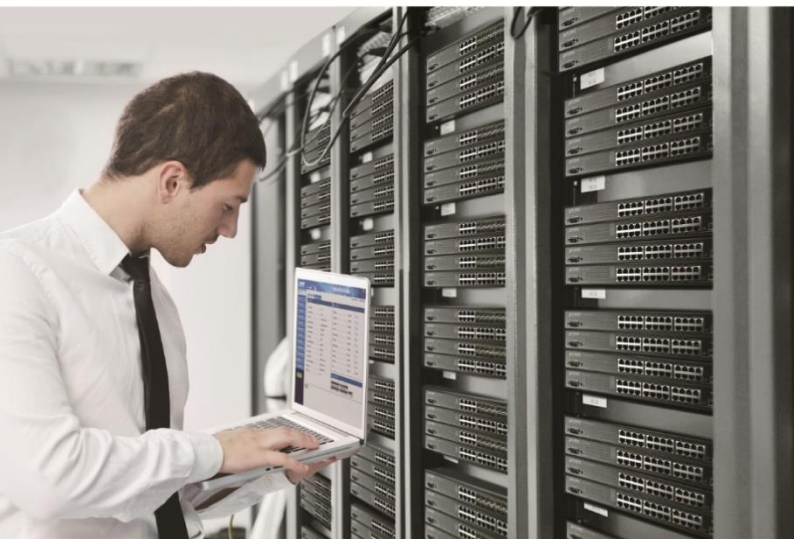




User's Manual

Industrial 5G NR Cellular Gateway

► VCG-2406WP-NR



Copyright

Copyright (C) 2025 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.

EU Representative

PLANET Technology Europe B.V.

Address: Posthoornstraat 11, 3011 WD Rotterdam, NL

Email: eu_rep@planet.com.tw

URL: www.planet.com.tw

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 device 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: VCG-2406WP-NR

Rev.: 1.0 (December, 2025)

Part No. EM-VCG-2406WP-NR_v1.0

Table of Contents

Chapter 1.	Product Introduction.....	7
1.1	Package Contents	7
1.2	Overview	8
1.3	Features	16
1.4	Product Specifications	19
Chapter 2.	Hardware Introduction	27
2.1	Physical Descriptions	27
2.2	Hardware Installation	29
2.2.1	Wall Mount Installation	29
2.2.2	Wall Hanging Installation	31
2.2.3	Grounding the Device	32
2.2.4	SIM Card Installation	33
2.2.5	5G NR Antenna Installation	34
2.2.6	Wi-Fi Antenna Installation	35
Chapter 3.	Preparation	36
3.1	Requirements.....	36
3.2	Setting TCP/IP on your PC	36
3.3	Planet Smart Discovery Utility.....	43
Chapter 4.	Web-based Management	45
4.1	Introduction	45
4.2	Logging in to the Cellular Gateway	45
4.3	Main Web Page.....	47
4.4	System	49
4.4.1	Setup Wizard	51
4.4.2	Dashboard	59
4.4.3	System Status.....	62
4.4.4	System Service	63
4.4.5	Statistics.....	64
4.4.6	Connection Status	65
4.4.7	High Availability	66
4.4.8	RADIUS	67
4.4.9	Captive Portal	68
4.4.10	SNMP	70
4.4.11	NMS	71
4.4.12	Fault Alarm.....	80

4.4.13	Digital Input / Output	81
4.4.14	Remote Syslog	83
4.5	Network	84
4.5.1	Priority	86
4.5.2	WAN	87
4.5.3	WAN Advanced	89
4.5.4	LAN Setup	90
4.5.5	Multi-Subnet	91
4.5.6	Routing	92
4.5.7	WAN IPv6 Setting	93
4.5.8	DHCP	94
4.5.9	DDNS	95
4.5.10	MAC Address Clone	97
4.6	Cellular	98
4.6.1	LTE/NR Configuration	99
4.6.2	LTE/NR Advanced	100
4.6.3	LTE/NR Status	102
4.6.4	LTE/NR Statistics	103
4.6.5	GPS	104
4.6.6	SMS	105
4.7	Security	106
4.7.1	Firewall	107
4.7.2	MAC Filtering	109
4.7.3	IP Filtering	110
4.7.4	Web Filtering	112
4.7.5	Port Forwarding	113
4.7.6	DMZ	115
4.8	Virtual Private Network	116
4.8.1	IPSec	117
4.8.2	GRE	121
4.8.3	PPTP Server	123
4.8.4	L2TP Server	125
4.8.5	SSL VPN	127
4.8.6	VPN Connection	128
4.8.7	SD WAN	129
4.9	AP Control	130
4.9.1	Preference	131
4.9.2	AP Search	132
4.9.3	AP Management	133
4.9.4	AP Group Management	134

4.9.5	SSID Profile	135
4.9.6	Radio 2.4G Profile	136
4.9.7	Radio 5G Profile	137
4.9.8	Statistics AP Status	138
4.9.9	Statistics Active Clients	139
4.9.10	Map It	140
4.9.11	Upload Map	141
4.10	Wireless	142
4.10.1	2.4G Wi-Fi	143
4.10.2	5G Wi-Fi	144
4.10.3	MAC ACL	145
4.10.4	Wi-Fi Advanced	146
4.10.5	Wi-Fi Statistics	147
4.10.6	Connection Status	148
4.11	Power over Ethernet	149
4.11.1	PoE Configuration	150
4.11.2	PoE Status	152
4.11.3	PoE Schedule	153
4.11.4	PD Alive Check	155
4.12	Maintenance	157
4.12.1	Administrator	158
4.12.2	Date and Time	159
4.12.3	Saving/Restoring Configuration	160
4.12.4	Upgrading Firmware	161
4.12.5	Reboot / Reset	162
4.12.6	Diagnostics	163
Appendix A: DDNS Application		164

Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial 5G NR Cellular Gateway, VCG-2406WP-NR. The descriptions of these models are as follows:

VCG-2406WP-NR	Industrial/Vehicle 5G NR Cellular Wireless Gateway with M12 PoE+
----------------------	--

“Cellular Gateway” mentioned in the manual refers to the VCG-2406WP-NR.

1.1 Package Contents

The package should contain the following:

- VCG-2406WP-NR x 1
- QR code Sheet x 1
- 2m 8-pin X-coded M12-to-RJ45 UTP cable x 1
- 5G NR antenna x 4
- 5G NR antenna extender with magnetic base x4
- Wi-Fi dual-band antenna x 2
- Wall-mounted kit x 1 set
- M12 Dust Cap x 6

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



The box does not contain the M12 5-pin K-coded female connector power cable.

1.2 Overview

Rugged Industrial 5G NR VPN Gateway Optimized for Vehicle Applications

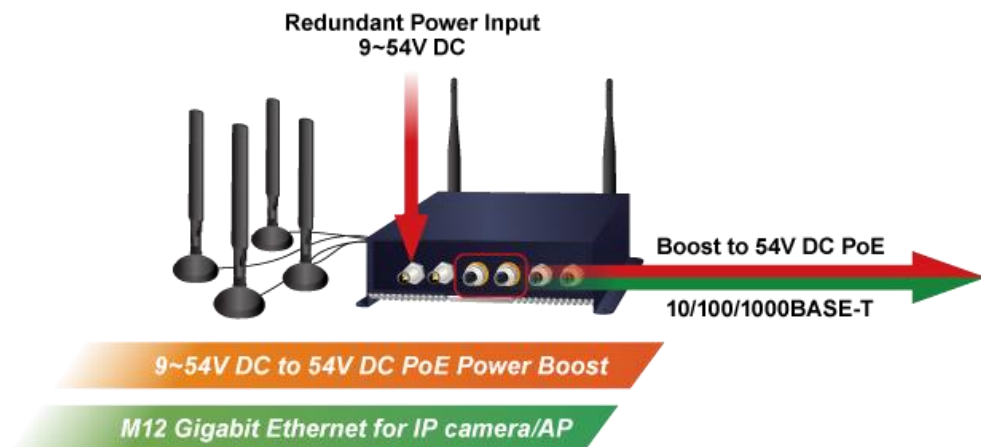
PLANET VCG-2406WP-NR is a purpose-built industrial-grade VPN security gateway designed specifically for in-vehicle networking and mission-critical mobile deployments. It integrates four Gigabit M12 X-coded Ethernet ports (including two IEEE 802.3at PoE+ ports, one configurable LAN/WAN port, and one dedicated LAN port) together with DI/DO interfaces, delivering secure and stable data transmission even under constant vibration and movement.

For reliable vehicle connectivity, the VCG-2406WP-NR supports SD-WAN, dual-WAN failover, and outbound load balancing to optimize bandwidth usage and maintain uninterrupted communication while on the move. Its rugged M12 connectors provide superior resistance against shock and vibration, and the IP50 aluminum enclosure with a wide operating temperature range from -40 to 75 °C ensures consistent performance in buses, railways, and other transportation environments.

Dual 9–54V DC redundant power inputs further guarantee continuous operation, meeting the stringent demands of vehicular and industrial deployments.

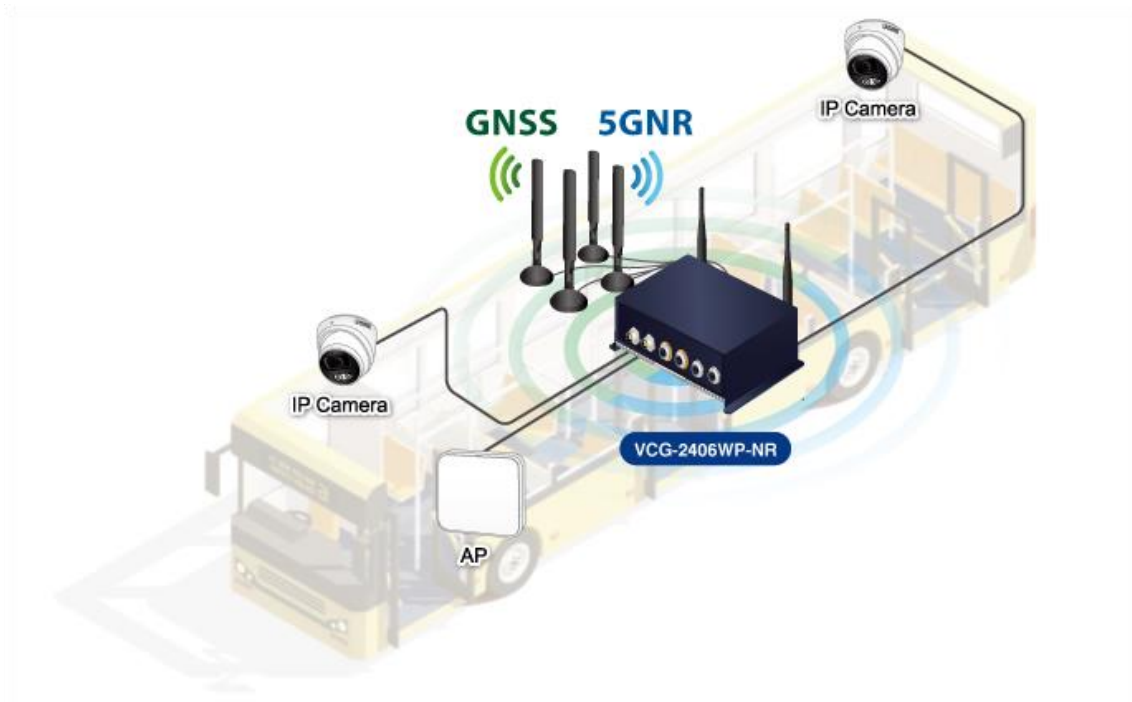
Stable PoE Power Boost for Vehicle Environments

The VCG-2406WP-NR features a built-in 9–54V DC to 54V PoE power boost, allowing the gateway to deliver stable IEEE 802.3at PoE+ output even when operating on fluctuating vehicle power systems. Through its rugged M12 Gigabit Ethernet interfaces, the device can directly power onboard IP cameras or wireless access points, ensuring reliable operation in harsh mobile environments.



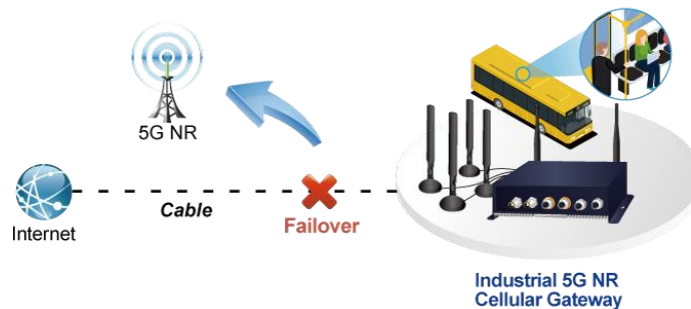
Seamless Onboard Device Integration for Vehicle Environments

The VCG-2406WP-NR enables reliable in-vehicle connectivity by integrating IP cameras and Wi-Fi access points through its rugged M12 Gigabit Ethernet interfaces. With 5G NR mobile broadband and multi-system GNSS positioning, the gateway provides stable data transmission and precise location tracking during vehicle operation, ensuring a dependable network foundation for modern transportation systems.



Automatic Failover between 5G NR and Gigabit WAN

The VCG-2406WP-NR integrates 5G NR connectivity with Gigabit Ethernet WAN. By supporting automatic failover between 5G NR and wired WAN interfaces, the device ensures always-on Internet connectivity. Users can flexibly assign priority for 5G NR or wired WAN, so if the primary connection fails, the backup WAN takes over instantly, maintaining uninterrupted network services.

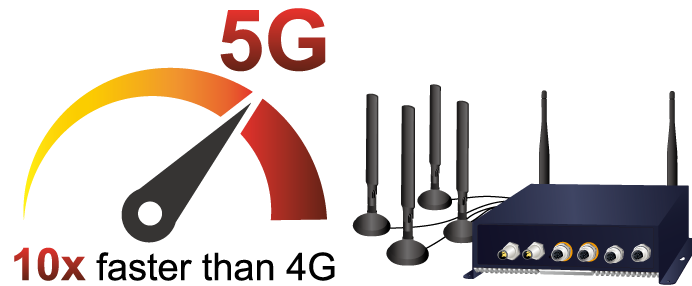


Ultra-Fast Speed 4G/5G Network*

The VCG-2406WP-NR supports 5G NR Sub-6 GHz with downlink speeds up to 2.4Gbps and uplink up to 900Mbps, as well as LTE downlink speeds up to 1.6Gbps. This high bandwidth reduces latency and enables premium connectivity for real-time services. Multi-band compatibility with LTE FDD/TDD and WCDMA ensures flexible deployment across regions.

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

Up to download speed **2.4Gbps**



Dual SIM Design

To enhance reliability, the VCG-2406WP-NR is equipped with two Nano-SIM slots supporting failover and roaming. When one SIM card loses connection, the system automatically switches to the other, ensuring uninterrupted cellular service. This design provides flexible connectivity for mobile and industrial applications such as public transportation, railway systems, and logistics operations.



Built-in Multi-System GNSS for Accurate Positioning

The VCG-2406WP-NR comes with an integrated GNSS (Global Navigation Satellite System) receiver supporting GPS, GLONASS, BeiDou, Galileo, and QZSS. This ensures precise and reliable location tracking, making the gateway an ideal choice for fleet management, intelligent transportation systems, and industrial monitoring scenarios where accurate real-time positioning is essential.

GNSS Positioning



Vibrationproof and Dustproof M12 Interfaces

The VCG-2406WP-NR is equipped with M12 X-coded Gigabit ports, an A-coded connector for DI/DO and alarm, and a K-coded connector for DC power input. These rugged interfaces provide secure and stable connections even under shock, vibration, dust, and temperature extremes, ensuring reliable Ethernet and I/O performance in demanding vehicular and industrial environments.

Wireless 11ax Brings Excellent Data Link Speed

The VCG-2406WP-NR adopts Wi-Fi 6 (802.11ax) technology, delivering up to 1800Mbps bandwidth with concurrent 2.4GHz and 5GHz dual-band operation. Equipped with high-power amplifiers and 2T2R antennas, it ensures reliable coverage even in complex industrial or vehicle environments. Wi-Fi 6 features such as MU-MIMO, OFDMA, Beamforming, and BSS Coloring optimize transmission efficiency, enabling smooth connectivity for multiple devices and IoT applications.

Wi-Fi Deployments and Authentication with Simplified Management

The VCG-2406WP-NR integrates a built-in AP controller, captive portal, RADIUS authentication, and DHCP server to simplify wireless network deployment. It allows enterprises and transportation systems to provide secure employee and guest Wi-Fi access without additional hardware, reducing cost and management complexity.



Built-in Unique PoE Functions for Powered Devices Management

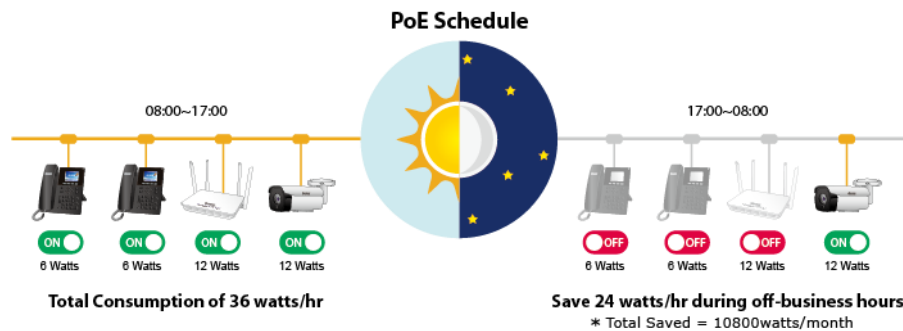
With two IEEE 802.3at PoE+ ports, the VCG-2406WP-NR delivers up to 36W per port and a total PoE budget of 60W. It also features the following special PoE management functions.

PoE Usage Monitoring

With PoE usage monitoring, it can show the PoE loading of each port, total PoE power usage and system status, such as overload, low voltage, over voltage and high temperature. User can obtain detailed information about the real-time PoE working condition of the VCG-2406WP-NR directly.

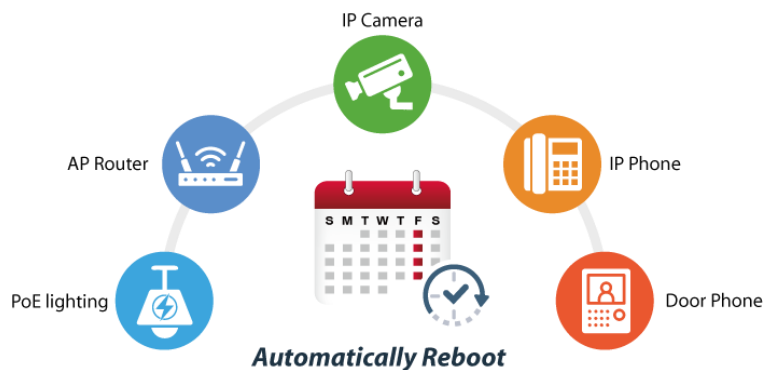
PoE Schedule

Under the trend of energy saving worldwide and contributing to environmental protection, the VCG-2406WP-NR can effectively control the power supply besides its capability of giving high watts power. The “PoE schedule” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and budget. It also increases security by powering off PDs that should not be in use during non-business hours.



Scheduled Power Recycling

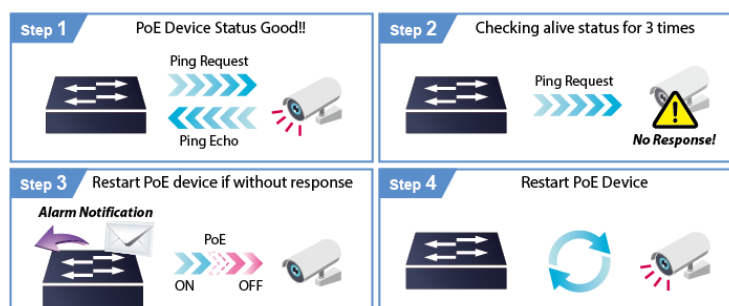
The VCG-2406WP-NR allows each of the connected PoE IP cameras or PoE wireless access points to reboot at a specific time each week. Therefore, it will reduce the chance of IP camera or AP crash resulting from buffer overflow.



PD Alive Check

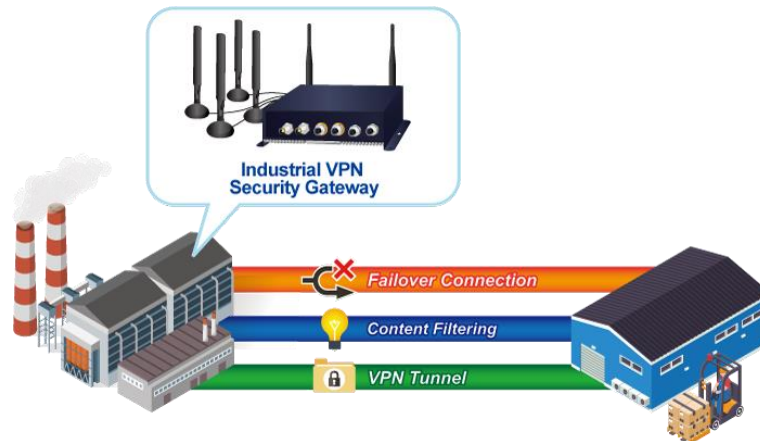
The VCG-2406WP-NR can be configured to monitor connected PD status in real time via ping action. Once the PD stops working and responding, the VCG-2406WP-NR will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.

