

User's Manual



Gateway

ICG-2515-NR Series



www.PLANET.com.tw





Copyright

Copyright (C) 2021 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

The is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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 5G NR Cellular Gateway Model: ICG-2515-NR and ICG-2515W-NR Rev.: 1.0 (November, 2021) Part No. EM-ICG-2515-NR series_v1.0



Table of Contents

Chapter	1. Produc	ct Introduction	7
1.1	Package C	Contents	8
1.3	Overview.		9
1.4	Features		14
1.5	Product Sp	pecifications	17
Chapter	2. Hardw	are Introduction	21
2.1	Physical D	escriptions	21
2.2	Hardware	Installation	23
Chapter	3. Prepar	ration	27
3.1	Requireme	ents	27
3.2	Setting TC	P/IP on your PC	28
3.3	Planet Sm	art Discovery Utility	35
Chapter	4. Web-b	ased Management	37
4.1	Introductio	n	37
4.2	Logging in	to the Cellular Gateway	37
4.3	Main Web	Page	
4.4	System		40
	4.4.1	Setup Wizard	42
	4.4.2	Dashboard	49
	4.4.3	System Status	51
	4.4.5	System Service	53
	4.4.7	Statistics	54
	4.4.8	Connection Status	55
	4.4.9	High Availability	56
	4.4.10	RADIUS	57
	4.4.11	Captive Portal	58
	4.4.12	SNMP	59
	4.4.13	NMS	60
	4.4.14	Fault Alarm	62
	4.4.15	Digital Input / Output	63
	4.4.16	Remote Syslog	65
4.5	Network		66
	4.5.1	Priority	67
	4.5.2	WAN	68



	4.5.3	WAN Advanced	69
	4.5.4	LAN Setup	70
	4.5.5	Multi-Subnet	71
	4.5.6	Routing	71
	4.5.7	WAN IPv6 Setting	73
	4.5.8	DHCP	73
	4.5.9	DDNS	75
	4.5.10	MAC Address Clone	77
4.6	Cellular		78
	4.6.1	LTE/NR Configuration	79
	4.6.2	LTE/NR Advanced	80
	4.6.3	LTE/NR Status	82
	4.6.4	LTE/NR Statistics	82
	4.6.6	GPS	83
	4.6.7	SMS	83
4.7	Security		84
	4.7.1	Firewall	85
	4.7.2	MAC Filtering	87
	4.7.3	IP Filtering	88
	4.7.5	Web Filtering	90
	4.7.7	Port Forwarding	91
	4.7.8	DMZ	92
4.8	Virtual Priv	vate Network	93
	4.8.1	IPSec	94
	4.8.2	GRE	97
	4.8.3	PPTP Server	99
	4.8.4	L2TP Server	101
	4.8.6	SSL VPN	103
	4.8.8	VPN Connection	104
4.9	AP Contro	ıl	105
	4.9.1	Preference	106
	4.9.2	AP Search	106
	4.9.4	AP Management	107
	4.9.5	AP Group Management	108
	4.9.6	SSID Profile	109
	4.9.8	Radio 2.4G Profile	110
	4.9.10	Radio 5G Profile	111
	4.9.11	Statistics AP Status	112
	4.9.12	Statistics Active Clients	112
	4.9.14	Map It	113



4.9.16	Upload Map	
4.10 Wirele	SS	
4.10.1	2.4G WiFi	
4.10.2	5G WiFi	
4.10.3	MAC ACL	
4.10.4	WiFi Advanced	
4.10.5	WiFi Statistics	
4.10.6	Connection Status	121
4.11 Mainte	enance	
4.11.1	Administrator	
4.11.2	Date and Time	
4.11.3	Saving/Restoring Configuration	
4.11.4	Upgrading Firmware	
4.11.5	Reboot / Reset	
4.11.6	Diagnostics	
Appendix A: DI	DNS Application	



Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial 5G NR Cellular Gateway, ICG-2515-NR Series. The descriptions of these models are as follows:

ICG-2515-NR Industrial 5G NR Cellular Gateway with 5-Port 10/100/1000T	
ICG-2515W-NR	Industrial 5G NR Cellular Wireless Gateway with 5-Port 10/100/1000T

"Cellular Gateway" mentioned in the manual refers to the above models.





1.1 Package Contents

The package should contain the following:

- Industrial 5G NR Cellular Gateway x 1
- Quick installation guide x 1
- PLANET CloudViewer QIG x1
- Wall-mount plate w/screw x 1 set
- RJ45 dust cap x 6
- 5G NR antenna x 4
- 5G NR antenna extension with magnetic base x 4
- Dual band Wi-Fi antenna x 2 (ICG-2515W-NR only
- Antenna dust cap x 4 (ICG-2515 W-NR x 6)



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



1.3 Overview

Powerful 5G NR and Wi-Fi 6 Industrial Networky Solution

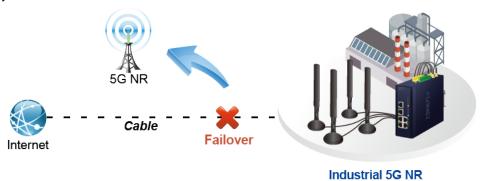
PLANET ICG-2515-NR series is an industrial-grade wireless cellular gateway for demanding mobile applications, M2M (machine-to-machine) and IoT deployments. Upgraded to the latest cellular technology of **5G NR (new radio)**, the ICG-2515-NR series is able to provide ultra-fast broadband access with 5G cellular network. The ICG-2515-NR series also features five Ethernet ports (4 LANs and 1 WAN), **IEEE 11ax Wi-Fi** capability, serial port (RS485), DI and DO interfaces, and VPN technology bundled in a compact yet rugged metal case. It establishes a fast cellular connection between Ethernet and serial port equipped devices. The ICG-2515-NR series is an integrated 5G NR and Wi-Fi 6 solution for industrial automation, digital factory and other industrial applications.



Create an Efficient & Secure Network with Planet 5G NR and SD-WAN Solution Industrial 5G NR Cellular Wireless Gateway with 5-Port 10/100/1000T

Automatic Failover between 5G NR and Gigabit WAN

Designed with 5G NR and Gigabit Ethernet WAN interfaces, the ICG-2515-NR series ensures Internet connectivity by featuring failover functionality between 5G NR and GbE WAN. The ICG-2515-NR series provides flexibility to set priority for 5G NR or GbE WAN connection. When the main WAN interface fails, the secondary WAN interface will automatically back up the connection to ensure always-on connectivity.



Cellular Gateway



Ultra-Fast Speed 4G/5G Network*

The ICG-2515-NR series supports 5G NR DL 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. The ICG-2515-NR series 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.

Up to download speed 2.4 Gbps



Wireless 11ax Brings Excellent Data Link Speed

The ICG-2515-NR series 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.

Dual SIM Design

To enhance reliability, the ICG-2515-NR series is equipped with dual SIM slots that support failover and roaming over to ensure uninterrupted connectivity for mission-critical cellular communications. It provides a more flexible and easier way for users to create an instant network sharing service via 5G-NR in public places like transportations, outdoor events, etc.





GPS Included

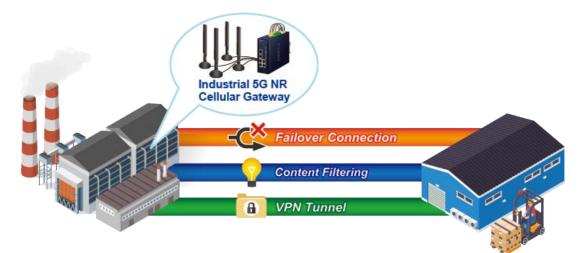
The ICG-2515-NR series is equipped with (global positioning system) feature. It adapts 5G-NR technology to incorporate multiple global navigation systems (GPS/GLONASS/BeiDou/Galileo/QZSS). It helps to position location of cellular gateway based on a network of satellites that continuously transmits necessary data. More signals transmitted from more satellites can triangulate its location on the ground, meaning any location can be easily tracked.



GNSS Positioning

Ideal High-Availability VPN Security Cellular gateway Solution for Industrial Environment

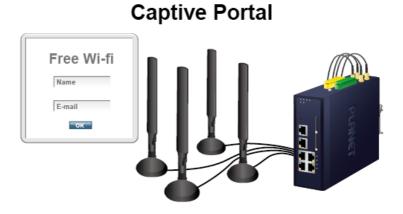
The ICG-2515-NR series provides complete data security and privacy for accessing and exchanging the most sensitive data, built-in IPSec VPN function with DES/3DES/AES encryption and MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication, and GRE, SSL, PPTP and L2TP server mechanism. The full VPN capability in the ICG-2515-NR series makes the connection secure, more flexible, and more capable.





Wi-Fi Deployments and Authentication with Simplified Management

The ICG-2515-NR series also provides a built-in AP Controller, Captive Portal, RADIUS and a DHCP server to facilitate small and medium businesses to deploy secure employee and guest access services without any additional server. The ICG-2515-NR series can offer a secure Wi-Fi network with easy installation for your business.



Centralized Remote Control of Managed APs

The ICG-2515-NR series provides centralized management of PLANET Smart AP series via a user-friendly Web GUI. It's easy to configure AP for the wireless SSID, radio band and security settings. With a four-step configuration process, wireless profiles for different purposes can be simultaneously delivered to multiple APs or AP groups to minimize deployment time, effort and cost.





For example, to configure multiple Smart APs of the same model, the ICG-2515-NR series allows clustering them to a managed group for unified management. According to requirements, wireless APs can be flexibly expanded or removed from a wireless AP group at any time. The AP cluster benefits bulk provision and bulk firmware upgrade through single entry point instead of having to configure settings in each of them separately.



Simplified Cluster Management with 4 Steps

Excellent Ability in Threat Defense

The ICG-2515-NR 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 ICG-2515-NR series is equipped with HTTPS web and SNMP management interfaces. With the built-in web-based management interface, the ICG-2515-NR series offers an easy-to-use, platform independent management and configuration facility. The ICG-2515-NR series supports SNMP and it can be managed via any management software based on the standard SNMP protocol.



