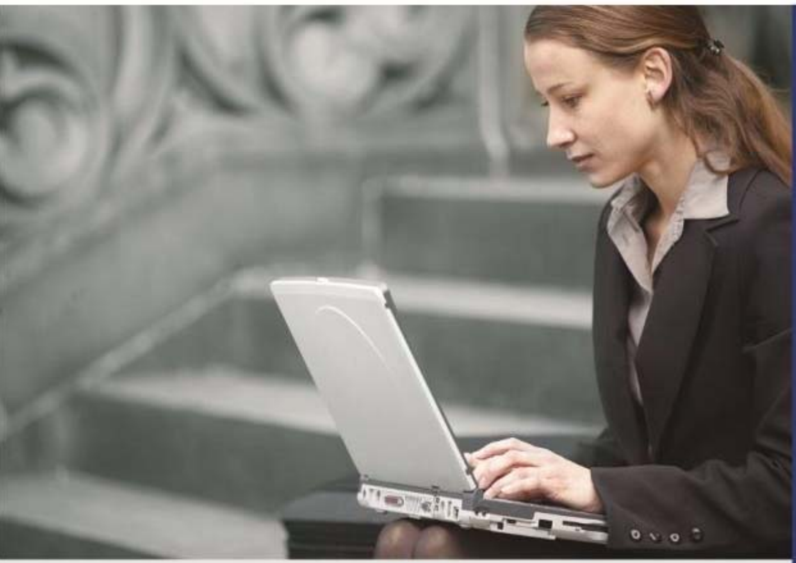
PLANET
Networking & Communication

User's Manual

Dual Band 802.11ax 1800Mbps

Wireless Access Point w/802.3at PoE

- ► WDAP-C1800AX
- ► WDAP-1800AX



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 5.15-5.25GHzHz 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 802.11ax Dual Band Ceiling-mount Wireless Access Point

Model: WDAP-C1800AX

Rev: 2.1 (November, 2021)

Part No. EM-WDAP-C1800AX_v2.0_WDAP-1800AX

Table of Contents

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WDAP-C1800AX Wireless AP. Please verify the contents inside the package box.

Package Contents of WDAP-C1800AX

WDAP-C1800AX	Quick Guide	Ethernet Cable	Mounting Kit

Package Contents of WDAP-1800AX

WDAP-1800AX	Quick Guide	L-type Bracket x 1
Screw Set x 1	U-bolt Kit x 2	RJ45 Waterproof Kit x 1

Note

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

1.2 Product Description (Please refer to PLANET website for WDAP-1800AX information.)

Ultra-high-speed Wi-Fi 6 Wireless LAN Solution

PLANET WDAP-C1800AX **1800Mbps Dual Band 802.11ax Wireless AP**, supporting **MU-MIMO, OFDMA, Seamless Roaming, Beamforming and BSS Coloring technology,** provides a maximum wireless speed of 1200Mbps in the 5GHz band and 600Mbps in the 2.4GHz band. The maximum number of client users is up to 150, ensuring more secure and robust connectivity with the adoption of Wi-Fi 6 technology.

Benefits of MU-MIMO, OFDMA, Seamless Roaming, Beamforming and BSS Coloring

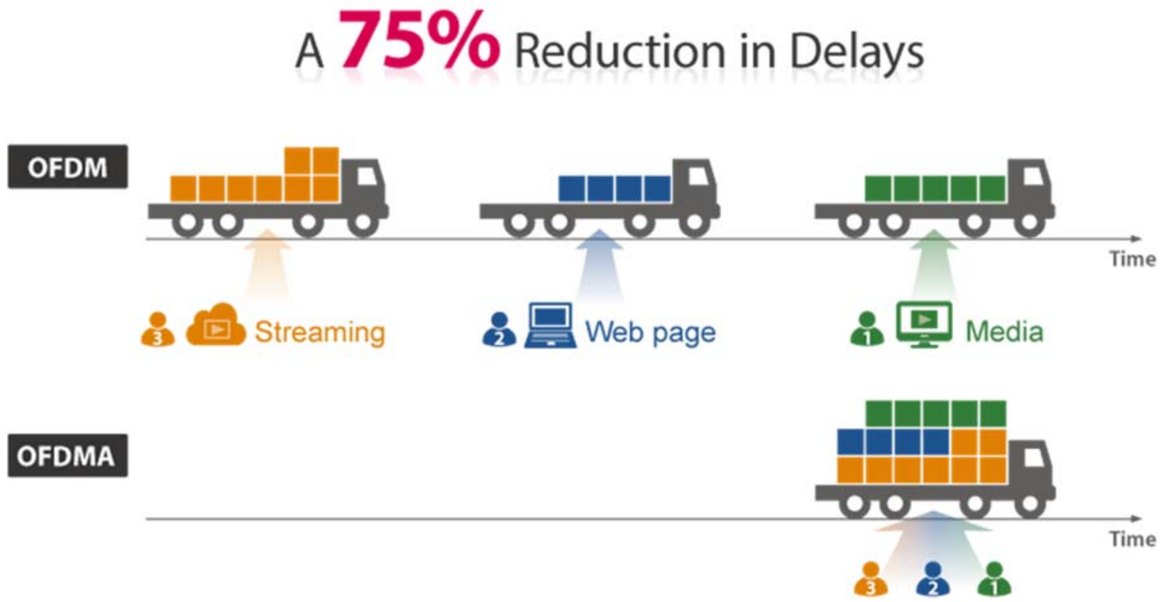
The WDAP-C1800AX can be installed in public areas such as hotspots, airports and conferences as OFDMA, a multi-user version of OFDM, enables the concurrent AP to communicate (uplink and downlink) with multiple clients by assigning subsets of subcarriers called resource units (RUs) to the individual clients. With MU-MIMO and Seamless Roaming technologies, it provides a better Wi-Fi user experience, reducing the likelihood of users turning off Wi-Fi and putting more load on the cellular network.

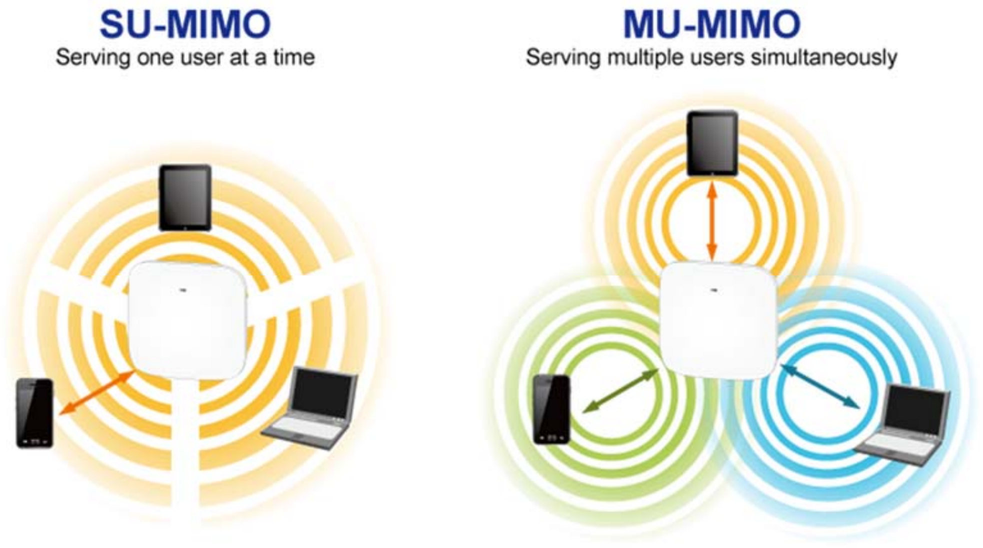
Beamforming is to improve your Wi-Fi signal when you are far away from your router. The BSS color is a numerical identifier of the BSS. 802.11ax radios that are able to differentiate between BSSs using BSS color identifier when other radios transmit on the same channel. These technologies also can solve Wi-Fi congestion issues in open work spaces and conference rooms. The WDAP-C1800AX can offer more powerful throughput coverage of up to 150 client users.

OFDMA (Orthogonal Frequency Division Multiple Access) Benefits

- Helps transmit small and large packets together to reduce bandwidth burden and improve data transmission performance
- Transmitting data at the same time can effectively reduce the transmission delay for longer frame and low-speed transmission.

- Improves the overall traffic quality, and effectively uses bandwidth in an environment where multiple people use the Internet.
- Increases the number of devices that can be connected to the AP.
- Reduces the power consumption of the device by way of the use of low bandwidth.

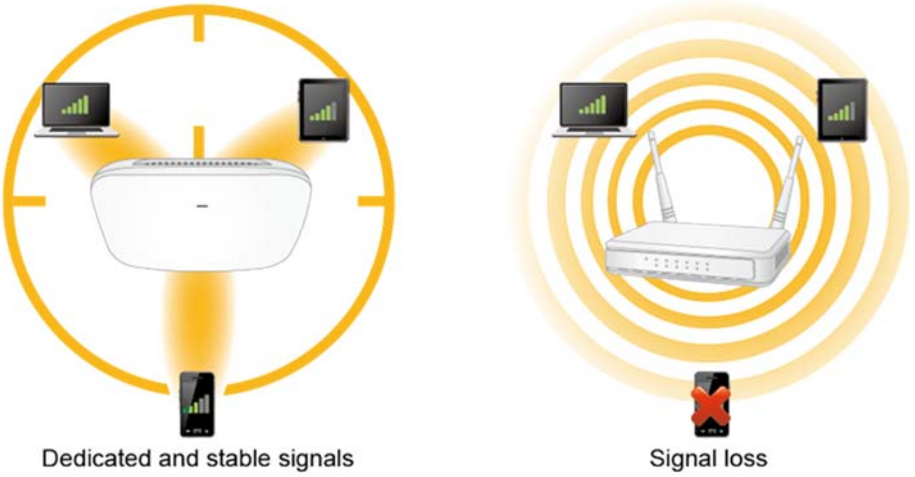



SU-MIMO
Serving one user at a time
MU-MIMO
Serving multiple users simultaneously

Beamforming

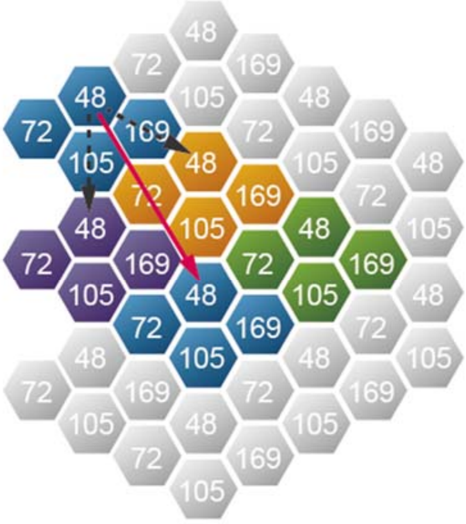
Beamforming is to improve your Wi-Fi signal when you are far away from your router. Wi-Fi beam forming narrows the focus of the router signal, sending it directly to your devices in a straight line, thus minimizing surrounding signal interference and increasing the strength of the signal that ultimately brings you the following benefits:

- Extend your Wi-Fi coverage
- Deliver a more stable Wi-Fi connection
- Deliver better Wi-Fi throughput
- Reduce router interference



■ BSS Coloring

The BSS color is a numerical identifier of the BSS. 802.11ax radios that are able to differentiate between BSSs using BSS color identifier when other radios transmit on the same channel. If the color is the same, this is considered to be an intra-BSS frame transmission. In other words, the transmitting radio belongs to the same BSS as the receiver. If the detected frame has a different BSS color from its own, then the STA considers the frame as an inter-BSS frame from an overlapping BSS.