PD Alive Check



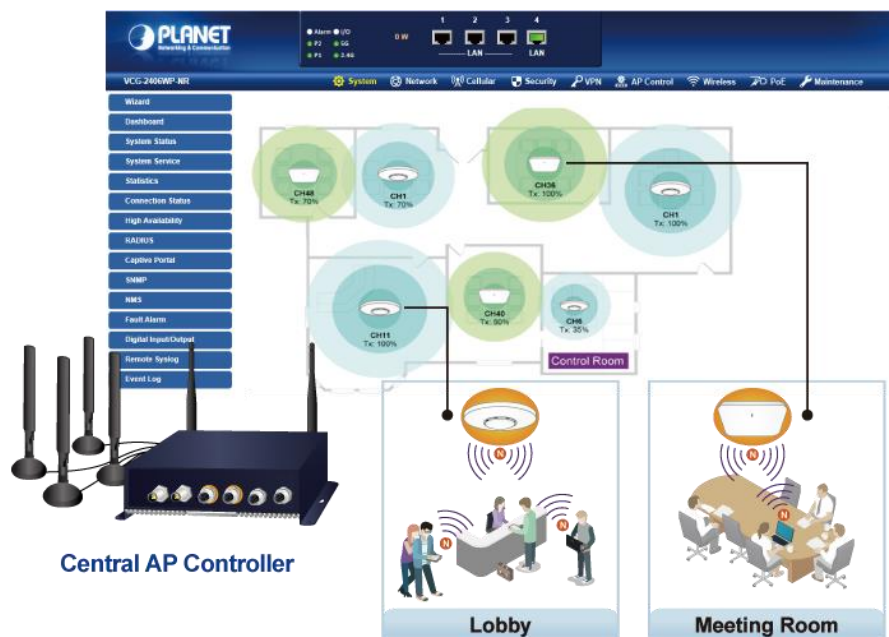
Ideal VPN Security Gateway Solution for Factories and Transportations

The VCG-2406WP-NR offers a full VPN feature set, including IPSec, SSL VPN, PPTP, L2TP, and GRE, with robust encryption (DES/3DES/AES) and authentication (MD5, SHA-1, SHA-256, etc.). With up to 60 VPN tunnels supported, it ensures secure remote access and private communications across industrial sites, railway systems, and vehicle networks.



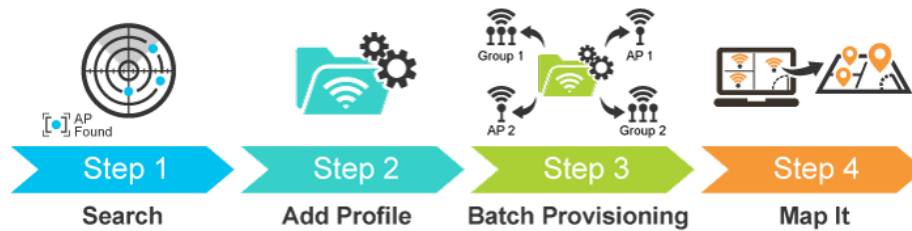
Centralized Remote Control of Managed APs

The VCG-2406WP-NR supports centralized management of PLANET Smart APs through its user-friendly web GUI. It allows administrators to configure SSIDs, security settings, and radio bands for multiple APs at once. Cluster management enables bulk provisioning, firmware upgrades, and monitoring, reducing deployment effort and ensuring consistent Wi-Fi service in transportation and industrial networks.



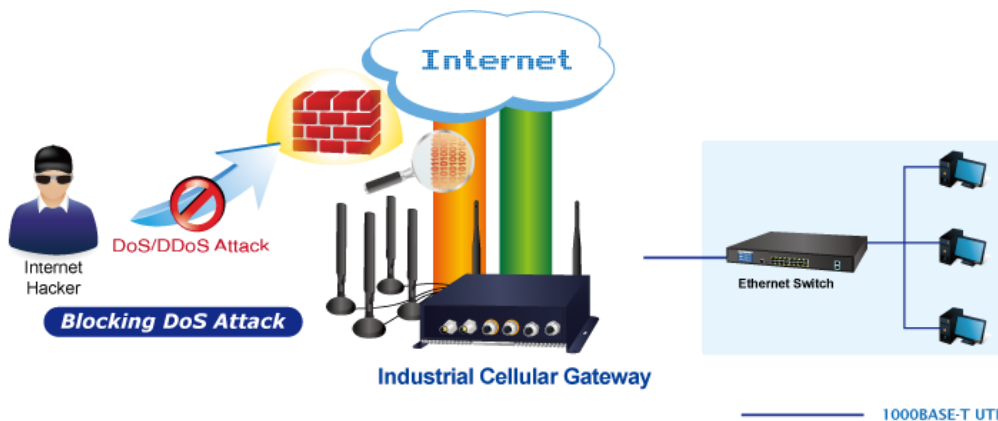
For example, to configure multiple smart APs of the same model, the VCG-2406WP-NR allows clustering them to a managed group for unified management. According to requirements, wireless APs can be flexibly expanded or removed from a wireless AP group at any time. The AP cluster benefits bulk provision 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 VCG-2406WP-NR features a built-in SPI (stateful packet inspection) firewall to protect against unauthorized access. It defends against DoS/DDoS attacks, port flooding, and abnormal traffic patterns, ensuring network stability. Virtual server and DMZ functions provide flexibility for hosting internal services securely while maintaining external accessibility.



Cybersecurity Network Solution to Minimize Security Risks

The VCG-2406WP-NR integrates comprehensive cybersecurity features for network protection. With HTTPS web management, SNMP v1/v2c/v3, and secure tunneling support, administrators can monitor and manage the device securely. Its intuitive web GUI and compatibility with PLANET's NMS controller further enhance ease of management while minimizing security risks.

Maximizing Work Efficiency with PLANET SD-WAN Gateway

With PLANET's integrated SD-WAN technology, the VCG-2406WP-NR enhances WAN optimization across multiple connections. It intelligently routes applications through the best available path, ensuring higher efficiency and reliability. SD-WAN improves application performance, increases business productivity, and reduces IT operational costs, making it ideal for distributed industrial and vehicle networks.

Convenient and Reliable Redundant Power System

The VCG-2406WP-NR is designed with dual 9–54V DC redundant power inputs to guarantee continuous operation in vehicle and industrial deployments. With reverse polarity protection and robust electrical isolation, the device ensures system reliability even under unstable power conditions. This design provides resilience and fault tolerance for mission-critical environments.

Remote Management Solution

PLANET's Universal Network Management System (UNI-NMS) and CloudNMS platform support IT staff by remotely managing all network devices and monitoring PDs' operational statuses. Thus, they're designed for both the enterprises and industries where deployments of PDs can be as remote as possible, without having to go to the actual location once a bug or faulty condition is found. With the UNI-NMS or CloudNMS platform, all kinds of businesses can now be speedily and efficiently managed from one platform.



1.3 Features

Highlights

- Dual-WAN failover and Dual-WAN load balancing
- Compliant with the IEEE 802.3at PoE+ with PD alive check/schedule management
- 1 x DI/DO and fault alarm
- 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 CloudNMS platform supported
- -40 to 75 degrees C operating temperature; fanless designs

Hardware

- 3 x 10/100/1000BASE-T M12 X-coded LAN ports with 2-port IEEE 802.3at PoE+ injector function
- 1 x 10/100/1000BASE-T M12 X-coded WAN/LAN port, auto-negotiation, auto MDI/MDI-X
- One M12 A-coded 5-pin male connector with alarm, digital input and digital output functions
- One M12 K-coded 5-pin male connector with input voltage range of 9 to 54 VDC
- 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

- 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

Power over Ethernet

- Complies with IEEE 802.3at Power over Ethernet Plus, end-span PSE
- Backward compatible with IEEE 802.3af/at Power over Ethernet
- Up to 2 ports of IEEE 802.3af / 802.3at devices powered
- Supports PoE power up to 36 watts for each PoE port
- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- PoE management
- Total PoE power budget control
 - Per port PoE function enable/disable
 - PoE port power feeding priority
 - Per PoE port power limitation
 - PD classification detection
 - PD alive check

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 CloudNMS platform for real-time monitoring

1.4 Product Specifications

Models	VCG-2406WP-NR
Hardware Specifications	
Copper Ports	Total: 4 × 10/100/1000BASE-T Ethernet ports, M12 8-pin X-coded female connectors Port assignments: • Ports 1–2: LAN ports with IEEE 802.3at PoE (PSE) • Port 3: Dedicated LAN port • Port 4: Configurable LAN/WAN port
SIM Interface	2 SIM card slots supporting Nano-SIM
Cellular Antenna	4 × 5 dBi gain external antennas, SMA-type connectors, for 5G NR
Wireless Antenna	2 × 2.4GHz and 5GHz dual-band external antennas with RP-SMA female connectors for Wi-Fi peak gain: 4.33 dBi @2.4GHz, 4.47 dBi @5GHz
DI & DO Interfaces	1 x M12 A-coded 5-pin male connector for DI/DO and alarm interface Pin 1 for DI and Pin 2 for DO Pin 3/4 for Alarm Pin 5 for GND
Alarm	One relay output for port breakdown and power failure. Alarm relay current carry ability: 1A @ 24V DC
Digital Input (DI)	One digital input (DI) Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input load to 24V DC, 10mA max.
Digital Output (DO)	One digital output (DO) Open collector to 24V DC, 100mA max.
Power Connector	Connector type: M12 K-coded, 5-pin male Pin assignment: Pin 1: V1– Pin 2: V1+ Pin 3: V2+ Pin 4: V2– Pin PE: GND
Number of Power Input	2
Power Requirements	Input voltage: 9–54 V DC

Power Consumption	Max.10.2 watts/ 34.8 BTU (Power on without any connection) Max. 81 watts/ 276.38 BTU (Full loading)
Enclosure	IP50 aluminum case
Reset Button	Press < 5 seconds: System reboot Press > 5 seconds: Restore factory default settings
Installation	Desktop Wall-mount
Weight	1725g
Dimensions	245 × 140.5 × 60 mm (W × D × H)
LED Indicators	System - P1 (Green): Power 1 status - P2 (Green): Power 2 status - Alarm (Red): System alarm indicator - I/O (Red): Digital input/output status Ethernet Interfaces (Ports 1–4) 10/100/1000 LNK/ACT (Green): Link/activity at 10/100/1000 Mbps PoE - PoE (Amber): Link/activity Wi-Fi 2.4G (Green): 2.4 GHz Wi-Fi status 5G (Green): 5 GHz Wi-Fi status Cellular SIM - SIM1 (Green): SIM card 1 status - SIM2 (Green): SIM card 2 status Cellular Signal Strength 4 levels (Green): Indicates signal strength (1–4 LEDs lit)
Multi Band Supports	
5G	NSA: n1/ 2/ 3/ 5/ 7/ 8/ 12/ 13/ 14/ 18/ 20/ 25/ 26/ 28/ 29/ 30/ 38/ 40/ 41/ 48/ 66/ 70/ 71/ 75/ 76/ 77/ 78/ 79 SA: n1/ 2/ 3/ 5/ 7/ 8/ 12/ 13/ 14/ 18/ 20/ 25/ 26/ 28/ 29/ 30/ 38/ 40/ 41/ 48/ 66/ 70/ 71/ 75/ 76/ 77/ 78/ 79
LTE	LTE-FDD: B1/ 2/ 3/ 4/ 5/ 7/ 8/ 12/ 13/ 14/ 17/ 18/ 19/ 20/ 25/ 26/ 28/ 29/ 30/ 32/ 66/ 71 LTE-TDD: B34/ 38/ 39/ 40/ 41/ 42/ 43/ 48 LAA: B46
UMTS/WCDMA	B1/ 2/ 4/ 5/ 8/ 19
GNSS	GPS/ GLONASS/ BDS/ Galileo/ QZSS
Data Transmission	5G SA Sub-6 data rate Max. 2.4 Gbps (DL) / Max. 900 Mbps

Throughput	(UL) 5G NSA Sub-6 data rate Max. 3.4 Gbps (DL) / Max. 550 Mbps (UL) LTE data rate Max. 1.6 Gbps (DL) / Max. 200 Mbps (UL) WCDMA data rate Max. 42 Mbps (DL) / Max. 5.76 Mbps (UL)
Power over Ethernet	
PoE Standard	IEEE 802.3af / 802.3at PoE+ PSE
PoE Power Supply Type	End-span
PoE Power Output	Per port 54V DC, 36 watts (max.)
Power Pin Assignment	1/2 (+), 3/6 (-)
PoE Power Budget	60 watts (max.)
Max. Number of Class 4 PDs	2
PoE Management	PD Alive Check Scheduled Power Recycling PoE Schedule PoE Usage Monitoring
Wireless	
Standard	IEEE 802.11a/n/ac/ax (5 GHz) IEEE 802.11g/b/n/ax (2.4 GHz)
Band Mode	2.4 GHz and 5 GHz concurrent mode
Frequency Range	2.4GHz FCC: 2.412~2.462GHz ETSI: 2.412GHz~2.472GHz 5GHz FCC: 5.150 – 5.850 GHz ETSI: 5.150 – 5.725 GHz
Operating Channels	2.4GHz FCC: Channels 1–11 ETSI: Channels 1–13 5GHz 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 ETSI - Non-DFS: 36, 40, 44, 48 - DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140

	Note: 5 GHz channel availability may vary by country according to local regulations.
Modulation Type	802.11ax: MIMO-OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM, 1024QAM) 802.11ac: OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM) 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM) 802.11b: DSSS (DBPSK / DQPSK / CCK)
Channel Width	20 MHz, 40 MHz, 80 MHz
Data Transmission Rates	Transmit: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz *The estimated transmission distance is based on the theory. The actual distance will vary in different environments.
Transmission Power	11b: 23 dBm ±1.5 dBm @11Mbps 11g: 20 dBm ±1.5 dBm @54Mbps 11g/n: 20 dBm ±1.5 dBm @MCS7, HT20 17 dBm@MCS7, HT40 11a: 19.5 dBm ±1.5 dBm @54Mbps 11a/n: 19.5 dBm ±1.5 dBm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20 dBm ±1.5 dBm @MCS8 11ac HT40: 17 dBm ±1.5 dBm @MCS9 11ac HT80: 14.5 dBm ±1.5 dBm @MCS9 11ax HT20: 20 dBm ±1.5 dBm @MCS9 11ax HT40: 17 dBm ±1.5 dBm @MCS9 11ax HT80: 14.5 dBm ±1.5 dBm @MCS11
Encryption Security	WEP: 64/128-bit encryption WPA / WPA2: TKIP / AES encryption WPA-PSK / WPA2-PSK: TKIP / AES encryption WPA3-PSK (SAE): AES encryption only 802.1X Authenticator
Wireless Advanced	Wi-Fi Multimedia (WMM) Auto channel selection Wireless output power management MAC address filtering
Wireless AP Management	
Maximum Managed APs	128
Maximum AP Groups	10
Maximum APs per AP Group	128
Wireless	WEP encryption security

Encryption/Security	WPA Personal / Enterprise (TKIP / AES) WPA2 Personal / Enterprise (TKIP / AES) WPA3 Personal Enterprise Class 802.1x
AP Auto Discovery	Supports AP auto discovery
SSID/RF Profile	Allows multiple wireless profiles creation and maintenance
Cluster Management	Allows AP grouping for bulk provisioning and batch upgrading
Bulk AP Provisioning	Supports bulk AP provisioning with user-defined profiles
Bulk AP Firmware Upgrade	Supports bulk AP firmware upgrade
Coverage Heat Map	Enables real signal coverage of managed AP reflecting on the uploaded zone maps
Status Monitoring	Real-time traffic statistics reporting of AP and activated clients
Graphical Statistics	Real-time and historical visibility of traffic flow [2]
Profile Backup/Restoration	Provides SSID, radio profile backup/restoration
SSIDs-to-VLANs Mapping	Allows to configure SSIDs-to-VLANs mapping in supported APs
Supported Access Point Models [1]	
Indoor AP	IAP-1800AX IAP-2400AX IAP-3600BE [2] IAP-3600BE-4PF [2] WDAP-3600BE [2] WDAP-W3600BE [2] WDAP-C5100BE WDAP-W3000AX WDAP-C3000AX WDAP-C7210E(V2) WDAP-C1800AX(V2) WDAP-W1800AXU WDAP-C7210E WDAP-W1200E WDAP-C7200E WDAP-W750E WNAP-C3220E WNAP-W2200UE
Outdoor AP	WDAP-3000AX WDAP-1800AX WDAP-850AC WDAP-802AC WBS-512AC

	WBS-502N WBS-202N WAP-552N WAP-252N WDAP-702AC WBS-502AC WBS-500N WBS-200N WAP-500N WAP-200N
Remarks	[1] The supported AP models may be changed after a firmware upgrade. [2] Planned via future firmware update.
Security Service	
Firewall Security	Cybersecurity Stateful Packet Inspection (SPI) Blocks DoS/DDoS attack
ALG (Application Layer Gateway)	SIP, RTSP, FTP, H.323, TFTP
NAT	Port forwarding DMZ Host UPnP
Content Filtering	MAC filtering IP filtering Web filtering
Bandwidth Management	Outbound load balancing Failover for dual-WAN QoS (Quality of Service)
Networking	
Routing Protocol	Routing: Static routing Dynamic routing: RIP, OSPF
VLAN	802.1q Tag-based, Port-based, Multi-VLAN
Multicast	IGMP Proxy
NAT Throughput	Up to 900 Mbps (test conditions TBA)
Outbound Load Balancing	Supported algorithms: Weight
Protocol	IPv4, IPv6, TCP/IP, UDP, ARP, HTTP, HTTPS, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, PPPoE, SNMPv1/v2c/v3,

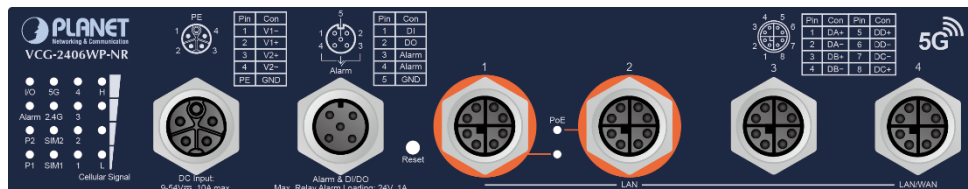
Key Features	HA (High Availability) Captive Portal RADIUS Server/Client AP Control
Advanced Functions	
VPN	IPSec / Remote Server: Net-to-Net, Host-to-Net modes GRE (Generic Routing Encapsulation) PPTP Server L2TP Server SSL VPN Server / Client (OpenVPN)
VPN Tunnels	Up to 60 (test conditions TBA)
VPN Throughput	Up to 108 Mbps (test conditions TBA)
Encryption Methods	DES 3DES AES (AES-128 / AES-192 / AES-256)
Authentication Methods	MD5 SHA-1 SHA-256 SHA-384 SHA-512
Management	
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility NMS controller supported
Secure Management Interfaces	SSHv2 TLS v1.2 SNMP v3
System Log	System event log
Others	Setup wizard Dashboard System status / service monitoring Statistics Connection status Auto reboot Diagnostics
Standards Conformance	
Regulatory Compliance	CE, FCC, E-Mark Vehicle Compliance Ready

Stability	IEC60068-2-32(Free fall) IEC60068-2-27(Shock) IEC60068-2-6(Vibration)
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)

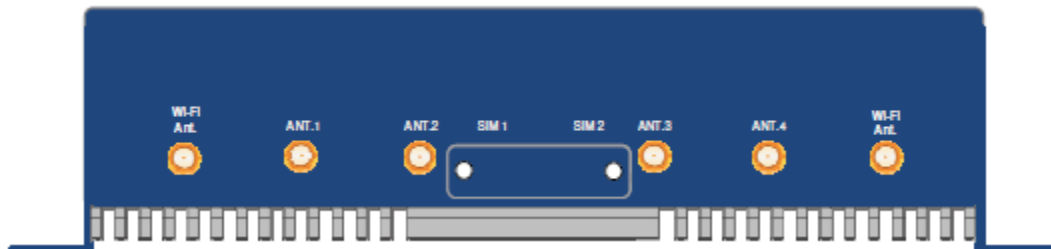
Chapter 2. Hardware Introduction

2.1 Physical Descriptions

Front View



Upper 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	Lights to indicate that power or port has failed.
I/O	Red	Lights to indicate that power or port has failed or DI has event.
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
5G	Green	Lights up when 5G Wi-Fi service is enabled

■ Per 10/100/1000Mbps M12 X-coded Port (Ports 1-4, PoE + on Port 1-2 only)

LED	Color	Function	
10/100/1000 LNK/ACT	Green	Lights:	To indicate the port is running in 10/100/1000Mbps speed and successfully established
		Blinks:	To indicate that the router is actively sending or receiving data over that port.
PoE-In-use	Amber	Lights:	To indicate the port is providing 48V~56V DC in-line power.
		Off:	To indicate the connected device is not a PoE Powered Device (PD)

