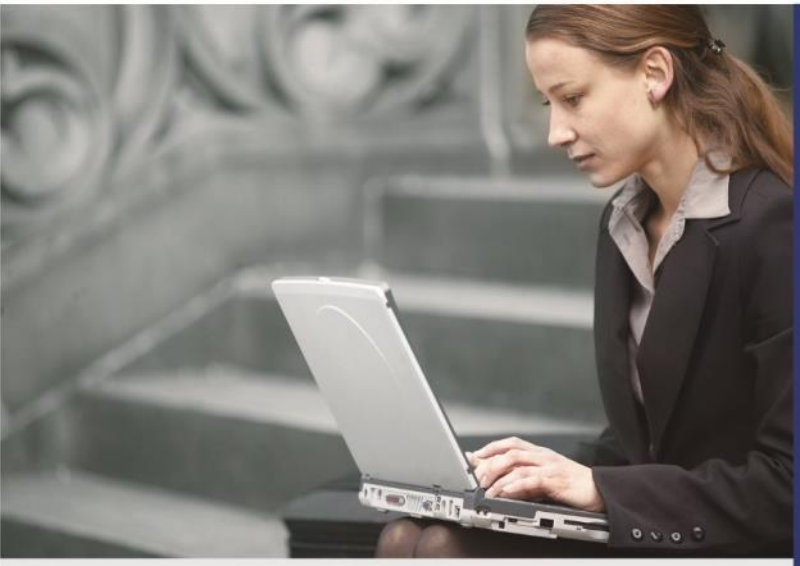
PLANET
Networking & Communication

User's Manual

Wi-Fi 7 Dual Band 802.11be 3600Mbps

Outdoor Wireless Access Point

WDAP-3600BE



Copyright

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

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

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

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

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and 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:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CE Compliance Statement

This device meets the RED 2014/53/EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The device complies with RF specifications when it is used at a safe distance of 20 cm from your body.

Safety

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

WEEE regulation

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

Revision

User Manual of PLANET Wi-Fi 7 802.11be 3600 Mbps Outdoor Wireless Access Point

Model: WDAP- 3600BE

Rev: 1.0 (Nov, 2025)

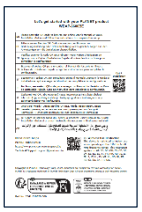
Part No. EM-WDAP-3600BE

Table of Contents

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET 802.11be 3600Mbps Wireless AP. Please verify the contents inside the package box.

WDAP-3600BE	Antenna x 2	Cable Tie x 2
CloudNMS App Sheet x 1	**QR Code Sheet x 1**	**Ethernet Cable x 1**
		

Note

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

IMPORTANT SAFETY PRECAUTIONS:

1) **LIVES MAY BE AT RISK!** Please be aware of the electrical wires around. Carefully read the section "**OUTDOOR INSTALLATION WARNING**" in the manual before installation.
2) Users **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.**
3) Users **MUST** power off the device first before connecting the antenna to it; otherwise, damage might be caused to the device itself.
4) 4) Power off the device before connecting any antennas to prevent damage

1.2 Product Description

Outdoor-grade Wi-Fi 7 AP for High-speed and Reliable Wireless Coverage

PLANET WDAP-3600BE is a rugged outdoor wireless access point that delivers **next-generation Wi-Fi 7 (802.11be)** performance with an aggregated throughput of up to **3600Mbps (2.4GHz: 688Mbps + 5GHz: 2882Mbps)**. Designed for harsh environments, it ensures **ultra-fast, low-latency, and stable connectivity** for outdoor campuses, industrial parks, resorts, and smart city deployments.

Ruggedized Outdoor Design

Built with a weatherproof housing, the WDAP-3600BE withstands **-30°C to 70°C operating temperatures** and harsh outdoor conditions. Combined with **dual high-gain external antennas**, it provides **extended coverage** and reliable performance in wide-area wireless deployments.

High-density Wi-Fi 7 Performance

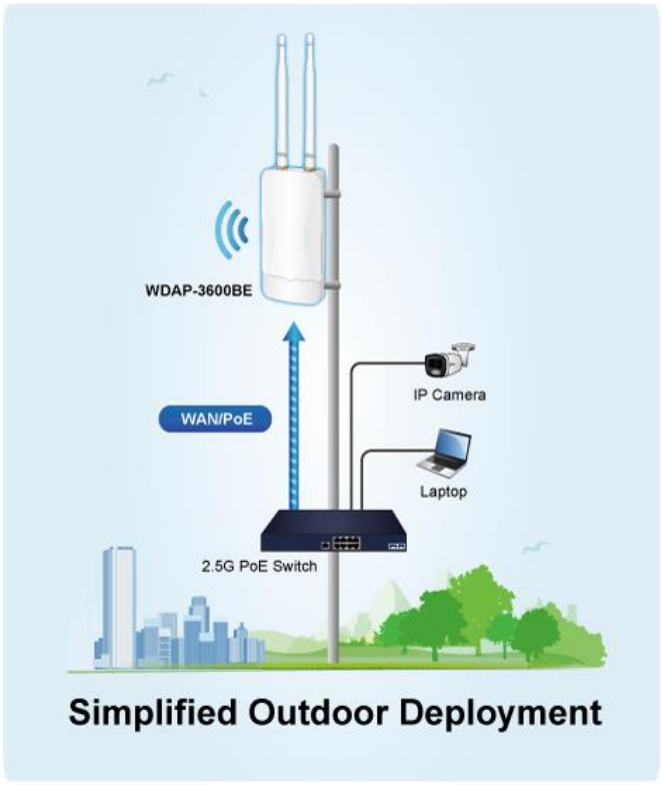
Equipped with advanced Wi-Fi 7 features such as **4096-QAM, MU-MIMO, OFDMA, BSS Coloring, and Beamforming**, the WDAP-3600BE supports multiple simultaneous users with consistent connectivity—ideal for outdoor public Wi-Fi, transportation hubs, and enterprise campuses.

Robust Security and Business-ready Features

To safeguard sensitive business and personal data, the WDAP-3600BE supports the latest **WPA3 encryption**, VLAN-to-SSID mapping, and client isolation. Combined with its flexible SSID configuration and advanced access control, it ensures a **secure and well-segmented wireless environment** for both commercial and hospitality applications.

Flexible Power and Deployment

The WDAP-3600BE supports **IEEE 802.3at PoE+** and **12V DC power**, providing flexible installation options. Its **1 × 2.5GBASE-T PoE WAN port** and **1 × Gigabit LAN port** enable high-speed wired backhaul while reducing cabling complexity.



Multiple Operation Modes for Various Applications

The WDAP-3600BE supports the simplified usage modes of **Access Point**, **Gateway**, **Repeater** and **WISP** mode, through which they provide more flexibility for users when wireless network is established. Compared with general wireless access points, the WDAP-3600BE offers more powerful and flexible capability for wireless clients.

PLANET CloudNMS – Cloud-Based Universal Network Management

PLANET's **CloudNMS** platform and mobile app empower IT staff to remotely manage all network devices and Powered Devices (PDs) in real time. Designed for enterprises and industries, CloudNMS minimizes the need for on-site troubleshooting by providing centralized monitoring, fault detection, and instant alerts.

With **CloudNMS**, businesses can manage diverse network deployments more **efficiently, securely, and intelligently**—all from a single cloud-based platform.

1.3 Product Features

Standard-compliant Outdoor Wireless LAN

- Compliant with IEEE 802.11a/b/g/n/ac/ax/be (Wi-Fi 7) dual-band wireless technology
- Dual-band concurrent operation with a maximum wireless throughput of 3600Mbps (2.4GHz: 688Mbps, 5GHz: 2882Mbps)
- Built-in support for advanced Wi-Fi 7 features: 4096-QAM, OFDMA, MU-MIMO, Beamforming, BSS Coloring, Seamless Roaming (802.11k/v/r)

Rugged Outdoor Hardware Design

- 1 × 100/1000/2500BASE-T PoE+ WAN port (802.3at PoE+ PD)
- 1 × 10/100/1000BASE-T LAN port
- Dual-band high-gain external antennas for extended outdoor coverage
- IP-rated weatherproof housing with wide temperature support (**-30°C ~ 70°C**)

Multiple Operation Modes and Wireless Features

- Flexible operation modes: Gateway, AP, Repeater, WISP
- Supports up to 8 SSIDs (4 per band) with VLAN-to-SSID mapping
- Wi-Fi Multimedia (WMM) for optimized audio/video streaming
- Real-time Wi-Fi channel analysis chart for interference management
- Seamless roaming with 802.11k/v/r to ensure uninterrupted client mobility

Secure Network Connection

- Comprehensive wireless security with WPA3 Personal, WPA2/WPA3 Personal, WPA2 Enterprise, WPA/WPA2 Enterprise
- VLAN support with SSID-to-VLAN mapping, plus IP/MAC filtering and client isolation
- Enhanced security with ACL management to prevent unauthorized access

Easy Deployment and Centralized Management

- Powered by 802.3af/at PoE+, simplifying installation by combining power and data through a single Ethernet cable
- Fully compatible with PLANET CloudNMS app, and AP Controllers, enabling centralized monitoring and management
- Self-healing mechanism through system auto-reboot scheduling
- User-friendly Web GUI and setup wizard for quick configuration and monitoring

Product Specifications

Product	**WDAP-3600BE** Wi-Fi 7 Dual Band 802.11be 3600Mbps Outdoor Wireless Access Point
Hardware Specifications	
Interfaces	WAN/PoE: 1 x 100/1000/2500BASE-T RJ45 port LAN: 1 x 10/100/1000BASE-T RJ45 port Auto-negotiation and auto MDI/MDI-X
Antennas	2 × External dual-band RP-SMA type antennas (2.4GHz / 5GHz: 5dBi)
Reset Button	Reset button on the rear side (Press 6-10 seconds to reset the device to factory default.)
LED Indicators	5 × Green LEDs for Power, LAN, WAN, and Wi-Fi (2.4GHz / 5GHz) status
Dimensions (W × D × H)	86 × 30 × 186 mm (without antennas)
Weight	550g
Material	ABS+PC
Power Requirements	IEEE 802.3af/at PoE (End-span only, Mid-span not supported), DC 12V/2A
Power Consumption	Max. 5.5 watts / 18.76 BTU (Power on without any connection) Max. 9.5 watts / 32.4 BTU (Full loading)
Mounting	Mast mounting
IP Level	IP65
Surge Protection	±2KV (Common Mode), ±1KV (Differential Mode)
Wireless Interface Specifications	
Standard	5GHz: IEEE 802.11be IEEE 802.11ax IEEE 802.11ac IEEE 802.11n IEEE 802.11a 2.4GHz: IEEE 802.11be IEEE 802.11ax IEEE 802.11n IEEE 802.11b IEEE 802.11g IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3bz 2500BASE-T IEEE 802.3x flow control

<table>
<tr><td></td><td>IEEE 802.11k, 802.11v, and 802.11r*
IEEE 802.11i</td></tr>
<tr><td>Media Access Control</td><td>CSMA/CA</td></tr>
<tr><td>Data Modulation</td><td>802.11be: MIMO-OFDM/OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM / 1024QAM / 4096QAM)
802.11ax: MIMO-OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM, 1024QAM)
802.11ac: MIMO-OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM)
802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM)
802.11b: DSSS (DBPSK / DQPSK / CCK)</td></tr>
<tr><td>Band Mode</td><td>2.4GHz / 5GHz concurrent mode</td></tr>
<tr><td>Frequency Range</td><td>2.4GHz:
FCC: 2.412~2.462GHz
ETSI: 2.412~2.472GHz
5GHz:
FCC: 5.180~5.240GHz, 5.745~5.825GHz
ETSI: 5.180~5.700GHz</td></tr>
<tr><td rowspan="3">Operating Channels</td><td>ETSI:
2.4GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 (13 Channels)
5GHz: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120,124,128,132, 136, 140 (19 channels)</td></tr>
<tr><td>FCC:
2.4GHz: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (11 channels)
5GHz: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116,120,124,128,132, 136, 140, 149, 153, 157, 161,165 (24 channels)</td></tr>
<tr><td>5GHz channel list may vary in different countries according to their regulations.</td></tr>
<tr><td rowspan="12">Max. Transmit Power (dBm)</td><td>FCC: up to 22 ± 2dBm
ETSI: < 19dBm (EIRP)</td></tr>
<tr><td><table>
<tr><th>Network Mode</th><th>Data Rate</th><th>Max. Transmit Power (dBm)</th></tr>
<tr><td colspan="3">2.4G Power</td></tr>
<tr><td rowspan="2">802.11b</td><td>11M</td><td>22 ± 2</td></tr>
<tr><td>1M</td><td>22 ± 2</td></tr>
<tr><td rowspan="2">802.11g</td><td>54M</td><td>20 ± 2</td></tr>
<tr><td>6M</td><td>22 ± 2</td></tr>
<tr><td rowspan="2">802.11n HT20</td><td>MCS7</td><td>18 ± 2</td></tr>
<tr><td>MCS0</td><td>20 ± 2</td></tr>
<tr><td rowspan="2">802.11n HT40</td><td>MCS7</td><td>18 ± 2</td></tr>
<tr><td>MCS0</td><td>20 ± 2</td></tr>
<tr><td rowspan="2">802.11ax HE20</td><td>MCS11</td><td>17 ± 2</td></tr>
<tr><td>MCS0</td><td>20 ± 2</td></tr>
<tr><td>802.11ax HE40</td><td>MCS11</td><td>17 ± 2</td></tr>
</table></td></tr>
</table>

		MCS0	21 ± 2
	802.11be EHT20	MCS13	16 ± 2
		MCS0	20 ± 2
	802.11be EHT40	MCS13	16 ± 2
		MCS0	20 ± 2
	5G Power		
	802.11a	54M	18 ± 2
		6M	20 ± 2
	802.11n HT20	MCS7	17 ± 2
		MCS0	19 ± 2
	802.11n HT40	MCS7	18 ± 2
		MCS0	19 ± 2
	802.11ac VHT20	MCS7	16 ± 2
		MCS0	19 ± 2
	802.11ac VHT40	MCS7	17 ± 2
		MCS0	19 ± 2
	802.11ac VHT80	MCS9	17 ± 2
		MCS0	19 ± 2
	802.11ax HE20	MCS11	16 ± 2
		MCS0	19 ± 2
	802.11ax HE40	MCS11	16 ± 2
		MCS0	19 ± 2
	802.11ax HE80	MCS11	15 ± 2
		MCS0	18 ± 2
	802.11ax HE160	MCS11	15 ± 2
		MCS0	19 ± 2
	802.11be EHT20	MCS13	15 ± 2
		MCS0	19 ± 2
	802.11be EHT40	MCS13	14 ± 2
		MCS0	19 ± 2
	802.11be EHT80	MCS13	14 ± 2
		MCS0	19 ± 2
	802.11be EHT160	MCS13	13 ± 2
		MCS0	18 ± 2
Receive Sensitivity	Network Mode	Data Rate	Receive Sensitivity (dBm)
	2.4GHz		
	802.11b	11Mbps	-90
		1Mbps	-98
	802.11g	54Mbps	-78
		6Mbps	-96
	802.11n HT20	MCS7	-76
		MCS0	-95
	802.11n HT40	MCS7	-73
		MCS0	-92
	802.11ax HE20	MCS11	-66
		MCS0	-96
	802.11ax HE40	MCS11	-63
		MCS0	-93

	802.11be EHT20	MCS13	-60
		MCS0	-86
	802.11be EHT40	MCS13	-60
		MCS0	-86
	5GHz		
	802.11a	54Mbps	-75
		6Mbps	-93
	802.11n HT20	MCS7	-74
		MCS0	-92
	802.11n HT40	MCS7	-71
		MCS0	-89
	802.11ac VHT20	MCS7	-69
		MCS0	-92
	802.11ac VHT40	MCS7	-64
		MCS0	-89
	802.11ac VHT80	MCS9	-61
		MCS0	-86
	802.11ax HE20	MCS11	-63
		MCS0	-93
	802.11ax HE40	MCS11	-60
		MCS0	-90
	802.11ax HE80	MCS11	-56
		MCS0	-87
	802.11ax HE160	MCS11	-54
		MCS0	-84
	802.11be EHT20	MCS13	-54
		MCS0	-86
	802.11be EHT40	MCS13	-52
		MCS0	-84
	802.11be EHT80	MCS13	-50
		MCS0	-82
	802.11be EHT160	MCS13	-48
		MCS0	-80
2.4G EVM	802.11b : ≤-10dB；802.11g : ≤-25dB；802.11n : ≤ -28dB；802.11ax : ≤ -35dB；802.11be : ≤-38dB		
5G EVM	802.11a : ≤-25dB；802.11n : ≤-28dB；802.11ac : ≤ -32dB；802.11ax : ≤ -35dB；802.11be : ≤-38dB		
Software Features			
LAN	Static IP / Dynamic IP		
WAN	Static IP Dynamic IP PPPoE / PPTP / L2TP		
Wireless Mode	Access Point Gateway Repeater WISP		

Channel Width	20MHz, 40MHz, 80MHz, 160MHz
Encryption Security	WPA3 Personal WPA2/WPA3 Personal WPA2 Personal (AES) WPA2 Personal (TKIP) WPA2 Personal (TKIP+AES) WPA/WPA2 Personal (AES) WPA/WPA2 Personal (TKIP) WPA/WPA2 Personal (TKIP+AES) WPA2 Enterprise (802.1X) WPA/WPA2 Enterprise (802.1X)
Supported EAP Methods	EAP - Transport Layer Security (TLS) EAP-Tunneled TLS (TTLS) + Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) Protected EAP (PEAP) v0 + EAP-MSCHAPv2 PEAP v1 + EAP-Generic Token Card (GTC)
Wireless Security	Enable/Disable SSID broadcast Wireless max. 32 MAC address filtering User isolation
Max. SSIDs	8 (4 per radio)
Max. Clients	256 (128 is suggested, depending on usage)
Wireless QoS	Supports Wi-Fi Multimedia (WMM)
Wireless Advanced	Auto Channel Selection 5-level Transmit Power Control Max (100%), Efficient (75%), Enhanced (50%), Standard (25%) or Min (15%) Client Limit Control, Coverage Threshold Wi-Fi channel analysis chart Seamless roaming Beamforming BSS coloring
Status Monitoring	Device status, wireless client List PLANET Smart Discovery DHCP client table System Log supports remote syslog server
VLAN	IEEE 802.1Q VLAN (VID: 1~4094) SSID-to-VLAN mapping to up to 4 SSIDs
Self-healing	Supports auto reboot settings per day/hour
Management	Remote management through PLANET DDNS/ Easy DDNS Configuration backup and restore Supports UPnP* Supports IGMP Proxy Supports PPTP/L2TP/IPSec VPN Pass-through Supports Captive Portal*, RADIUS Server/Client
Central Management	Applicable controllers: NMS APC, WS APC, VR/IVR APC, ICG APC, PLANET CloudNMS
Environment & Certification	

Temperature	Operating: -30~ 70 degrees C Storage: -40 ~ 70 degrees C
Humidity	Operating: 10 ~ 90% (non-condensing) Storage: 5 ~ 95% (non-condensing)
Regulatory	CE, RoHS
Remarks [*]: The feature will be supported through firmware/system upgrade.	

Chapter 2. Physical Descriptions

2.1 Product Outlook

- **Dimensions**

  86 x 30 x 186 mm (without antennas)

- **Weight**

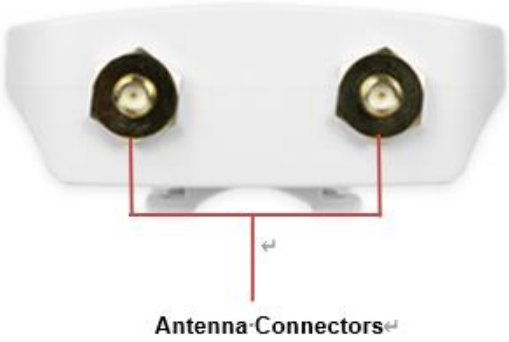
  550 g

Appearance

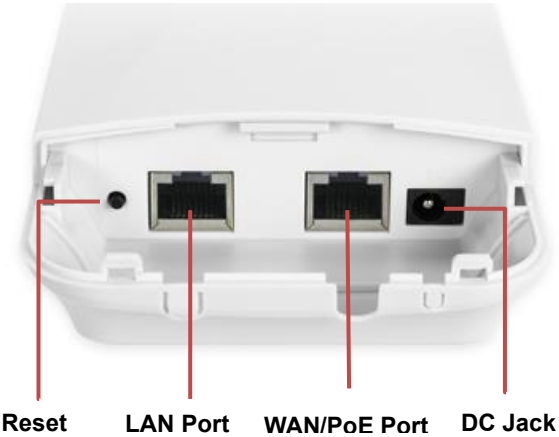
Front Side

Rear Side

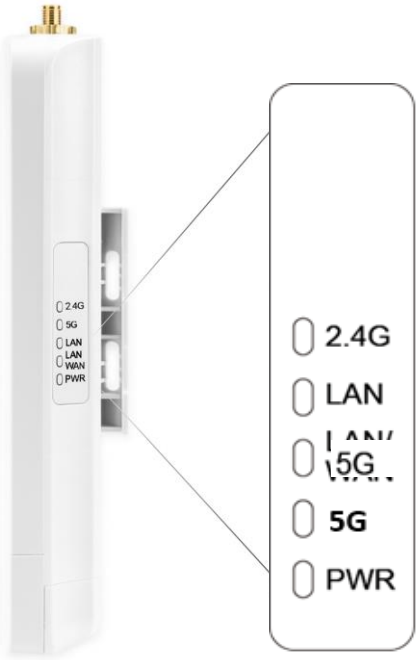
Top Side



Bottom Side



LED definition



LED	STATUS	FUNCTION
2.4G	On (**Green**)	2.4 GHz WLAN is on / traffic present.
	Off	2.4 GHz WLAN radios disabled.
LAN	On (**Green**)	Link established (10/100/1000 Mbps).
LAN/ WAN	On (**Green**)	Link established (100/1000/2500 Mbps).
5G	On (**Green**)	5 GHz WLAN is on / traffic present.
	Off	5 GHz WLAN radios disabled.
PWR	On (**Green**)	The device is powered on and booting.
	Off	Power off.

Hardware Interface Definition

Object	Description
Antenna Connectors	2 × RP-SMA
PoE LAN Port	1 × 2.5GBASE-T WAN PoE, auto MDI/MDI-X 802.3at PoE+ supported, 48~54VDC In
Reset Button	Press and hold the **Reset** button for 6~10 seconds to return to the factory default setting.
Grounding Terminal	The grounding wire must be attached to this port to prevent damage to the AP from direct lightning strike.

Chapter 3. Hardware Installation

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

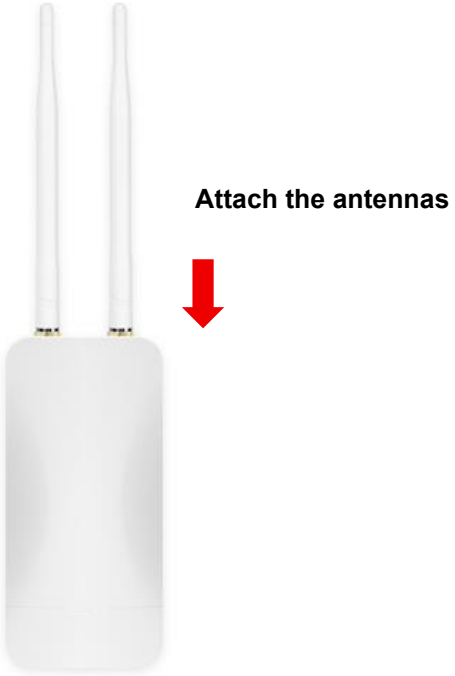
3.1 System Requirements

- Broadband Internet Access Service (Cable/xDSL/Ethernet connection)
- One IEEE 802.3at PoE switch (supply power to the WDAP-3600BE)
- PCs with a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- PCs running Windows 98/ME, NT4.0, 2000/XP, Windows Vista / Win 7 / 10 / 11, MAC OS 9 or later, Linux, UNIX or other platforms compatible with **TCP/IP** protocols

It is recommended to use Internet Explorer 11, Edge, Firefox or Chrome to access the AP.

3.2 Hardware Installation -- Installing the AP

Step 1. Attach the two RP-SMA antennas to the antenna connectors on top of the device.



Step 2. Mount the unit on a pole using the provided cable ties.

Step 3. Insert the RJ-45 Ethernet cable into the PoE WAN port through the waterproof gland and tighten it securely.

Step 4. Plug the other end into a PoE+ (IEEE 802.3at End-span) switch or PoE injector.

Step 5. (Optional) Connect a 12 V DC 2 A power adapter if PoE is not used.

Step 6. Power LED will light green when the device is on.

3.3 Manual Network Setup -- TCP/IP Configuration

The WDAP-3600BE IP address default is **DHCP Client** mode and fallback IP is **192.168.1.253**,and the fallback default subnet mask is 255.255.255.0. These values can be changed as you want. In this guide, we use all the default values for description.

Connect the WDAP-3600BE with your PC by plugging one end of an Ethernet cable in the LAN port of the AP and the other end in the LAN port of PC. The WDAP-3600BE is powered by a PoE switch.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in Windows 11. And the procedures in other operating systems are similar. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter manual if needed.

3.3.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx (If the default IP address of the WDAP-3600BE is 192.168.1.253, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 252.) and subnet mask is 255.255.255.0.

1 Select **Use the following IP address**, and then configure the IP address of the PC.

2 For example, the default IP address of the WDAP-3600BE is 192.168.1.253 and the DSL router is 192.168.1.254, or you may choose from 192.168.1.1 to 192.168.1.252.

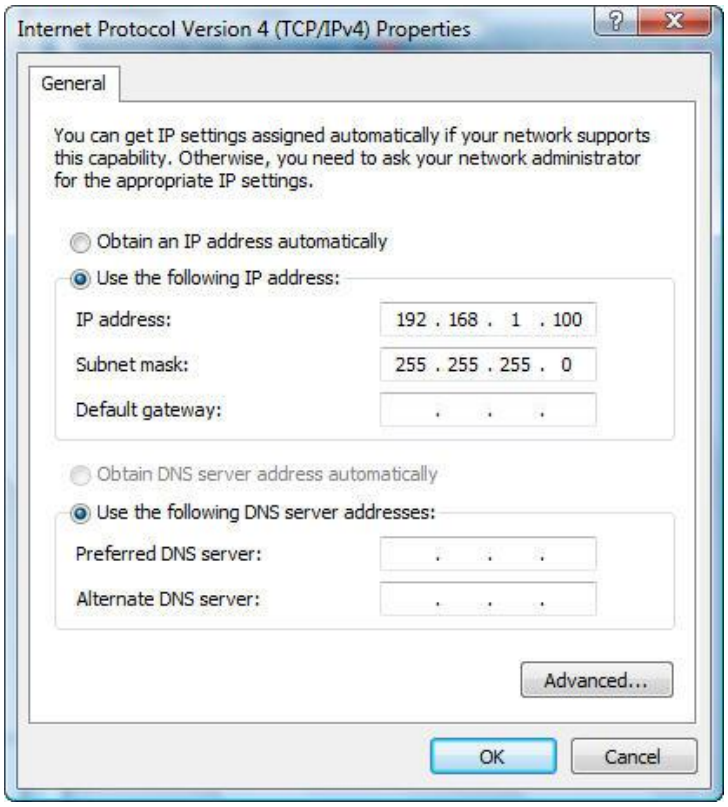


Figure 3-6 TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 11** OS. Please follow the steps below:

1. Click on **Start > Run**.
2. Type "**cmd**" in the Search box.

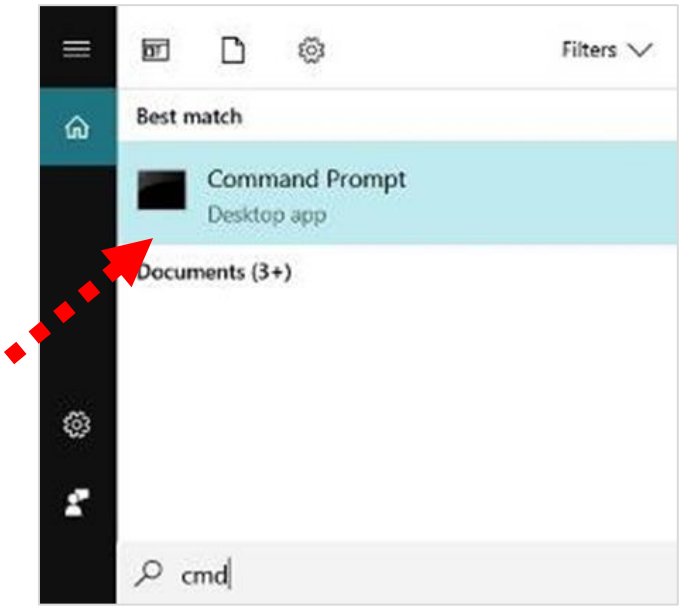


Figure 3-7 Windows Start Menu

3. Open a command prompt, type ping **192.168.1.253** and then press **Enter**.

   - If the result displayed is similar to **Figure 3-7**, it means the connection between your PC and the AP has been established well.

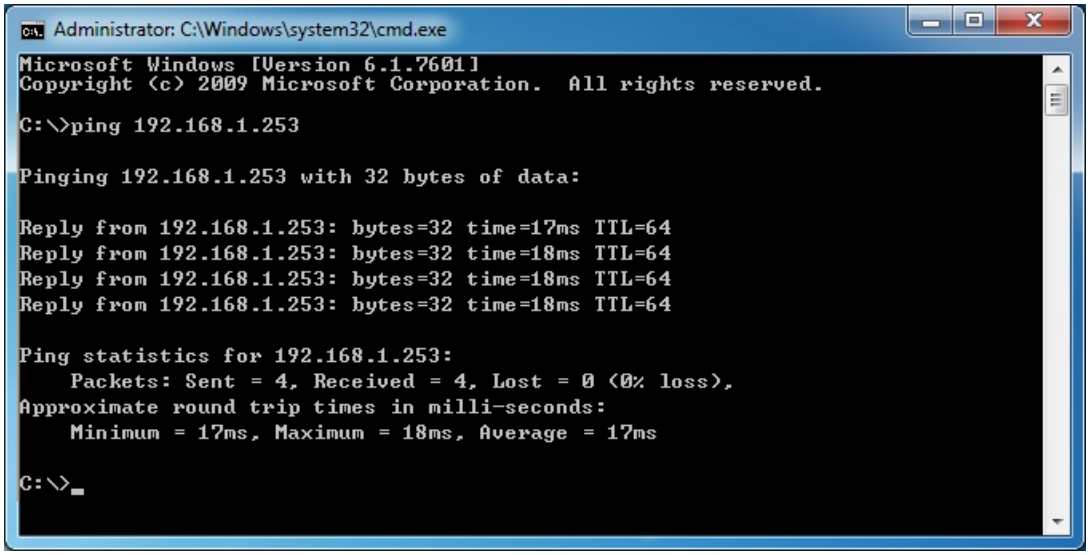


Figure 3-7 Successful Result of Ping Command

- If the result displayed is similar to **3-8**, it means the connection between your PC and the AP has failed.

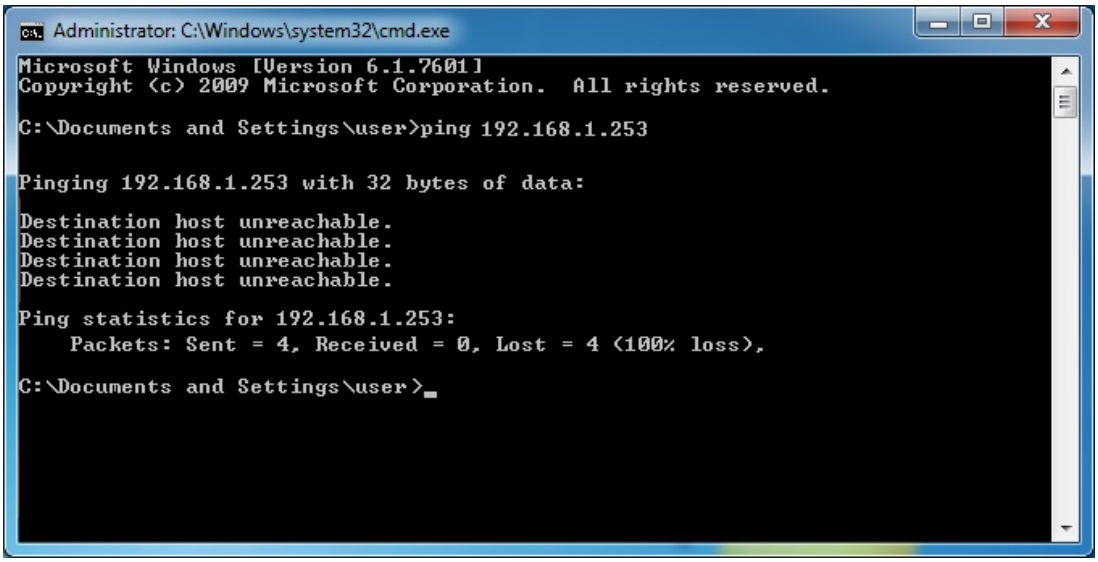


Figure 3-8 Failed Result of Ping Command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

3.4 Starting Setup in the Web UI

It is easy to configure and manage the AP with the web browser.

Step 1. To access the configuration utility, open a web-browser and enter the default IP address https://192.168.1.253 in the web address field of the browser.

