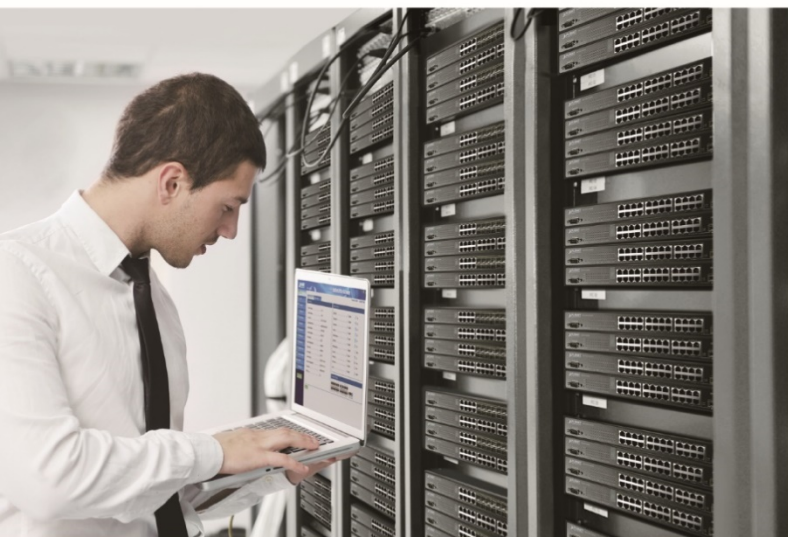


User's Manual

Industrial LoRaWAN Gateway

▶ LCG-300 Series



Copyright

Copyright (C) 2022 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

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.

FCC Compliance Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

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

CE mark Warning



This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

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-300, LCG-300W and LCG-300-NR

Rev.: 1.1 (Dec., 2022)

Part No. EM-LCG-300 series_v1.1

Table of Contents

Chapter 1. Product Introduction.....	7
1.1 Package Contents.....	7
1.2 Overview	8
1.3 Features	12
1.4 Product Specifications	14
Chapter 2. Hardware Introduction	21
2.1 Physical Descriptions	21
2.2 Hardware Installation	24
2.2.1 LoRa Antenna Installation	24
2.2.2 Wi-Fi Antenna Installation	24
2.2.3 5G NR Antenna Installation.....	25
2.2.4 Grounding the Device.....	28
2.2.5 Wiring the Fault Alarm Contact	28
Chapter 3. Preparation	29
3.1 Requirements.....	29
3.2 Setting TCP/IP on your PC	29
3.3 Planet Smart Discovery Utility.....	33
Chapter 4. Web-based Management	35
4.1 Introduction	35
4.2 Logging in to the LoRaWAN Gateway	35
4.3 Main Web Page.....	36
4.4 System	38
4.4.1 Setup Wizard	40
4.4.2 Dashboard	48
4.4.3 System Status.....	51
4.4.4 System Service.....	52
4.4.5 Statistics.....	53
4.4.6 Connection Status	54
4.4.7 SNMP.....	55
4.4.8 NMS	56
4.4.9 Fault Alarm.....	58
4.4.10 Digital Input / Output.....	59
4.4.11 Modbus	61
4.4.12 Remote Syslog	62

4.4.13	Event Log.....	62
4.5	Network.....	63
4.5.1	Priority.....	64
4.5.2	WAN.....	65
4.5.3	WAN Advanced.....	67
4.5.4	LAN Setup.....	68
4.5.5	Multi-Subnet.....	69
4.5.6	VLAN.....	69
4.5.7	UPnP.....	70
4.5.8	Routing.....	70
4.5.9	RIP.....	71
4.5.10	OSPF.....	72
4.5.11	IGMP.....	72
4.5.12	IPv6.....	73
4.5.13	DHCP.....	74
4.5.14	DDNS.....	76
4.5.15	MAC Address Clone.....	78
4.6	Cellular.....	79
4.6.1	LTE/NR Configuration.....	80
4.6.2	LTE/NR Advanced.....	81
4.6.3	LTE/NR Status.....	82
4.6.4	LTE/NR Statistics.....	83
4.6.5	GPS.....	83
4.6.6	SMS.....	84
4.7	LoRa 85	
4.7.1	LoRa.....	86
4.7.2	LoRaWAN.....	87
4.7.3	ABP Decryption.....	88
4.7.4	MQTT.....	89
4.7.5	LoRa Log.....	90
4.8	Security.....	91
4.8.1	Firewall.....	92
4.8.2	MAC Filtering.....	94
4.8.3	IP Filtering.....	95
4.8.4	Web Filtering.....	96
4.8.5	Port Forwarding.....	97
4.8.6	QoS.....	98
4.8.7	DMZ.....	99
4.9	VPN 101	
4.9.1	IPSec.....	102

4.9.2	IPsec Remote Server.....	105
4.9.3	GRE	105
4.9.4	PPTP Server	107
4.9.5	L2TP Server.....	109
4.9.6	SSL VPN.....	111
4.9.7	VPN Connection	112
4.10	Wireless	113
4.10.1	2.4G Wi-Fi.....	114
4.10.2	5G Wi-Fi.....	115
4.10.3	MAC ACL	116
4.10.4	Wi-Fi Advanced.....	117
4.10.5	Wi-Fi Statistics	118
4.10.6	Connection Status	119
4.11	Maintenance.....	120
4.11.1	Administrator.....	121
4.11.2	Date and Time	122
4.11.3	Saving/Restoring Configuration	123
4.11.4	Upgrading Firmware	124
4.11.5	Reboot / Reset.....	125
4.11.6	Auto Reboot.....	125
4.11.7	Diagnostics	126
Appendix A: DDNS Application		127
Appendix B: LoRaWAN Settings.....		128
	Setting Up to Connect with TTN (The Things Network).....	128
	Setting Up to Connect with Built-in ABP Decoder.....	133

Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial LoRaWAN Gateway, LCG-300 Series. The descriptions of these models are as follows:

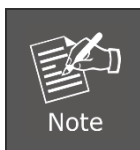
LCG-300	Industrial LoRaWAN Gateway with 5-Port 10/100/1000T
LCG-300W	Industrial LoRaWAN Wireless Gateway with 5-Port 10/100/1000T
LCG-300-NR	Industrial LoRaWAN + 5G NR Cellular Gateway with 5-Port 10/100/1000T

“LoRaWAN Gateway” mentioned in the manual refers to the above models.

1.1 Package Contents

The package should contain the following:

Model Name Item	LCG-300	LCG-300W	LCG-300-NR
Industrial LoRaWAN Gateway	1	1	1
Quick Installation Guide (QR code)	1	1	1
CloudViewer QIG	1	1	1
Wall-mount Kit	1	1	1
RJ45 Dust Cap	6	6	6
LoRa Antenna	1	1	1
LoRa Antenna Extender with Magnetic Base	1	1	1
Dual band Wi-Fi Antenna	--	2	--
Antenna Dust Cap	1	3	5
5G NR Antenna	--	--	4
5G NR Antenna Extender with Magnetic Base	--	--	4



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

1.2 Overview

Connect to LoRa Network with Excellent LoRaWAN Gateway

PLANET LCG-300 series is an industrial-grade LoRaWAN gateway with reliable connectivity for IoT deployments. With LoRaWAN protocol support, it helps to bridge LoRa wireless network to an IP network. The LoRa wireless allows sensors to transmit data over extremely long ranges with low power consumption. The LCG-300 series is fully compatible with LoRaWAN protocol and supports connection with up to 300 end-nodes. It also provides pre-configured standard LoRaWAN frequency bands for different countries. PLANET LCG-300 series is a best choice to help you to promote the implementation of AIoT network.



Comprehensive Features for Industrial Environment

The LCG-300 also features five Ethernet ports (4 LANs and 1 WAN), serial port (RS-485), and DI and DO interfaces designed in a compact yet rugged metal case. The LCG-300 also features several main categories across your industrial network deployments:

- SSL VPN and robust hybrid VPN (IPSec/PPTP/L2TP over IPSec)
- Cybersecurity and SPI firewall security protection
- Easy management with setup wizard, DHCP server and dashboard

LoRaWAN Compatibility

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. The LCG-300 is LoRaWAN compatible and make sure it works well with LoRa sensor without any problem.

LoRaWAN Compatibility

The LCG-300 Series is LoRaWAN compatible and make sure it works well with LoRa sensor without any problem. 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.

Ideal High-Availability VPN Security Router Solution for Industrial Environment

The LCG-300 series 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-300 series makes the connection secure, more flexible, and more capable.

Excellent Ability in Threat Defense

The LCG-300 series 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

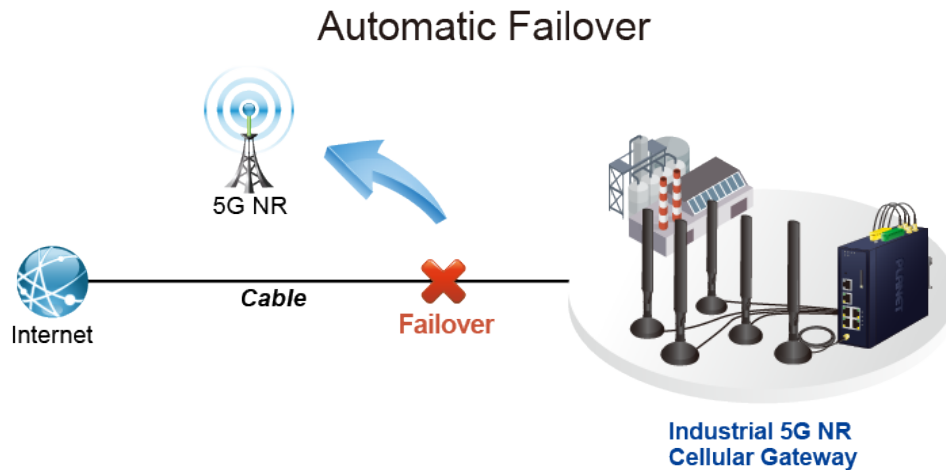
The cybersecurity feature included to protect the switch management in a mission-critical network virtually needs no effort and cost to install. For efficient management, the LCG-300 series is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the LCG-300 series offers an easy-to-use, platform independent management and configuration facility. The LCG-300 series supports SNMP and it can be managed via any management software based on the standard SNMP protocol.

Maximizing Work Efficiency with PLANET SD-WAN Gateway

PLANET LCG-300 series incorporated in SD-WAN (software-defined wide area network) function can greatly increase WAN optimization for multiple WAN links to be managed. 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.

Automatic Failover between 5G NR and Dual WAN (For LCG-300-NR only)

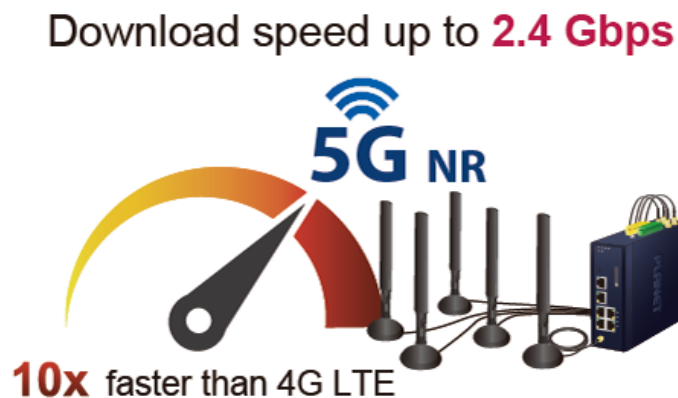
With 5G NR, and dual Gigabyte Ethernet WAN interfaces, the LCG-300-NR ensures Internet connectivity by featuring failover functionality between 5G NR and dual WAN. It provides flexibility to set priority for 5G NR or dual WAN connection. When the main WAN interface fails, the secondary WAN interface will automatically back up the connection to ensure always-on connectivity.



Ultra-Fast Speed 4G/5G Network* (For LCG-300-NR only)

The LCG-300-NR supports 5G NR DL (downlink) speeds higher than 2.4 Gbps and 4G LTE DL speeds of up to 1 Gbps. The 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 (For LCG-300-NR only)

The LCG-300-NR is equipped with (global positioning system) feature. It adapts 5G-NR technology to incorporate multiple global navigation systems (GPS/GLONASS/BeiDou/Galileo/QZSS). It helps to position location of cellular gateway based on a network of satellites that continuously transmits necessary data. More signals transmitted from more satellites can triangulate its location on the ground, meaning any location can be easily tracked.

Wireless 11ax Brings Excellent Data Link Speed (For LCG-300W only)

The LCG-300W is designed with high power amplifier and 2 highly-sensitive antennas which provide stronger signal and excellent coverage even in the wide-ranging or bad environment. With adjustable transmit power option, the administrator can flexibly reduce or increase the output power for various environments, thus reducing interference to achieve maximum performance. Equipped with the next-generation Wi-Fi 6 (802.11ax) wireless network standard, the total bandwidth reaches **1800Mbps**, and the 2-stream transmission technology improves the transmission efficiency of multiple devices, making AR/VR/IoT applications smoother. The IEEE 802.11ax also optimizes MU-MIMO (Multi-User MIMO) mechanism to serve multiple devices simultaneously.

1.3 Features

Key Features

- Supports EU868, US915, AS923 (Sub 1G)
- 8 programmable parallel demodulation paths
- 2 x DI/DO and 1 serial port (RS485) for Modbus applications
- SSL VPN and robust hybrid VPN (IPSec/PPTP/L2TP over IPSec)
- Stateful packet inspection (SPI) firewall and content filtering
- Blocks DoS/DDOS attack, port range forwarding
- Planet NMS controller system and CloudViewer app supported
- -45 to 75 degrees C operating temperature; DIN-rail and fanless designs

Hardware

- **4 x 10/100/1000BASE-T** RJ45 LAN ports, auto-negotiation, auto MDI/MDI-X
- **1 x 10/100/1000BASE-T** RJ45 WAN port, auto-negotiation, auto MDI/MDI-X
- **1 x** LoRa antenna
- **1 x** serial console port (RS485)
- **1 x** reset button

LoRa Interface

- Supports EU868/AU915/US915/AS923(Sub 1G)
- 8 programmable parallel demodulation paths

RF Interface Characteristics (LCG-300W only)

- Features 2.4GHz (802.11b/g/n/ax) and 5GHz (802.11a/n/ac/ax) dual band for carrying high load traffic
- 2T2R MIMO technology for enhanced throughput and coverage
- Provides multiple adjustable transmit power control
- High speed up to 1.8Gbps (600Mbps for 2.4GHz or 1200Mbps for 5GHz) wireless data rate

Cellular Interface (LCG-300-NR only)

- 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

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 ALGs (Application Layer Gateway)
- Blocks SYN/ICMP Flooding

VPN Features

- IPSec/Remote Server (Net-to-Net, Host-to-Net), GRE, PPTP Server, L2TP Server, SSL Server/Client (Open VPN)
- Max. Connection Tunnel Entries: 60 VPN tunnels,
- Encryption methods: DES, 3DES, AES, AES-128/192/256
- Authentication methods: MD5, SHA-1, SHA-256, SHA-384, SHA-512

Networking

- Outbound load balancing
- Failover for dual-WAN
- Static IP/PPPoE/DHCP client for WAN
- 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

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 CloudViewer app for real-time monitoring

1.4 Product Specifications

LCG-300W, LCG-300

Models	LCG-300W	LCG-300
Hardware Specifications		
Copper Ports	5 10/100/1000BASE-T RJ45 Ethernet ports including 3 LAN ports (Ports 1 to 3) 1 LAN/WAN port (Port 4) 1 WAN port (Port 5)	
Serial Interface	RJ45 serial port	
Cellular Antenna	2 dBi external antennas with SMA connectors for LoRa	
DI & DO Interfaces	2 Digital Input (DI): Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input Load to 24V DC, 10mA max. 2 Digital Output (DO): Open collector to 24V DC, 100mA max.	
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2	
Reset Button	< 5 sec: System reboot > 5 sec: Factory default	
Enclosure	IP30 metal case	
Installation	DIN rail, desktop, wall-mounting	
Dimensions	50 x 135 x 135 mm (W x D x H)	
Weight	0.9 kg	0.9 kg
Power Requirements	9~54V DC, 1.3A	9~54V DC, 1.3A
Power Consumption	12.5 W / 42.7 BTU	8 watts/ 27.3 BTU
LED Indicators	<p>System: P1 (Green), P2 (Green) Alarm (Red), I/O (Red)</p> <p>Ethernet Interfaces (Ports 1-4 and WAN Port): 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber)</p> <p>LoRa: LoRa (Green)</p> <p>Wi-Fi: 2.4G(Green), 5G(Green)</p>	<p>System: P1 (Green), P2 (Green) Alarm (Red), I/O (Red)</p> <p>Ethernet Interfaces (Ports 1-4 and WAN Port): 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber)</p> <p>LoRa : LoRa (Green)</p>

LoRaWAN			
Frequency Band	EU version: 863~870MHZ US version: 902~928MH IN865/EU868/RU864/US915/AU915/KR920/AS923		
Receiving Sensitivity	-142.5dBm		
Output Power	27dBm Max.		
Wireless			
Standard	IEEE 802.11a/n/ac/ax 5GHz IEEE 802.11g/b/n/ax 2.4GHz	--	
Band Mode	2.4G & 5G concurrent mode		
Frequency Range	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz	--
	5GHz	5.15GHz ~5.875GHz	--
Operating Channels	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13	--
	5GHz	<u>America FCC:</u> Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140 <u>Europe ETSI:</u> Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.	--
Channel Width	20MHz, 40MHz, 80MHz		--
Data Transmission Rates	Transmit: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz *The estimated transmission distance is based on the theory.		--

	The actual distance will vary in different environments.	
Transmission Power	11b: 23dbm+/- 1.5dbm @11Mbps 11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20 17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS11	--
Encryption Security	WEP (64/128-bit) encryption security WPA / WPA2 (TKIP/AES) WPA-PSK / WPA2-PSK (TKIP/AES) / WPA3-PSK (TKIP/AES) 802.1x Authenticator	--
Wireless Advanced	Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering	--
Advanced Functions		
VPN	<ul style="list-style-type: none"> ■ IPsec/Remote Server (Net-to-Net, Host-to-Net) ■ GRE ■ PPTP Server ■ L2TP Server ■ SSL Server/Client (Open VPN) 	
VPN Tunnels	Max. 60	
VPN Throughput	Max. 100Mbps	
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting	
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm	
Management		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility and NMS controller supported	
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3	
System Log	System Event Log	

Others	Setup wizard Dashboard System status/service Statistics Connection status Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment	
Operating	Temperature: -40 ~ 75 degrees C Relative humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -40 ~ 85 degrees C Relative humidity: 5 ~ 90% (non-condensing)

LCG-300-NR

Product	LCG-300-NR
Hardware Specifications	
Ethernet	5 10/100/1000BASE-T RJ45 Ethernet ports including -3 LAN ports (Ports 1 to 3) -1 LAN/WAN port (Port 4) -1 WAN port (Port 5)
Serial Interface	RJ45 type RS485 for Modbus TCP
Cellular Antenna	5 dBi external antennas with SMA connectors for 5G-NR
SIM Interface	1 SIM card slot with mini SIM card tray
LoRa Antenna	2 dBi external antennas with SMA connectors for LoRa
DI & DO Interfaces	2 Digital Input (DI): Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input Load to 24V DC, 10mA max. 2 Digital Output (DO): Open collector to 24V DC, 100mA max.
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
Enclosure	IP30 metal case

Installation	DIN-rail, desktop, wall-mounting
LED Indicators	<p>System: P1, P2, LoRa, SIM (Green) Alarm, I/O (Red)</p> <p>Interfaces (Ports 1-4 and WAN Port): 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber)</p> <p>Cellular signal: 4 levels (Green)</p>
Dimensions (W x D x H)	50 x 135 x 135 mm
Weight	924g
Power Requirements – DC	9~54V DC, 1.5A Max.
Power Consumption	Max. 3.9 watts/13.2 BTU (No Loading) Max. 11.6 watts/39.5 BTU (Full loading)
LoRaWAN	
Frequency Band	LCG-300-NR-EU: 863~870MHz (IN865/EU868/RU864) LCG-300-NR-US: 902~928MHz (US915/AU915/KR920/AS923)
Receiving Sensitivity	-142.5dBm
Output Power	27dBm Max.
Multi Band Supports	
5G SUB6 BANDS	<p>NSA: n1/n2/n3/n5/n7/n8/n12/n13/n14/n18/n20/n25/n28/n29/n30/n38/n40/n41/n48/n66/n70/n71/n75/n76/n77/n78/n79</p> <p>SA: n1/n2/n3/n5/n7/n8/n12/n13/n14/n18/n20/n25/n28/n29/n30/n38/n40/n41/n48/n66/n70/n71/n75/n76/n77/n78/n79</p>
LTE BANDS	<p>FDD: B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29/B30/B32/B66/B71</p> <p>TDD: B34/B38/B39/B40/B41/B42/B43/B48</p> <p>LAA: B46</p>
UMTS BANDS	<p>FDD: B1/B2/B8/B4/B5/B19 MAX DL SPEED: DL3.4Gbps; UL 550 Mbps GNSS: GPS/ GLONASS/ BDS/ Galileo/ QZSS</p> <p>TDD: MAX DL SPEED DL 2.4 Gbps; UL 900 Mbps</p>
WCDMA	B1/B2/B3/B4/B5/B8
GNSS	GPS L1+L5 dual bands/GLONASS/BeiDou/Galileo/QZSS
Data Transmission Throughput	2.4Gbps (DL)/500Mbps (UL) for NR 1Gbps (DL)/200Mbps (UL) for LTE

	42Mbps (DL)/5.76Mbps (UL) for HSPA+
Security Service	
Firewall Security	Cybersecurity SSL (HTTPS) Inspection Stateful Packet Inspection (SPI) Blocks DoS/DDoS attack
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN 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. 900Mbps
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,
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control
Advanced Functions	
VPN Function	IPSec/Remote Server (Net-to-Net, Host-to-Net) GRE PPTP Server L2TP Server SSL Server/Client (Open VPN)
VPN Tunnels	Max. 60
VPN Throughput	Max. 108Mbps
Encryption Methods	DES, 3DES, AES or AES-128/192/256 encrypting
Authentication Methods	MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm

Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility/UNI-NMS supported
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System status/service Statistics Connection status Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC
Environment	
Operating	Temperature: -40 ~ 75 degrees C Relative humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -40 ~ 85 degrees C Relative humidity: 5 ~ 90% (non-condensing)

Chapter 2. Hardware Introduction

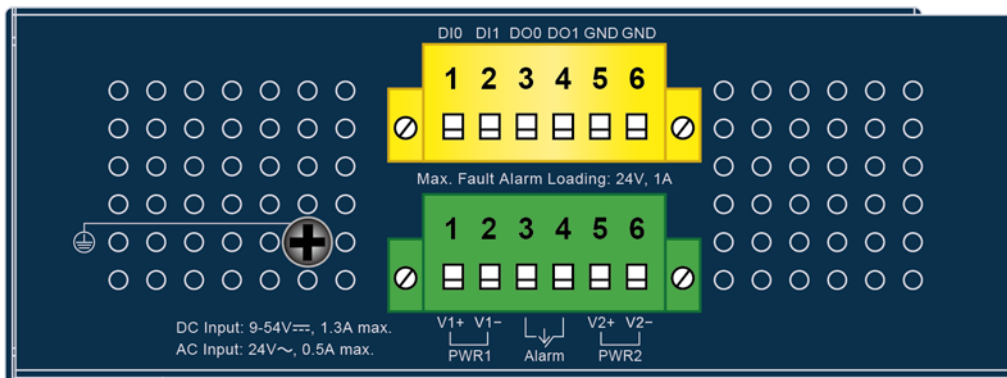
2.1 Physical Descriptions

Front View

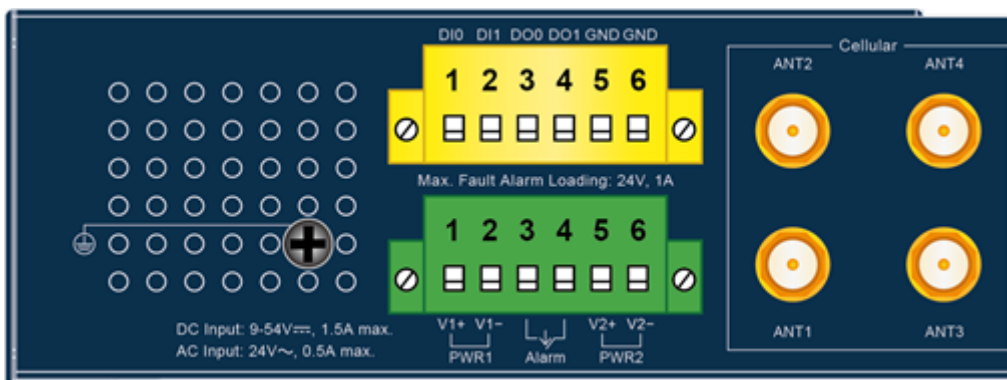


Top View

LCG-300, LCG-300W



LCG-300-NR



LED Definition:

■ System

LED	Color	Function
P1	Green	Lights to indicate DC power input 1 has power.
P2	Green	Lights to indicate DC power input 2 has power.
Alarm	Red	Lights to indicate that power or port has failed.
I/O	Red	Lights to indicate that power or port has failed or DI has event.
LoRa	Green	Lights to indicate the LoRaWAN is enabled successfully.
2.4G	Green	Lights up when 2.4G Wi-Fi service is enabled (LCG-300W only).
5G	Green	Lights up when 5G Wi-Fi service is enabled (LCG-300W only).
SIM	Green	Indicates SIM is connecting successfully (LCG-300-NR only).