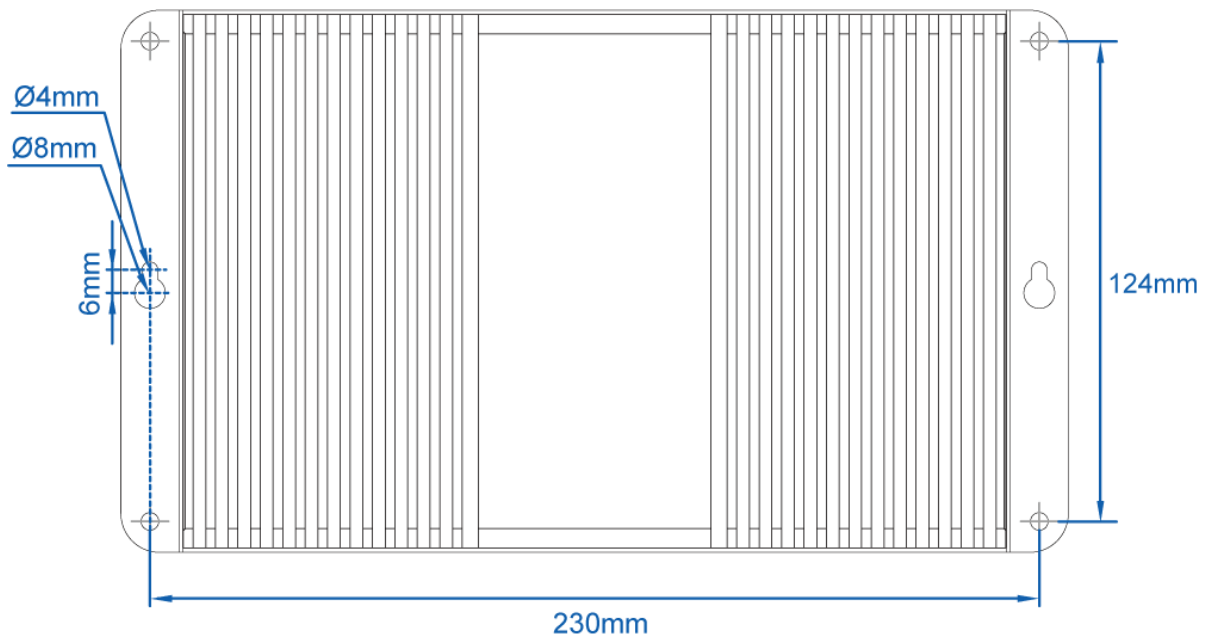
2.2 Hardware Installation

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

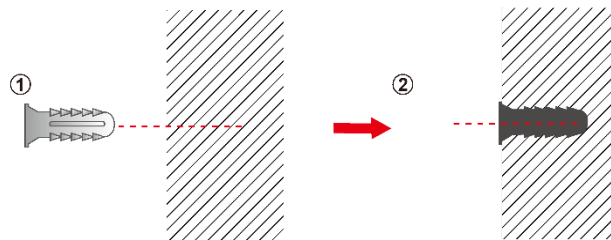
2.2.1 Wall Mount Installation

To install the Wall-mount Managed Switch on the wall, simply follow the following steps:

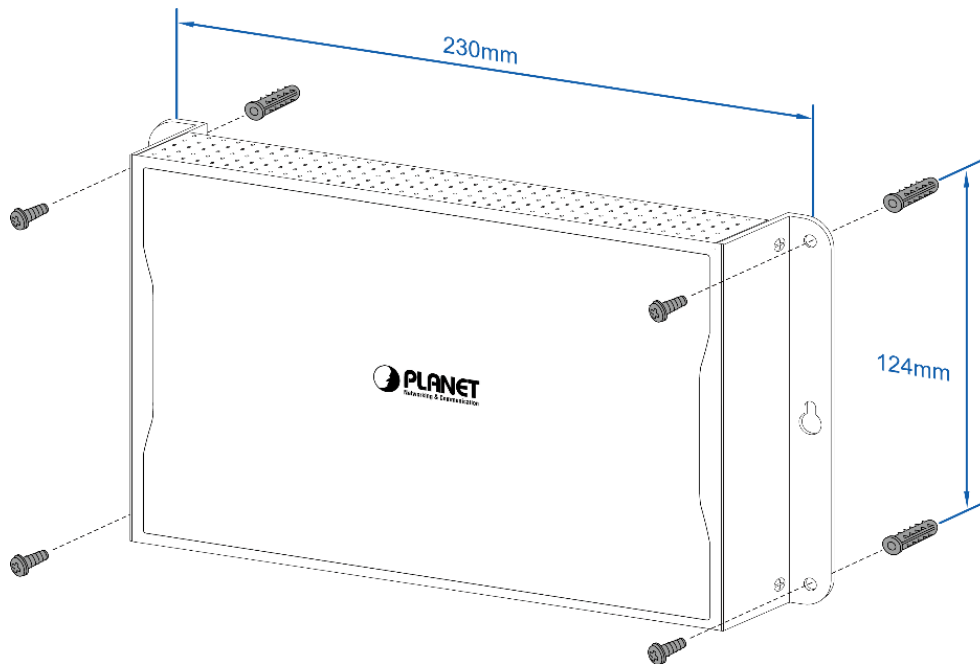
Step 1: Drill 4 holes with **8mm** diameter on the wall. The horizontal and vertical distances between the 2 holes are **230mm** and **124mm**, respectively.



Step 2: Hammer the four anchors into the four holes.



Step 3: Then the four given screws are screwed into the anchors to finish the wall-mount installation, as shown below.



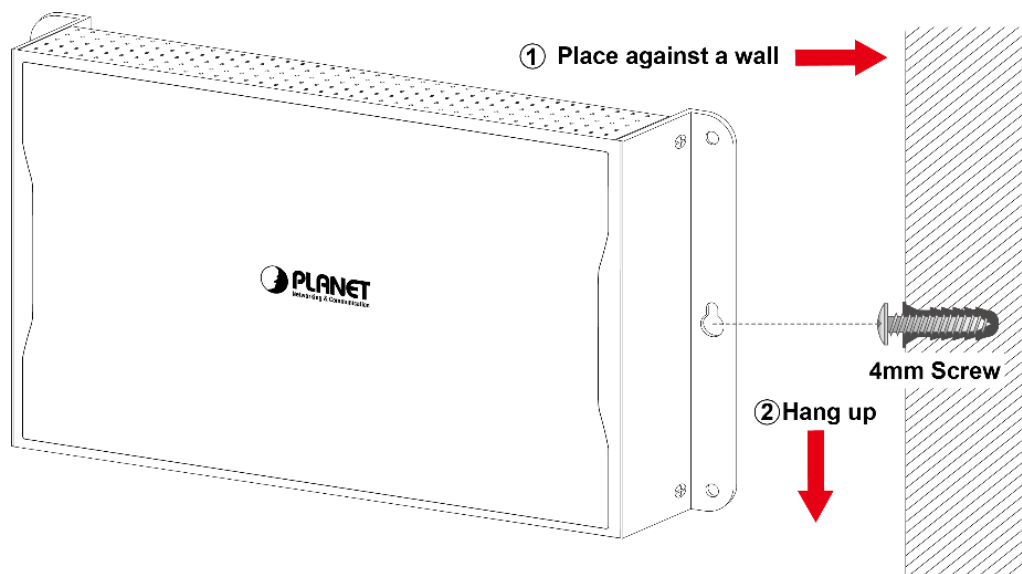
2.2.2 Wall Hanging Installation

To hang the Wall-mount Managed Switch on the wall, simply follow the following steps:

Step 1: Drill 2 holes (one hole on each side) with 8mm diameter on the wall; the distance between the 2 holes is 230 mm and the line through them must be horizontal.

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

Step 3: The switch, shown in the picture below, can now be hung on the wall.

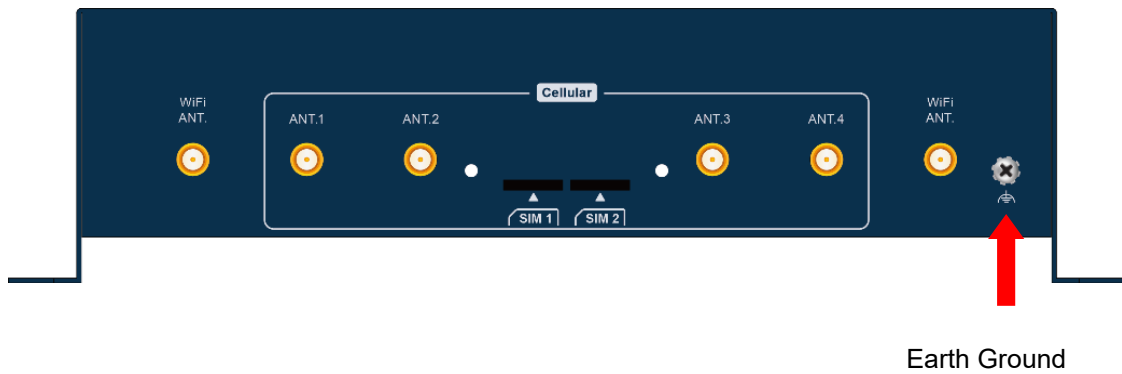


CAUTION

Make sure the equipment is securely wall-mounted as strong vibration could cause it to drop or break.

2.2.3 Grounding the Device

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



2.2.4 SIM Card Installation

A. Locate the SIM card slot on the device.



B. Insert the SIM card directly into the slot with the gold-colored contacts facing downwards, and push it in completely.

C. Make sure the SIM card is securely in place before use.

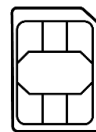
- **A Nano SIM card with 5G NR and 4G LTE subscription**



Mini SIM card



Micro SIM card

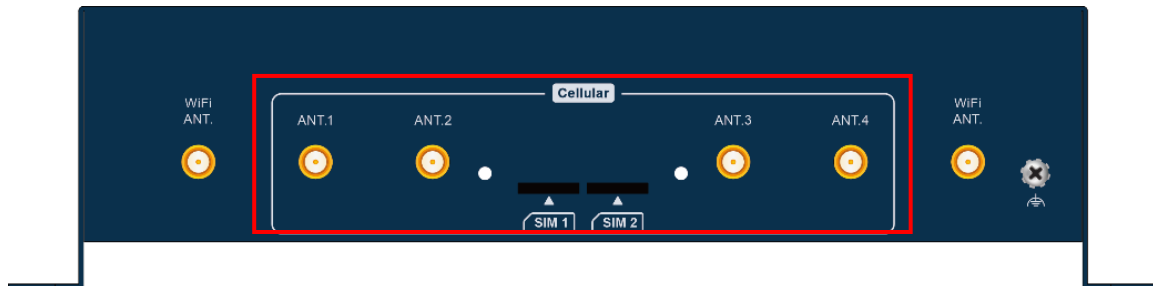


Nano SIM card

2.2.5 5G NR Antenna Installation

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

Four Female SMA Connectors



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

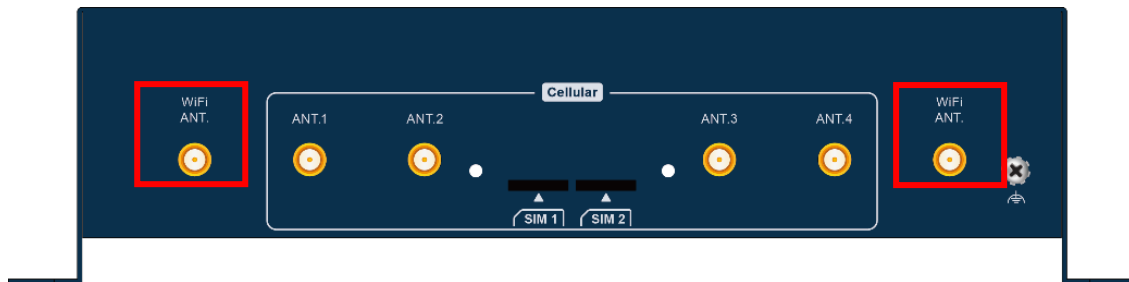


2.2.6 Wi-Fi Antenna Installation

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.

Two Wi-Fi RP-SMA connectors



Please use PLANET dual-band Wi-Fi antenna for high efficiency to avoid low efficacy.

Chapter 3. Preparation

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

3.1 Requirements

User is able to confirm the following items before configuration:

1. Please confirm the network is working properly; it is strongly suggested to test your network connection by connecting your computer directly to ISP.
2. Suggested operating systems: Windows 7/8/10/11, macOS 10.12 or later, Linux Kernel 2.6.18 or later, or other modern operating system are compatible with TCP/IP Protocols.
3. Recommended web browsers: Google Chrome, Microsoft Edge or Mozilla Firefox.

3.2 Setting TCP/IP on your PC

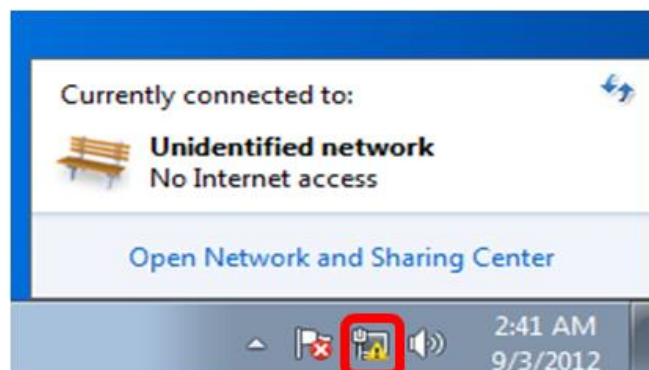
The default IP address of the cellular gateway is 192.168.1.1, and the DHCP Server is on. Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the VPN cellular gateway

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

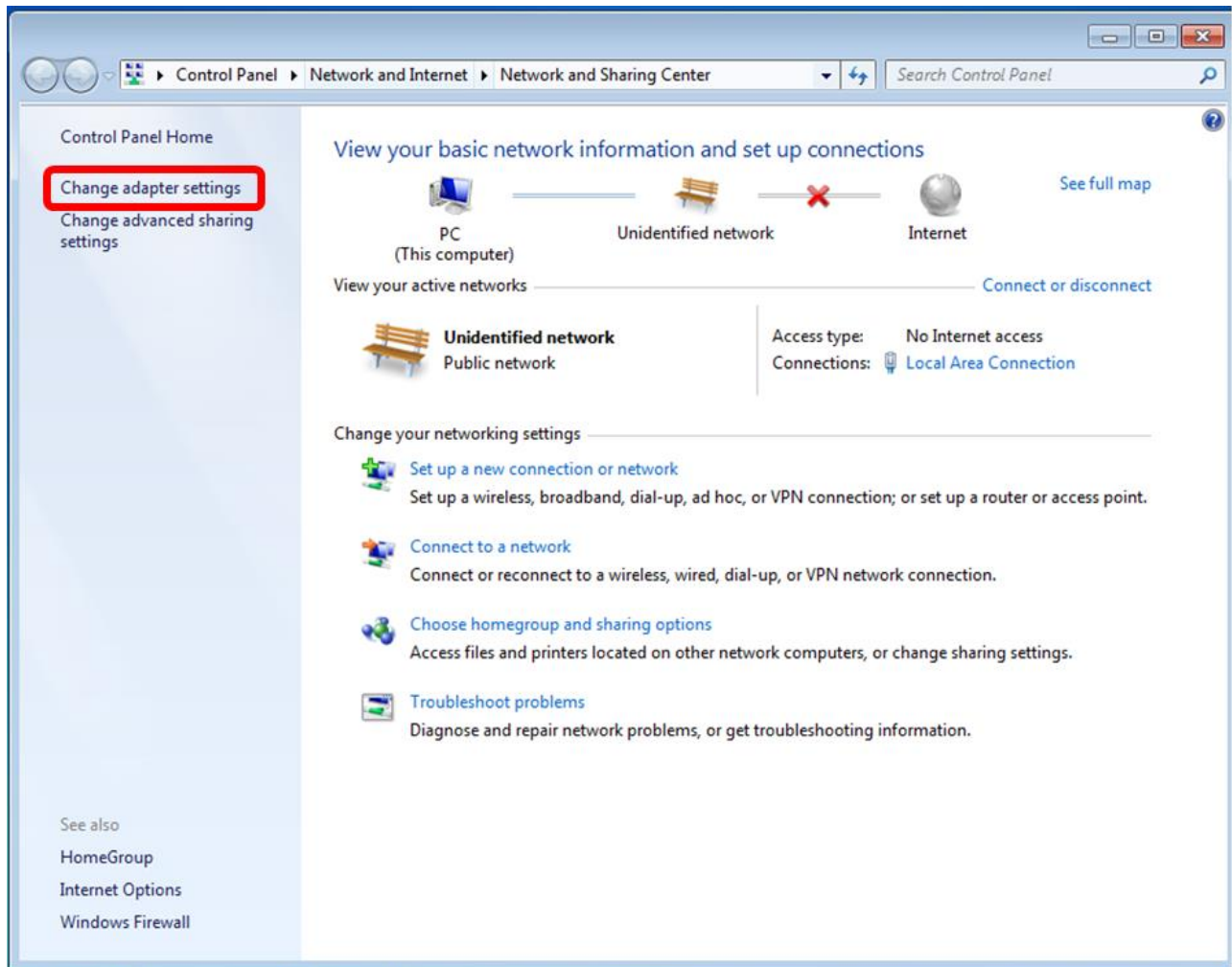
Windows 7/8

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

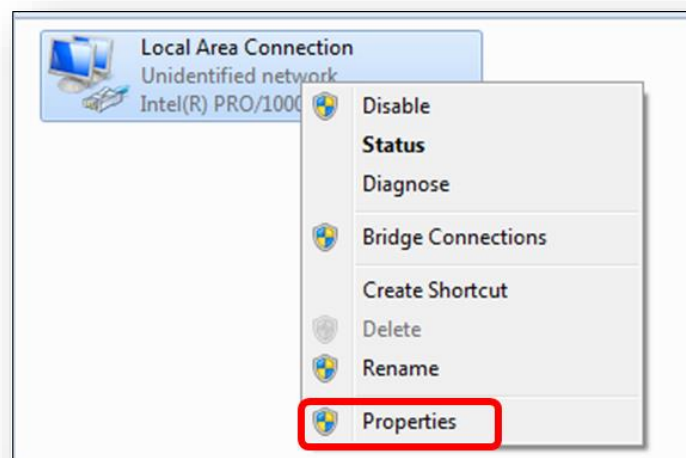
1. Click on the network icon from the right side of the taskbar and then click on "Open Network and Sharing Center".



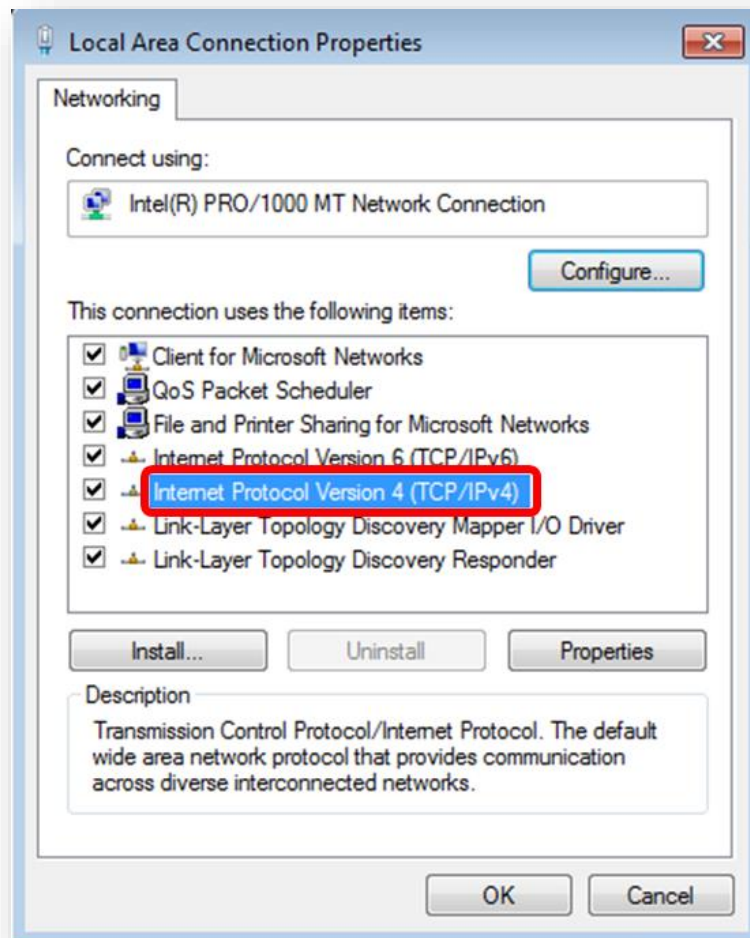
2. Click **"Change adapter settings"**.