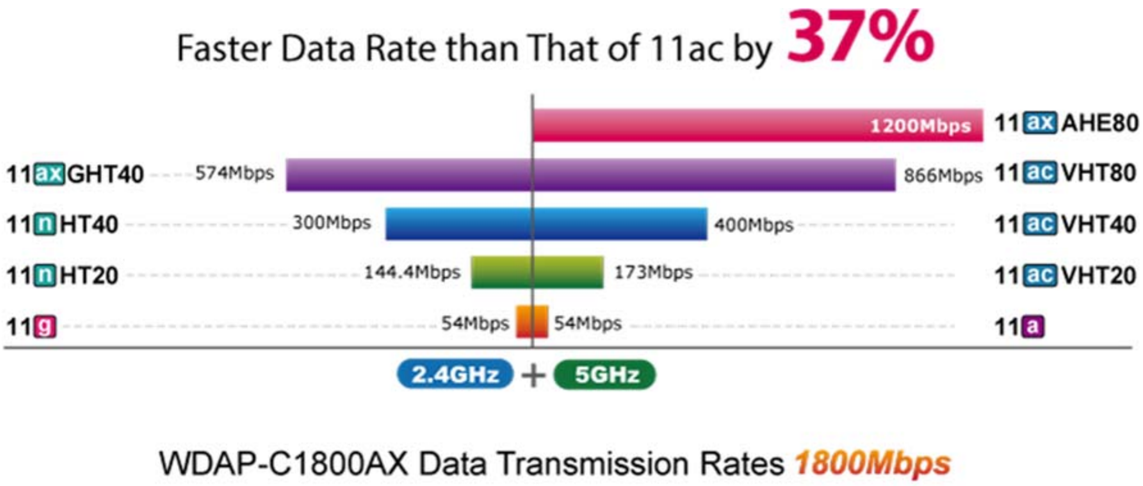
WPA3 Next Generation Security for Your WLAN Solution

WPA3 is the next generation Wi-Fi security technology that provides the most advanced security protocol to the market. WPA3 makes your connection more secure by preventing hackers from easily cracking your password no matter how simplified the password is. WPA3 can also provide more reliable password-based authentication, so it can better protect the security of individual users.

* WDAP-C1800AX only supports WPA3-Personal.

Super Power Dual band WLAN Solution

PLANET WDAP-C1800AX, adopting the IEEE 802.11ax Wi-Fi 6 standard, provides a high-speed transmission. The maximum wireless speed in 2.4GHz band is up to 11AX of 574Mbps, and in the 5GHz band is up to 11AX of 1201Mbps. Both the **2.4GHz and 5GHz** wireless connections can also be used simultaneously.

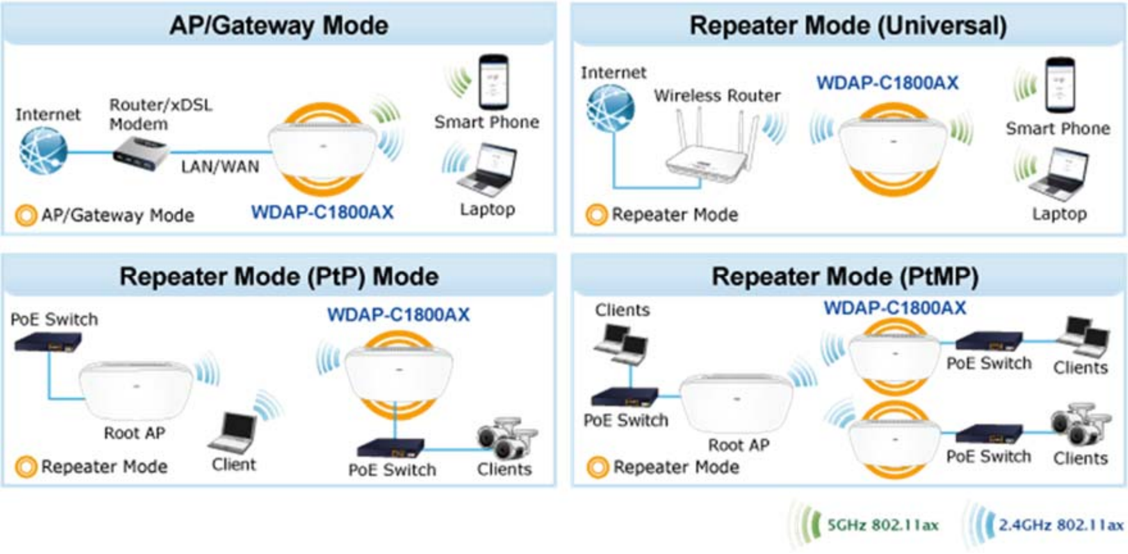


Advanced Security and Rigorous Authentication

The WDAP-C1800AX supports WPA/WPA2/WPA3 wireless encryptions, WPA2 Enterprise, and WPA/WPA2 Enterprise, which can effectively prevent eavesdropping by unauthorized users or bandwidth occupied by unauthenticated wireless access. Furthermore, any users are granted or denied access to the wireless LAN network based on the ACL (Access Control List) that the administrator pre-established.

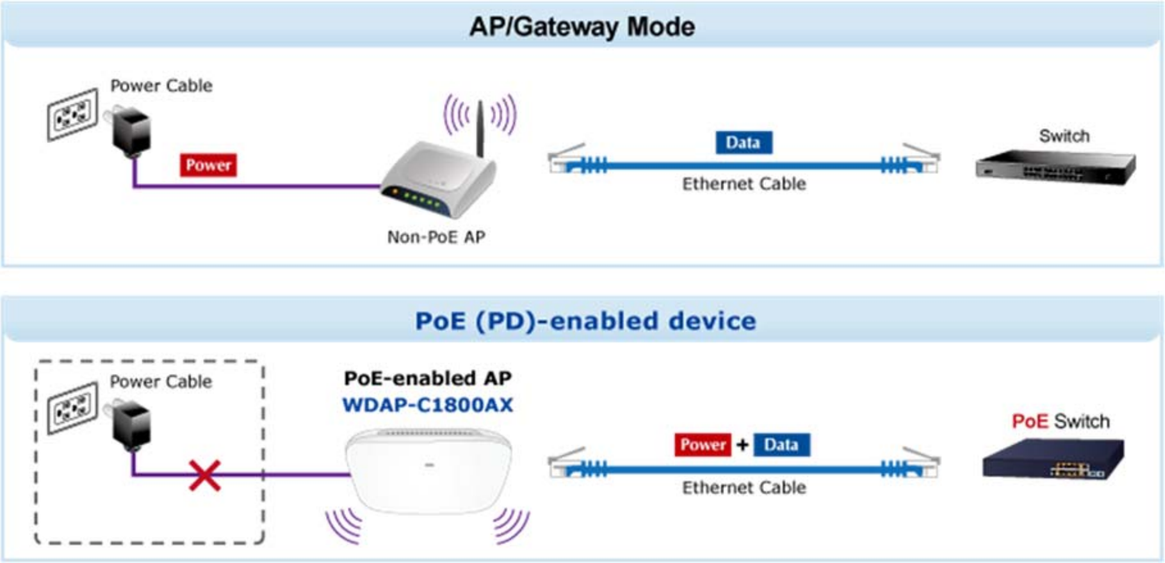
Multiple Operation Modes for Various Applications

The WDAP-C1800AX supports the simplified usage modes of AP, Gateway and Repeater, through which they provide more flexibility for users when wireless network is established. Compared with general wireless access points, the WDAP-C1800AX offers more powerful and flexible capability for wireless clients.



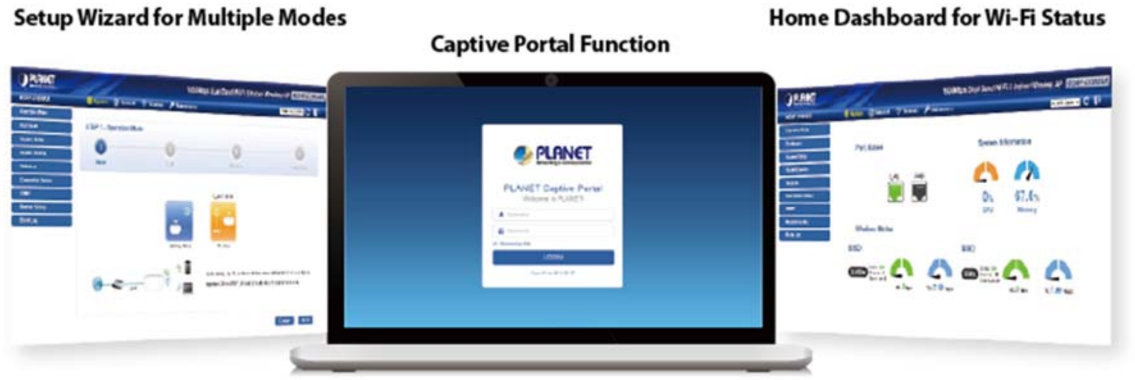
Ceiling-mount Design for Your Environment

With the standard IEEE802.3at Power over Ethernet (PoE) design, the WDAP-C1800AX can be easily installed in the areas where power outlets are not available. By supporting the standard IEEE 802.3at PoE PD power scheme, the WDAP-C1800AX can be powered and networked by a single UTP cable, effectively eliminating the needs of dedicated electrical outlets on the ceiling and reducing the cabling cost. Furthermore, the system administrator is able to arrange the PoE schedule of the WDAP-C1800AX by working with the managed PoE switch.