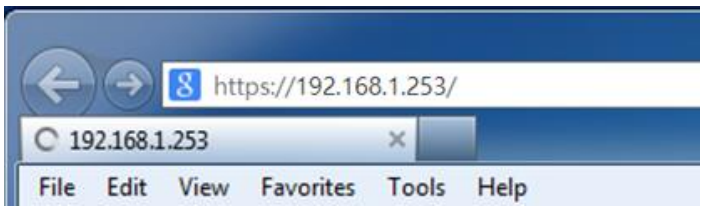


Figure 3-9 Login by Default IP Address

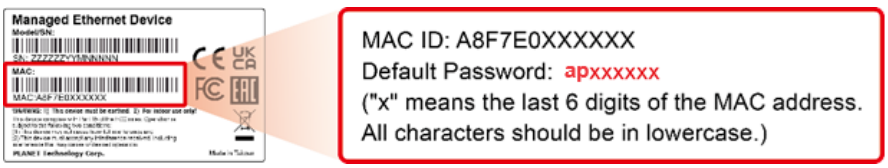
Step 2. When the login window pops up, please enter username and password. Please enter the default user name "**admin**" and password. Refer to Step 3 to determine your initial login password.

Figure 3-10 Login Window

Step 3. Default Username: admin

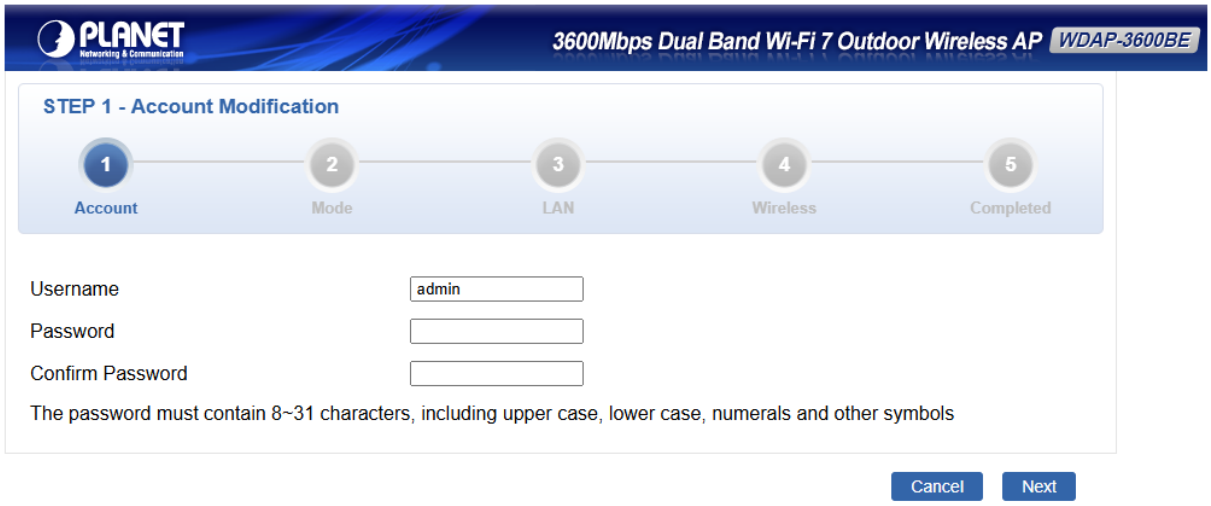
Default Password: ap + the last 6 characters of the MAC ID in lowercase

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



Step 4. After logging in, you will be prompted to change the initial username and password to a permanent one.

The Password must contain 8 to 31 characters, including uppercase, lowercase, numerals and other symbols. Please note spaces (blanks) are not accepted.



Note

If the above screen does not pop up, it may mean that your web browser has been set to a proxy. Go to Tools menu> Internet Options> Connections> LAN Settings on the screen that appears, uncheck **Using Proxy** and click **OK** to finish it.

3.5 Planet Smart Discovery Utility

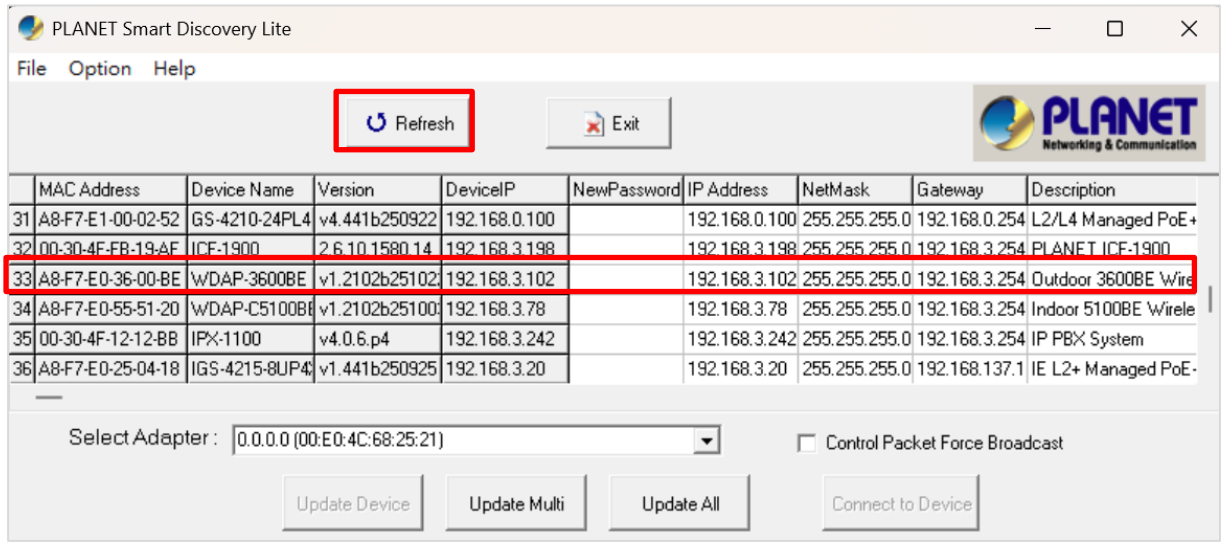
To easily list the WDAP-3600BE in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution.

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

Step 1: Download the **Planet Smart Discovery Utility** to administrator PC.

Step 2: Run this utility and the following screen appears.

Step 3: Press **"Refresh"** for the current connected devices in the discovery list as shown in the following screen:



Step 4: Press **"Connect to Device"** and then the Web login screen appears.

Note

The fields in the white background can be modified directly and then you can apply the new setting by clicking "**Update Device**".

Chapter 4. Web-based Management

This chapter delivers a detailed presentation of AP's functionalities and allows you to manage the AP with ease. **(The web GUI and topology below uses the WDAP-3600BE as an example.)**

Figure 4-1 Main Web Pag

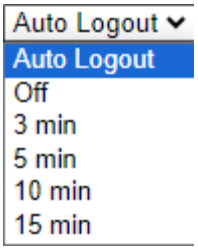
Main Menu

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 4-2 and 4-3.

Figure 4-2: Function Menu

Object	Description
System	Provides system information of the router.
Network	Provides WAN, LAN and network configuration of the router.
Security	Provides firewall and security configuration of the router.
Wireless	Provides wireless configuration of the router.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the router.

Figure 4-3: Function Button

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

4.1 System

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

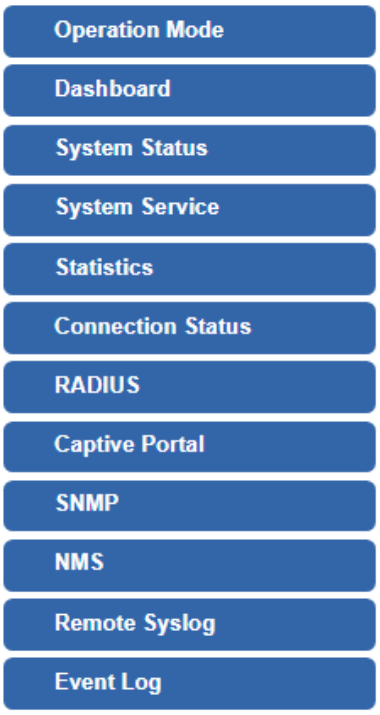


Figure 4-4: System Menu

Object	Description
Operation Mode	The Wizard will guide the user to configuring the router 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
RADIUS	Enable/Disable RADIUS on routers
Captive Portal	Enable/Disable Captive Portal on routers
SNMP	Display SNMP system information
NMS	Enable/Disable NMS on routers
Remote Syslog	Enable Captive Portal on routers
Event Log	Display Event Log information

4.1.1 Operation Mode

The Wizard guides you to configuring the WDAP-3600BE in a different mode, including AP, gateway, repeater and WISP modes. The wizard also supports MESH function set up.

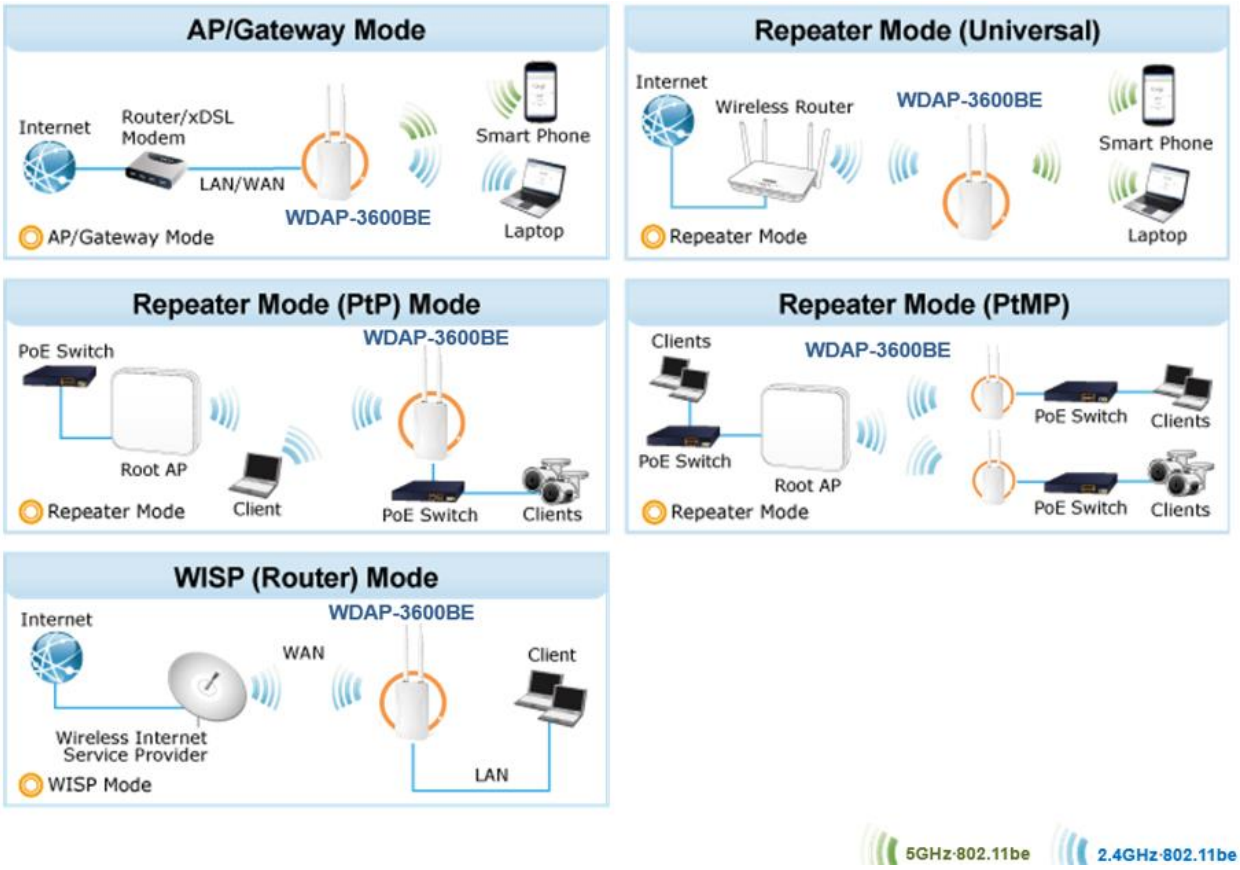


Figure 4-5 Operation Mode

The default operation mode is AP Mode.

4.1.2 Gateway Mode (Router)

Click “**Wizard**” → “**Gateway Mode**” and the following page will be displayed. This section allows you to configure the Gateway mode.

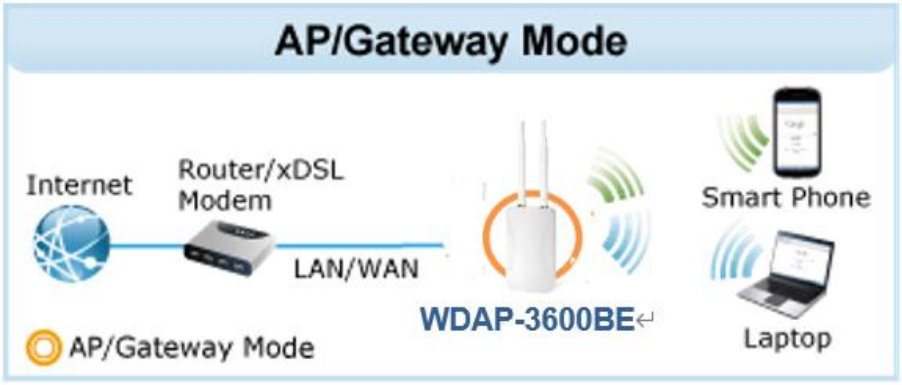
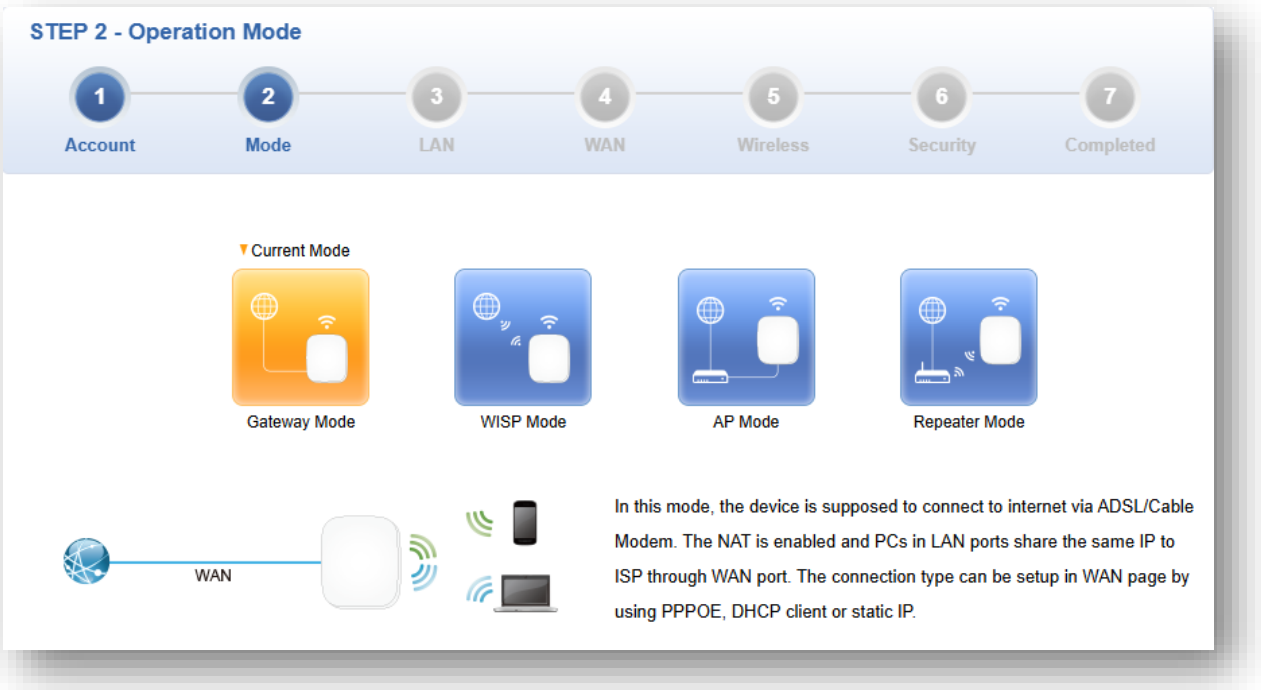


Figure 4-7: Setup Wizard

Step 1: Operation Mode

Select operation Mode.



Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 5-5.

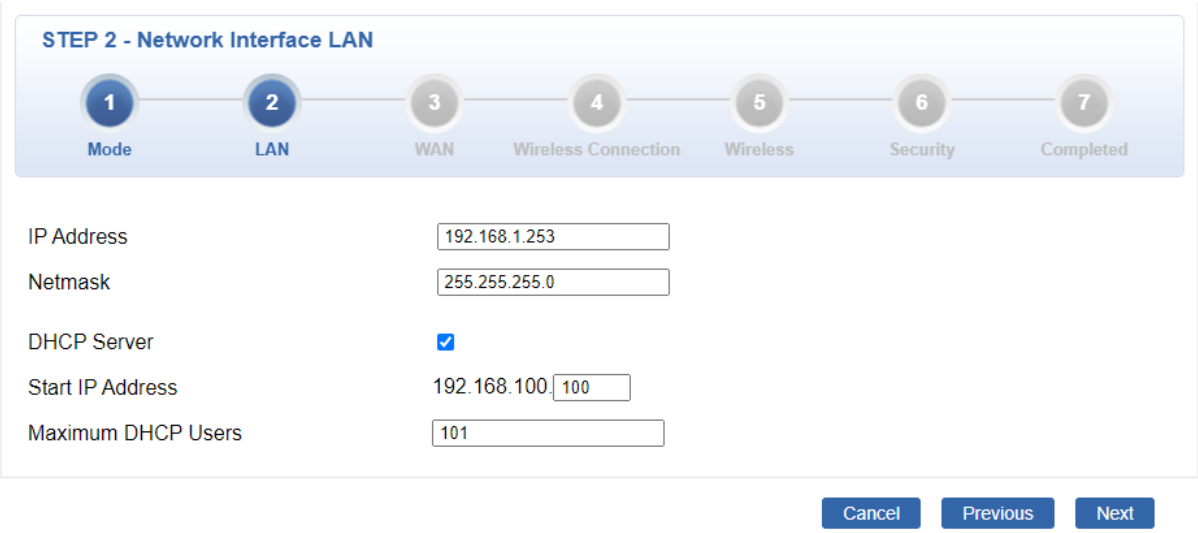


Figure 4-8: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your router. 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 router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the router 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: WAN Interface

The router supports two access modes on the WAN side shown in Figure 4-9

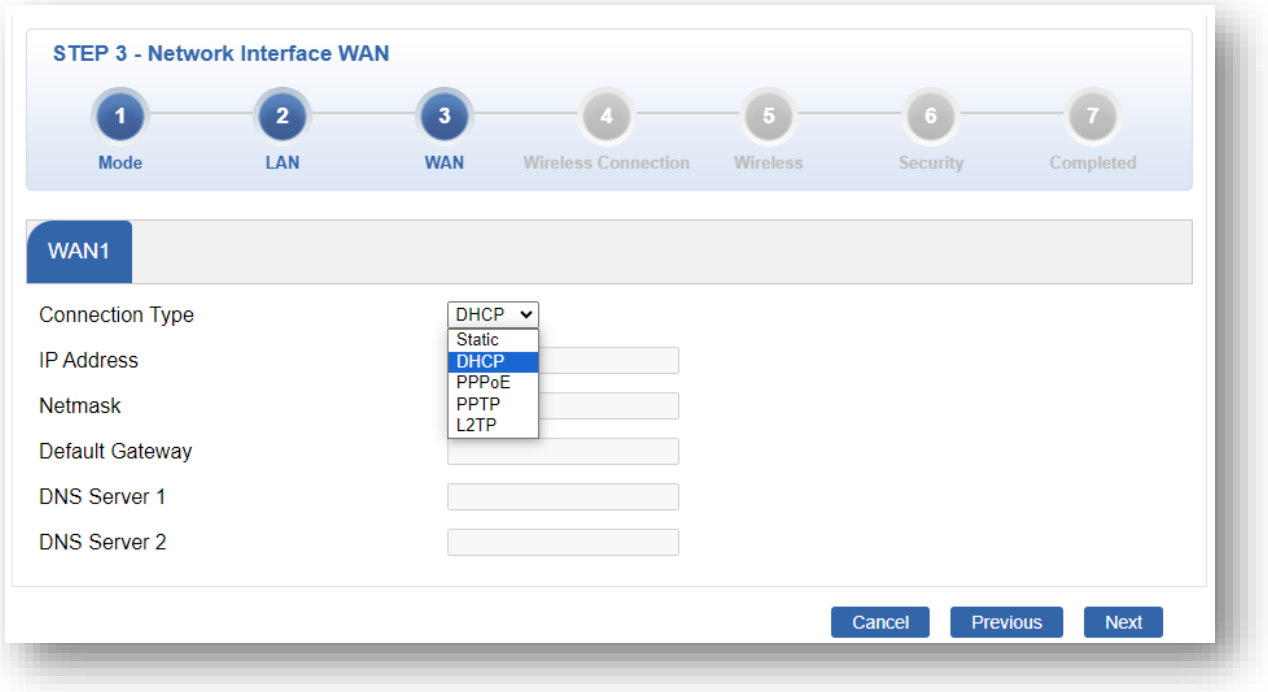


Figure 4-9: Setup Wizard – WAN 1 Configuration

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 router will not accept the IP address if it is not in this format. The setup is shown in Figure 4-10.

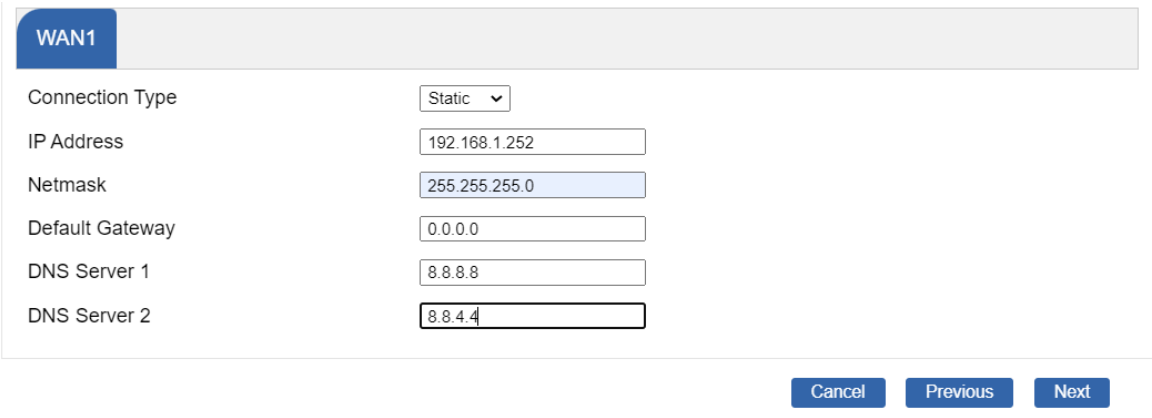


Figure 4-10: WAN Interface Setup – Static IP Setup

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 4-11.

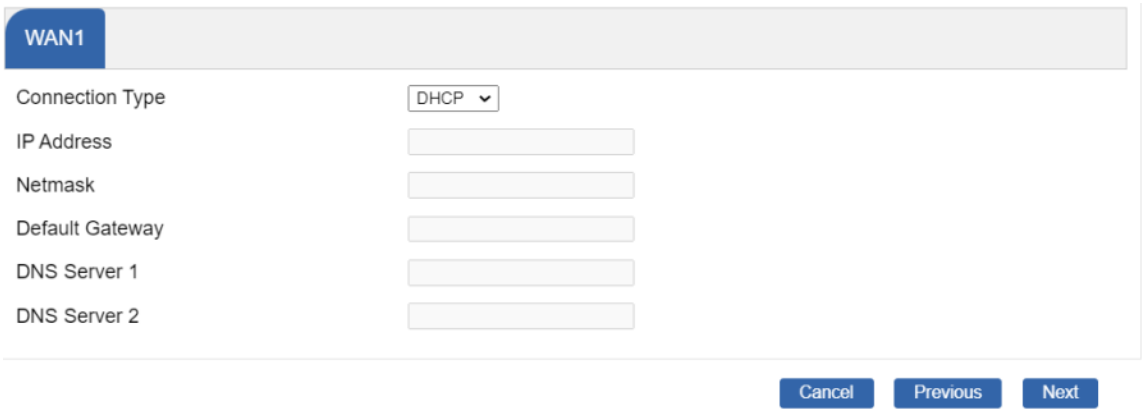


Figure 4-11: WAN Interface Setup – DHCP Setup

Step 4: Network Interface Wireless Connection

Set up the Security Settings as shown in Figure 5-9.

Figure 4-12: Wireless Connection- set up

Object	Description
Mesh Wi-Fi Mode	Select the Mesh role for Master or Node to enable Mesh function. The default configuration is disabled.
Select Radio	Select 2.4GHz or 5GHz for MESH ID radio.
Mesh ID	Enter the Mesh ID, just like SSID, or use the Scan button to discover Mesh ID from the Master/Node Mesh AP.
Encryption	Selector is for the encryption for the sake of security. WPA3 Personal Open WPA3 Personal WPA2/WPA3 Personal WPA2 Personal (AES) WPA2 Personal (TKIP) WPA2 Personal (TKIP+AES) WPA/WPA2 Personal (AES) WPA/WPA2 Personal (TKIP) WPA/WPA2 Personal (TKIP+AES) WPA Personal (AES) WPA Personal (TKIP) WPA Personal (TKIP+AES) WPA2 Enterprise WPA/WPA2 Enterprise
Passphrase	Enter the password for Mesh ID; the default configuration is null.
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.

Step 5: Network Interface Wireless

Set up the Security Settings as shown in Figure 4-13.

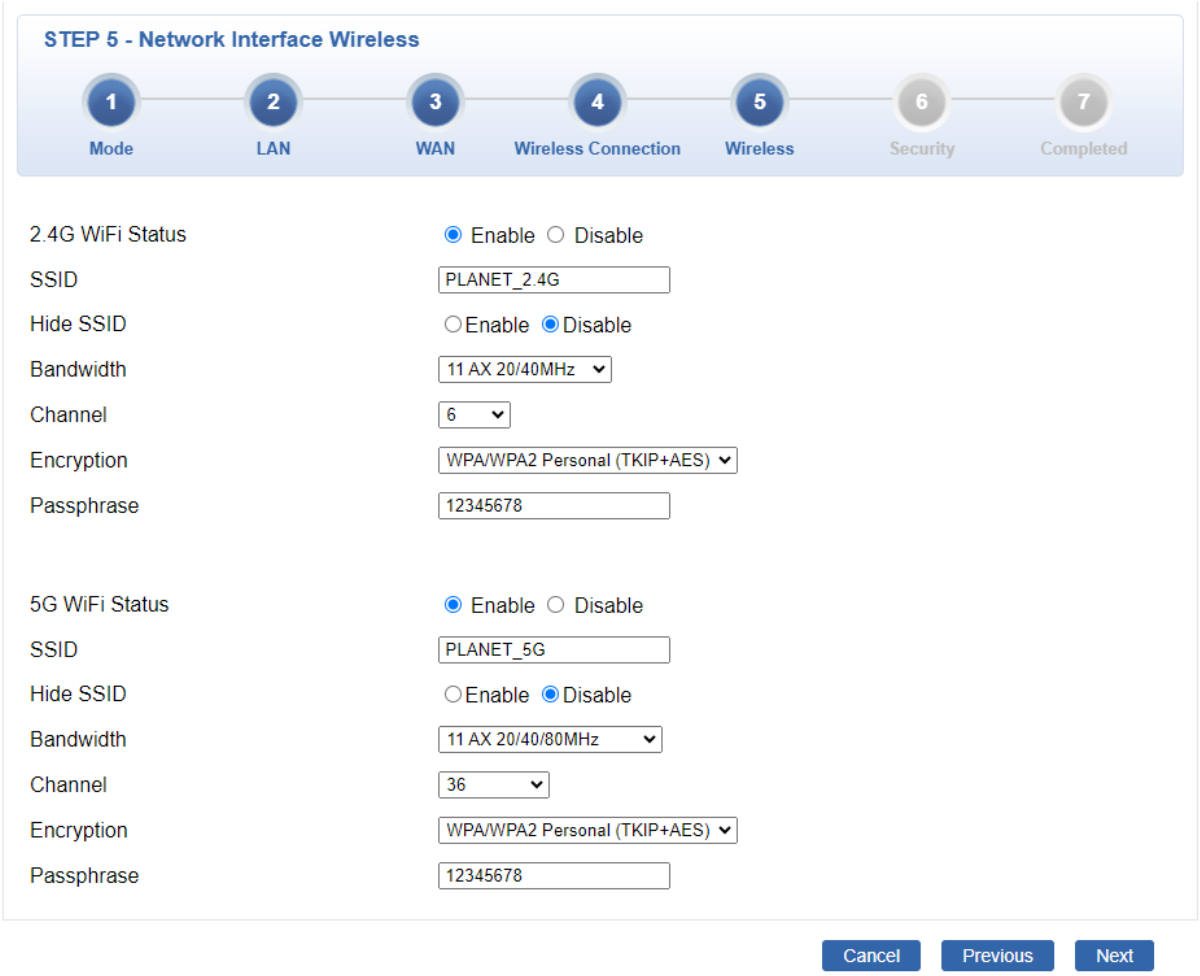


Figure 4-13: Wireless Setup

Object	Description
2.4G/5G Wi-Fi Status	Enable or Disable 2.4GHz/5GHz radio.
SSID	Enter the SSID ID name. The default configuration is PLANET_2.4G/PLANET_5G.
Bandwidth	Select bandwidth for 2.4GHz/5GHz
Channel	Select channel for 2.4GHz/5GHz
Encryption	Selector is the encryption for the sake of security. WPA3 Personal Open WPA3 Personal WPA2/WPA3 Personal WPA2 Personal (AES) WPA2 Personal (TKIP) WPA2 Personal (TKIP+AES) WPA/WPA2 Personal (AES) WPA/WPA2 Personal (TKIP) WPA/WPA2 Personal (TKIP+AES) WPA Personal (AES) WPA Personal (TKIP) WPA Personal (TKIP+AES) WPA2 Enterprise WPA/WPA2 Enterprise
Passphrase	Enter the password for SSID; the default configuration is null.
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.

Step 6: Security Setting

Set up the Security Settings as shown in Figure 4-14.

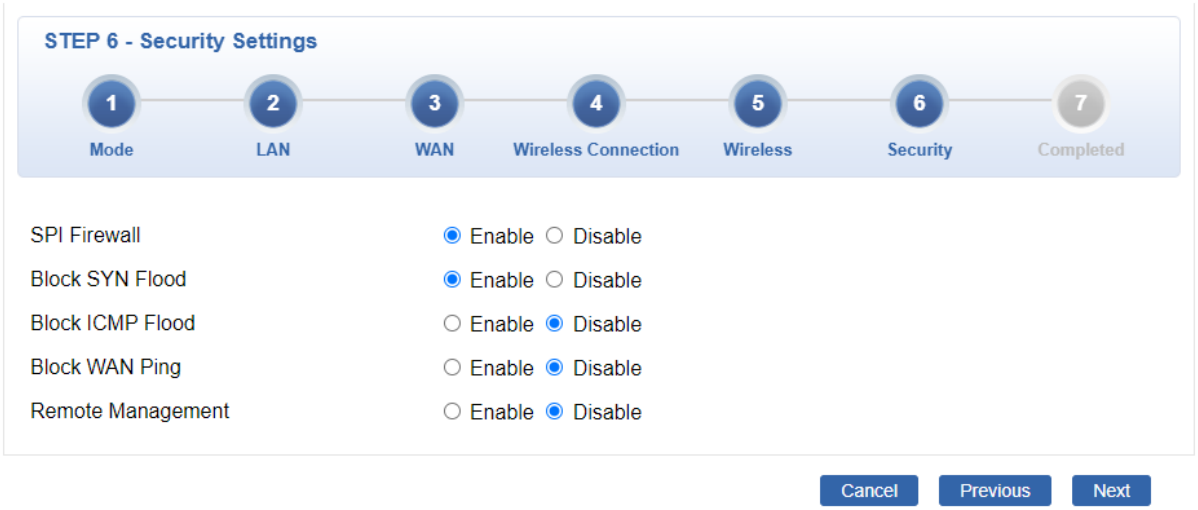


Figure 4-14: Setup Wizard –Security Setting

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

Step 7: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in Figure 4-15.

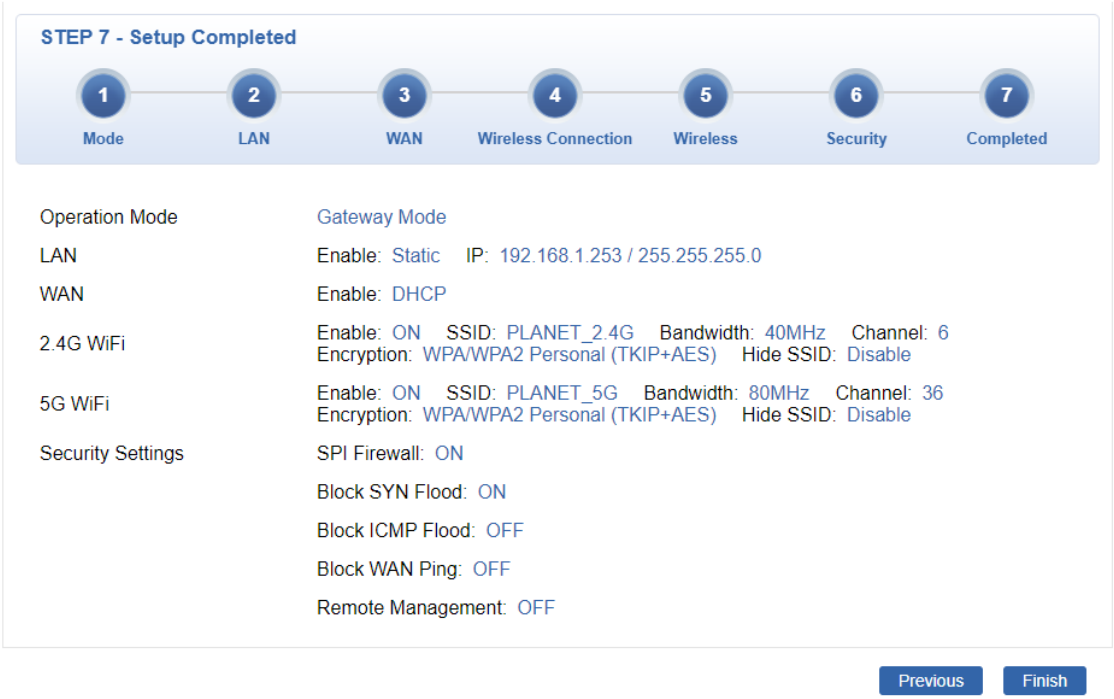


Figure 4-15: Setup Wizard – Setup Completed

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

4.1.3 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 4-16.