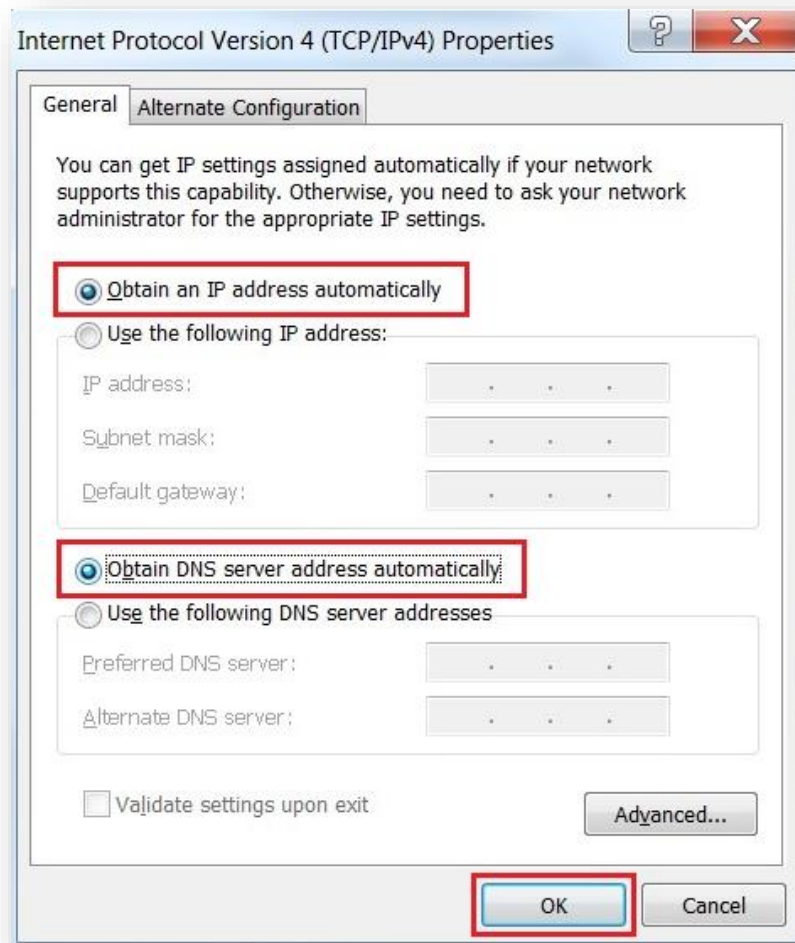
3. Right-click on the Local Area Connection and select Properties.



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



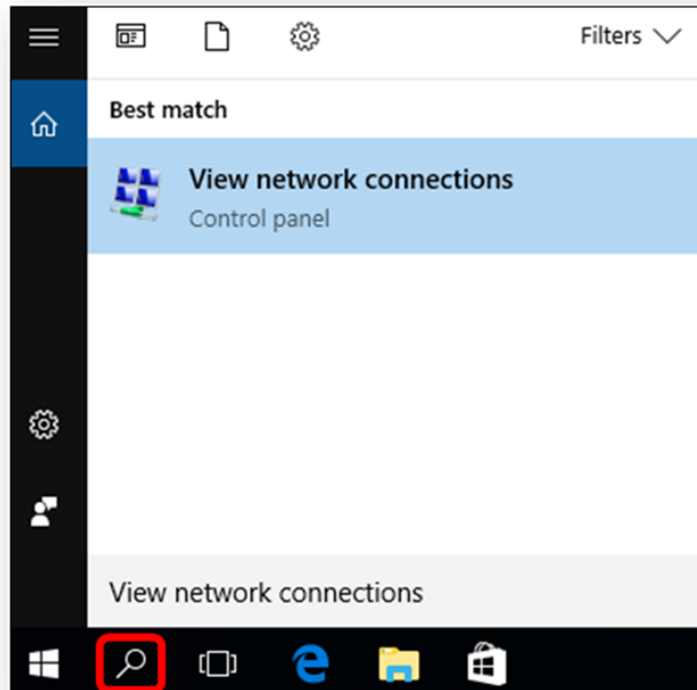
5. Select **"Use the following IP address"** and **"Obtain DNS server address automatically"**, and then click the **"OK"** button.



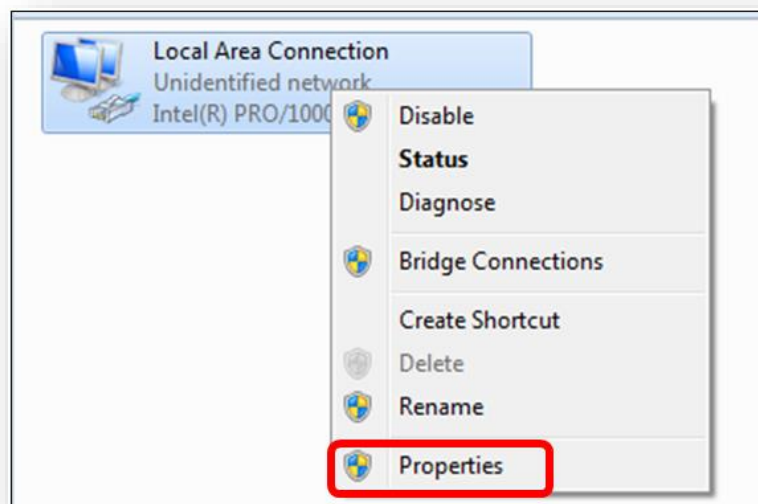
Windows 10

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

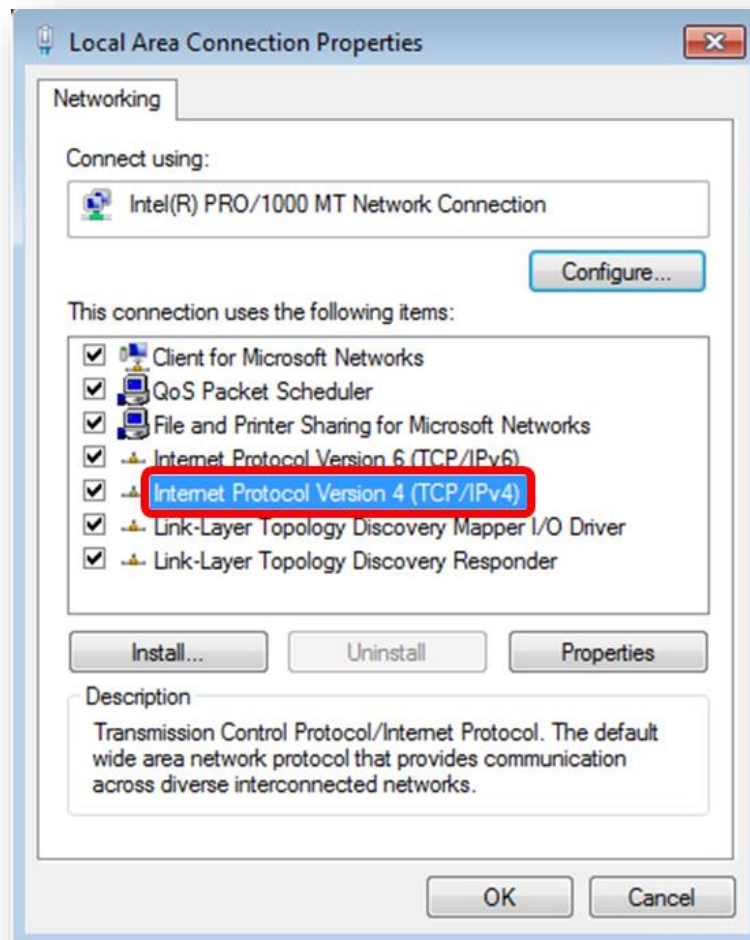
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



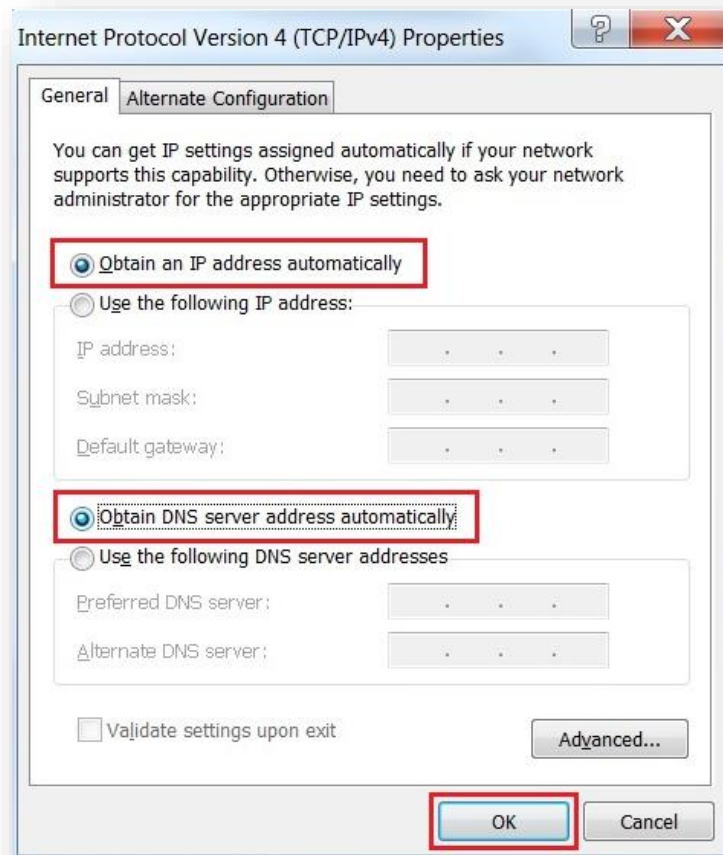
2. Right-click on the Local Area Connection and select Properties.



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



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



3.3 Planet Smart Discovery Utility

For easily listing the 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.

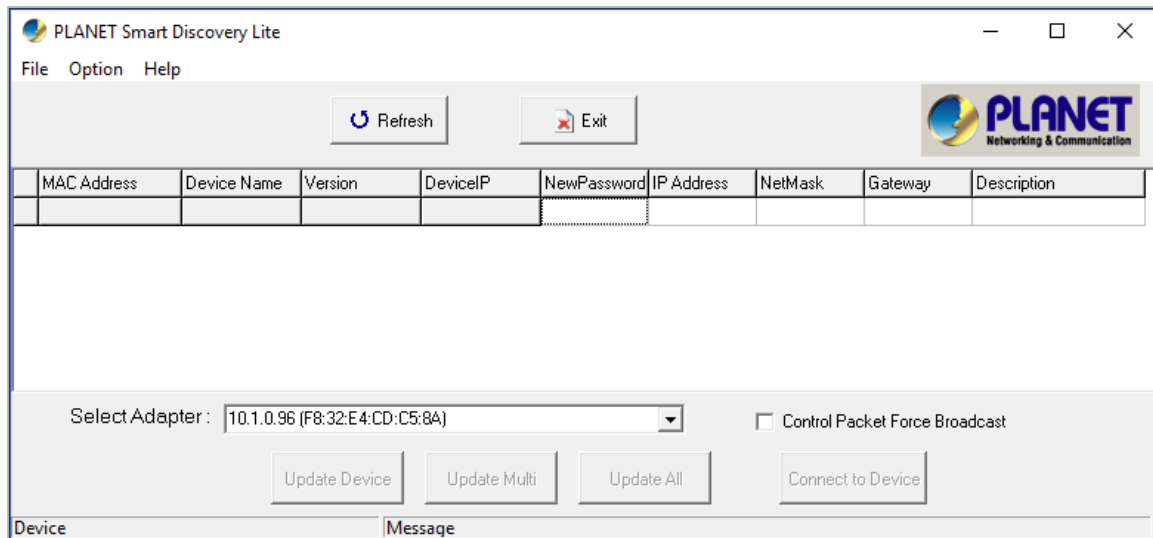


Figure 3-1-6: Planet Smart Discovery Utility Screen



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

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

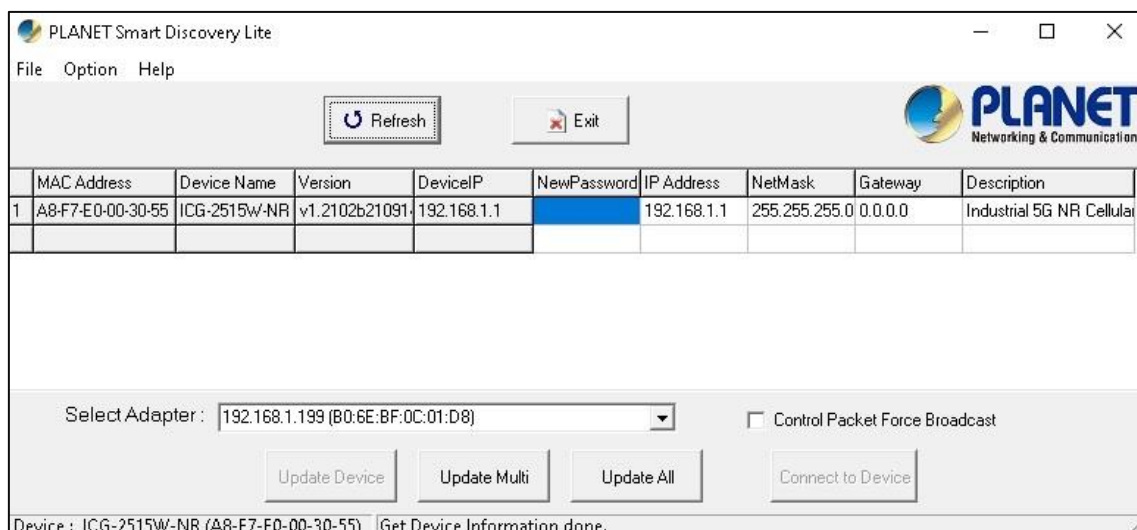


Figure 3-1-7: Planet Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.
2. After setup is completed, press the “**Update Device**”, “**Update Multi**” or “**Update All**” button to take effect. The functions of the 3 buttons above are shown below:
 - **Update Device**: use current setting on one single device.
 - **Update Multi**: use current setting on choose multi-devices.
 - **Update All**: use current setting on whole devices in the list.The same functions mentioned above also can be found in “**Option**” tools bar.
3. To click the “**Control Packet Force Broadcast**” function, it allows you to assign a new setting value to the device under a different IP subnet address.
4. Press the “**Connect to Device**” button and the Web login screen appears.

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

Chapter 4. Web-based Management

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

4.1 Introduction

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

4.2 Logging in to the 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.

Default IP address: **192.168.1.1**

Default user name: **admin**

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

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

Default SSID (5G): **PLANET_5G**

When Login dialog box appears, please enter the default user name and password. Refer to Figure 4.2-1 to determine your initial login password. Default IP address is 192.168.1.1, default username is admin and default password is cg + the last 6 characters of the MAC ID in lowercase.

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

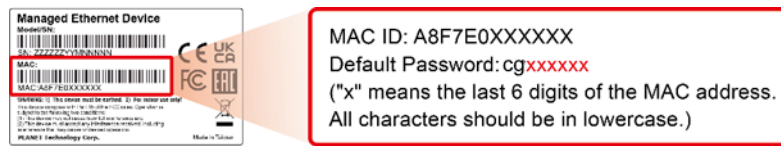


Figure 錯誤! 所指定的樣式的文字不存在文件中。-1: MAC ID Label



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

4.3 Main Web Page

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



Figure 4-3-1: Main Web Page

■ Web Panel

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



Figure 4-3-2: Web Panel

Object	Icon	Function
M12		To indicate the port comes with the M12 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 4-3-3 and 4-3-4](#).



Figure 4-3-3: Function Menu

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 (Wireless model only)
PoE	Provides PoE Management configuration of industrial wall-mount Gigabit router.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the cellular gateway



Figure 4-3-4: Function Button

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

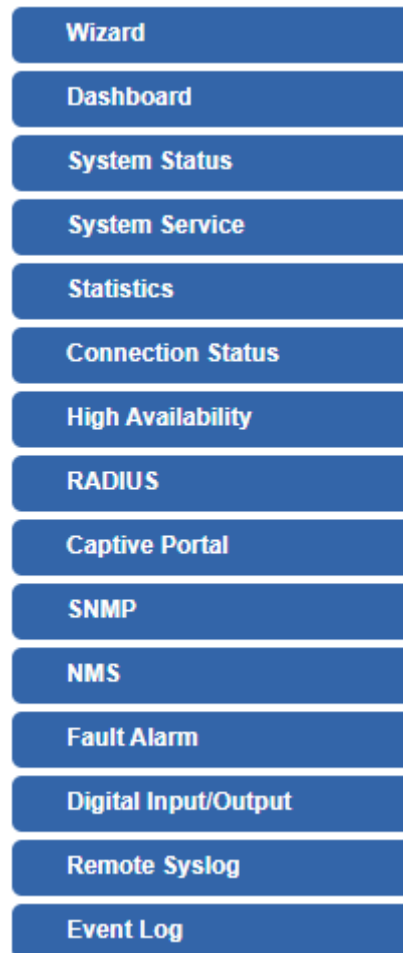


Figure 4-4-1: System Menu

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
Fault Alarm	One relay output for power failure. Alarm relay current carry ability
Digital Input/Output	Digital Input/Output Control Configuration page
Remote Syslog	Enable/Disable Remote System on cellular gateway
Event Log	Display Event Log information

4.4.1 Setup Wizard

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](#).



Figure 4-4-2: Setup Wizard

Step 1: Account Modification

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

The form displays the 'STEP 1 - Account Modification' progress bar at the top, with Step 1 'Account' highlighted. Below the progress bar, there are three input fields: 'Username' (pre-filled with 'admin'), 'Password', and 'Confirm Password'. Below these fields, a note states: 'The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols'.

Figure 4-4-3: Account Modification

Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in [Figure 4-4-4](#).

STEP 2 - Network Interface LAN

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

IP Address

Netmask

DHCP Server

Start IP Address

Maximum DHCP Users

192.168.1.1

255.255.255.0

☒

192.168.1.100

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. If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the cellular gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the 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 previously saved values.

Step 3: Priority Interface

The cellular gateway supports two access modes on the WAN side shown in [Figure 4-4-5](#)

STEP 3 - WAN Priority

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

WAN Priority Auto

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

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

Step 4: WAN Interface

The cellular gateway supports two access modes on the WAN side shown in [Figure 4-4-6](#)

STEP 4 - Network Interface WAN

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

WAN1 WAN2 LTE/NR 1 LTE/NR 2

Connection Type DHCP

IP Address

Netmask

Default Gateway

DNS Server 1

DNS Server 2

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

Mode 1 -- Static IP

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

Object	Description
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.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

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

WAN1 WAN2 LTE/NR 1 LTE/NR 2

Connection Type DHCP ▼

IP Address

Netmask

Default Gateway

DNS Server 1

DNS Server 2

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

Step 4: Wireless Setting

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

STEP 5 - Network Interface Wireless

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

2.4G WiFi Status ☒ Enable ☐ Disable

SSID

Hide SSID ☐ Enable ☒ Disable

Bandwidth 20MHz ▼

Channel 6 ▼

Encryption Open ▼

5G WiFi Status ☒ Enable ☐ Disable

SSID

Hide SSID ☐ Enable ☒ Disable

Bandwidth 80MHz ▼

Channel 36 ▼

Encryption Open ▼

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

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

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

Step 5: Security Setting

Set up the Security Settings as shown in [Figure 4-4-10](#).