Optimized Efficiency in AP Management

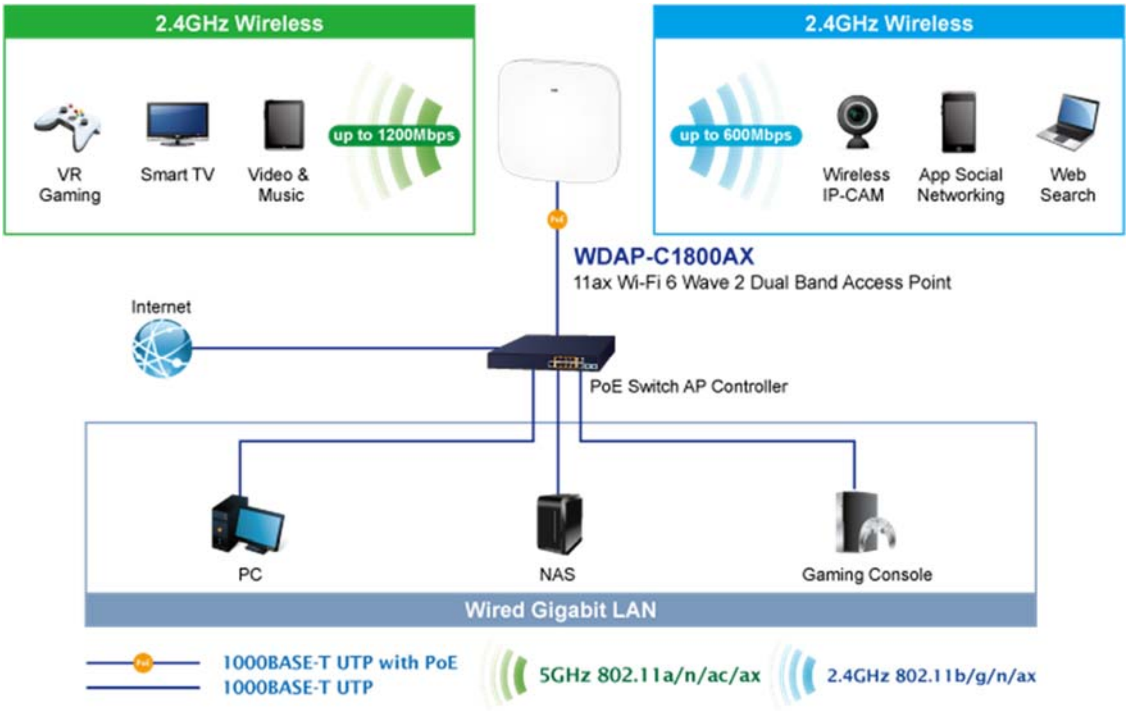
The brand-new GUI configuration wizard helps the system administrator easily set up the WDAP-C1800AX step by step. Besides, the built-in Wi-Fi analyzer provides real-time channel utilization to prevent channel overlapping to assure greater performance. With the automatic transmission power mechanism, distance control and scheduling reboot setting, the WDAP-C1800AX is easy for the administrator to deploy and manage without on-site maintenance. Moreover, you can use PLANET NMS-500 or NMS-1000V AP control function to deliver wireless profiles to multiple APs simultaneously, thus making the central management simple.


Setup Wizard for Multiple Modes
Captive Portal Function
Home Dashboard for Wi-Fi Status
PLANET
PLANET Captive Portal

Applications

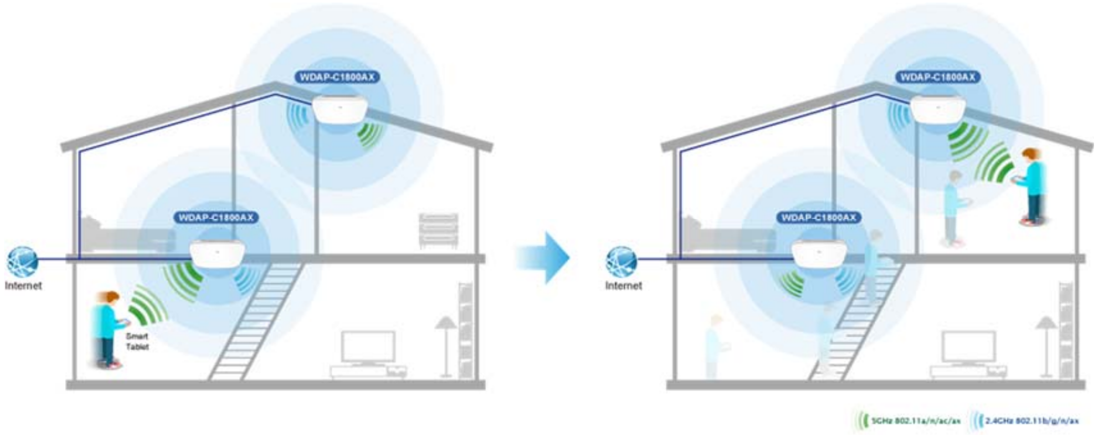
Extreme High Speed and Wi-Fi 6 Technology Make Wireless Transmission More Powerful

The WDAP-C1800AX delivers the dual band and more bandwidth to avoid signal interference and ensure the best Wi-Fi performance. It allows you to check e-mails and surf the Internet via the 2.4GHz band and simultaneously watch full high-definition (HD) video or any other multimedia application via one 5GHz band. Besides, many client users can be connected to Wi-Fi at the same time. The maximum number of client users is up to 150. Moreover, the Gigabit Ethernet port of the WDAP-C1800AX offers ultra-fast wired connections that utilize the maximum wireless bandwidth; therefore, users will experience a fast wireless speed of over 650Mbps. With the outstanding stability of high-speed wireless transmission, the WDAP-C1800AX can provide users with excellent experience in multimedia streaming with your mobile devices anywhere, anytime.



Seamless Roaming and Better Coverage

Moving between a traditional Wi-Fi AP or router and range extender, your Wi-Fi signal can experience lag or a dropped connection. With Seamless Roaming and intuitive technology, moving from room to room is never a problem now that your devices are switched to the strongest Wi-Fi signal automatically. The WDAP-W1800AX features advanced 2T2R MU-MIMO technology which reduces the effect of dead spot, so that it can get better coverage of the existing wireless network. Furthermore, the repeater mode supported by the WDAP-W1800AX helps to minimize the effort of installation, thus reducing cabling cost.


WDAP-C1800AX
WDAP-C1800AX
Internet
Smart Tablet
WDAP-C1800AX
WDAP-C1800AX
Internet
5GHz 802.11a/n/ac/ax
2.4GHz 802.11b/g/n/ax

1.3 Product Features (Please refer to PLANET website for WDAP-1800AX information.)

Industrial Compliant Wireless LAN

- Compliant with the IEEE 802.11a/b/g/n/ac/ax wireless technology
- Equipped with 10/100/1000Mbps RJ45 ports, and auto MDI/MDI-X

RF Interface Characteristics

- 802.11ax 2T2R architecture with data rate of up to 1800Mbps (600Mbps in 2.4GHz and 1200Mbps in 5GHz)
- High output power with multiply-adjustable transmit power control

Multiple Operation Modes and Wireless Features

- Multiple operation modes: AP, gateway and repeater
- Supports OFDMA (orthogonal frequency division multiple access)
- Supports MU-MIMO (multi-user multiple-input multiple-output), Beamforming and BSS Coloring
- WMM (Wi-Fi multimedia) provides higher priority to multimedia transmitting over wireless
- Coverage threshold to limit the weak signal of clients occupying session
- Real-time Wi-Fi channel analysis chart and client limit control for better performance
- Support Terminal Seamless Roaming with 802.11k, 802.11v, and 802.11r

Secure Network Connection

- Full encryption supported: 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 and WPA/WPA2 Enterprise
- Supports 802.1Q port VLAN
- Supports IP/Port/MAC address/URL filtering, DoS, SPI firewall
- Supports DMZ and port forwarding
- Bandwidth control per IP address to increase network stability

Easy Deployment and Management

- Supports PLANET AP Controllers in AP mode
- Easy discovery by PLANET Smart Discovery

- Self-healing mechanism through system auto reboot setting
- System status monitoring through remote syslog server
- Gateway mode supports PLANET DDNS/Easy DDNS, Captive Portal, RADIUS Server/Client

1.4 Product Specifications

Product	**WDAP-C1800AX** Dual Band 802.11ax 1800Mbps Ceiling-mount Wireless Access Point
Hardware Specifications	
Interfaces	LAN 2 x 10/100/1000BASE-T RJ45 port Auto-negotiation and auto MDI/MDI-X
Antennas	Gain: 4 x Internal 4dBi antenna (2.4G x2, 5G x2)
Reset Button	Reset button on the rear side (Press over 5 seconds to reset the device to factory default)
LED Indicators	Power, SYS
Dimensions (W x D x H)	186 x 186 x 35.8 mm
Weight	380 ± 5g
Power Requirements	48V DC IN, 0.5A, IEEE 802.3at PoE+ (WAN/PoE were changed port) 12V DC IN, 2.0A from DC Jack (5.5 x 2.1mm)
Power Consumption	< 15W
Mounting	Ceiling Mount
Wireless Interface Specifications	
Standard	IEEE 802.11ax IEEE 802.11ac IEEE 802.11n IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3x flow control IEEE 802.11k, 802.11v, and 802.11r
Media Access Control	CSMA/CA
Data Modulation	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)
Band Mode	2.4GHz / 5GHz concurrent mode
Frequency Range	**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		
Operating Channels	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) 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) **5GHz channel list may vary in different countries according to their regulations.**		
Max. Transmit Power (dBm)	FCC: up to 20 ± 1dBm ETSI: < 19dBm (EIRP)		
Receive Sensitivity	**Network Mode**	**Data Rate**	**Receive Sensitivity (dBm)**
	2.4GHz		
	802.11b	1Mbps	-92
		11Mbps	-85
	802.11g	6Mbps	-90
		54Mbps	-72
	802.11n HT20	MCS0	-88
		MCS7	-70
	802.11n HT40	MCS0	-86
		MCS7	-68
	802.11ax HT20	MCS0	-85
		MCS11	-60
	802.11ax HT40	MCS0	-85
		MCS11	-56
	5GHz		
	802.11a	6Mbps	-92
		54Mbps	-72
	802.11n HT20	MCS0	-90
		MCS7	-70
	802.11n HT40	MCS0	-88
		MCS7	-68
	802.11ac HT20	MCS0	-90
		MCS7	-70
	802.11ac HT40	MCS0	-88
		MCS7	-68
	802.11ac HT80	MCS0	-85

		MCS9	-58
	802.11ax HT20	MCS0	-88
		MCS11	-62
	802.11ax HT40	MCS0	-86
		MCS11	-58
	802.11ax HT80	MCS0	-84
		MCS11	-55

Software Features	
LAN	Static IP / *Dynamic IP
WAN	Static IP Dynamic IP PPPoE/PPTP/L2TP
Wireless Mode	Access Point Gateway Repeater
Channel Width	20MHz, 40MHz, 80MHz
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 and WPA/WPA2 Enterprise
Wireless Security	Enable/Disable SSID Broadcast Wireless Max. 32 MAC address filtering User Isolation
Max. SSIDs	8 (4 per radio)
Max. Clients	150 (100 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-500, NMS-1000V, PLANET CloudViewer
Environment & Certification	
Temperature	Operating: -20~ 55 degrees C Storage: -40 ~ 70 degrees C
Humidity	Operating: 10 ~ 90% (non-condensing) Storage: 5 ~ 90% (non-condensing)
Regulatory	CE, RoHS
Remarks [*]: The feature will be supported through firmware/system upgrade.	