■ LAN Per 10/100/1000Mbps Port (Ports 1 to 4)

LED	Color	Function	
1000 LNK/ACT	Green	Lights:	To indicate that the port is operating at 1000Mbps.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	Amber	Lights:	To indicate that the port is operating at 10/100Mbps.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ WAN Per 10/100/1000Mbps Port (Port 5)

LED	Color	Function	
1000 LNK/ACT	Green	Lights:	To indicate that the port is operating at 1000Mbps.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	Amber	Lights:	To indicate that the port is operating at 10/100Mbps.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ Cellular Signal (LCG-300-NR only)

LED	Color	Function	
Cellular Signal (High)	Green	Lights:	Indicates the signal is normal or high.
Cellular Signal (Low)	Green	Lights:	Indicates the signal is low.

2.2 Hardware Installation

Refer to the illustration and follow the simple steps below to quickly install your **LoRaWAN Gateway**.

2.2.1 LoRa Antenna Installation

Step 1: Connect LoRa antennas to the LoRa antenna extension.

Step 2: Fasten the LoRa antenna extensions to the connectors.



2.2.2 Wi-Fi Antenna Installation

(For LCG-300W Only)

Step 1: Fasten the two dual-band antennas to the antenna connectors on the front panel of the LoRaWAN Gateway.

Step 2: You can bend the antennas to fit your actual needs.



2.2.3 5G NR Antenna Installation

(For LCG-300-NR Only)

Step 1: Connect 5G NR antennas to the 5G NR antenna extender.

Step 2: Fasten the 5G NR antenna extenders to the connectors. Z



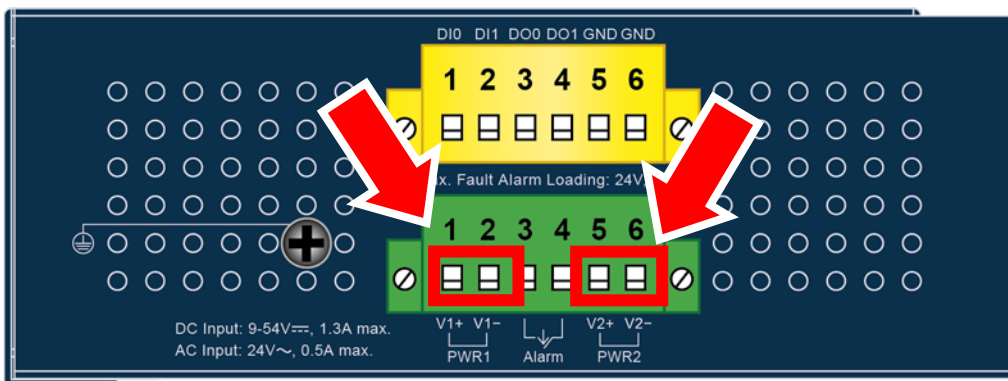
Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of LoRaWAN Gateway is used for two DC redundant power inputs. Please follow the steps below to insert the power wire.

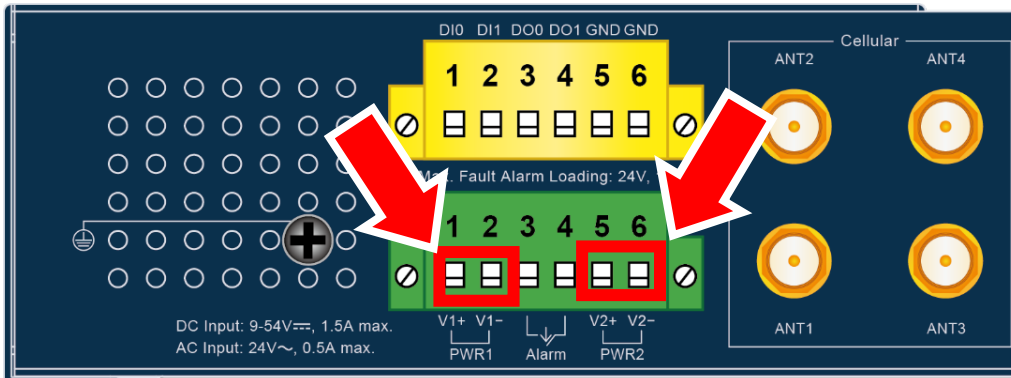


When performing any of the procedures like inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

1. Insert positive and negative DC power wires into contacts 1 and 2 for POWER 1, or 5 and 6 for POWER 2.



LCG-300/LCG-300W



LCG-300-NR



Please make sure the input voltage is under the specification of the LoRaWAN Gateway.

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



1	2	3	4	5	6
Power 1		Alarm		Power 2	
+	-			+	-



The wire gauge for the terminal block should be in the range between 12 and 24 AWG.

CAUTION

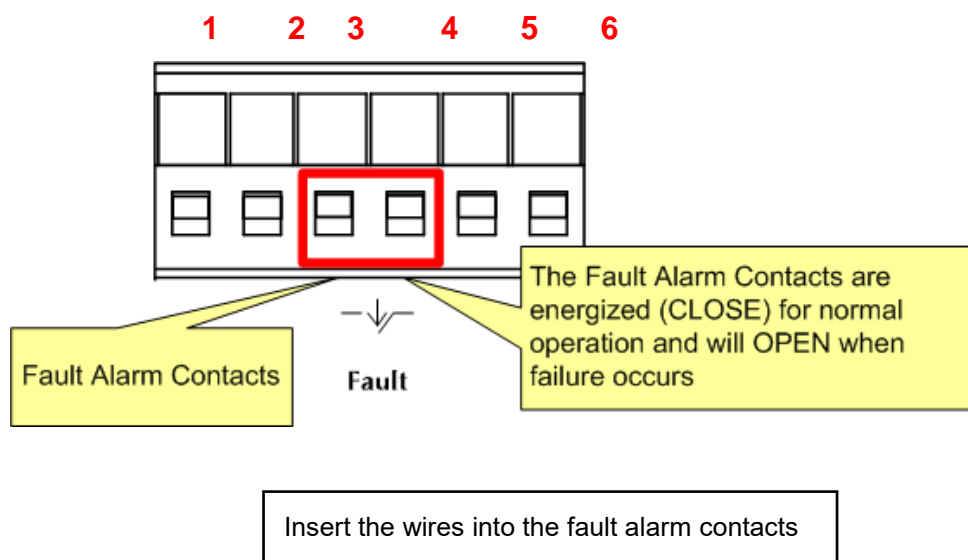
PWR1 and PWR2 must provide the **same DC voltage** while operating with dual power input.

2.2.4 Grounding the Device

User **MUST** complete grounding wired with the device; otherwise, a sudden lightning could cause fatal damage to the device. EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

2.2.5 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the LoRaWAN Gateway will detect the fault status of the power failure or port failure, and then will form an open circuit. The following illustration shows an application example for wiring the fault alarm contacts



1. The wire gauge for the terminal block should be in the range between 12 and 24 AWG.
2. Alarm relay circuit accepts up to 24V (max.) and 1A current.

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.
3. Recommended web browsers: Edge / Firefox / 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 on. 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

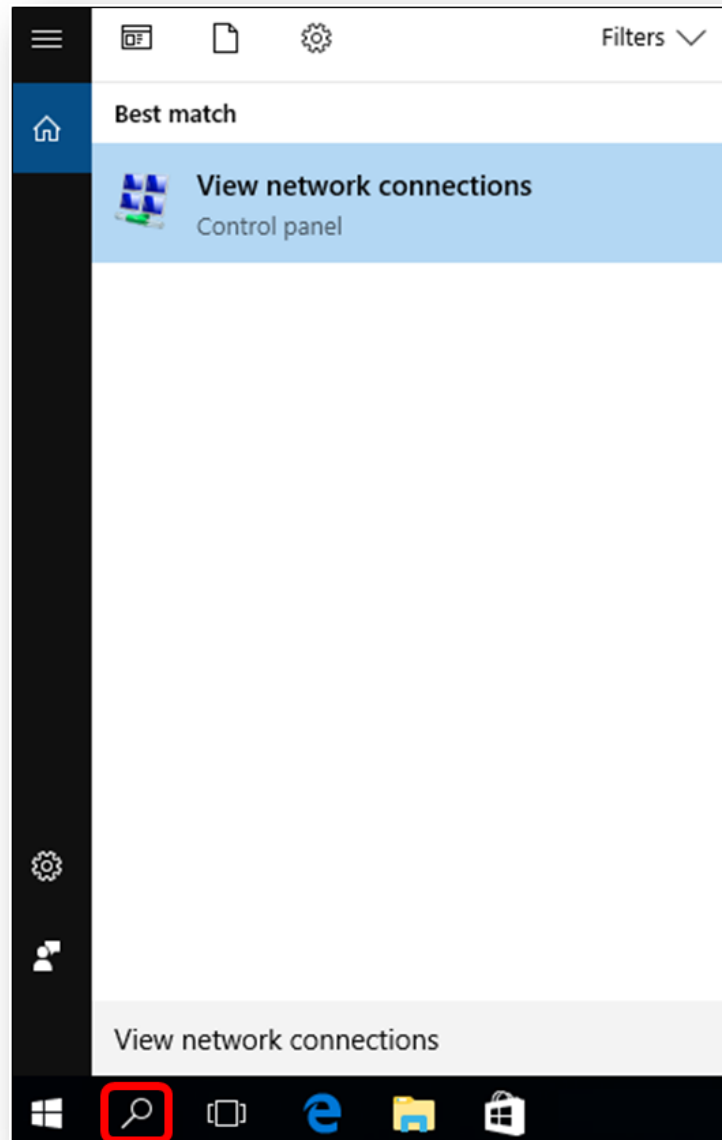
Please refer to the following to set the IP address of the connected PC.

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

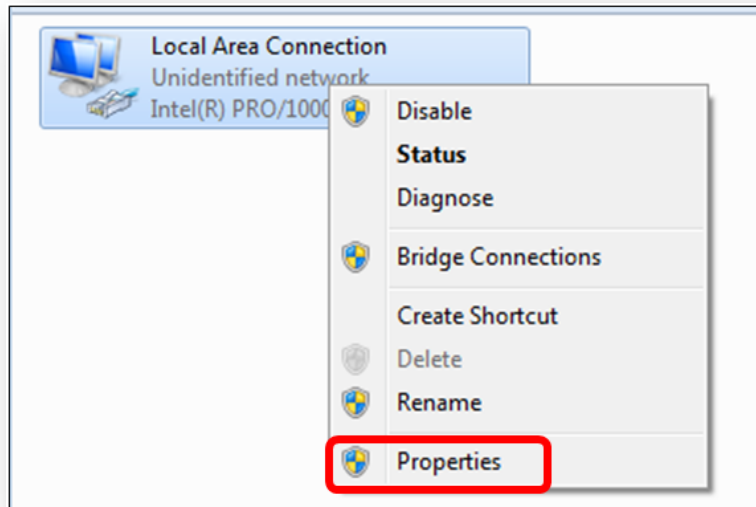
Windows 10

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

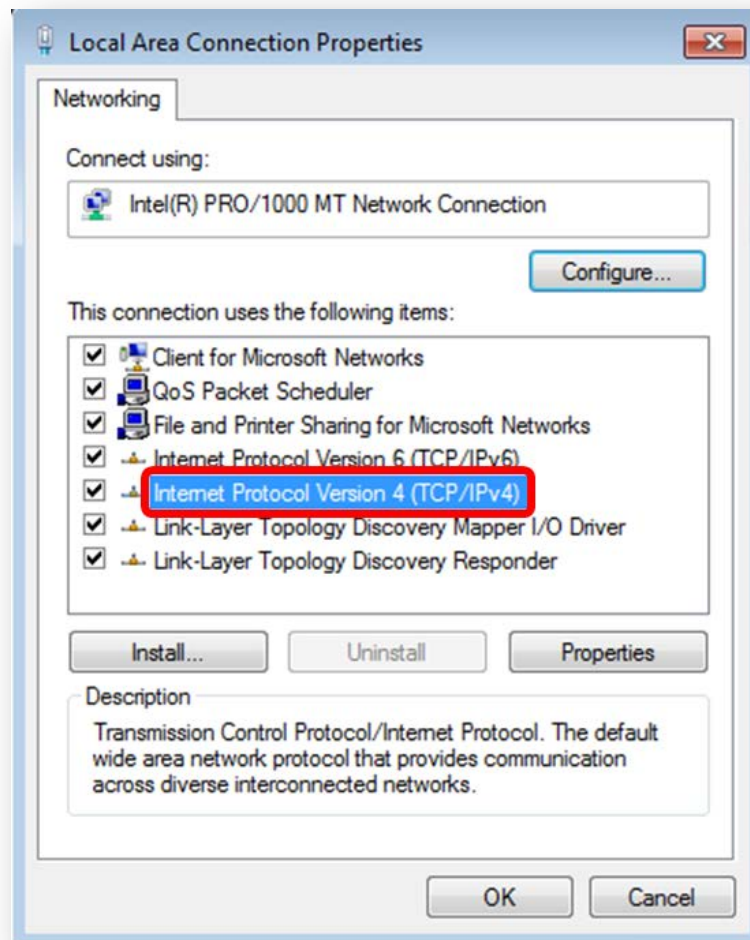
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



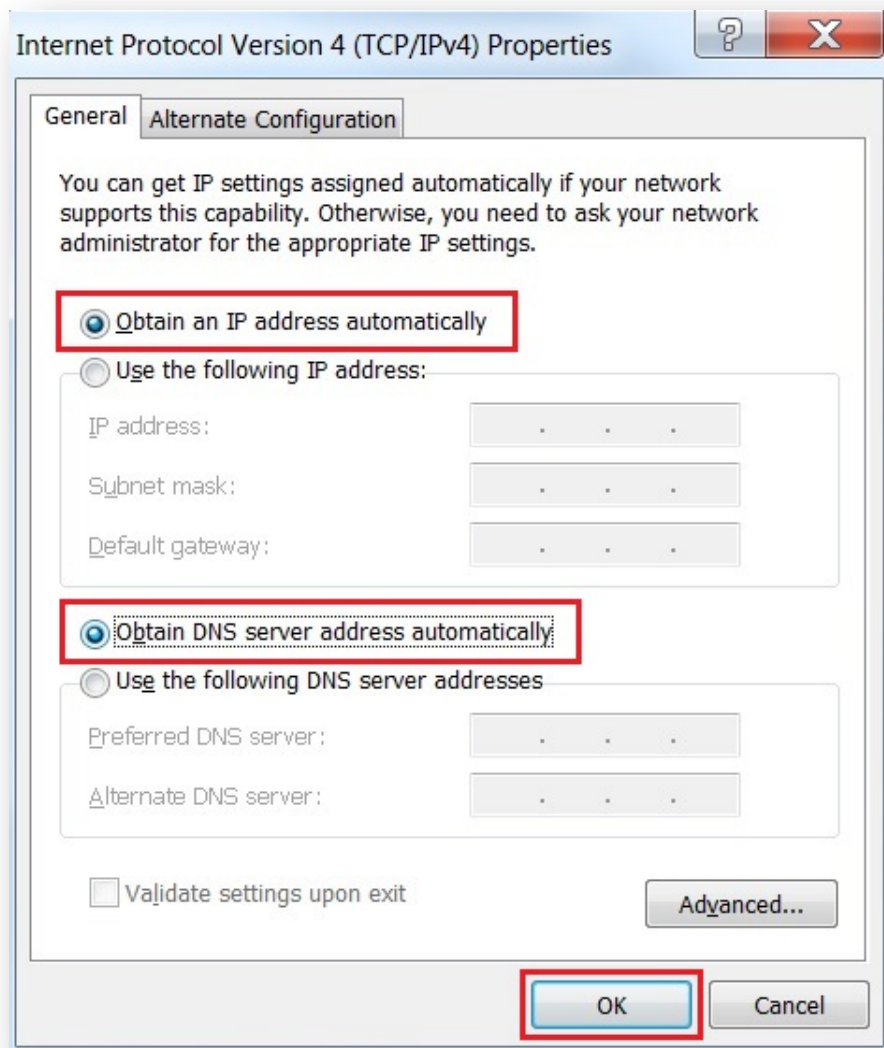
2. Right-click on the Local Area Connection and select Properties.



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



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



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.

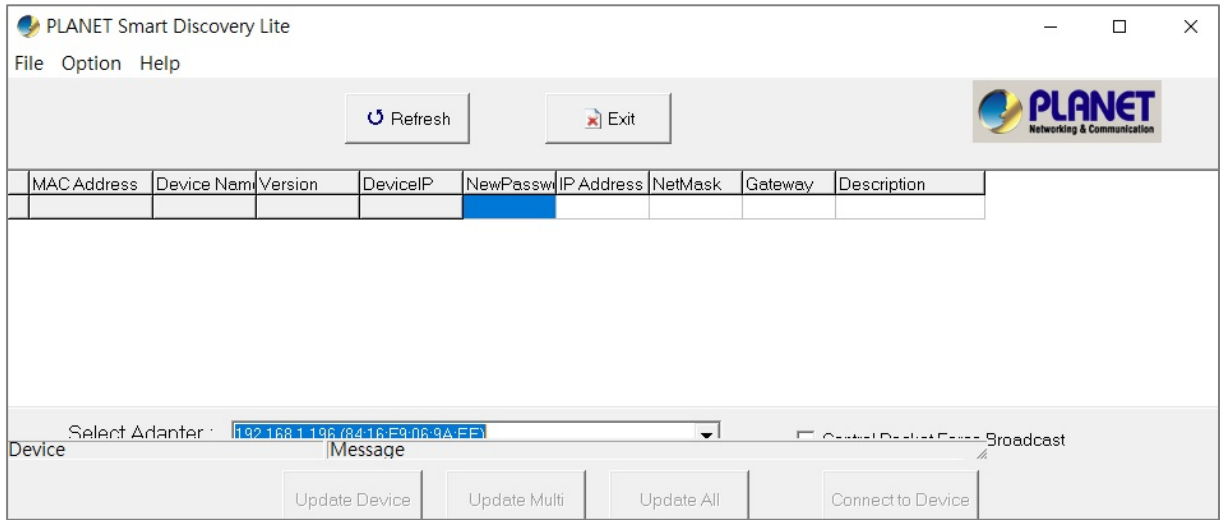


Figure 3-1-6: Planet Smart Discovery Utility Screen



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:

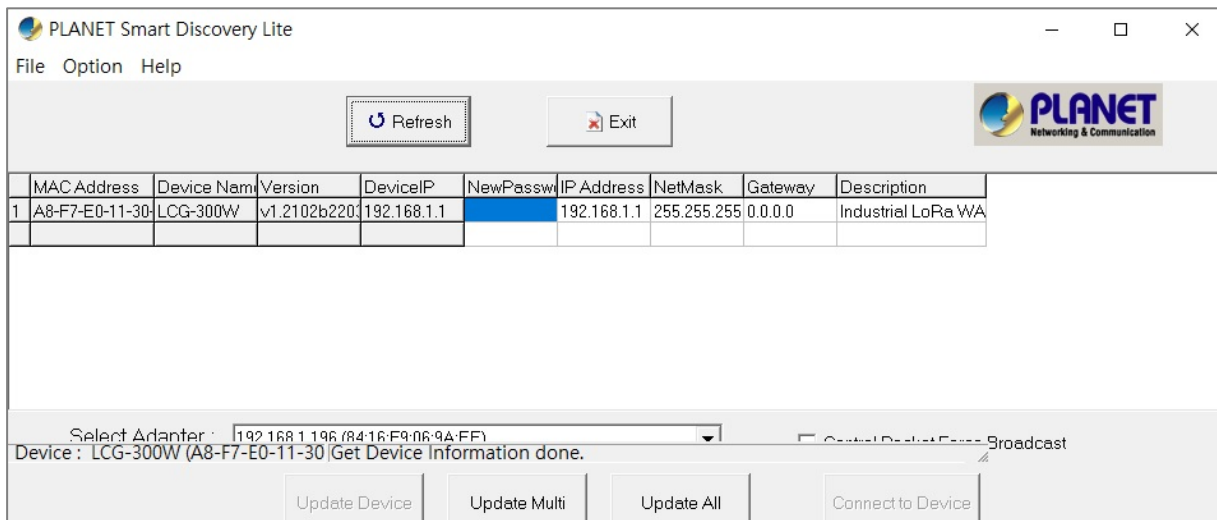


Figure 3-1-7: Planet Smart Discovery Utility Screen

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 (port 1) 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.



