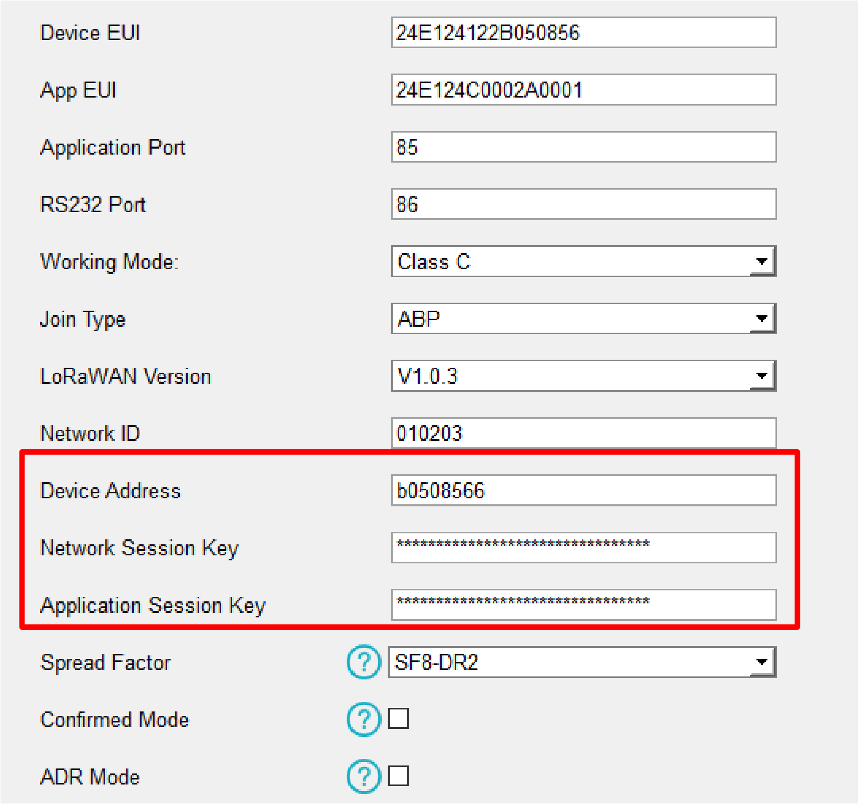
Supported Frequency : US915

Enabled Channel Index: 8-15

| Channel Index | Frequency/MHz | Channel Spacing/MHz | BW/kHz |
|---|---|---|---|
| 0 - 15 | 902.3 - 905.3 | 0.2 | 125 |
| 16 - 31 | 905.5 - 908.5 | 0.2 | 125 |
| 32 - 47 | 908.7 - 911.7 | 0.2 | 125 |
| 48 - 63 | 911.9 - 914.9 | 0.2 | 125 |
| 64 - 71 | 903.0 - 914.2 | 1.6 | 500 |

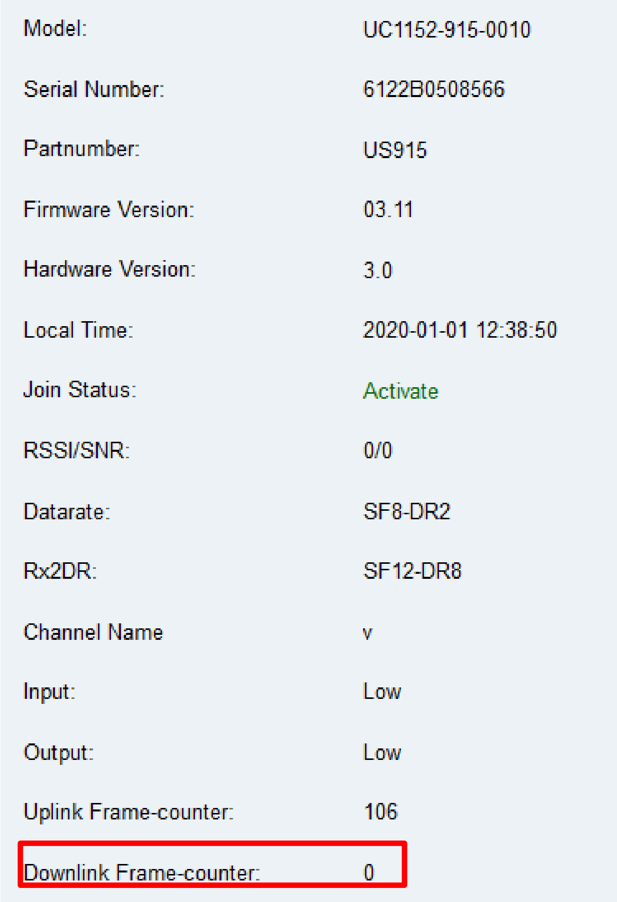
Note:
64 channels numbered 0 to 63 utilizing LoRa 125 kHz BW starting at 902.3 MHz and incrementing linearly by 0.2 MHz to 914.9
8 channels numbered 64 to 71 utilizing LoRa 500 kHz BW starting at 903.0 MHz and incrementing linearly by 1.6 MHz to 914.2