STEP 6 - Security Settings

1
Account

2
LAN

3
Priority

4
WAN

5
Wireless

6
Security

7
Completed

SPI Firewall

Block SYN Flood

Block ICMP Flood

Block WAN Ping

Remote Management

☒ Enable ☐ Disable

☒ Enable ☐ Disable

☐ Enable ☒ Disable

☐ Enable ☒ Disable

☐ Enable ☒ Disable

Figure 4-4-10: Setup Wizard –Security Setting

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

Step 6: Setup Completed

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

STEP 7 - Setup Completed

1
Account

2
LAN

3
Priority

4
WAN

5
Wireless

6
Security

7
Completed

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

[Previous](#)
[Finish](#)

Figure 4-4-11: Setup Wizard – Setup Completed

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

4.4.2 Dashboard

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

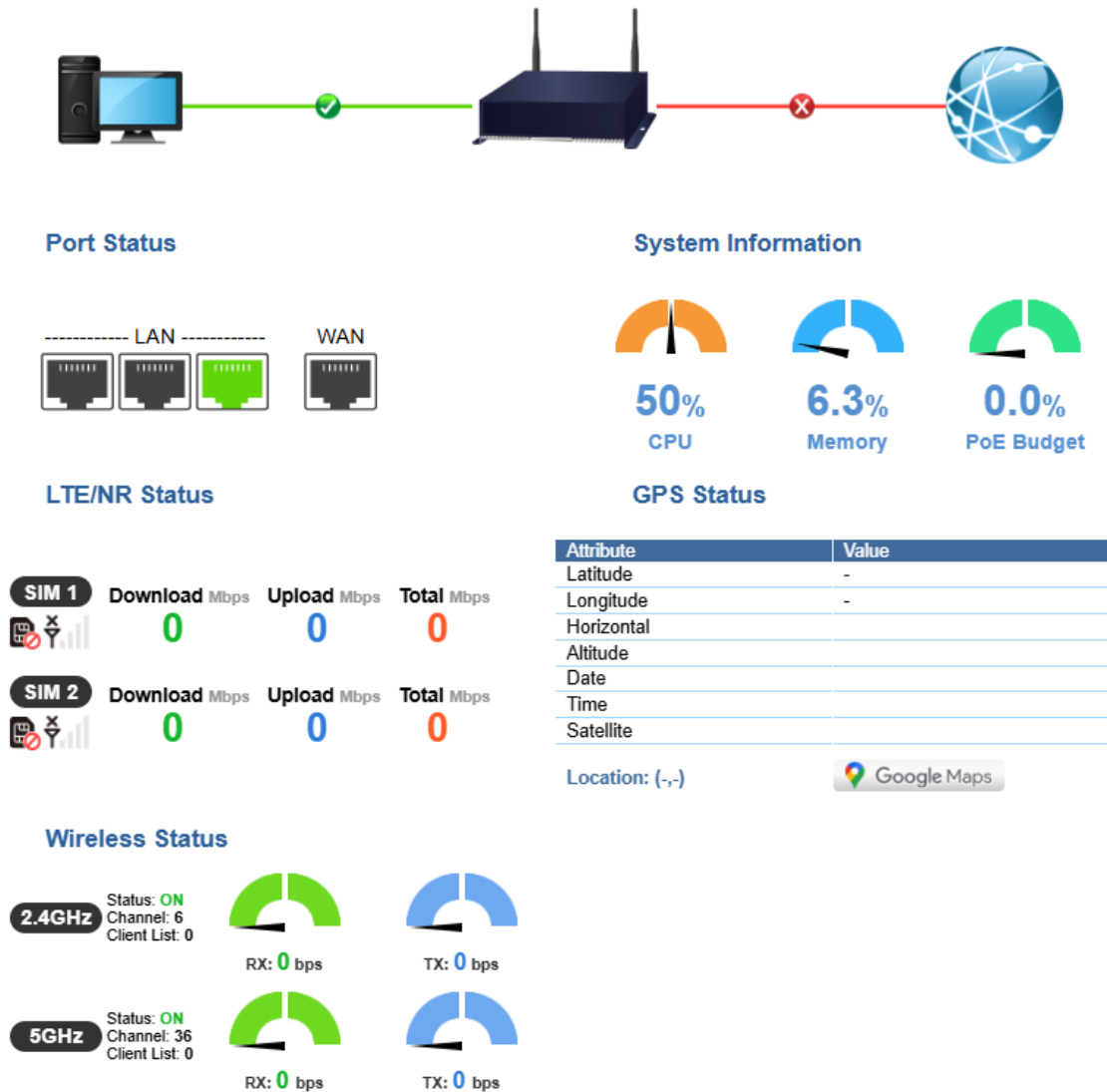


Figure 4-4-12: Dashboard

WAN/LAN Connection Status

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

Port Status

Object	Description
	Ethernet port is in use.
	Ethernet port is not in use.

System Information

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

LTE/NR Status

Object	Description
SIM	SIM signal ■  5G signal ■  4G signal ■  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](#).

Device Information	
Model Name	VCG-2406WP-NR
Firmware Version	v1.2102b250917
Region	ETSI
Current Time	2025-12-10 Wednesday 13:29:51
Running Time	0 day, 03:17:36
Power Status	PWR1:OFF, PWR2:ON
Alarm Status	Normal
DI and DO Status	Normal

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

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

2.4GHz WiFi	
Status	ON
SSID	PLANET_2.4G
Channel	6
Encryption	WPA2 Personal (TKIP+AES)
MAC Address	A8:F7:E0:87:85:5C

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

LTE/NR 1	
Activated SIM	SIM1
SIM Status	Ready
Operator	Far EasTone
IP Address	10.230.118.25
Netmask	255.255.255.252
Default Gateway	10.230.118.26
Running Time	00:13:06
Roaming	No

Figure 4-4-13: System Status

4.4.4 System Service

This page displays system service information as shown in [Figure 4-4-14](#).

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

Secured Server Service			
#	Action	Service	Status
1	✓ Enabled	Cybersecurity	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	✗ Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32
6	✗ Disabled	IPSec VPN Server	(Active / Maximum Tunnels) 0 / 32
7	✗ Disabled	GRE	(Active / Maximum Tunnels) 0 / 5
8	✗ Disabled	PPTP	(Active / Maximum Tunnels) 0 / 91
9	✗ Disabled	SSL VPN	(Active / Maximum Tunnels) 0 / 100
10	✗ Disabled	L2TP	(Active Tunnels) 0

Figure 4-4-14: System Service

4.4.5 Statistics

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

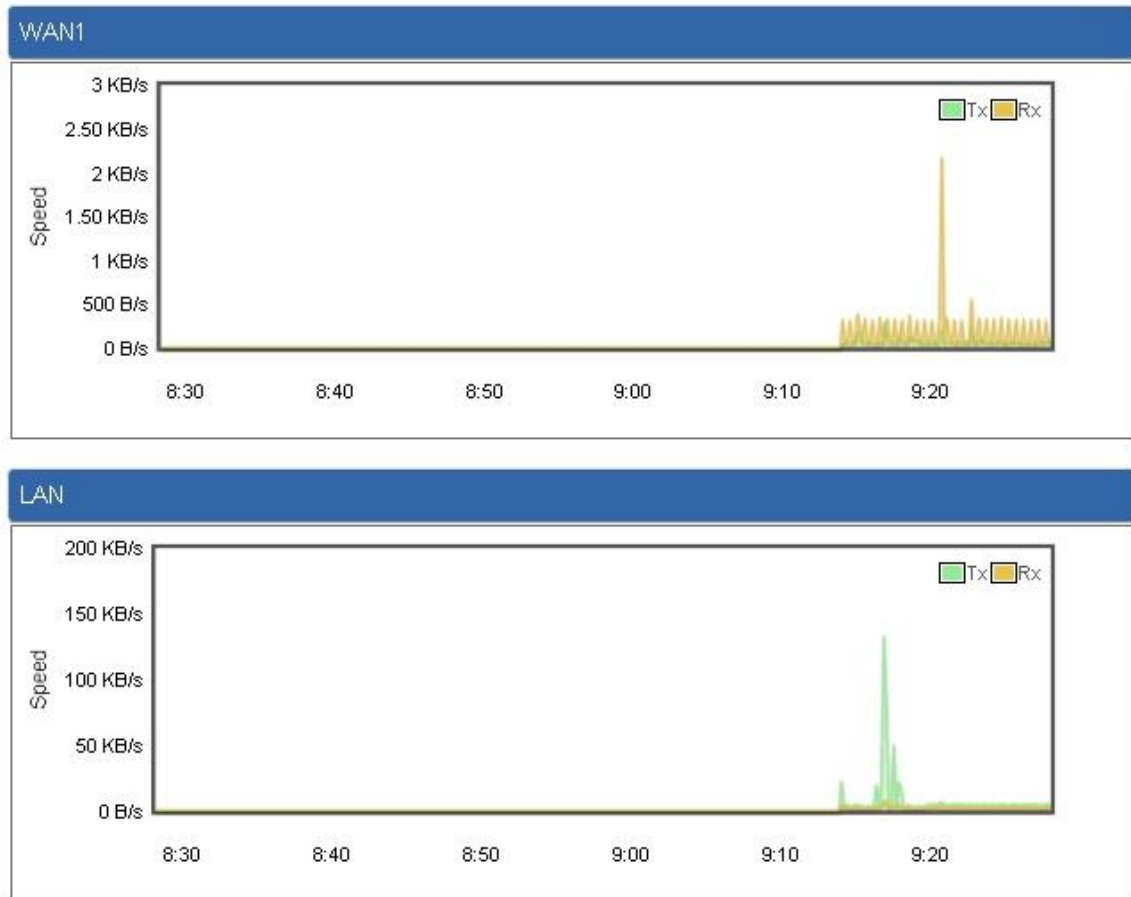


Figure 4-4-15: Statistics

4.4.6 Connection Status

The page shows the DHCP Table and ARP Table. The status is shown in [Figure 4-4-16](#).

DHCP Table			
Name	IP Address	MAC Address	Expiration Time

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

Figure 4-4-16: Connection Status

4.4.7 High Availability

High Availability (HA) is a system redundant that two cellular gateway of VCG-2406WP-NR 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 shows the High Availability configuration. The High Availability page is shown in [Figure 4-4-17](#).

High Availability Configuration

High Availability

Username

Password

Mode

Virtual IP address

Virtual IP Mask

Interface

Connected Status

☒ Enable
 ☐ Disable

Master ▾

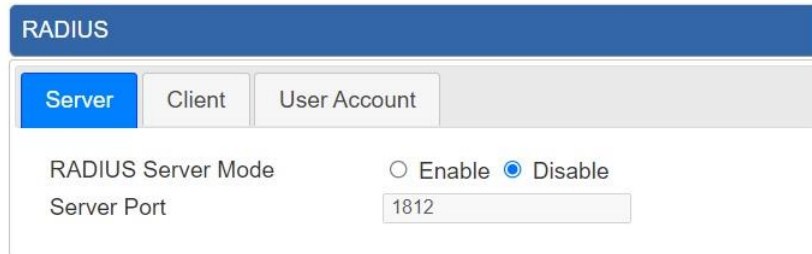
LAN ▾

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

4.4.8 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](#).

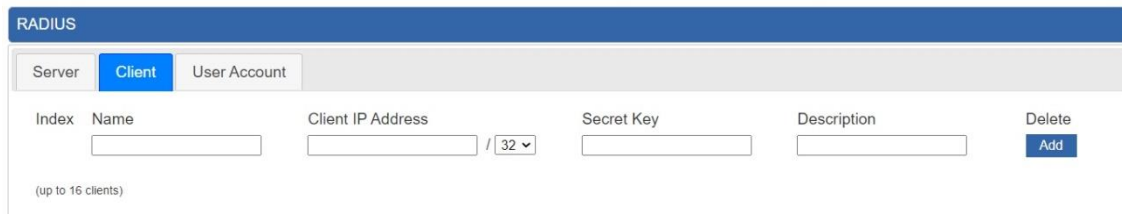


The screenshot shows the 'RADIUS' configuration page with three tabs: 'Server' (selected), 'Client', and 'User Account'. Under the 'Server' tab, there are two settings: 'RADIUS Server Mode' with radio buttons for 'Enable' and 'Disable' (where 'Disable' is selected), and 'Server Port' with a text input field containing the value '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](#).



The screenshot shows the 'RADIUS' configuration page with three tabs: 'Server', 'Client' (selected), and 'User Account'. Under the 'Client' tab, there is a table for adding clients. The table has columns: 'Index', 'Name', 'Client IP Address', 'Secret Key', 'Description', and 'Delete'. The 'Client IP Address' column includes a dropdown menu showing '32'. Below the table, there is a note '(up to 16 clients)'. An 'Add' button is located at the bottom right of the table.

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

4.4.9 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](#).

Captive Portal

Config

Custom

Captive Portal

☐ Enable ☒ Disable

Interfaces

LAN Subnet 1 ▼

Authentication Type

Local RADIUS Server

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

Captive Portal

Config

Custom

Background

fffff

Title Word Color

3365a9

Description Word Color

949494

Title

PLANET Captive Portal

(Max 256 characters. Allow special symbols and HTML.)

Description

Welcome to PLANET!

(Max 1280 characters. Allow special symbols and HTML.)

Current Image



Upload Image

選擇檔案

未選擇任何檔案

Size: up to 1M

Format Limit: .jpg .gif .bmp .png

ent-2

Apply Settings

Cancel Changes

Preview

4.4.10 SNMP

This page provides SNMP setting as shown in [Figure 4-4-21](#).

SNMP

SNMP

☒ Enable ☐ Disable

SNMP Versions

SNMP v1,v2c ▼

Read Community

public

Write Community

private

Engine ID

SNMP v3 Security Level

AuthPriv ▼

SNMP v3 User Name

SNMP v3 Auth Protocol

MD5 ▼

SNMP v3 Auth Password

SNMP v3 Privacy Protocol

DES ▼

SNMP v3 Privacy Password

System Identification

System Name

VR-300P

System Location

System Contact

sales@planet.com.tw

Apply Settings

Cancel Changes

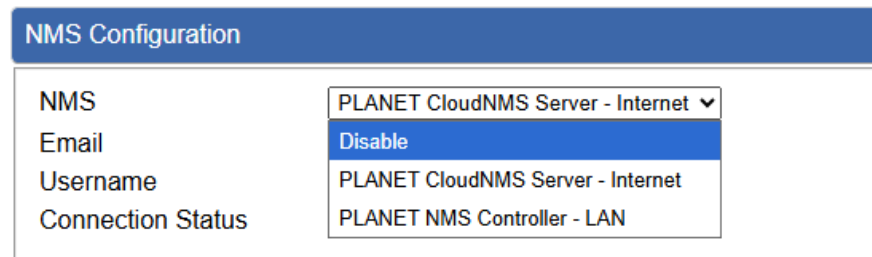
Figure 4-4-21: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the 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.
Cancel Changes	Press this button to undo any changes made locally and revert to previously saved values.

4.4.11 NMS

The VCG-2406WP-NR can support both NMS controller and CloudNMS Sever for remote management. PLANET's NMS Controller is a Network Management System that can monitor all kinds of deployed network devices, such as managed switches, media converters, routers, smart APs, VoIP phones, IP cameras, etc., compliant with the SNMP Protocol, ONVIF Protocol and PLANET Smart Discovery utility. The CloudNMS is a free networking service designed for PLANET Products. This service provides simplified network monitoring and real-time network status. Working with PLANET CloudNMS 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.



The screenshot shows the 'NMS Configuration' page. It features a dropdown menu for 'NMS' with the following options: 'PLANET CloudNMS Server - Internet', 'Disable', 'PLANET CloudNMS Server - Internet', and 'PLANET NMS Controller - LAN'. The 'Email' field is set to 'Disable'. The 'Username' field is set to 'PLANET CloudNMS Server - Internet'. The 'Connection Status' field is set to 'PLANET NMS Controller - LAN'.

Figure 4-4-22 NMS Configuration Page

The NMS Controller – LAN Configuration screens in [Figure 4-4-23](#) appear.



The screenshot shows the 'NMS Controller – LAN Configuration' page. It features a dropdown menu for 'NMS' with the following options: 'PLANET NMS Controller - LAN'. The 'NMS Controller IP address' field is empty. The 'Authorization Status' field shows a key icon and the text 'Unauthorized'. At the bottom, there are three buttons: 'Apply Settings', 'Cancel Changes', and 'Unbind'.

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

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

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

NMS Configuration

NMS

PLANET CloudNMS Server - Internet ▼

Email

Username

Connection Status

Not enabled

Apply Settings

Cancel Changes

Unbind

Figure 4-4-24 CloudNMS Server

Object	Description
Email	The email registered on CloudNMS Server
Password	The password of your CloudNMS account
Connection Status	Indicates the status of connecting CloudNMS Server

Step 1: Enable the Service

Go to the NMS Configuration page of the WDAP-W3600BE and enable PLANET CloudNMS Server – Internet feature.

System
Network
Wireless
Maintenance

Operation Mode
Dashboard
System Status
System Service
Statistics
Connection Status
RADIUS
SNMP
NMS
Remote Syslog
Event Log

NMS Configuration

NMS

Disable ▼

Disable

PLANET CloudNMS Server - Internet

Apply Settings

Cancel Changes

System
Network
Wireless
Maintenance

Operation Mode
Dashboard
System Status
System Service
Statistics
Connection Status
RADIUS
SNMP
NMS
Remote Syslog
Event Log

NMS Configuration

NMS
PLANET CloudNMS Server - Internet

Email
Username
Connection Status
Success

Apply Settings
Cancel Changes
Unbind



Scan this QR code with the CloudNMS App to add the service

Step 2: Access the CloudNMS Platform

Open a browser and go to <https://www.cloudnms.planet.com.tw>,
or download the PLANET CloudNMS App from the App Store or Google Play.

Web:



Get APP



PLANET CloudNMS

Username
Password

☒ Remember Me
Forgot Password?

LOGIN

Sign in with


Don't have an account? Sign up
Term of Use | Support list

App:

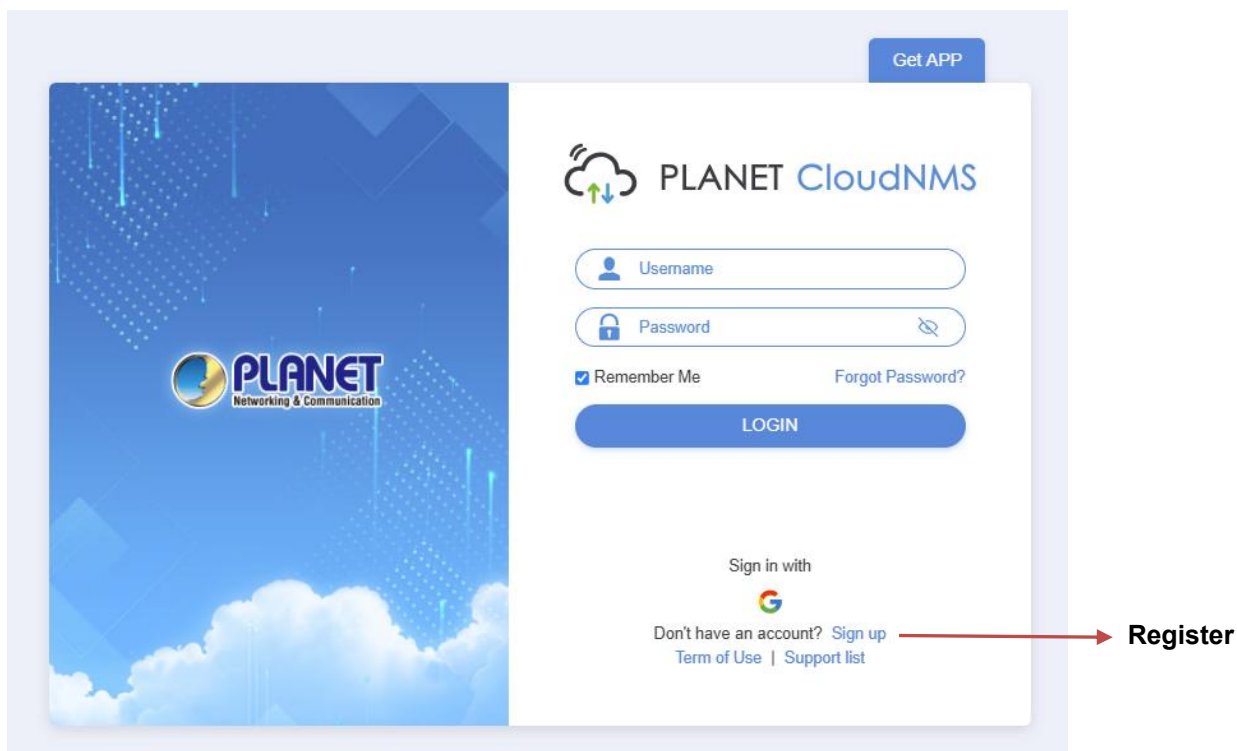


Step 3: Register an Account

Launch the PLANET CloudNMS Platform or App, and log in with your CloudNMS account.

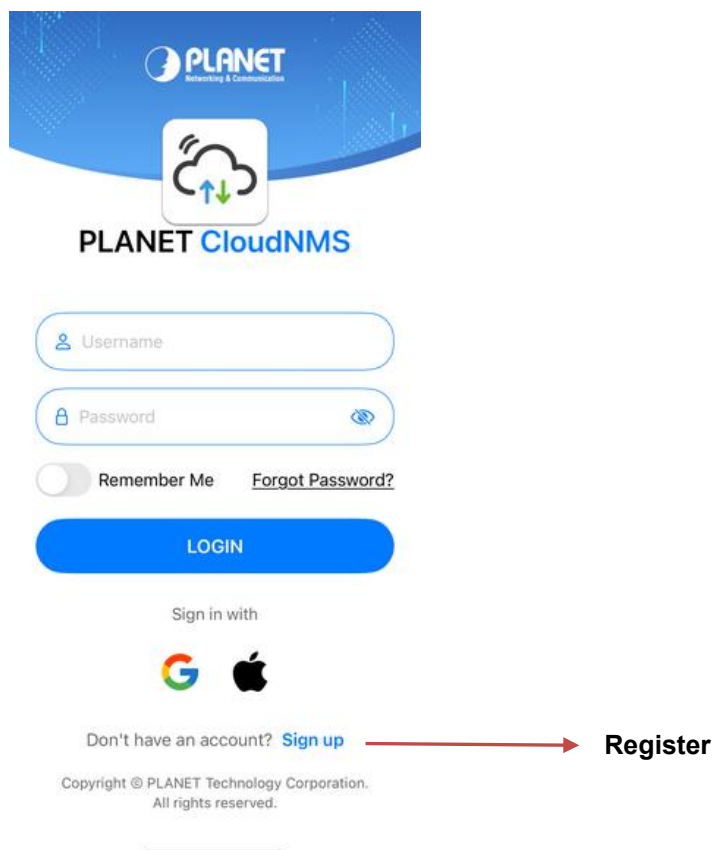
If you don't have an account, register one with your e-mail address first, or use SSO.