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

- Step 2.** The browser prompts you for the login credentials. (Both are “**admin**” by default.)

Default IP address: **192.168.1.1**

Default user name: **admin**

Default password: **admin**

Default SSID (2.4G): **PLANET_2.4G (LCG-300W only)**

Default SSID (5G): **PLANET_5G (LCG-300W only)**



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 web main page displays the web panel, main menu, function menu, and the main information in the center.

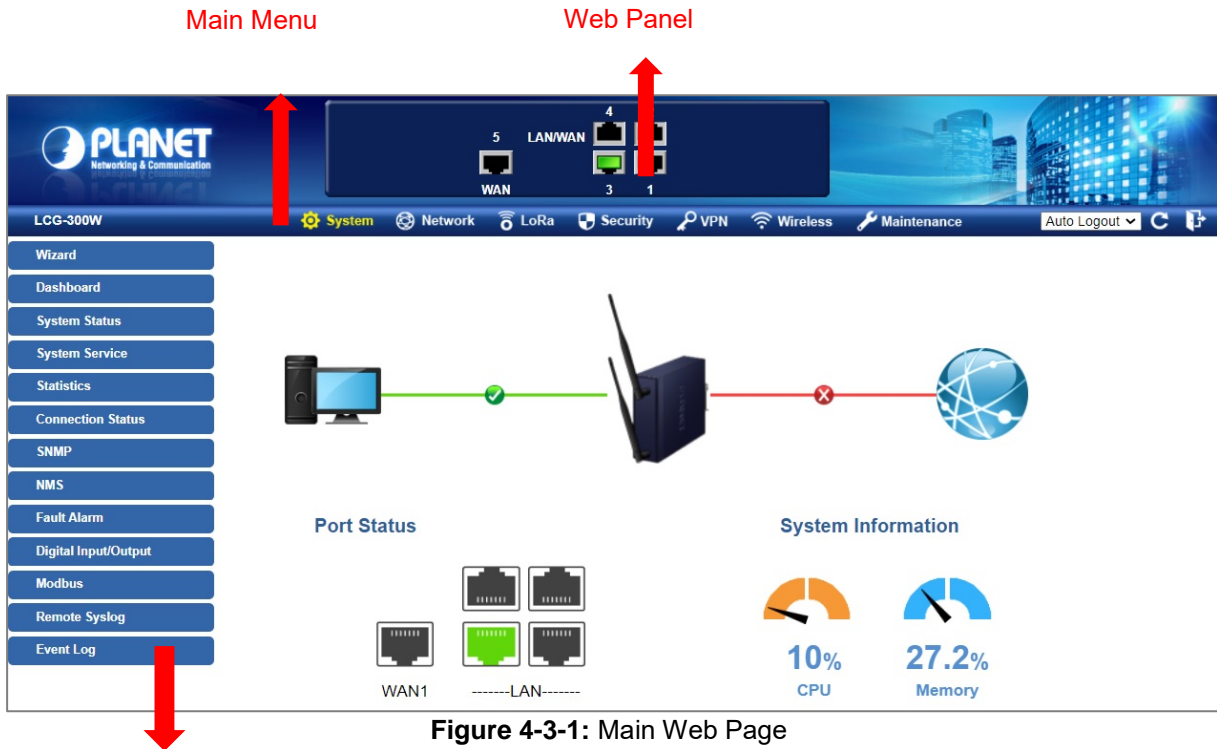


Figure 4-3-1: Main Web Page

Function Menu

■ **Web Panel**

The web panel displays an image of the device's ports as shown in [Figure 4-3-2](#).



Figure 4-2: Web Panel

Object	Icon	Function
WAN/LAN		To indicate the LAN with the RJ45 plug-in.
		To indicate network data is sending or receiving

■ 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: LCG-300W Function Menu





Figure 4-3-2: LCG-300-NR 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 (VR-300FW-NR Only).
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 (LCG-300W only)
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 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.

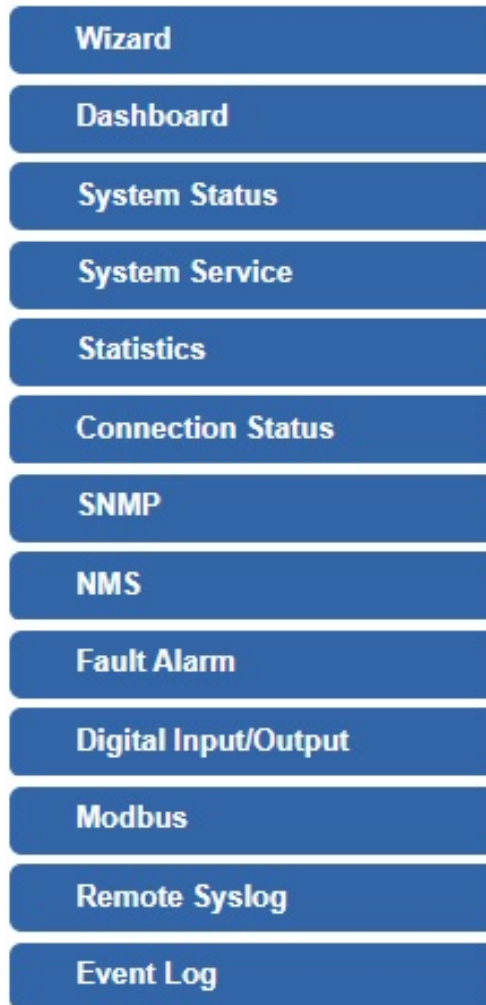


Figure 4-4-1: System Menu

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
Fault Alarm	Configure fault alarm on LoRaWAN Gateway
Digital Input/Output	Configure digital input and output 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](#).

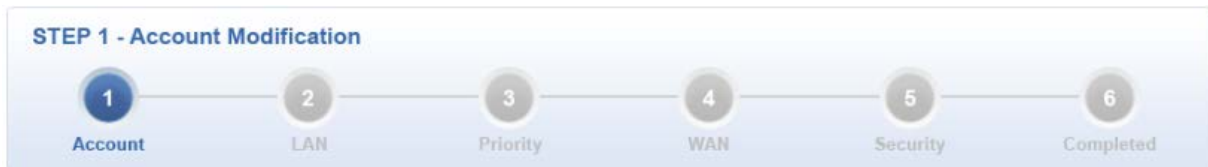
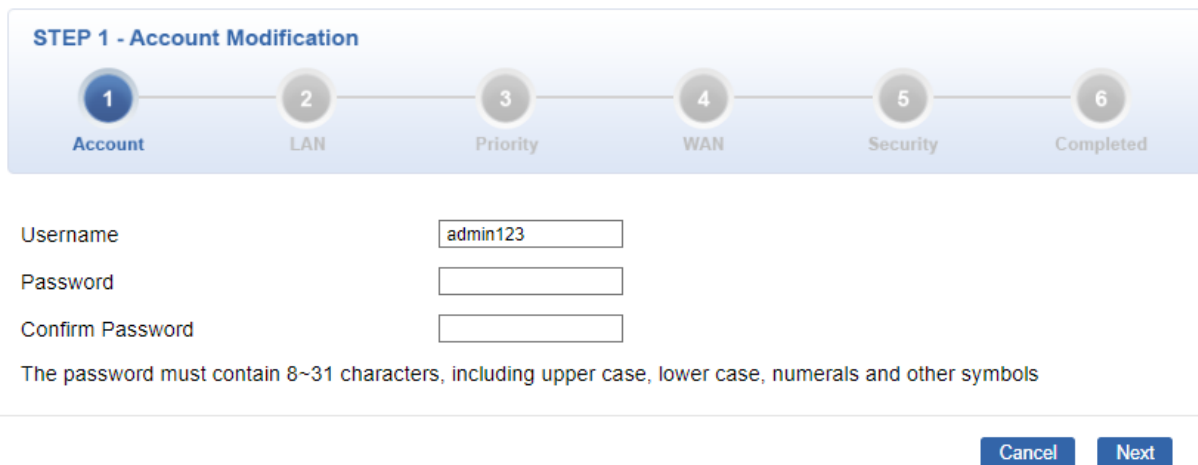


Figure 4-4-2: Setup Wizard

Step 1: Account Modification

Set up the Username and Password for the Account Modification as shown in [Figure 4-4-3](#).

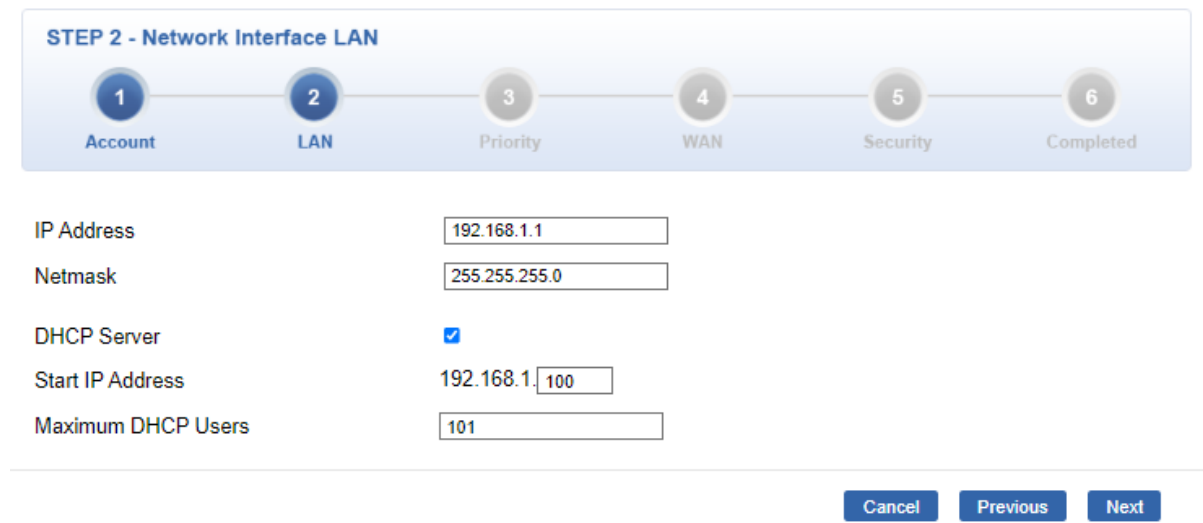


The screenshot shows the 'STEP 1 - Account Modification' screen. At the top, there is a progress bar with six steps: 1. Account (active), 2. LAN, 3. Priority, 4. WAN, 5. Security, and 6. Completed. Below the progress bar, there are three input fields: 'Username' with the value 'admin123', 'Password', and 'Confirm Password'. Below the input fields, there is a note: 'The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

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

1 Account 2 LAN 3 Priority 4 WAN 5 Security 6 Completed

IP Address: 192.168.1.1

Netmask: 255.255.255.0

DHCP Server:

Start IP Address: 192.168.1.100

Maximum DHCP Users: 101

Cancel Previous Next

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. 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. Please do not set it to the same IP address of the LoRaWAN Gateway
Maximum DHCP Users	By default, the maximum DHCP users are 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: Priority Interface (LCG-300-NR Only)

The cellular VPN Security Router supports two access modes on the WAN side shown below:

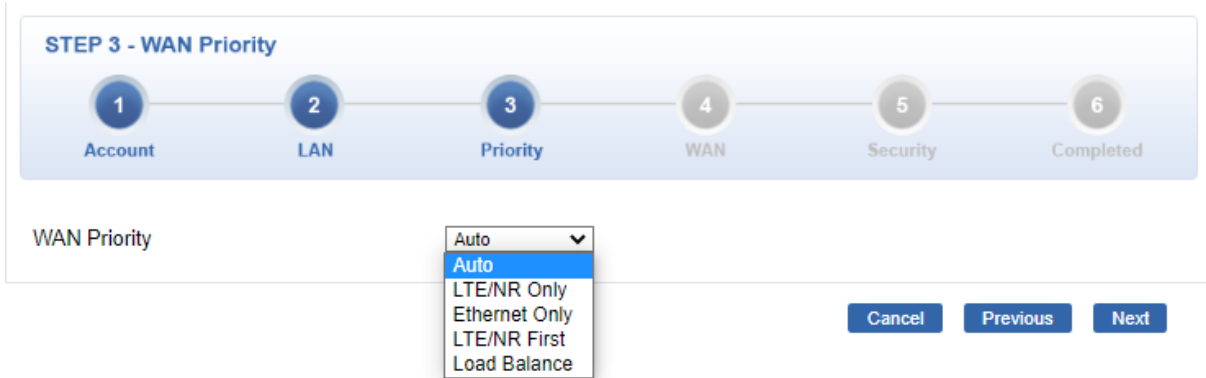


Figure: Setup Priority Configuration

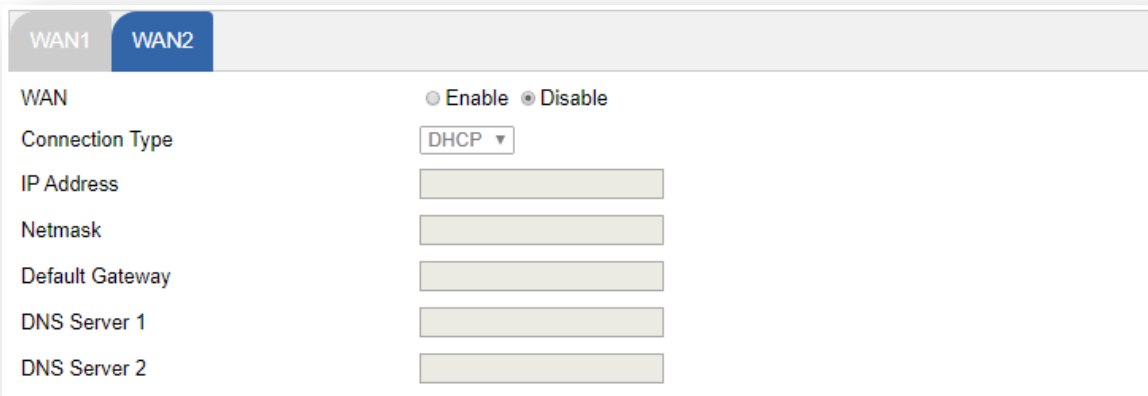
Object	Description
WAN Priority	<ul style="list-style-type: none"> ■ Auto: WAN Ethernet is first priority and second priority is NR/LTE. The default is Auto. ■ LTE/NR Only: The priority is only LTE/NR ■ ETH Only: The priority is only Ethernet. ■ LTE/NR First: LTE/NR is first priority and second priority is Ethernet

Step 4: WAN Interface

The LoRaWAN Gateway supports two access modes on the WAN side shown in below



Figure 4-4-5: Setup Wizard – WAN 1 Configuration

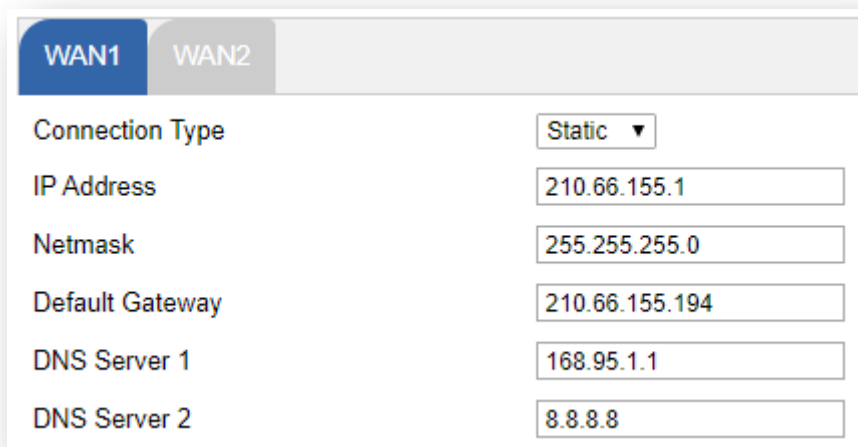


The screenshot shows the WAN2 configuration page. At the top, there are tabs for WAN1 and WAN2, with WAN2 selected. Below the tabs, there are radio buttons for 'Enable' and 'Disable', with 'Disable' selected. A 'Connection Type' dropdown menu is set to 'DHCP'. Below this are six input fields for IP Address, Netmask, Default Gateway, DNS Server 1, and DNS Server 2, all of which are currently empty.

Figure 4-4-6: Setup Wizard – WAN Configuration

Mode 1 -- Static IP

Select **Static IP Address** if all the Internet port's IP information is provided to you by your ISP. You will need to enter the **IP Address**, **Netmask**, **Default Gateway** and **DNS Server** provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The LoRaWAN Gateway will not accept the IP address if it is not in this format. The setup is shown in [Figure 4-4-7](#).



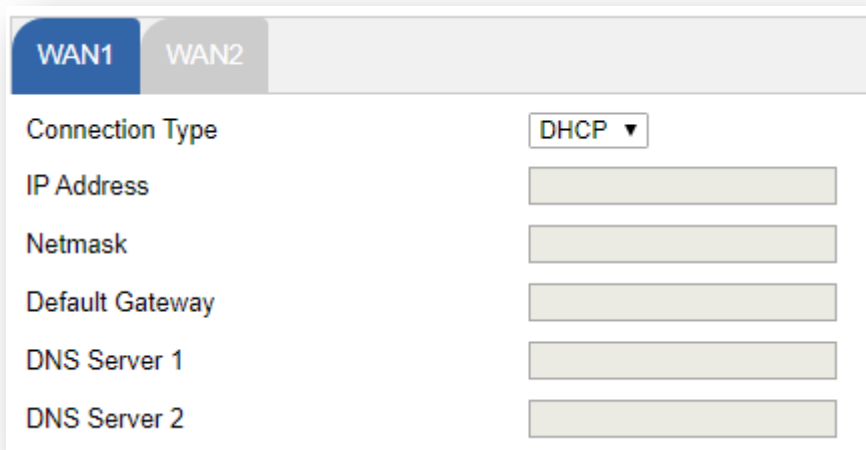
The screenshot shows the WAN2 configuration page with 'WAN1' selected. The 'Connection Type' dropdown menu is set to 'Static'. The input fields are filled with the following values: IP Address: 210.66.155.1, Netmask: 255.255.255.0, Default Gateway: 210.66.155.194, DNS Server 1: 168.95.1.1, and DNS Server 2: 8.8.8.8.

Figure 4-4-7: WAN Interface Setup – Static IP Setup

Object	Description
IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown in [Figure 4-4-8](#).



The screenshot shows a configuration window for WAN1. At the top, there are two tabs: 'WAN1' (selected) and 'WAN2'. Below the tabs, the 'Connection Type' is set to 'DHCP' via a dropdown menu. Below this, there are six input fields for 'IP Address', 'Netmask', 'Default Gateway', 'DNS Server 1', and 'DNS Server 2', all of which are currently empty.

Figure 4-4-8: WAN Interface Setup – DHCP Setup

Step 5: Wireless Setting (LCG-300W Only)

Set up the Wireless Settings as shown below

STEP 5 - Network Interface Wireless

1 Account
2 LAN
3 Priority
4 WAN
5 Wireless
6 Security
7 Completed

2.4G WiFi Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

5G WiFi Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

Figure: Setup Wizard – Security 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"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

Object	Description
5G Wireless Status	Allows user to enable or disable 5G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G".
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz" or "80MHz"
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

Step 5: Security Setting

Set up the Wireless Settings as shown in [Figure 4-4-9](#).

STEP 5 - Security Settings

1
Account

2
LAN

3
Priority

4
WAN

5
Security

6
Completed

SPI Firewall	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block SYN Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Block ICMP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block WAN Ping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Cancel
Previous
Next

Figure 4-4-9: Setup Wizard –Security Setting

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. 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. 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. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the LoRaWAN Gateway from the Internet network. 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 4-4-11](#).

STEP 6 - Setup Completed

1
Account

2
LAN

3
Priority

4
WAN

5
Security

6
Completed

LAN	Enable: Static IP: 192.168.1.1 / 255.255.255.0
WAN	Priority: Auto
WAN1	Enable: DHCP
WAN2	Enable: OFF
LTE/NR 1	Enable: ON
Security Settings	SPI Firewall: ON
	Block SYN Flood: ON
	Block ICMP Flood: OFF
	Block WAN Ping: OFF
	Remote Management: OFF

Previous
Finish

Figure 4-4-11: 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](#).