Product	**WDAP-1800AX** Dual Band 802.11ax 1800Mbps Outdoor Wireless AP
Hardware	
Interface	PoE WAN: 1 x 10/100/1000BASE-T, auto-MDI/MDIX, 802.3at PoE In
Antenna	Built-in four N-type connectors
Button	Reset button (Press over 5 seconds to reset the device to factory default)
Dimensions (W x D x H)	231 x 80 x 295 mm
Weight	2.5kg
Material	Aluminum
Power Requirement	48V 0.5A, IEEE 802.3at PoE+
Power Consumption (max.)	< 15W
Mounting Type	Mast mounting
IP Level	IP67
ESD Protection	±8kV air gap discharge ±4kV contact discharge
Surge Protection	±20kV
Wireless Interface Specifications	
Standard Support **WDAP-C1800AX(V2)**	IEEE 802.11ax IEEE 802.11ac IEEE 802.11n IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3x flow control IEEE 802.11k, 802.11v, and 802.11r
Media Access Control	CSMA/CA
Date Modulation	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)
Band Mode	2.4GHz / 5GHz concurrent mode
Frequency Band	**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		
Operating Channels	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) 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) **5GHz channel list may vary in different countries depending on their regulations.**		
Max. Transmit Power (dBm)	FCC: up to 20 ± 1dBm ETSI: < 19dBm (EIRP)		
Receiver Sensitivity (dBm)	**Network Mode**	**Data Rate**	**Receive Sensitivity (dBm)**
	2.4GHz		
	802.11b	1Mbps	-92
		11Mbps	-85
	802.11g	6Mbps	-90
		54Mbps	-72
	802.11n HT20	MCS0	-88
		MCS7	-70
	802.11n HT40	MCS0	-86
		MCS7	-68
	802.11ax HT20	MCS0	-85
		MCS11	-60
	802.11ax HT40	MCS0	-85
		MCS11	-56
	5GHz		
	802.11a	6Mbps	-92
		54Mbps	-72
	802.11n HT20	MCS0	-90
		MCS7	-70
	802.11n HT40	MCS0	-88
		MCS7	-68
	802.11ac HT20	MCS0	-90
		MCS7	-70

	802.11ac HT40	MCS0	-88
		MCS7	-68
	802.11ac HT80	MCS0	-85
		MCS9	-58
	802.11ax HT20	MCS0	-88
		MCS11	-62
	802.11ax HT40	MCS0	-86
		MCS11	-58
	802.11ax HT80	MCS0	-84
		MCS11	-55

Software	
LAN	Static IP / *DHCP Client
WAN	■ Static IP ■ Dynamic IP ■ PPPoE/PPTP/L2TP
Wireless Modes	Access Point Gateway Repeater
Channel Width	20MHz, 40MHz, 80MHz
Encryption Type	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, WPA/WPA2 Enterprise
Wireless Security	Enable/Disable SSID Broadcast Wireless MAC address filtering User Isolation
Max. SSIDs	8 (4 per radio)
Max. Wireless Clients	150 (100 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

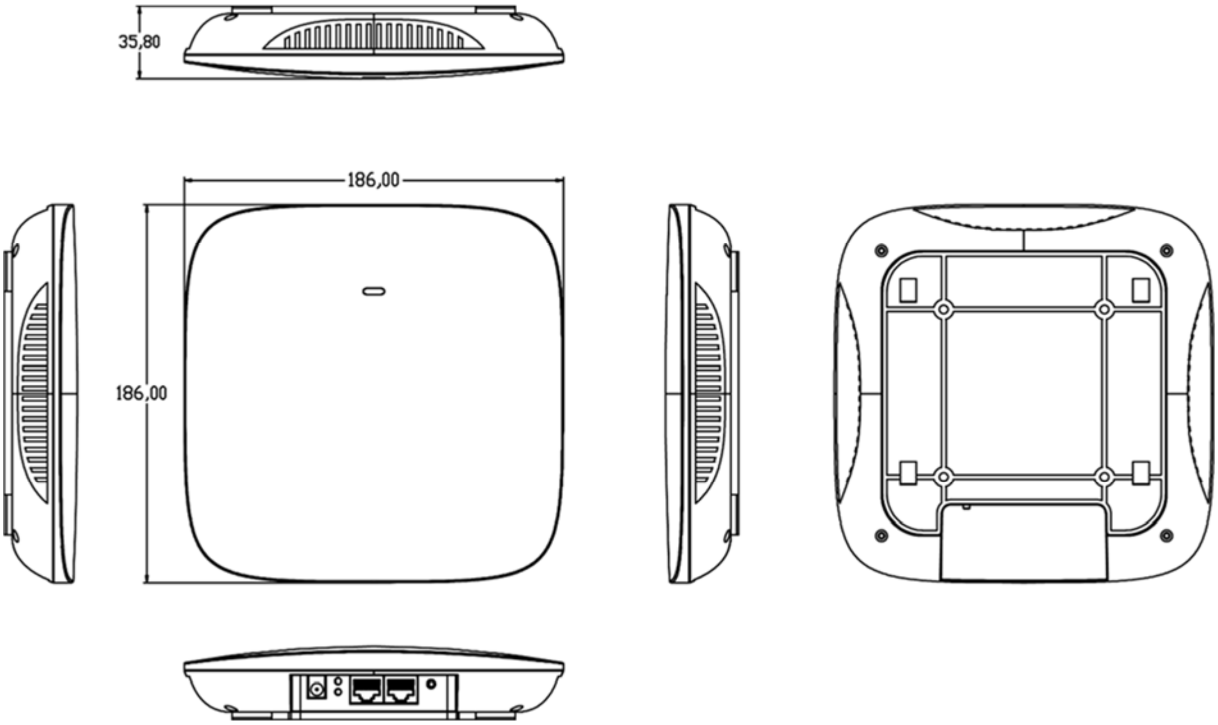
	System Log supports remote syslog server
VLAN	*IEEE 802.1Q VLAN (VID: 1~4094) *SSID-to-VLAN mapping to up to 4 SSIDs
Self-healing	Supports auto reboot settings per day/hour
Management	Remote management through PLANET DDNS/ Easy DDNS Configuration backup and restore Supports UPnP Supports IGMP Proxy Supports PPTP/L2TP/IPSec VPN Pass-through Supports Captive Portal, RADIUS Server/Client
Central Management	Applicable controllers: NMS-500, NMS-1000V, *PLANET CloudViewer App
Remarks [*]: The feature will be supported through firmware/system upgrade.	
Environment & Certification	
Operating Temperature	-40~70 degrees C
Operating Humidity	5~95% (non-condensing)
Storage Temperature	-40 ~ 70 degrees C
Regulatory	CE, RoHS

Chapter 2. Physical Descriptions

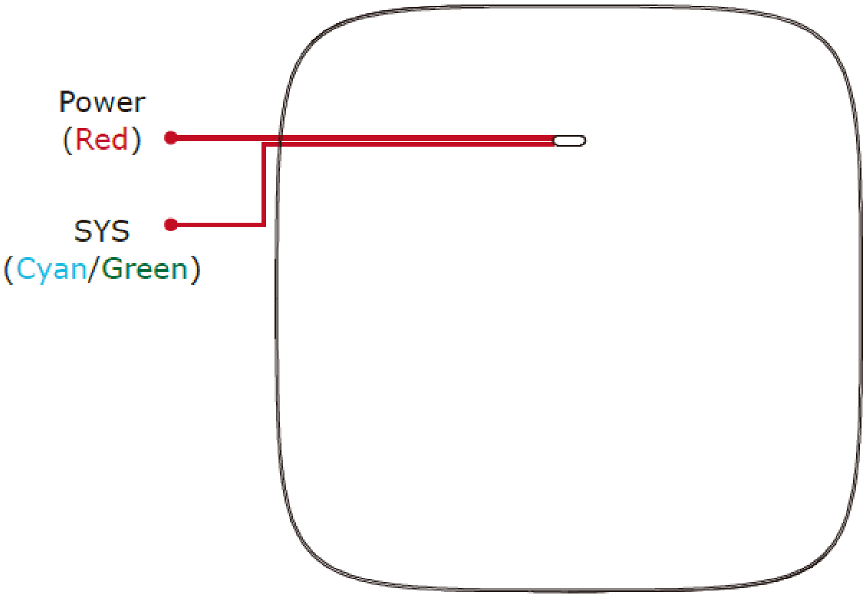
2.1 Product Outlook

WDAP-C1800AX

- **Dimensions:** 186 x 186 x 35.8mm
- **Weight:** 380 ±5GHz
- **Triple Viewing**



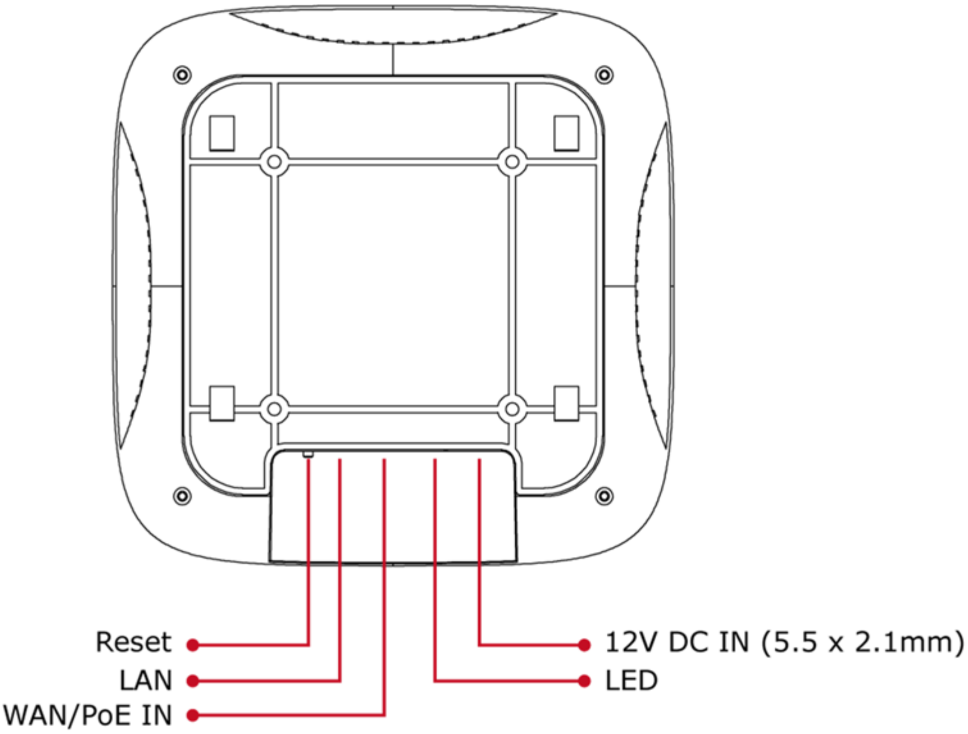
Front View



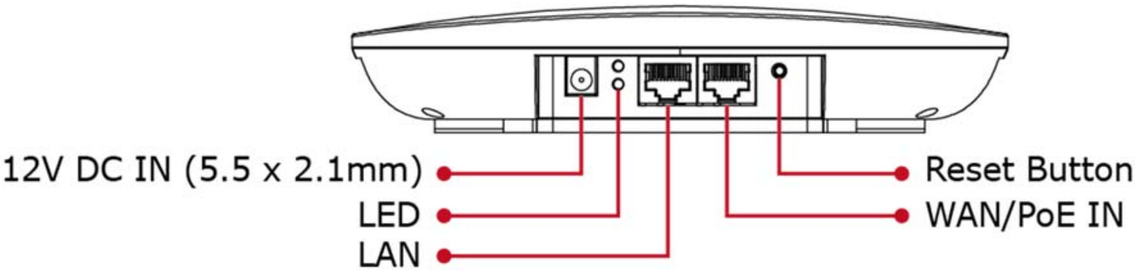
LED Definition

LED	STATUS	FUNCTION
PWR	On (Red)	The access point is on.
	Off	System is operating.
SYS	On	Wireless LAN is initializing.
	Blinking (**Cyan**/**Green**)	2.4GHzHz/5GHzHz wireless LAN is working.