Web:



The image shows the web login page for PLANET CloudNMS. On the left is a large blue graphic with the PLANET logo and a cloud background. On the right is a white login form. At the top right of the form is a 'Get APP' button. The form contains a 'PLANET CloudNMS' header, a 'Username' input field, a 'Password' input field with a toggle icon, a 'Remember Me' checkbox, and a 'Forgot Password?' link. Below these is a blue 'LOGIN' button. At the bottom, it says 'Sign in with' followed by a Google icon. Below that is a link 'Don't have an account? Sign up' with a red arrow pointing to the word 'Register'. At the very bottom are links for 'Term of Use' and 'Support list'.

App:



The image shows the app login page for PLANET CloudNMS. It features a blue header with the PLANET logo. Below the header is a white login form. The form contains a 'PLANET CloudNMS' header, a 'Username' input field, a 'Password' input field with a toggle icon, a 'Remember Me' toggle switch, and a 'Forgot Password?' link. Below these is a blue 'LOGIN' button. At the bottom, it says 'Sign in with' followed by Google and Apple icons. Below that is a link 'Don't have an account? Sign up' with a red arrow pointing to the word 'Register'. At the very bottom is a copyright notice: 'Copyright © PLANET Technology Corporation. All rights reserved.'

Step 4: Bind the Device**Via Web:**

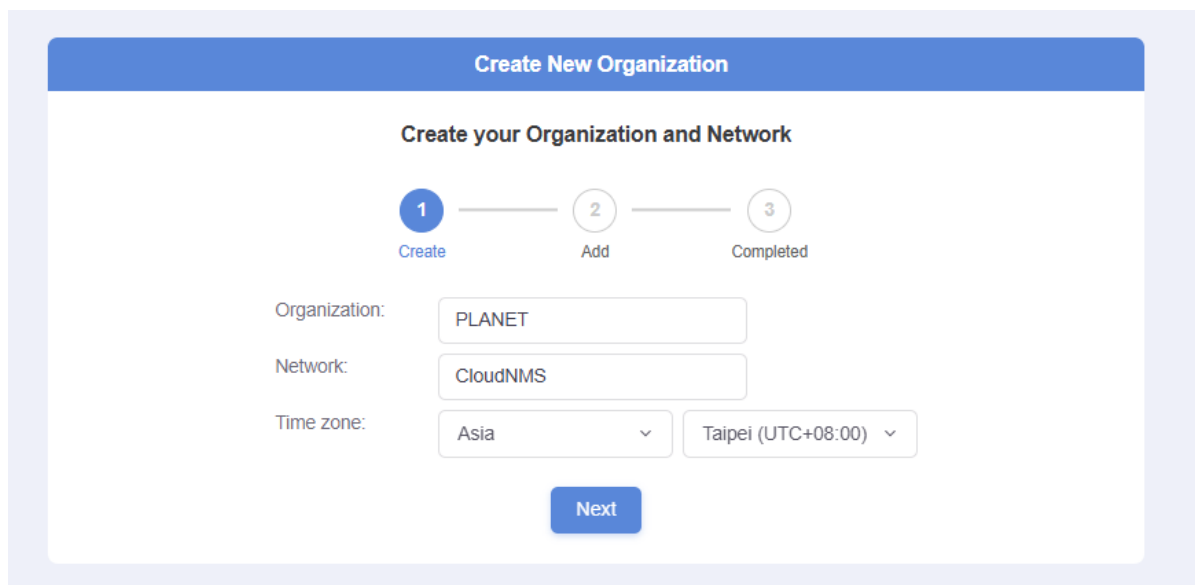
- Log in to the PLANET CloudNMS Platform.
- Create an Organization and a Network for the device.
- Enter the required device information and complete the setup wizard.

Via App:

- Launch the PLANET CloudNMS App and sign in with your CloudNMS account.
- Create an Organization and a Network for the device, then go to the Add Device process.
- Enter the required device information or Scan the QR code of the device, and complete the setup wizard.

Web:

1. Create an Organization and a Network



Create New Organization

Create your Organization and Network

1 — 2 — 3
Create Add Completed

Organization:

Network:

Time zone:

Next

2. Enter the required device information

Create New Organization

Add your device(s) to PLANET CloudNMS

1
Create

2
Add

3
Completed

+ Add

1 Devices

Download Import Template

Import

MAC Address	Serial Number	Name	Model
a8:f7:e0:1 Format: XX:XX:XX:XX:XX:XX	XXXXXXXXXXXX Enter a 14-character serial number	Switch 01 Enter the device name	VCG-2406WP-NR

☐ Auto-skip invalid devices

Back

Next

3. Finish

Create New Organization

New Organization Information

1
Create

2
Add

3
Completed

Organization Information

Organization	PLANET
Network	CloudNMS
Time Zone	Asia/Taipei

Devices

0
Switch(es)

1
Access point(s)

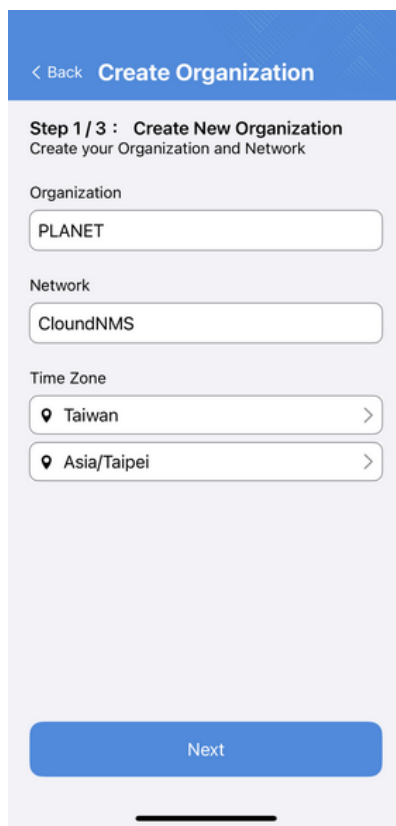
0
Router(s)

Download Import History

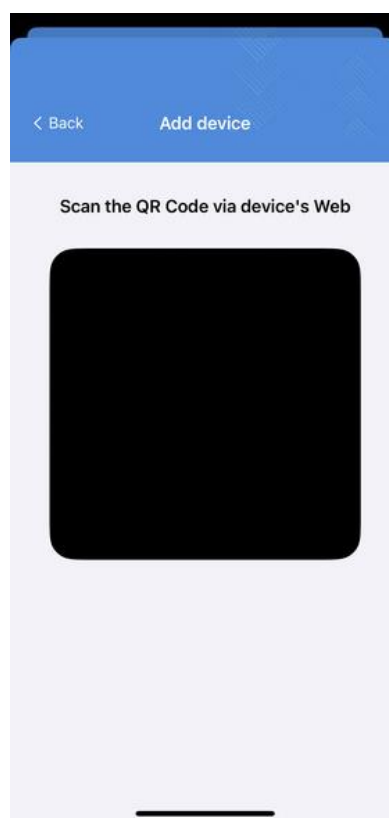
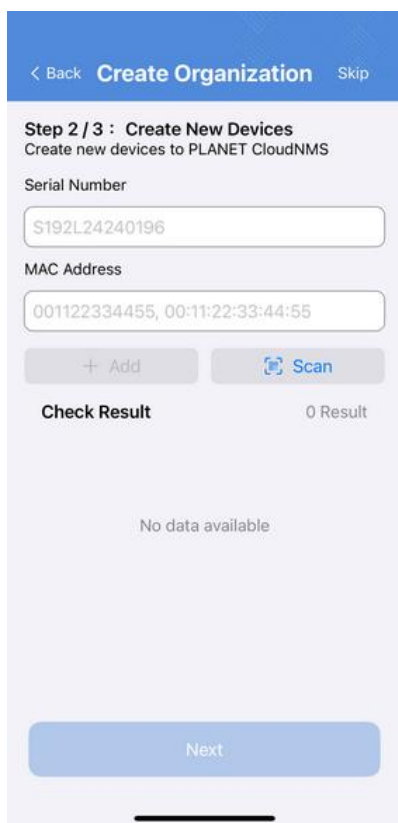
Finish Setup and Go to Dashboard

App:

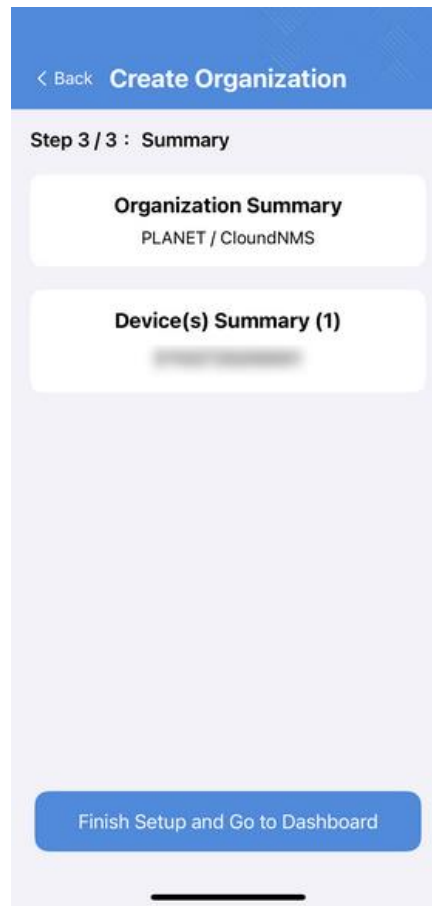
1. Create an Organization and a Network



2. Enter the required device information or Scan QR code

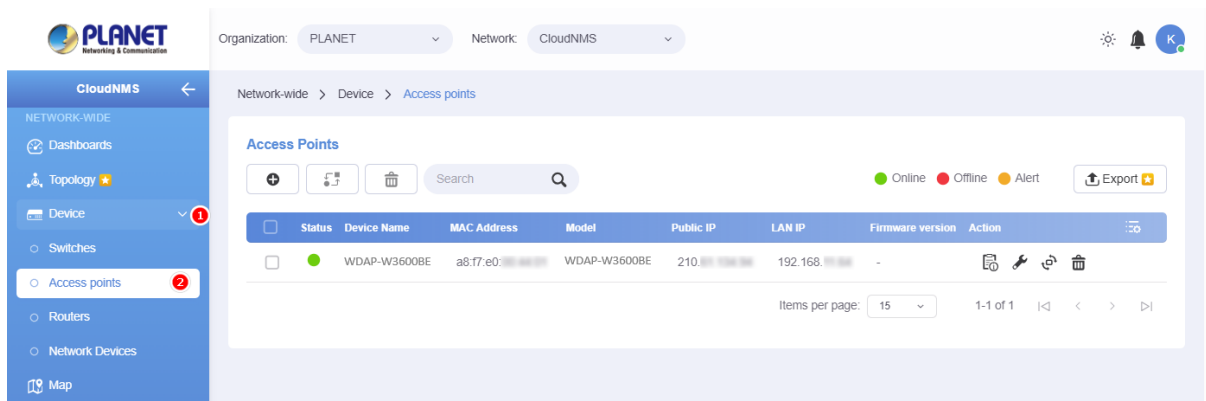


3. Finish

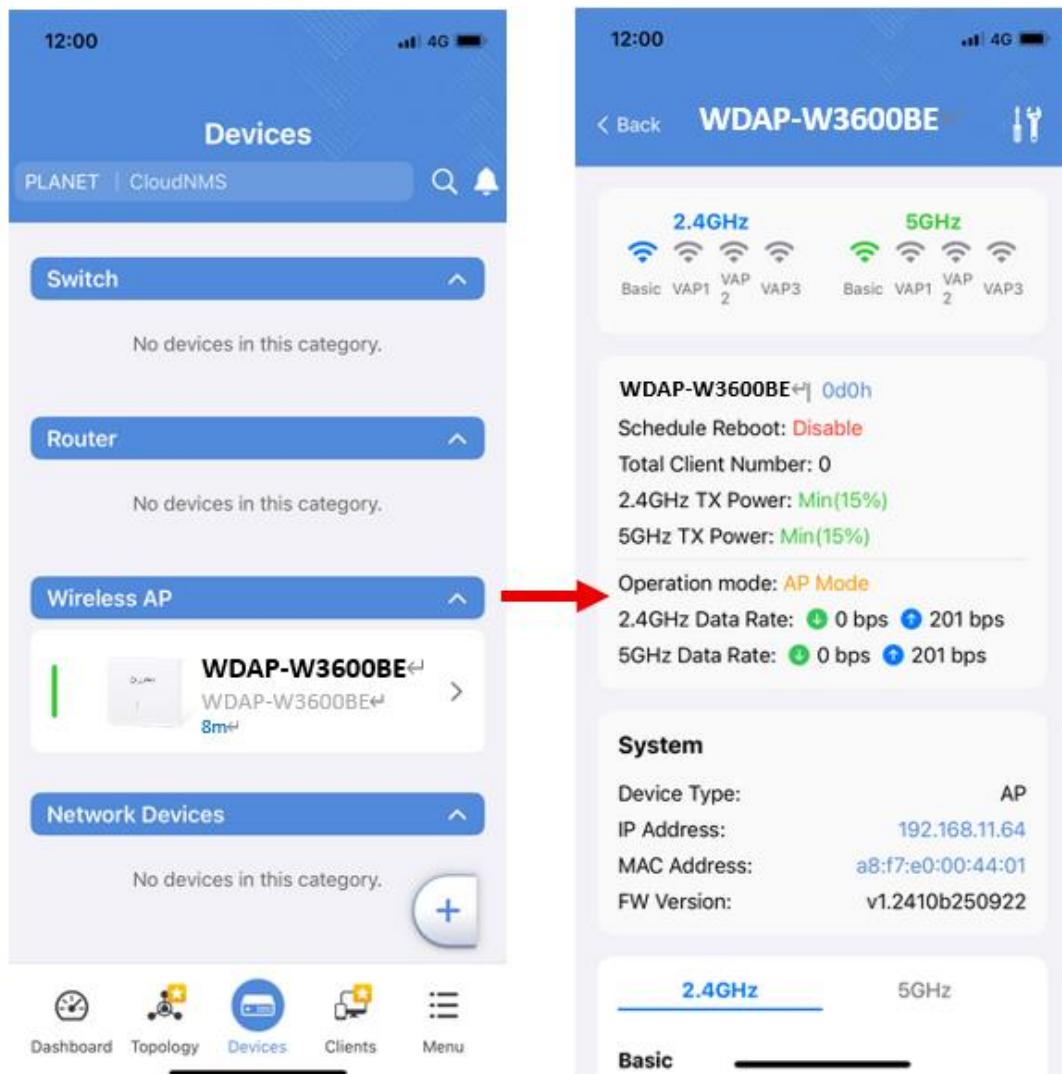


Step 5: Finish

Web:



App:



The following screen based on the WDAP-W3600BE is the same as the VCG-2406WP-NR.

4.4.12 Fault Alarm

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

Fault Alarm Control Configuration

Fault Alarm Output					
Enable	☐ Enable				
Record	☐ System Log ☐ SMS				
Event	☐ Power Fail ☐ Port Fail				
Power Alarm	☐ PWR1 ☐ PWR2				
Port Alarm	1	2	3	4	5
	☐	☐	☐	☐	☐

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 or Power is not working.
Power Alarm	Controls whether PWR1 or PWR2 or both are not working.
Port Alarm	Controls whether a port or ports is/ are not working.

4.4.13 Digital Input / Output

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

Digital Input/Output Control Configuration

Digital Input 0

Enable	☐ Enable
DI Condition	High to Low ▼
Event Description	
Action	☐ System Log ☐ SMS

Digital Output 0

Enable	☐ Enable		
Action	☐ Power Fail	☐ Port Fail	☐ DI 0
DO Condition	High to Low ▼		
Power Alarm	☐ PWR1	☐ PWR2	
Port Fail Alarm	1 ☐	2 ☐	3 ☐ 4 ☐

Figure 4-4-26: Digital Input / Output

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 customized 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) which means if Digital Output has detected these events, then Digital 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.

4.4.14 Remote Syslog

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

Remote Syslog

Enable	☐
Syslog Server	
Port Destination	(1~65535)

Figure 4-4-27: Connection Status

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](#).



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. The default configuration is disabled.
UPnP	Disable or enable the UPnP function.

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

4.5.1 Priority

This page provides WAN priority setting as shown in [Figure 4-5-2](#).

Priority

WAN Priority

Auto ▼

Figure 4-5-2: Priority

Object	Description
WAN Priority	■ Auto: WAN Ethernet is first priority and second priority is NR/LTE. The default is auto. ■ LTE/NR Only: The priority is only LTE/NR ■ ETH Only: The priority is only Ethernet. ■ LTE/NR First: LTE/NR is first priority and second priority is Ethernet

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

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2

WAN2

WAN
☐ Enable ☒ Disable

Connection Type

IP Address

Netmask

Gateway

DNS Server 1

DNS Server 2

Figure 4-5-3: WAN

Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.	
	Static	Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP. 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. IP Address Enter the IP address assigned by your ISP.

Object	Description
	Netmask 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.
	DHCP Select DHCP Client to obtain IP Address information automatically from your ISP.



Note

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

3 ▾

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

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

Apply Settings

Cancel Changes

Figure 4-5-4: LAN Setup

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

4.5.4 LAN Setup

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

LAN Configuration

IP Address	192.168.1.1
Netmask	255.255.255.0

Apply Settings

Cancel Changes

Figure 4-5-5: LAN Setup

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

4.5.5 Multi-Subnet

This page provides multi-subnet setting as shown in [Figure 4-5-6](#).

Multi-Subnet Configuration			
Name	Network		DHCP Server
LAN Subnet 1	IP Address	192.168.1.1	V
	Netmask	255.255.255.0	
LAN Subnet 2	IP Address	192.168.3.1	☒
	Netmask	255.255.255.0	
LAN Subnet 3	IP Address	192.168.5.1	☒
	Netmask	255.255.255.0	
LAN Subnet 4	IP Address	192.168.7.1	☒
	Netmask	255.255.255.0	

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](#).

Routing config list							
Number	Type	Destination	Netmask	Gateway	Interface	Comment	Action

Current Routing table in the system				
Number	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.0.180	LOCAL
2	0.0.0.0	0.0.0.0	192.168.1.18	WAN1
3	0.0.0.0	0.0.0.0	192.168.1.19	WAN2
4	192.168.0.0	255.255.255.0	0.0.0.0	LAN
5	192.168.1.0	255.255.255.0	0.0.0.0	WAN1
6	192.168.1.0	255.255.255.0	0.0.0.0	WAN2

Add Route

Figure 4-5-7: Routing table

Add a routing rule

Type	Host ▼
Destination	
Netmask	255.255.255.255 /32 ▼
Gateway	
Interface	LAN ▼
Comment	

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

4.5.7 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

WAN2 IPv6 Setting

Connection Type

IPv6 Address

Subnet Prefix Length

Default Gateway

Apply Settings
Cancel Changes

Figure 4-5-9: IPv6 WAN setup

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

4.5.8 DHCP

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

DHCP Server

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

Figure 4-5-10: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the cellular gateway will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the cellular gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the 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.
Set DNS	By default, it is set as Automatically, and the DNS server is the cellular gateway's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the cellular gateway Default is 1440 minutes.
Domain Name	Input a domain name for the cellular gateway 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** (<http://www.planetddns.com>) and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in [Figure 4-5-11](#).

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 (<http://www.planetddns.com>). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

PLANET Easy DDNS

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your cellular gateway, and check the DDNS menu and just enable it. You don't need to go to <http://www.planetddns.com> to apply for a new account. Once you enabled the Easy DDNS, your PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the 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 Service	☒ Enable ☐ Disable
Interface	WAN1 ▼
DDNS Type	PLANET DDNS ▼
Easy DDNS	Disable ▼
User Name	
Password	
Host Name	
Interval	120
Update Status	unknow status

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

4.5.10 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

☐ Enable
 ☒ Disable

MAC Address

MAC Address Clone - WAN2

Clone WAN MAC

☐ Enable
 ☒ Disable

MAC Address

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.



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.
MTU	Maximum transfer unit, Default is 1500 .

4.6.2 LTE/NR Advanced

This page provides LTE/NR advanced configuration as shown in [Figure 4-6-3](#).

LTE/NR Advanced

Current SIM Card

SIM 1 Disconnect

Disable Roaming

☒ Yes ☐ No

Used SIM

☒ Dual SIM ☐ SIM1 ☐ SIM2

SIM Priority

☒ Auto ☐ SIM1 ☐ SIM2

Roaming Switch

☐ Switch to another SIM when roaming is detected

Connect Retry Number

(1~100)*60 seconds

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

SIM1

SIM2

SIM PIN

Confirmed SIM PIN

APN

Username

Password

Confirmed Password

Auth

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
Roaming Switch	Switch to another SIM when roaming is detected. System will switch to 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.
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](#).