1.4 Features

Key Features

- Global 5G NR (NSA/SA)/4G LTE network with dual SIM design for cellular network redundancy
- Automatic failover between 5G NR and Gigabit WAN
- Complies with IEEE 802.11ax and IEEE 802.11a/b/g/n/ac standards (ICG-2515W-NR only)
- 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
- High Availability, AP Controller, Captive Portal and RADIUS
- 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
- 4 x 5G NR antennas
- 2 x SIM card slots
- 1 x serial console port (RS485)
- 1 x reset button

Cellular Interface

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

RF Interface Characteristics (ICG-2515W-NR 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



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 for Ethernet WANs
- Auto-failover between Ethernet WANs and cellular network
- High Availability
- Captive Portal
- RADIUS Server/Client
- 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



1.5 Product Specifications

Models	ICG-2515W-NR	ICG-2515-NR	
Hardware Specificati	ions		
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		
SIM Interface	2 SIM card slots with mini SIM card tra	у	
Cellular Antenna	5 dBi external antennas with SMA con	nectors for 5G-NR	
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	0.8 kg	
Power Requirements	9~54V DC, 1.5A	9~54V DC, 0.5A	
Power Consumption	10 W / 34.12 BTU	6.16 watts/ 21.02 BTU	
Power Consumption10 W / 34.12 BTUSystem: P1 (Green), P2 (Green) Alarm (Red), I/O (Red)Ethernet Interfaces (Ports 1-4 WAN Port): 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber)Cellular SIM: SIM1 and SIM2 (Green) 4 levels (Green)		System: P1 (Green), P2 (Green) Alarm (Red), I/O (Red) Ethernet Interfaces (Ports 1-4 and WAN Port): 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber) Cellular SIM: SIM1 and SIM2 (Green) Cellular signal: 4 levels (Green)	





	2.40	G(Green), 5G(Green)	
Multi Band Supports			
5G NR	n1/n2/n	3/n5/n7/n8/n12/n20/n25/n28/n3	38/n40/n41/n48/n66/n71/n77/n78/n79
LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29/B30/ B32/B46/B66/B71		
LTE-TDD	B34/B38/B39/B40/B41/B42/B43/B48		
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+		
Wireless			
Standard)2.11a/n/ac/ax 5GHz)2.11g/b/n/ax 2.4GHz	
Band Mode	2.4G &	5G concurrent mode	
Frequency Range	2.4GHz 5GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz 5.15GHz ~5.875GHz	
	ЭĞПZ		
	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13	
Operating Channels	5GHz	America FCC: 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 will vary in different countries according to their regulations.	
Channel Width	20MHz,	40MHz, 80MHz	
Data Transmission Rates	1200 MI	it: 600 Mbps* for 2.4 GHz and ops* for 5 GHz :: 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.			
	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			
Transmission Power	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			
	WEP (64/128-bit) encryption security			
Enorumtion Coourity	WPA / WPA2 (TKIP/AES)			
Encryption Security	WPA-PSK / WPA2-PSK (TKIP/AES) /			
	WPA3-PSK (TKIP/AES) 802.1x Authenticator			
	Wi-Fi Multimedia (WMM) Auto channel selection			
Wireless Advanced				
	Wireless output power management MAC address filtering			
Advenced Eurotiene	MAG address intering			
Advanced Functions				
	 IPSec/Remote Server (Net-to-Net GRE 	ι, ποsτ-το-inet)		
VPN				
VPN				
VPN Tunnels	 SSL Server/Client (Open VPN) Max. 60 			
VPN Throughput	Max. 60Mbps			
Encryption Methods		encrypting		
Authentication		DES, 3DES, AES or AES-128/192/256 encrypting MD5/SHA-1/SHA-256/SHA-384/SHA-512 authentication algorithm		
Methods				
Management				
Basic Management	Web browser			
Interfaces	SNMP v1, v2c			



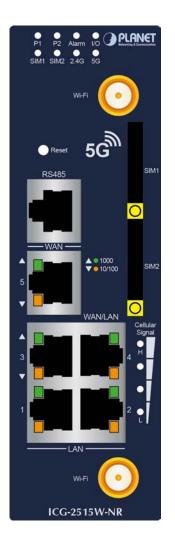
	PLANET Smart Discovery utility and NMS controller supported
Secure Management Interfaces	SSHv2, TLSv1.2, SNMP v3
System Log	System Event Log
Others	Setup wizard Dashboard System status/service Statistics Connection status Auto reboot Diagnostics
Standards Conforma	nce
Regulatory Compliance	CE, FCC
Environment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

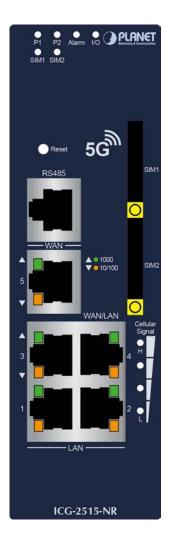


Chapter 2. Hardware Introduction

2.1 Physical Descriptions

Front View







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	ights to indicate that power or port has failed.	
I/O	Red	Lights to indicate that power or port has failed or DI has event.	
SIM1	Green	Lights to indicate the SIM1 is connecting successfully.	
SIM2	Green	Lights to indicate the SIM2 is connecting successfully.	
2.4G	Green	Lights up when 2.4G Wi-Fi service is enabled (ICG-2515W-NR only)	
5G	Green	Lights up when 5G Wi-Fi service is enabled (ICG-2515W-NR only)	

LAN Per 10/100/1000Mbps port (Port-1 to Port-4)

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

WAN Per 10/100/1000Mbps port (Port-5)

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



2.2 Hardware Installation

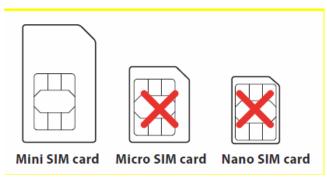
Refer to the illustration and follow the simple steps below to quickly install your Cellular Gateway.

2.2.1 SIM Card Installation

A. Insert an ejector pin into the yellow button next to the tray to loosen the tray.



- B. Pull out the tray gently from the tray slot. Place the SIM card on the tray with the gold-colored contacts facing upwards.
- C. Insert the tray back into the tray slot..
- A mini SIM card with 5G NR and 4G LTE subscription





2.2.2 5G NR Antenna Installation

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

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



2.2.3 Wi-Fi Antenna Installation

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

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





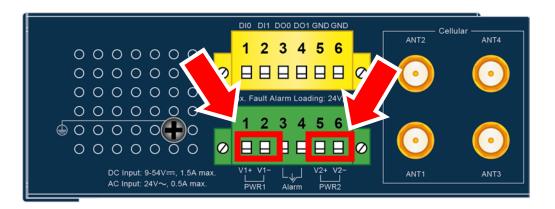
3.4 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of Cellular 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.

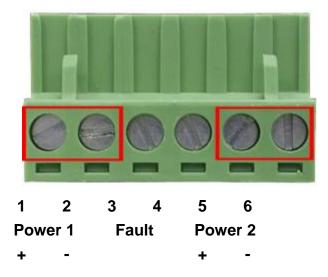
1. Insert positive and negative DC power wires into contacts 1 and 2 for POWER 1, or 5 and 6 for POWER 2.





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

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







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

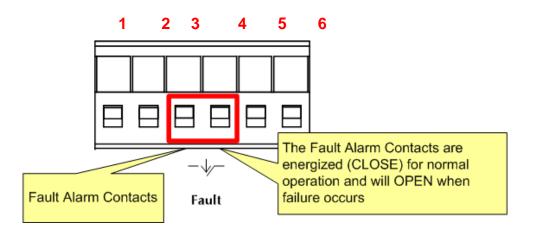
CAUTION PWR1 and PWR2 must provide the **same DC voltage** while operating with dual power input.

3.5 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 CONVERED UNDER WARRANTY.

3.6 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 Cellular 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



Insert the wires into 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: IE / Firefox / Chrome.



3.2 Setting TCP/IP on your PC

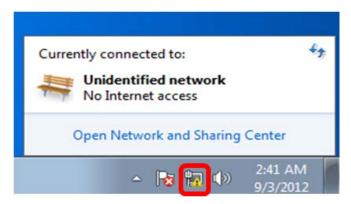
The default IP address of the cellular gateway is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN cellular gateway

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

Windows 7/8

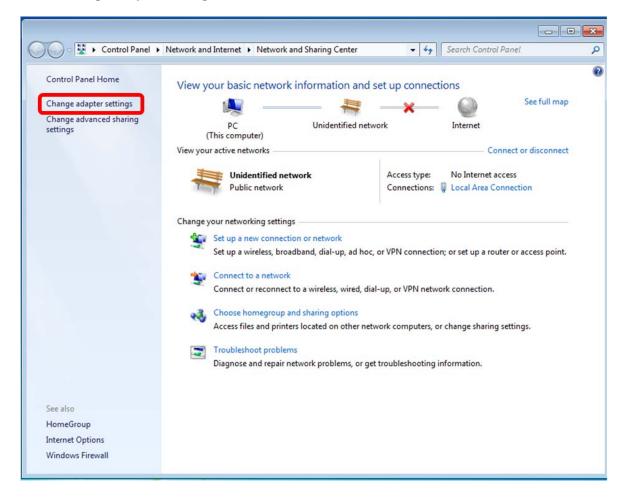
If you are using Windows 7/8, please refer to the following:

1. Click on the network icon from the right side of the taskbar and then click on "Open Network and Sharing Center".





2. Click "Change adapter settings".



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

Intel(R) PRO/100	9	Disable
		Status
		Diagnose
	۲	Bridge Connections
		Create Shortcut
	0	Delete
	3	Rename
	8	Properties



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

Intel(R) PRO	1000 MT Network	Connection	1
		6	Configure
his connection use	s the following iten	ns:	Coningure
 ✓ Internet Pre ✓ Unk-Layer ✓ Link-Layer Install 	otocol Version 6 (T otocol Version 4 (T Topology Discove	CP/IPv6) CP/IPv4) ny Mapper I/	/O Driver
wide area networ	trol Protocol/Interr k protocol that pro erconnected netw	vides comm	



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

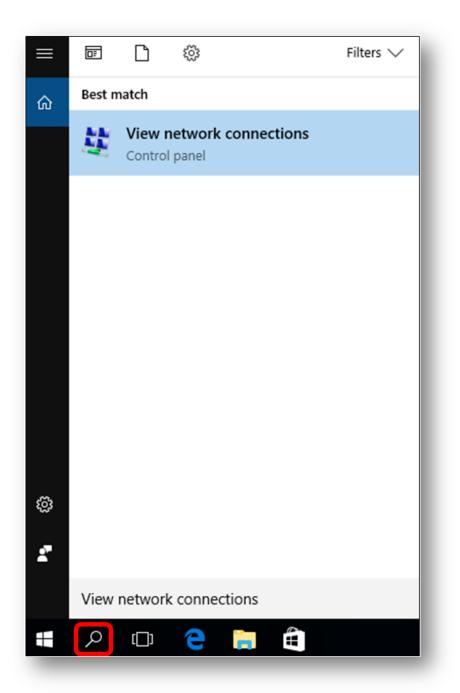
ou can get IP settings assigned auto pports this capability. Otherwise, yo Iministrator for the appropriate IP so	u need to			
Obtain an IP address automatica	_			
Use the following IP address:				
<u>I</u> P address:				
S <u>u</u> bnet mask:				
<u>D</u> efault gateway:				
Obtain DNS server address autor	matically	1		
Use the following DNS server ad		-		
Preferred DNS server:				
Alternate DNS server:				
Validate settings upon exit			Adv	anced



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.