Rear View



Bottom Panel

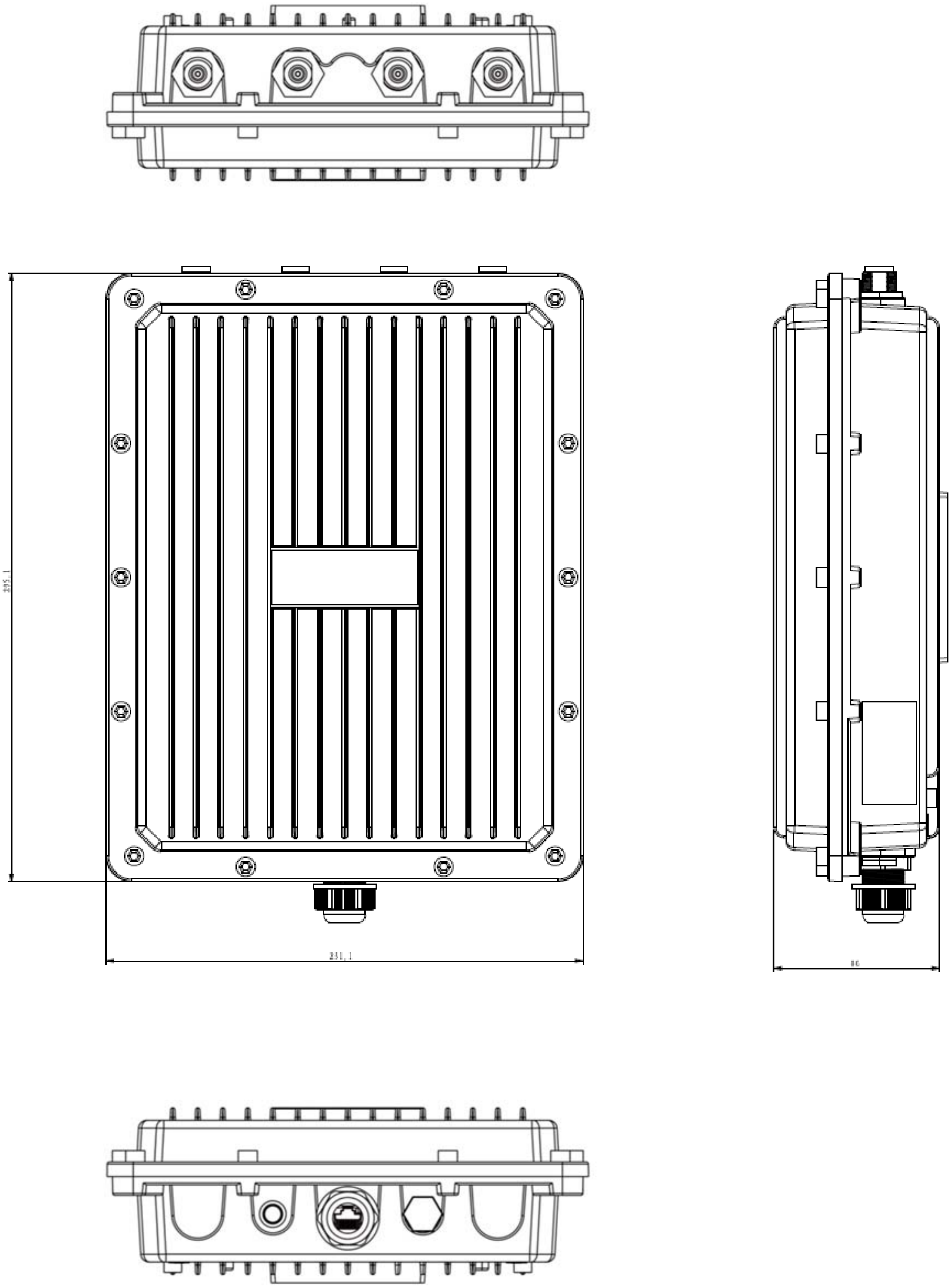


Port definition

Object	Description
12V DC	12V DC port for the power adapter(DC-Jack 5.5 x 2.1mm)
LED	The access point is on.
PoE	LAN port with Power over Ethernet (PoE) IN
LAN	LAN port connecting to the network equipment.
Reset	To restore to the factory default setting, press and hold the Reset Button for about 15 seconds, and then release it.

WDAP-1800AX

- **Dimensions:** 231 x 80 x 295mm
- **Weight:** 2500 ±5GHz
- **Apperance**



Port & Connector

Hardware Interface Definition

Object	Description
Antenna Connectors	4 N-type (female) antenna connectors
PoE LAN Port	10/100/1000Mbps RJ45 port, auto MDI/MDI-X 802.3at PoE+ supported, 48VDC In
Reset Button	Press and hold the **Reset** button for over 5 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. Preparation

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-C1800AX)
- 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, MAC OS 9 or later, Linux, UNIX or other platforms compatible with **TCP/IP** protocols

Note

1. The AP in the following instructions refers to PLANET WDAP-C1800AX. (Please refer to WDAP-1800AX QIG to install the AP)
2. It is recommended to use Internet Explorer 11, Firefox or Chrome to access the AP.

3.2 Hardware Installation Installing the AP

Before installing the AP, make sure your PoE switch is connected to the Internet through the broadband service successfully at this moment. If there is any problem, please contact your local ISP.

Please install the AP according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

Step 1. Take the mounting bracket, put it on the target place by aligning the holes and fix it with the supplied screws.

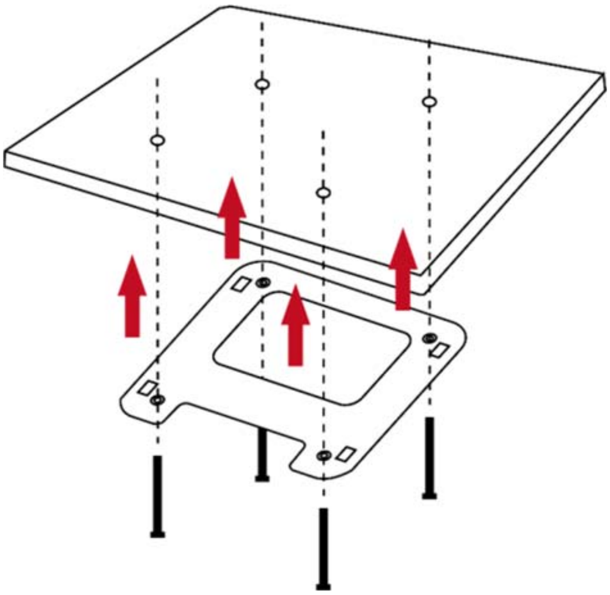


Figure 3-1 Mounting the Bracket

Step 2. Load the device into the mounting bracket, and be sure the device is mated with fixed screws. Then, lock the device in position and plug the Ethernet cable into the WDAP-C1800AX.

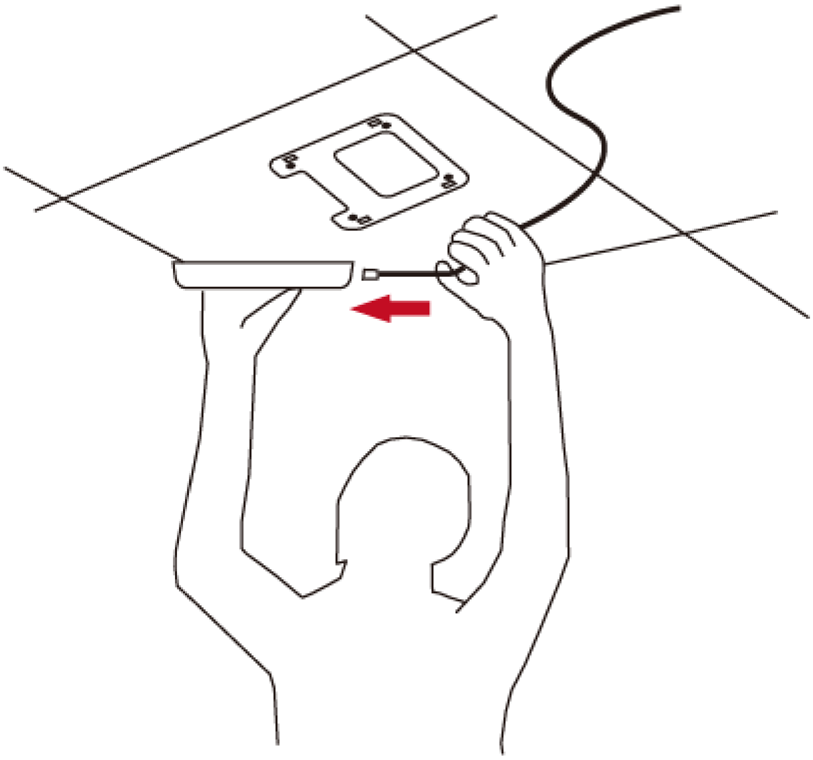


Figure 3-2 Connecting the Ethernet Cable

Step 3. Plug the other end of the Ethernet cable into the PoE switch.

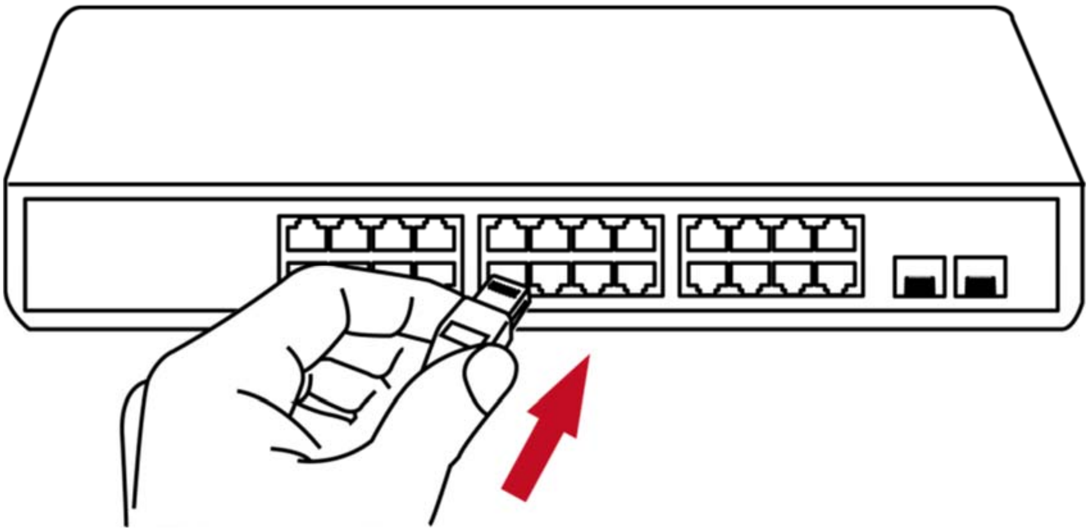


Figure 3-3 Connecting the PoE Injector

3.3 Manual Network Setup -- TCP/IP Configuration

The default IP address of the WDAP-C1800AX is **192.168.1.253**. And the 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-C1800AX 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-C1800AX is powered by a PoE switch.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 10**. 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.