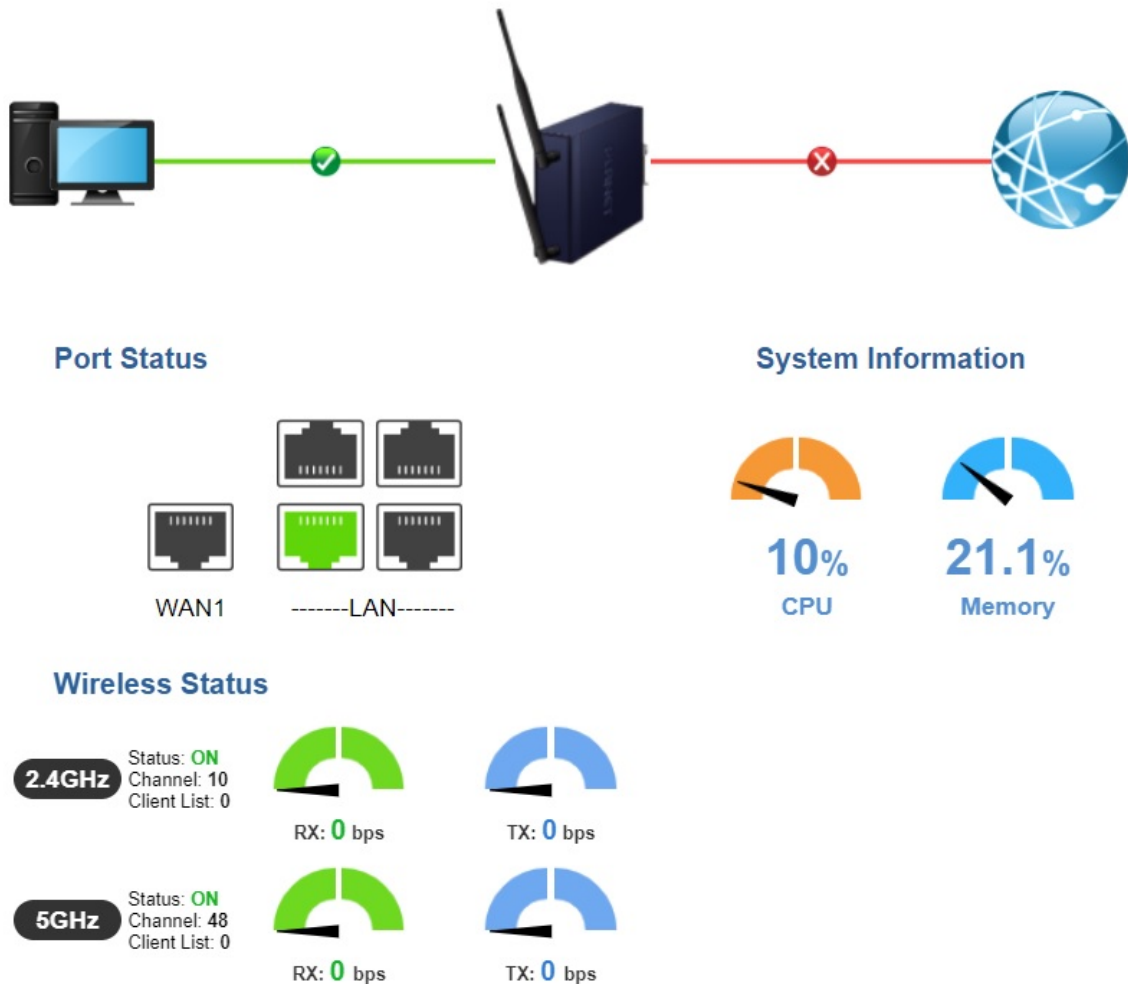







Figure 4-4-12: Dashboard

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

Object	Description
CPU	Display the CPU loading
Memory	Display the memory usage

Wireless Status (LCG-300W Only)

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

LTE/NR Status (LCG-300-NR Only)

LTE/NR Status






GPS Status

Attribute	Value
Latitude	-
Longitude	-
Horizontal	
Altitude	
Date	
Time	
Satellite	

Location:(-,-)



Object	Description
SIM	SIM signal <ul style="list-style-type: none"> ■  5G signal ■  4G signal ■  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-300W
Firmware Version	v1.2102b220303
Region	ETSI
Current Time	2022-04-22 Friday 17:11:23
Running Time	0 day, 00:48:34
Power Status	PWR1:ON, PWR2:ON
Alarm Status	Alarm
DI and DO Status	Triggered

WAN1	
MAC Address	A8:F7:E0:11:30:53
Connection Type	DHCP
Display Name	WAN1
IP Address	
Netmask	
Default Gateway	

LAN	
MAC Address	A8:F7:E0:11:30:52
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	LCG300W_2.4G
Channel	10
Encryption	WPA2 Personal (TKIP+AES)
MAC Address	A8:F7:E0:11:30:57






5GHz WiFi	
Status	ON
SSID	LCG300W-cloudviewer_test 1
Channel	48
Encryption	WPA2/WPA3 Personal
MAC Address	A8:F7:E0:11:30:58

LTE/NR 1	
Activated SIM	SIM1
SIM Status	Ready
Operator	Far EasTone
IP Address	10.130.5.22
Netmask	255.255.255.252
Default Gateway	10.130.5.21
Running Time	05:28:48
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](#).

Server Service			
#	Action	Service	Status
1	 Enabled	DHCP Service	DHCP Table: 1
2	 Disabled	DDNS Service	Not enabled
3	 Disabled	Quality of Service	
4	 Enabled	2.4GHz WiFi	SSID: LCG300W_2.4G
5	 Enabled	5GHz WiFi	SSID: LCG300W-cloudviewer_test 1











Secured Server Service			
#	Action	Service	Status
1	 Enabled	Cybersecurity	TLS 1.2, TLS 1.3
2	 Enabled	SPI Firewall	
3	 Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	 Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	 Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32
6	 Disabled	IPSec VPN Server	(Active / Maximum Tunnels) 0 / 32
7	 Disabled	GRE	(Active / Maximum Tunnels) 0 / 5
8	 Disabled	PPTP	(Active / Maximum Tunnels) 0 / 91
9	 Disabled	SSL VPN	(Active / Maximum Tunnels) 0 / 100
10	 Disabled	L2TP	(Active Tunnels) 0

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 WAN and LAN. The statistics are shown in [Figure 4-4-15](#).

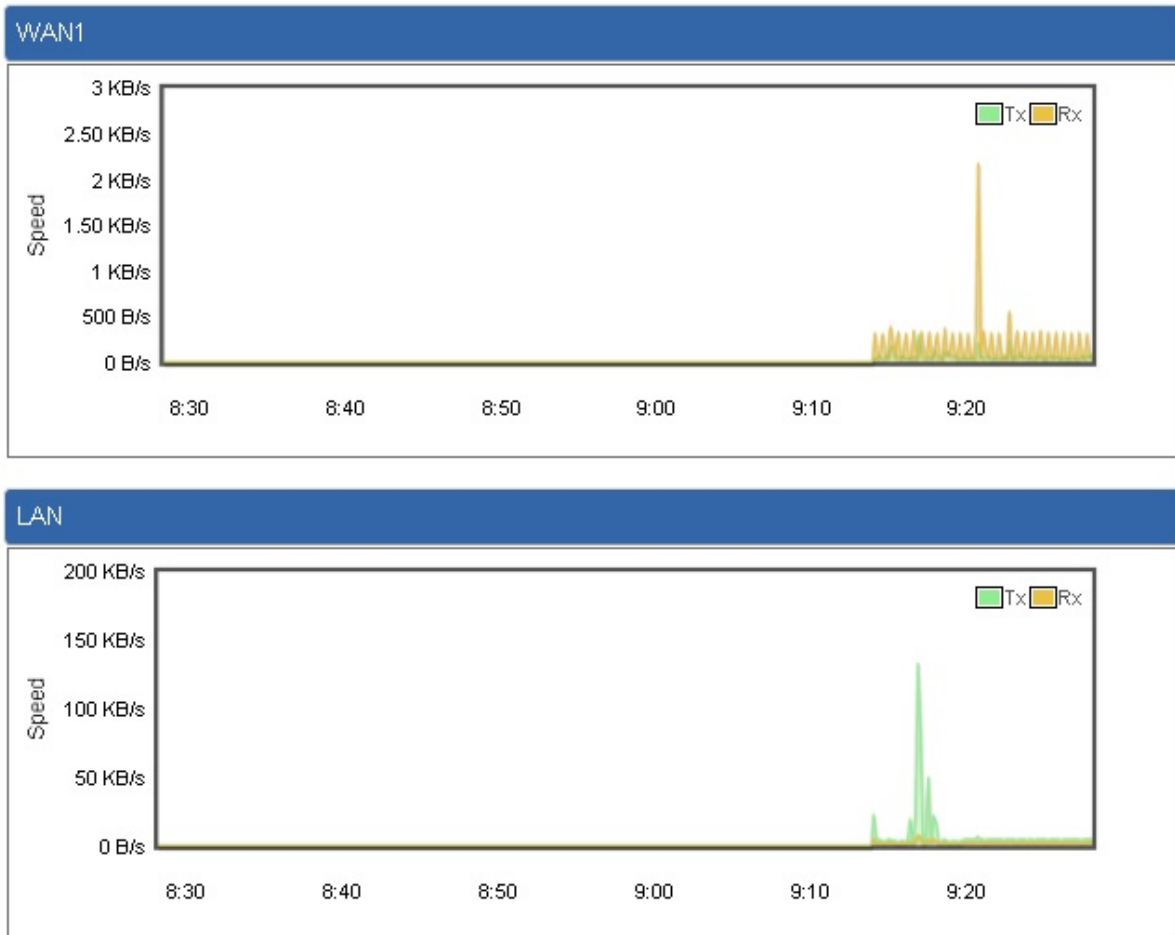


Figure 4-4-15: Statistics

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	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SNMP Versions	<input type="text" value="SNMP v1,v2c"/>
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>
Engine ID	<input type="text"/>
SNMP v3 Security Level	<input type="text" value="AuthPriv"/>
SNMP v3 User Name	<input type="text"/>
SNMP v3 Auth Protocol	<input type="text" value="MD5"/>
SNMP v3 Auth Password	<input type="text"/>
SNMP v3 Privacy Protocol	<input type="text" value="DES"/>
SNMP v3 Privacy Password	<input type="text"/>

System Identification

System Name	<input type="text" value="VR-300P"/>
System Location	<input type="text"/>
System Contact	<input type="text" value="sales@planet.com.tw"/>

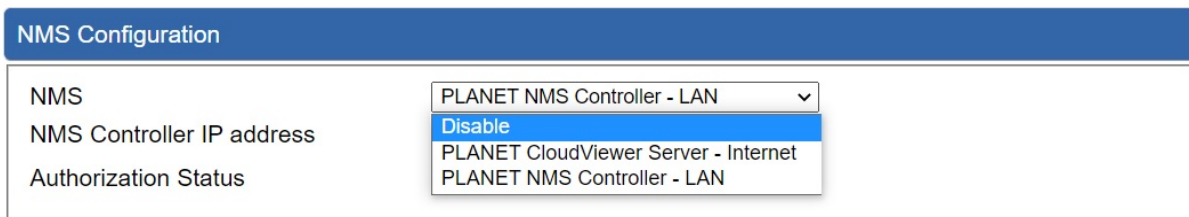
Figure 4-4-21: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. 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.

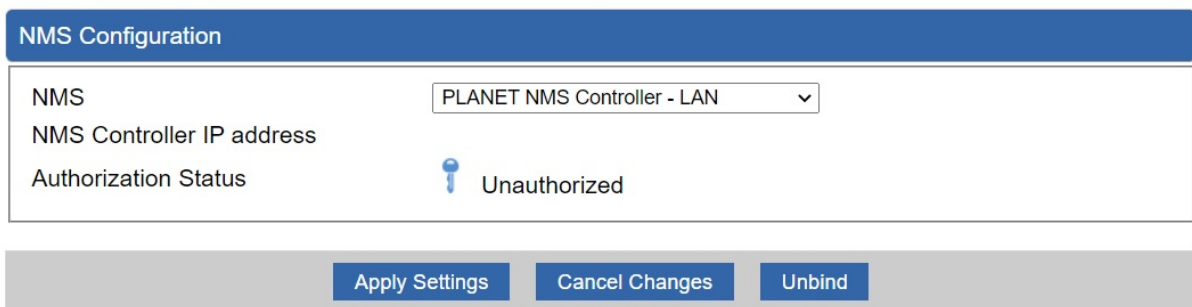
NMS Configuration is shown in [Figure 4-4-22](#)..



The screenshot shows the 'NMS Configuration' page. It features a blue header with the title 'NMS Configuration'. Below the header, there are three rows of configuration options: 'NMS', 'NMS Controller IP address', and 'Authorization Status'. The 'NMS' dropdown is set to 'PLANET NMS Controller - LAN'. The 'NMS Controller IP address' dropdown is open, showing options: 'Disable' (highlighted in blue), 'PLANET CloudViewer Server - Internet', and 'PLANET NMS Controller - LAN'. The 'Authorization Status' field is currently empty.

Figure 4-4-22 NMS Configuration Page

LAN Configuration is shown in [Figure 4-4-23](#).



The screenshot shows the 'NMS Configuration' page with the 'NMS Controller IP address' dropdown set to 'PLANET NMS Controller - LAN'. The 'Authorization Status' is now 'Unauthorized', indicated by a blue key icon. At the bottom of the page, there are three buttons: 'Apply Settings', 'Cancel Changes', and 'Unbind'.

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

Object	Description
<ul style="list-style-type: none"> NMS Controller IP address 	The IP address of NMS Controller
<ul style="list-style-type: none"> 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	<input type="text" value="PLANET CloudViewer Server - Internet"/>
Email	<input type="text"/>
Password	<input type="password"/>
Connection Status	Not enabled

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

Object	Description
<ul style="list-style-type: none"> Email 	The email registered on CloudViewer Server
<ul style="list-style-type: none"> Password 	The password of your CloudViewer account
<ul style="list-style-type: none"> Connection Status 	Indicates the status of connecting CloudViewer Server

4.4.9 Fault Alarm

This page provides fault alarm setting as shown in [Figure 4-4-25](#).

Fault Alarm Control Configuration					
Fault Alarm Output					
Enable	<input type="checkbox"/> Enable				
Record	<input type="checkbox"/> System Log <input type="checkbox"/> SMS				
Event	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail				
Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2				
Port Alarm	1	2	3	4	5
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 4-4-25: Fault Alarm

Object	Description
• Enable	Controls whether Fault Alarm is enabled.
• Record	Controls whether Record is sending System log or SMS.
• Event	Detects there is Port Failure or Power Failure, or both.
• Power Alarm	Detects PWR1 or PWR2 is at fault, or both.
• Port Alarm	Detects which Port or all is or are at fault.

4.4.10 Digital Input / Output

This page provides Digital Input / Output setting as shown in [Figure 4-4-26](#).

Digital Input/Output Control Configuration										
Digital Input 0					Digital Input 1					
Enable	<input type="checkbox"/> Enable				Enable	<input type="checkbox"/> Enable				
DI Condition	High to Low ▾				DI Condition	High to Low ▾				
Event Description	<input type="text"/>				Event Description	<input type="text"/>				
Action	<input type="checkbox"/> System Log <input type="checkbox"/> SMS				Action	<input type="checkbox"/> System Log <input type="checkbox"/> SMS				
Digital Output 0					Digital Output 1					
Enable	<input type="checkbox"/> Enable				Enable	<input type="checkbox"/> Enable				
Action	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1				Action	<input type="checkbox"/> Power Fail <input type="checkbox"/> Port Fail <input type="checkbox"/> DI 0 <input type="checkbox"/> DI 1				
DO Condition	High to Low ▾				DO Condition	High to Low ▾				
Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2				Power Alarm	<input type="checkbox"/> PWR1 <input type="checkbox"/> PWR2				
Port Fail Alarm	1	2	3	4	5	1	2	3	4	5
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 4-4-26: Digital Input / Output

Object	Description
<ul style="list-style-type: none"> Enable 	<p>Check the Enable checkbox to enable Digital Input / output function. Uncheck the Enable checkbox to disable Digital input / output function.</p>
<ul style="list-style-type: none"> Condition 	<p>As Digital Input:</p> <p>Allows user to select High to Low or Low to High. This means a signal received by system is from High to Low or From Low to High. It will trigger an action that logs a customized message or issue the message from the switch.</p> <p>As Digital Output:</p> <p>Allows user to select High to Low or Low to High. This means that when the switch's power fails or port fails, the system will issue a High or Low signal to an external device such as an alarm.</p>
<ul style="list-style-type: none"> Event Description 	<p>Allows user to set a customized message for Digital Input function alarm.</p>

<ul style="list-style-type: none"> • Action 	<p>As Digital Input:</p> <p>Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP.</p> <p>As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them.</p> <p>As Digital Output:</p> <p>Allows user to monitor an alarm from port failure, power failure, Digital Input 0 (DI 0) and Digital Input 1(DI 1) which means if Digital Output has detected these events, then Digital Output would be triggered according to the setting of Condition.</p>
<ul style="list-style-type: none"> • Power Alarm 	<p>Allows user to choose which power module that needs to be monitored.</p>
<ul style="list-style-type: none"> • Port Alarm 	<p>Allows user to choose which port that needs to be monitored.</p>

4.4.11 Modbus

This page provides Modbus setting as shown in [Figure 4-4-27](#).

Modbus Configuration

Modbus TCP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Serial device	<input type="text" value="RS-485"/>
Baudrate	<input type="text" value="9600"/>
Databits	<input type="text" value="8"/>
Parity	<input type="text" value="None"/>
Stopbits	<input type="text" value="1"/>
TCP Slave Port	<input type="text" value="502"/>

Figure 4-4-27: Modbus

Object	Description
• Enable	Enable/disable Modbus function.
• Serial device	The industrial device server supports three interfaces.
• Baudrate	The rate of data transmission to and from the attached serial device.
• Databit	Indicates the number of the bits in a transmitted data package.
• Parity	This parameter controls the error checking mode.
• Stopbits	The stop bit follows the data and parity bits in serial communication.
• TCP Slave Port	The data service center's listening port.

4.4.12 Remote Syslog

This page provides remote syslog setting as shown in [Figure 4-4-28](#).

Remote Syslog

Enable	<input type="checkbox"/>
Syslog Server	<input style="width: 150px;" type="text"/>
Port Destination	<input style="width: 150px;" type="text"/> (1~65535)

Figure 4-4-28: 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

4.4.13 Event Log

This page provides Event Log as shown below.

Event Log

1

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

Clear All Event Logs

Figure 4-4-28: Remote Syslog

4.5 Network

The Network function provides WAN, LAN and network configurations of the LoRaWAN Gateway as shown in [Figure 4-5-1](#).

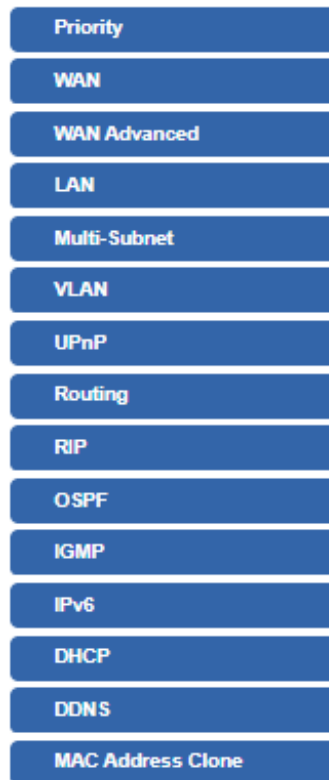


Figure 4-5-1: Network Menu

Object	Description
Priority	Allows setting WAN Priority interface.
WAN	Allows setting WAN interface.
WAN Advanced	Allows setting WAN Advanced settings.
LAN	Allows setting LAN interface.
Multi-Subnet	Allows setting Multi-Subnet1 ~ Subnet4 interface.
VLAN	Disable or enable the VLAN function. The default configuration is disabled.
UPnP	Disable or enable the UPnP function. The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function. The default configuration is disabled.
OSPF	Disable or enable the OSPF function. The default configuration is disabled.

IGMP	Disable or enable the IGMP function. 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 Priority

This page provides WAN priority setting as shown below.

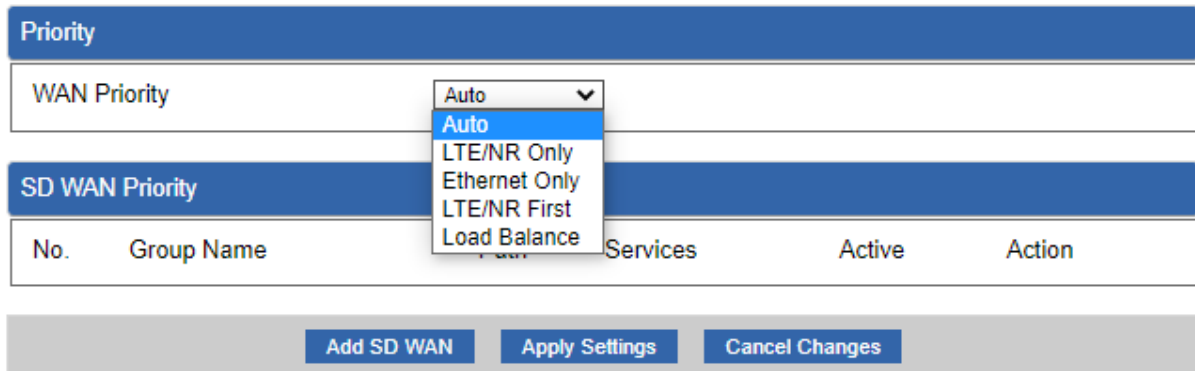


Figure: Priority

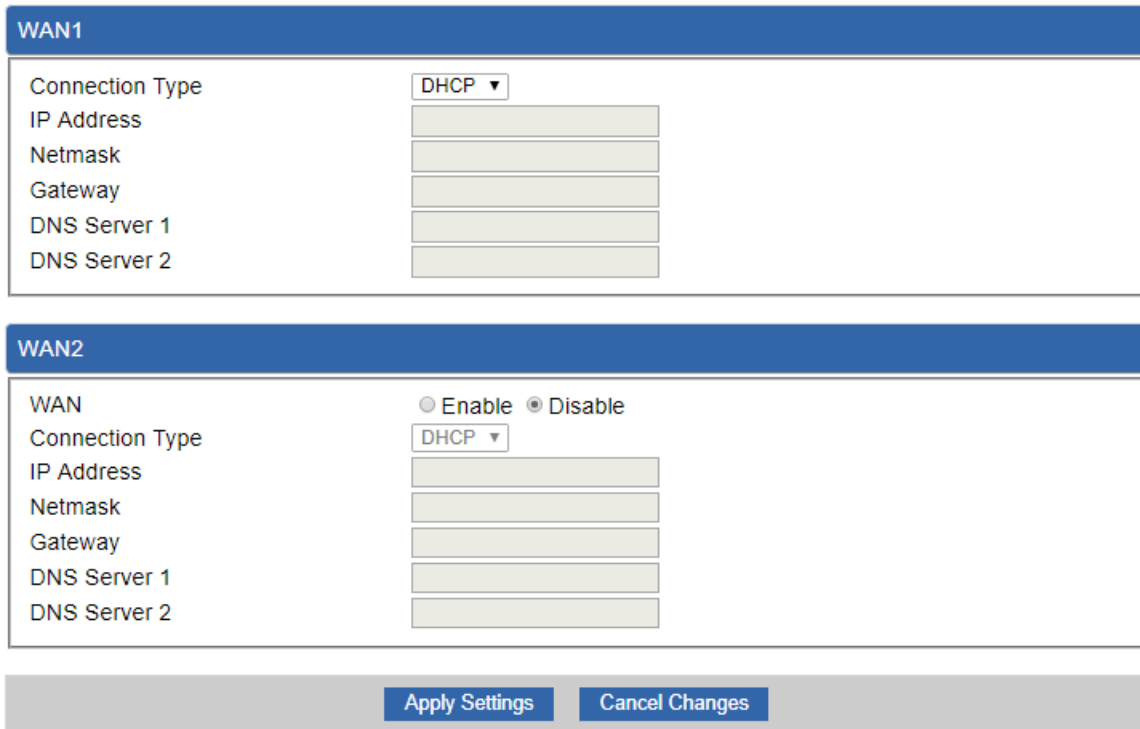
Object	Description
WAN Priority	<ul style="list-style-type: none"> ■ Auto: WAN Ethernet is first priority and second priority is NR/LTE. The default is auto. ■ LTE/NR Only: The priority is only LTE/NR ■ Ethernet Only: The priority is only Ethernet. ■ LTE/NR First: LTE/NR is first priority and second priority is Ethernet ■ Load Balance: The priority is Load Balance.