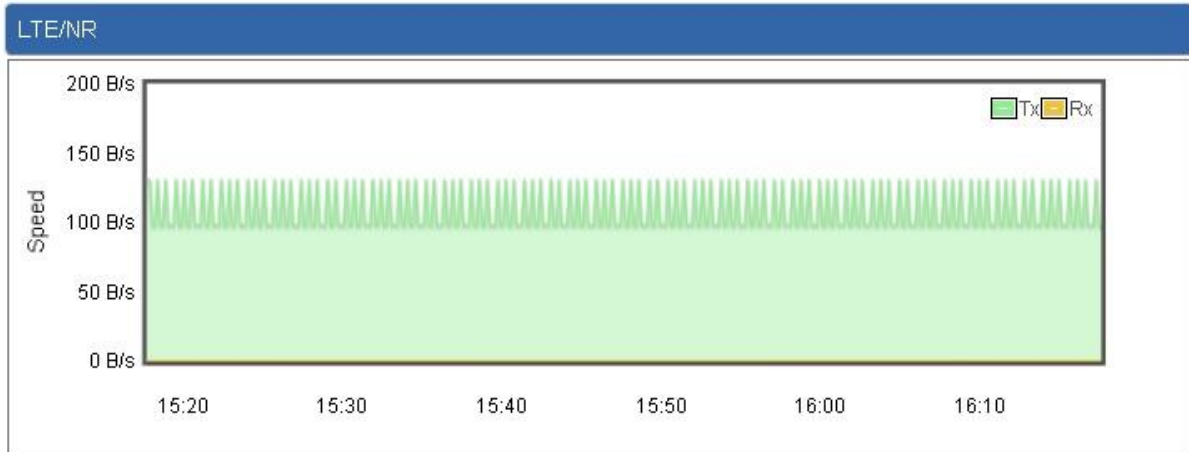


Figure 4-6-5: LTE/NR statistics

4.6.5 GPS

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



Figure 4-6-6: GPS

4.6.6 SMS

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

SMS Configuration

Name	
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

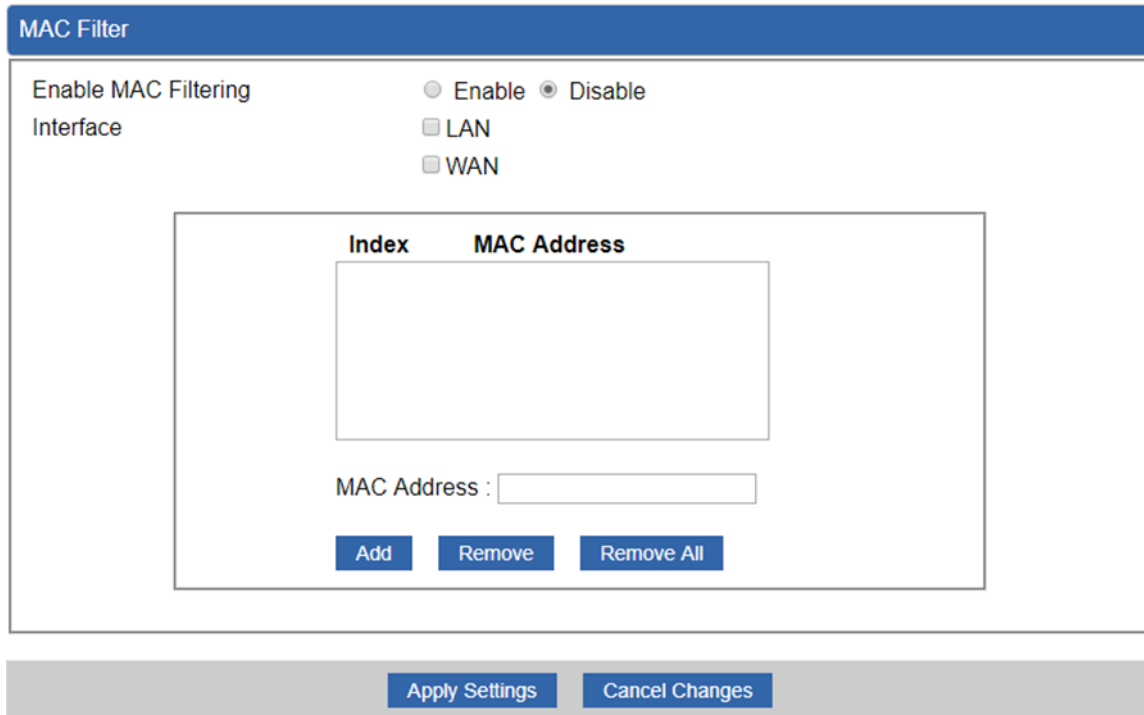
Cancel Changes

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.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block FIN Flood	If the function is enabled, when the number of the current FIN packets is beyond the set value, the cellular gateway will start the blocking function immediately. The default configuration is disabled.
Block UDP Flood	If the function is enabled, when the number of the current UDP-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.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the 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](#).



The figure shows a web-based configuration interface for MAC Filtering. At the top, there is a blue header bar labeled "MAC Filter". Below this, the interface is divided into two main sections. The first section, titled "Enable MAC Filtering", contains two radio buttons: "Enable" (unselected) and "Disable" (selected). Below this, there is a section titled "Interface" with two checkboxes: "LAN" (unselected) and "WAN" (unselected). The second section is a large white box containing a table with two columns: "Index" and "MAC Address". The table is currently empty. Below the table, there is a text input field labeled "MAC Address :". At the bottom of this section, there are three buttons: "Add", "Remove", and "Remove All". At the very bottom of the interface, there are two buttons: "Apply Settings" and "Cancel Changes".

Figure 4-7-3: MAC Filtering

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

4.7.3 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
 ☒ Disable

IP Filtering Rules

No.	Active	Source IP	Destination IP	Port Range	Protocol	Action
Add IP Filtering Rule						

Figure 4-7-4: IP Filtering

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

IP Filter Rule Setting

Enable ☒

Source IP Address /

Destination IP Address /

Destination Port -

Protocol

☐ Anywhere

☐ Anywhere

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

4.7.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in [Figure 4-7-6](#). Block those URLs which contain keywords listed below.

Web Filtering

Web Filtering

☐ Enable
 ☒ Disable

Web Filtering Rules

No.	Rule Enable	Filter Keyword	Filter Type	Action
Add Web Filtering Rule				

Figure 4-7-6: Web Filtering

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

Web Filter Settings

Status

Enable ▾

Filter Keyword

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.

4.7.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in [Figure 4-7-8](#). These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your 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

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 Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols.
External Service Port	Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in

Object	Description
	both the start and finish fields.
Virtual Server IP Address	Enter the local IP address.
Internal Service Port	Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

4.7.6 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 ☐ Enable ☒ Disable
DMZ IP Address

DMZ - WAN2

DMZ ☐ Enable ☒ Disable
DMZ IP Address

Apply Settings

Cancel Changes

Figure 4-7-9: DMZ

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

4.8 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](#)

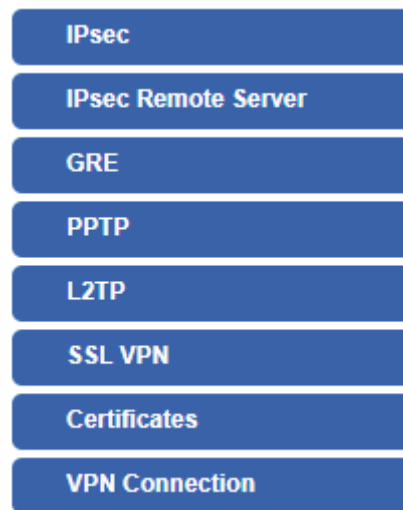


Figure 4-8-1: VPN Menu

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

4.8.1 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](#).

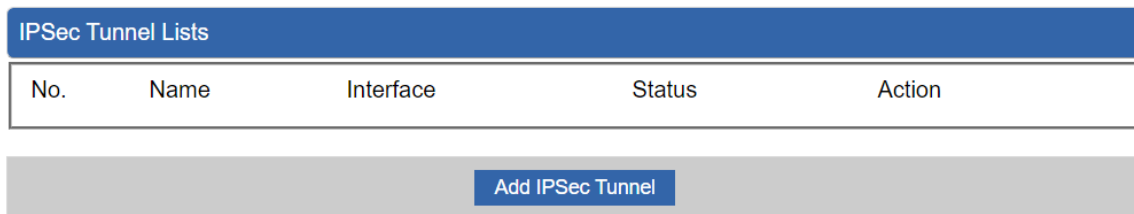


Figure 4-8-2: IPSec

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

Remote IP Address

Remote Network

Remote Netmask

Detection

Dead Peer Detection ☒

Time Interval Seconds Timeout Seconds Action

Authentication

Preshare Key

IKE Setting

Phase 1

IKE ☒ v1 ☐ v2

Connection Type ☒ Main ☐ Aggressive

ISAKMP DH Group

IKE SA Lifetime hours

Phase 2

ESP

ESP Keylife hours

Perfect Forward Secrecy (PFS) ☐ Yes ☒ No

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.
Dead Peer Detection	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. When VPN detects opposite party reaction time, the function will take one of the actions: "Hold" stand for the system will retain IPsec SA, "Clear" stand for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPsec SA and reset VPN tunnel.
Preshare Key	Enter a pass phrase to be used to authenticate the other side of the tunnel. Should be the same as the remote host.
IKE	Select the IKE (Internet Key Exchange) version.
Connection Type	1. Main. 2. Aggressive.
ISAKMP	It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 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.
Perfect Forward Secrecy (PFS)	Set the function as enable or disable.

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 GRE Tunnel									

Figure 4-8-4: GRE

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

GRE Tunnel

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

☐ Enable ☒ Disable

Broadcast

☐ Enable ☒ Disable

Force MPPE Encryption

☒ Enable ☐ Disable

CHAP

☒ Enable ☐ Disable

MSCHAP

☒ Enable ☐ Disable

MSCHAP v2

☒ Enable ☐ Disable

DNS1

DNS2

WINS1

WINS2

Server IP Address

Clients IP Address Start

Clients IP Address End

	User	Password
1	test	test
2	user	1234
3	user	1234
4	user	1234
5	user	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 Encryption	Set the encryption as enable or disable.
CHAP	Set the authentication as enable or disable.
MSCHAP	Set the authentication as enable or disable.
MSCHAP v2	Set the authentication as enable or disable.

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

4.8.4 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

Clients IP Address Start

Clients IP Address End

With IPsec

☐ Enable ☒ Disable

Preshare Key

Users

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

IPsec

Phase 1

Connection Type

☒ Main ☐ Aggressive

ISAKMP

DH Group

IKE SA Lifetime

hours

Phase 2

ESP

ESP Keylife

hours

Apply Settings

Cancel Changes

Figure 4-8-7: L2TP Server

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

Object	Description
Preshare Key	Enter a pass phrase.
User and Password	Create the username and password for the VPN client.
Connection Type	1. Main. 2. Aggressive.
ISAKMP	It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign to which key size or Preshare Key and algorithm to use. The SA comes in many connection ways. 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.

4.8.5 SSL VPN

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

SSL Server

SSL VPN Server

Port

Tunnel Protocol

Virtual Network Device

Interface

VPN Network

Network Mask

Encryption Cipher

Hash Algorithm

Export client.ovpn

☐ Enable
 ☒ Disable

1194

UDP ▾

TUN ▾

LAN ▾

192.168.1.1

192.168.20.0

255.255.255.0

AES-128 CBC ▾

SHA1 ▾

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).

4.8.6 VPN Connection

This page shows the VPN connection status as shown in [Figure 4-8-9](#).

VPN Connection Status						
IPsec GRE PPTP L2TP SSL VPN						
Type	Connected Time	Local IP	Remote IP	Local Subnet	Remote Subnet	

Figure 4-8-9: VPN Connection Status

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

4.8.7 SD WAN

This page shows the SD WAN Configuration status as shown below.

SD WAN Configuration

SD WAN

☐ Enable ☒ Disable

SD WAN Lists

No.	Group Name	Local Subnet	Remote Subnet	Gateway	Action
-----	------------	--------------	---------------	---------	--------

SD WAN Configuration

Group Name

IPsec Tunnel

☐

☐

Weight

Gateway

WAN1 ()
WAN2 ()

Figure 4-8-10: SD WAN Configuration

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 shown in [Figure 4-9-2](#).

AP Preference

Region	FCC
RO Community	public
RW Community	private

Figure 4-9-2: AP Control Menu

Note: 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.

Follow the steps below :

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

Step 2. Choose which AP you want to add.

Step 3. Press the Apply button to finish addition.



AP Search

Num.	MAC Address	Device Type	Model No.	Version	Device	Device Description	
1	a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0-Build20200321122005	192.168.0.101		☐
2	a8:f7:e0:3c:5f:ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0-Build20200422115453	192.168.0.102		☐

Search Apply 10 (10..1024)

Note: When using AP Search, the AP's IP Address must be the same as WS-Series Switch IP domain.

4.9.3 AP Management

On this page, you can manage your APs, including checking AP online status, configuring AP (IP address, Mask, SSID and Radio profile), rebooting AP, firmware update, and deleting AP in the AP Control system.

Status

AP Management

☐ Online
 ☐ Offline
 ☐ Disable

AP Group	Status	MAC Address	Device Type	Model No.	Version	IP Address	Device Description	Action
		a8:f7:e0:46:2e:38	Wireless	WDAP-C7200E	WDAP-C7200E-AP-FCC-V3.0-Build20200321122005	192.168.0.101		
		a8:f7:e0:3c:5f:ab	Wireless	WNAP-C3220E	WNAP-C3220E-AP-FCC-V3.0-Build20200422115453	192.168.0.102		

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
	Setting: edit setting and allocate profile to AP
	Link: link to the AP's web page
	Firmware Update: Upgrade AP's firmware
	Reboot: Reboot the AP
	Delete: Delete the AP from the LED Control control list: Control the AP's LED.
	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. Press the Apply button to complete the setup of AP.

4.9.4 AP Group Management

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

AP Group Management

	Num.	Group Name	Group Description	Action				
☐	1	GroupTest1	test					
☐	2	GroupTest2	test					

Action:

Object	Description
	Add new group: Click it to add an AP group
	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			
AP Group Description			

<< Add Remove >>

	2.4G Profile	5G Profile
SSID 1	Disable	Disable
SSID 2	Disable	Disable
SSID 3	Disable	Disable
SSID 4	Disable	Disable
Radio 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 the group member setting area and press the Add button.
4. Select AP Group SSID profile and Radio Profile.
5. Press the Apply button to finish the creation of 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.

4.9.5 SSID Profile

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

Radio Profile 2.4GHz






	Num	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Action
☐	1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	 
☐	2	WNAP-C3220E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	 

Radio Profile 2.4GHz Configuration

Radio Profile Configuration	
Model No.	WAP-200N
Basic Setting	
Radio Profile Description	
Wireless Mode	11b/g/n mixed mode
Channel Bandwidth	20MHz
Channel	Auto
MCS	Auto
Tx Power	Auto
Client Limit	☒ 64 (1 to 64)

Action:

Object	Description
	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.
	Delete: Click it to delete the single profile.

4.9.6 Radio 2.4G Profile

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

Radio Profile 2.4GHz

	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Action
☐	1	WDAP-C7200E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	 
☐	2	WNAP-C3220E	test_2.4G	11b/g/n mixed mode	Auto	40MHz	100%	N/A	 

Action:

Object	Description
	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.
	Delete: Click it to delete the single profile.

Radio Profile 2.4GHz Configuration

Apply Back Reset

Radio Profile Configuration	
Model No.	WAP-200N
Basic Setting	
Radio Profile Description	
Wireless Mode	11b/g/n mixed mode
Channel Bandwidth	20MHz
Channel	Auto
MCS	Auto
Tx Power	Auto
Client Limit	☒ 64 (1 to 64)

Note:

1. Strongly suggest you 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.

4.9.7 Radio 5G Profile

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

Radio Profile 5GHz

	Num.	Model No.	Profile Name	Wireless Mode	Channel ID	Channel Bandwidth	Tx Power	Data Rate	Action
☐	1	WDAP-C7200E	test_5G	11n/ac mixed mode	Auto	40MHz	100%	N/A	 

Action:

Object	Description
	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.
	Delete: Click it to delete the single profile.

Radio Profile 5GHz Configuration

Apply Back Reset

Radio Profile Configuration	
Model No.	WAP-500N
Basic Setting	
Radio Profile Description	
Wireless Mode	11a/n mixed mode
Channel Bandwidth	40MHz
Channel	Auto
Client Limit	☒ 64 (1 to 64)

Note:

1. Strongly suggest you 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.

4.9.8 Statistics AP Status

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

Statistic > Managed APs Filter by Context 10 (10..64) 

● Online ● Offline ● Disable

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.

4.9.9 Statistics Active Clients

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

Statistic > Active Clients

Filter by MAC, IP, SSID, Band

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.

4.9.10 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 referring to its real transmission power and channel allocation.

The interface consists of a left sidebar and a main map area.

Top Screenshot:

- Left Sidebar:**

I	S	Device Description	A
1		WDAP-C7200E	☐
2		WNAP-C3220E	☐

AP Group

Band

Transparency

Scale

1 : 30.3030303030305m
- Main Map Area:**

Scale bar: 0, 50 m, 100 m, 150 m, 200 m, 250 m, 300 m

Buttons: Save, test

Dialog Box: "Please draw a straight line to estimate distance with a mouse." "What is the physical distance of the draw line?" [] m Set Cancel

Bottom Screenshot:

- Left Sidebar:**

I	S	Device Description	A
1		WDAP-C7200E	☒
2		WNAP-C3220E	☒

AP Group

Band

Transparency

Scale

1 : 39.21568627450981m
- Main Map Area:**

Scale bar: 0, 50 m, 100 m, 150 m, 200 m, 250 m, 300 m, 350 m

Buttons: Save, test

Map shows floor plan with AP coverage circles and a scale bar.

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 mapping managed APs to the actual position.

4.9.11 Upload Map

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

Upload Map



Map	New Map ▾
Upload File	選擇檔案 尚未選擇任何檔案
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 Wi-Fi	Allows to configure 2.4G Wi-Fi.
5G Wi-Fi	Allows to configure 5G Wi-Fi.
MAC ACL	Allows to configure MAC ACL.
Wi-Fi Advanced	Allows to configure advanced setting of Wi-Fi.
Wi-Fi Statistics	Displays the statistics of Wi-Fi traffic.
Connection Status	Displays the connection status.

4.10.1 2.4G Wi-Fi

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

2.4G WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status

☒ Enable ☐ Disable

Wireless Name (SSID)

Hide SSID

☐ Enable ☒ Disable

Bandwidth

20MHz

▼

Channel

6

▼

Encryption

Open

▼

WiFi Multimedia

☒ Enable ☐ Disable

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

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

4.10.2 5G Wi-Fi

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

5G WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status

☒ Enable ☐ Disable

Wireless Name (SSID)

Hide SSID

☐ Enable ☒ Disable

Bandwidth

▼

Channel

▼

Encryption

▼

WiFi Multimedia

☒ Enable ☐ Disable

Figure 4-10-3: 5G WFI

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

4.10.3 MAC ACL

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

MAC ACL

MAC ACL ☐ Enable ☒ Disable

MAC ACL Rules

Index	Active	Device Name	MAC Address	Action
		abc	00:30:4F:00:00:01	Add Scan

Figure 4-10-4: MAC ACL

Object	Description
Active	Allows the devices to pass the MAC ACL rule
Device Name	Set an allowed device name
MAC Address	Set an allowed device MAC address
Add	Press the “ Add ” button to add end-device that is scanned from wireless network and mark them
Scan	Connect to client list

4.10.4 Wi-Fi Advanced

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

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

Figure 4-10-5: Wi-Fi Advanced

Object	Description
2.4G Mode	11AC: Select 802.11B/G or 802.11N/G 11AX: Select 802.11B/G or 802.11N/G or 802.11AX
5G Mode	11AC: Select 802.11A or 802.11AN or 802.11AC 11AX: Select 802.11A or 802.11AN or 802.11AC or 802.11AX
2.4GHz Maximum Associated Clients	The maximum users are 64
5GHz Maximum Associated Clients	The maximum users are 64
2.4G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm
5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -90dBm
2.4G TX Power	The range of transmit power is Max (100%) , Efficient (75%) , Enhanced (50%) , Standard (25%) or Min (15%) . In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power
5G TX Power	The range of transmit power is Max (100%) , Efficient (75%) , Enhanced (50%) , Standard (25%) or Min (15%) . In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power

4.10.5 Wi-Fi Statistics

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

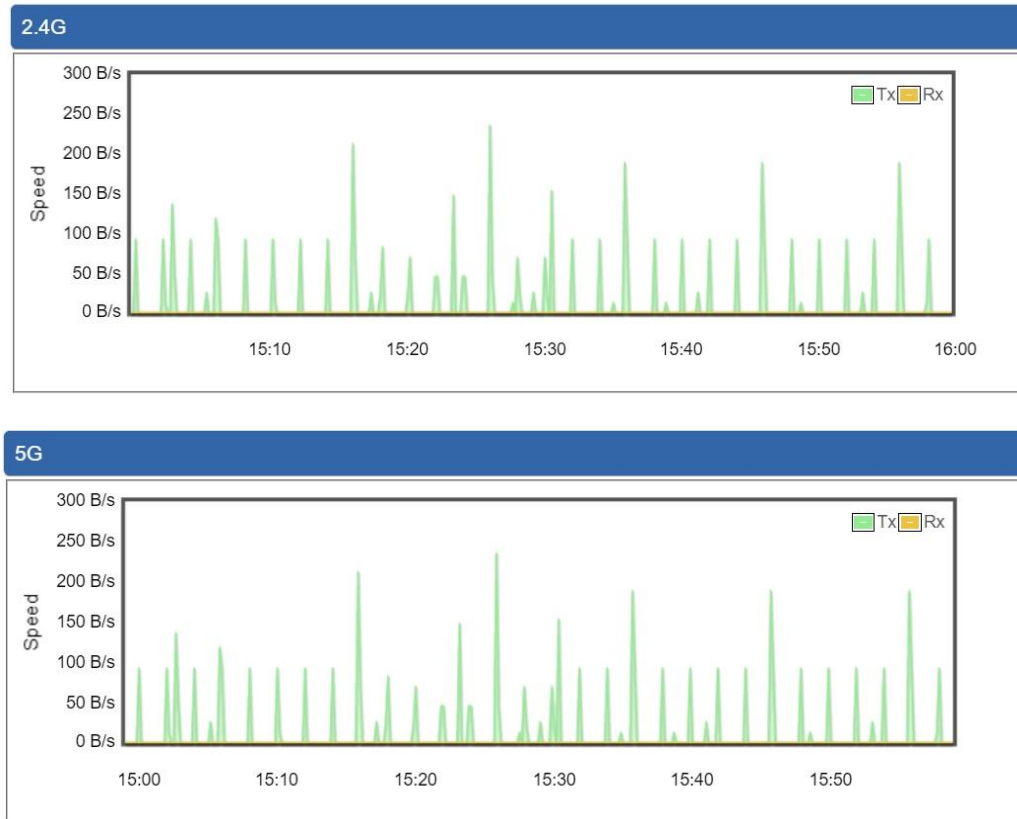


Figure 4-10-6: Wi-Fi Statistics

4.10.6 Connection Status

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

Client List				
No.	Name	MAC Address	Signal	Connected Time

Figure 4-10-7: Connection Status

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

4.11 Power over Ethernet

The PoE menu provides the following features for managing the system.