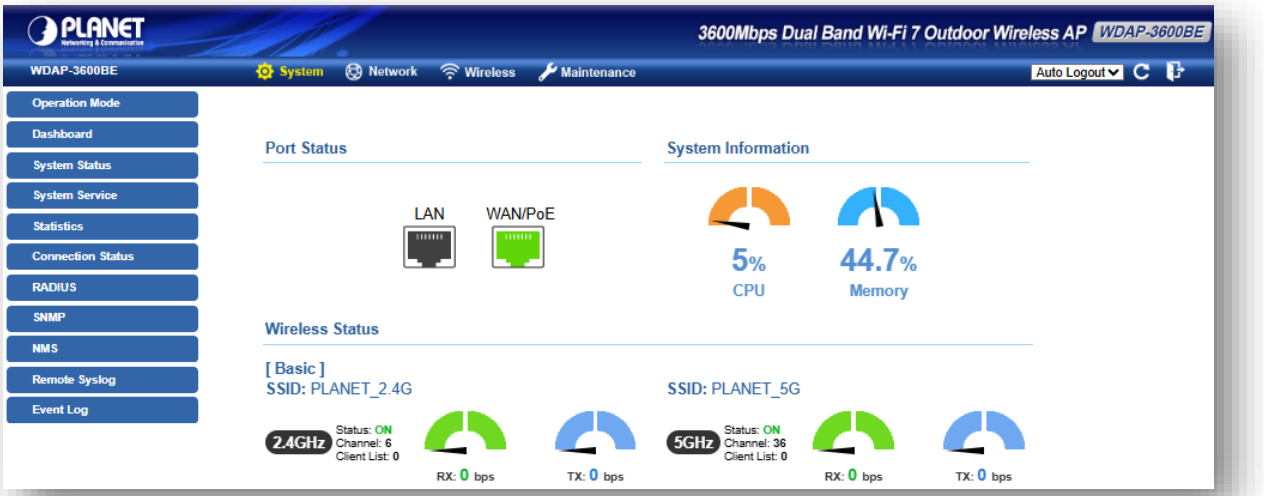


Figure 4-16: Dashboard

Port Status

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

Wireless Status

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

System Information

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

4.1.4 System Status

This page displays system information as shown in Figure 4-17.

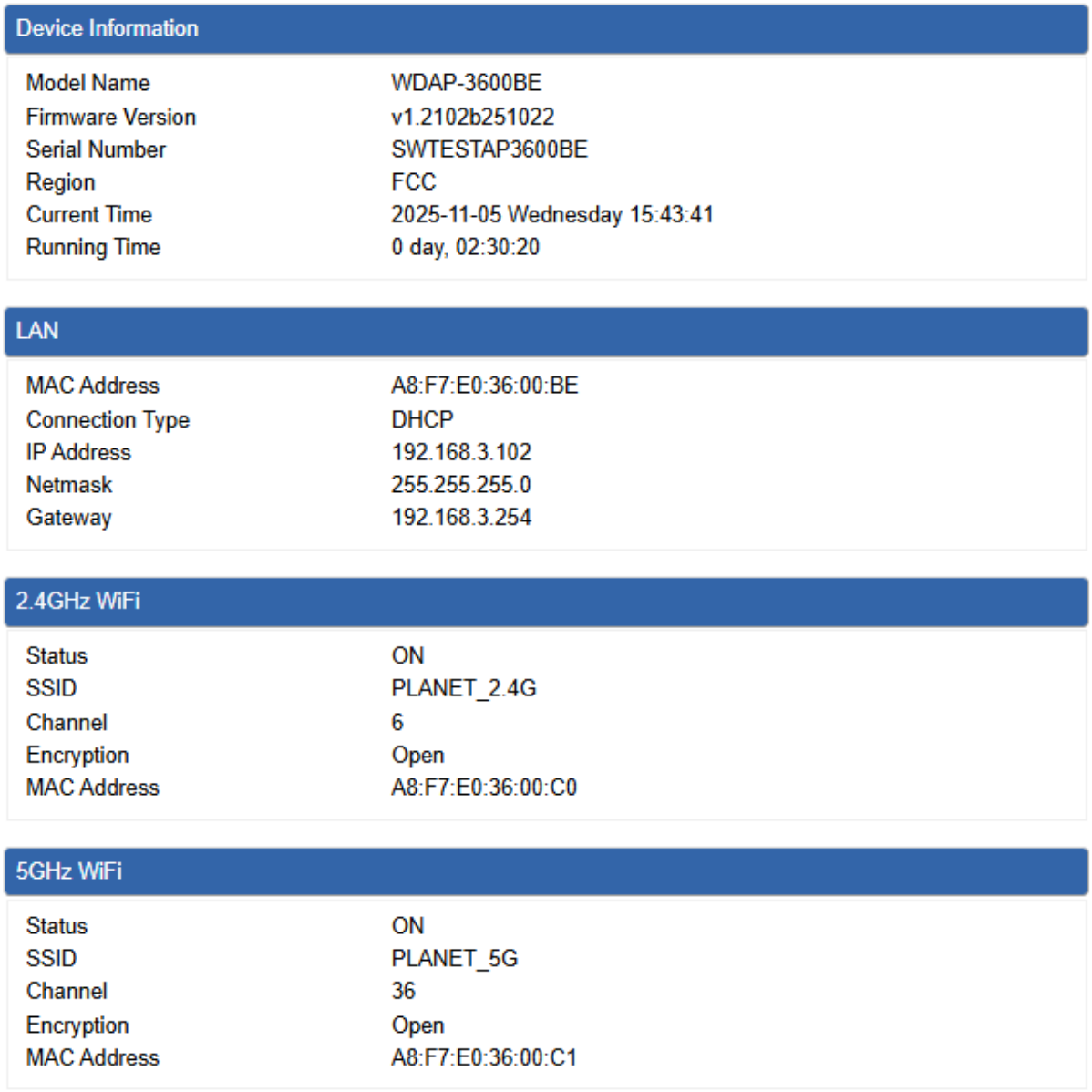


Figure 4-17: Status

4.1.5 System Service

This page displays the number of packets that pass through the router on the WAN and LAN. The statistics are shown in Figure 4-18.

Server Service

#	Action	Service	Status
1	Enabled	DHCP Service	DHCP Table: 5
2	Disabled	DDNS Service	Not enabled
3	Disabled	Quality of Service	
4	Disabled	RADIUS Service	
5	Disabled	Captive Portal	
6	Enabled	2.4G WiFi	SSID: PLANET_2.4G
7	Enabled	5G WiFi	SSID: PLANET_5G

Secured Server Service

#	Action	Service	Status
1	Enabled	Cyberseurity	TLS 1.1, TLS 1.2, TLS 1.3
2	Enabled	SPI Firewall	
3	Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32

Figure 4-18: Service

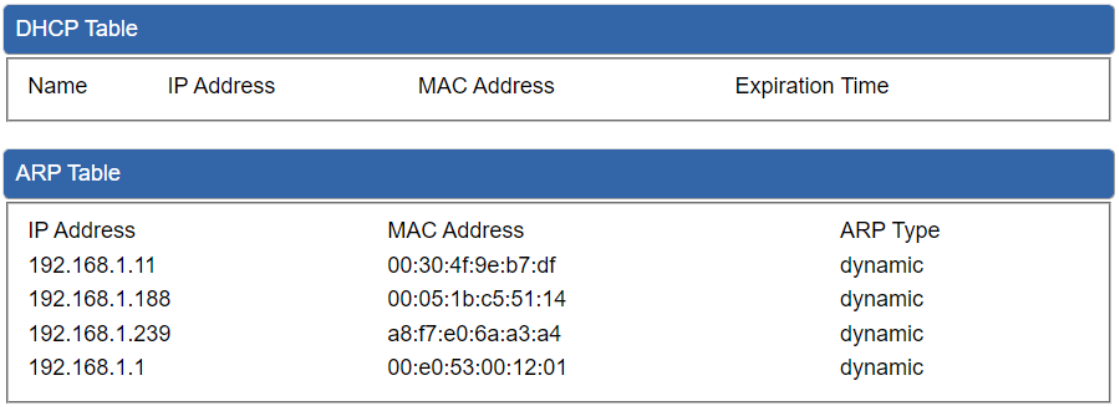
4.1.6 Statistics

This page displays the number of packets that pass through the router on the WAN and LAN. The statistics are shown in Figure 4-19.

Figure 4-19: Statistics

4.1.7 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in Figure 4-20.



DHCP Table

Name	IP Address	MAC Address	Expiration Time

ARP Table

IP Address	MAC Address	ARP Type
192.168.1.11	00:30:4f:9e:b7:df	dynamic
192.168.1.188	00:05:1b:c5:51:14	dynamic
192.168.1.239	a8:f7:e0:6a:a3:a4	dynamic
192.168.1.1	00:e0:53:00:12:01	dynamic

Figure 4-20: Connection Status

4.1.8 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 4-21.

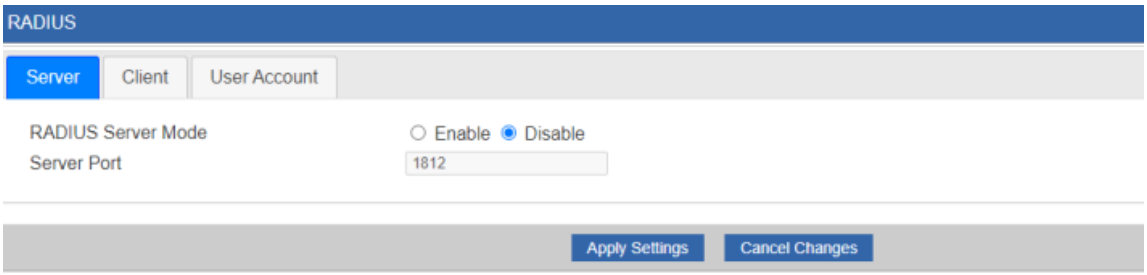


Figure 4-21: RADIUS

Object	Description
RADIUS	Disable or enable the RADIUS function. The default configuration is disabled.
Server Port	Default: 1812

4.1.9 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 4-22.

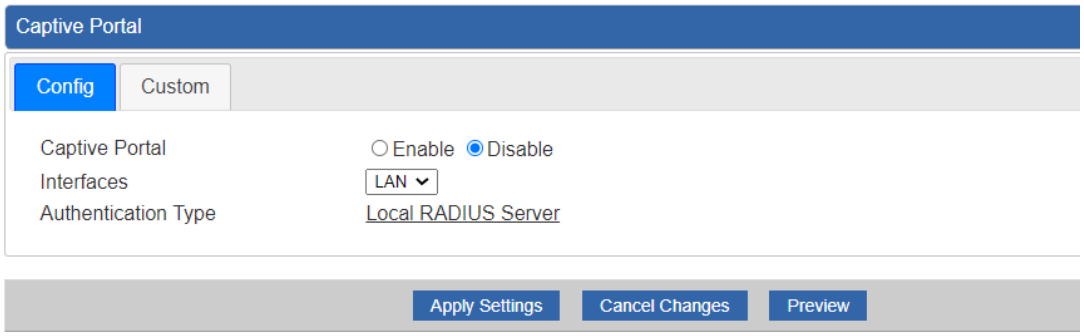


Figure 4-22: Captive Portal

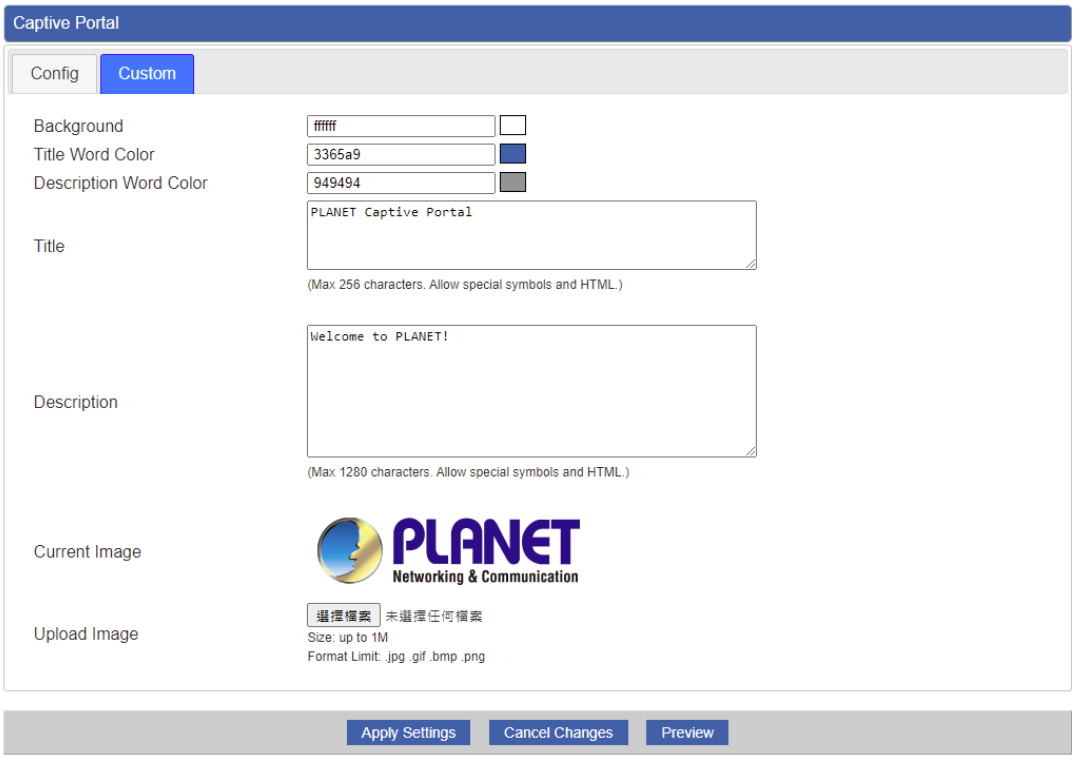
Object	Description
Captive Portal	Disable or enable the Captive Portal function. The default configuration is disabled.

Note

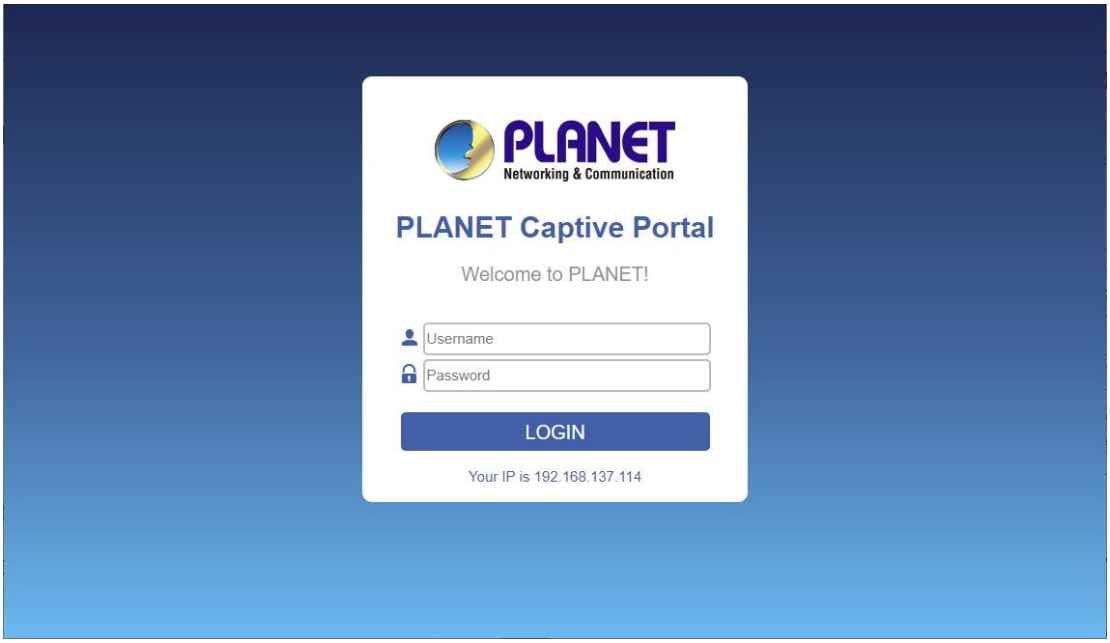
Captive Portal function can be only configured at **Gateway Mode**

■ Customizing the Custom Captive Portal Web Page

1. Click **Custom**



2. After configure and upload image, click **Apply Settings** button
3. Click **Preview** to check the Captive Portal login page



4.1.10 SNMP

This page provides SNMP setting of the router as shown in Figure 4-23.

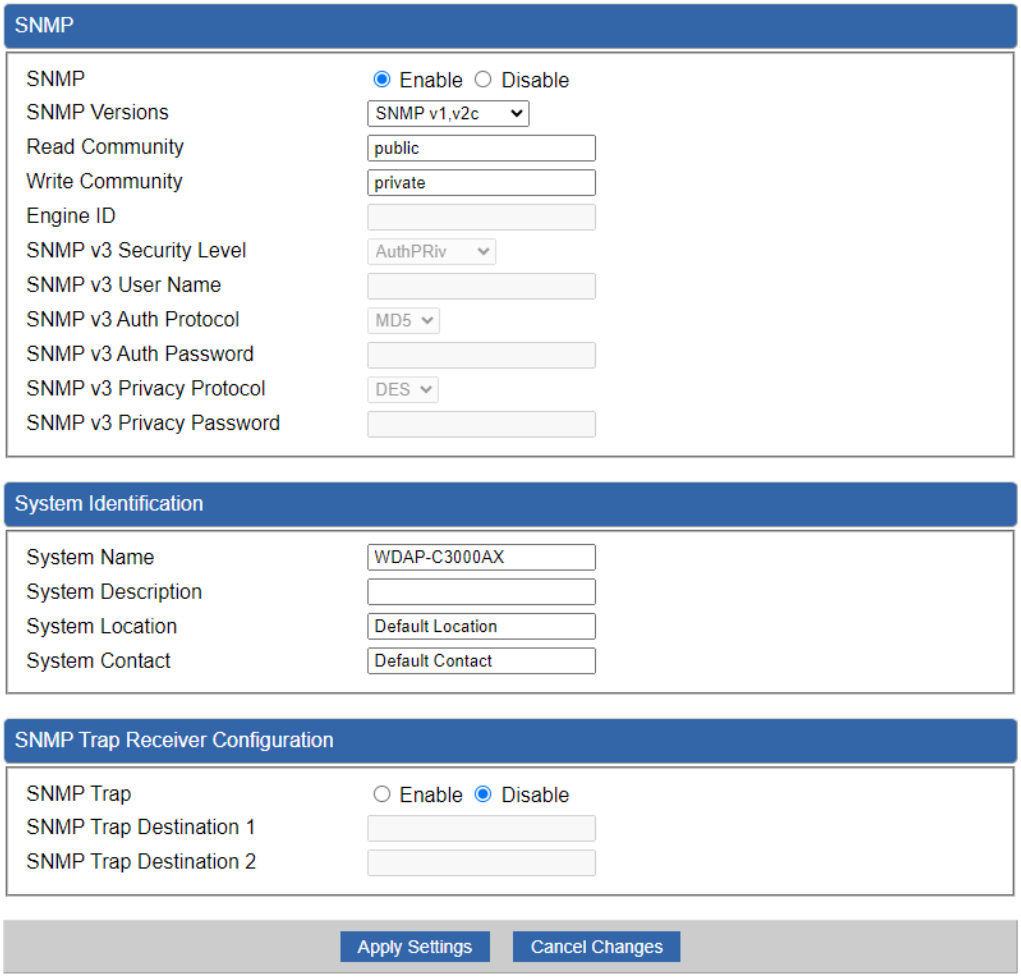


Figure 4-23: SNMP

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 router.
System Name	Allows entering characters for system name of the router.
System Location	Allows entering characters for system location of the router.
System Contact	Allows entering characters for system contact of the router.
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.

4.1.11 NMS

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

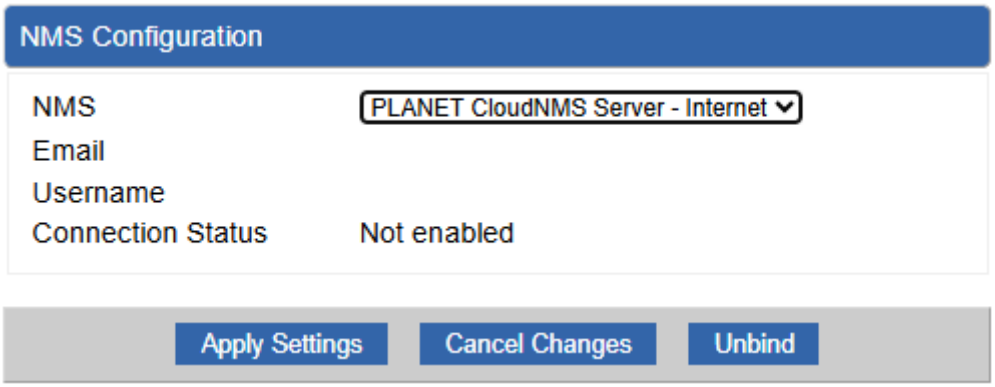
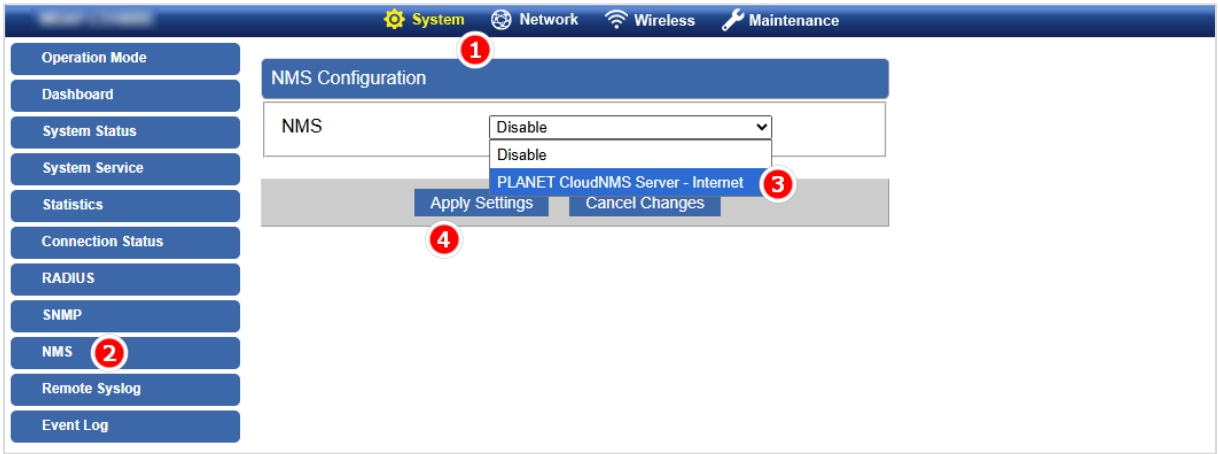


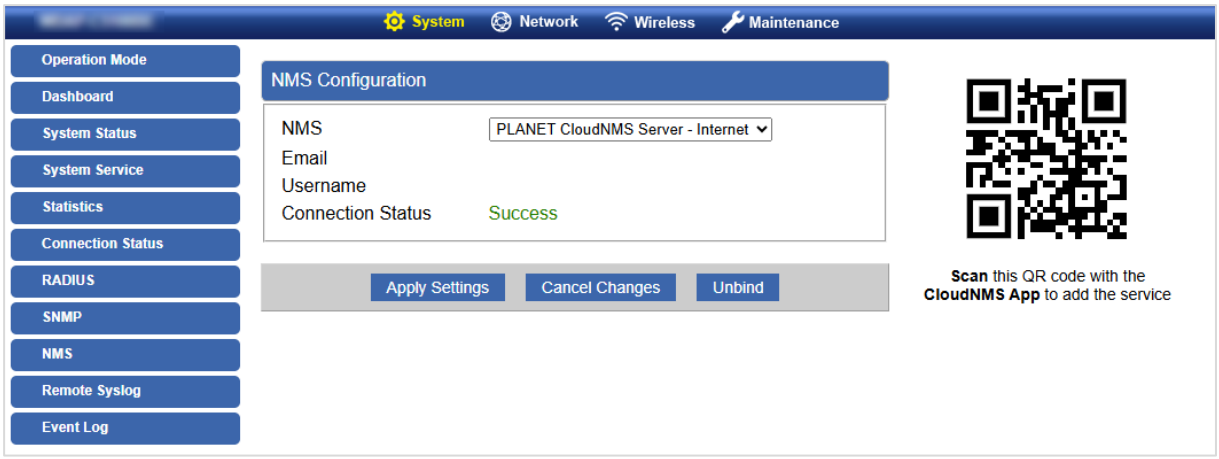
Figure 4-24: CloudNMS Server

Object	Description
Email	The email is 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-3600BE and enable PLANET CloudNMS Server – Internet feature.



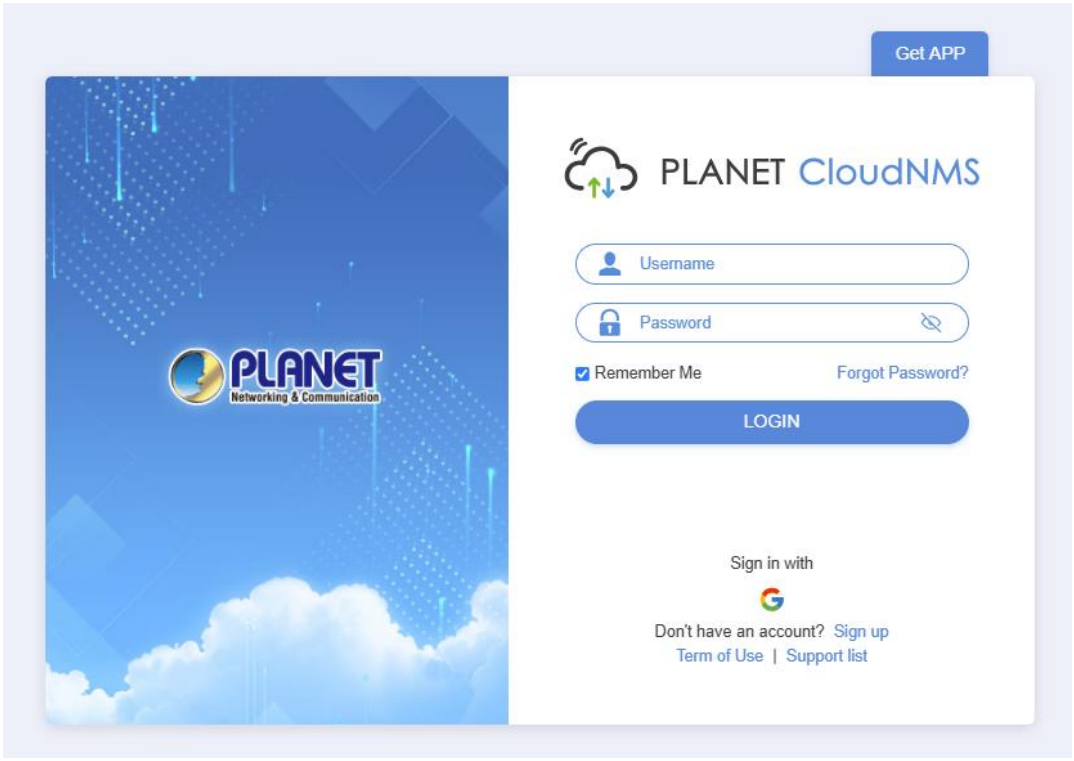


Step 2: Access the CloudViewer Platform

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:



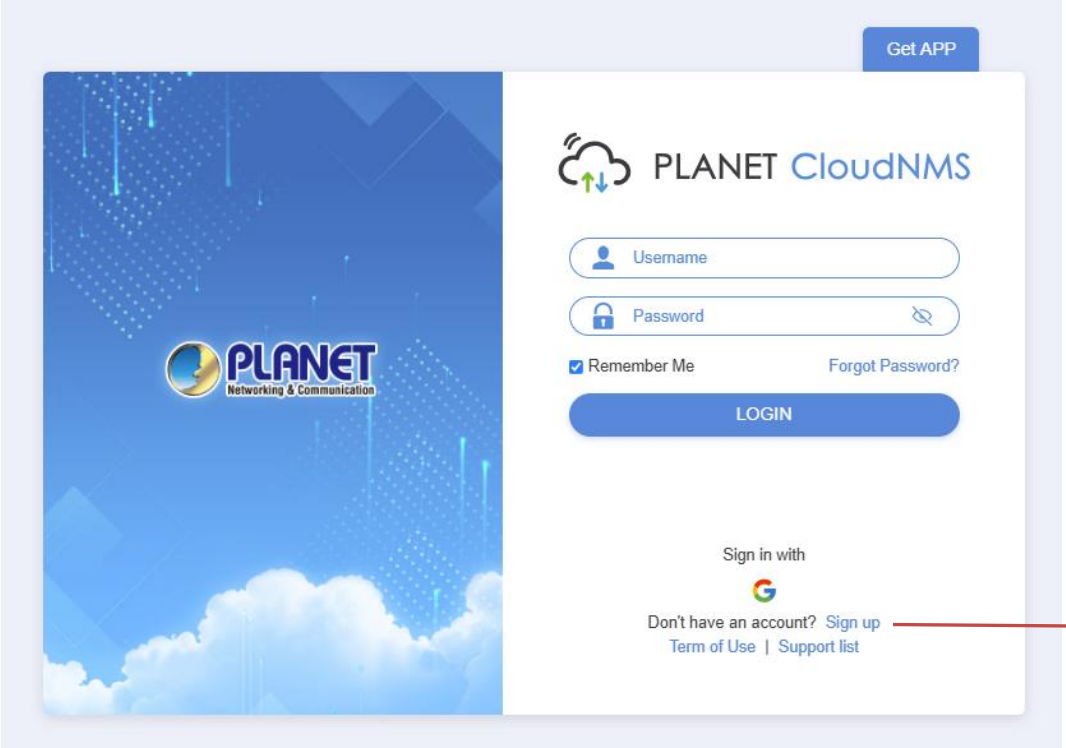
App:

Step 3: Register an Account

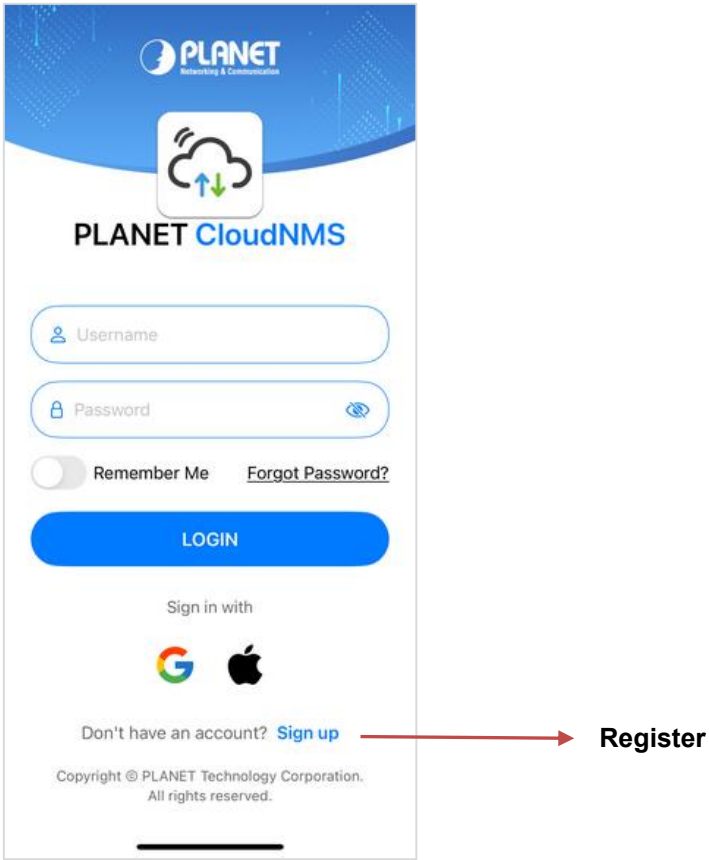
Launch the PLANET CloudNMS Platform or App, and log in with your CloudNMS account.

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

Web:



App:



Step 4: Bind the Device

Via Web:

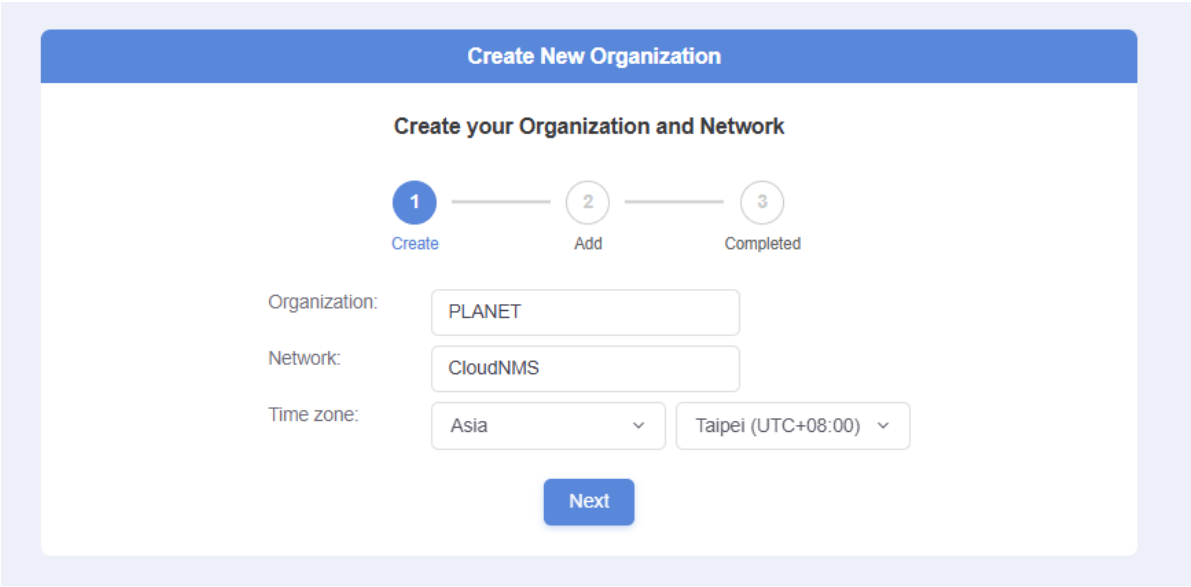
- Log in to the PLANET CloudNMS Platform.
- Create an Organization and a Network for the device.
- Enter the required device information and complete the setup wizard.