Object	Description
Active	■ Enable / Disable the Active
Group Name	■ Setting the Group Name.
Path	■ Setting the SD-WAN To / To SD-WAN
Service Port or Group	■ Setting the Service Port or Group Border Gateway Protocol

4.5.2 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the LoRaWAN Gateway as shown in [Figure 4-5-2](#)

Here you may select the access method by clicking the item value of WAN access type.



The screenshot displays a configuration interface for WAN settings. It is divided into two main sections: WAN1 and WAN2. Each section has a blue header bar with the section name. Below each header is a white box containing configuration fields. At the bottom of the interface is a grey bar with two buttons: 'Apply Settings' and 'Cancel Changes'.

WAN1

Connection Type	DHCP ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>


WAN2

WAN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Type	DHCP ▾
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Apply Settings Cancel Changes

Figure 4-5-2: WAN

Object	Description
WAN Access Type	<p>Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.</p>
	<p>Static</p> <p>Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP.</p> <p>Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The LoRaWAN Gateway will not accept the IP address if it is not in this format.</p> <p>IP Address Enter the IP address assigned by your ISP.</p> <p>Netmask Enter the Subnet Mask assigned by your ISP.</p> <p>Gateway Enter the Gateway assigned by your ISP.</p> <p>DNS Server The DNS server information will be supplied by your ISP.</p>
	<p>DHCP</p> <p>Select DHCP Client to obtain IP Address information automatically from your ISP.</p>

 Note	<p>WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the LoRaWAN Gateway will not work properly. In case of emergency, press the hardware-based "Reset" button.</p>
--	--

4.5.3 WAN Advanced

This page is used to configure the advanced parameters for Internet area network which connects to the WAN port of your LoRaWAN Gateway as shown in [Figure 4-5-3](#). Here you may change the setting for Load Balance Weight, Detect Interval, Detect Link Up Threshold, etc.

WAN1

Load Balance Weight	<input type="text" value="3"/>	
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Detect Interval	<input type="text" value="5"/>	Seconds
Detect Link Up Threshold	<input type="text" value="8"/>	Time(s)
Detect Link Down Threshold	<input type="text" value="3"/>	Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>	
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>	

WAN2

Load Balance Weight	<input type="text" value="2"/>	
External Connection Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Detect Interval	<input type="text" value="5"/>	Seconds
Detect Link Up Threshold	<input type="text" value="8"/>	Time(s)
Detect Link Down Threshold	<input type="text" value="3"/>	Time(s)
Custom Detect Host 1	<input type="text" value="8.8.8.8"/>	
Custom Detect Host 2	<input type="text" value="208.67.222.222"/>	

Apply Settings
Cancel Changes

Figure 4-5-3: LAN Setup

Object	Description
Load Balance Weight	Load Balance Weight allows you to set a relative weight (from 1 - 10) for each WAN port.
External Connection Detection	Enable to detect the status of WAN connection.
Detect Interval	Set the detect interval as you need. The recommended value is 5 (default).
Detect Link Up Threshold	Set the times for detecting link up. The recommended value is 8 (default).
Detect Link Down Threshold	Set the times for detecting link down. The recommended value is 3 (default).
Custom Detect Host	The host is used to check whether the internet connection is alive or not.

4.5.4 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

Apply Settings
Cancel Changes

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 .

4.5.5 Multi-Subnet

This page provides multi-subnet setting as shown in [Figure 4-5-5](#).

Multi-Subnet Configuration

Name	Network	IP Address	Netmask	DHCP Server
LAN Subnet 1	IP Address	192.168.1.1	255.255.255.0	V
LAN Subnet 2	IP Address	<input type="text" value="192.168.3.1"/>	<input type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>
LAN Subnet 3	IP Address	<input type="text" value="192.168.5.1"/>	<input type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>
LAN Subnet 4	IP Address	<input type="text" value="192.168.7.1"/>	<input type="text" value="255.255.255.0"/>	<input checked="" type="checkbox"/>

Figure 4-5-5: Multi-Subnet

4.5.6 VLAN

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

VLAN Configuration

VLAN Enable Disable

WAN Port

WAN VLAN ID

VLAN Table

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	Action
Management Group	LAN Subnet 1 (192.168.1.1)		<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	<input type="text" value="UNTAG"/>	

VLAN Table Configuration

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	
<input type="text"/>	<input type="text" value="Switch VLAN"/>	<input type="text"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="text" value="OFF"/>	<input type="button" value="Add"/>

Figure: VLAN Configuration

4.5.7 UPnP

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

UPnP Configuration

UPnP Enable Disable

Figure: VLAN Configuration

4.5.8 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

Destination

Netmask

Gateway

Interface

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. 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.

4.5.9 RIP

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

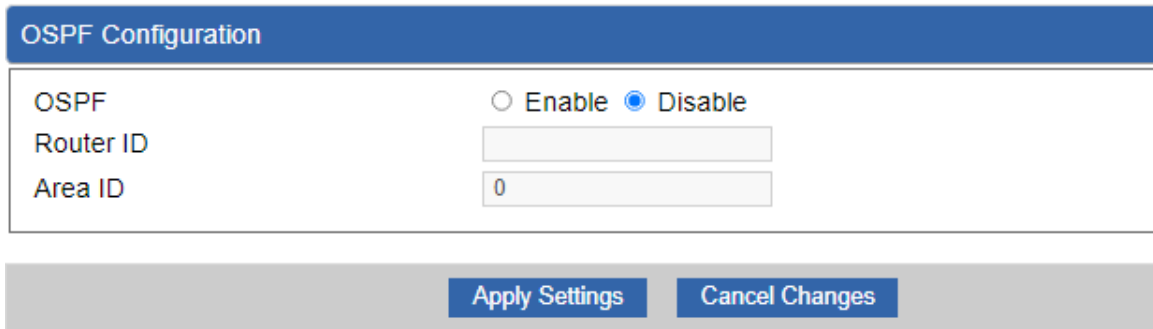
RIP Configuration

Dynamic Route	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RIP Versions	<input type="text" value="RIP 2"/>

Figure: OSPF Configuration table

4.5.10 OSPF

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

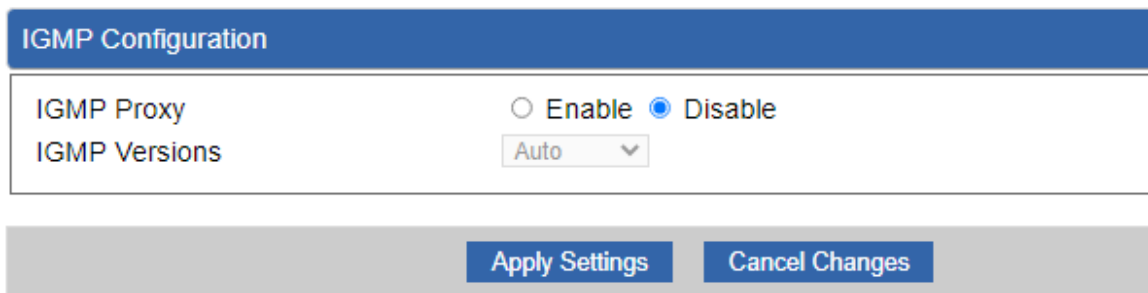


The image shows a configuration form titled "OSPF Configuration". It contains three fields: "OSPF" with radio buttons for "Enable" and "Disable" (where "Disable" is selected), "Router ID" with an empty text input field, and "Area ID" with a text input field containing the value "0". At the bottom of the form are two buttons: "Apply Settings" and "Cancel Changes".

Figure: Routing table

4.5.11 IGMP

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



The image shows a configuration form titled "IGMP Configuration". It contains two fields: "IGMP Proxy" with radio buttons for "Enable" and "Disable" (where "Disable" is selected), and "IGMP Versions" with a dropdown menu currently set to "Auto". At the bottom of the form are two buttons: "Apply Settings" and "Cancel Changes".

Figure: Routing table

4.5.12 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 - WAN1

Connection Type	<input type="text" value="DHCP"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>
IPv6 DNS Server 1	<input type="text"/>
IPv6 DNS Server 2	<input type="text"/>

IPv6 - WAN2

Connection Type	<input type="text" value="DHCP"/>
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>
Default Gateway	<input type="text"/>
IPv6 DNS Server 1	<input type="text"/>
IPv6 DNS Server 2	<input type="text"/>

IPv6 - LAN

Type	<input checked="" type="radio"/> Delegate Prefix from WAN <input type="radio"/> Static
Static Address	<input type="text"/>
Subnet Prefix Length	<input type="text" value="64"/>

DHCPv6

Address Assign	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful <input type="radio"/> Passthrough <input type="radio"/> 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.

4.5.13 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 Server

DHCP Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Start IP Address	192.168.1. <input style="width: 50px; border: 1px solid #ccc;" type="text" value="100"/>	
Maximum DHCP Users	<input style="width: 100px; border: 1px solid #ccc;" type="text" value="101"/>	
Set DNS	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually	
Primary DNS Server	<input style="width: 100%; border: 1px solid #ccc;" type="text"/>	
Secondary DNS Server	<input style="width: 100%; border: 1px solid #ccc;" type="text"/>	
WINS	<input style="width: 100%; border: 1px solid #ccc;" type="text"/>	
Lease Time	<input style="width: 80px; border: 1px solid #ccc;" type="text" value="1440"/>	minutes
Domain Name	<input style="width: 100%; border: 1px solid #ccc;" type="text" value="PLANET"/>	

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. Please do not set it to the same IP address of the LoRaWAN Gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning 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.
Set DNS	By default, it is set as Automatically, and the DNS server is the LoRaWAN Gateway's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS	Input a specific DNS server.

Object	Description
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 Default is 1440 minutes.
Domain Name	Input a domain name for the LoRaWAN Gateway Default is Planet.

4.5.14 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)

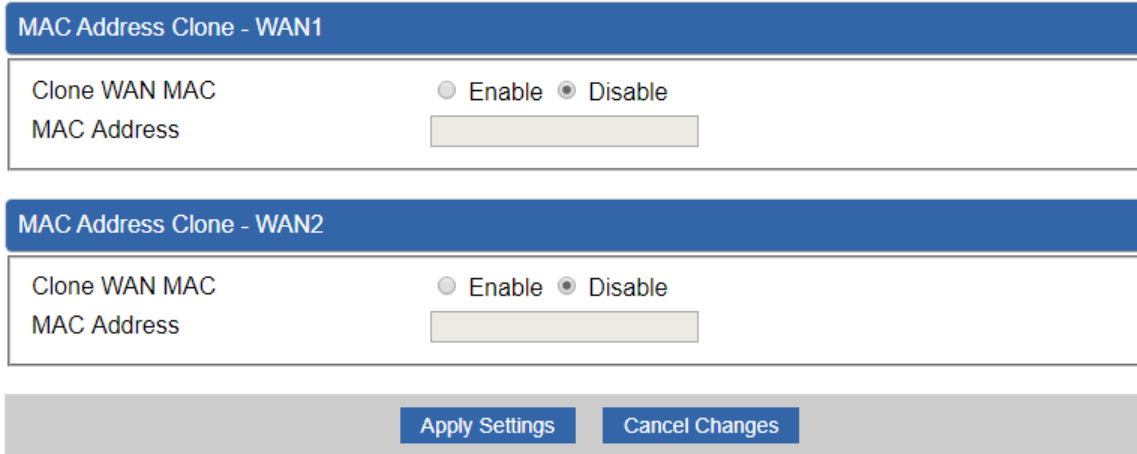
Dynamic Domain Name Service	
DDNS Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interface	WAN1 ▼
DDNS Type	PLANET DDNS ▼
Easy DDNS	Disable ▼
User Name	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Interval	120
Update Status	unknow status

Figure 4-5-10: PLANET DDNS

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: <ol style="list-style-type: none"> 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. 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. 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 into DDNS service.
Password	The password is used to log into 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.

4.5.15 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown in [Figure 4-5-11](#).



The screenshot shows two identical configuration panels for WAN1 and WAN2. Each panel has a blue header with the interface name. Below the header, there is a 'Clone WAN MAC' label with two radio buttons: 'Enable' (unselected) and 'Disable' (selected). Underneath is a 'MAC Address' label followed by a text input field. At the bottom of the entire configuration area, there are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 4-5-11: MAC Address Clone

Object	Description
Clone WAN MAC	Set the function as enable or disable.
MAC Address	Input a MAC Address, such as A8:F7:E0:00:06:62.

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.

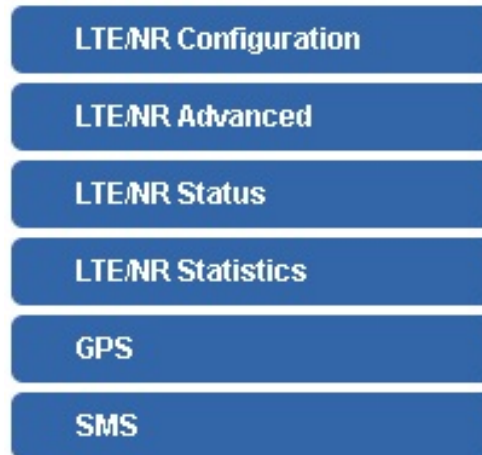


Figure 4-6-1: Cellular menu

Object	Description
LTE/NR Configuration	Allows setting LTE/NR configuration.
LTE/NR Advanced	Allows setting SIM configuration.
LTE/NR Status	Display the status of cellular.
LTE/NR Statistics	Display the statistics of cellular.
GPS	Display 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	<input style="width: 100%;" type="text" value="Auto"/>
MTU	<input style="width: 150px;" type="text" value="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: <ul style="list-style-type: none"> ■ Auto: Automatically connect the possible band. ■ 4G&5G Only: Connect to 4G or 5G network only. ■ 5G Only: Connect to 5G network only. ■ 4G Only: Connect to 4G network only. ■ 3G Only: Connect to 3G network only. ■ 2G Only: Connect to 2G 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 (1~100)*60 seconds

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

SIM1

SIM PIN

Confirmed SIM PIN

APN

Username

Password

Confirmed Password

Auth ▼

Apply Settings
Cancel Changes

Figure 4-6-3: LTE/NR advanced

Object	Description
Current SIM Card	Display which SIM slot is using.
Disable Roaming	<ul style="list-style-type: none"> ■ Disable: SIM gets connection even it is in roaming state. ■ Enable: SIM would not get connection when in roaming state.
Used SIM	Configure which SIM card or dual SIM cards is used.
SIM Priority	Configure priority of SIM card
Roaming Switch	Switch to another SIM when roaming is detected. System will switch to SIM slot when current SIM is in roaming state and the other SIM slot is in READY state.

Object	Description
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 <ul style="list-style-type: none"> ■ None ■ PAP ■ 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](#).

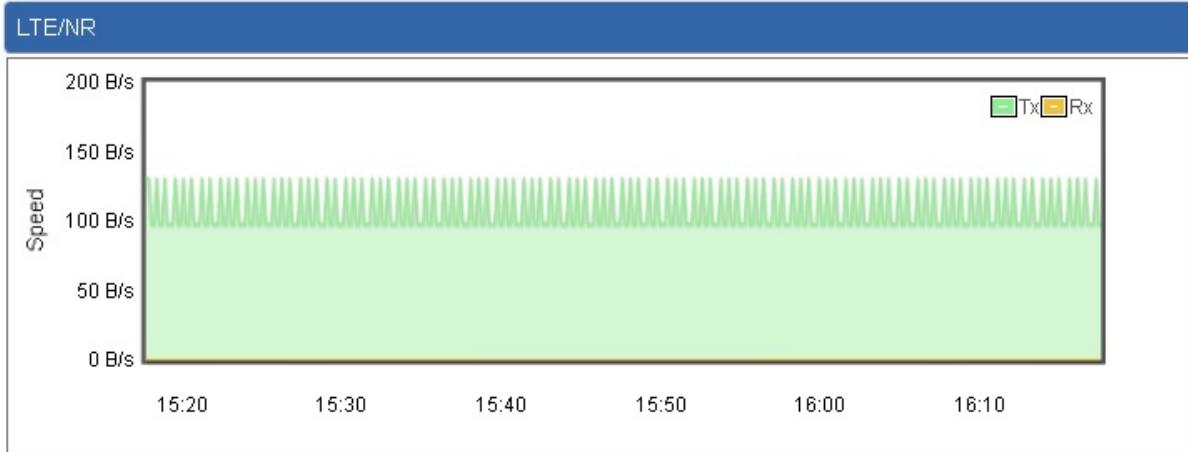


Figure 4-6-5: LTE/NR statistics

4.6.5 GPS

This page displays GPS status as shown in [Figure 4-6-6](#).

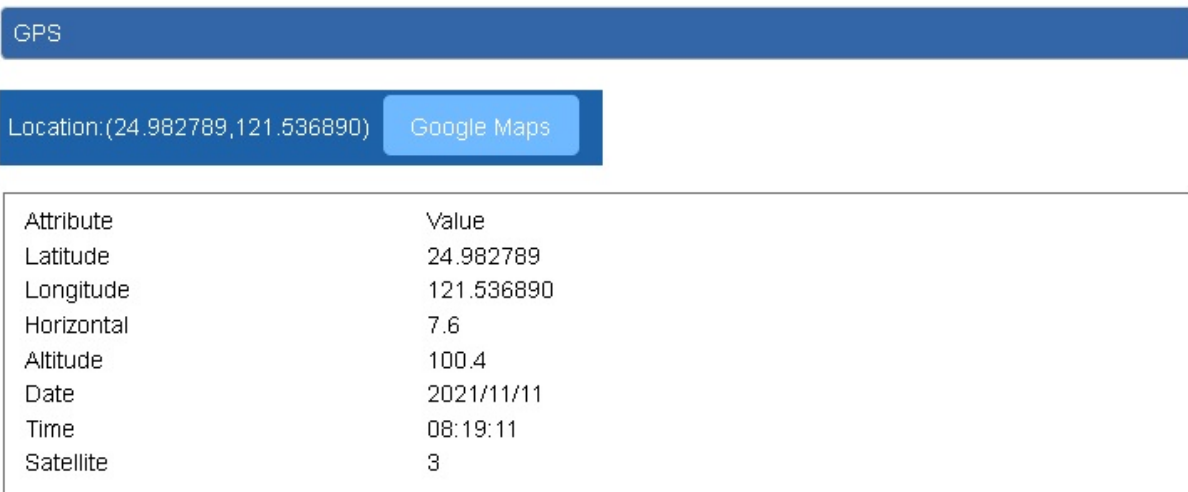


Figure 4-6-6: GPS

4.6.6 SMS

This page provides SMS configuration as shown in [Figure 4-6-7](#).

SMS Configuration

Name	<input type="text"/>
Phone	<input type="text"/>
Email	<input type="text"/>

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 4-6-1](#). Please refer to the following sections for the details.

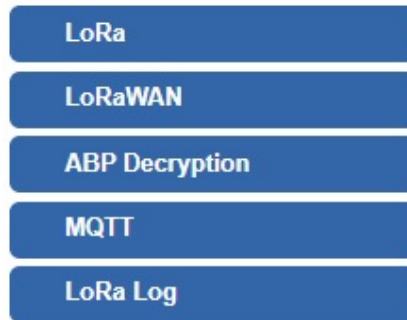


Figure 4-6-1: Cellular menu

Object	Description
LoRa	Allows setting LoRa configuration.
LoRaWAN	Allows setting LoRaWAN configuration.
ABP Decryption	Allows setting ABP Decryption configuration.
MQTT	Allows setting MQTT configuration.
LoRa Log	Displays LoRa log

4.7.1 LoRa

This page provides LoRa configuration as shown in [Figure 4-6-2](#).

LoRa Configuration

Keep Alive Period (sec)	<input style="width: 150px;" type="text" value="30"/>
Frequency Plan	<input style="width: 200px;" type="text" value="EU868 Europe 868Mhz (863~870)"/> ▼

Apply Settings
Cancel Changes

Figure 4-6-2: LoRa 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 we use, so to receive the LoRaWAN packets from the LoRaWAN sensor EU: 863~870MHz (IN865/EU868/RU864) US: 902~928MHz (US915/AU915/KR920/AS923)

4.7.2 LoRaWAN

This page provides LoRaWAN configuration as shown in [Figure 4-6-3](#).

LoRa Configuration

LoRaWAN Server Mode	<input type="text" value="LoRaWAN UDP"/>
Email	<input type="text"/>
Gateway ID	<input type="text"/>
Server Provider	<input type="text" value="The Things of Network V3"/>
Server Address	<input type="text" value="eu1.cloud.thethings.network"/>
Uplink Port	<input type="text" value="1700"/>
Downlink Port	<input type="text" value="1700"/>

Figure 4-6-3: LTE/NR advanced

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

4.7.3 ABP Decryption

This page provides ABP Decryption configuration as shown in [Figure 4-6-4](#).

ABP Decryption

ABP Decryption Enable Disable

ABP Keys

No.	Dev ADDR	APP Session Key	Network Session Key	Decoder	Action
<div style="background-color: #0056b3; color: white; padding: 2px 5px; font-weight: bold; display: inline-block;">Add ABP Key</div>					

Figure 4-6-4: 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

4.7.4 MQTT

This page provides MQTT Client Configuration as shown in [Figure 4-6-5](#).

MQTT Client Configuration

Enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Quality of Service [-q]	QoS 0 ▾		
Broker Address [-h]	<input type="text"/>		
Broker Port [-p]	<input type="text" value="1883"/>		
User ID [-u]	<input type="text"/>		
Password [-P]	<input type="password"/>		👁
Client ID [-i]	<input type="text"/>		
Certificate [--cert]	N/A <input type="button" value="Choose File"/> No file chosen	<input type="button" value="Upload Certificate"/>	
Key [--key]	N/A <input type="button" value="Choose File"/> No file chosen	<input type="button" value="Upload Key"/>	
CA File [--cafile]	N/A <input type="button" value="Choose File"/> No file chosen	<input type="button" value="Upload CA File"/>	

Figure 4-6-5: MQTT Client Configuration

Object	Description
Enable	Enable or disable MQTT service
Quality of Service	The level of quality of service
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

4.7.5 LoRa Log

This page shows the frequency for LoRa radio and traffics as shown in [Figure 4-6-6](#).