3. Set Device Address, Network Session Key and Application Session Key



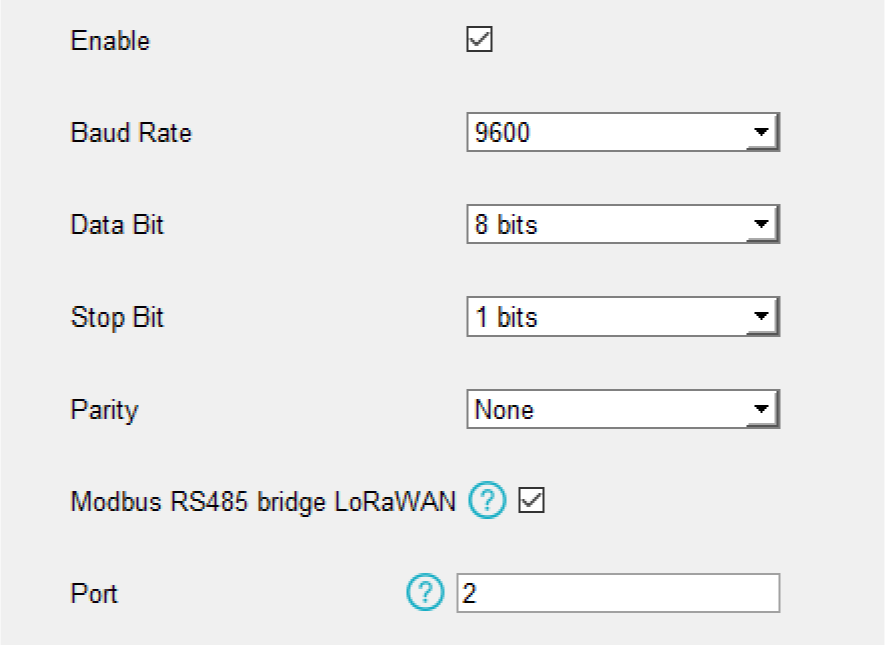
| | |
|---|---|
| Device EUI | 24E124122B050856 |
| App EUI | 24E124C0002A0001 |
| Application Port | 85 |
| RS232 Port | 86 |
| Working Mode: | Class C |
| Join Type | ABP |
| LoRaWAN Version | V1.0.3 |
| Network ID | 010203 |
| Device Address | b0508566 |
| Network Session Key | ******************************** |
| Application Session Key | ******************************** |
| Spread Factor | SF8-DR2 |
| Confirmed Mode | ☐ |
| ADR Mode | ☐ |

4. Check the data of **Downlink Frame-counter.**



| | |
|---|---|
| Model: | UC1152-915-0010 |
| Serial Number: | 6122B0508566 |
| Partnumber: | US915 |
| Firmware Version: | 03.11 |
| Hardware Version: | 3.0 |
| Local Time: | 2020-01-01 12:38:50 |
| Join Status: | Activate |
| RSSI/SNR: | 0/0 |
| Datarate: | SF8-DR2 |
| Rx2DR: | SF12-DR8 |
| Channel Name | v |
| Input: | Low |
| Output: | Low |
| Uplink Frame-counter: | 106 |
| Downlink Frame-counter: | 0 |

5. Enable the RS-485 setting, check the item of Modbus RS485 bridge LoRaWAN and set Port. (The Port must be the same as the Port of Modbus setting in LCG-300.)



| | |
|---|---|
| Enable | ☑ |
| Baud Rate | 9600 |
| Data Bit | 8 bits |
| Stop Bit | 1 bits |
| Parity | None |
| Modbus RS485 bridge LoRaWAN ? | ☑ |
| Port ? | 2 |