Via App:

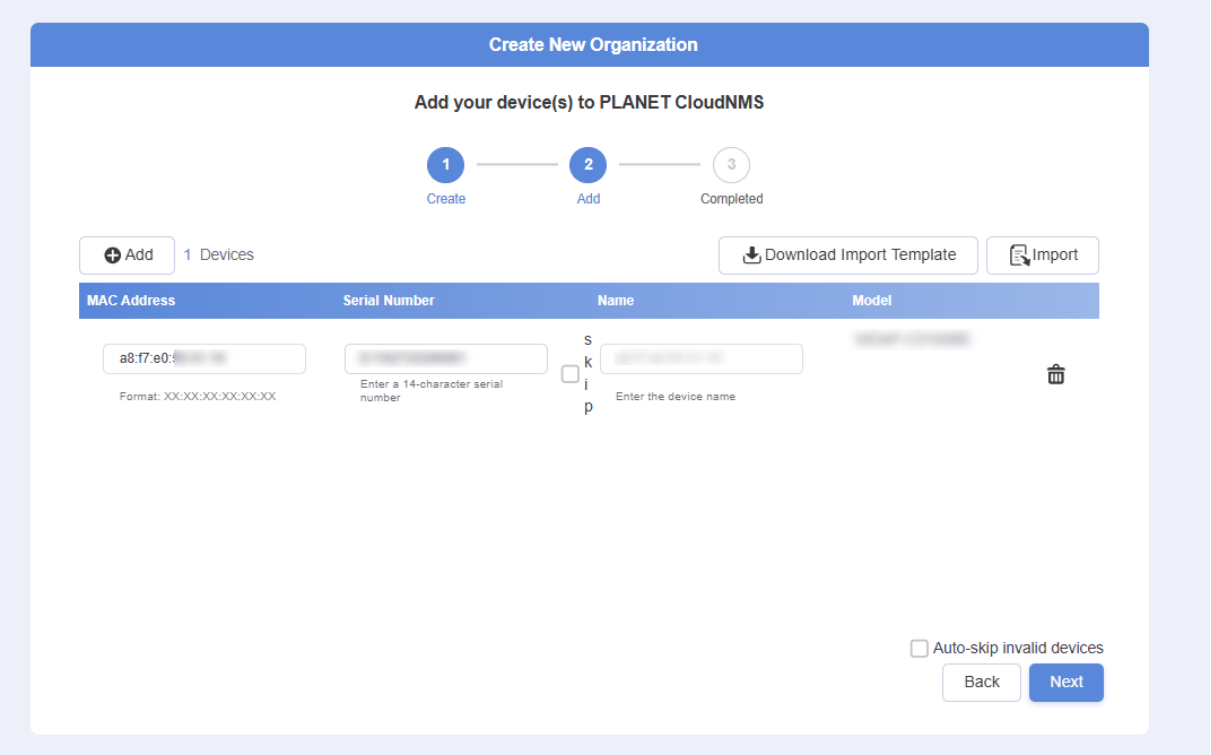
- Launch the PLANET CloudNMS App and sign in with your CloudNMS account.
- Create an Organization and a Network for the device, then go to the Add Device process.
- Enter the required device information or Scan the QR code of the device, and complete the setup wizard.

Web:

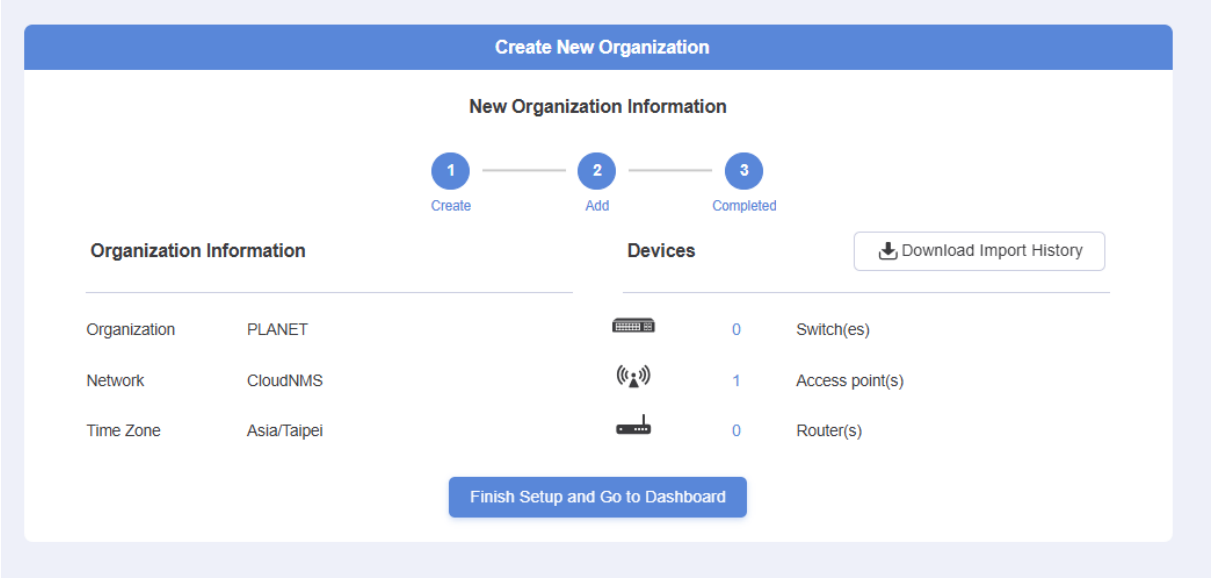
1. Create an Organization and a Network



2. Enter the required device information

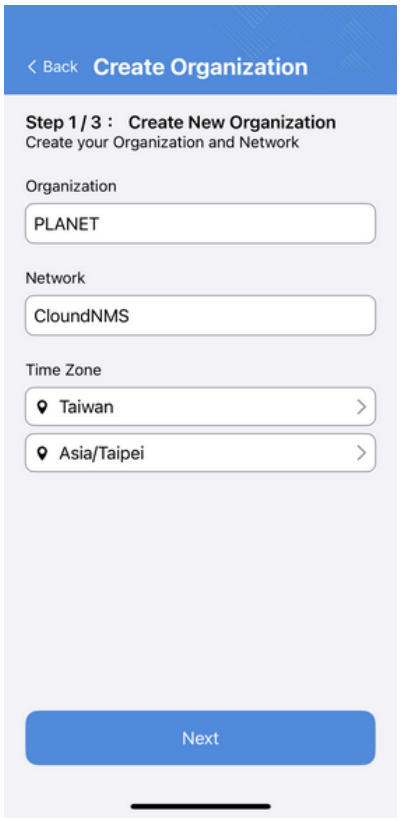


3. Finish

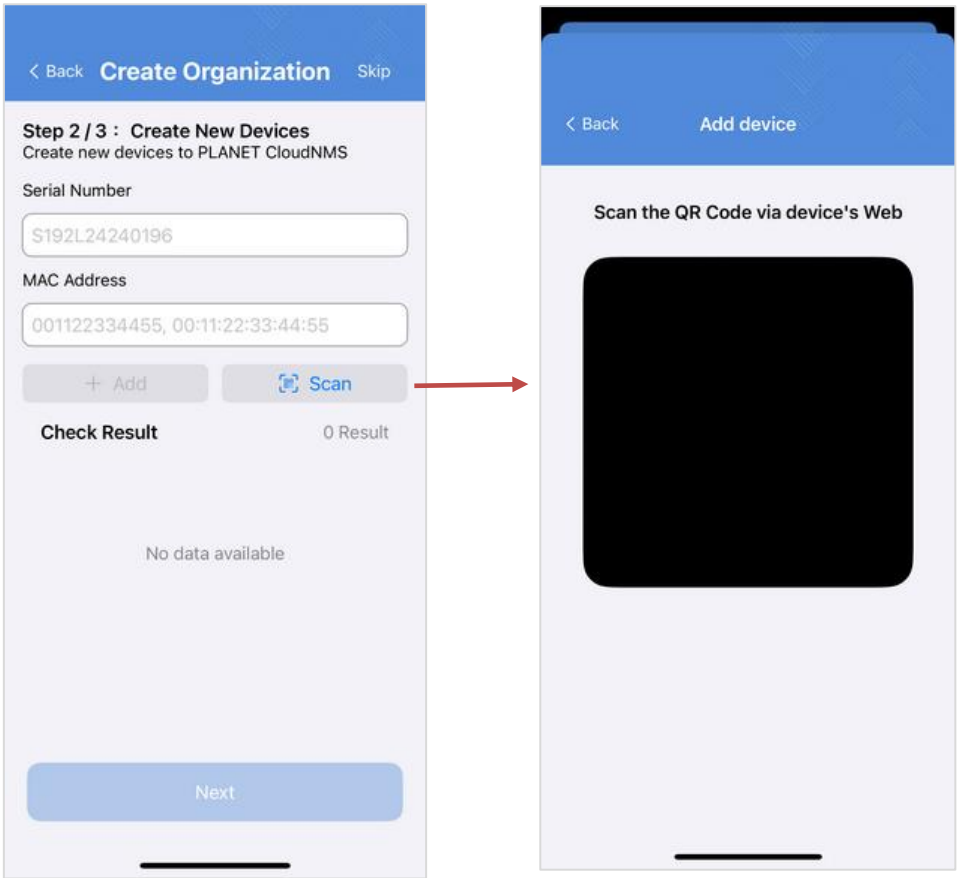


App:

1. Create an Organization and a Network



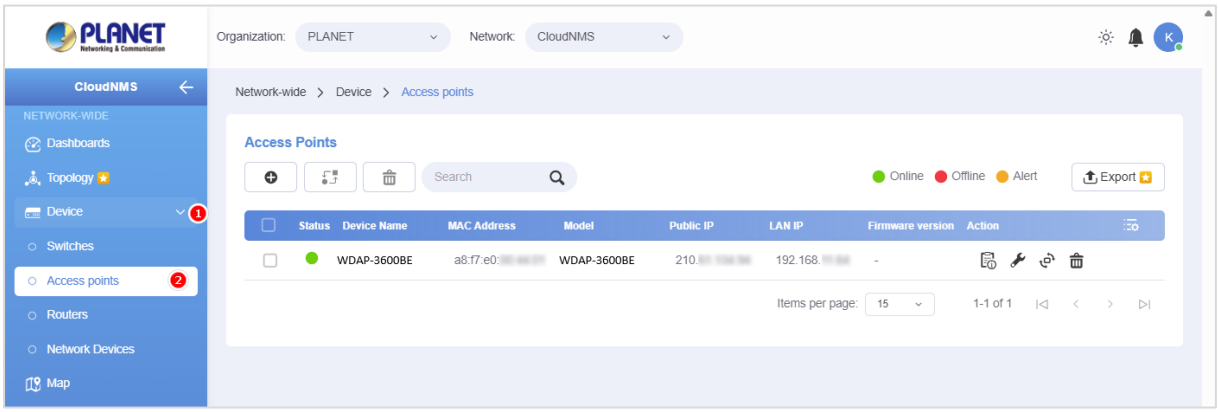
2. Enter the required device information or Scan QR code



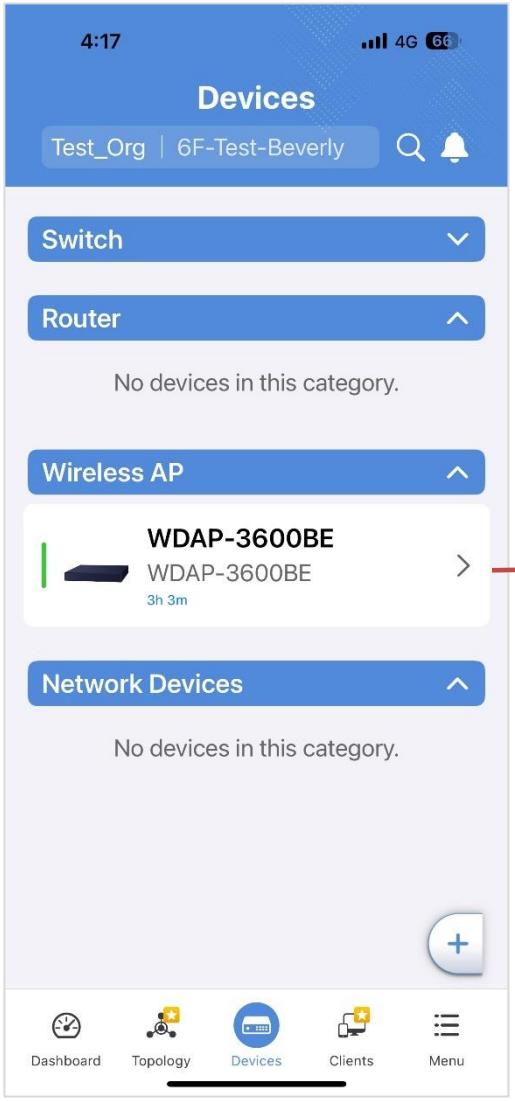
3. Finish

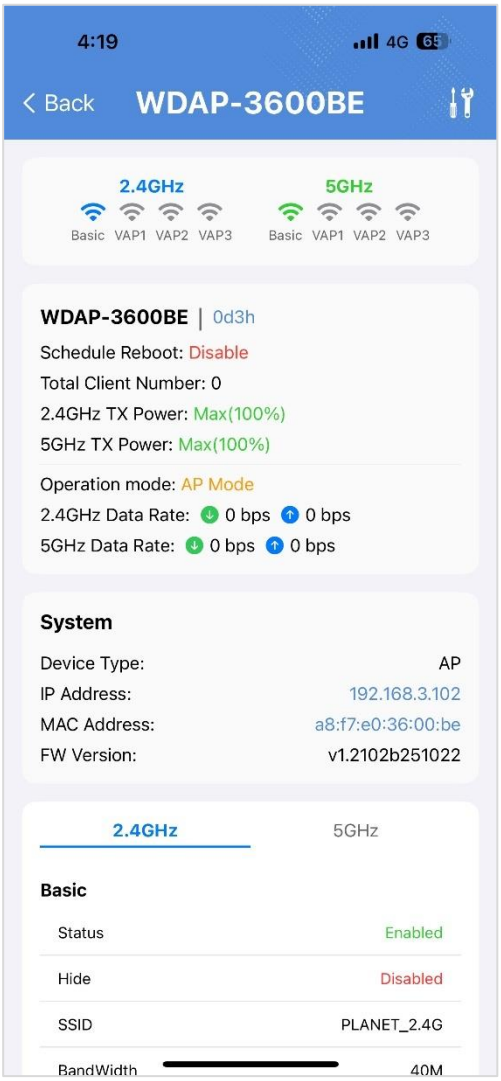
Step 5: Finish

Web:



App:


4:17
4G
Devices
Test_Org | 6F-Test-Beverly
Switch
Router
No devices in this category.
Wireless AP
WDAP-3600BE
WDAP-3600BE
3h 3m
Network Devices
No devices in this category.
Dashboard
Topology
Devices
Clients
Menu


4:19
4G
Back
WDAP-3600BE
2.4GHz
Basic VAP1 VAP2 VAP3
5GHz
Basic VAP1 VAP2 VAP3
WDAP-3600BE | 0d3h
Schedule Reboot: Disable
Total Client Number: 0
2.4GHz TX Power: Max(100%)
5GHz TX Power: Max(100%)
Operation mode: AP Mode
2.4GHz Data Rate: 0 bps 0 bps
5GHz Data Rate: 0 bps 0 bps
System
Device Type: AP
IP Address: 192.168.3.102
MAC Address: a8:f7:e0:36:00:be
FW Version: v1.2102b251022
2.4GHz
5GHz
Basic
Status Enabled
Hide Disabled
SSID PLANET_2.4G
BandWidth 40M

4.1.12 Remote Syslog

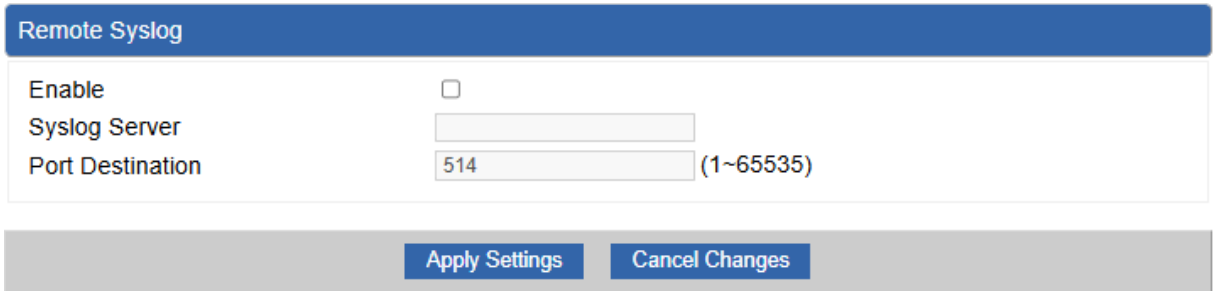


Figure 4-25: Remote Syslog

Object	Description
Enable Remote Syslog	Enable or disable the Remote Syslog function. When enabled, system logs will be sent to the specified Syslog server.
Syslog Server	Enter the IP address or domain name of the remote Syslog server.
Port Destination	Specify the destination port of the Syslog server (default: 514).

4.1.13 Event Log

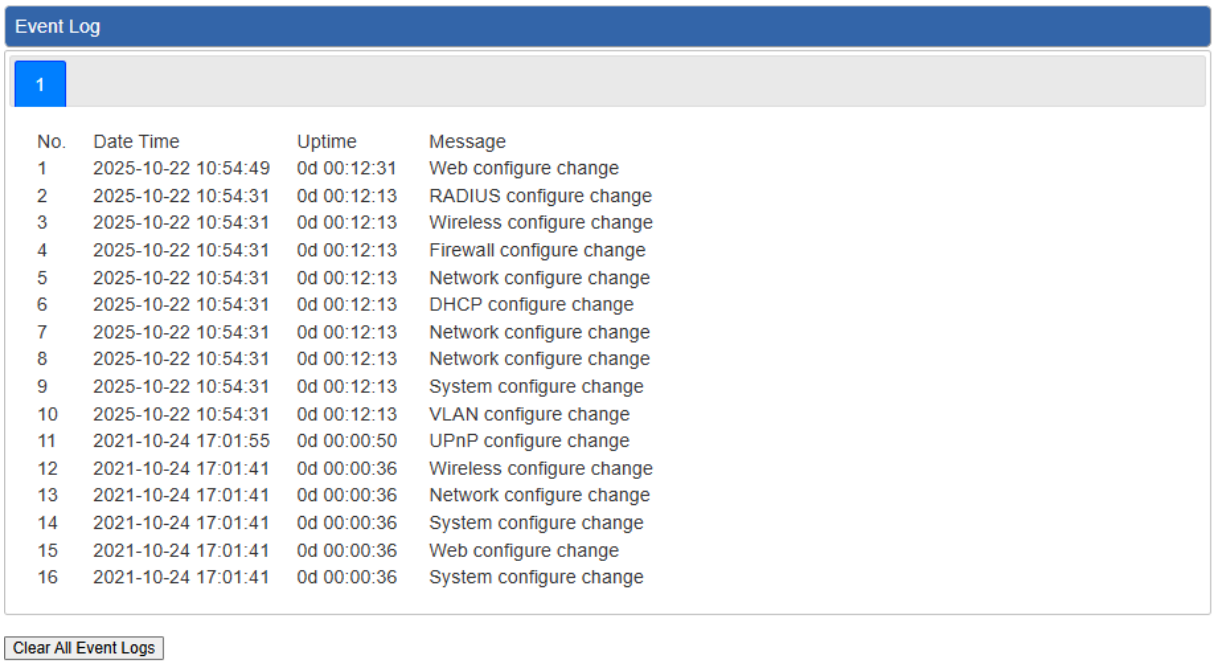


Figure 4-26: Event Log

Object	Description
Event Log	Display Event Log information

4.2 Network

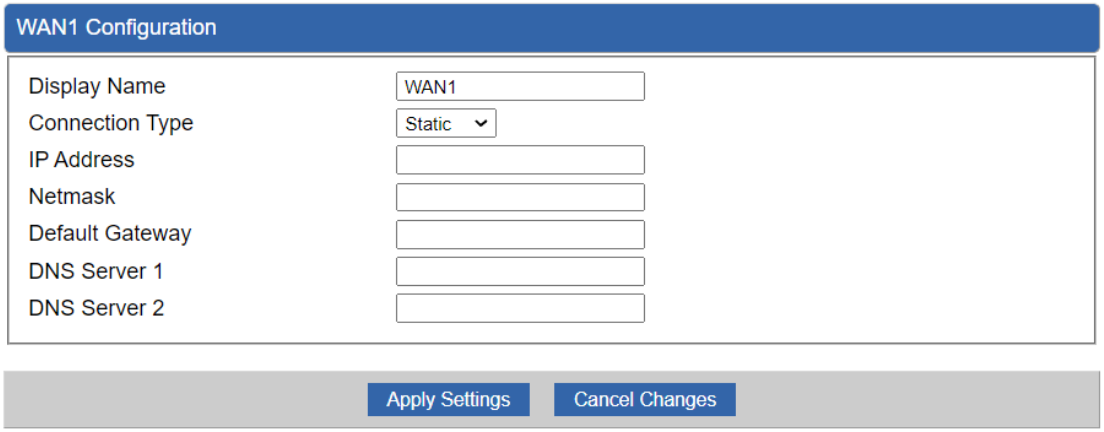
The Network function provides WAN, LAN and network configuration of the router as shown in Figure 4-27.

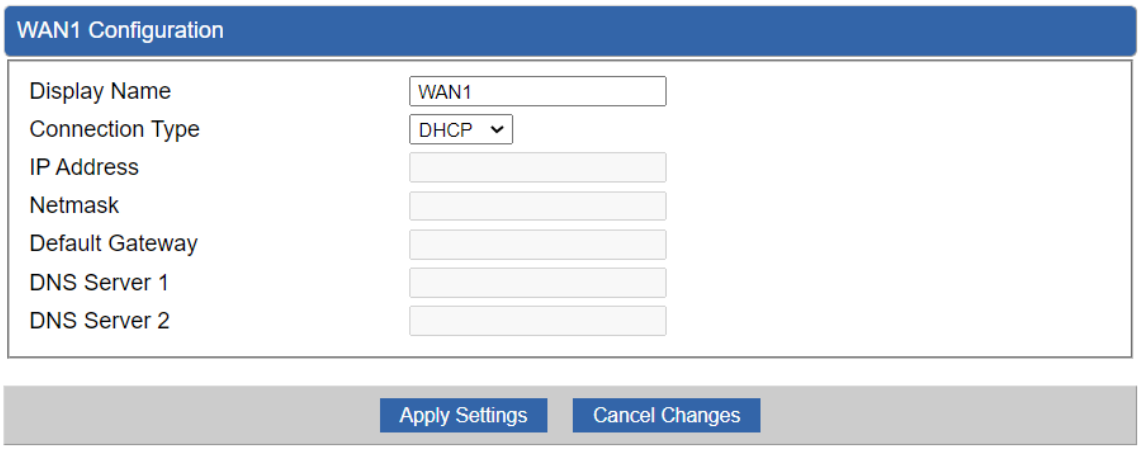
Figure 4-27: Network Menu

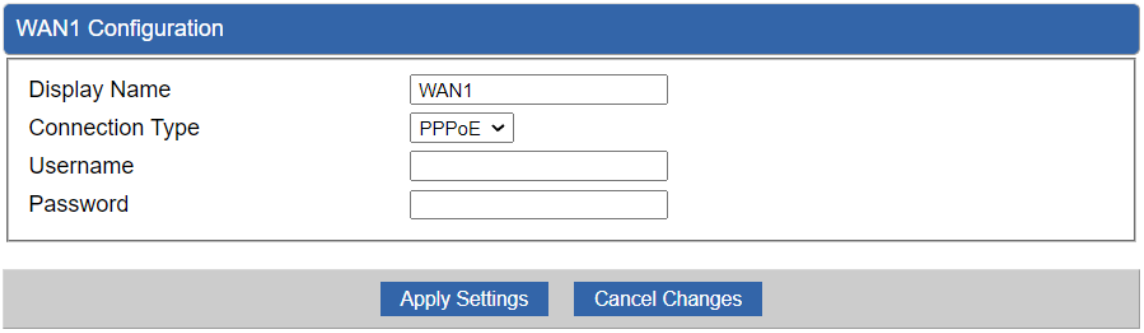
Object	Description
WAN	Allows setting WAN interface.
LAN	Allows setting LAN interface.
UPnP	Disable or enable the UPnP function. The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function. The default configuration is disabled.
OSPF	Disable or enable the 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.

4.2.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the router as shown in Figure 4-28. Here you may select the access method by clicking the item value of WAN access type.







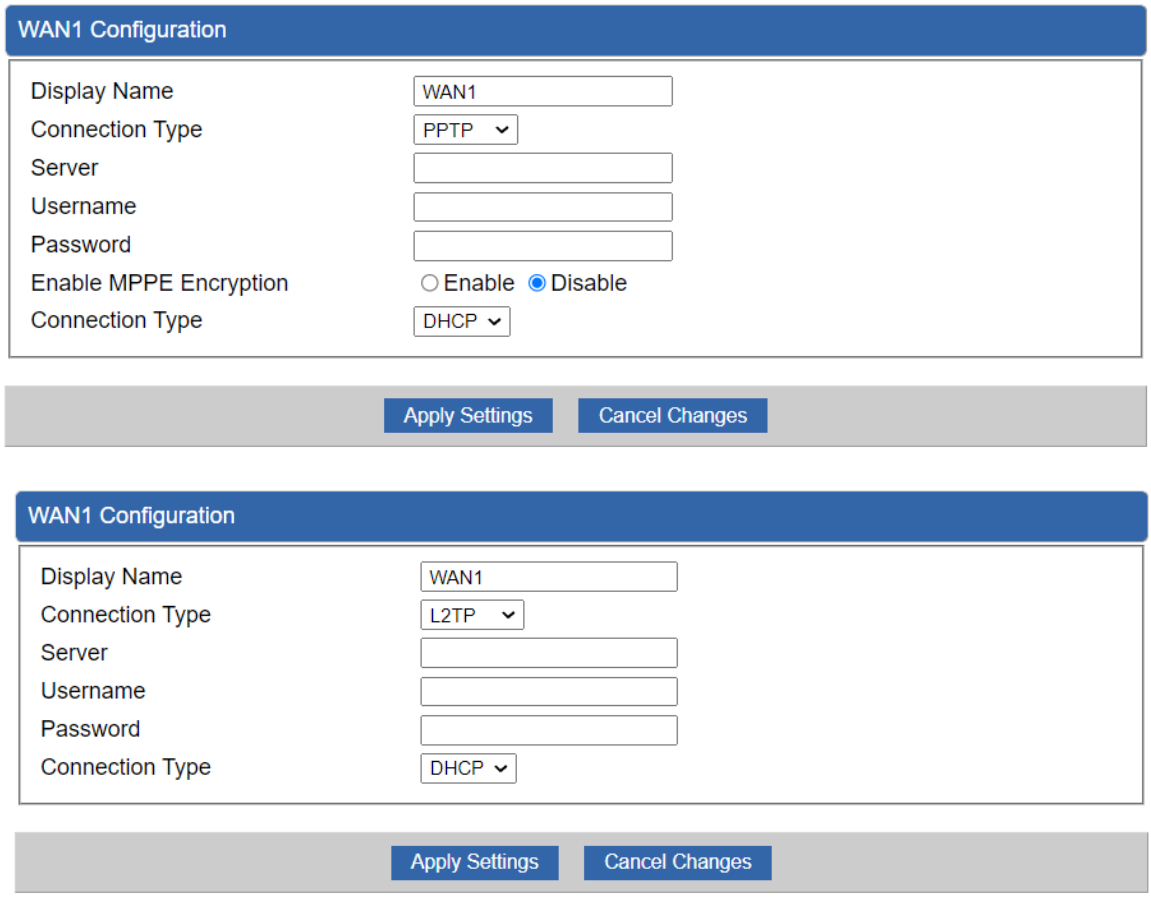


Figure 4-28: WAN

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 router will not accept the IP address if it is not in this format. **IP Address** Enter the IP address assigned by your ISP. **Netmask** Enter the Subnet Mask assigned by your ISP. **Gateway** Enter the Gateway assigned by your ISP.

Object	Description	
		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.
	PPPoE	Select PPPOE if your ISP is using a PPPoE connection and provide you with PPPoE user name and password info.
	PPTP	Enable or disable PPTP to pass through PPTP communication data.
	L2TP	Enable or disable L2TP to pass through L2TP communication data.

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

4.2.2 LAN

This page is used to configure the parameters for local area network which connects to the LAN port of your router as shown in Figure 4-29. Here you may change the settings for IP address, subnet mask, DHCP, etc.

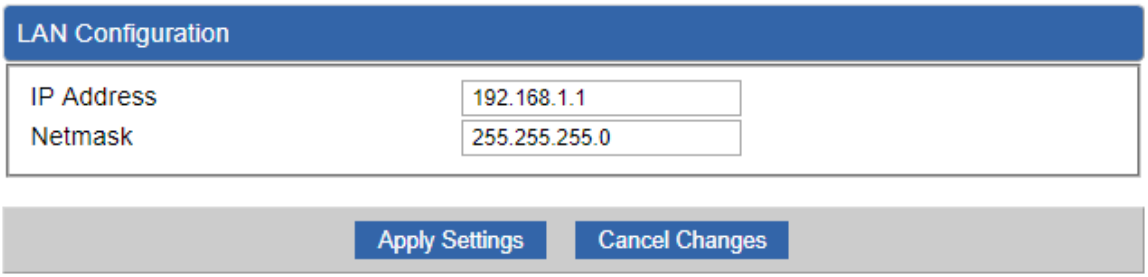


Figure 4-29: LAN Setup

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

4.2.3 UPnP

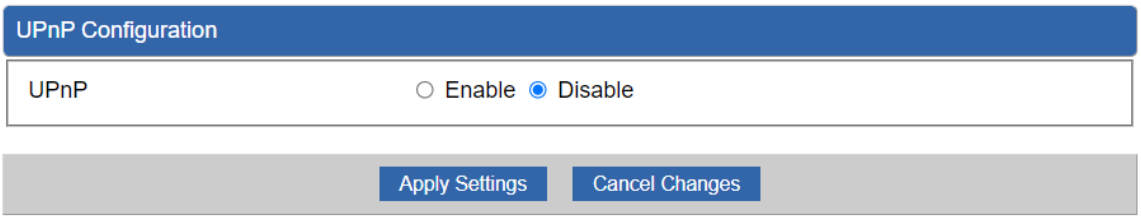


Figure 4-30: UPnP

Object	Description
UPnP	Set the function as enable or disable

4.2.4 Routing

Please refer to the following sections for the details as shown in Figures 5-28 and 29.

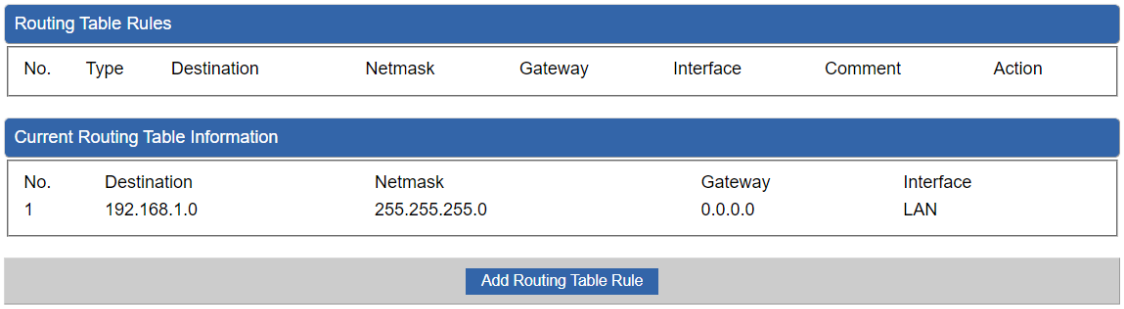


Figure 4-31: Routing table

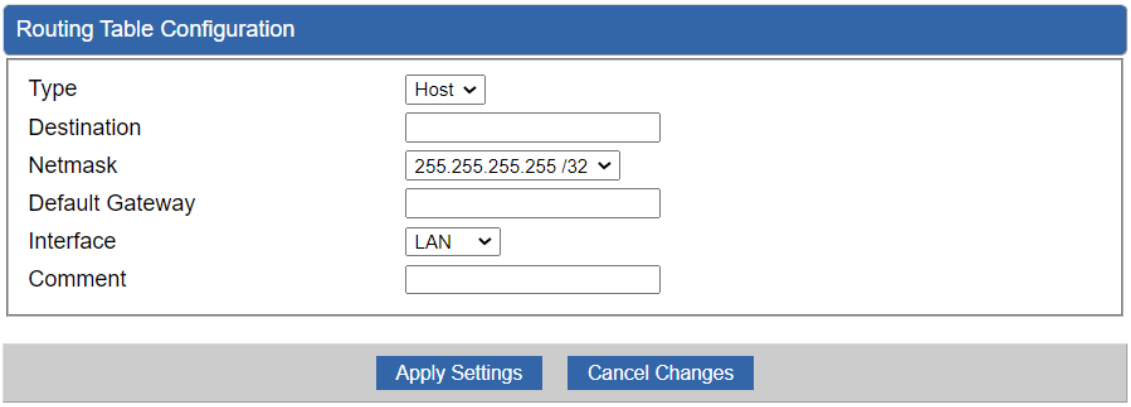


Figure 4-32: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router 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.