Local Area Conne Unidentified netw		
Intel(R) PRO/1000	0	Disable
		Status
		Diagnose
	۲	Bridge Connections
		Create Shortcut
	0	Delete
	۲	Rename
	0	Properties

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

Intel(R) PRO.	/1000 MT Network	Connection
		Configure
his connection use	es the following item	ns:
Client for M	Aicrosoft Networks	
QoS Pack	et Scheduler	
🗹 具 File and Pr	inter Sharing for Mi	crosoft Networks
 Internet Pr 	otocol Version 6 (T)	CP/IPv6)
🗹 🔺 Internet Pr	otocol Version 4 (T	CP/IPv4)
🗹 🔺 Link-Layer	Topology Discover	ry Mapper I/O Driver
Link-Layer	Topology Discover	ry Responder
Install	Uninstall	Properties
I ISLdII		
Description	and Destand (Internet	at Destaural The default
Description Transmission Cor		net Protocol. The default
Description Transmission Cor wide area networ		vides communication





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

Alternate Configuration (ou can get IP settings assigned auto supports this capability. Otherwise, y	ou need to			ork
dministrator for the appropriate IP :	_			
O Use the following IP address:				
IP address:				
S <u>u</u> bnet mask:				
Default gateway:				
 Obtain DNS server address auto Use the following DNS server address automatic server and the following DNS server address automatic server and the following DNS server address automatic server address automat]		
Preferred DNS server:				
<u>A</u> lternate DNS server:				
Validate settings upon exit			Adva	anced
		ОК		Cancel



3.3 Planet Smart Discovery Utility

For easily listing the cellular 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.

🍠 PLANET Smart D	-							_		×
File Option Help										
		U Refres	sh	🖹 Exit			9		ANG & Commun	
MAC Address	Device Name	Version	DevicelP	NewPassword	IP Address	NetMask	Gateway	Descript	ion	
				J						
Select Adapter : 10.1.0.96 (F8:32:E4:CD:C5:8A) Control Packet Force Broadcast Update Device Update Multi Update All Connect to Device										
Device		Mes	sage							

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:

9	🐓 PLANET Smart Discovery Lite							_3		×	
Fi	le Option Help										
			O Refre	sh	🖹 Exit			9		RAN ng & Commu	
	MAC Address	Device Name	Version	DevicelP	NewPassword	IP Address	NetMask	Gateway	Descript	tion	
1	A8-F7-E0-00-30-55	ICG-2515W-NR	v1.2102b21091	192.168.1.1		192.168.1.1	255.255.255.0	0.0.0.0	Industria	al 5G NR C	Cellular

Select Adapter : 192	.168.1.199 (B0:6E:BF:C	C:01:D8)	•	Control Packet Force Broadcast
	Update Device	Update Multi	Update All	Connect to Device
Device + ICG 2515\0/ NP /A9 E	7 E0 00 20 55) Got	Deuice Information	dono	

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



- 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 Cellular Gateway

Refer to the steps below to configure the cellular gateway:

Step 1. Connect the IT administrator's PC and cellular 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 cellular gateway is enabled. Therefore, the LAN PC will get IP from the VPN cellular 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 (ICG-2515W-NR only)** Default SSID (5G): **PLANET_5G (ICG-2515W-NR 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.



Function Menu

Figure 4-3-1: Main Web Page

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

		5
Object	lcon	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 in Figures 4-3-2 and 4-3-3.

🔅 System 🕲 Network 🛞 Cellular 🕞 Security 🎤 VPN 🏯 AP Control 🅱 Wireless 🎤 Maintenance

Object	Description
System	Provides System information of the cellular gateway
Network	Provides WAN, LAN and network configuration of the cellular gateway
Cellular	Provides Cellular configuration of the cellular gateway
Security	Provides Firewall and security configuration of the cellular gateway
VPN	Provides VPN configuration of the cellular gateway
AP Control	Provides AP Control configuration of the cellular gateway
Wireless	Provides wireless configuration of the cellular gateway (ICG-2515W-NR only)
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the cellular gateway

Figure 4-3-2: Function Menu



Figure 4-3-3: Function Button

Object	Description
C	Click the " Refresh button " to refresh the current web page.
F	Click the "Logout button" to log out the web UI of the cellular gateway



4.4 System

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

Wizard
Dashboard
System Status
System Service
Statistics
Connection Status
High Availability
RADIUS
Captive Portal
SNMP
NMS
Fault Alarm
Digital Input/Output
Remote Syslog
Event Log

Figure 4-4-1: System Menu

Object	Description
Wizard	The Wizard will guide the user to configuring the cellular
	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
High Availability	Enable/Disable High Availability on cellular gateway



RADIUS	Enable/Disable RADIUS on cellular gateway
Captive Portal	Enable/Disable Captive Portal on cellular gateway
SNMP	Display SNMP system information
NMS	Enable/Disable NMS on cellular gateway
Remote Syslog	Enable Captive Portal on cellular gateway
Event Log	Display Event Log information



Setup Wizard 4.4.1

The Wizard will guide the user to configuring the cellular 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 cellular gateway via Setup Wizard as shown in Figure 4-4-2.

	2	3	- (4)	5	6	-7
Account	LAN	Priority	WAN	Wireless	Security	Completed

Jre 4-4-2: Setup wizard

Step 1: Account Modi	fication
----------------------	----------

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

Account LAN Priority WAN Wireless Security Comple	1	_2_		-4-			-7
	Account	LAN	Priority	WAN	Wireless	Security	Completed
Jsername admin	Isername		admin				
Password			admin				

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 - Networ	rk Interface LA	N				
1	2		-4-		-6-	-7
Account	LAN	Priority	WAN	Wireless	Security	Completed
IP Address		192.168.1.1	1			
Netmask		255.255.25	5.0			
DHCP Server						
Start IP Address		192.168.1	. 100			
Maximum DHCP Us	sers	101				

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



Object	Description	
IP Address	Enter the IP address of your cellular 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.	
DHCP Server	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.	
Start IP Address	Please do not set it to the same IP address of the cellular gateway	
	By default, the maximum DHCP users are 101, which means the	
Maximum DHCP Users	cellular 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 the next step.	
Cancel	Press this button to undo any changes made locally and revert to	
Callee	previously saved values.	

Step 3: Priority Interface

The cellular gateway supports two access modes on the WAN side shown in Figure 4-4-5



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

Object	Description
	■ Auto: WAN Ethernet is first priority and second priority is NR/LTE. The default
	is Auto.
WAN Priority	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

STEP 4 - Netwo	rk Interface W/	AN				
1	2	3	-4-			-7
Account	LAN	Priority	WAN	Wireless	Security	Completed
WAN1 WAN2	LTE/NR 1	LTE/NR 2				
Connection Type		DHCP 🗸]			
⊃ Address						
Vetmask						
Default Gateway						
NS Server 1						
NS Server 2						
	Fig	ure 4-4-6: Setu	ıp Wizard – V	VAN Configura	tion	

The cellular gateway supports two access modes on the WAN side shown in Figure 4-4-6

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 cellular gateway will not accept the IP address if it is not in this format. The setup is shown in Figure 4-4-7.

WAN1 WAN2 LTE/NR 1 LTE/	NR 2		
Connection Type	Static 🗸		
IP Address	210.61.134.96		
Netmask	255.255.255.0		
Default Gateway	210.61.134.254		
DNS Server 1	8.8.8.8		
DNS Server 2			

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.		
Ormani	Press this button to undo any changes made locally and revert to		
Cancel	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.

WAN1	WAN2 LTE/NR 1	LTE/NR 2	
Connectio	on Type	DHCP 🗸	
IP Addres	S		
Netmask			
Default Ga	ateway		
DNS Serv	/er 1		
DNS Serv	ver 2		

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

Step 5: Wireless Setting

Set up the Wireless Settings as shown in Figure 4-4-9.



STEP 5 - Network Interface Wireless						
1	2		-4-			
Account	LAN	Priority	WAN	Wireless	Security	Completed
2.4G WiFi Status		Enable	O Disable			
SSID		PLANET_2.4	IG			
Hide SSID		OEnable	 Disable 			
Bandwidth		20MHz 🗸				
Channel		6 🗸				
Encryption		Open		~		
5G WiFi Status		Enable	O Disable			
SSID		PLANET_5G	;			
Hide SSID		OEnable	 Disable 			
Bandwidth		80MHz 🗸				
Channel		36 🗸]			
Encryption		Open		~		
	F	igure 4-4-9:	Setup Wiz	ard –Securi	ty Setting	

Object	Description			
2.4G 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			

Object	Description
5G Wireless Status	Allows user to enable or disable 5G WiFi
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 "
WiFi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function

Step 6: Security Setting



Set up the Security Settings as shown in Figure 4-4-10.



Object	Description		
	The SPI Firewall prevents attack and improper access to network		
SPI Firewall	resources.		
	The default configuration is enabled.		
	SYN Flood is a popular attack way. DoS and DDoS are TCP		
Block SYN Flood	protocols. Hackers like using this method to make a fake connection		
BIOCK STIN FIOOU	that involves the CPU, memory, and so on.		
	The default configuration is enabled.		
	ICMP is kind of a pack of TCP/IP; its important function is to transfer		
Block ICMP Flood	simple signal on the Internet. There are two normal attack ways		
BIOCK ICMIP FIOOD	which hackers like to use, Ping of Death and Smurf attack.		
	The default configuration is disabled.		
	Enable the function to allow the Ping access from the Internet		
Block WAN Ping	network.		
	The default configuration is disabled.		
	Enable the function to allow the web server access of the cellular		
Remote Management	gateway from the Internet network.		
	The default configuration is disabled.		



Previous

Finish

Step 5: Setup Completed

STEP 7 - Setup C	ompleted					
0	2	3	-	- 6	6	-7
Account	LAN	Priority	WAN	Wireless	Security	Completed
LAN	Enable: Static	IP: 192.168.1	.1/255.255.255	i.0		
WAN	Priority: Auto					
WAN1	Enable: DHCF	2				
WAN2	Enable: OFF					
LTE/NR 1	Enable: ON					
LTE/NR 2	Enable: ON					
2.4G WiFi	Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHz Channel: 6 Encryption: Open Hide SSID: Disable					
5G WiFi	Enable: ON SSID: PLANET_5G Bandwidth: 80MHz Channel: 36 Encryption: Open Hide SSID: Disable					
Security Settings	SPI Firewall: 0	DN .				
	Block SYN Flo	od: ON				
	Block ICMP Flo	od: OFF				
	Block WAN Pin	ig: OFF				
	Remote Manag	gement: ON				

The page will show the summary of LAN, WAN and Security settings as shown in Figure 4-4-11.

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.	
Abut Shite Shite Shite Shares	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.	
	USB port is in use.	
	USB port is not in use.	

System Information

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

LTE/NR Status

Object	Description	
SIM	SIM signal 5G 5G signal 4G 4G signal 3G 3G signal	
Download	Download data rate of SIM	
Upload	Upload data rate of SIM	
Total	Total data rate of SIM	



Wireless Status

Object		Description
RX: 0 bps	TX: 0 bps	Wireless is in use.
RX: 0 bps	TX: 0 bps	Wireless is not in use.