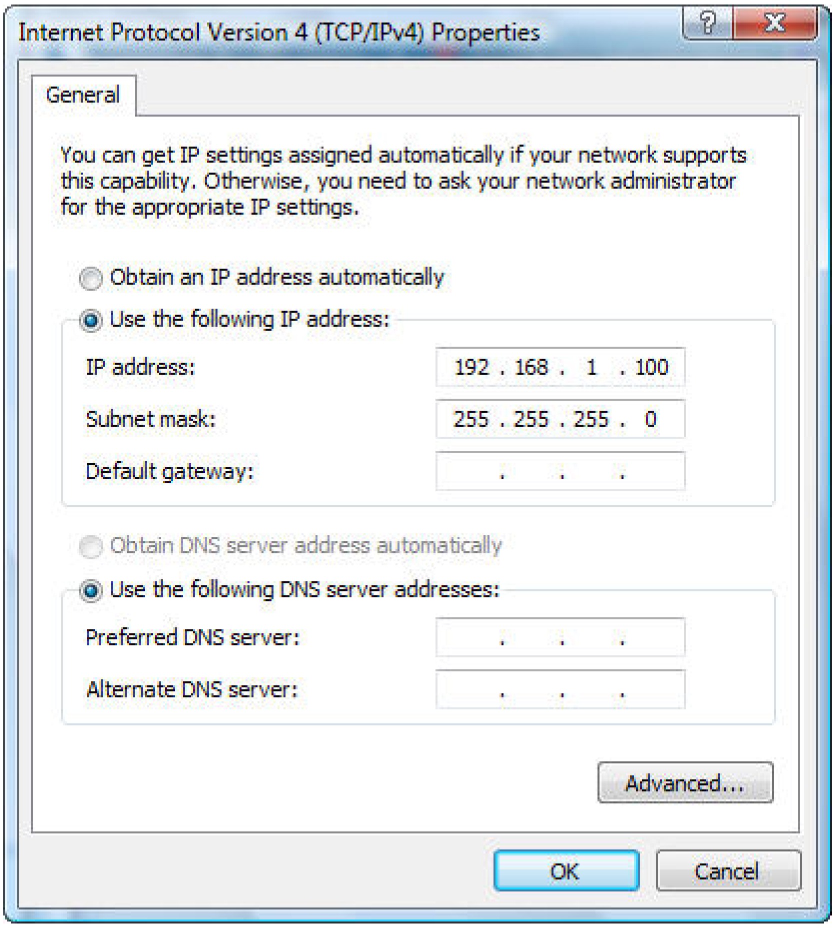
3.3.1 Configuring the IP Address Manually

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-C1800AX 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-C1800AX 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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 3-4 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 10** OS. Please follow the steps below:

1. Click on **Start > Run**.

2. Type “**cmd**” in the Search box.

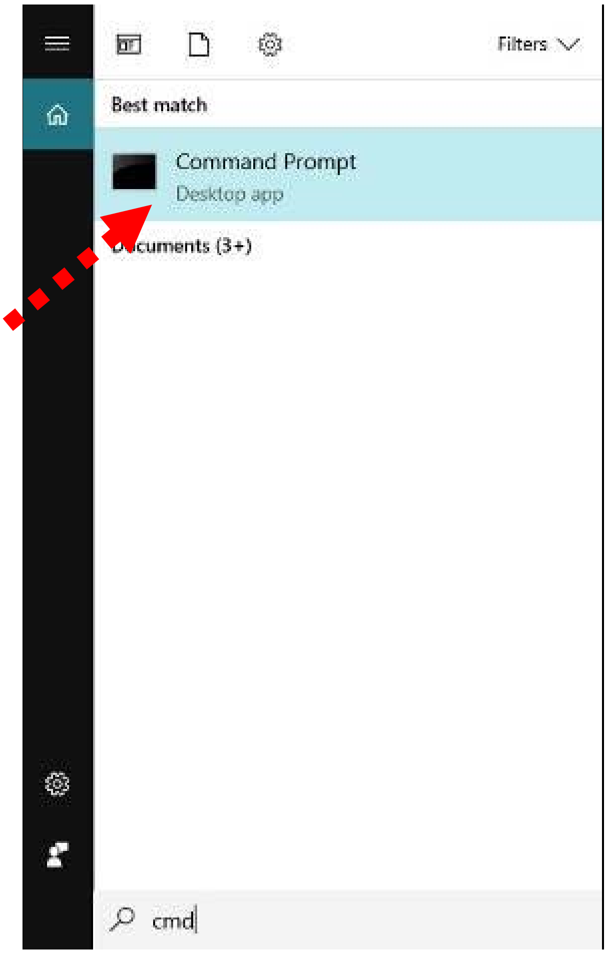
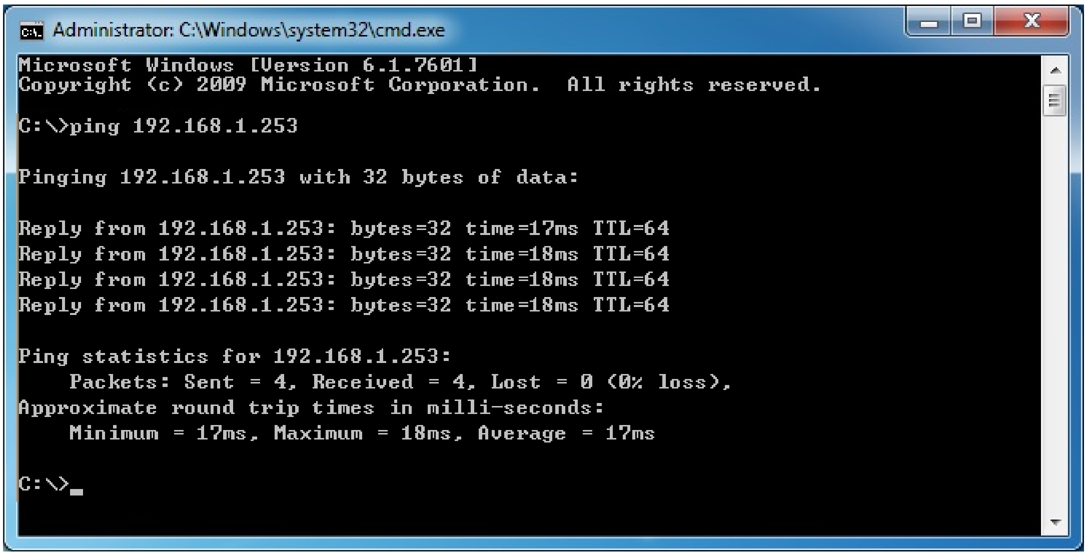


Figure 3-5 Windows Start Menu

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

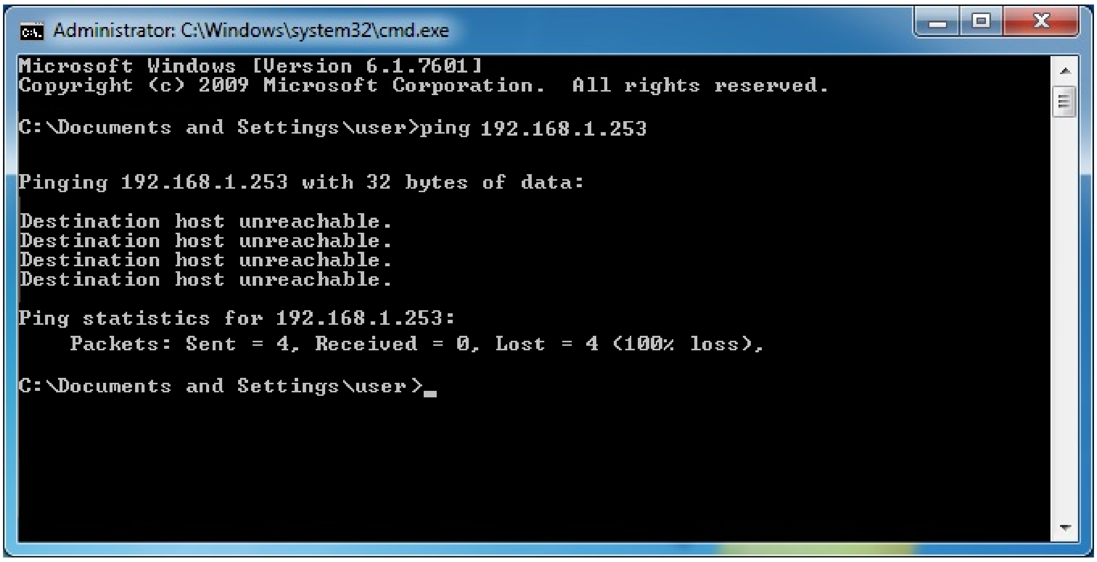
   - If the result displayed is similar to **Figure 4-3**, it means the connection between your PC and the AP has been established well.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time=17ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms

C:\>_
```

Figure 3-6 Successful Result of Ping Command

- If the result displayed is similar to **Figure 4-4**, it means the connection between your PC and the AP has failed.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Documents and Settings\user>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\user>_
```

Figure 3-7 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 http://192.168.1.253 in the web address field of the browser.

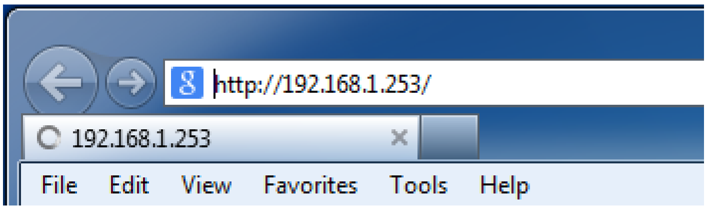


Figure 3-8 Login by Default IP Address

Step 1. When the login window pops up, please enter username and password. The default username and password are "**admin**". Then click the **LOGIN** button to continue.

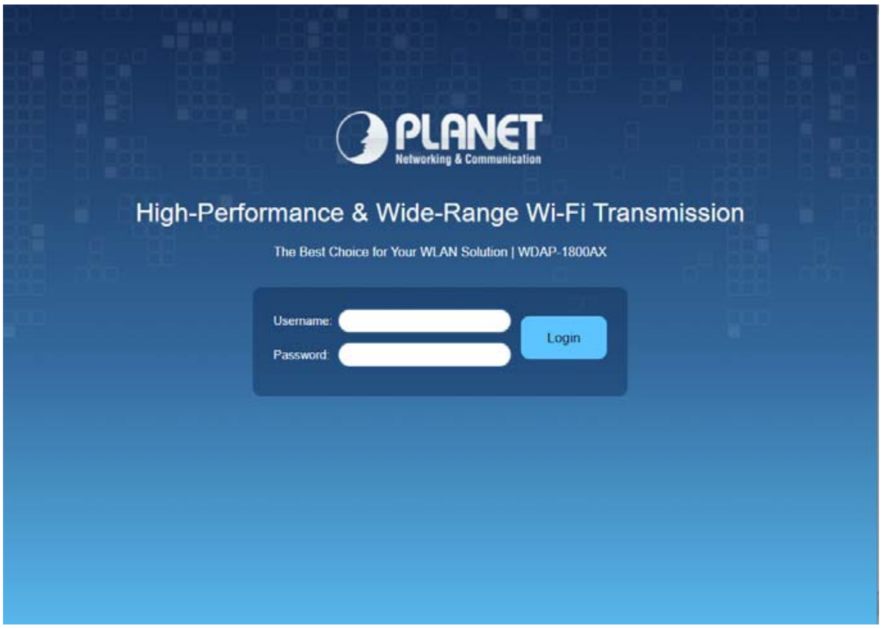

PLANET
Networking & Communication
High-Performance & Wide-Range Wi-Fi Transmission
The Best Choice for Your WLAN Solution | WDAP-1800AX
Username:
Password:
Login

Figure 3-9 Login Window

Default IP Address: **192.168.1.253**

Default Password: **admin**

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-C1800AX in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution.