4.2.5 RIP

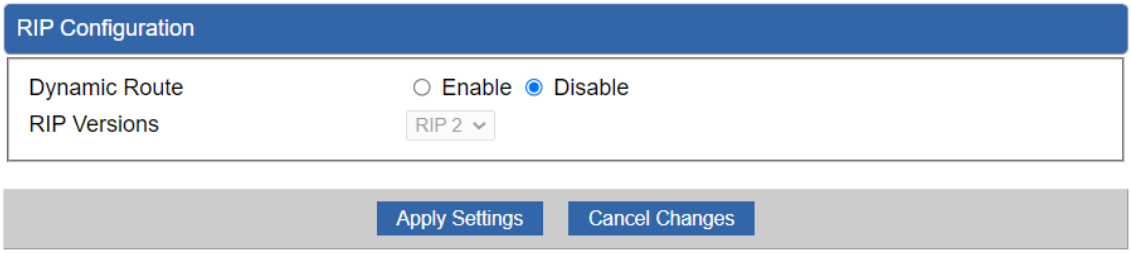


Figure 4-33 RIP

Object	Description
Dynamic Route	Disable or enable the RIP function
RIP Versions	Set RIP Versions

4.2.6 OSPF

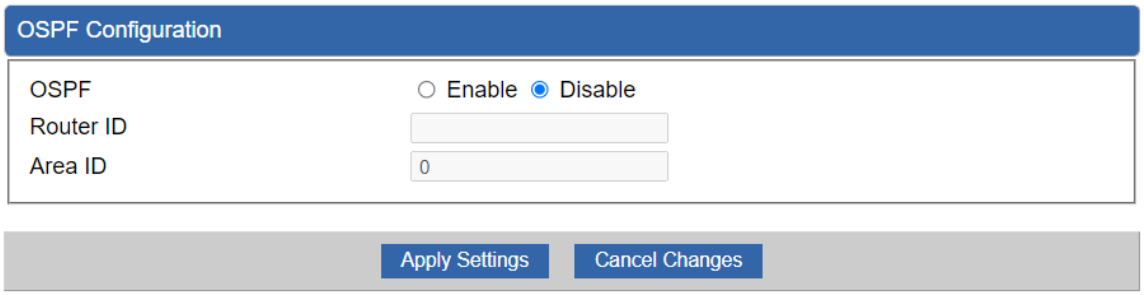


Figure 4-34: OSPF

Object	Description
OSPF	Enable the OSPF function.
Router ID	Set Router ID
Area ID	Set Area ID

4.2.7 IGMP

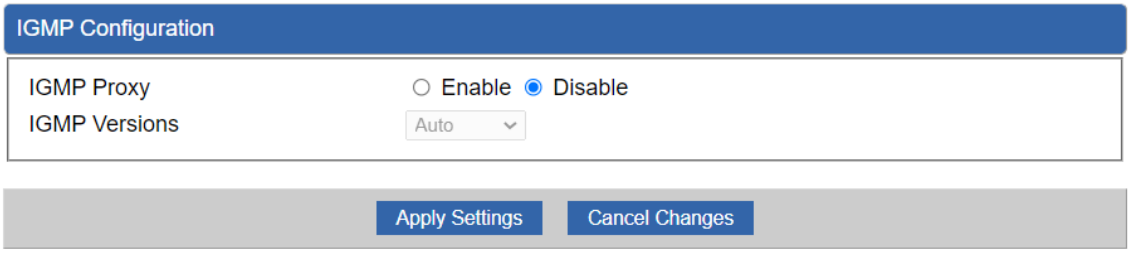


Figure 4-35: IGMP

Object	Description
IGMP	Enable the IGMP function.
IGMP Versions	Select the GMP Versions

4.2.8 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in Figure 4-36. It allows you to enable IPv6 function and set up the parameters of the router's WAN. In this setting you may change WAN connection type and other settings.

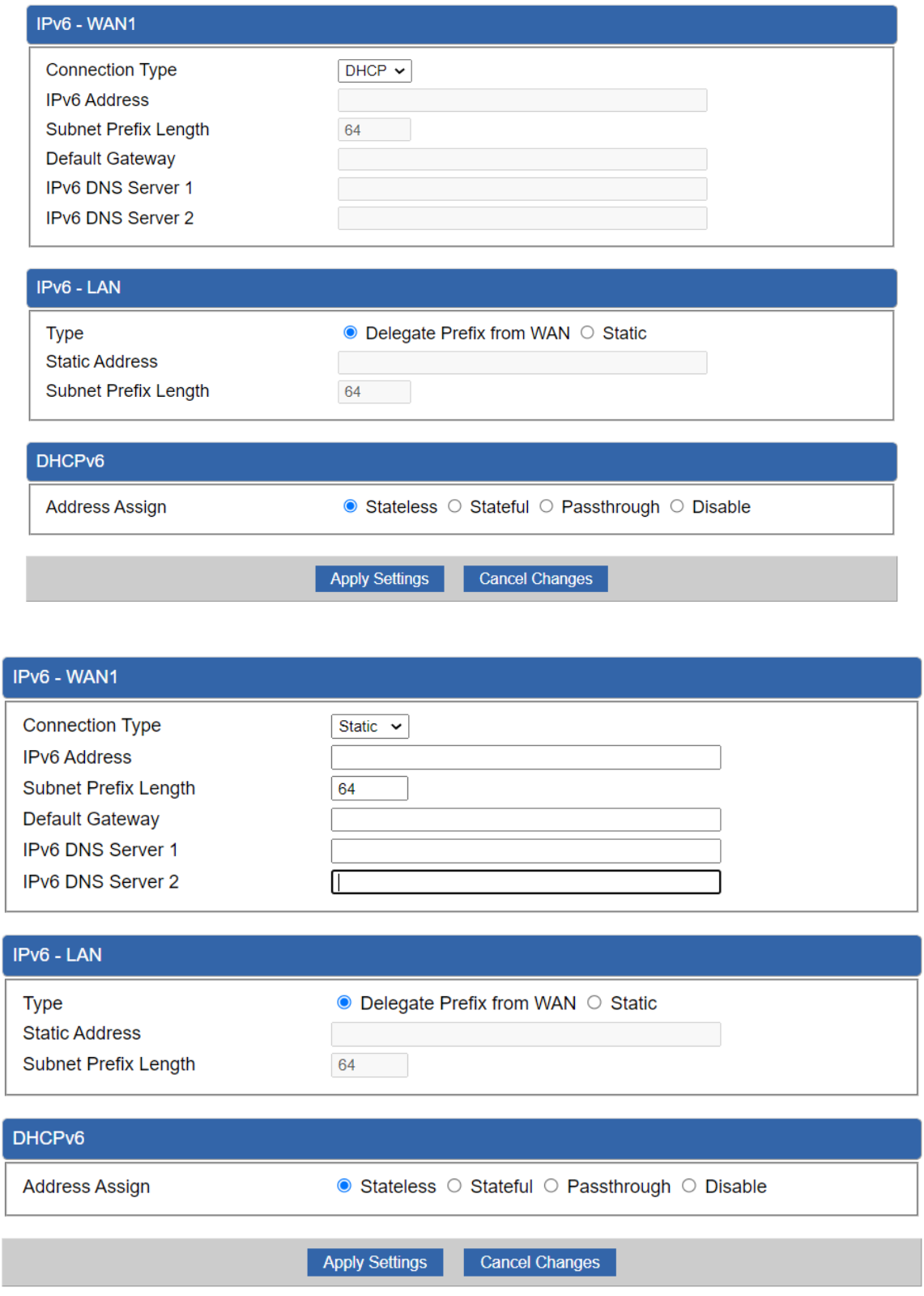


Figure 4-36: IPv6 WAN setup

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.
IPv6 DNS Server 1	Input a specific DNS server
IPv6 DNS Server 2	Input a specific DNS server

4.2.9 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 4-37.

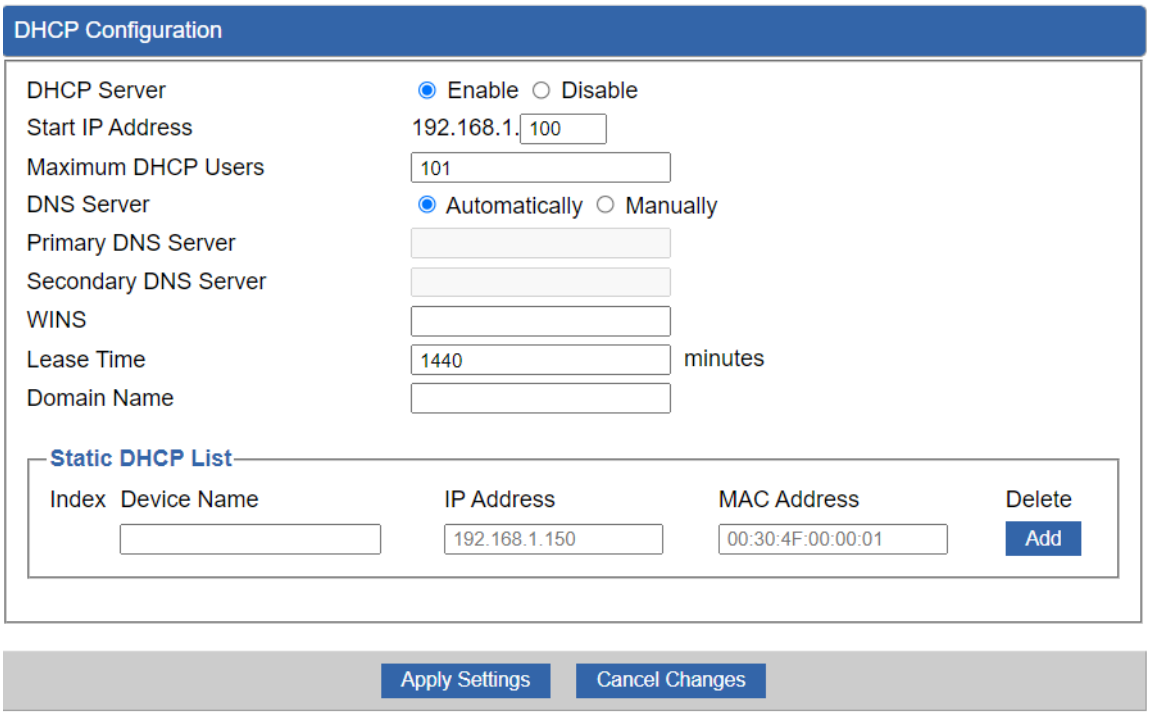


Figure 4-38: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the router 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 router.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the router 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.
DNS Server	By default, it is set as Automatically, and the DNS server is the router's LAN IP address. If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.

Object	Description
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 router. Default is 1440 minutes.
Domain Name	Input a domain name for the router.

4.2.10 DDNS

The router 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 5-35.

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 router, 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 router’s MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

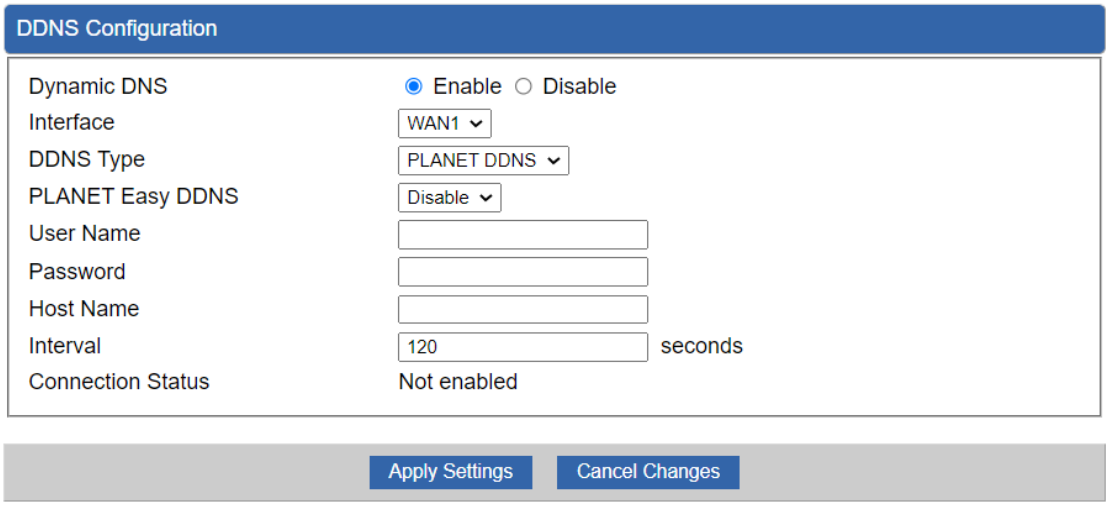


Figure 4-39: PLANET DDNS

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.
Connection Status	Show the connection status of the DDNS function.

4.3 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in Figure 4-40. Please refer to the following sections for the details.

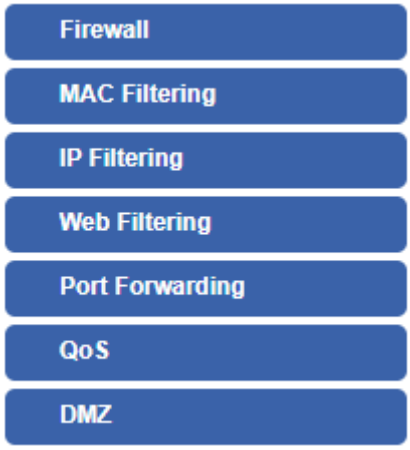


Figure 4-40: Security menu

Object	Description
Firewall	Allows setting DoS (Denial of Service) protection as enable.
MAC Filtering	Allows setting MAC Filtering.
IP Filtering	Allows setting IP Filtering.
Web Filtering	Allows setting Web Filtering.
Port Forwarding	Allows setting Port Forwarding.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.

4.3.1 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 router can prevent specific DoS attacks as shown in Figure 4-41.

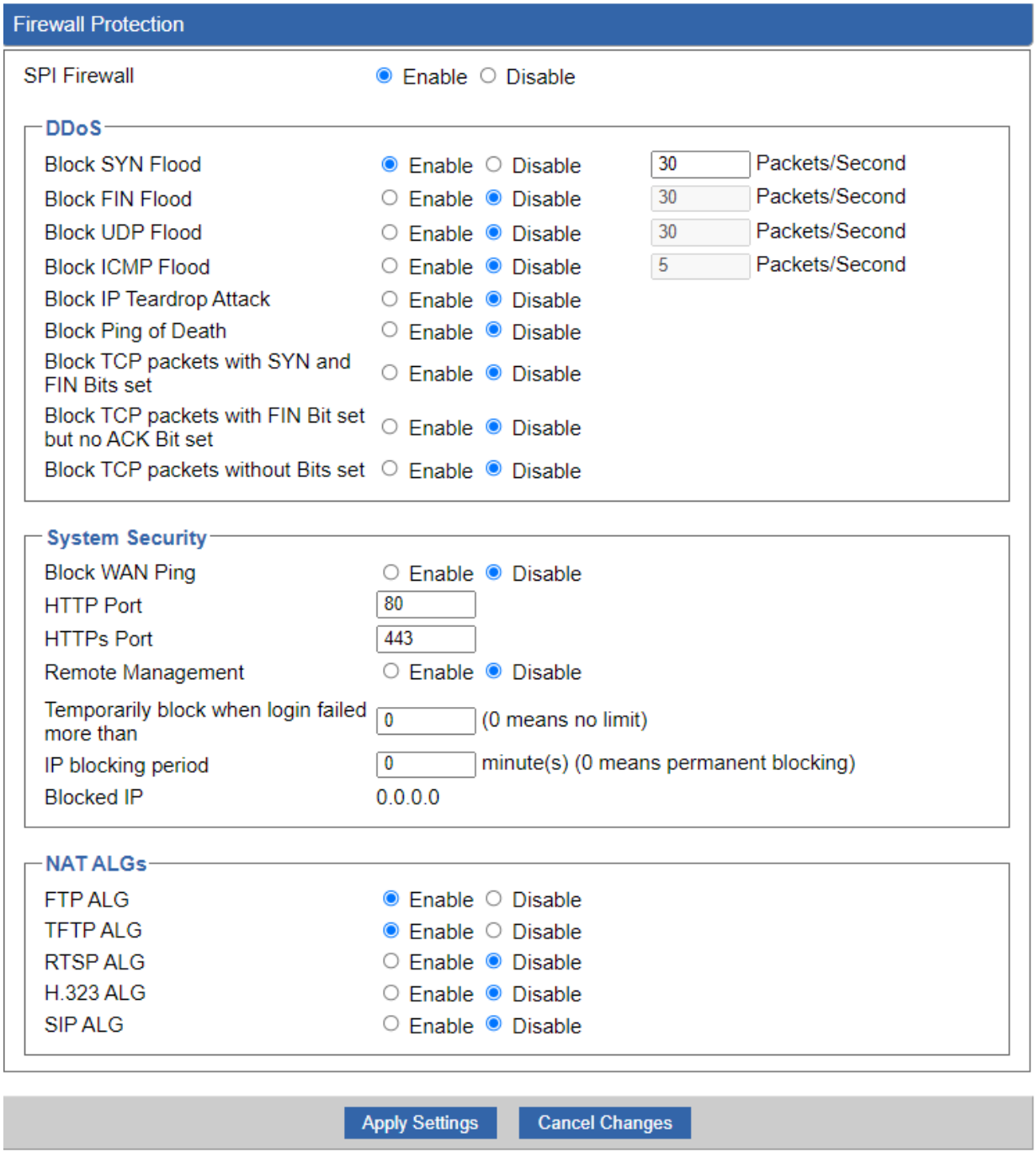


Figure 4-42: Firewall

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 router will start the blocking function immediately. The default configuration is disabled.
Block UDP Flood	If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the router 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 router will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.
Ping Of Death	If the function is enabled, the router 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.
TCP packets with SYN and FIN Bits set	Set the function as enable or disable
TCP packets with FIN Bit set but no ACK Bit set	Set the function as enable or disable
TCP packets without Bits set	Set the function as enable or disable
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
HTTP Port	The default is 80.
HTTPs Port	The default is 443.
Remote Management	Enable the function to allow the web server access of the router from the Internet network. The default configuration is disabled.

Temporarily block when login failed	The default is 0. (0 means no limit)
IP blocking period	The default is 0. (0 means permanent blocking)
Blocked IP	0.0.0.0
FTP ALG	Set the function as enable or disable
TFTP ALG	Set the function as enable or disable
RTSP ALG	Set the function as enable or disable
H.323 ALG	Set the function as enable or disable
SIP ALG	Set the function as enable or disable

4.3.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the router. Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-43.

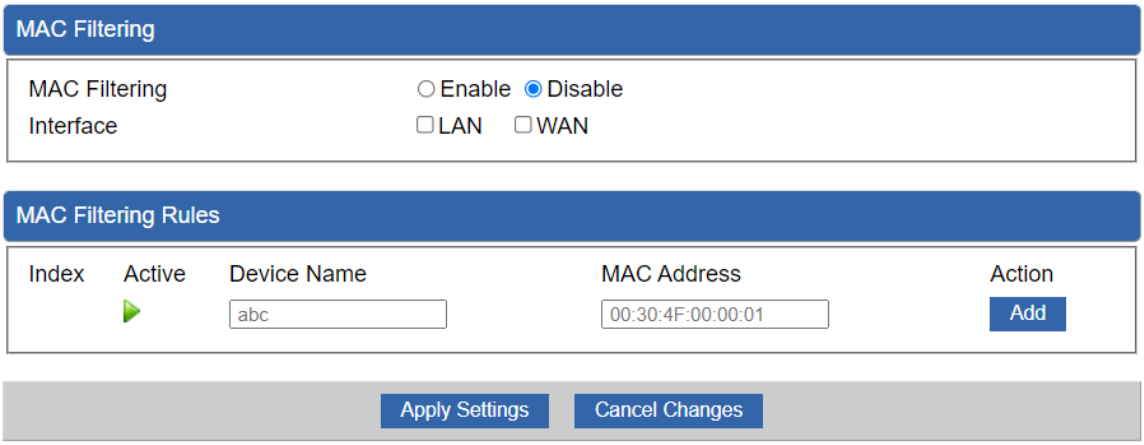


Figure 4-43: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the router 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.

4.3.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in Figure 4-44. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

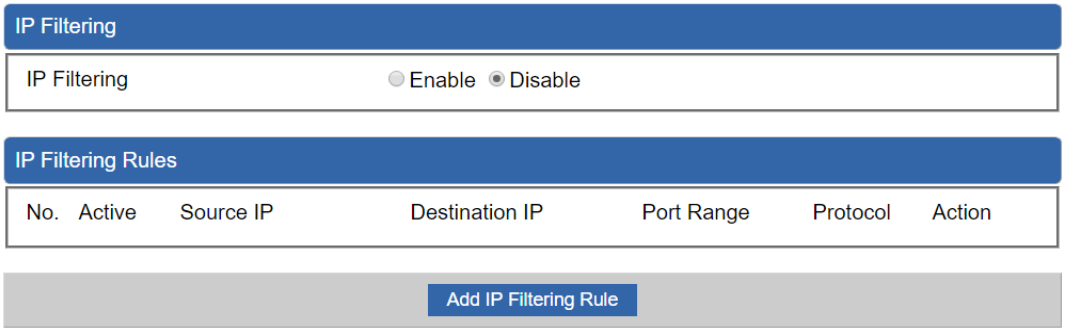


Figure 4-44: IP Filtering

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

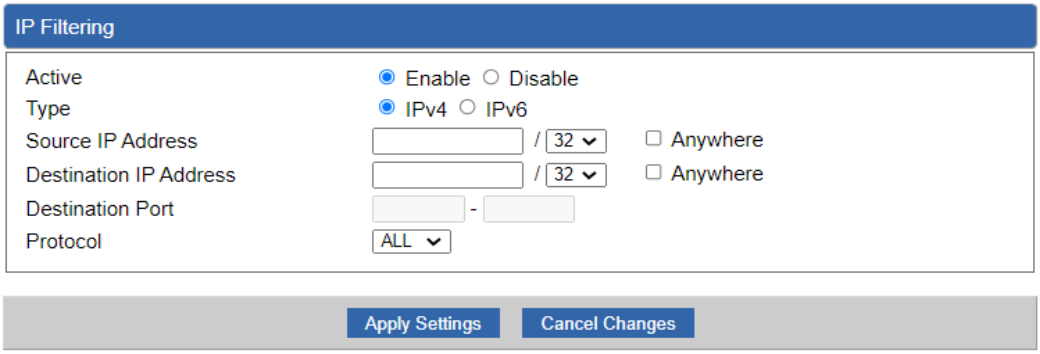


Figure 4-45: IP Filter Rule Setting

Object	Description
Enable	Set the rule as enable or disable.
Type	Set the type as IPv4 or IPv6
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.

Object	Description
	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.

4.3.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-46. Block those URLs which contain keywords listed below.

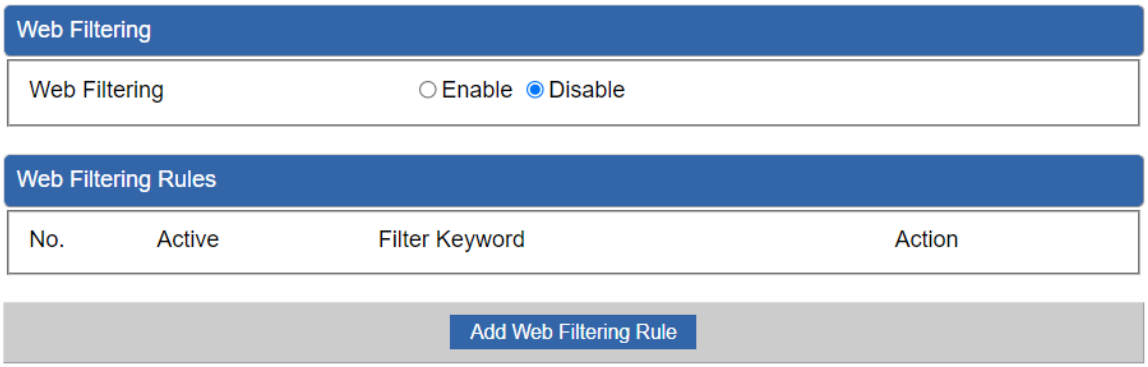


Figure 4-46: Web Filtering

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.

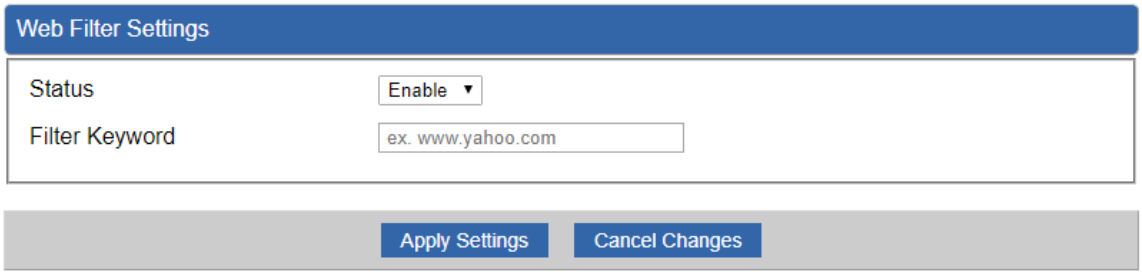


Figure 4-47: Web Filtering Rule Setting

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.

4.3.5 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 4-48. 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 Router's NAT firewall.

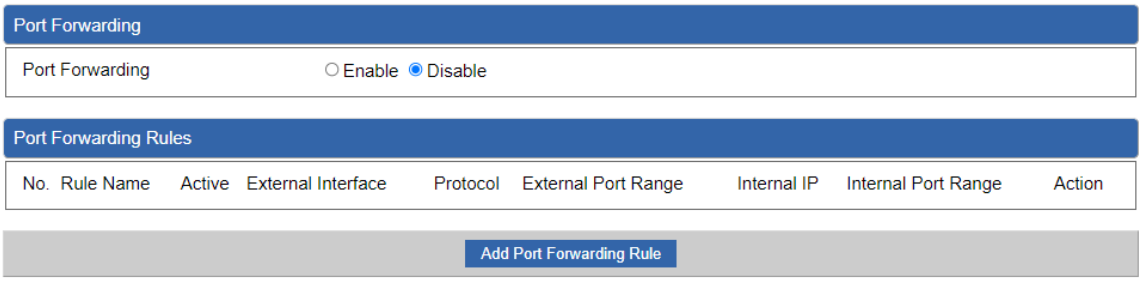


Figure 4-48: Port Forwarding

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

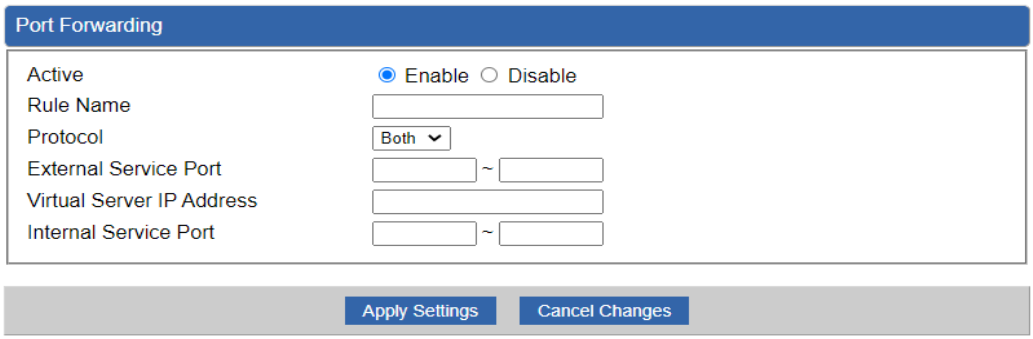


Figure 4-49: Port Forwarding Rule Setting

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

Object	Description
	service. If the service uses a single port number, enter it in both the start and finish fields.

4.3.6 QoS

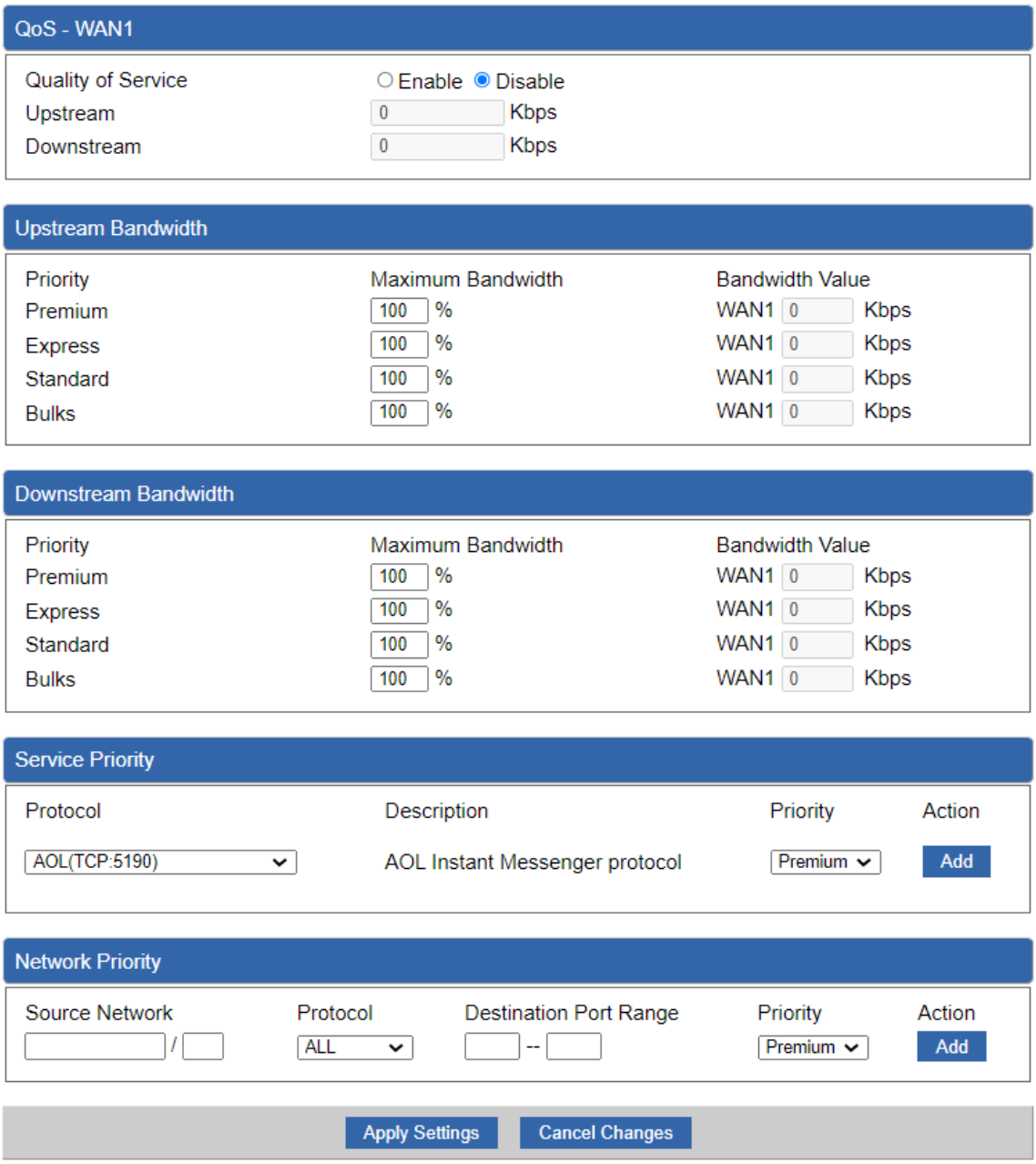


Figure 4-50: QoS Setting

Object	Description
QoS - WAN1	Enable/disable QoS function
Upstream Bandwidth	Setting Upstream Bandwidth
Downstream Bandwidth	Setting Downstream Bandwidth
Service Priority	Setting Service Priority
Network Priority	Setting Network Priority

4.3.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in Figure 4-51. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

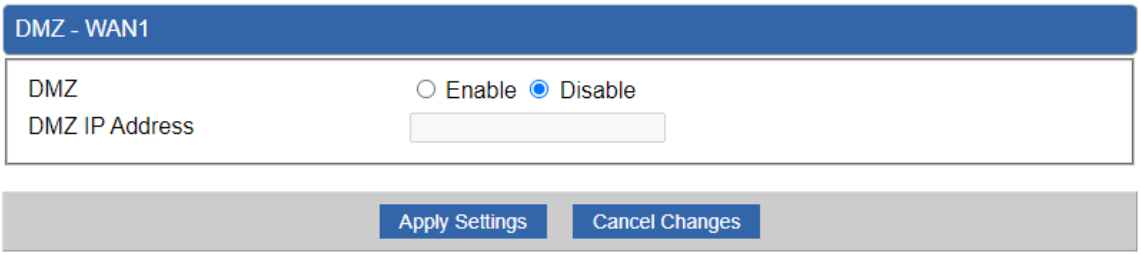


Figure 4-51: DMZ

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.