4.4.3 System Status

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

Model NameICG-2515W-NRFirmware Versionv1.2102b211018Current Time2021-11-12 Friday 09:12:32Running Time0 day, 00:07:57WAN1MAC AddressA8:F7:E0:87:85:58Connection TypeDHCPDisplay NameWAN1IP Address192.168.0.177Netmask255.255.255.0Default Gateway192.168.0.1MAC AddressAddress192.168.0.1LANCatego Colspan="2">Colspan="2"MAC AddressA8:F7:E0:87:65:57IP Address192.168.1.10DHCP SenviceEnableDHCP Colients101 <td< th=""><th colspan="3">Device Information</th></td<>	Device Information		
Current Time 2021-11-12 Friday 09:12:32 Running Time 0 day, 00:07:57 WAN1 MAC Address A8:F7:E0:87:85:58 Connection Type DHCP Display Name WAN1 IP Address 192.168.0.177 Netmask 255.255.255.0 Default Gateway 192.168.0.1 MAC Address A9:F7:E0:87:85:57 IP Address 192.168.0.1 MAC Address A9:F7:E0:87:85:57 IP Address 192.168.1.1 MAC Address A9:F7:E0:87:85:57 IP Address 192.168.1.1 Netmask 256.255.256.0 DHCP Start IP Address 192.168.1.100 DHCP End IP Address 192.168.1.100 DHCP End IP Address 192.168.1.200 Max DHCP Clients 101 Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	Model Name	ICG-2515W-NR	
Running Time 0 day, 00:07:57 WAN1	Firmware Version	v1.2102b211018	
WAN1 MAC Address A8: F7: E0:87:85:58 Connection Type DHCP Display Name WAN1 IP Address 192:168:0.177 Netmask 255:255:255:0 Default Gateway 192:168:0.1 IAN MAC Address A8: F7: E0:87:85:57 IP Address 192:168:0.1 MAC Address A8: F7: E0:87:85:57 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 Z4GHz WiFi Status ON SSID PLANET_2:4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	Current Time	2021-11-12 Friday 09:12:32	
MAC AddressA8:F7:E0:87:85:58Connection TypeDHCPDisplay NameVVAN1IP Address192.168.0.177Netmask255.255.255.0Default Gateway192.168.0.1IANMAC AddressA8:F7:E0:87:85:57IP Address192.168.1.1Netmask255.255.0DHCP ServiceEnableDHCP ServiceEnableDHCP Start IP Address192.168.1.200Max DHCP Clients101StatusStatusONSSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)	Running Time	0 day, 00:07:57	
Connection Type DHCP Display Name WAN1 IP Address 192.168.0.177 Netmask 255.255.255.0 Default Gateway 192.168.0.1 MAC Address A9:F7:E0:87:85:57 IP Address 192.168.1.1 MAC Address 255.255.255.0 DHCP Service Enable DHCP Service DHCP Start IP Address 192.168.1.100 DHCP End IP Address 192.168.1.200 Max DHCP Clients 101 Zume Zume Zum Zum Max DHCP Clients 0N SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	WAN1		
Display Name WAN1 IP Address 192.168.0.177 Netmask 255.255.265.0 Default Gateway 192.168.0.1 Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Colspan="2">Image: Colspan="2">Image: Colspan="2" To Colspan="2"	MAC Address	A8:F7:E0:87:85:58	
IP Address 192.168.0.177 Netmask 255.255.0 Default Gateway 192.168.0.1 IAN MAC Address MAC Address A8:F7:E0:87:85:57 IP Address 192.168.1.1 Netmask 255.255.0 DHCP Service Enable DHCP Start IP Address 192.168.1.200 Max DHCP Clients 101 Z.4GHz WiFi Status SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	Connection Type	DHCP	
Netmask255.255.255.0Default Gateway192.168.0.1LANA8:F7:E0:87:85:57IP AddressA8:F7:E0:87:85:57IP Address192.168.1.1Netmask255.255.255.0DHCP ServiceEnableDHCP Start IP Address192.168.1.100DHCP End IP Address192.168.1.200Max DHCP Clients101Z.4GHz WiFiStatusONSSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)	Display Name	WAN1	
Default Gateway 192.168.0.1 LAN	IP Address	192.168.0.177	
LAN MAC Address A8:F7:E0:87:85:57 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 Status SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	Netmask	255.255.255.0	
MAC AddressA8:F7:E0:87:85:57IP Address192.168.1.1Netmask255.255.255.0DHCP ServiceEnableDHCP Start IP Address192.168.1.100DHCP End IP Address192.168.1.200Max DHCP Clients101Z.4GHz WiFiStatusONSSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)	Default Gateway	192.168.0.1	
MAC AddressA8:F7:E0:87:85:57IP Address192.168.1.1Netmask255.255.255.0DHCP ServiceEnableDHCP Start IP Address192.168.1.100DHCP End IP Address192.168.1.200Max DHCP Clients101Z.4GHz WiFiStatusONSSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)	LAN		
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 ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
Netmask255.255.255.0DHCP ServiceEnableDHCP Start IP Address192.168.1.100DHCP End IP Address192.168.1.200Max DHCP Clients101Z.4GHz WiFiStatusStatusONSSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)			
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 PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
DHCP Start IP Address 192.168.1.100 DHCP End IP Address 192.168.1.200 Max DHCP Clients 101 2.4GHz WiFi Status SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
DHCP End IP Address 192.168.1.200 Max DHCP Clients 101 2.4GHz WiFi Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	DHCP Service	Enable	
Max DHCP Clients 101 2.4GHz WiFi ON Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
2.4GHz WiFi Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)	Max DHCP Clients	101	
Status ON SSID PLANET_2.4G Channel 6 Encryption WPA2 Personal (TKIP+AES)			
SSIDPLANET_2.4GChannel6EncryptionWPA2 Personal (TKIP+AES)	2.4GHZ WIFI		
Channel 6 Encryption WPA2 Personal (TKIP+AES)	Status	ON	
Channel 6 Encryption WPA2 Personal (TKIP+AES)	SSID	PLANET_2.4G	
	Channel		
	Encryption	WPA2 Personal (TKIP+AES)	
	MAC Address	A8:F7:E0:87:85:5C	



5GHz WiFi

SSID

Status ON PLANET_5G Channel 36 WPA2 Personal (TKIP+AES) Encryption MAC Address A8:F7:E0:87:85:5D

LTE/NR 1

Activated SIM SIM Status Operator IP Address Netmask Default Gateway Running Time Roaming

SIM1 Ready Far EasTone 10.230.118.25 255.255.255.252 10.230.118.26 00:13:06 No

Figure 4-4-13: System Status



4.4.5 System Service

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

Serv	Server Service		
#	Action	Service	Status
1	Enabled	DHCP Service	DHCP Table: 1
2	X Disabled	DDNS Service	Not enabled
3	Enabled	WAN Priority	Auto
4	Enabled	SIM Priority	Auto SIM1
5	X Disabled	LTE/NR Roaming	
6	X Disabled	Quality of Service	
7	X Disabled	High Availability	
8	X Disabled	RADIUS Service	
9	X Disabled	Captive Portal	
10	Enabled	2.4GHz WiFi	SSID: PLANET_2.4G
11	Enabled	5GHz WiFi	SSID: PLANET_5G

Sec	Secured Server Service			
#	Action	Service	Status	
1	Enabled	Cyberseurity	TLS 1.1, 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	X Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32	
6	X Disabled	IPSec VPN Server	(Active / Maximum Tunnels) 0 / 32	
7	X 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



4.4.7 Statistics

This page displays the number of packets that pass through the cellular gateway on the WAN and LAN. The statistics are shown in Figure 4-4-15.

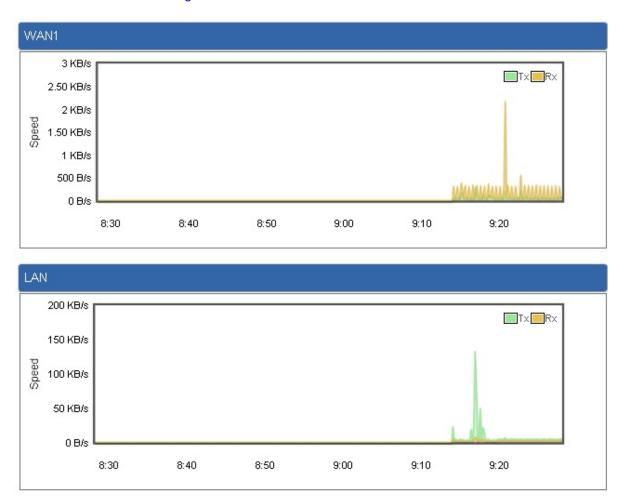


Figure 4-4-15: Statistics



4.4.8 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	
8.8.8.8		00:00:00:00:00:00	ARP Type
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



4.4.9 High Availability

High Availability (HA) is a system redundant that two cellular gateway of ICG-2515-NR series can be set up in a master/slave configuration. The master cellular gateway provides the Internet connection but, in the case of hardware or WAN connectivity failure, the slave (backup) cellular gateway automatically takes over Internet connection. It provides redundant hardware and software that make the system available despite failures. The page will show the High Availability configuration. The High Availability page is shown in Figure 4-4-17.

High Availability Configuration	
High Availability	Enable O Disable
Username	
Password	
Mode	Master 🗸
Virtual IP address	
Virtual IP Mask	
Interface	
Connected Status	

Figure 4-4-17: High Availability

Object	Description	
High Availability	Disable or enable the High Availability function.	
	The default configuration is disabled.	
Username	Create the username for the HA.	
Password	Create the password for the HA.	
Mode	Choose Master or Slave role	
Virtual IP address	Assign an IP address as a virtual IP.	
Virtual mask	Assign a mask address as a virtual mask.	
Interface	Use interface	
Connection Status	Display the HA status	



4.4.10 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting. The RADIUS Server page is shown in Figure 4-4-18.

RADIUS			
Server	Client	User Account	
RADIUS	Server Mo	de O Er	nable 🖲 Disable
Server Port		1812	

Figure 4-4-18: RADIUS Server

Object	Description
RADIUS	Disable or enable the RADIUS function.
	The default configuration is disabled.
Server Port	UDP port number for authentication

The RADIUS client page is shown in Figure 4-4-19.

RADIUS					
Server	Client User Acco	punt			
Index	Name	Client IP Address	Secret Key ✓	Description	Delete Add
(up to 16	clients)				

Figure 4-4-19: RADIUS Client

Object	Description	
Name	Describe client's name	
Client IP address	Describe client's IP address	
Secret Key	The RADIUS server and client share a secret key that is used to authenticate the messages sent between server and client.	
Description	Describe client's information	



4.4.11 Captive Portal

Captive portal service gives the ability to organize a public (or guest) Wi-Fi zone with user authorization. A captive portal is the authorization page that forcibly redirects users who connect to the public network before accessing the Internet. The Captive portal page is shown in Figure 4-4-20.