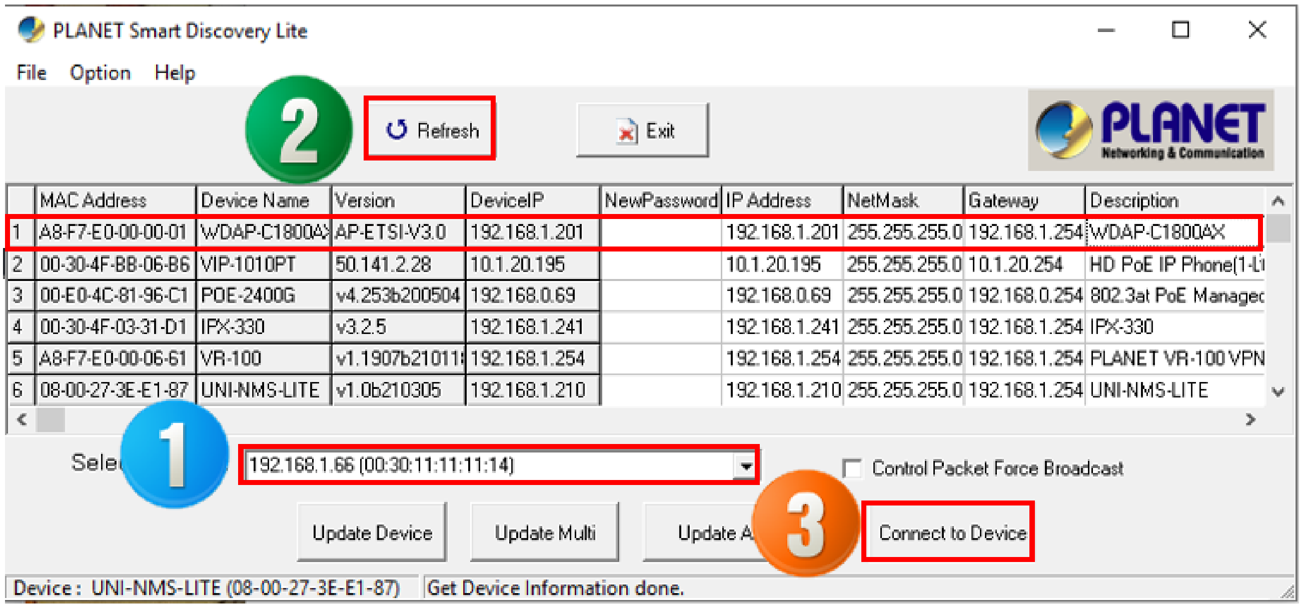
The following installation instructions guide you to running the Planet Smart Discovery Utility.

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

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

Planet_Utility.exe
PLANET Corp.

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



	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description
1	A8-F7-E0-00-00-01	WDAP-C1800A)	AP-ETSI-V3.0	192.168.1.201		192.168.1.201	255.255.255.0	192.168.1.254	WDAP-C1800AX
2	00-30-4F-BB-06-B6	VIP-1010PT	50.141.2.28	10.1.20.195		10.1.20.195	255.255.255.0	10.1.20.254	HD PoE IP Phone(1-Li
3	00-E0-4C-81-96-C1	POE-2400G	v4.253b200504	192.168.0.69		192.168.0.69	255.255.255.0	192.168.0.254	802.3at PoE Managec
4	00-30-4F-03-31-D1	IPX-330	v3.2.5	192.168.1.241		192.168.1.241	255.255.255.0	192.168.1.254	IPX-330
5	A8-F7-E0-00-06-61	VR-100	v1.1907b21011!	192.168.1.254		192.168.1.254	255.255.255.0	192.168.1.254	PLANET VR-100 VPN
6	08-00-27-3E-E1-87	UNI-NMS-LITE	v1.0b210305	192.168.1.210		192.168.1.210	255.255.255.0	192.168.1.254	UNI-NMS-LITE

192.168.1.66 (00:30:11:11:11:14)

□ Control Packet Force Broadcast

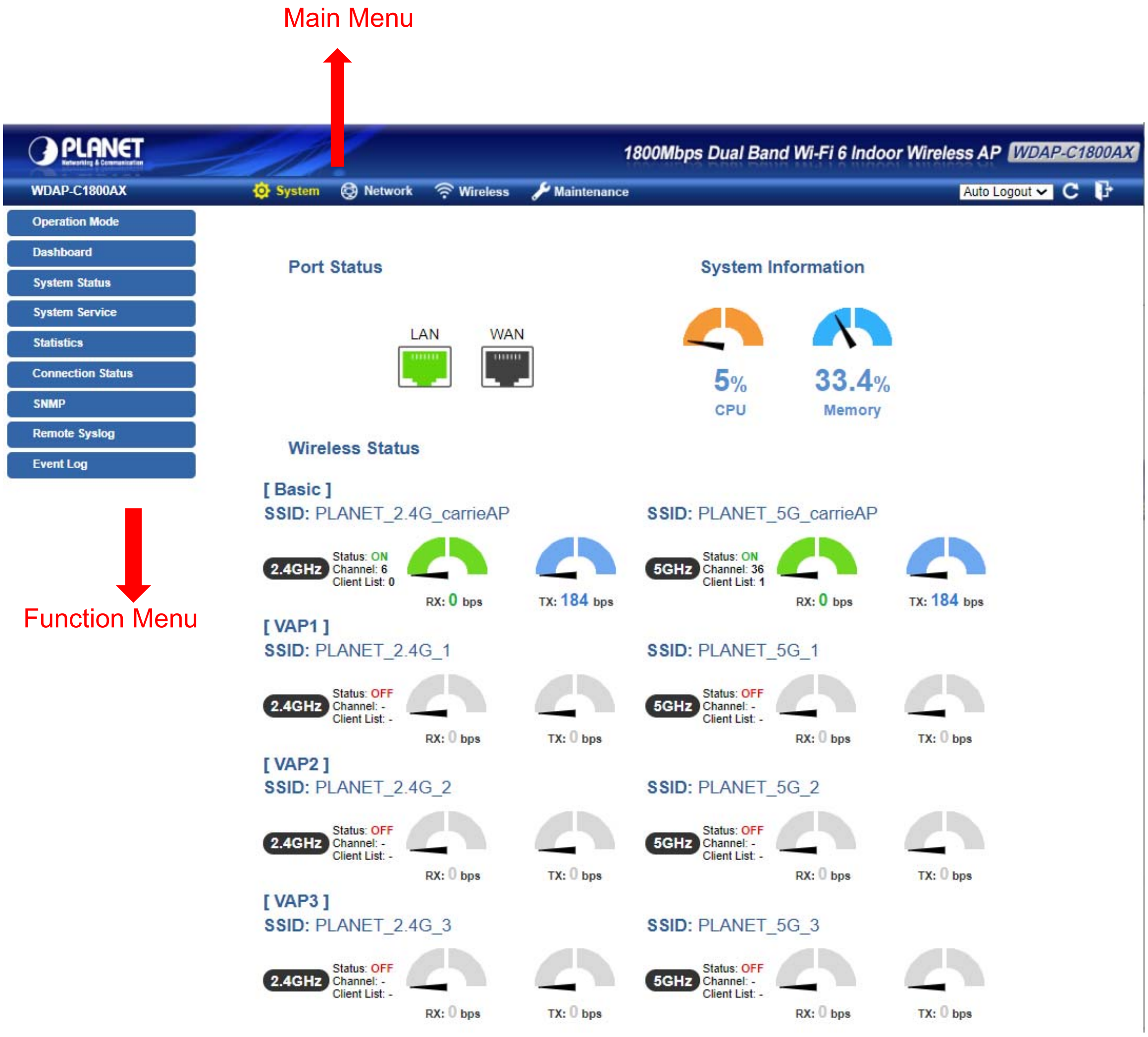
Device : UNI-NMS-LITE (08-00-27-3E-E1-87) Get Device Information done.

Step 3: 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-C1800AX as an example.)**



[Basic]
SSID: PLANET_2.4G_carrieAP — 2.4GHz Status: ON Channel: 6 Client List: 0 — RX: 0 bps TX: 184 bps
SSID: PLANET_5G_carrieAP — 5GHz Status: ON Channel: 36 Client List: 1 — RX: 0 bps TX: 184 bps

[VAP1]
SSID: PLANET_2.4G_1 — 2.4GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps
SSID: PLANET_5G_1 — 5GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps

[VAP2]
SSID: PLANET_2.4G_2 — 2.4GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps
SSID: PLANET_5G_2 — 5GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps

[VAP3]
SSID: PLANET_2.4G_3 — 2.4GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps
SSID: PLANET_5G_3 — 5GHz Status: OFF Channel: - Client List: - — RX: 0 bps TX: 0 bps

Figure 4-1 Main Web Page

■ Main Menu

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown in Figures 4-2 and 4-3.

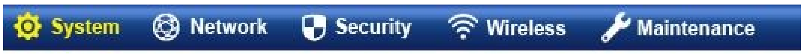


Figure 4-2: Function Menu

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.

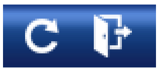


Figure 4-3: Function Button

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.

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.

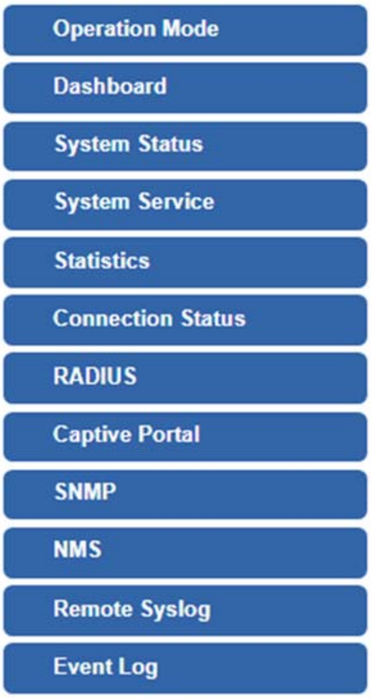


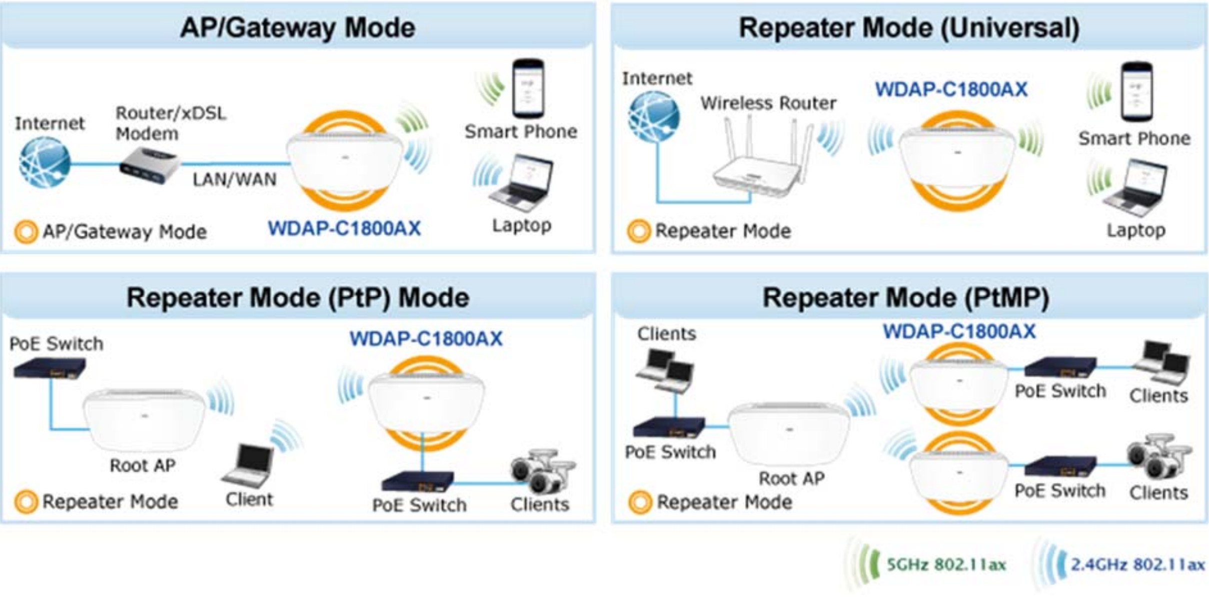
Figure 4-4: System Menu

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-C1800AX in a different mode, including AP, gateway and repeater modes.