4.4 Wireless

The Wireless menu provides the following features for managing the system

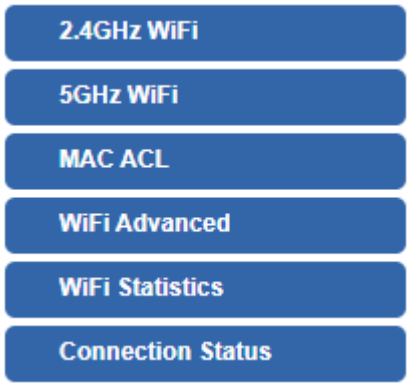
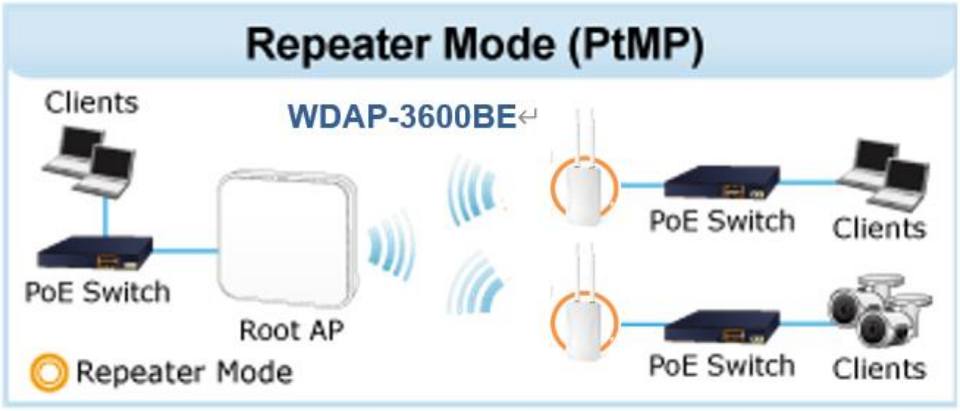


Figure 4-52: Wireless Menu

Object	Description
2.4G Wi-Fi	Allow to configure 2.4G Wi-Fi.
5G Wi-Fi	Allow to configure 5G Wi-Fi.
MAC ACL	Allow configure MAC ACL.
Wi-Fi Advanced	Allow to configure advanced setting of Wi-Fi.
Wi-Fi Statistics	Display the statistics of Wi-Fi traffic.
Connection Status	Display the connection status.

4.4.1 Repeater



This page allows the user to define Repeater

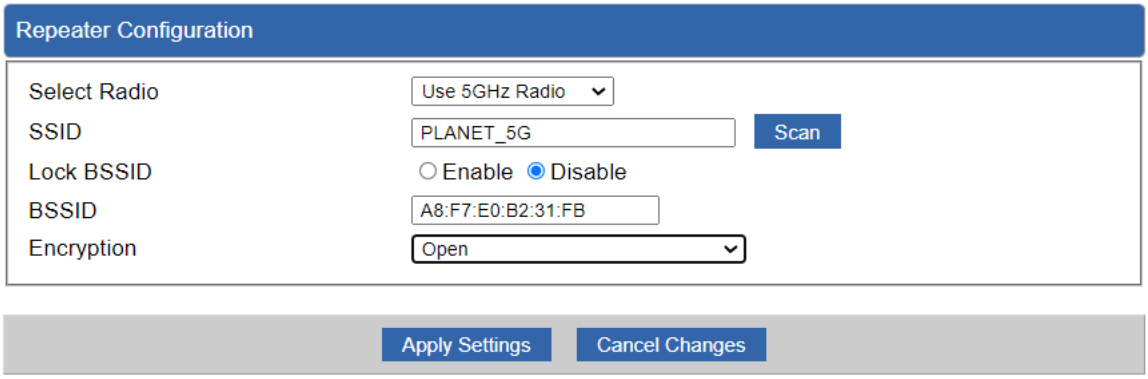


Figure 4-53: Repeater

Object	Description
Select Radio	Select “**2.4GHz**” or “**5GHz**” wireless LAN.
SSID (Wireless Name)	Enter the root AP’s SSID or press “**Scan**” to select.
Lock BSSID	Enable/disable to lock the root AP’s MAC address.
BSSID	The root AP’s MAC address
Encryption	Select the wireless encryption of root AP. The default is “**Open**”

4.4.2 2.4G Wi-Fi

This page allows the user to define 2.4G Wi-Fi.

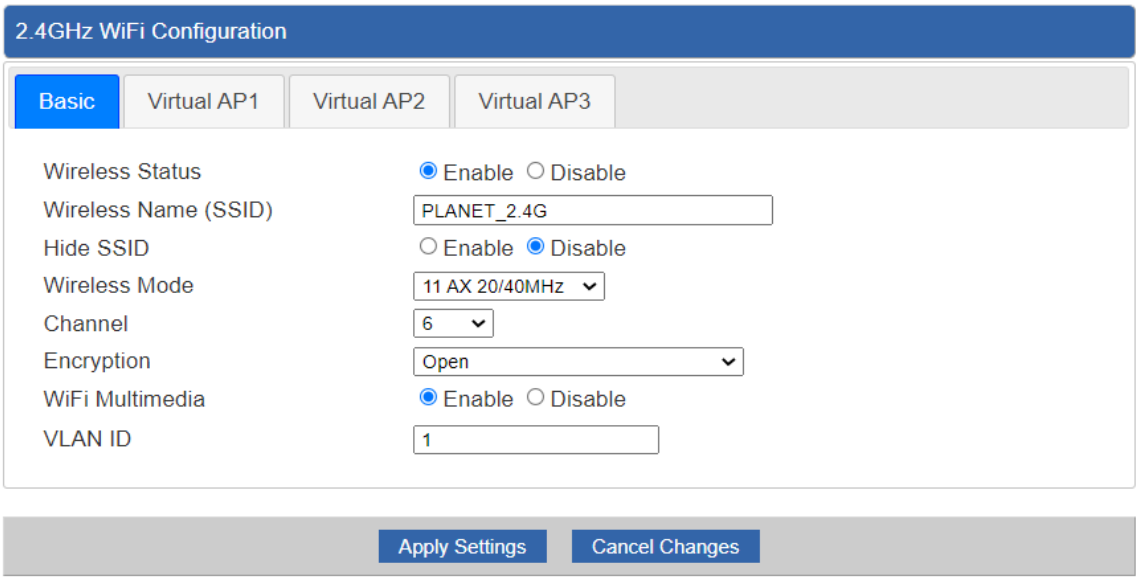


Figure 4-54: 2.4G Wi-Fi

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
Wireless Mode	Select the operating wireless mode
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
VLAN ID	Setting VLAN ID

4.4.3 5G Wi-Fi

This page allows the user to define 5G Wi-Fi.

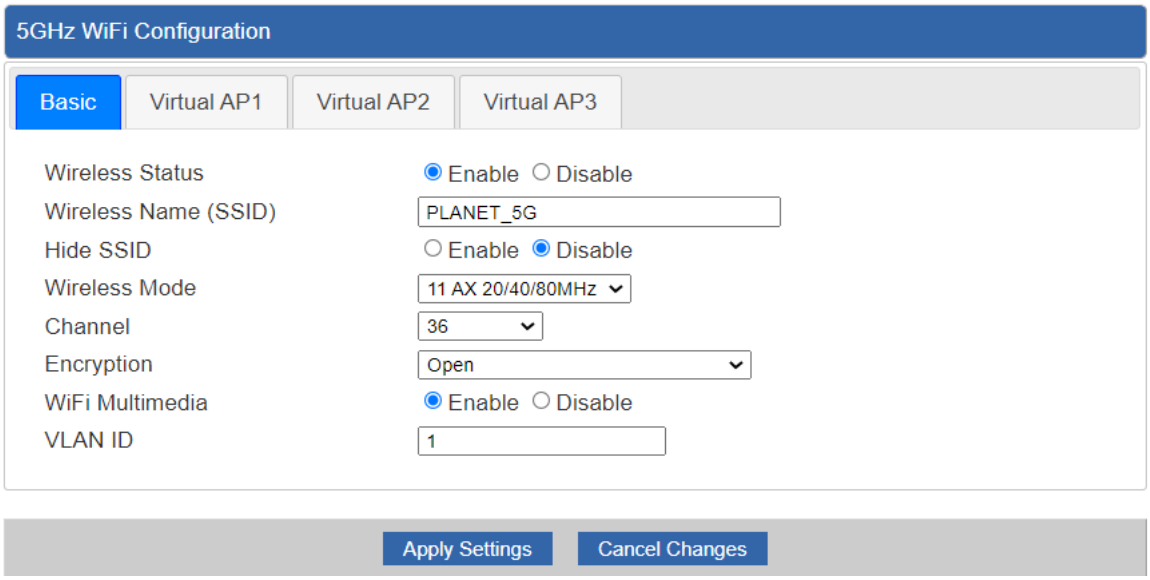


Figure 4-55: 5G Wi-Fi

Object	Description
Wireless Status	Allows user to enable or disable 5G Wi-Fi
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G"
Hide SSID	Allows user to enable or disable SSID
Wireless Mode	Select the operating wireless mode
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
VLAN ID	Setting VLAN ID

4.4.4 MAC ACL

This page allows the user to define MAC ACL.

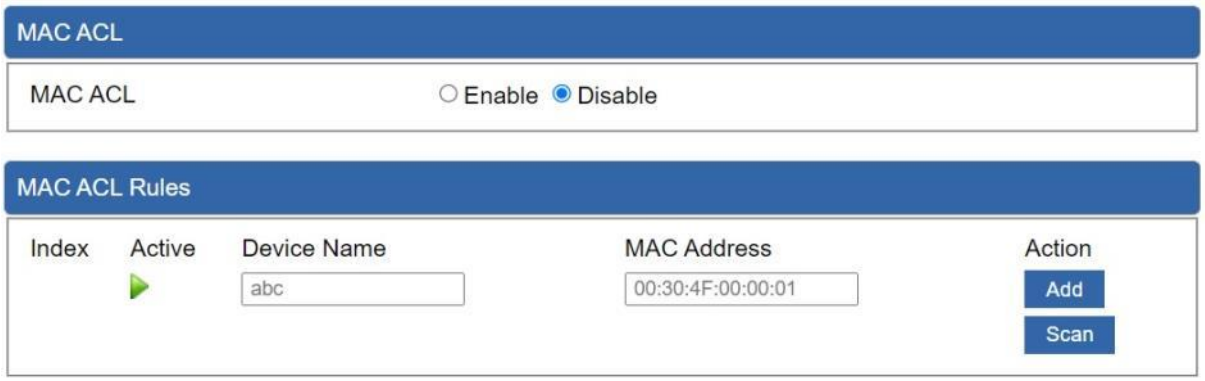


Figure 4-57: MAC ACL

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

4.4.5 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi.

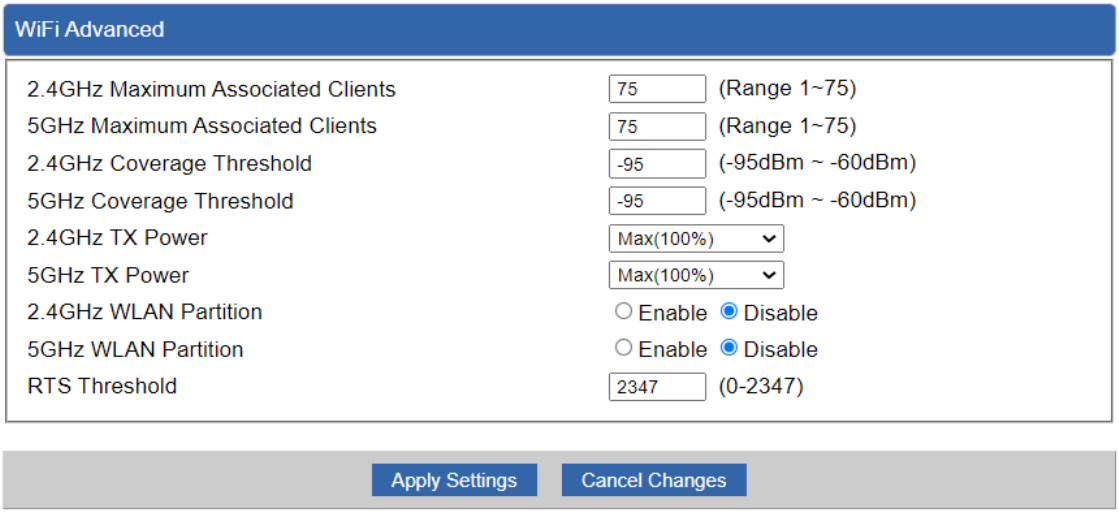


Figure 4-58: Wi-Fi Advanced

Object	Description
2.4GHz Maximum Associated Clients	The maximum users are 75
5GHz Maximum Associated Clients	The maximum users are 75
2.4G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -95dBm
5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -95dBm
2.4G TX Power	The range of transmit power is **Max (100%)**, **Efficient (75%)**, **Enhanced (50%), Standard (25%)** or **Min (15%)**. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power
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
2.4GHz WLAN Partition	Set the function as enable or disable
5GHz WLAN Partition	Set the function as enable or disable
RTS Threshold	Enable or Disable RTS/CTS protocol. It can be used in the following scenarios and used by Stations or Wireless AP.

	1) When medium is too noisy or lots of interferences are present. If the AP/Station cannot get a chance to send a packet, the RTS/CTS mechanism can be initiated to get the packet sent. 2) In mixed mode, the hidden node problem can be avoided. The default value is **2347**

4.4.6 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

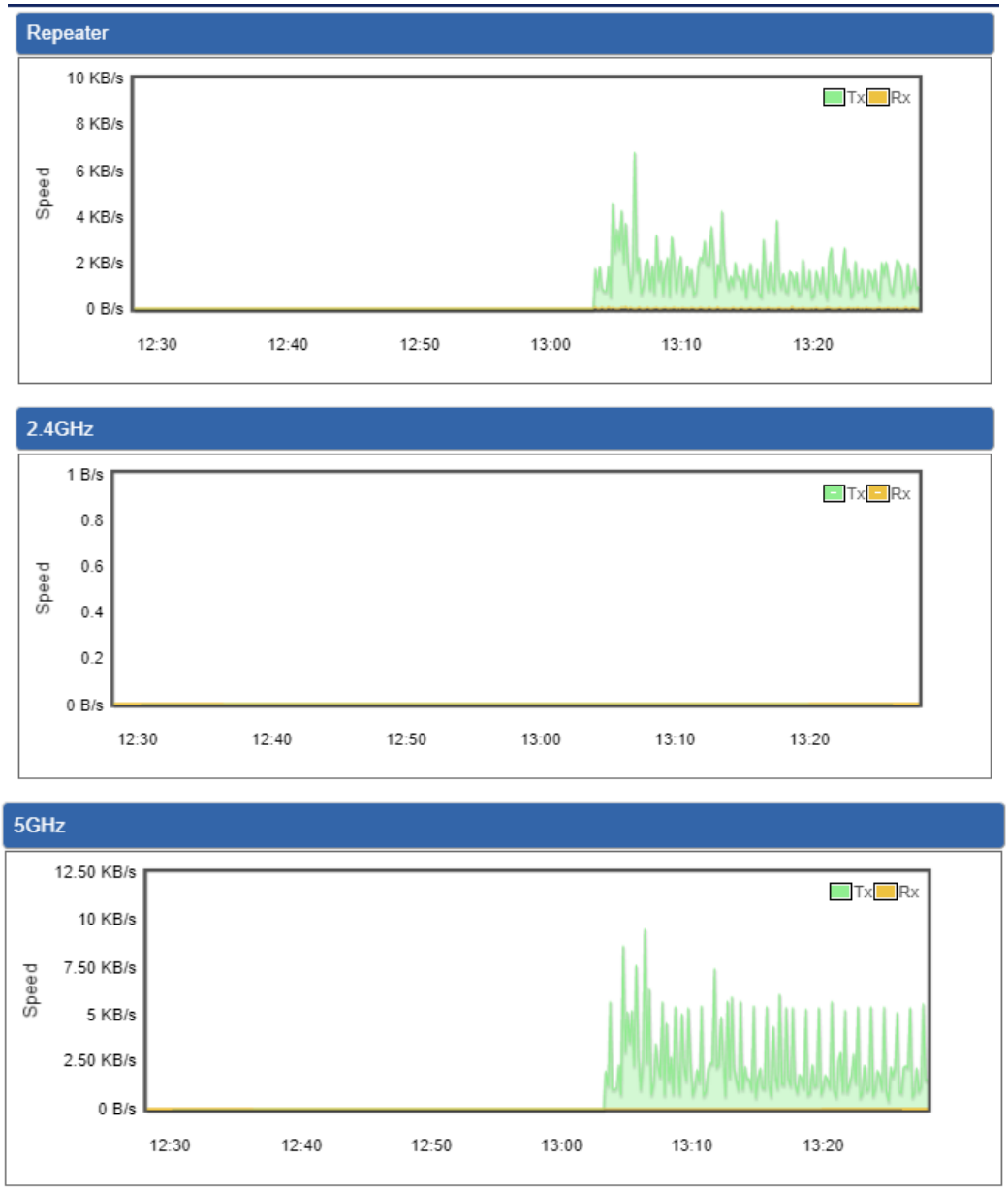


Figure 4-59: Wi-Fi Statistics

4.4.7 Connection Status

This page shows the host names and MAC address of all the clients in your network

Figure 4-60: 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.

4.5 Maintenance

The Maintenance menu provides the following features for managing the system

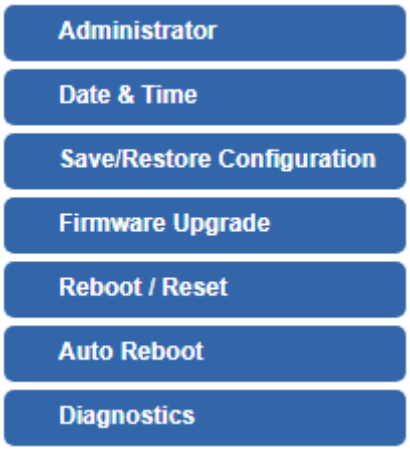


Figure 4-61: Maintenance

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the router's configuration to local or USB sticker. Restore the router'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.

4.5.1 Administrator

To ensure the router's security is secure, you will be asked for your password when you access the router'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 4-62.

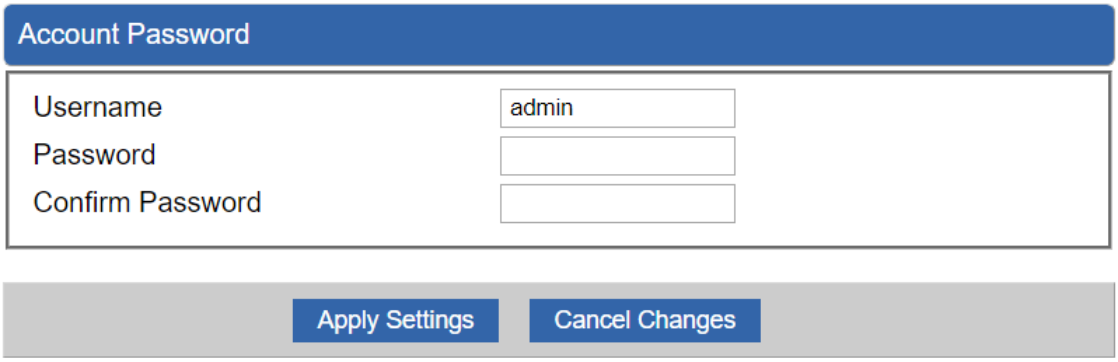


Figure 4-62: Administrator

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

4.5.2 Date and Time

This section assists you in setting the system time of the router. 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 4-63.

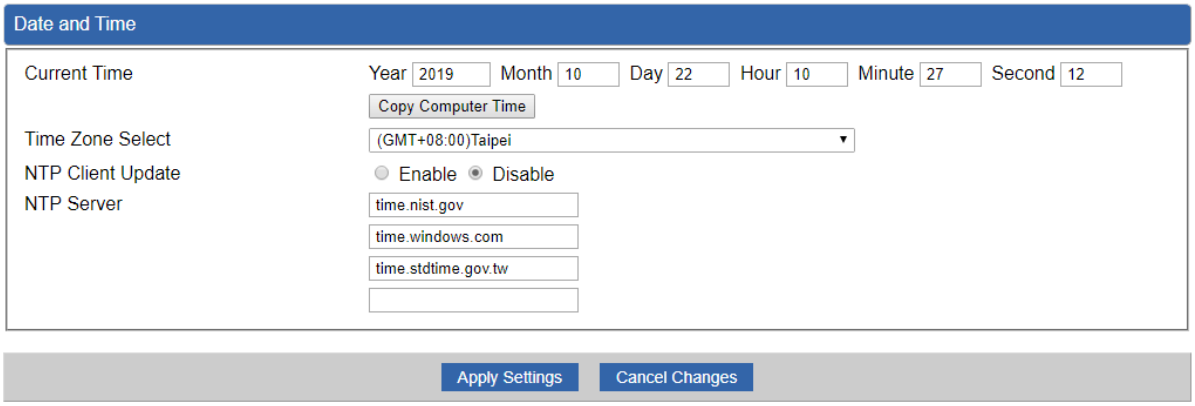


Figure 4-63: Date and Time

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

4.5.3 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 4-64 is shown below:

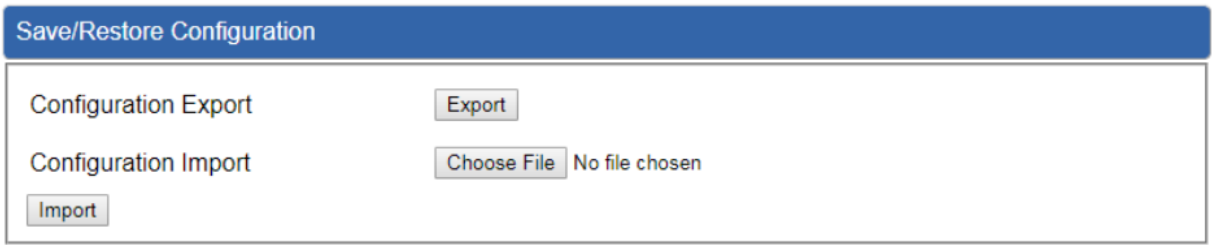


Figure 4-64: Save/Restore Configuration

■ Save Setting to PC

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

4.5.4 Firmware Upgrading

This page provides the firmware upgrade of the router as shown in Figure 4-65.

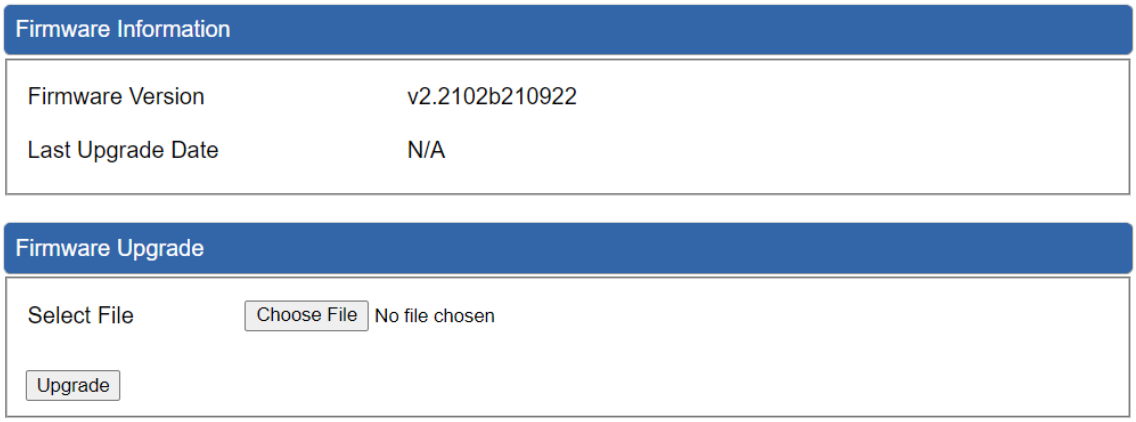


Figure 4-65: Firmware upgrade

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

4.5.5 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 4-66 is shown below:

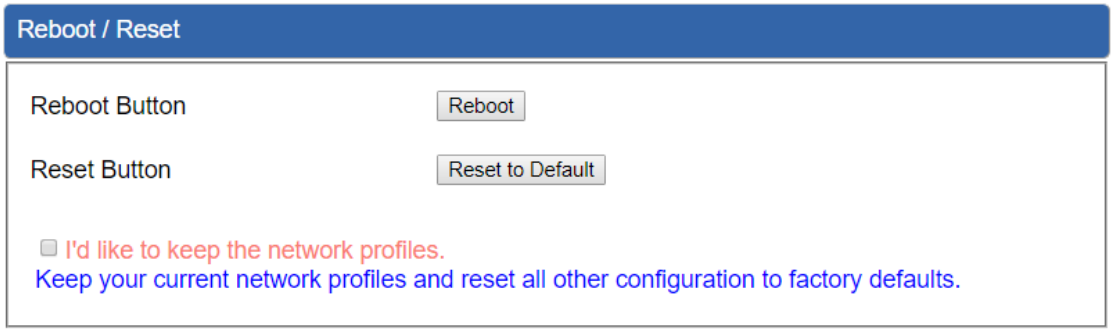


Figure 4-66: Reboot/Reset

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

4.5.6 Auto Reboot

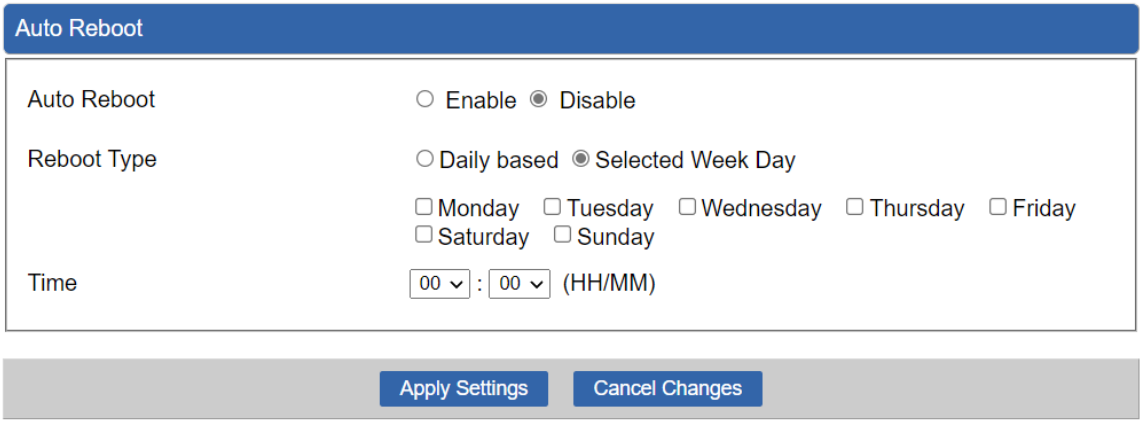


Figure 4-67: Auto Reboot

Object	Description
Auto Reboot	Disable or enable the Auto Reboot function.
Reboot Type	Set the function type.
Time	Select reboot time for clock

4.5.7 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “Ping”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping is shown in Figure 4-68.

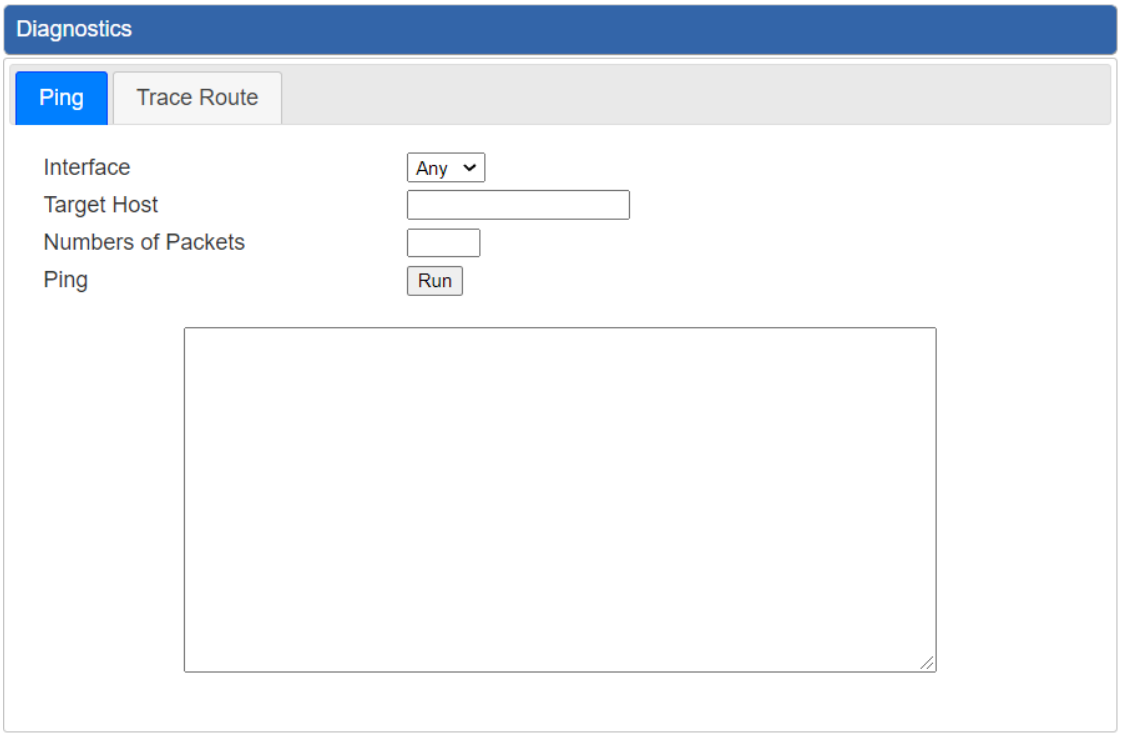


Figure 4-68: Ping

Object	Description
Interface	Select an interface of the router.
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.

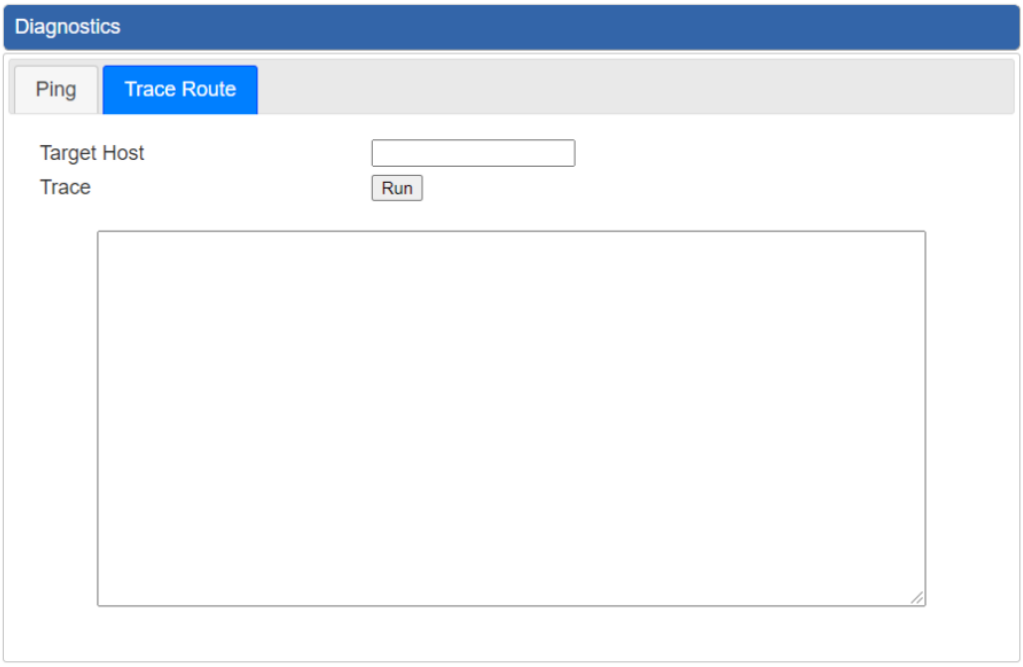


Figure 4-69: Trace Route

Object	Description
Target Host	The destination IP Address or domain.
Trace	The time of ping.

Note

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

Chapter 5. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WDAP-3600BE is configured to "**default**".

5.1 Windows 7/8/10/11 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

Step 1: Right-click on the **network icon** displayed in the system tray

Figure 5-1 Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [**default**]

(2) Click the [**Connect**] button

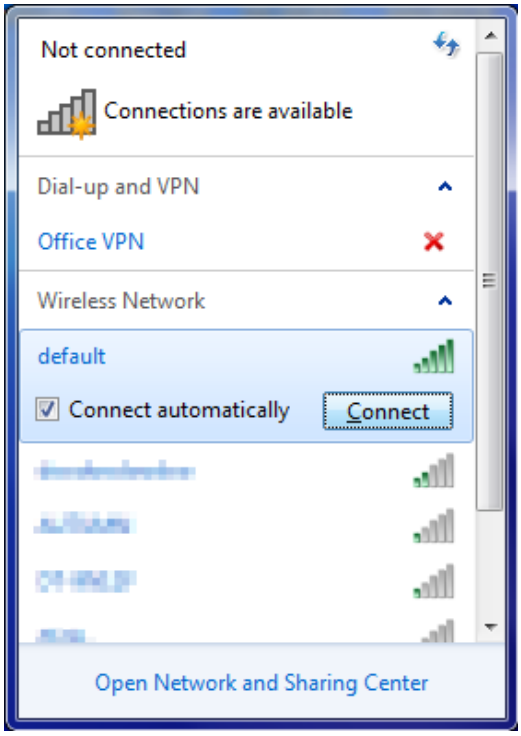


Figure 5-2 WLAN AutoConfig

Note

If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

Step 3: Enter the **encryption key** of the wireless AP

(1) The Connect to a Network box will appear.

(2) Enter the encryption key that is configured in section 5.7.2.1

(3) Click the [OK] button.

Figure 5-3 Typing the Network Key

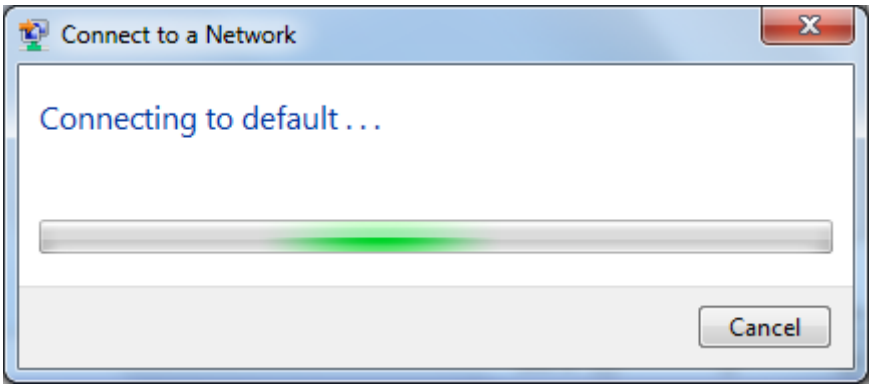


Figure 5-4 Connecting to a Network

Step 4: Check if "**Connected**" is displayed.