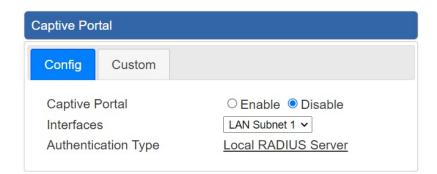


Figure 4-4-20: Captive portal

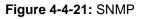
Object	Description	
Captive portal	Disable or enable the Captive portal function.	
	The default configuration is disabled.	
Interface	Choose subnet interface	
	LAN Subnet 1	
	LAN Subnet 2	
	LAN Subnet 3	
	LAN Subnet 4	
Authentication Type	Support local RADIUS server	



4.4.12 SNMP

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

SNMP	
SNMP	Enable O Disable
SNMP Versions	SNMP v1,v2c V
Read Community	public
Write Community	private
Engine ID	
SNMP v3 Security Level	AuthPRiv 🗸
SNMP v3 User Name	
SNMP v3 Auth Protocol	MD5 🗸
SNMP v3 Auth Password	
SNMP v3 Privacy Protocol	DES 🗸
SNMP v3 Privacy Password	
System Identification	
System Name	VR-300P
System Location	
System Contact	sales@planet.com.tw
	Apply Settings Cancel Changes



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
	cellular gateway
System Name	Allows entering characters for system name of the cellular gateway
System Location	Allows entering characters for system location of the cellular gateway
System Contact	Allows entering characters for system contact of the cellular gateway
Apply Settings	Press this button to save and apply changes.
Canaal Changes	Press this button to undo any changes made locally and revert to
Cancel Changes	previously saved values.



4.4.13 NMS

The ICG-2515-NR series can support both NMS controller and CloudViewer Sever for remote management. PLANET'S NMS Controller is a Network Management System 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. Any other services are not included.

NMS Configuration screens in Figure 4-4-22 appear.

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

Figure 4-4-22 NMS Configuration Page

The NMS Controller – LAN Configuration screens in Figure 4-4-23 appear.

NMS Configuration	
NMS NMS Controller IP address Authorization Status	PLANET NMS Controller - LAN Unauthorized
	Apply Settings Cancel Changes Unbind

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

Object	Description
NMS Controller IP	The IP address of NMS Controller
address	
Authorization	Indicate the authorization status of the switch to NMS Controller
Status	



The CloudViewer Server – Internet screens in Figure 4-4-24 appear.

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

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

Object	Description
• Email	The email registered on CloudViewer Server
Password	The password of your CloudViewer account
Connection Status	Indicate the status of connecting CloudViewer Server



4.4.14 Fault Alarm

Fault Alarm Control Configuration					
Fault Alarm Output					
Enable	Enabl	e			
Record	Syste	m Log	SMS		
Event	Powe	er Fail 🗌	Port Fa	ail	
Power Alarm	PWR1	I PW	R2		
	1	2	3	4	5
Port Alarm					

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

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	Controls whether Port Fail or Power Fail or both for fault detecting.
Power Alarm	Controls whether PWR1 or PWR2 or both for fault detecting.
Port Alarm	Controls which Ports or all for fault detecting.



4.4.15 Digital Input / Output

This page provides Digital Input / Output setting as shown in Figure 4-4-26.

Digita	l Input 0		Digital Input 1
Enable DEnable		Enable	Enable
DI Condition High to Lo	w 🗸	DI Condition	High to Low 🗸
Event		Event	
Description		Description	
Action System	Log SMS	Action	System Log SMS

	Digital Output 0		Digital Output 1
Enable	Enable	Enable	Enable
Action	📃 Power Fail 🗌 Port Fail 🗌 DI 0 🔤 DI 1	Action	Power Fail Port Fail DI 0 DI 1
DO Condition	High to Low 💙	DO Condition	High to Low 💙
Power Alarm	PWR1 PWR2	Power Alarm	PWR1 PWR2
	1 2 3 4 5		1 2 3 4 5
Port Fail Alarm		Port Fail Alarm	



Object	Description
Enable	Check the Enable checkbox to enable Digital Input / output function.
	Uncheck the Enable checkbox to disable Digital input / output
	function.
Condition	As Digital Input:
	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 customize message or
	issue the message from the switch.
	As Digital Output:
	Allows user to select High to Low or Low to High. This means that
	when the switch is power-failed or port-failed, then system will
	issue a High or Low signal to an external device such as an alarm.
Event Description	Allows user to set a customized message for Digital Input function
	alarming.
Action	As Digital Input:
	Allows user to record alarm message to System log, syslog or
	issues out via SNMP Trap or SMTP.
	As default SNMP Trap and SMTP are disabled, please enable
	them first if you want to issue alarm message via them.
	As Digital Output:



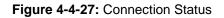
	Allows user to monitor an alarm from port failure, power failure,
	Digital Input 0 (DI 0) and Digital Input 1(DI 1) which means if
	Digital Output has detected these events, then Digitial Output
	would be triggered according to the setting of Condition.
Power Alarm	Allows user to choose which power module that needs to be
	monitored.
Port Alarm	Allows user to choose which port that needs to be monitored.



4.4.16 Remote Syslog

This page provides remote syslog setting as shown in Figure 4-4-27.

Remote Syslog		
Enable Syslog Server		
Port Destination	(1~65535)	



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



4.5 Network

The Network function provides WAN, LAN and network configuration of the cellular gateway as shown in Figure 4-5-1.

Priority
WAN
WAN Advanced
LAN
Multi-Subnet
VLAN
UPnP
Routing
RIP
OSPF
IGMP
IPv6
DHCP
DDNS
MAC Address Clone

Figure 4-5-1: Network Menu

Object	Description
Priority	Allows setting priority of WAN 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.
VLAN	The default configuration is disabled.
UPnP	Disable or enable the UPnP function.

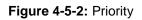


	The default configuration is disabled.
Routing	Allows setting Route.
	Disable or enable the RIP function.
RIP	The default configuration is disabled.
OSDE	Disable or enable the OSPF function.
OSPF	The default configuration is disabled.
IGMP	Disable or enable the IGMP function.
IGINIP	The default configuration is disabled.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.
MAC Address	Allows setting WAN MAC Address Clone
Clone	Allows setting WAN MAC Address Clone.

4.5.1 Priority

This page provides WAN priority setting as shown in Figure 4-5-2.

Priority	
WAN Priority	Auto



Object	Description
	• Auto: WAN Ethernet is first priority and second priority is NR/LTE. The default
	is auto.
WAN Priority	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



4.5.2 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the cellular gateway as shown in Figure 4-5-3. Here you may select the access method by clicking the item value of WAN access type.

WAN1	
Connection Type	DHCP V
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	
WAN2	
WAN	© Enable ● Disable
Connection Type	DHCP V
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	
<u> </u>	

Figure 4-5-3: WAN

Cancel Changes

Apply Settings

Object		Description
		ct the corresponding WAN Access Type for the Internet, he correct parameters from your local ISP in the fields
	which appea	ar below.
		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
WAN Access Type	Static	address, Netmask, Gateway, and DNS Server provided
		to you by your ISP.
		Each IP address entered in the fields must be in the
	Static	appropriate IP form, which are four octets separated by
		a dot (x.x.x.x). The cellular gateway will not accept the
		IP address if it is not in this format.
		IP Address
		Enter the IP address assigned by your ISP.
		Netmask



Object		Description
		Enter the Subnet Mask assigned by your ISP.
		Gateway
		Enter the Gateway assigned by your ISP.
		DNS Server
		The DNS server information will be supplied by your
		ISP.
	DUOD	Select DHCP Client to obtain IP Address information
	DHCP	automatically from your ISP.



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

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 cellular gateway as shown in Figure 4-5-4. Here you may change the setting for Load Balance Weight, Detect Interval, Detect Link Up Threshold, etc...

WAN1	
Load Balance Weight External Connection Detection	3 ▼ ● Enable ● Disable
Detect Interval	5 Seconds
Detect Link Up Threshold	8 Time(s)
Detect Link Down Threshold	3 Time(s)
Custom Detect Host 1	8.8.8.8
Custom Detect Host 2	208.67.222.222
WAN2	
Load Balance Weight	2 🔻
External Connection Detection	Enable Disable
Detect Interval	5 Seconds
Detect Link Up Threshold	8 Time(s)
Detect Link Down Threshold	3 Time(s)
Custom Detect Host 1	8.8.8.8
Custom Detect Host 2	208.67.222.222
I	
	Apply Settings Cancel Changes

Figure 4-5-4: LAN Setup

Object	Description
Upject	Description



Object	Description		
Lood Dolongo Wainht	Load Balance Weight allows you to set a relative weight (from 1 - 10)		
Load Balance Weight	for each WAN port.		
External Connection			
Detection	Enable to detect the status of WAN connection.		
Defect informed	Set the detect interval as you need.		
Detect Interval	The recommended value is 5 (default).		
Detect Link Up	Set the times for detecting link up.		
Threshold	The recommended value is 8 (default).		
Detect Link Down	Set the times for detecting link down.		
Threshold	The recommended value is 3 (default).		
Custom Detect Heat	The host is used to check whether the internet connection is alive or		
Custom Detect Host	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 cellular gateway as shown in Figure 4-5-5. Here you may change the settings for IP address, subnet mask, DHCP, etc.

IP Address	192.168.1.1	
Netmask	255.255.255.0	

Figure 4-5-5: LAN Setup

Object	Description		
	The LAN IP address of the cellular gateway and default is		
IP Address	192.168.1.1.		
Net Mask	Default is 255.255.255.0 .		



4.5.5 Multi-Subnet

Name	Network		DHCP Server	
LAN Subnet 1	IP Address	192.168.1.1	V	
LAN Subhet I	Netmask	255.255.255.0	v	
	IP Address	192.168.3.1		
AN Subnet 2	Netmask	255.255.255.0		
	IP Address	192.168.5.1		
LAN Subnet 3	Netmask	255.255.255.0		
LAN Cubrat 4	IP Address	192.168.7.1		
LAN Subnet 4	Netmask	255.255.255.0		

This page provides multi-subnet setting as shown in Figure 4-5-6.

Figure 4-5-6: Multi-Subnet

4.5.6 Routing

Please refer to the following sections for the details as shown in Figures 4-5-7 and 4-5-8.

Number	Туре	Destination	Netmask	Gateway	Interface	Comment	Action
Current Routi	ng table in th	ie system					
Number	Desti	nation	Netmask		Gateway	I	nterface
1	0.0.0.	0	0.0.0		192.168.0.180	l	LOCAL
2	0.0.0.	0	0.0.0		192.168.1.18	١	WAN1
3	0.0.0.	0	0.0.0		192.168.1.19	١	WAN2
4	192.1	68.0.0	255.255.255.0		0.0.0.0	l	AN
5	192.1	68.1.0	255.255.255.0		0.0.0.0	١	WAN1
6	192.1	68.1.0	255.255.255.0		0.0.0.0	١	WAN2

Figure 4-5-7: Routing table



Add a routing rule	
Type Destination Netmask Gateway Interface Comment	Host ▼ 255.255.255.255 /32 ▼ LAN ▼
	Apply Settings Cancel Changes

Figure 4-5-8: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote cellular gateway (or other network gateway) that the local cellular 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
	There are two types: Host and Net.
Туре	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.
	The gateway is the router or host's IP address to which packet was
Gateway	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
Interface	router when this route is used.
Comment	Enter any words for recognition.