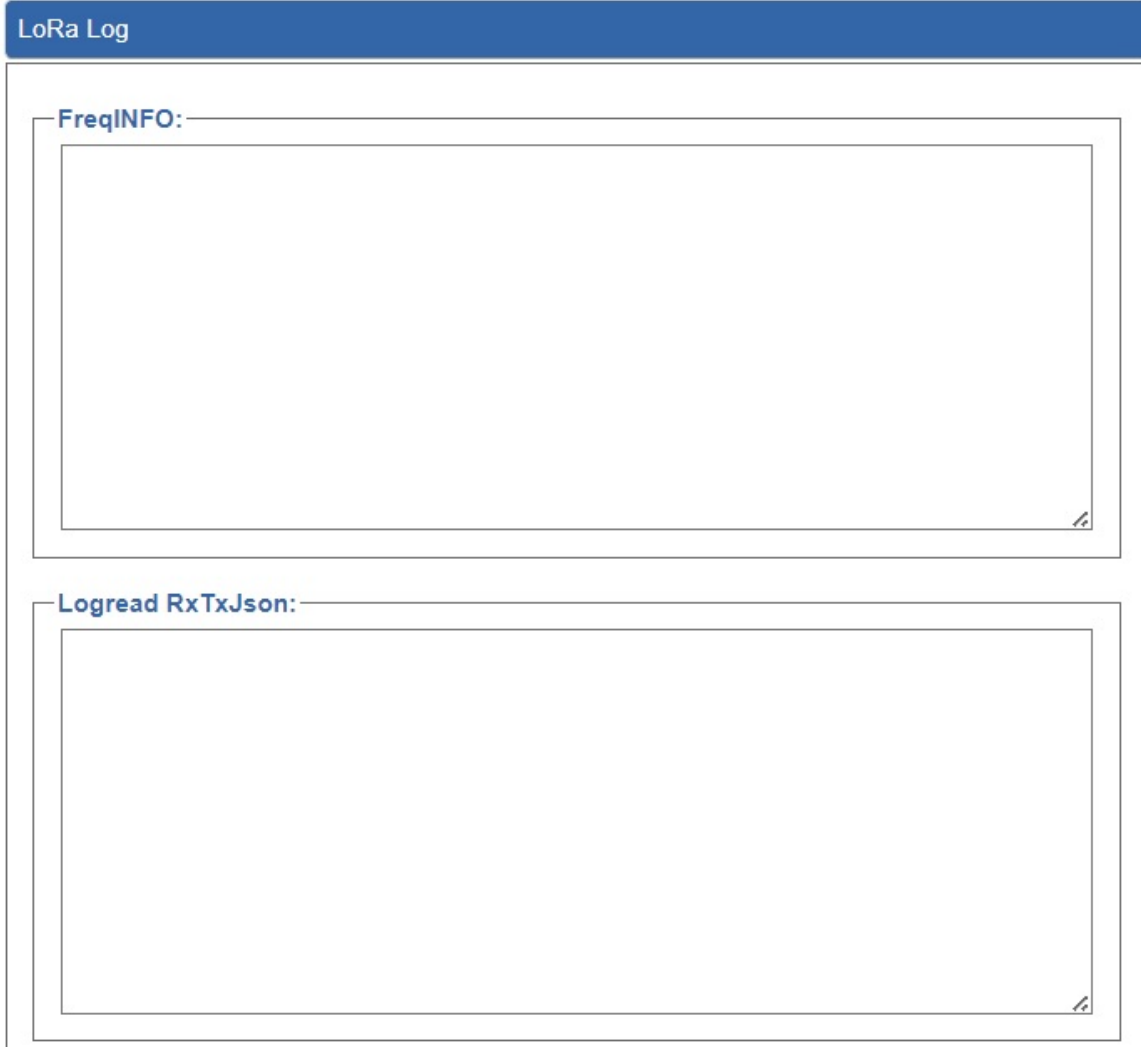


Figure 4-6-6: LoRa Radio and traffics

4.8 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in [Figure 4-7-1](#). Please refer to the following sections for the details.



Figure 4-7-1: 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 Forwarding	Allows setting Port Forwarding.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.

4.8.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The LoRaWAN Gateway can prevent specific DoS attacks as shown in [Figure 4-7-2](#).

Firewall Protection

SPI Firewall Enable Disable

DDos

Block SYN Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block FIN Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block UDP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="30"/>	Packets/Second
Block ICMP Flood	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<input type="text" value="5"/>	Packets/Second
IP TearDrop	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
PingOfDeath	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

System Security

Block WAN Ping Enable Disable

Remote Management Enable Disable

Apply Settings
Cancel Changes

Figure 4-7-2: Firewall

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. 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. 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. 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. The default configuration is disabled.

<p>Block ICMP Flood</p>	<p>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. The default configuration is disabled.</p>
<p>IP TearDrop</p>	<p>If the function is enabled, the LoRaWAN Gateway will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.</p>
<p>Ping Of Death</p>	<p>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.</p>
<p>Block WAN Ping</p>	<p>Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.</p>
<p>Remote Management</p>	<p>Enable the function to allow the web server access of the LoRaWAN Gateway from the Internet network. The default configuration is disabled.</p>

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 4-7-3](#).

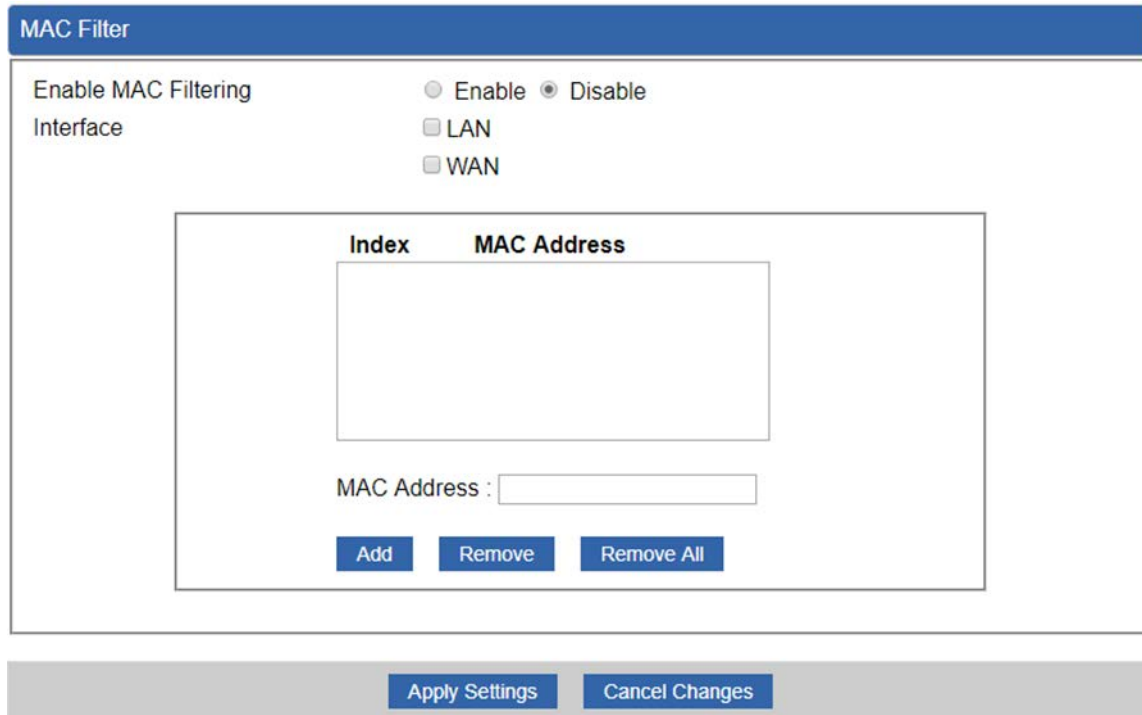


Figure 4-7-3: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. 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 4-7-4](#). To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

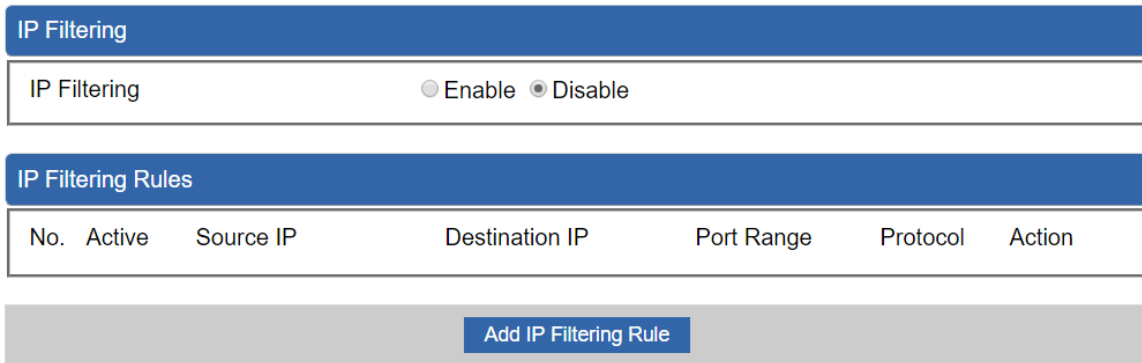


Figure 4-7-4: IP Filtering

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.

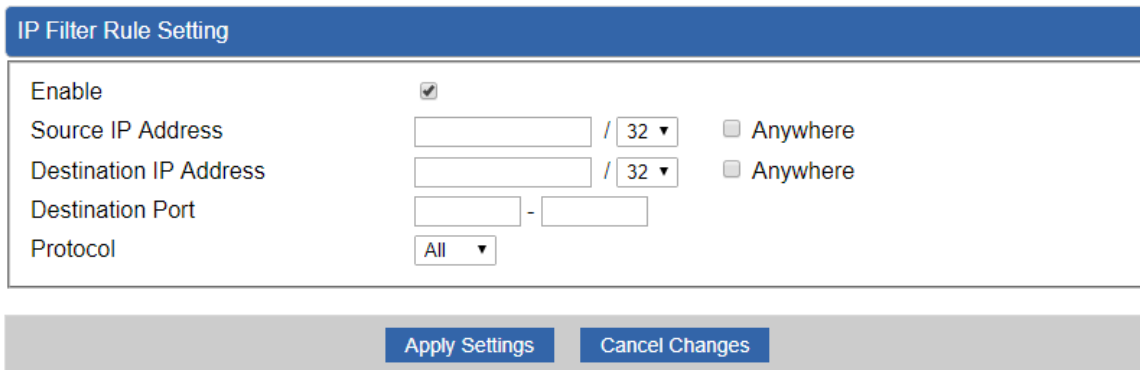


Figure 4-7-5: IP Filter Rule Setting

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.

Object	Description
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.
Destination Port	Input the port of destination IP Address which you want to block. Leave it as blank if you want to block all ports of the web site.
Protocol	Select the protocol type (TCP, UDP or all). 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 4-7-6](#). 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
<div style="background-color: #4a7ebb; color: white; padding: 2px 10px; border-radius: 3px; display: inline-block;">Add Web Filtering Rule</div>				

Figure 4-7-6: 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

Filter Keyword

Apply Settings

Cancel Changes

Figure 4-7-7 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 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 4-7-8](#). 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.

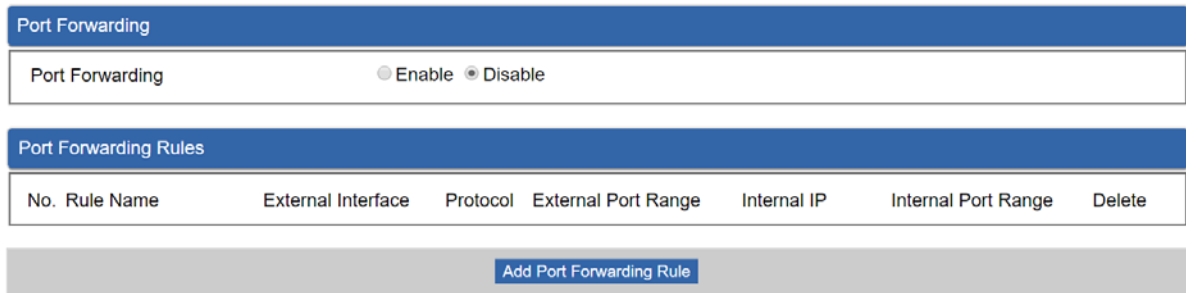


Figure 4-7-8: Port Forwarding

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.

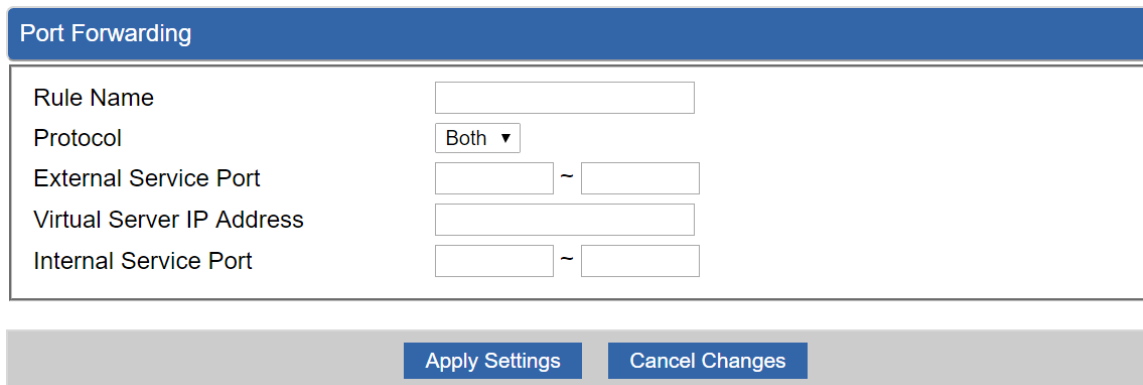


Figure 4-7-9: Port Forwarding Rule Setting

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

Object	Description
	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.

4.8.6 QoS

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

QoS - WAN1

Quality of Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upstream	<input type="text" value="0"/> Kbps
Downstream	<input type="text" value="0"/> Kbps

QoS - WAN2

Quality of Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upstream	<input type="text" value="0"/> Kbps
Downstream	<input type="text" value="0"/> Kbps

Upstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
		WAN2 <input type="text" value="0"/> Kbps
Express	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
		WAN2 <input type="text" value="0"/> Kbps
Standard	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
		WAN2 <input type="text" value="0"/> Kbps
Bulks	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps
		WAN2 <input type="text" value="0"/> Kbps

Downstream Bandwidth		
Priority	Maximum Bandwidth	Bandwidth Value
Premium	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Express	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Standard	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps
Bulks	<input type="text" value="100"/> %	WAN1 <input type="text" value="0"/> Kbps WAN2 <input type="text" value="0"/> Kbps

Service Priority			
Protocol	Description	Priority	Action
<input type="text" value="AOL(TCP:5190)"/> ▼	AOL Instant Messenger protocol	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

Network Priority				
Source Network	Protocol	Destination Port Range	Priority	Action
<input type="text"/> / <input type="text"/>	<input type="text" value="ALL"/> ▼	<input type="text"/> -- <input type="text"/>	<input type="text" value="Premium"/> ▼	<input type="button" value="Add"/>

4.8.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in [Figure 4-7-9](#). Typically the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ - WAN1	
DMZ	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ IP Address	<input type="text"/>

DMZ - WAN2	
DMZ	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ IP Address	<input type="text"/>

Figure 4-7-9: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

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 4-8-1](#)

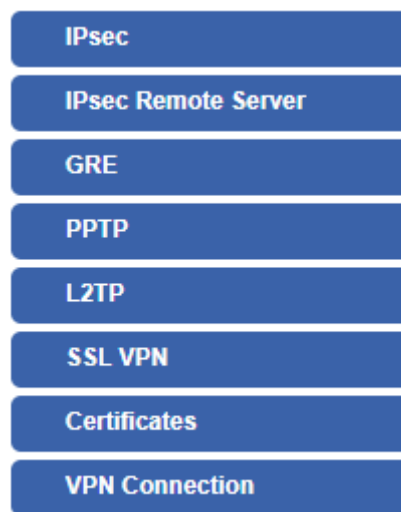


Figure 4-8-1: VPN Menu

Object	Description
IPsec	Allows setting IPsec function.
IPsec Remote Server	Disable or enable the IPsec Remote Server function. 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 4-8-2](#).

IPsec Tunnel Lists

No.	Name	Interface	Status	Action
<div style="background-color: #0056b3; color: white; padding: 2px 10px; display: inline-block; border-radius: 3px;">Add IPsec Tunnel</div>				

Figure 4-8-2: 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 /24

Remote IP Address

Remote Network

Remote Netmask /24

Detection

Dead Peer Detection

Time Interval Seconds Timeout Seconds Action

Authentication

Preshare Key

IKE Setting

Phase 1

IKE v1 v2

Connection Type Main Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Perfect Forward Secrecy (PFS) Yes No

Apply Settings

Cancel Changes

Figure 4-8-3: IPsec Tunnel

Object	Description
IPSec Tunnel Enable	Check the box to enable the function.
Tunnel Name	Enter any words for recognition.
Interface	<p>This is only available for host-to-host connections and specifies to which interface the host is connecting.</p> <ol style="list-style-type: none"> 1. WAN 1. 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	<p>Set up the detection time of DPD (Dead Peer Detection).</p> <p>By default, the DPD detection's gap is 30 seconds, over 150 seconds to think that is the broken line.</p> <p>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.</p>
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	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.

ISAKMP	<p>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.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 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. 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. 4. SHA2: Either 256, 384 or 512 can be chosen 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 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	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 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. 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. 4. SHA2: Either 256, 384 or 512 can be chosen. 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
	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	<input type="button" value="Add"/>

Authentication

Certificate Self-signed certificate

Preshare Key

IPsec

Phase 1

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

IKE SA Lifetime hours

Phase 2

ESP AES (128 bit) ▼ SHA1 ▼

ESP Keylife hours

4.9.3 GRE

This section assists you in setting the GRE Tunnel as shown in [Figure 4-8-4](#).

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
<input type="button" value="Add GRE Tunnel"/>									

Figure 4-8-4: 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	<input type="text" value="Disable"/>
Name	<input type="text" value="Tunnel name"/>
Through	<input type="text" value="LAN"/>
Peer Wan IP Address	<input type="text" value="Remote IP Address"/>
Peer Subnet Mask	<input type="text" value="10.10.10.0/24"/>
Peer Tunnel IP Address	<input type="text" value="10.10.10.2"/>
Local Tunnel IP Address	<input type="text" value="10.10.10.1"/>
Local Subnet Mask	<input type="text" value="255.255.255.255 /32"/>

Figure 4-8-5: 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. <ol style="list-style-type: none"> 1. LAN. 2. WAN 1. 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 4-8-6](#).

PPTP Server

PPTP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Force MPPE Encryption	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
CHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MSCHAP v2	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DNS1	<input type="text"/>
DNS2	<input type="text"/>
WINS1	<input type="text"/>
WINS2	<input type="text"/>
Server IP Address	<input type="text" value="192.168.10.1"/>
Clients IP Address Start	<input type="text" value="192.168.10.10"/>
Clients IP Address End	<input type="text" value="192.168.10.100"/>

	User	Password
1	<input type="text" value="test"/>	<input type="text" value="test"/>
2	<input type="text" value="user"/>	<input type="text" value="1234"/>
3	<input type="text" value="user"/>	<input type="text" value="1234"/>
4	<input type="text" value="user"/>	<input type="text" value="1234"/>
5	<input type="text" value="user"/>	<input type="text" value="1234"/>

Figure 4-8-6: 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 4-8-7](#).

L2TP Server

L2TP Server Enable Disable

Server IP Address

Clients IP Address Start

Clients IP Address End

With IPsec Enable Disable

Preshare Key

Users

	User	Password
1	<input type="text" value="test"/>	<input type="text" value="test"/>
2	<input type="text" value="user"/>	<input type="text" value="1234"/>
3	<input type="text" value="user"/>	<input type="text" value="1234"/>
4	<input type="text" value="user"/>	<input type="text" value="1234"/>
5	<input type="text" value="user"/>	<input type="text" value="1234"/>

IPsec

Phase 1

Connection Type Main Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Figure 4-8-7: 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.

Object	Description
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	<ol style="list-style-type: none"> 1. Main. 2. Aggressive.
ISAKMP	<p>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.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 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. 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. 4. SHA2: Either 256, 384 or 512 can be chosen. 5. MD5 Algorithm: MD5 processes a variably long message into a fixed-length output of 128 bits. 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	<p>It offers AES, 3 DES, SHA 1, SHA2, and MD5.</p> <ol style="list-style-type: none"> 1. AES: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays. 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. 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. 4. SHA2: Either 256, 384 or 512 can be chosen. 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 4-8-8](#).

SSL Server

SSL VPN Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Port	<input type="text" value="1194"/>
Tunnel Protocol	<input type="text" value="UDP"/>
Virtual Network Device	<input type="text" value="TUN"/>
Interface	<input type="text" value="LAN"/> 192.168.1.1
VPN Network	<input type="text" value="192.168.20.0"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Encryption Cipher	<input type="text" value="AES-128 CBC"/>
Hash Algorithm	<input type="text" value="SHA1"/>
Export client.ovpn	<input type="button" value="Export"/>

Figure 4-8-8: 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 4-8-9](#).

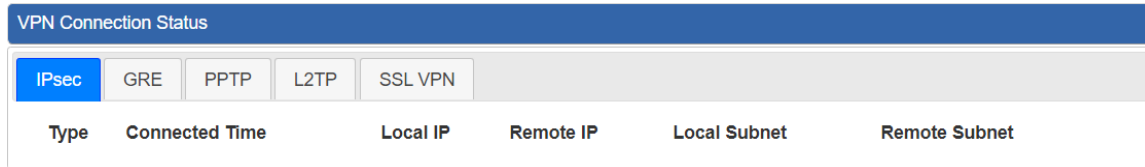


Figure 4-8-9: VPN Connection Status

Object	Description
VPN Connection Status	Click the IPsec/GRE/.../SSL VPN bookmark to check the current connection status.

4.10 Wireless

The Wireless menu provides the following features as shown in [Figure 4-10-1](#)

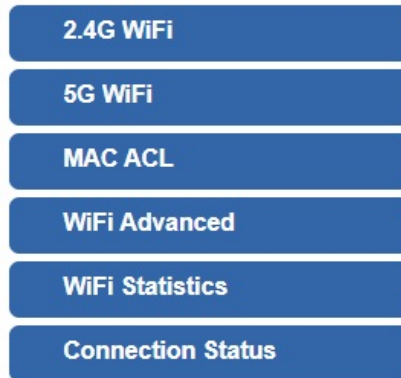


Figure 4-9-1: Wireless Menu

Object	Description
2.4G Wi-Fi	Allow to configure 2.4G Wi-Fi.
5G Wi-Fi	Allow to configure 5G 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](#).