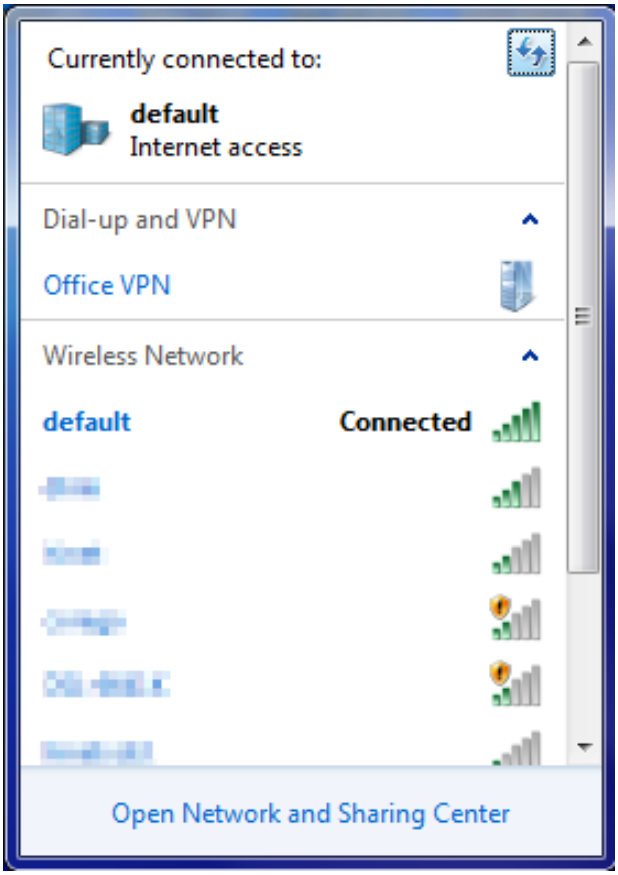


Figure 5-5 Connected to a Network

5.2 Mac OS X 10.x

In the following sections, the default SSID of the WDAP series is configured to “default”.

Step 1: Right-click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear.

Figure 5-6 Mac OS – Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [**default**].

(2) Double-click on the selected SSID.

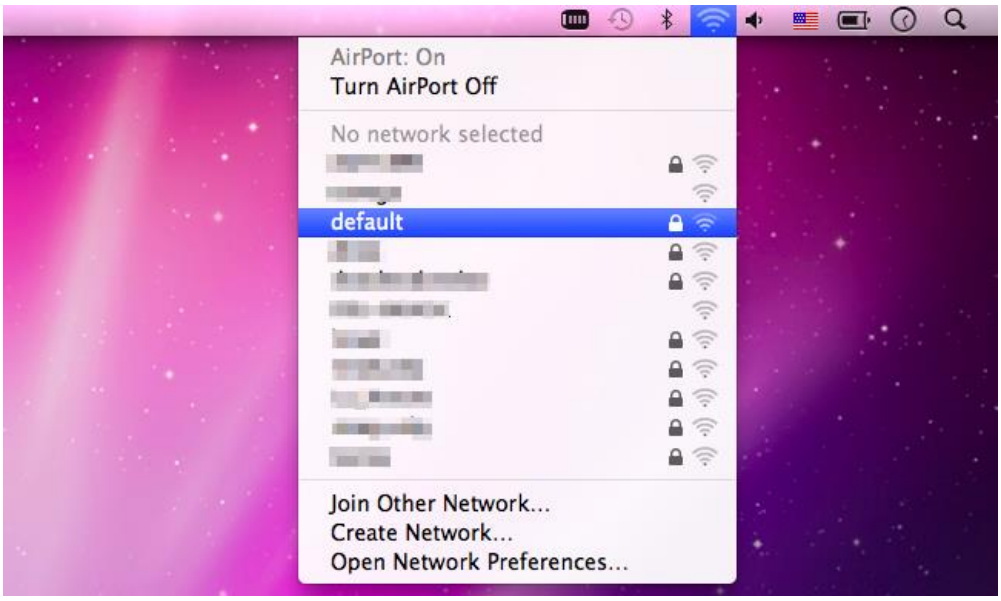


Figure 5-7 Highlighting and Selecting the Wireless Network

Step 3: Enter the **encryption key** of the wireless AP

(1) Enter the encryption key that is configured in section 5.7.2.1

(2) Click the [OK] button.

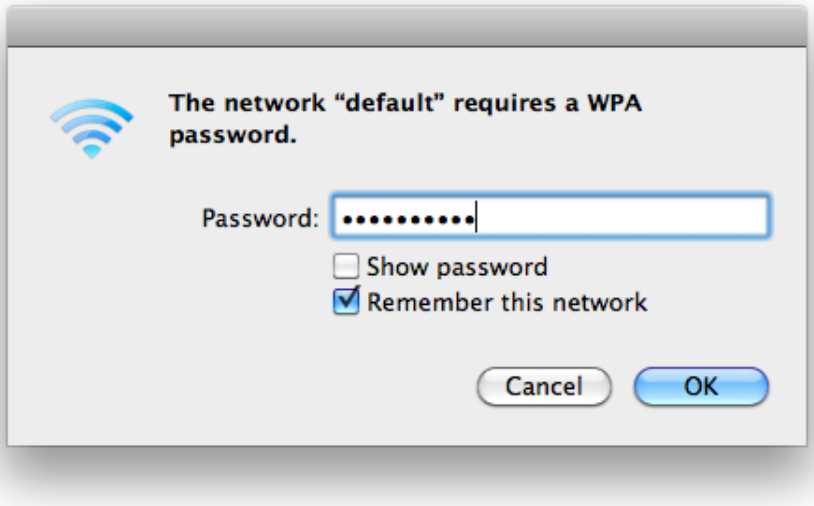


Figure 5-8 Enter the Password

Note

If you will be connecting to this Wireless AP in the future, check [**Remember this network**].

Step 4: Check if the AirPort is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in front of the SSID.

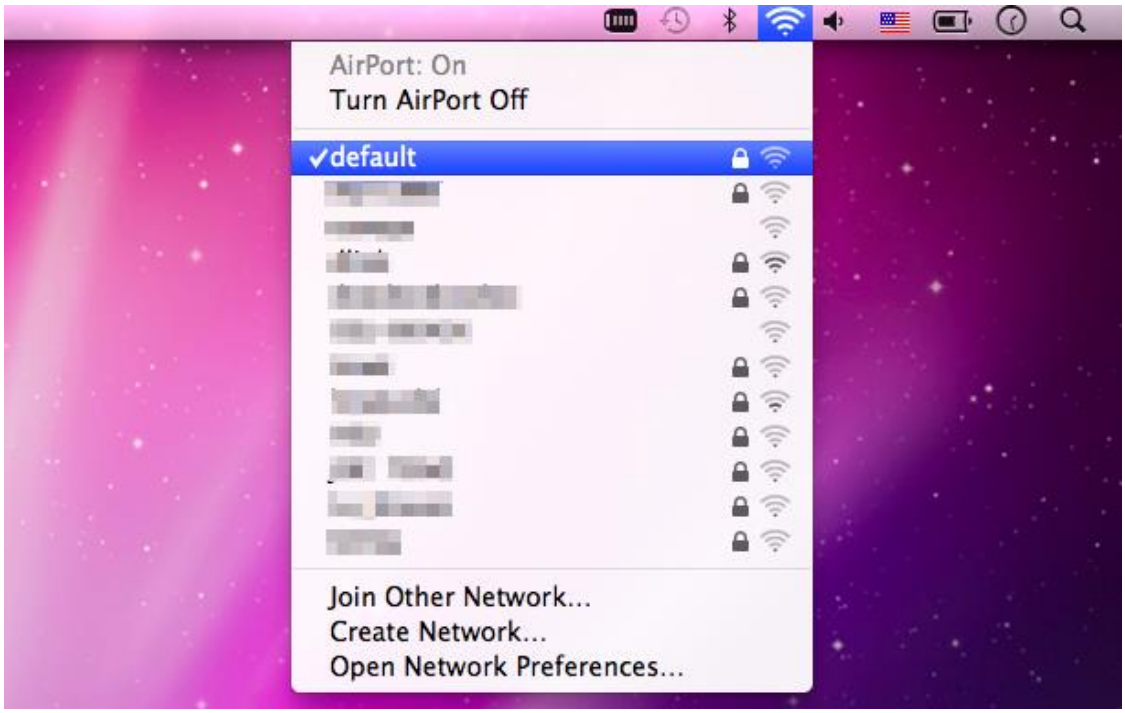


Figure 5-9 Connected to the Network

There is another way to configure the MAC OS X wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

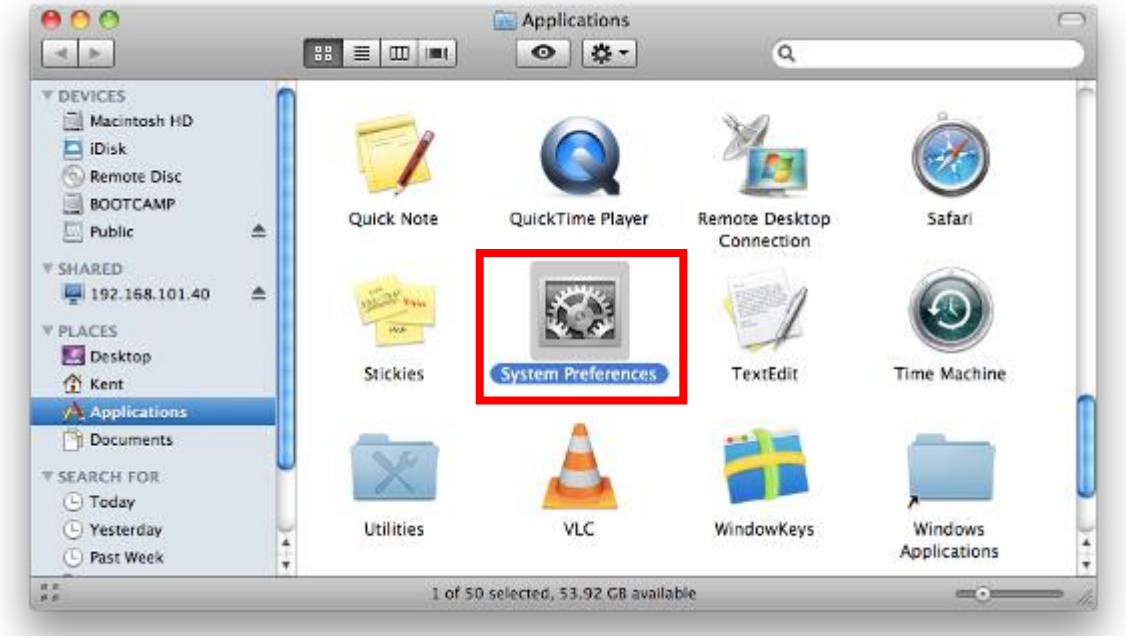


Figure 5-10 System Preferences

Step 2: Open **Network Preference** by clicking on the [**Network**] icon

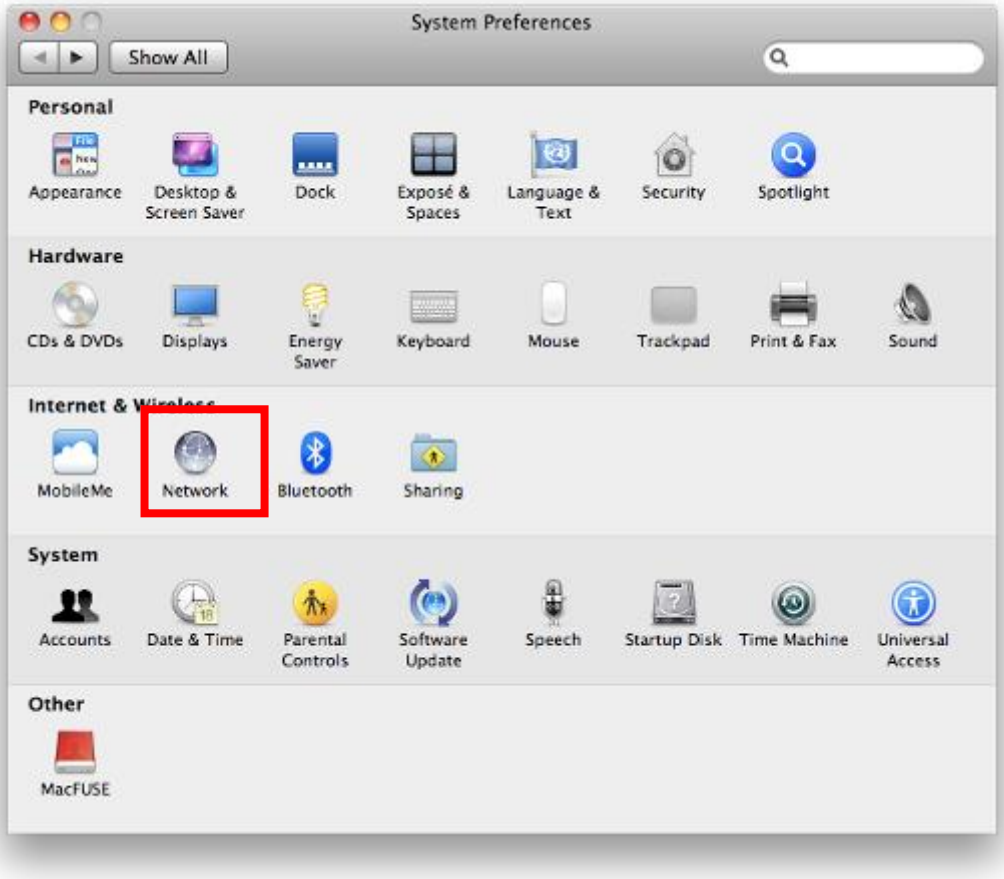


Figure 5-11 System Preferences -- Network

Step 3: Check Wi-Fi setting and select the available wireless network

(1) Choose the **AirPort** on the left menu (make sure it is ON)

(2) Select Network Name [**default**] here

If this is the first time to connect to the Wireless AP, it should show “No network selected”.

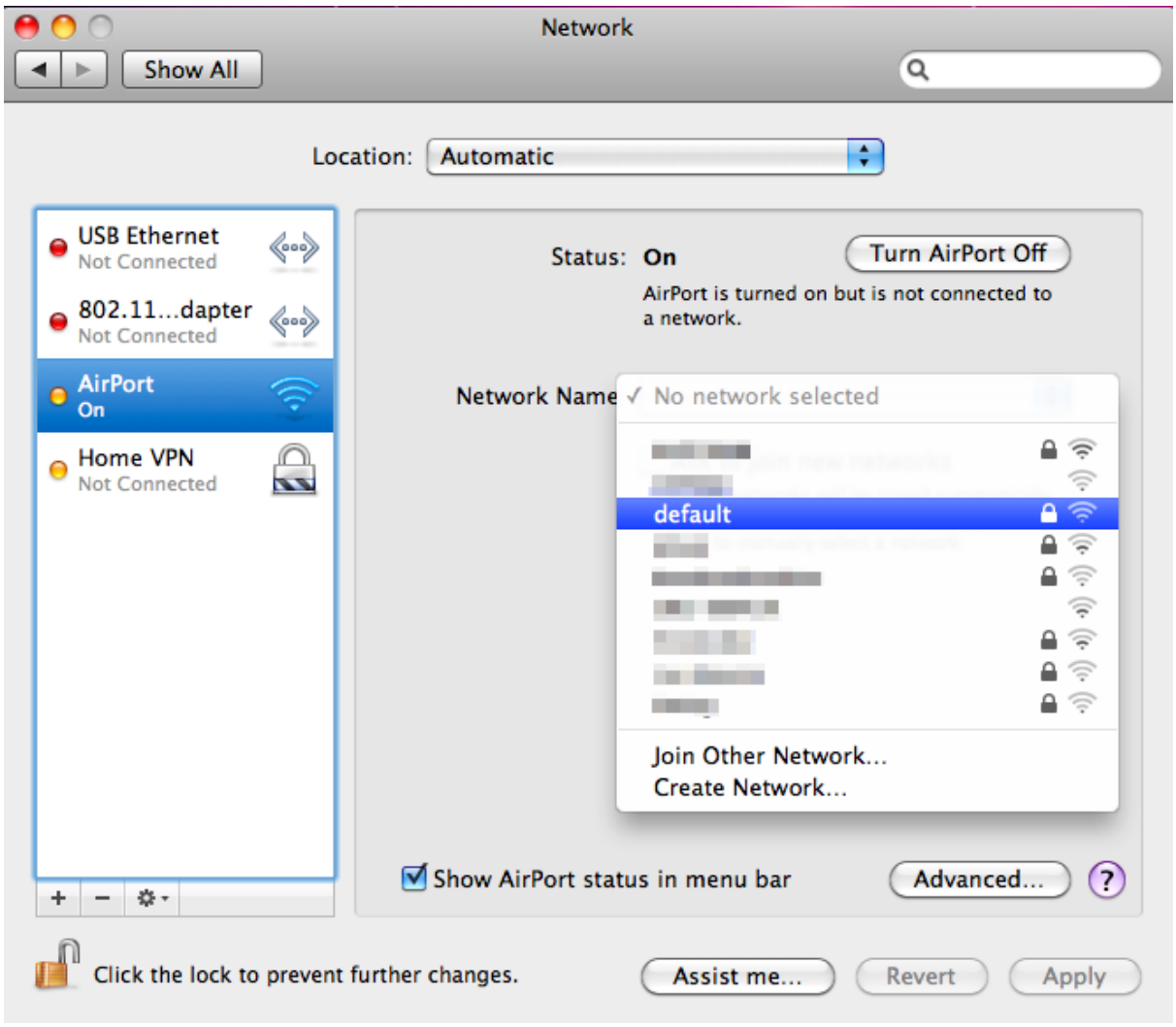


Figure 5-12 Selecting the Wireless Network

5.3 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the WDAP series is configured to "**default**".

Step 1: Tap the [**Settings**] icon displayed in the home screen

Figure 5-13 iPhone – Settings icon

Step 2: Check Wi-Fi setting and select the available wireless network

(1) Tap [**General**] \ [**Network**]

(2) Tap [**Wi-Fi**]

If this is the first time to connect to the Wireless AP, it should show "Not Connected".

Figure 5-14 Wi-Fi Setting

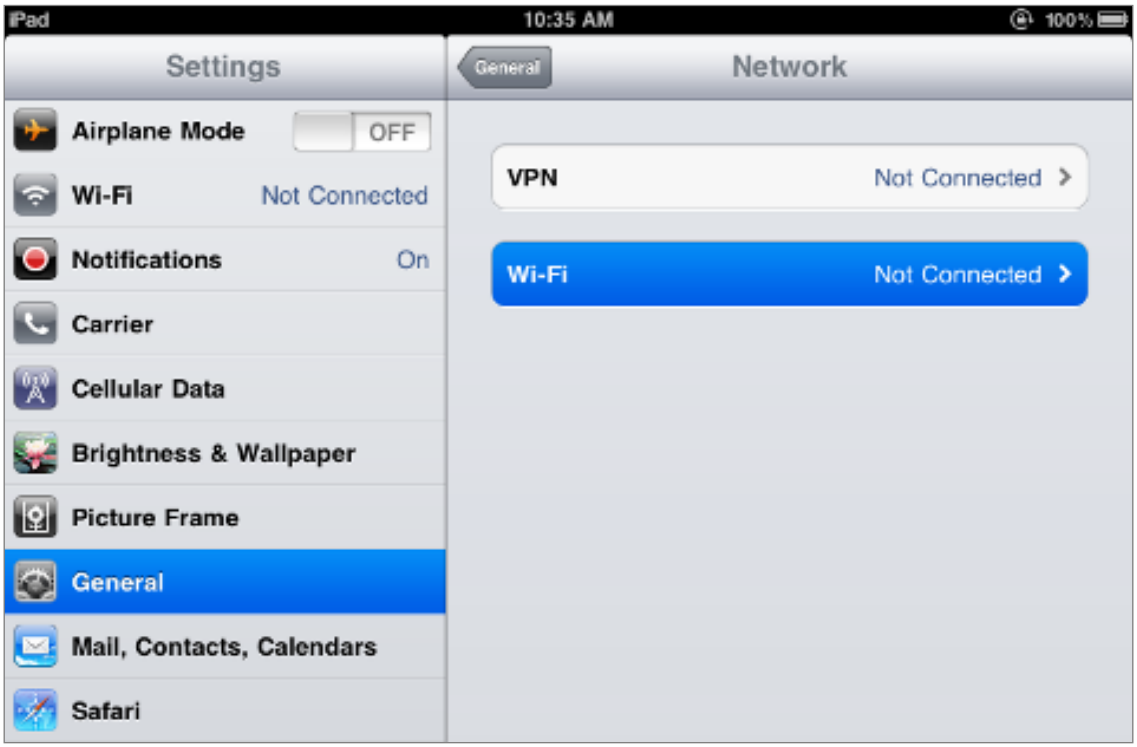


Figure 5-15 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [**default**]

Figure 5-16 Turning on Wi-Fi

Step 4: Enter the **encryption key** of the Wireless AP

(1) The password input screen will be displayed.

(2) Enter the encryption key that is configured in section 5.7.2.1

(3) Tap the [**Join**] button.

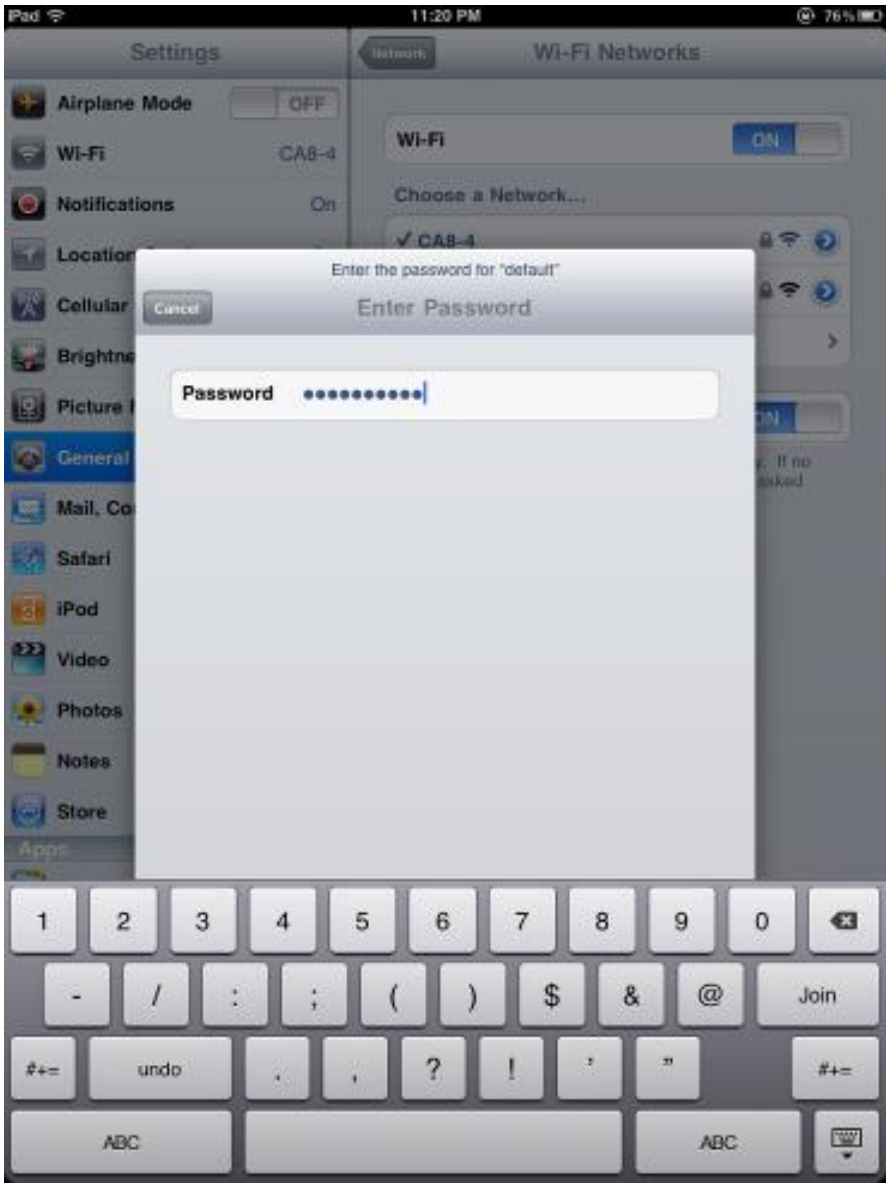


Figure 5-17 iPhone -- Entering the Password

Step 5: Check if the device is connected to the selected wireless network.

If “Yes”, then there will be a “check” symbol in front of the SSID.

Figure 5-18 iPhone -- Connected to the Network

Appendix A: DDNS Application

Configur**ing 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

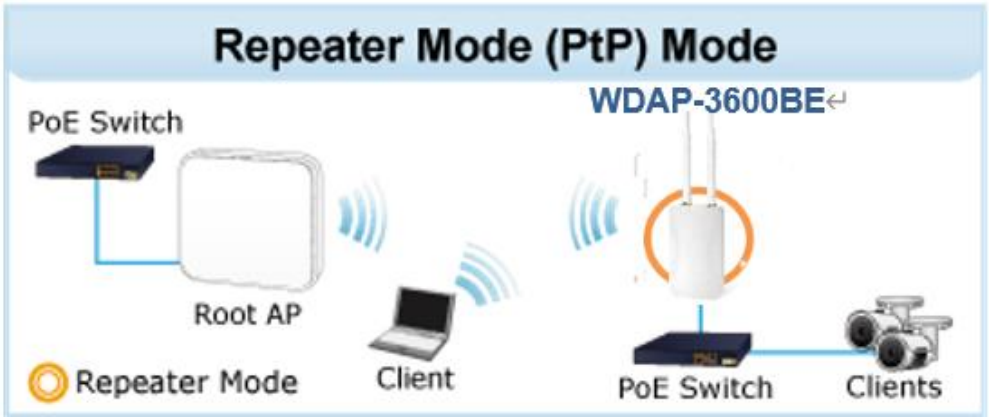
Step 2: Enable DDNS option through accessing web page of the device.

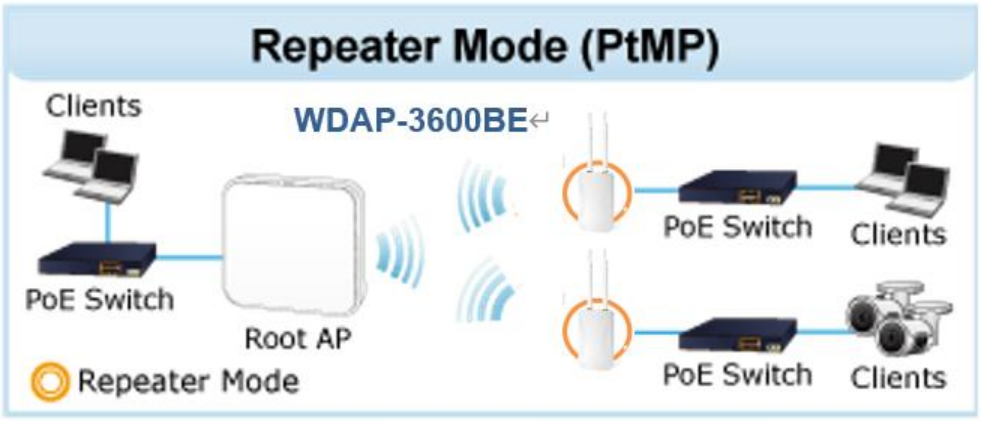
Step 3: Input all DDNS settings.

Appendix B: FAQs

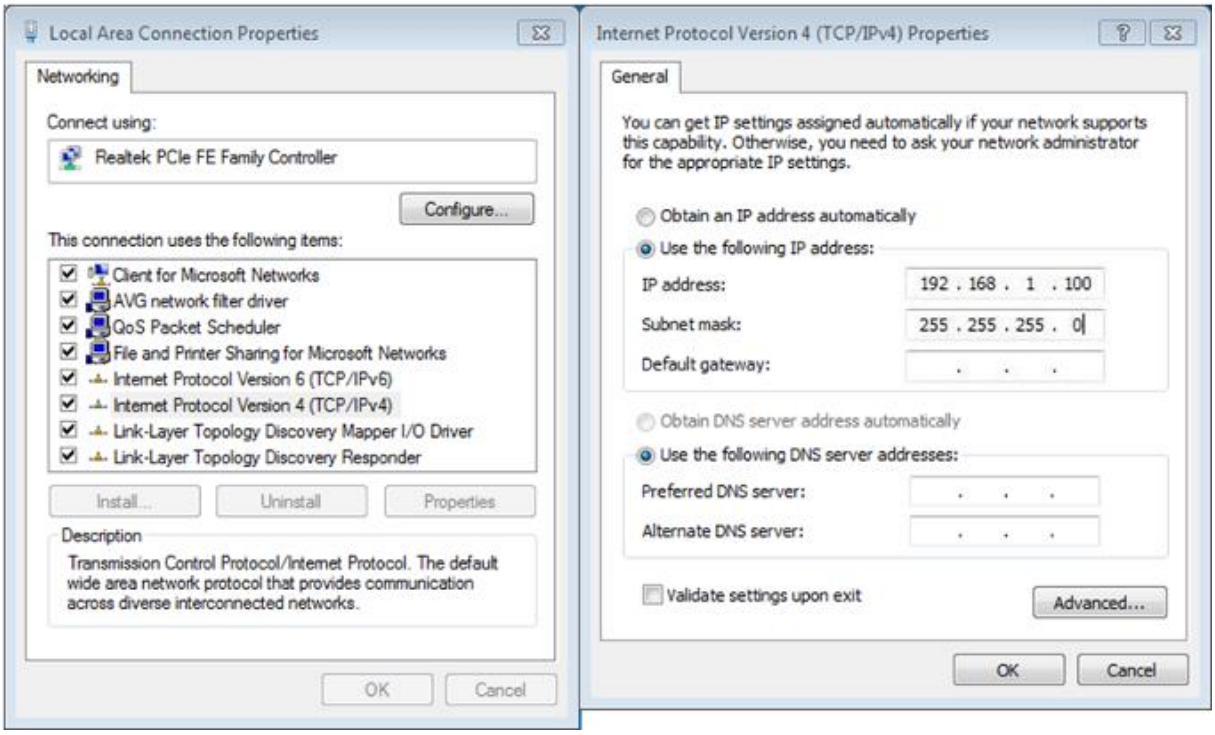
How to Set Up the AP Client Connection

Topology (The topology below uses the WDAP-3600BE as an example):

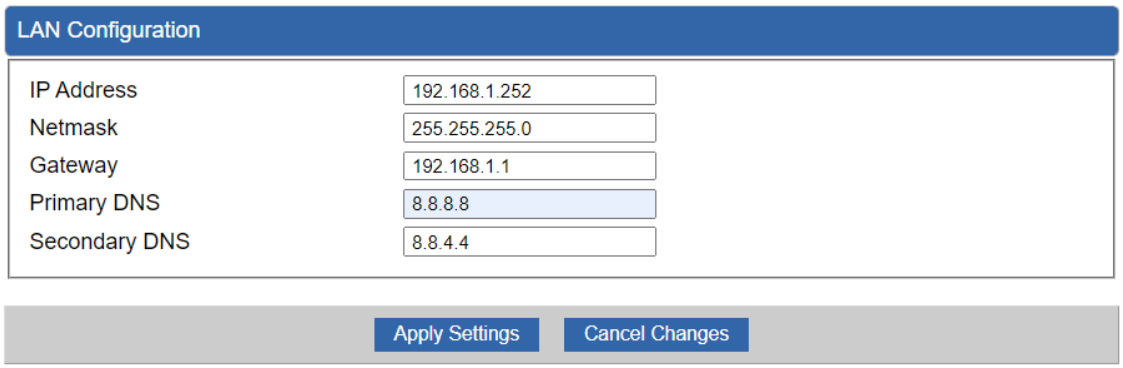




Step 1. Use static IP in the PCs that are connected with AP-1(Site-1) and AP-2(Site-2). In this case, Site-1 is "**192.168.1.100**", and Site-2 is "**192.168.1.200**".



Step 2. In AP-2, change the default IP to the same IP range but different from AP-1. In this case, the IP is changed to **192.168.1.252**.

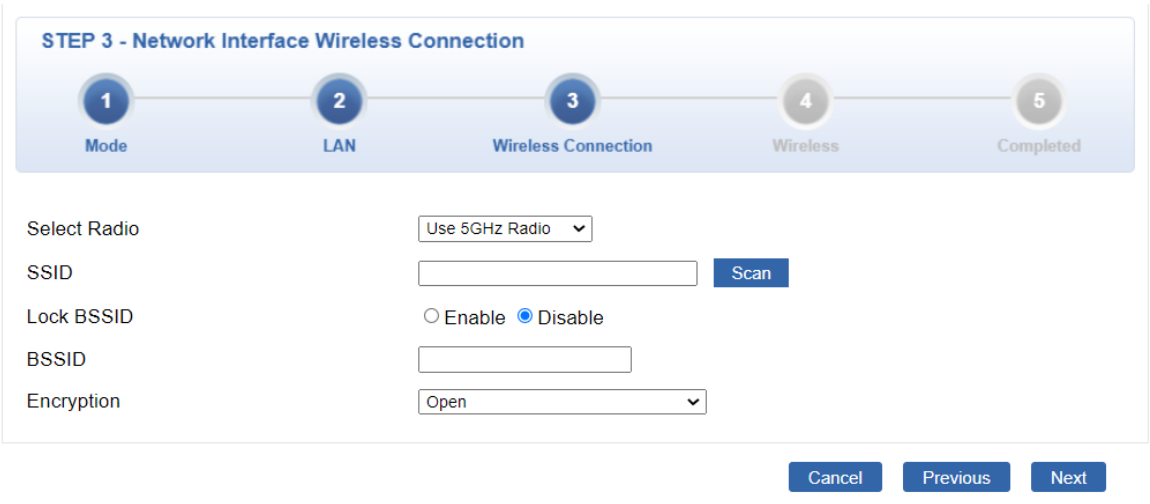


Step 3. In AP-1, go to "**Wizard**" to configure it to **AP Mode**. In AP-2, configure it to **Repeater Mode**.