4.5.7 WAN IPv6 Setting

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the cellular gateway as shown in Figure 4-5-9. It allows you to enable IPv6 function and set up the parameters of the cellular gateway's WAN. In this setting you may change WAN connection type and other settings.

WAN1 IPv6 Setting	
Connection Type IPv6 Address Subnet Prefix Length Default Gateway	DHCP • 64
WAN2 IPv6 Setting	
Connection Type IPv6 Address Subnet Prefix Length Default Gateway	DHCP • 64



ngs Cancel Changes



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

4.5.8 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown in Figure 4-5-10.



DHCP Server	
DHCP Service	• Enable O Disable
Start IP Address	192.168.1. 100
Maximum DHCP Users	101
Set DNS	Automatically O Manually
Primary DNS Server	
Secondary DNS Server	
WINS	
Lease Time	1440 minutes
Domain Name	PLANET

Apply Settings Cancel Changes

Figure 4-5-10: DHCP

Object	Description	
	By default, the DHCP Server is enabled, meaning the cellular	
DHCP Service	gateway will assign IP addresses to the DHCP clients automatically.	
	If user needs to disable the function, please set it as disable.	
	By default, the start IP address is 192.168.1.100.	
Start IP Address	Please do not set it to the same IP address of the cellular gateway	
	By default, the maximum DHCP users are 101, meaning the cellular	
	gateway will provide DHCP client with IP address from	
Maximum DHCP Users	192.168.1.100 to 192.168.1.200 when the start IP address is	
	192.168.1.100.	
	By default, it is set as Automatically, and the DNS server is the	
0-4 DN0	cellular gateway's LAN IP address.	
Set DNS	If user needs to use specific DNS server, please set it as Manually,	
	and then input a specific DNS server.	
Primary/Secondary DNS		
Server	Input a specific DNS server.	
WINS	Input a WINS server if needed.	
	Set the time for using one assigned IP. After the lease time, the	
	DHCP client will need to get new IP addresses from the cellular	
Lease Time	gateway	
	Default is 1440 minutes.	
Demois Neme	Input a domain name for the cellular gateway	
Domain Name	Default is Planet.	



4.5.9 DDNS

The cellular 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 (**<u>http://www.planetddns.com</u>**)** 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 4-5-11.

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 (<u>http://www.planetddns.com</u>). 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 cellular gateway, and check the DDNS menu and just enable it. You don't need to go to <u>http://www.planetddns.com</u> to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxx 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 cellular gateway's MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

Dynamic Domain Name Service	
DDNS Servcie	• Enable O Disable
Interface	WAN1 T
DDNS Type	PLANET DDNS V
Easy DDNS	Disable V
User Name	
Password	
Host Name	
Interval	120
Update Status	unknow status

Apply Settings Cancel Changes



Figure 4-5-11: 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.	
Interface	By default, the interface is WAN 1.	
	There are three options:	
	1. PLANET DDNS: Activate PLANET DDNS service.	
	2. DynDNS: Activate DynDNS service.	
DDNS Type	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.	
	When the PLANET DDNS service is activated, user is able to select	
	to enable or disable Easy DDNS.	
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.	



4.5.10 MAC Address Clone

Clone or change the MAC address of the WAN interface. The setup is shown in Figure 4-5-12.

MAC Address Clone - WAN1	
Clone WAN MAC MAC Address	Enable Disable
MAC Address Clone - WAN2	
Clone WAN MAC MAC Address	Enable Disable
	Apply Settings Cancel Changes

Figure 4-5-12: 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.

LTE/NR Configuration
LTE/NR Advanced
LTE/NR Status
LTE/NR Statistics
GPS
SMS

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	Auto 🗸	
MTU	1500) min: 700; max: 1500

Figure 4-6-2: LTE/NR configuration

Object	Description	
LTE/NR Config	Indicates what kind of LTE will be used. Possible modes are:	
	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.	
МТО	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	SIM 1 Disconnect
Disable Roaming	● Yes ○ No
Used SIM	Dual SIM O SIM1 O SIM2
SIM Priority	Auto O SIM1 O SIM2
Roaming Switch	Switch to another SIM when roaming is detected
Connect Retry Number	3 (1~100)*60 seconds
Reboot when LTE/NR the on	ly connection which has continuous link down for 5 times (3~15)
SIM1 SIM2	
SIM PIN	
Confirmed SIM PIN	
APN	internet
Username	
Password	
Confirmed Password	
Auth	NONE V

Figure 4-6-3: LTE/NR advanced

Object	Description
Current SIM Card	Display which SIM slot is using.
Disable Roaming	 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 is used or dual SIM cards.
SIM Priority	Configure priority of SIM card
	Switch to another SIM when roaming is detected. System will switch
Roaming Switch	SIM slot when current SIM is in roaming state and another SIM slot
	is in READY state.

Object	Description
SIM PIN	Configure PIN code to unlock SIM PIN.



Object	Description
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
	■ None
	■ PAP
	CHAP



4.6.3 LTE/NR Status

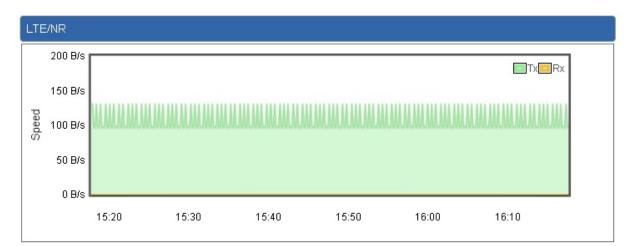
This page displays LTE/NR status as shown in Figure 4-6-4.

LTE/NR Status		
SIM Card	SIM1	SIM2
SIM Status	Ready	Not Inserted
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.







4.6.6 GPS

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

GPS	
Location:(24.982789,121.536890)) Google Maps
Attribute	Value
Latitude	24.982789
Longitude	121.536890
Horizontal	7.6
Altitude	100.4
Date	2021/11/11
Time	08:19:11
Satellite	3

Figure 4-6-6: GPS

4.6.7 SMS

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

SMS Configuration	
Name	
Phone	
Email	

Figure 4-6-7: SMS

Object	Description
Name	Configure user's name
Phone	Configure user's phone number
Email	Configure user's email



4.7 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 Range Forwarding	Allows setting Port Forwarding.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.



4.7.1 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 cellular gateway can prevent specific DoS attacks as shown in Figure 4-7-2.

Firewall Protection		
SPI Firewall	🖲 Enable 🔍 Disable	
DDos		
Block SYN Flood	💿 Enable 🔍 Disable	30 Packets/Second
Block FIN Flood	Enable Disable	30 Packets/Second
Block UDP Flood	Enable Disable	30 Packets/Second
Block ICMP Flood	Enable Disable	5 Packets/Second
IP TearDrop	Enable Disable	
PingOfDeath	Enable 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.	
	SYN Flood is a popular attack way. DoS and DDoS are TCP	
	protocols. Hackers like using this method to make a fake connection	
Block SYN Flood	that involves the CPU, memory, and so on.	
	The default configuration is enabled.	
	If the function is enabled, when the number of the current FIN	
Diack FIN Flood	packets is beyond the set value, the cellular gateway will start the	
Block FIN Flood	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 cellular gateway	
	will start the blocking function immediately.	
	The default configuration is disabled.	



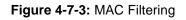
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer
	simple signal on the Internet. There are two normal attack ways
	which hackers like to use, Ping of Death and Smurf attack.
	The default configuration is disabled.
IP TearDrop	If the function is enabled, the cellular gateway will block Teardrop
	attack that is targeting on TCP/IP fragmentation reassembly codes.
Ping Of Death	If the function is enabled, the cellular 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.
	Enable the function to allow the Ping access from the Internet
Block WAN Ping	network.
	The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the cellular
	gateway from the Internet network.
	The default configuration is disabled.



4.7.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the cellular gateway Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-7-3.

MAC Filter	
Enable MAC Filtering Interface	 Enable Disable LAN WAN
	Index MAC Address
	Add Remove Remove All
	Add Remove Remove All
	Apply Settings Cancel Changes



Object	Description
	Set the function as enable or disable.
Enable MAC Filtering	When the function is enabled, the cellular 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
Interface	a LAN device's MAC address, please select LAN, vice versa.
	Input a MAC address you want to control, such as
MAC Address	A8:F7:E0:00:06:62.
A -1 -1	When you input a MAC address, please click the "Add" button to add
Add	it into the list.
Damana	If you want to remove a MAC address from the list, please click on
Remove	the MAC address, and then click the "Remove" button to remove it.
Damasua All	If you want to remove all MAC addresses from the list, please click
Remove All	the "Remove All" button to remove all.



4.7.3 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.

IP Filtering						
IP Filtering		Enable Isable				
IP Filtering Rule	es					
No. Active	Source IP	Destination IP	Port Range	Protocol	Action	
Add IP Filtering Rule						
Figure 4-7-4: IP Filtering						
Object Description						

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

IP Filter Rule Setting	
Enable	✓
Source IP Address	/ 32 V Anywhere
Destination IP Address	/ 32 V Anywhere
Destination Port	
Protocol	All 🔻
	Apply Settings Cancel Changes

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.



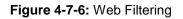
Object	Description		
Anywhere (of destination	Check the box if you want to control all web sites, meaning the LAN		
IP Address)	user can't visit any web site.		
Destingtion Part	Input the port of destination IP Address which you want to block.		
Destination Port	Leave it as blank if you want to block all ports of the web site.		
Destand	Select the protocol type (TCP, UDP or all).		
Protocol	If you are unsure, please leave it to the default all protocol.		



4.7.5 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 Fil	Itering					
Web Filtering © Enable ® Disable						
Web Fil	Web Filtering Rules					
No.	Rule Enable	Filter Keyword	Filter Type	Action		
		·				
		Add Web Filtering R	ule			



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	Enable ex. www.yahoo.com
	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.			



4.7.7 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 Cellular gateway's NAT firewall.

Port Forwarding						
Port Forwarding	Enable Disable					
Port Forwarding Rules						
No. Rule Name	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Delete
Add Port Forwarding Rule						

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.	

Port Forwarding	
Rule Name	
Protocol	Both v
External Service Port	~
Virtual Server IP Address	
Internal Service Port	~
	Apply Settings Cancel Changes

Figure 4-7-9: Port Forwarding Rule Setting

Object	Description
Rule NameEnter 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.
	Enter the external ports you want to control. For TCP and UDP
External Service Port	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.