2.4G WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Bandwidth ▾

Channel ▾

Encryption ▾

WiFi Multimedia Enable Disable

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

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 5G Wi-Fi

This page allows the user to define 5G Wi-Fi as shown in [Figure 4-10-3](#).

5G WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Bandwidth ▾

Channel ▾

Encryption ▾

WiFi Multimedia Enable Disable

Figure 4-10-3: 5G Wi-Fi

Object	Description
Wireless Status	Allows user to enable or disable 5G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G"
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, "20MHz" or "40MHz" or "80MHz"
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "Open"
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

4.10.3 MAC ACL

This page provides MAC ACL configuration as shown in [Figure 4-10-4](#).

MAC ACL

MAC ACL Enable Disable

MAC ACL Rules


Index	Active	Device Name	MAC Address	Action
		<input type="text" value="abc"/>	<input type="text" value="00:30:4F:00:00:01"/>	<div style="background-color: #2e5496; color: white; padding: 2px 5px; margin-bottom: 2px;">Add</div> <div style="background-color: #2e5496; color: white; padding: 2px 5px;">Scan</div>

Figure 4-10-4: MAC ACL

Object	Description
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

4.10.4 Wi-Fi Advanced

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

WiFi Advanced	
2.4G Mode	11 AX ▾
5G Mode	11 AX ▾
2.4GHz Maximum Associated Clients	32 (Range 1~64)
5GHz Maximum Associated Clients	32 (Range 1~64)
2.4G Coverage Threshold	-90 (-95dBm ~ -60dBm)
5G Coverage Threshold	-90 (-95dBm ~ -60dBm)
2.4G TX Power	Max(100%) ▾
5G TX Power	Max(100%) ▾

Figure 4-10-5: Wi-Fi advanced

Object	Description
2.4G Mode	11AC: Select 802.11B/G or 802.11N/G 11AX: Select 802.11B/G or 802.11N/G or 802.11AX
5G Mode	11AC: Select 802.11A or 802.11AN or 802.11AC 11AX: Select 802.11A or 802.11AN or 802.11AC or 802.11AX
2.4GHz Maximum Associated Clients	The maximum users are 64
5GHz 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 -90dBm
5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm
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
5G 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

4.10.5 Wi-Fi Statistics

This page displays Wi-Fi statistics as shown in [Figure 4-10-6](#).

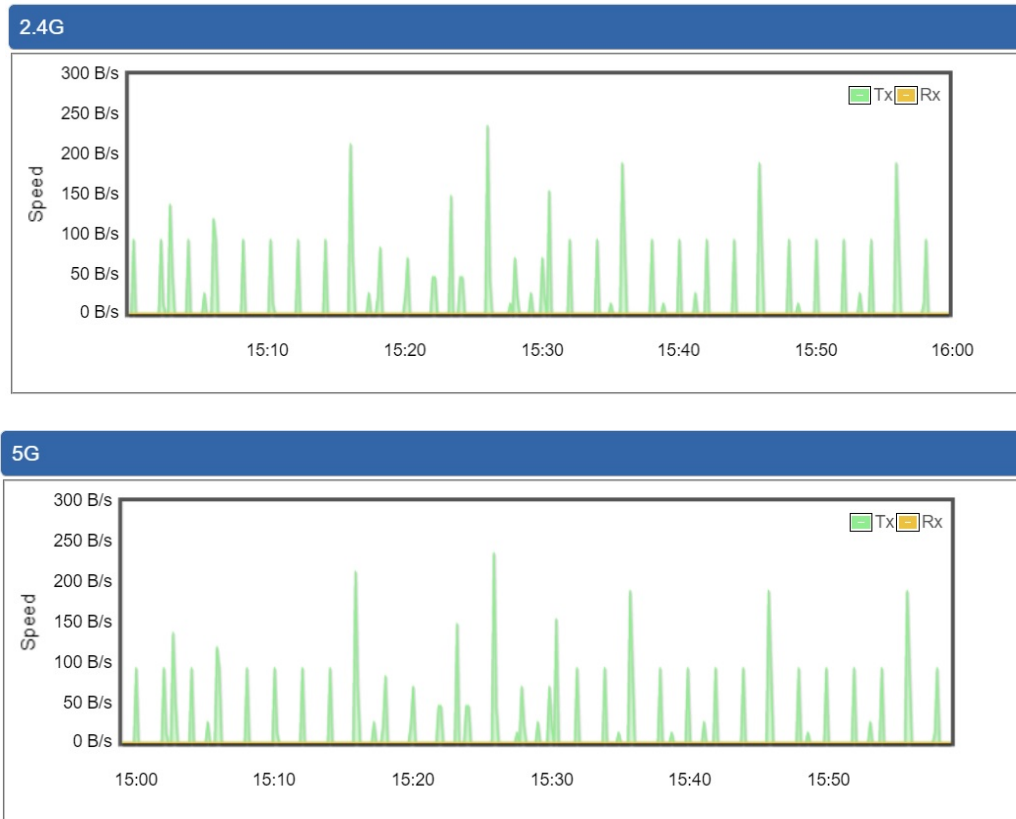


Figure 4-10-6: Wi-Fi Statistics

4.10.6 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](#).

Client List				
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. 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	<input type="text" value="admin"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Apply Settings
Cancel Changes

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.

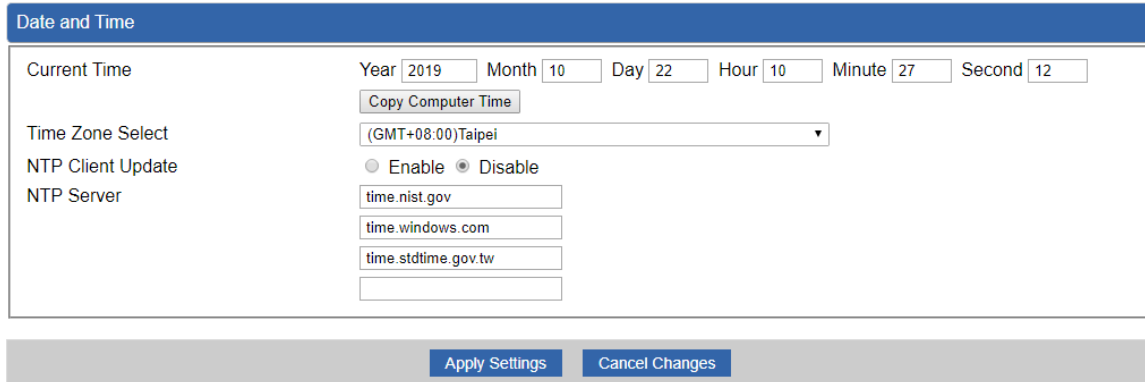
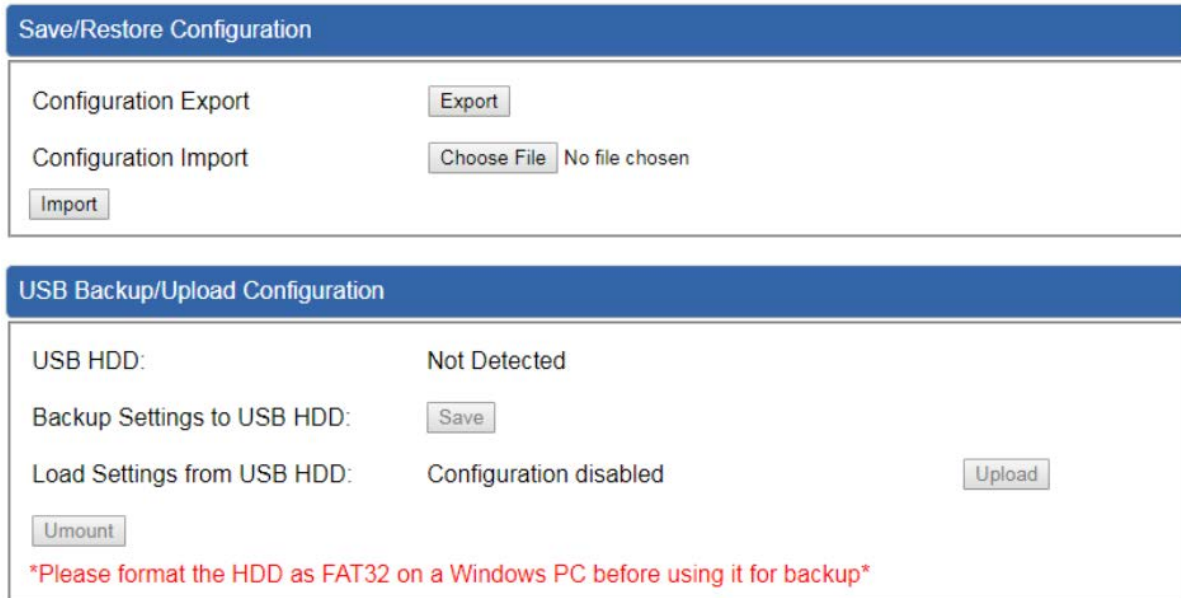


Figure 4-11-3: Date and Time

Object	Description
Current Time	Show the current time. 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:


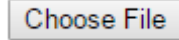



The screenshot shows two main sections:




- Save/Restore Configuration:** Contains 'Configuration Export' with an 'Export' button, and 'Configuration Import' with a 'Choose File' button (displaying 'No file chosen') and an 'Import' button.
- USB Backup/Upload Configuration:** Shows 'USB HDD: Not Detected', 'Backup Settings to USB HDD' with a 'Save' button, and 'Load Settings from USB HDD: Configuration disabled' with an 'Upload' button. There is also an 'Unmount' button and a red warning note: '*Please format the HDD as FAT32 on a Windows PC before using it for backup*'

Figure 4-11-4: Saving/Restoring Configuration

■ Save Setting to PC

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

■ Save Setting to USB Storage

Object	Description
USB Storage	The status of USB storage.
Backup Settings to USB Storage	Press the  button to save setting file to USB storage.
Load Settings from USB Storage	Press the  button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the LoRaWAN Gateway, please press the  button first.

4.11.4 Upgrading Firmware

This page provides the firmware upgrade function as shown in [Figure 4-11-5](#)

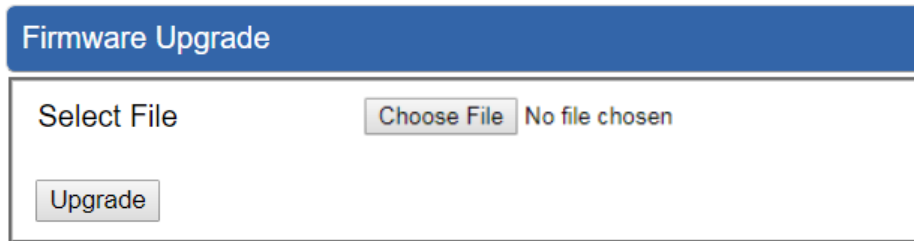


Figure 4-11-5: Firmware Upgrade

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 <input type="button" value="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 : (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](#)

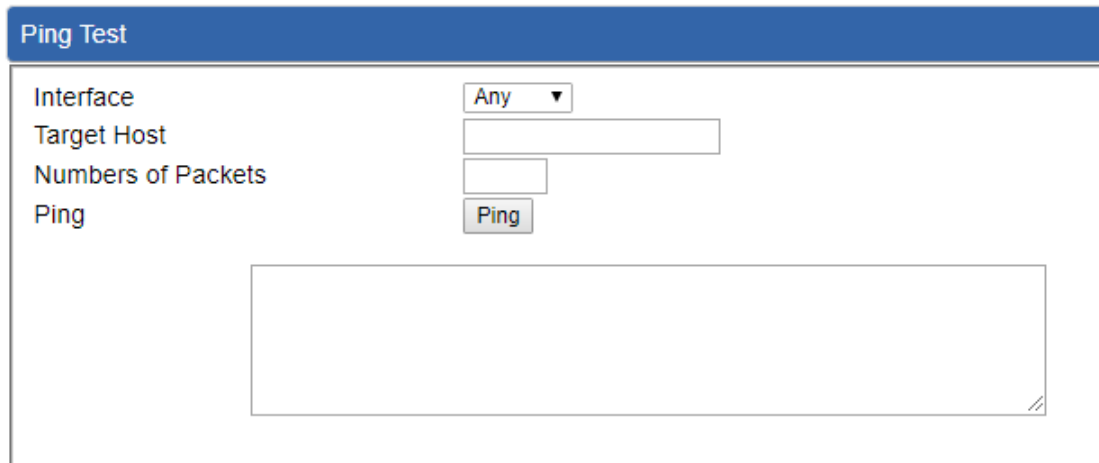


Figure 4-11-7: Diagnostics

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.



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.

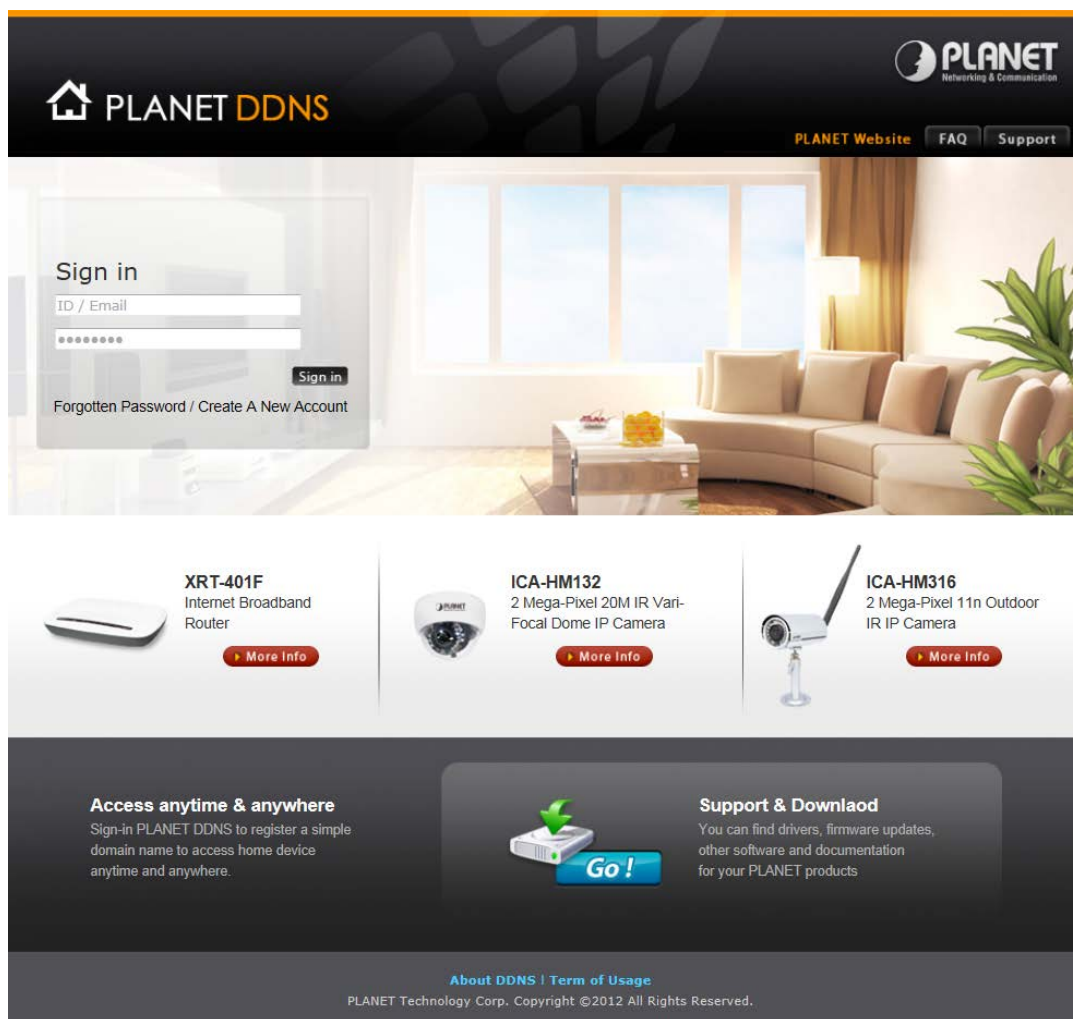
Appendix A: DDNS Application

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.



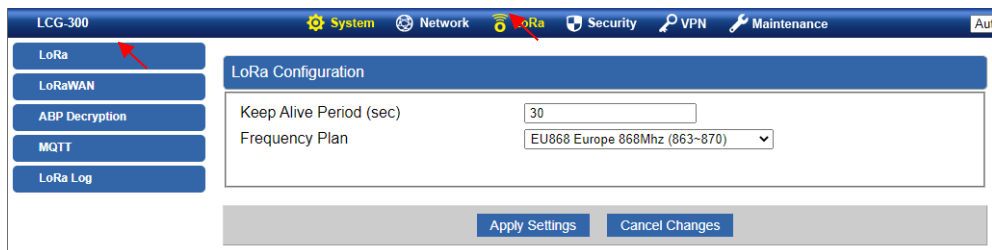
The screenshot displays the PLANET DDNS website. At the top, there is a navigation bar with the PLANET logo and links for 'PLANET Website', 'FAQ', and 'Support'. The main content area features a 'Sign in' form with fields for 'ID / Email' and a password, a 'Sign in' button, and links for 'Forgotten Password / Create A New Account'. Below the form, three product cards are shown: 'XRT-401F Internet Broadband Router', 'ICA-HM132 2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera', and 'ICA-HM316 2 Mega-Pixel 11m Outdoor IR IP Camera', each with a 'More Info' button. At the bottom, there are two promotional boxes: 'Access anytime & anywhere' and 'Support & Download'. The footer contains the text 'About DDNS | Term of Usage' and 'PLANET Technology Corp. Copyright ©2012 All Rights Reserved.'

Appendix B: LoRaWAN Settings

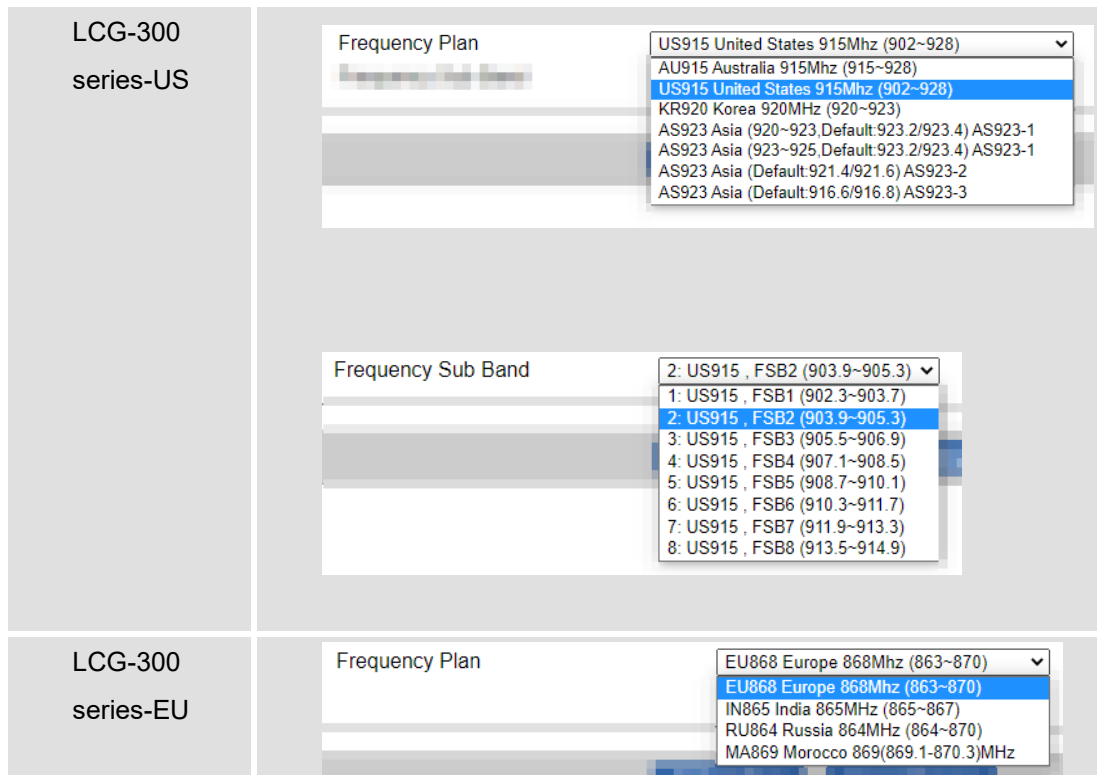
Setting Up to Connect with TTN (The Things Network)

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.



- c. 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.)



2. LoRaWAN Setting

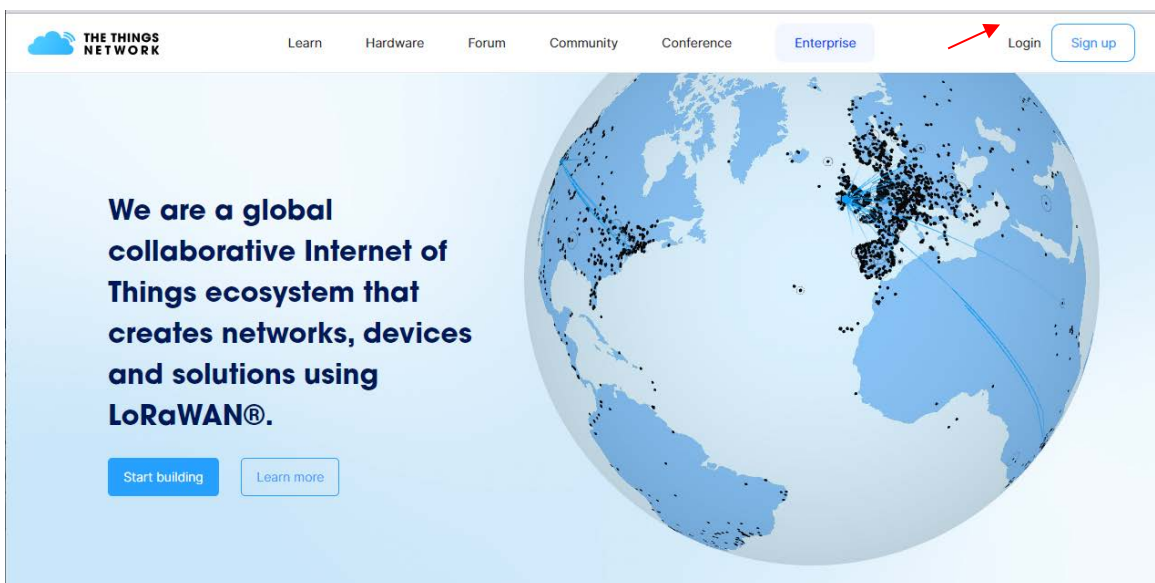
Click **LoRaWAN** and input the related data.