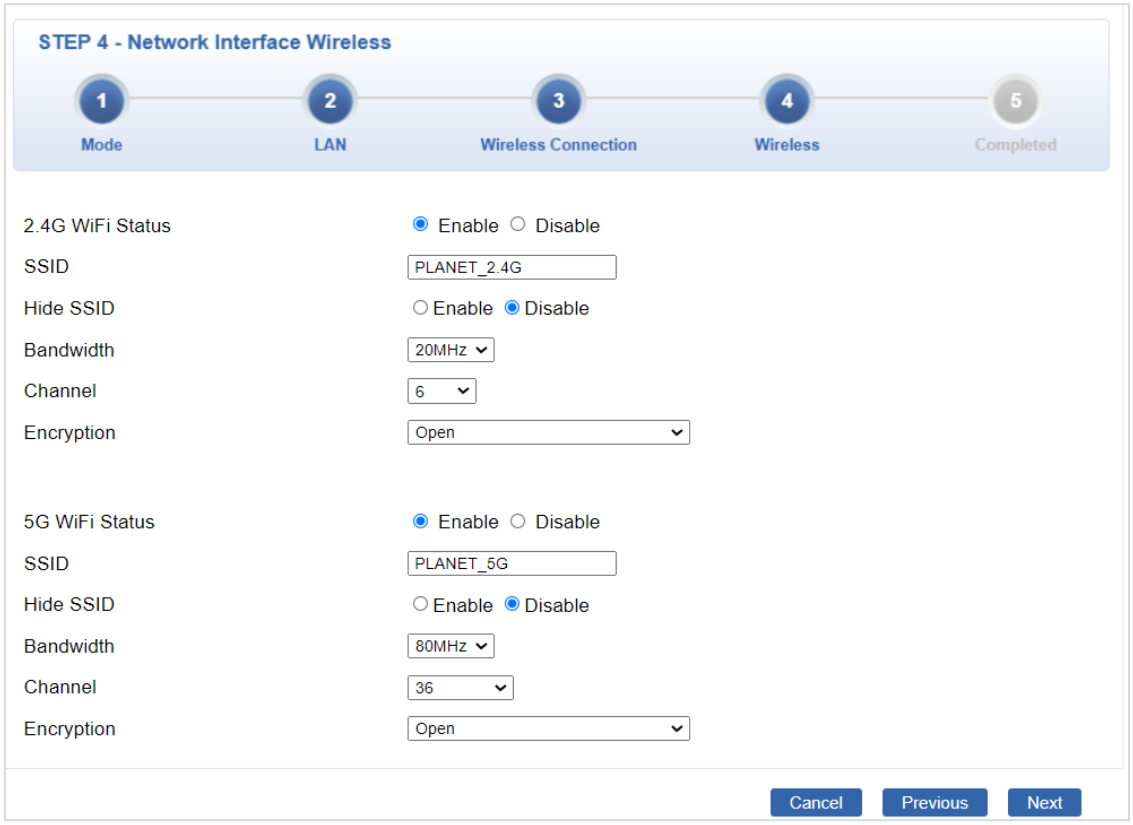
AP-1

AP-2

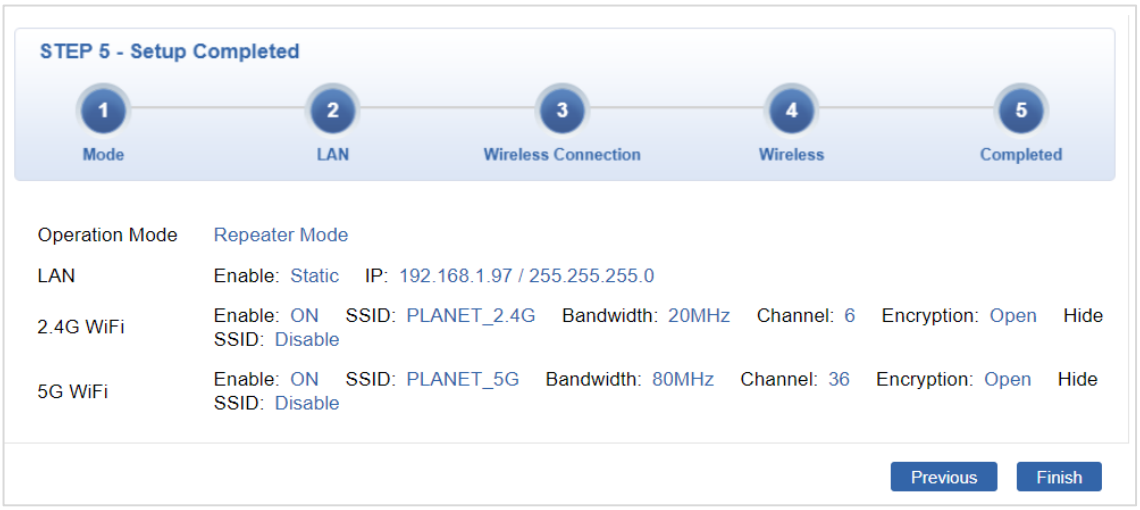
Step 4. In AP-2, press "**Scan "** to search the AP-1. You can also enter the MAC address, SSID, encryption and bandwidth if you know what they are.



Step 5. Click "**Next**" to finish the setting.

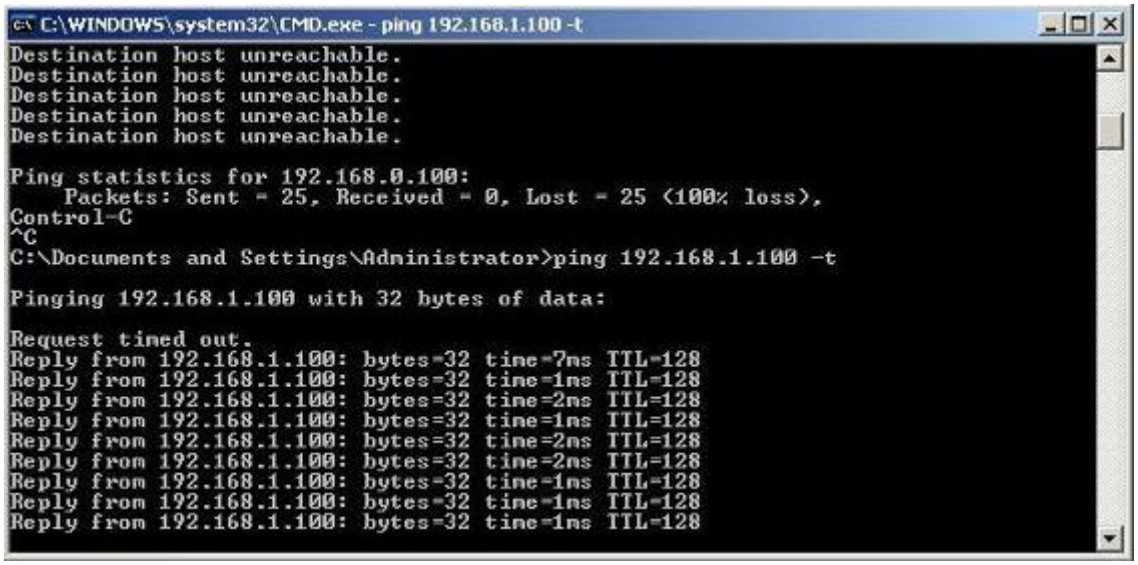


Step 6. Setup Completed

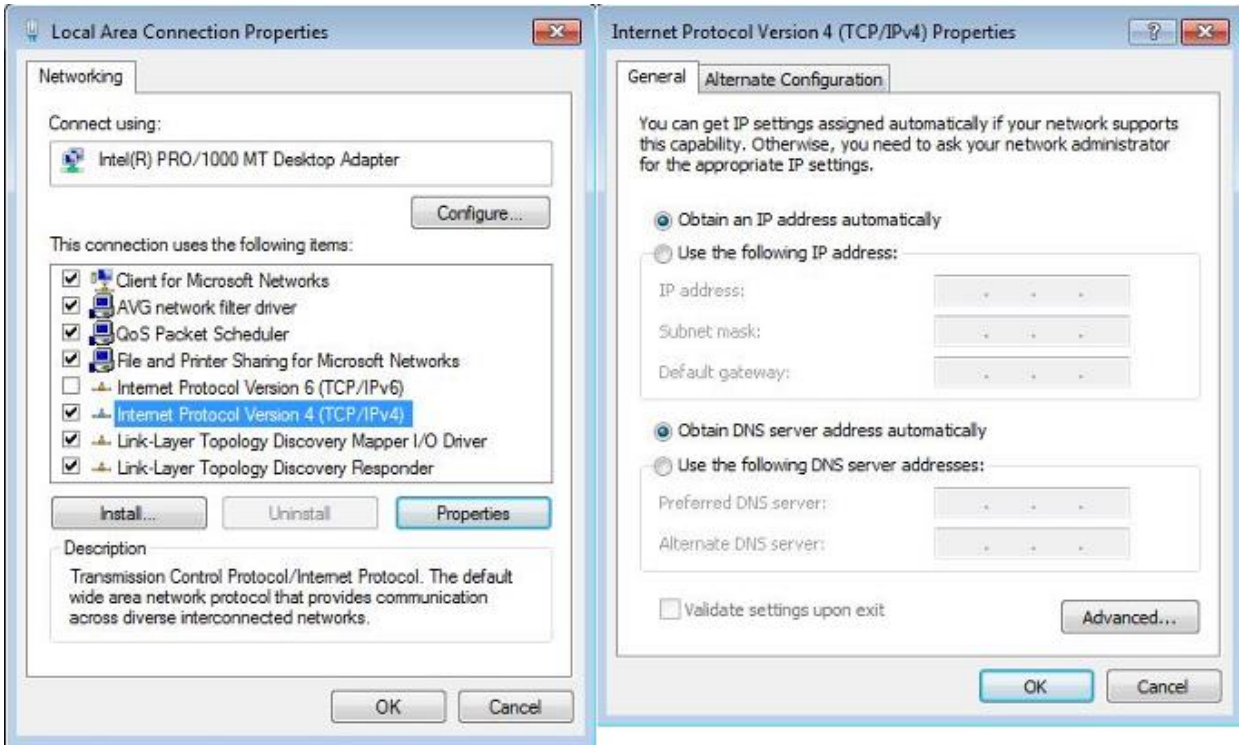


Step 7. Use command line tool to ping each other to ensure the link is successfully established.

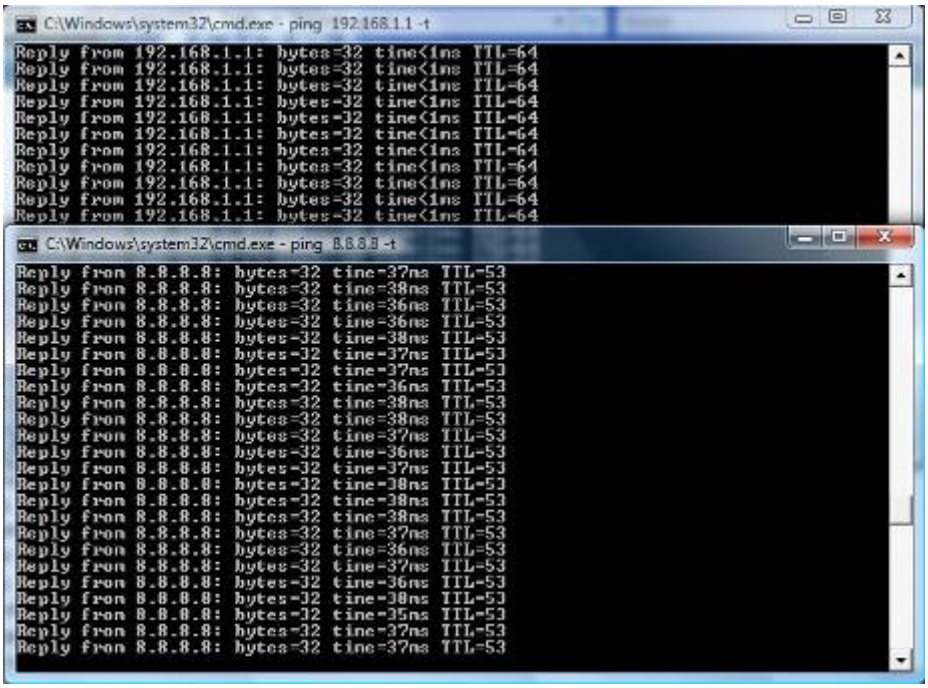
From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.100.



Step 8. Configure the TCP/IP settings of Site-2 to "**Obtain an IP address automatically**".



Step 9. Use command line tool to ping the DNS (e.g., Google) to ensure Site-2 can access internet through the wireless connection.



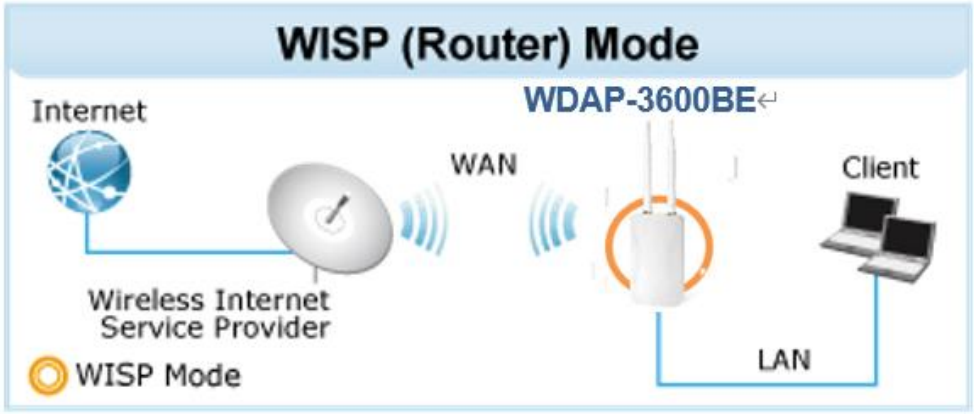
Note

The following hints should be noted:

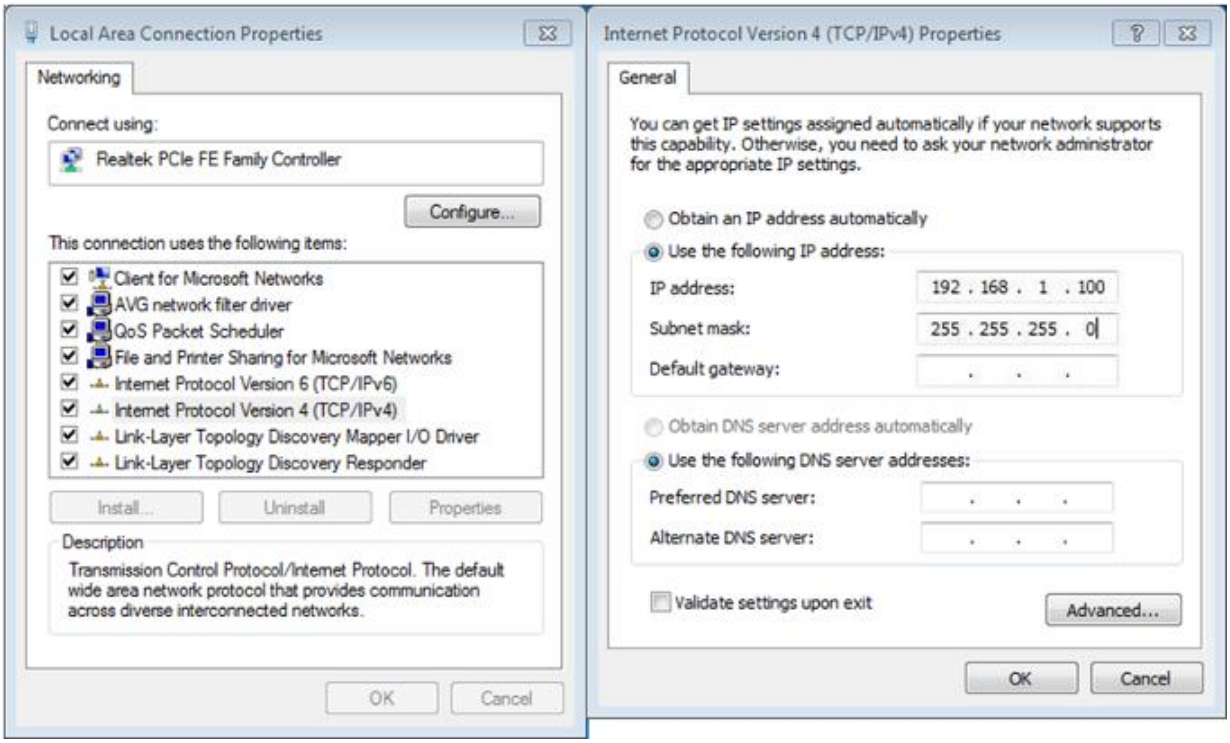
1) The encryption method must be the same as that of both sites if configured.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "RF Output Power" of both sites.
4) For the long distance connection over 1km, please adjust the "Distance" to the actual distance or double the actual distance.

How to Set Up WISP Connection

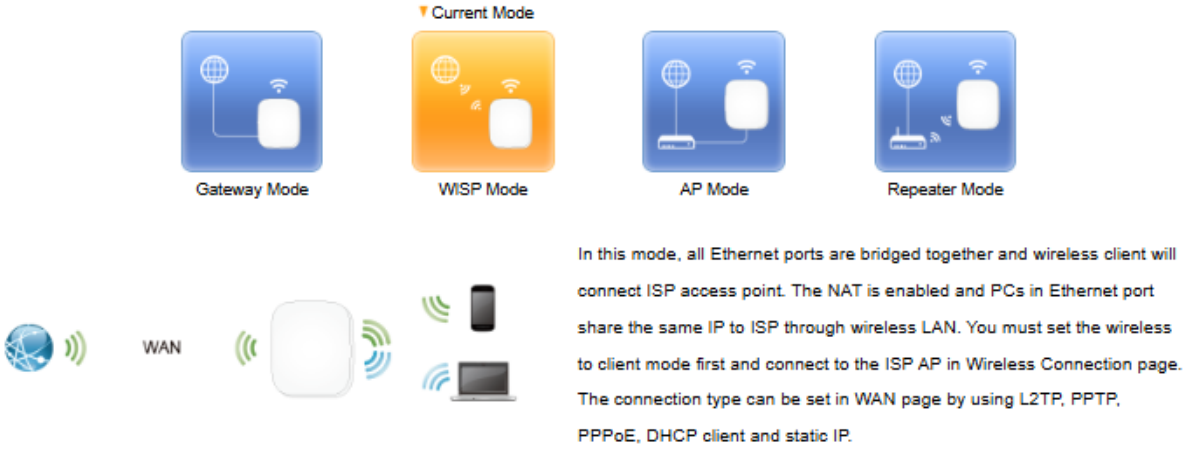
Topology (The topology below uses the WDAP-3600BE as an example):



Step 1. Use static IP in the PC (Client) that is connected with the AP. In this case, the IP address of client is "**192.168.1.100**".

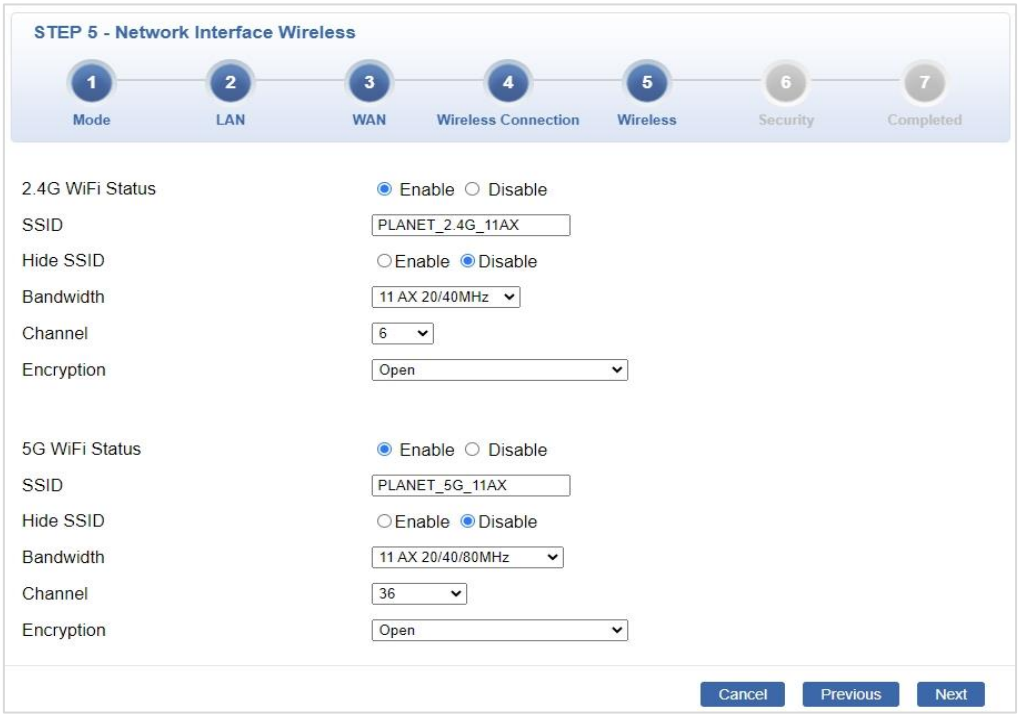


Step 2. In AP, go to "**Wizard**" to configure it in **WISP Mode**.

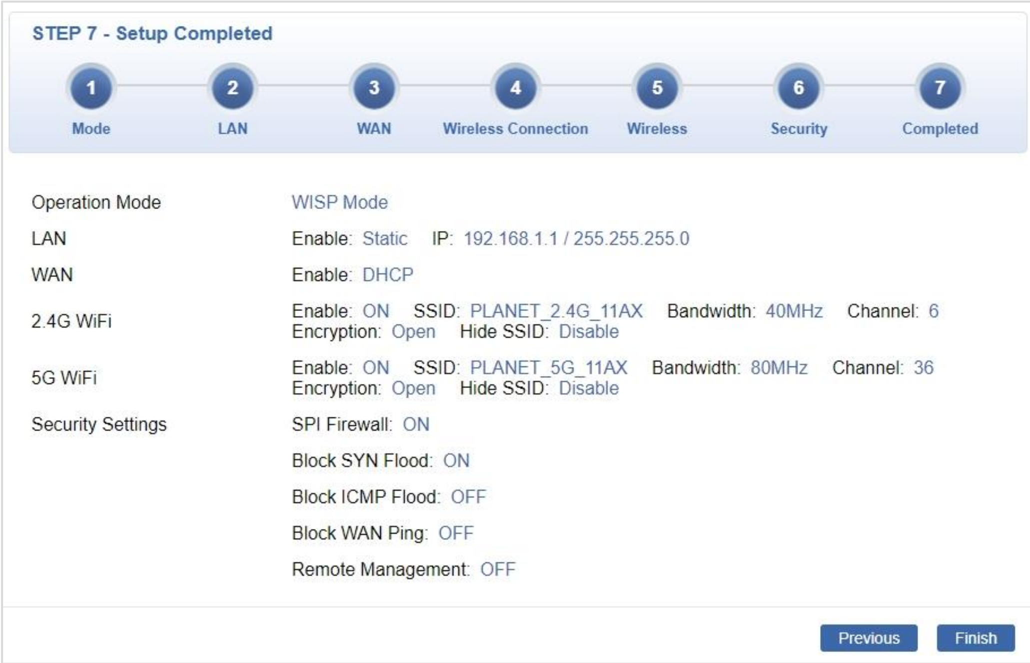


Step 3. Press "**Scan"** to search **the Wi-Fi of WAN devices**. You can also enter the MAC address, SSID, encryption and bandwidth if you know what they are.

Step 4. Click "**Next**" to finish the setting.



Step 5. Setup Completed



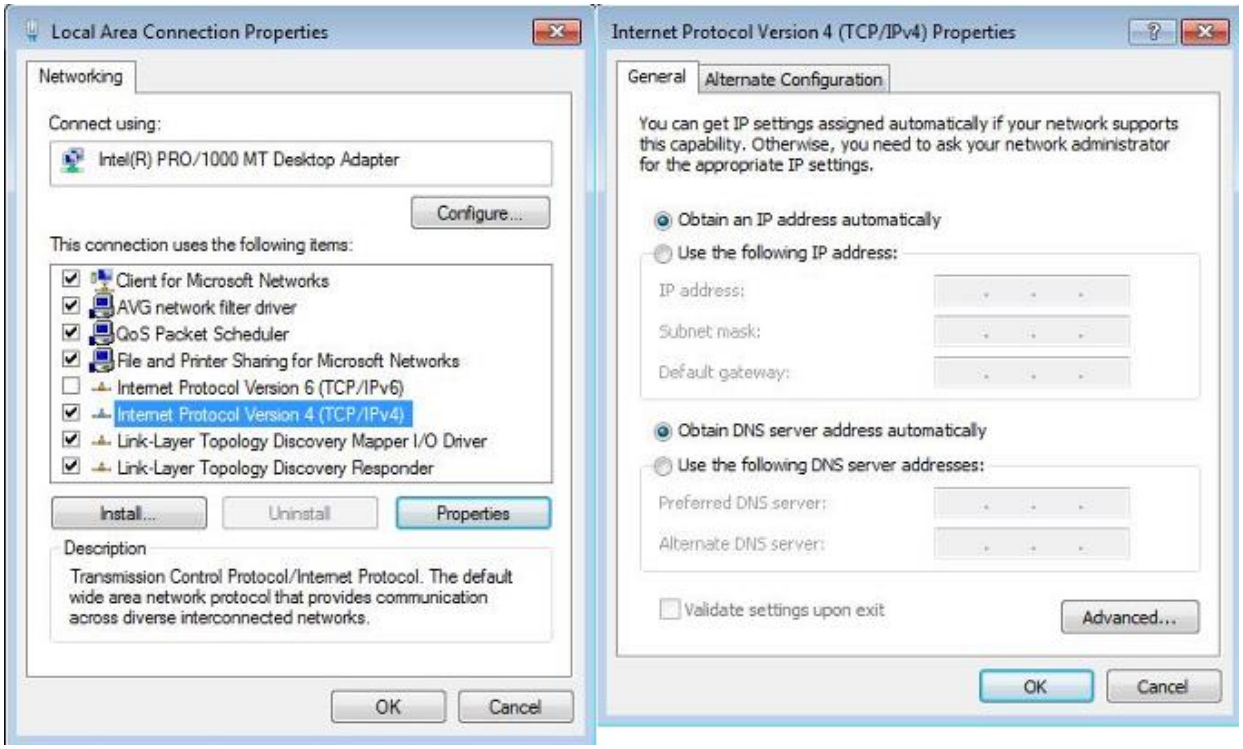
Step 6. Use command line tool to ping each other to ensure the link is successfully established.

From client, ping 192.168.1.253 (the AP's IP)

```
C:\>ping 192.168.1.253 -t

Pinging 192.168.1.253 with 32 bytes of data:
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
Reply from 192.168.1.253: bytes=32 time<1ms TTL=64
```

Step 7. Configure the TCP/IP settings of PC to "**Obtain an IP address automatically**".



Step 8. Use command line tool to ping the DNS (e.g., Google) to ensure client can access internet through the wireless connection.

```
C:\>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=26ms TTL=54
Reply from 8.8.8.8: bytes=32 time=21ms TTL=54
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=20ms TTL=54
Reply from 8.8.8.8: bytes=32 time=19ms TTL=54
Reply from 8.8.8.8: bytes=32 time=22ms TTL=54
Reply from 8.8.8.8: bytes=32 time=23ms TTL=54
Reply from 8.8.8.8: bytes=32 time=27ms TTL=54
Reply from 8.8.8.8: bytes=32 time=21ms TTL=54
Reply from 8.8.8.8: bytes=32 time=20ms TTL=54
Reply from 8.8.8.8: bytes=32 time=21ms TTL=54
Reply from 8.8.8.8: bytes=32 time=20ms TTL=54
Reply from 8.8.8.8: bytes=32 time=20ms TTL=54
Reply from 8.8.8.8: bytes=32 time=21ms TTL=54
```

Note

The following hints should be noted:

1) The encryption method must be the same as that of both sites if configured.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "RF Output Power" of both sites.
4) For the long distance connection over 1km, please adjust the "Distance" to the actual distance or double the actual distance.

Appendix C: Troubleshooting

If you find the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the dealer for help. Some problems can be solved by yourself within a very short time.

Scenario	Solution
The AP is not responding to me when I want to access it by Web browser.	a. Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be correctly and firmly inserted into the AP. b. If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered. c. You must use the same IP address section which AP uses. d. Are you using MAC or IP address filter? Try to connect the AP by another computer and see if it works; if not, please reset the AP to the factory default settings by pressing the 'reset' button for over 7 seconds. e. Use the Smart Discovery Tool to see if you can find the AP or not. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all the solutions above don't work, contact the dealer for help.
I can't get connected to the Internet.	a. Go to 'Status' -> 'Internet Connection' menu on the router connected to the AP, and check Internet connection status. b. Please be patient. Sometimes Internet is just that slow. c. If you've connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password entered in the router's settings again. e. Call your Internet service provider and check if there's something wrong with their service. f. If you just can't connect to one or more website, but you can still use other internet services, please check

Scenario	Solution
	URL/Keyword filter. g. Try to reset the AP and try again later. h. Reset the device provided by your Internet service provider too. i. Try to use IP address instead of host name. If you can use IP address to communicate with a remote server, but can't use host name, please check DNS setting.
I can't locate my AP by my wireless device.	a. 'Broadcast ESSID' set to off? b. Both two antennas are properly secured. c. Are you too far from your AP? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	a. Internet is slow sometimes. Please be patient. b. Try to reset the AP and see if it's better after that. c. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. d. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; the password is wrong.	a. Make sure you're connecting to the correct IP address of the AP. b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The AP becomes hot	a. This is not a malfunction, if you can keep your hand on the AP's case. b. If you smell something wrong or see the smoke coming out from AP or A/C power adapter, please disconnect the AP and power source from utility power (make sure it's safe before you're doing this), and call your dealer of purchase for help.

Appendix D: Glossary

802.11ax - 802.11ax is a wireless networking standard in the 802.11 family by adding OFDMA, MU-MIMO (which is marketed under the brand name Wi-Fi 6), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5GHz band 20、40、80、160MHz.

802.11ac - 802.11ac is a wireless networking standard in the 802.11 family by adding MU-MIMO (which is marketed under the brand name Wi-Fi 5), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5GHz band.

802.11n - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.

802.11a - 802.11a was an amendment to the IEEE 802.11 wireless local network specifications that defined requirements for an orthogonal frequency division multiplexing (OFDM) communication system. It was originally designed to support wireless communication in the unlicensed national information infrastructure (U-NII) bands (in the 5–6 GHz frequency range) as regulated in the United States by the Code of Federal Regulations, Title 47, Section 15.407.

802.11b - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHzHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

802.11g - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHzHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.

DMZ (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

DNS (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.

Domain Name - A descriptive name for an address or group of addresses on the Internet.

DSL (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.

MTU (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.

NAT (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

SSID - A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

Wi-Fi - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation, declares that this 11be Wireless AP is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.	Lietuviškai	Šiuo PLANET Technology Corporation,, skelbia, kad 11be Wireless AP tenkina visus svarbiausius 2014/53/EU direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation, tímto prohlašuje, že tato 11be Wireless AP splňuje základní požadavky a další příslušná ustanovení směrnice 2014/53/EU.	Magyar	A gyártó PLANET Technology Corporation, kijelenti, hogy ez a 11be Wireless AP megfelel az 2014/53/EU irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation, erklærer herved, at følgende udstyr 11be Wireless AP overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU	Malti	Hawnhekk, PLANET Technology Corporation, jiddikjara li dan 11be Wireless AP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU
Deutsch	Hiermit erklärt PLANET Technology Corporation, dass sich dieses Gerät 11be Wireless AP in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 2014/53/EU befindet". (BMWi)	Nederlands	Hierbij verklaart , PLANET Technology orporation, dat 11be Wireless AP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU
Eestikeeles	Käesolevaga kinnitab PLANET Technology Corporation, et see 11be Wireless AP vastab Euroopa Nõukogu direktiivi 2014/53/EU põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation, oświadcza, że 11be Wireless AP spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 2014/53/EU.
Ελληνικά	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ , PLANET Technology Corporation, ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ 11be Wireless ΑΡΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU	Português	PLANET Technology Corporation, declara que este 11be Wireless AP está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Español	Por medio de la presente, PLANET Technology Corporation, declara que 11be Wireless AP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU	Slovensky	Výrobca PLANET Technology Corporation, týmto deklaruje, že táto 11be Wireless AP je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 2014/53/EU.
Français	Par la présente, PLANET Technology Corporation, déclare que les appareils du 11be Wireless AP sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU	Slovensko	PLANET Technology Corporation, s tem potrjuje, da je ta 11be Wireless AP skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 2014/53/EU

Italiano	Con la presente , PLANET Technology Corporation, dichiara che questo 11be Wireless AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.	Suomi	PLANET Technology Corporation, vakuuttaa täten että 11be Wireless AP tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo PLANET Technology Corporation, apliecina, ka šī 11be Wireless AP atbilst Direktīvas 2014/53/EU pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation, att denna 11be Wireless AP står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.