Object	Description	
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.	

4.7.8 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 DMZ IP Address	Enable Isable
DMZ - WAN2	
DMZ DMZ IP Address	Enable Disable
	Apply Settings Cancel Changes

Figure 4-7-9: DMZ

Object	Description
	Set the function as enable or disable. If the DMZ function is enabled,
DMZ	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.



4.8 Virtual Private Network

To obtain a private and secure network link, the cellular 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

IPsec
IPsec Remote Server
GRE
рртр
L2TP
SSL VPN
Certificates
VPN Connection

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.
РРТР	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.



4.8.1 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 Tu	unnel Lists				
No.	Name	Interface	Status	Action	
		Add	IPSec Tunnel		

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	255.255.255.0 /24 🔹
Remote IP Address	
Remote Network	
Remote Netmask	255.255.255.0 /24 🔹
- Detection	
Dead Peer Detection	Times ut (52
Time Interval 30 Seconds	Timeout 150 Seconds Action Restart •
-Authentication	
Preshare Key	
KE Setting	
Phase 1	
IKE	● v1 ◎ v2
Connection Type	Main Aggressive
ISAKMP	AES (128 bit) • SHA1 • DH Group 2 (1024) •
IKE SA Lifetime	3 hours
Phase 2	
ESP	AES (128 bit) SHA1
ESP Keylife	1 hours
Perfect Forward Secrecy (PFS)	○ Yes ● No

- 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	This is only available for host-to-host connections and specifies to which interface the host is connecting.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 cellular 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.			
	Set up the detection time of DPD (Dead Peer Detection).			
	By default, the DPD detection's gap is 30 seconds, over 150 seconds			
	to think that is the broken line.			
Dead Peer Detection	When VPN detects opposite party reaction time, the function will take			
	one of the actions: "Hold" stand for the system will retain IPSec SA,			
	"Clear" stand for the tunnel will clean away and waits for the new			
	sessions, "Restart" will delete the IPSec SA and reset VPN tunnel.			
Preshare Key	Enter a pass phrase to be used to authenticate the other side of the			
Treshare Ney	tunnel. Should be the same as the remote host.			
IKE	Select the IKE (Internet Key Exchange) version.			
Connection Type	1. Main.			
	2. Aggressive.			
	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.			
	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			
ISAKMP	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.			
	It offers AES, 3 DES, SHA 1, SHA2, and MD5.			
ESP	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	Set the function as enable or disable.		
Secrecy (PFS)			

4.8.2 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
			Add GR	E 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	Disable •
Name	Tunnel name
Through	LAN •
Peer Wan IP Address	Remote IP Address
Peer Subnet Mask	10.10.10.0/24
Peer Tunnel IP Address	10.10.10.2
Local Tunnel IP Address	10.10.10.1
Local Subnet Mask	255.255.255.255 /32 🔻

Apply Settings

Cancel Changes

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. 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	Input the Tunnel IP address of remote host.	
Address		
Local Tunnel IP	Input the Tunnel IP address of remote host.	
Address		
Local Netmask	Input the Tunnel IP address of the cellular gateway	



4.8.3 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 Broadcast Force MPPE Encryption CHAP MSCHAP MSCHAP v2 DNS1 DNS2	 Enable Disable Enable Disable Enable Disable Enable Disable Enable Disable
WINS1 WINS2 Server IP Address Clients IP Address Start Clients IP Address End	192.168.10.1 192.168.10.10 192.168.10.100
User1test2user3user4user5user	Password test 1234 1234 1234 1234 1234

Apply Settings

Cancel Changes

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	Set the encryption as enable or disable.
Encryption	
СНАР	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	
WIN5	WINS server IP address to client.	
Server IP Address	Input the IP address of the PPTP Server. For instance, "192.168.10.1".	
	When the VPN connection is established, the VPN client will get IP	
Clients IP Address	address from the VPN Server. Please set the range of IP Address. For	
(Start/End)	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.	



4.8.4 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	192.168.50.1
Clients IP Address Start	192.168.50.100
Clients IP Address End	192.168.50.200
With IPsec	Enable Isable
Preshare Key	
User	Password
1 test	test
2 user	1234
3 user	1234
4 user	1234
5 user	1234
	1204
- IPsec	
Phase 1	
Connection Type	Main Aggressive
ISAKMP	AES(128 bit) SHA1 DH Group 14 (2048)
IKE SA Lifetime	3 hours
Phase 2	
ESP	AES (128 bit) V SHA1 V
ESP Keylife	1 hours

Apply Settings Cancel Changes

Curren onange.

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".
	When the VPN connection is established, the VPN client will get IP
Clients IP Address	address from the VPN Server. Please set the range of IP Address. For
(Start/End)	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	 Main. Aggressive. 		
ISAKMP	 It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 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	 It offers AES, 3 DES, SHA 1, SHA2, and MD5. 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.		



4.8.6 SSL VPN

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

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

Apply Settings Cancel Changes

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).



4.8.8 VPN Connection

This page shows the VPN connection status as shown in Figure 4-8-9.

VPN Conn	ection Sta	tus						
IPsec	GRE	PPTP	L2TP	SSL VPN				
Туре	Connected Time		Local IP	Remote IP	Local Subnet	Remote Subnet		

Figure 4-8-9: VF	N Connection Status
------------------	---------------------

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



4.9 AP Control

The AP Control menu provides the following features for managing the system as Figure 4-9-1 is shown below:

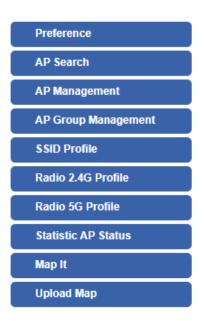


Figure 4-9-1: AP Control Menu

Object	Description		
Preference	Edit region, RO community, RW community		
AP Search	Search APs in the same domain		
AP Management	Config APs IP Address, Subnet Mask, SSID and Radio Profiles		
AP Group Management	Grouping same model AP		
SSID Profile Setup SSID Profile			
Radio 2.4G Profile	Setup Radio 2.4G Profiles		
Radio 5G Profile	Setup Radio 5G Profiles		
Statistics AP Status	Show the status of managed APs		
Statistics Active Clients	Show the status of active clients		
Map It	Edit the map of AP location and coverage		
Upload Map	Search APs in the same domain		



4.9.1 Preference

On this page, you can choose the device region of FCC or ETSI. Then edit RO community and RW community for public or private use. Select Apply or Reset. This screenshot is as shown in Figure 4-9-2.

AP Preference

Region	FCC ~
RO Community	public
RW Community	private

Figure 4-9-2: AP Control Menu

Noted: Device of FCC and device of ETIS cannot be shown at the same time.

4.9.2 AP Search

On this page, you can add new APs in your AP Control System.

Step as follows :

Step 1. Press the Search button to discover PLANET devices.

Step 2. Waiting for few time, Choose which AP you want to add.

Step 3. Press the Apply button to finish addition.

P Search				Step1. Search	Apply Step3	P Q 10 (101024)	۲
Num.	MAC Address	Device Type	Model No.	Version	Devic	Device Description	-
1	a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0-Build20200321122005	192.168.0.101	O (O)	0
2	a8:f7:e0:3c:5f:ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0-Build20200422115453	192.168.0.102		0

Note: When use AP Search, The APs IP Address must be same as WS-Series Switch IP domain



4.9.4 AP Management

On this page, you can management your APs, Including check AP online status, config AP (IP address, Mask, SSID and Radio profile), reboot AP, firmware update, delete AP in the AP Control system.

Status

	nagemen nline 🔴 C	t Offline 🔘 Disa	ble				<i>ф</i>	Apply Filter by Co	ntext		Q	10 (10	64)	0
	Status	AP Group	MAC Address	Device Type	Model No.	Version	IP Address	Device Description			Ac	tion		
0	•		a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0- Build20200321122005	192.168.0.101		989	8		9	0	龠
	•		a8:f7:e0:3c:5f.ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0- Build20200422115453	192.168.0.102		669	0		\$	\bigcirc	龠

Object	Description	
	Connection status: online, offline, Wi-Fi disabled	
	In progress: action in progress	
 Finished/Successful: action finished and successful. 		
×	Failed: action failed.	

Action

Object	Description
60	Setting: edit setting and allocate profile to AP
C	Link: link to the AP's web page
Ŧ	Firmware Update: Upgrade AP's firmware
^c	Reboot: Reboot the AP
 	Delete: Delete the AP from the control list LED Control: Control the AP's LED.
:@:Q@	Mouse-click in a sequential order: LED blink-> LED off-> LED on

Notes:

- 1. To configure multiple APs at one time, select multiple APs and then choose one of the action icons on the top of the page. The "Link" action is not allowed for multiple APs.
- 2. When finish setup AP, you need to press Apply button to complete setup.



4.9.5 AP Group Management

On the AP Group Management page, you can create AP group and control one or more AP groups.

roup Management				14	i s	Apply	Filter by Context	Q	10 (1010)	0
	Num.	Group Name	Group Description	Action						
	1	GroupTest1	test	191	AIN		6	Q	會	
0	2	GroupTest2	test	TOT	ALC: N		6	Q	龠	

Action:

Object	Description
¢.	Add new group: Click it to add an AP group
E 8	Delete selected item: Click it to delete the selected AP group

AP Group Config						Apply	Back	Reset
	AP Group Configured	Group Member Setting						
Model No.	WAP-200N 🗸		Current AP Group Members			Available Managed APs		
AP Group Name				*	1			*
AP Group Description								
		-			<< Add			
					Description			
					Remove >>			
				÷				-
		2.4G Pro	ofile		5G Profile			
	SSID 1 Disable 🗸			Disable 🛩				
	SSID 2 Disable 🗸			Disable 🗸				
	SSID 3 Disable 🗸			Disable 🗸				
	SSID 4 Disable 🗸			Disable 🗸				
Rad	tio Profile Disable 🗸			Disable 🗸				

Create Group:

- 1. Select AP Model No. you want to Add
- 2. Type AP Group Name and AP Group Description.
- 3. Select AP you want to add in group member setting area and press Add button.
- 4. Select AP Group SSID profile and Radio Profile.
- 5. Press Apply button to finish create ap group.

Note:

To do profile provisioning to multiple AP groups at one time, select multiple AP groups, and then click the "Apply" button.

The "Link" action is not allowed for multiple APs or AP group.



4.9.6 SSID Profile

On the SSID profile configuration page, enter the value that you preferred and then click "Apply" to save

e prof	file									
adio Profile	2.4GHz						Filter by Profile Na	me Q 1	0 (108)	0
	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Act	ion
	1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	989	命
	2	WNAP-C3220E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	101	龠
		Model No.	WAP-200N ~		Profile Configuration					
		Model No.	WAP-200N V							
					Basic Setting					
	Radio P	rofile Description								
		Wireless Mode	11b/g/n mixed mode	~						
	Ch	annel Bandwidth	20MHz ¥							
		Channel	Auto 🛩							
		MCS	Auto 👻							
		Tx Power	Auto 🗸							

Action:

Client Limit 🖬 64

(1 to 64)

Object	Description
C	Add new profile: Click it to add a new profile.
E Se	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
â	Delete: Click it to delete the single profile.