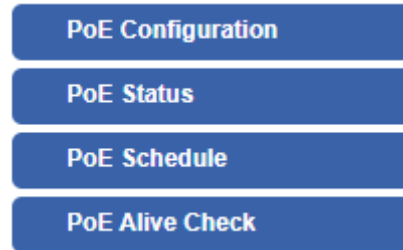


Figure 錯誤! 所指定的樣式的文字不存在文件中。 **1-1 PoE Menu**

Object	Description
PoE Configuration	Allows to centralize management of PoE power for PDs.
PoE Status	Displays the current PoE usage.
PoE Schedule	Allows centralizing management of PoE power for providing schedule.
PD Alive Check	Allows centralizing management of PoE power for checking PDs alive.

4.11.1 PoE Configuration

This section allows the user to inspect and configure the current PoE configuration setting.

PoE Configuration

System PoE Admin Mode Enable ▾

Power Supply 51 V

Power Limit Mode Consumption

Power Allocation

0 / 120 W

Port	Description	PoE Function	Schedule	Power Mode	Priority	Device Class	Current Used [mA]	Powered Used [W]
All		<All> ▾	<All> ▾	AT/AF	<All> ▾			
1		Enable ▾	None ▾	AT/AF	High ▾	--	0	0
2		Enable ▾	None ▾	AT/AF	High ▾	--	0	0
3		Enable ▾	None ▾	AT/AF	High ▾	--	0	0
4		Enable ▾	None ▾	AT/AF	High ▾	--	0	0
Total							0	0

Apply Settings
Cancel Changes

Figure 錯誤! 所指定的樣式的文字不存在文件中。 **1-2** PoE configuration

Object	Description
System PoE Admin Mode	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not to supply power.
PoE Function	There are three modes for PoE mode. ■ Enable: enable PoE function. ■ Disable: disable PoE function. ■ Schedule: enable PoE function in schedule mode.
Schedule	Indicates the scheduled profile mode. Possible profiles are: ■ Profile1 ■ Profile2 ■ Profile3 ■ Profile4
Priority	The Priority represents PoE ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in case the total power consumption is over the total power budget. In this case, the port with the lowest priority will be turned off, and power for the port of higher priority will be offered.
Device Class	Displays the class of the PD attached to the port, as established by the classification process. Class 0 is the default for PDs. The PD is

	powered based on PoE Class level if the system is working in Classification mode. The PD will return to Class 0 to 4 in accordance with the maximum power
Current Used [mA]	The Power Used shows how much current the PD currently is using.
Powered Used [W]	The Power Used shows how much power the PD currently is using.

4.11.2 PoE Status

This section provides per port PoE status.

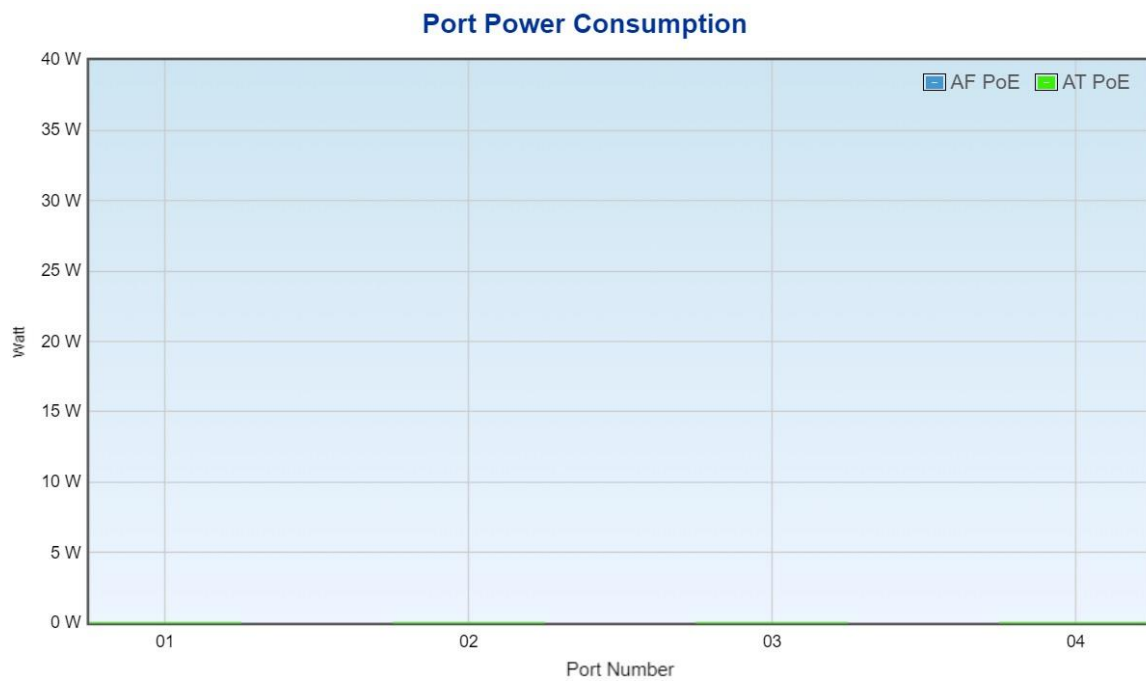


Figure 錯誤! 所指定的樣式的文字不存在文件中。 **1-3** Port Power Consumption

4.11.3 PoE Schedule

This page allows the user to define PoE schedule and scheduled power recycling.

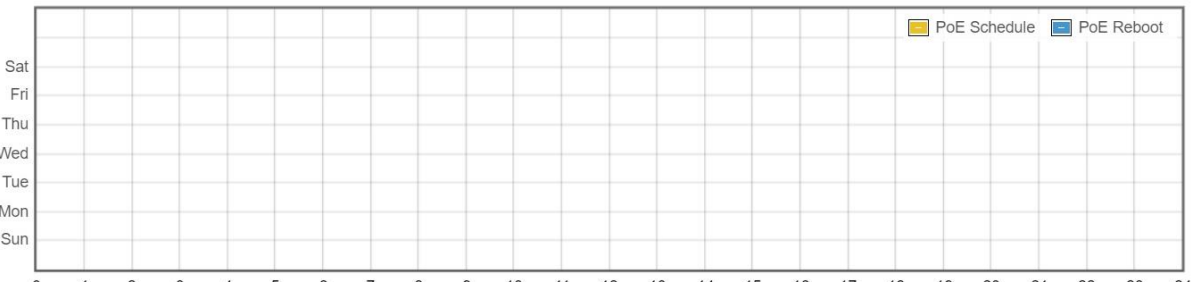
Please press the **Add New Rule** button to start setting PoE Schedule function. You have to set PoE schedule to profile and then go back to PoE Port Configuration, and select “**Schedule**” mode from per port “**PoE Mode**” option to enable you to indicate which schedule profile could be applied to the PoE port.

PoE Schedule

Profile Profile 1 ▾

Week Day	Start Hour	Start Min	End Hour	End Min	Reboot Enable	Reboot Only	Reboot Hour	Reboot Min	Delete
Sun ▾	00 ▾	00 ▾	23 ▾	59 ▾	☐	☐	00 ▾	00 ▾	Add

Apply Settings
Cancel Changes



The grid shows a 7-day week (Sun to Sat) on the y-axis and 24 hours on the x-axis. A legend indicates yellow squares for 'PoE Schedule' and blue squares for 'PoE Reboot'. The grid is currently empty.

Figure 錯誤! 所指定的樣式的文字不存在文件中。 **1-4** PoE schedule Configuration

Object	Description
Profile	Set the schedule profile mode. Possible profiles are: Profile1 Profile2 Profile3 Profile4
Week Day	Allows user to set week day for defining PoE function by enabling it on the day.
Start Hour	Allows user to set what hour PoE function does by enabling it.
Start Min	Allows user to set what minute PoE function does by enabling it.
End Hour	Allows user to set what hour PoE function does by disabling it.
End Min	Allows user to set what minute PoE function does by disabling it.

Reboot Enable	Allows user to enable or disable the whole PoE port reboot by PoE reboot schedule. Please note that if you want PoE schedule and PoE reboot schedule to work at the same time, please use this function, and don't use Reboot Only function. This function offers administrator to reboot PoE device at an indicated time if administrator has this kind of requirement.
Reboot Only	Allows user to reboot PoE function by PoE reboot schedule. Please note that if administrator enables this function, PoE schedule will not set time to profile. This function is just for PoE port to reset at an indicated time.
Reboot Hour	Allows user to set what hour PoE reboots. This function is only for PoE reboot schedule.
Reboot Min	Allows user to set what minute PoE reboots. This function is only for PoE reboot schedule.

4.11.4 PD Alive Check

The VPN Router can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and without response, the PoE Switch is going to restart PoE port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.

PoE Alive Configuration						
Port	Mode	Remote PD IP Address	Interval Time(10~300s)	Retry Count(1~5)	Action	Reboot Time (30~180s)
All	<All> ▾			<All> ▾	<All> ▾	
1	Disable ▾	192.168.1.10	10	1 ▾	None ▾	30
2	Disable ▾	192.168.1.11	10	1 ▾	None ▾	30
3	Disable ▾	192.168.1.12	10	1 ▾	None ▾	30
4	Disable ▾	192.168.1.13	10	1 ▾	None ▾	30

Figure 錯誤! 所指定的樣式的文字不存在文件中。 **1-5 PoE Alive Configuration**

Object	Description
Mode	Allows user to enable or disable per port PD Alive Check function. By default, all ports are disabled.
Remote PD IP Address	This column allows user to set PoE device IP address for system making ping to the PoE device. Please note that the PD's IP address must be set to the same network segment with the PoE Switch.
Interval Time (10~300s)	This column allows user to set how long system should issue a ping request to PD for detecting whether PD is alive or dead. Interval time range is from 10 seconds to 300 seconds.
Retry Count (1~5)	This column allows user to set the number of times system retries ping to PD. For example, if we set count 2, it means that if system retries ping to the PD and the PD doesn't response continuously, the PoE port will be reset.
Action	Allows user to set which action will be applied if the PD is without any response. The PoE Switch Series offers the following 3 actions: ■ PD Reboot: It means system will reset the PoE port that is connected to the PD. ■ PD Reboot & Alarm: It means system will reset the PoE port and issue an alarm message via Syslog. ■ Alarm: It means system will issue an alarm message via Syslog.
Reboot Time (30~180s)	This column allows user to set the PoE device rebooting time as there

	are so many kinds of PoE devices on the market and they have a different rebooting time.
--	---

The PD Alive-check is not a defining standard, so the PoE device on the market doesn't report reboot done information to the PoE Switch. Thus, user has to make sure how long the PD will take to finish booting, and then set the time value to this column.

System is going to check the PD again according to the reboot time. If you are not sure of the precise booting time, we suggest you set it longer.

4.12 Maintenance

The Maintenance menu provides the following features for managing the system as shown in [Figure 4-12-1](#)



Figure 4-12-1: 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.

4.12.1 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 4-12-2](#).

Account Password

Username	admin
Password	
Confirm Password	

Apply Settings

Cancel Changes

Figure 4-12-2: Account and Password Page

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

4.12.2 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 4-12-3.

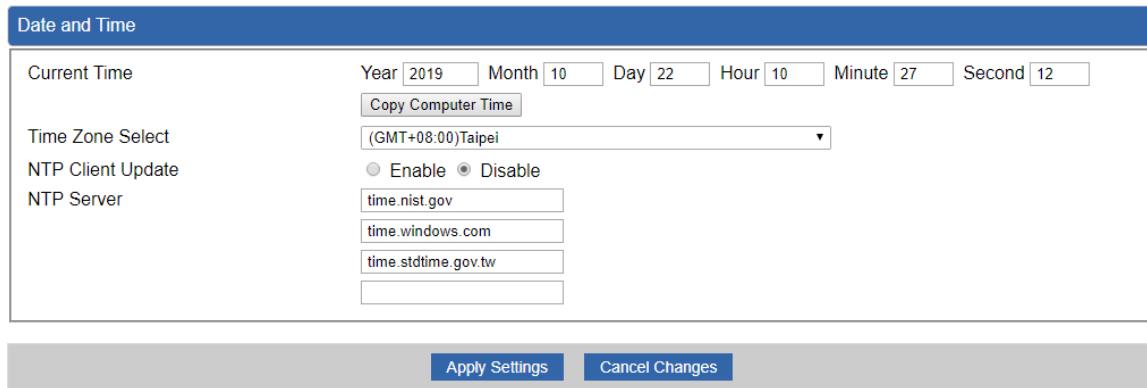


Figure 4-12-3: Date and Time Page

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.

4.12.3 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 4-12-4](#) is shown below:

Save/Restore Configuration

Configuration Export

Configuration Import

No file chosen

USB Backup/Upload Configuration

USB HDD:

Backup Settings to USB HDD:

Load Settings from USB HDD:

Not Detected

Configuration disabled

Please format the HDD as FAT32 on a Windows PC before using it for backup

Figure 4-12-4: 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 USB Storage	Press the Save button to save setting file to USB storage.
Load Settings from 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 the “Unmount” button first.

4.12.4 Upgrading Firmware

This page provides the firmware upgrade function as shown in [Figure 4-12-5](#)

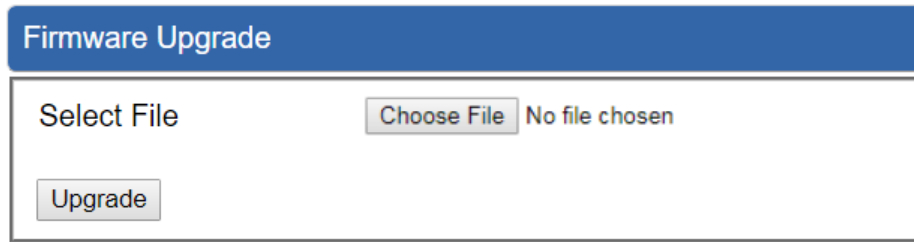


Figure 4-12-5: Firmware Upgrade Page

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

4.12.5 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 4-12-6](#) is shown below:

Reboot / Reset

Reboot Button

Reset Button

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

Reboot

Reset to Default

Figure 4-12-6: 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.

4.12.6 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 4-12-7](#)

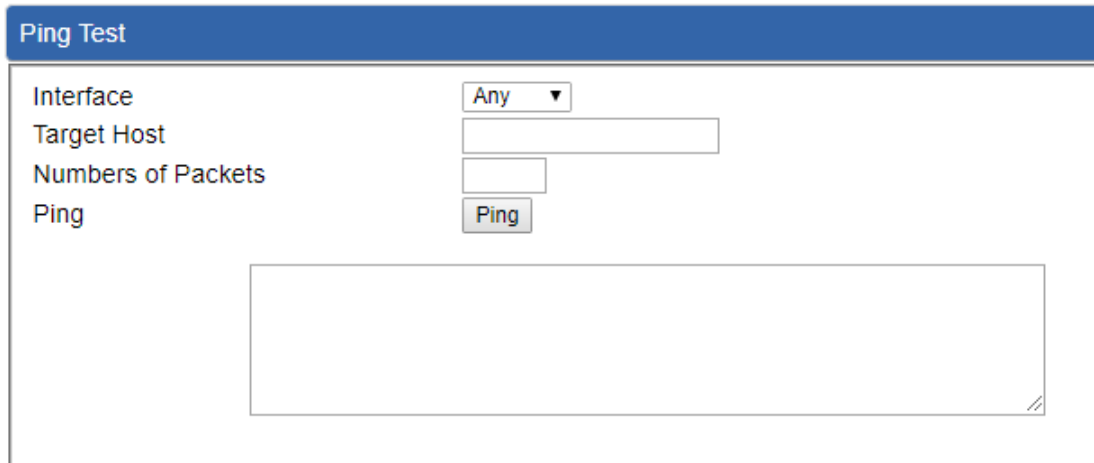


Figure 4-12-7: Diagnostics Page

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.

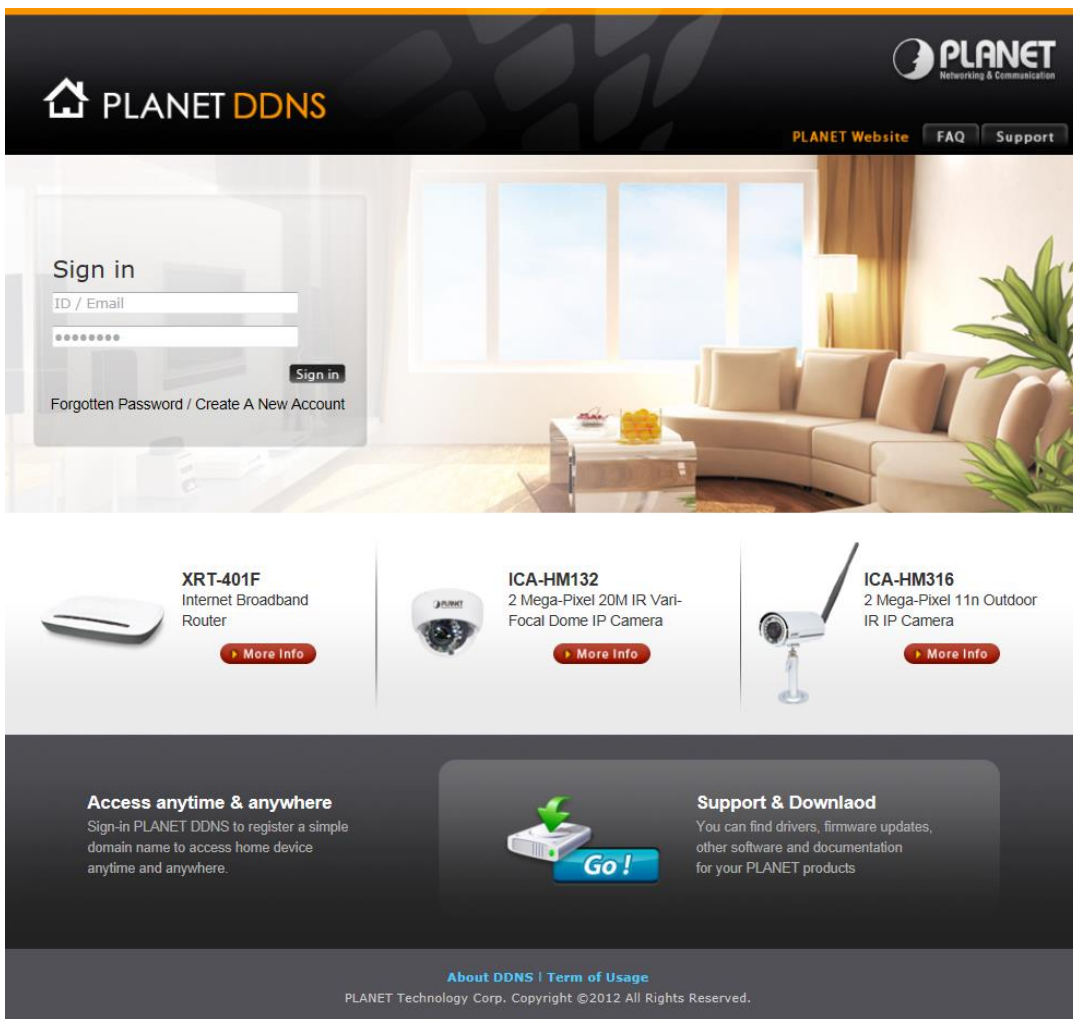
Appendix A: DDNS Application

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 <http://planetddns.com>

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

Step 3: Input all DDNS settings.



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