LoRa	LoRa Configuration														
LoRaWAN															
ABP Decryption															
MQTT															
LoRa Log															
<table border="1" style="width: 100%;"> <tr> <td>LoRaWAN Server Mode</td> <td>LoRaWAN UDP</td> </tr> <tr> <td>Email</td> <td><input type="text"/></td> </tr> <tr> <td>Gateway ID</td> <td><input type="text"/></td> </tr> <tr> <td>Server Provider</td> <td>The Things of Network V3</td> </tr> <tr> <td>Server Address</td> <td>eu1.cloud.thethings.network</td> </tr> <tr> <td>Uplink Port</td> <td>1700</td> </tr> <tr> <td>Downlink Port</td> <td>1700</td> </tr> </table>		LoRaWAN Server Mode	LoRaWAN UDP	Email	<input type="text"/>	Gateway ID	<input type="text"/>	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	<input type="text"/>														
Gateway ID	<input type="text"/>														
Server Provider	The Things of Network V3														
Server Address	eu1.cloud.thethings.network														
Uplink Port	1700														
Downlink Port	1700														
<input type="button" value="Apply Settings"/> <input type="button" value="Cancel Changes"/>															

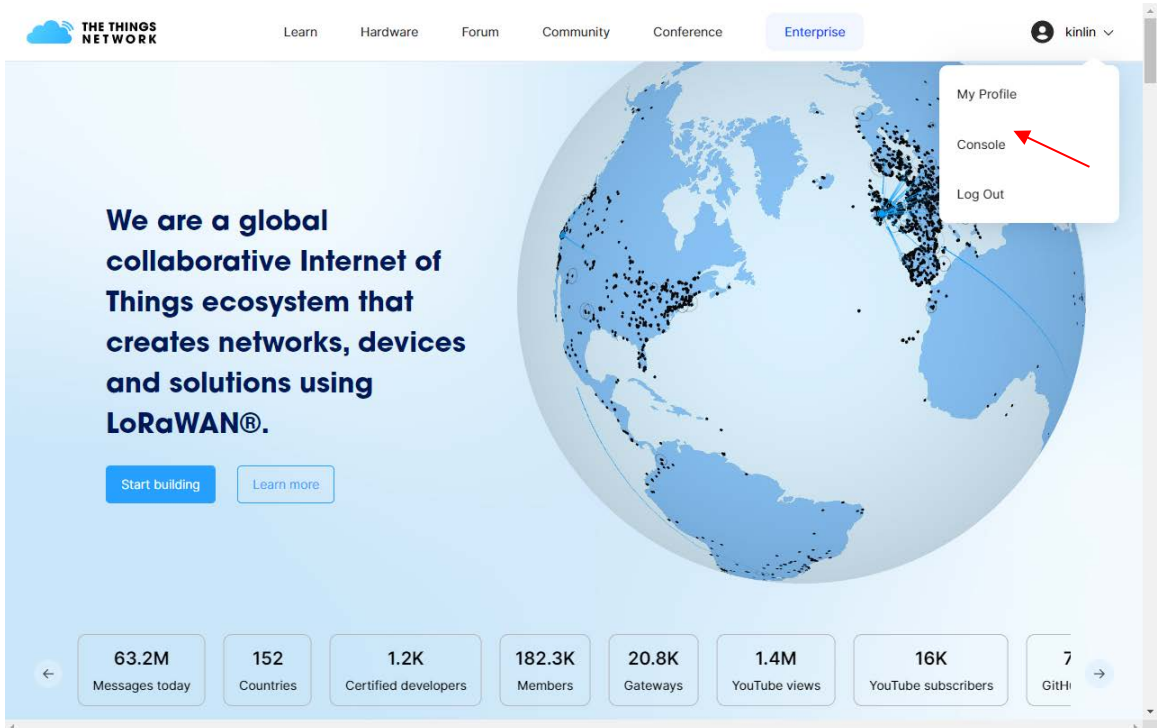
LoRaWAN Server Mode	LoRaWAN UDP
Email	kinlin.planet@gmail.com (TTN account)
Gateway ID	a8f7e01234567895
Server Provider	The Things of Network V3
Server Address	eu1.cloud.thethings.network nam1.cloud.thethings.network au1.cloud.thethings.network
Uplink Port	1700
Downlink Port	1700

The Setting Up of the Things Network

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

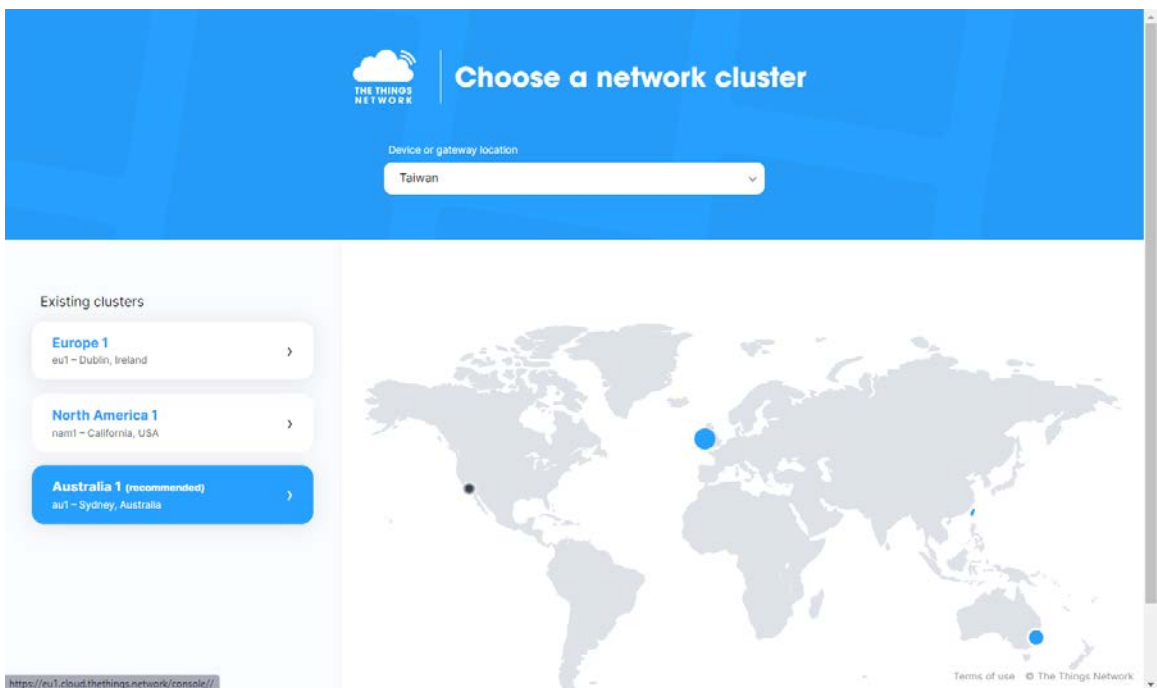


a. After logging in, select “console” under “account” shown in the upper right corner of the page.



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

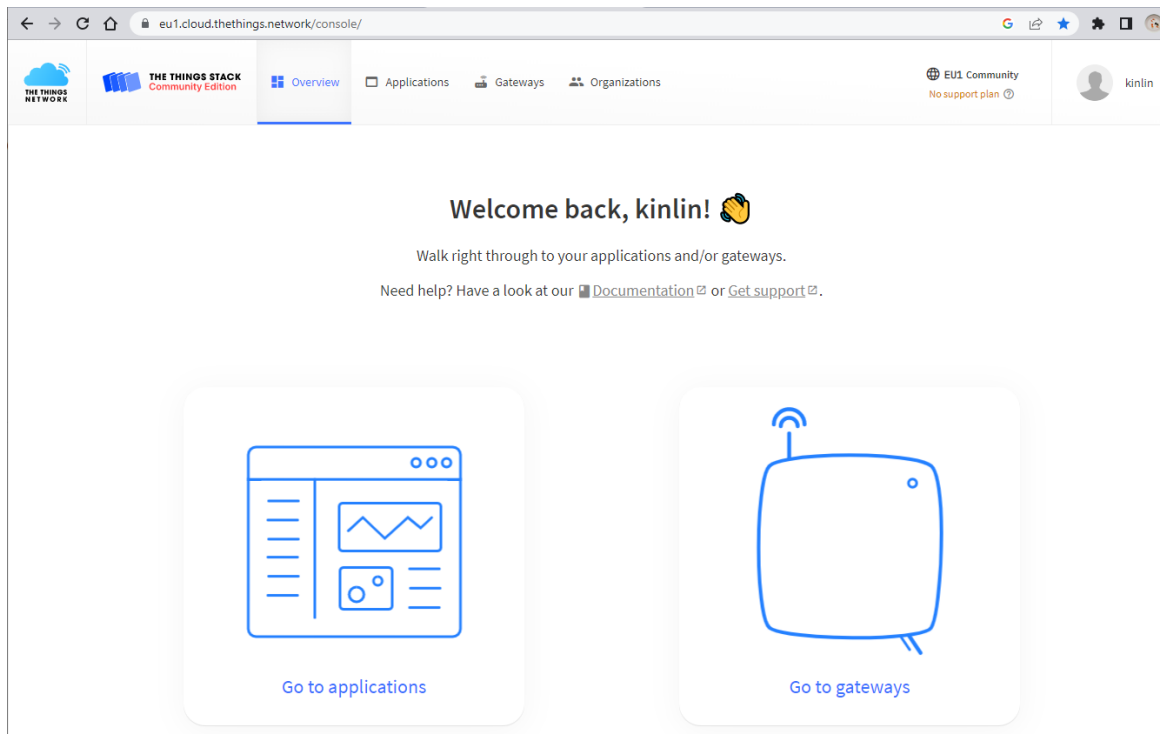
(The test case: Europe 1)



c. The console page

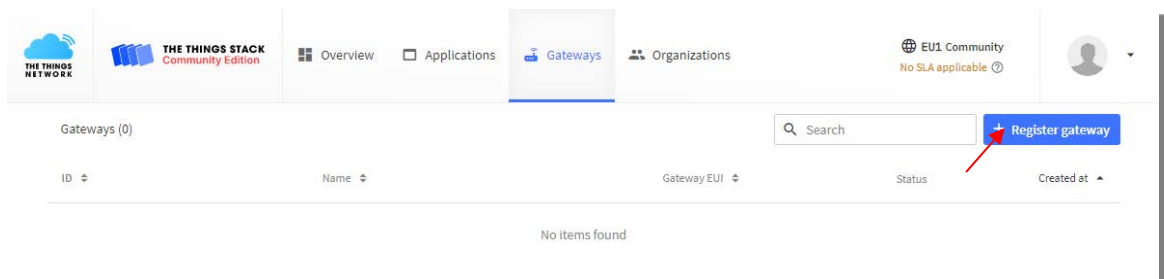
“Go to application” is for setting LoRa node and LoRa sensor.

“Go to gateways” is for setting LoRaWAN gateway.



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](#).

Gateway EUI [Ⓢ]

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 ⓘ *

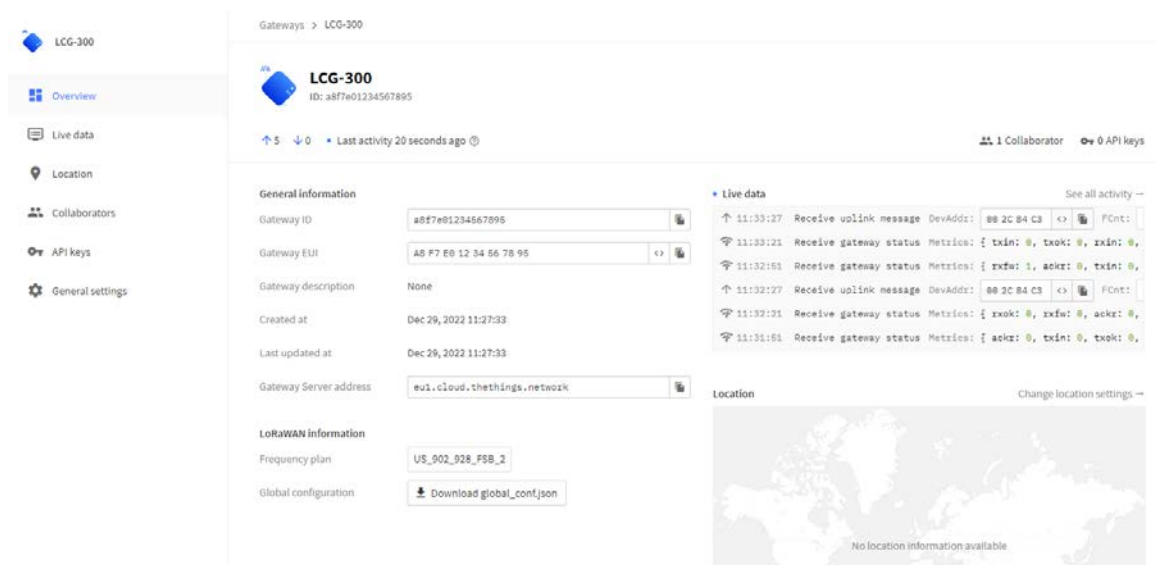
Select... | v

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.



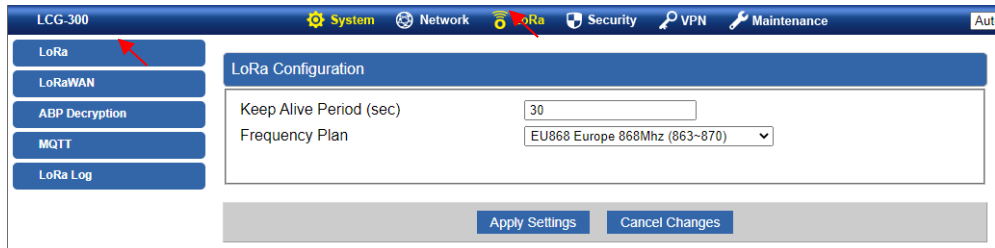
The screenshot shows the TTN Gateway configuration page for a gateway named "LCG-300" with ID "a8f7e01234567895". The page is divided into several sections:

- 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:** A list of recent events including "Receive uplink message" and "Receive gateway status" with associated timestamps and metrics.
- Location:** A map showing the gateway's location, currently displaying "No location information available".

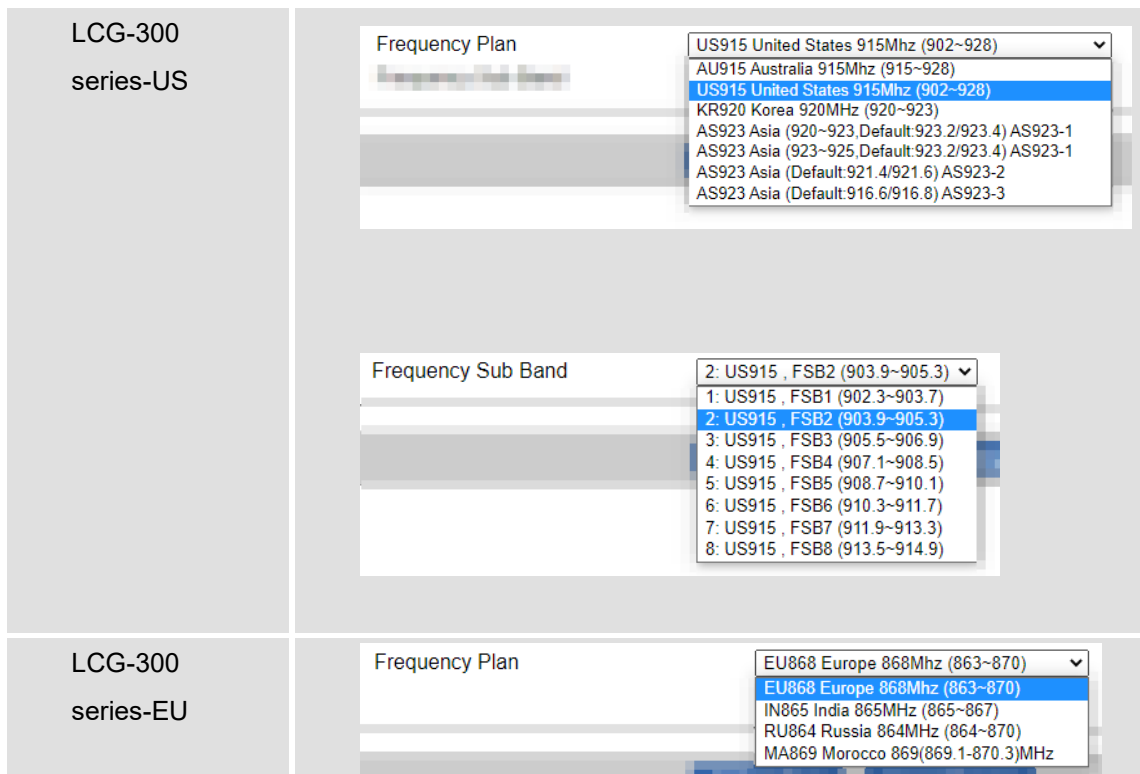
Setting Up to Connect with Built-in ABP Decoder

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.

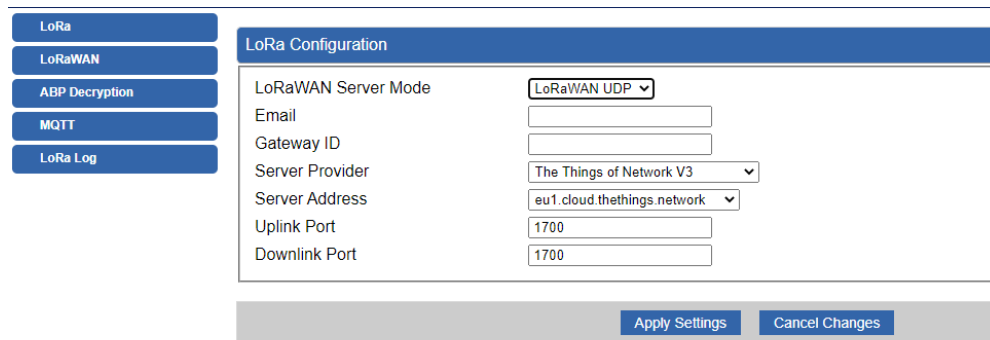


- c. Select the **Frequency Plan** for your local area. Some frequency bands support **Frequency Sub Band**.
(In this case [LCG-300-US], select “US915” for frequency band and “US915 and FSB2” for frequency sub band.)



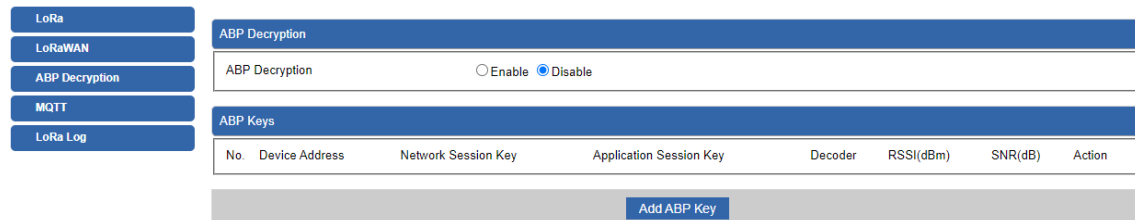
2. LoRaWAN Setting

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

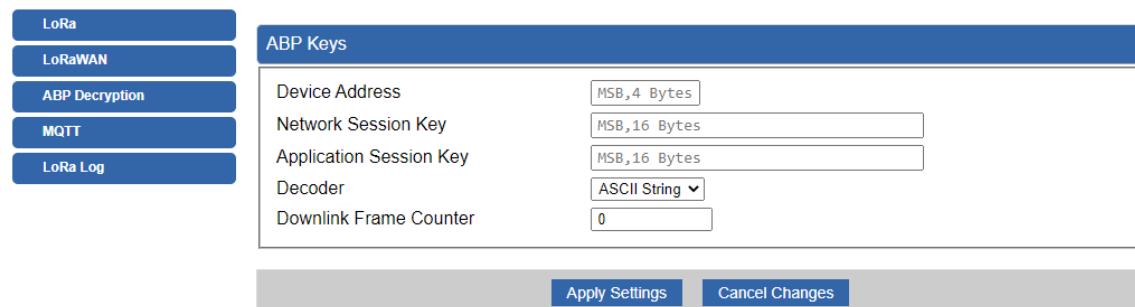


LoRaWAN Server Mode	LoRaWAN UDP
Email	kinlin.planet@gmail.com
Gateway ID	a8f7e01234567895
Server Provider	Built-in ABP Decoder
Uplink Port	1700
Downlink Port	1700

3. ABP Decryption



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

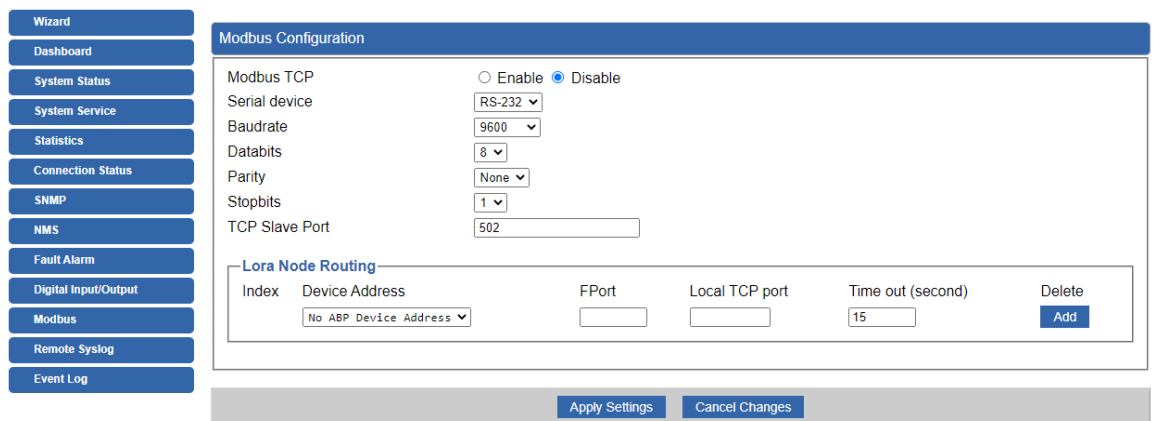


Device Address	*B0508566
Network Session Key	*A04106056144579AD82F86DF0EF42A2F
Application Session Key	*A4A197D52E8BFA3AC3DD4D1F303CF54F
Decoder	ACSII String
Downlink Frame Counter	*0

***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.



- 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

Save

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	? <input type="checkbox"/>
ADR Mode	? <input type="checkbox"/>

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	<input checked="" type="checkbox"/>
Baud Rate	9600
Data Bit	8 bits
Stop Bit	1 bits
Parity	None
Modbus RS485 bridge LoRaWAN	<input checked="" type="checkbox"/>
Port	2