4.9.8 Radio 2.4G Profile

On the Radio profile configuration page, enter the value that you preferred and then click "Apply" to save the profile.

Profile	Profile 2.4GHz						Filter by Profile Na	ne Q	10 (108)	0
	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Act	on
0	1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	100	畲
	2	WNAP-C3220E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	1010	龠

Action:

Object	Description
5	Add new profile: Click it to add a new profile.
	Delete selected item: Click it to delete the selected profile.
	Edit: Click it to edit the profile.
Ê	Delete: Click it to delete the single profile.

Profile 2.4GHz Configuration	on	Apply	Back	Reset
	Radio Profile Configurati	on		
Model No.	WAP-200N ¥			
	Basic Setting			
Radio Profile Description				
Wreless Mode	11b/g/n mixed mode 🗸			
Channel Bandwidth	20MHz V			
Channel	Auto V			
MCS	Auto V			
Tx Power	Auto 🗸			
Client Limit	64 (1 to 64)			

Notes:

- Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.
- 2. WMM Capable is not allowed to be disabled.



4.9.10 Radio 5G Profile

On the Radio profile configuration page, enter the value that you preferred and then click "Apply" to save the profile.

o Profile	5GHz					iii.	B Ex	Filter by Profile Nam	e Q	10 (108)	0
	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandy	width	Tx Power	Data Rate	Act	ion
0	1	WDAP-C7200E	test_5G	11n/ac mixed mode	Auto	40MHz		100%	N/A	666	會

Action:

Object	Description
4	Add new profile: Click it to add a new profile.
1 8:	Delete selected item: Click it to delete the selected profile.
10	Edit: Click it to edit the profile.
â	Delete: Click it to delete the single profile.

Radio Profile 5GHz Configuration		Apply	Back	Reset				
	Radio Profile Configuration							
Model No.	WAP-500N V							
	Basic Setting							
Radio Profile Description								
Wireless Mode	11a/n mixed mode 🗸							
Channel Bandwidth	40MHz V							
Channel	Auto ~							
Client Limit	🛛 64 (1 to 64)							

Notes:

- Strongly suggest you to keep the values as default except the fields like Channel, Network Mode, Channel Bandwidth, Tx Power, IAPP, and Tx/Rx to prevent any unexpected error or impact on the performance.
- 2. WMM Capable is not allowed to be disabled.



4.9.11 Statistics AP Status

On this page, you can observe the current configuration of all managed APs.

	atistic > Managed APs ↓ Online ● Offline ● Disable							Filter by Co	ntext Q	10 (1064)	
Num.	Status	MAC Address	IP Address	Model No.	Name	firmware	AP Group	2.4GHz SSID Profile	5GHz SSID Profile	2.4GHz Radio Profile	5GHz Radio Profile
1	•	a8:f7:e0:46:2e:38	192.168.0.102	WDAP-C7200E		WDAP-C7200E-AP-FCC-V3.0- Build20200321122005					
2	•	a8:f7:e0:3c:5f ab	192.168.0.101	WNAP-C3220E		WNAP-C3220E-AP-FCC-V3.0- Build20200422115453			N/A		N/A

Filter: You can filter the AP list by entering the keyword in the field next to the magnifier icon. The keyword should be in any context that belongs to the fields of this page.

4.9.12 Statistics Active Clients

On this page, you can observe the statuses of all associated clients including traffic statistics, transmission speed and RSSI signal strength.

Sta	itistic > A	active Clients					Filter by N	IAC, IP, SSID, Band	Q	10 (10256)	۲
	Num.	Client MAC Address	AP MAC Address	AP SSID	Band	Tx (KB)	Rx (KB)	Speed (Mbps)		RSSI (dBm)	
	1	00:00:00:00:00:00	a8:f7:e0:46:2e:38	SSIDtest_2.4G	2.4GHz	0	0	0		0	

Filter: You can filter the search result by entering the keywords in the field next to the magnifier icon. The keywords include MAC Address, IP Address, SSID and Band.



4.9.14 Map It

On this page you can add managed APs to the actual position against the floor map. This is convenient to user to view and adjust the actual deployment by reference to its real transmission power and channel allocation.

I S Device Description A 1 Image: Comparison of the second secon	° 4	50 m	100 m 	150 m	200 m	Save test v 250 m 300
				It line to estimate distance of the draw line?		100
AP Group Band Transparency Scale 1:30.3030303030305m Cancel	100 m			Jeomen		
I S Device Description A 1 Image: Comparison of the second secon	0 -	50 m 100) m 150 m	200 m	250 m 	Save test ~
c	m os					
AP Group Band Transparency Scale 1 : 39.21568627450981m Set	100 HIGH			Jeamen		

- 1. Click "Scale" to start to reset the map scale.
- 2. Press the set button to draw a line on the map. Fill its physical distance in the blank and press Set or Cancel. For example, in the graph below, set the door width to 0.8 m

Note: You need to upload map image first before managed APs to the actual position.



4.9.16 Upload Map

On this page, the system allows you to upload your floor map to the system.

Upload Map		k A	Apply
Map	New Map 🗸		
Upload File	選擇攝業 未婚理任何催興		
New Description			
File Size	Bytes		

Note: The system allows user to upload up to 10 floor maps.



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 WiFi	Allow to configure 2.4G WiFi.
5G WiFi	Allow to configure 5G WiFi.
MAC ACL	Allow configure MAC ACL.
WiFi Advanced	Allow to configure advanced setting of WiFi.
WiFi Statistics	Display the statistics of WiFi traffic.
Connection Status	Display the connection status.



4.10.1 2.4G WiFi

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

2.4G WiFi	2.4G WiFi Configuration				
Basic	Virtual AP1	Virtual AP2	Virtual AP3		
	s Status s Name (SSID)		Enable O Disable	9	
Hide SSID		OE	○ Enable		
Bandwi Channe		20N 6	∕IHz ✓		
Encryption		Ope	Open 🗸		
WiFi Mu	ultimedia	• E	Enable O Disable	9	

Figure 4-10-2: 2.4G WFI

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 WiFi

This page allows the user to define 5G WiFi as shown in Figure 4-10-3.

5G WiFi C	G WiFi Configuration			
Basic	Virtual AP1	Virtual AP2	Virtual AP3	
Wireless Status		• E	Enable O Disable	
Wireless Name (SSID)		PL	PLANET_5G	
Hide SSID		() E	Enable 💿 Disable	
Bandwidth		801	MHz 🗸	
Channel		36	~	
Encryption		Ор	Open 🗸	
WiFi Multimedia		🔘 E	Enable O Disable	

Figure 4-10-3: 5G WFI

Object	Description
Wireless Status	Allows user to enable or disable 5G WiFi
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 "
WiFi 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 AC	L				
MAC A	CL	⊖ Ena	○ Enable		
MAC AC	MAC ACL Rules				
Index	Active	Device Name	MAC Address	Action	
		abc	00:30:4F:00:00:01	Add	
				Scan	

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 WiFi Advanced

This page allows the user to define advanced setting of WiF 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%) ~

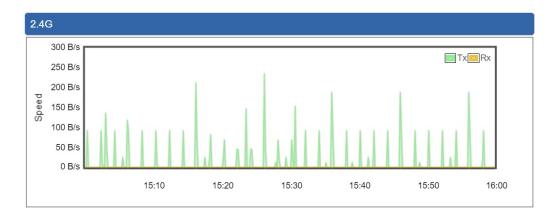
Figure 4-10-5: WiFi advanced

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	The maximum users are 64
Clients	
5GHz Maximum Associated	The maximum users are 64
Clients	
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 WiFi Statistics

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



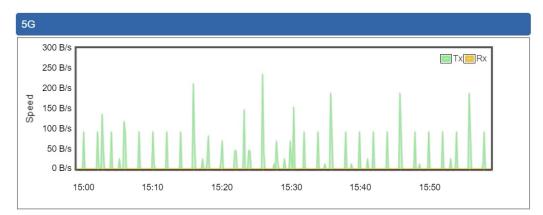


Figure 4-10-6: WiFi statistics



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 Li	ist				
No.	Name	MAC Address	Signal	Connected Time	

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

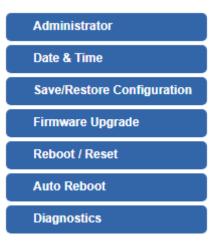


Figure 4-11-1: Maintenance Menu

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the cellular gateway's configuration to local or USB sticker. Restore the cellular 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 cellular gateway's security is secure, you will be asked for your password when you access the cellular gateway's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords as shown in Figure 4-11-2.

Account Password	
Username	admin
Password	
Confirm Password	

Apply Settings Cancel Changes

Figure 4-11-2: account and password page

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 cellular gateway. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown in Figure 4-11-3.

Date and Time	
Current Time	Year 2019 Month 10 Day 22 Hour 10 Minute 27 Second 12
	Copy Computer Time
Time Zone Select	(GMT+08:00)Taipei ▼
NTP Client Update	Enable Disable
NTP Server	time.nist.gov
	time.windows.com
	time.stdtime.gov.tw
	Apply Settings Cancel Changes

Figure 4-11-3: date and time page

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 cellular
	gateway will set its time based on your selection.
NTP Client Update	Once this function is enabled, cellular gateway will automatically update
	current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.



4.11.3 Saving/Restoring Configuration

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

Save/Restore Configuration		
Configuration Export Configuration Import Import	Export Choose File No file chosen	
USB Backup/Upload Configuration		
USB HDD:	Not Detected	
Backup Settings to USB HDD:	Save	
Load Settings from USB HDD:	Configuration disabled	Upload
Umount *Please format the HDD as FAT32 o	n 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 Export button to save setting file to PC.	
Configuration Import	Press the Choose File button to select the setting file, and then	
	press the Import button to upload setting file from PC.	

Save Setting to USB Storage

Object	Description
USB Storage	The status of USB storage.
Backup Settings to	C
USB Storage	Press the Save button to save setting file to USB storage.
Load Settings from	Pross the Upload button to upload sotting file from LISB storage
USB Storage	Press the Upload button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the cellular gateway, please press



Object	Description	
	the Umount button first.	

4.11.4 Upgrading Firmware

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

Firmware Upgrade	
Select File	Choose File No file chosen
Upgrade	

Figure 4-11-5: firmware upgrade page

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	Reboot	
Reset Button	Reset to Default	
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/reset page

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



4.11.6 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

Ping Test	
Interface Target Host Numbers of Packe Ping	ts Ping

Figure 4-11-7: diagnostics page

Object	Description
Interface	Select an interface of the cellular 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 cellular 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 <u>http://planetddns.com</u>
- Step 2: Enable DDNS option through accessing web page of the device.
- Step 3: Input all DDNS settings.