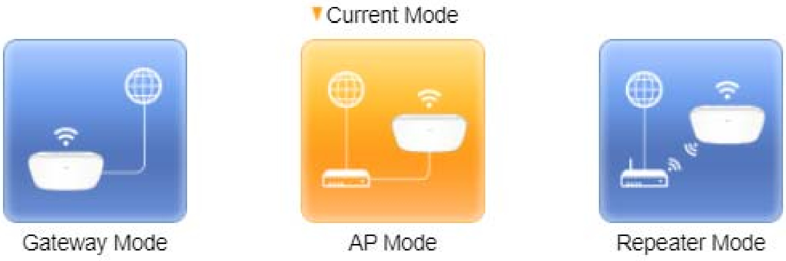


Figure 4-5 Operation Mode

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.

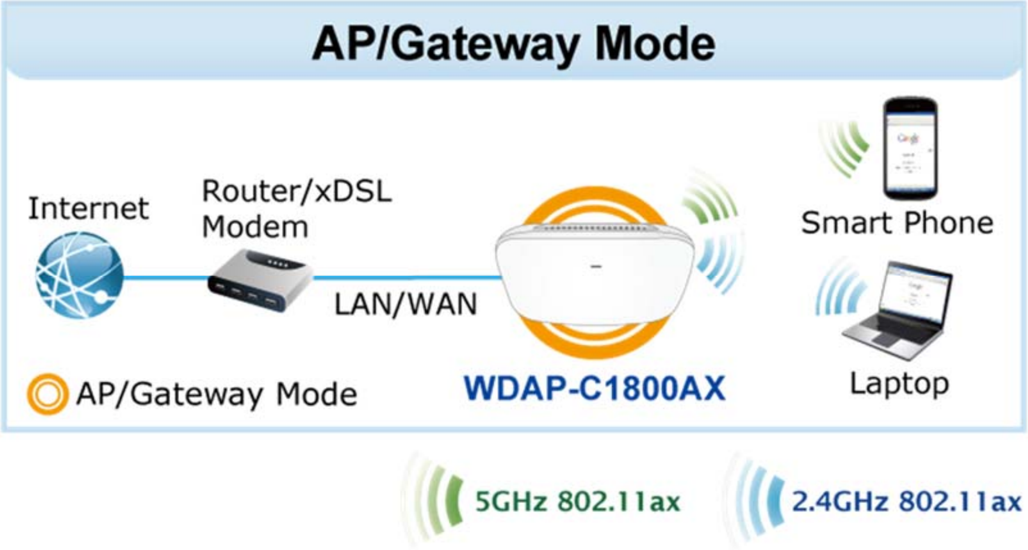
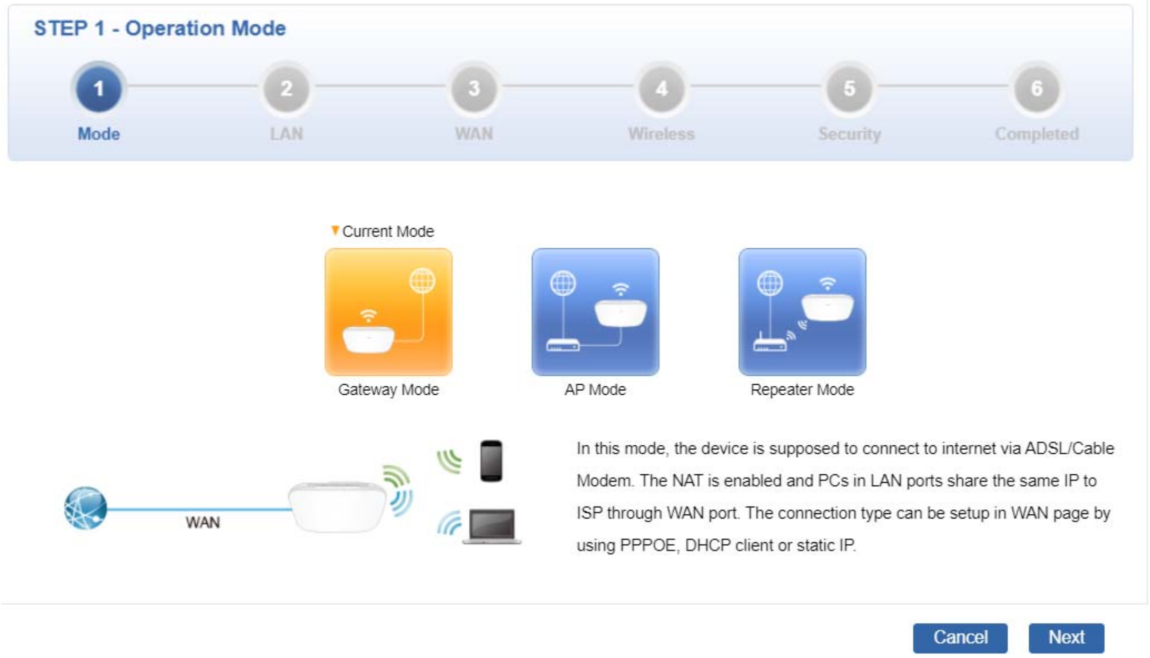


Figure 4-6: Setup Wizard

Step 1: Operation Mode

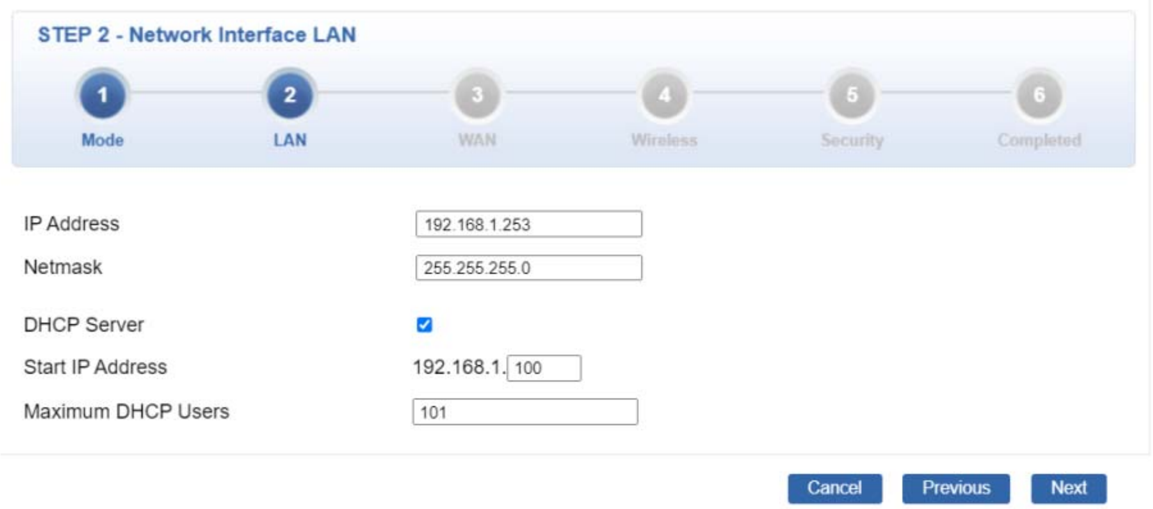
Select operation Mode.



In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 4-7.



IP Address 192.168.1.253

Netmask 255.255.255.0

DHCP Server ☑

Start IP Address 192.168.1.100

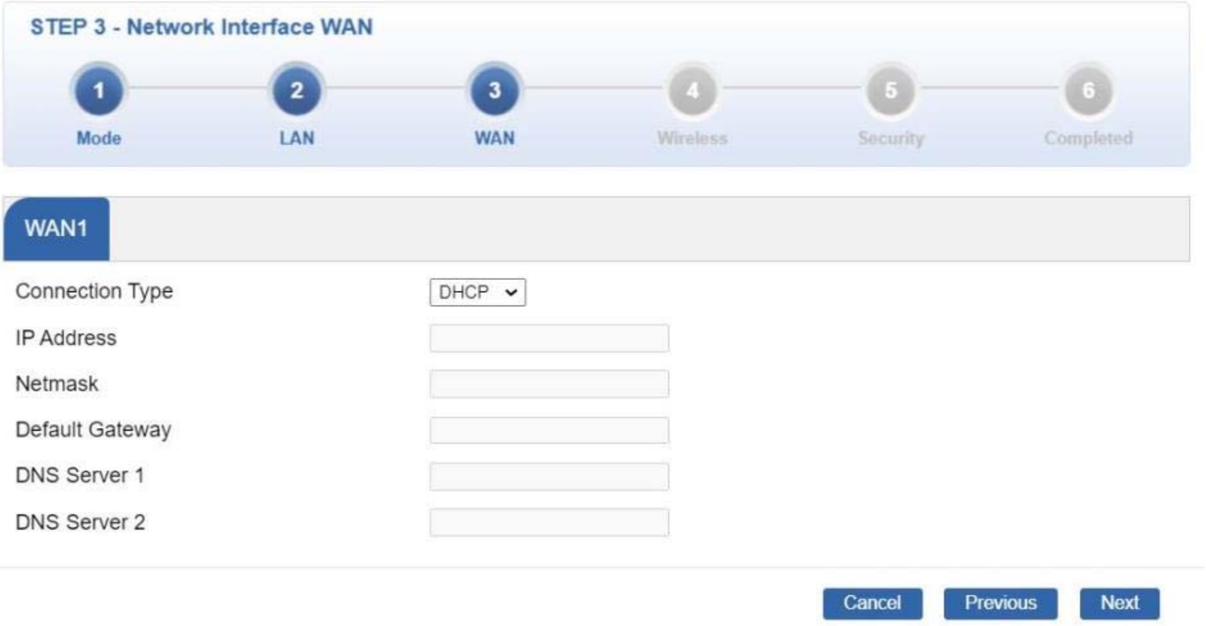
Maximum DHCP Users 101

Figure 4-7: 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 4-8



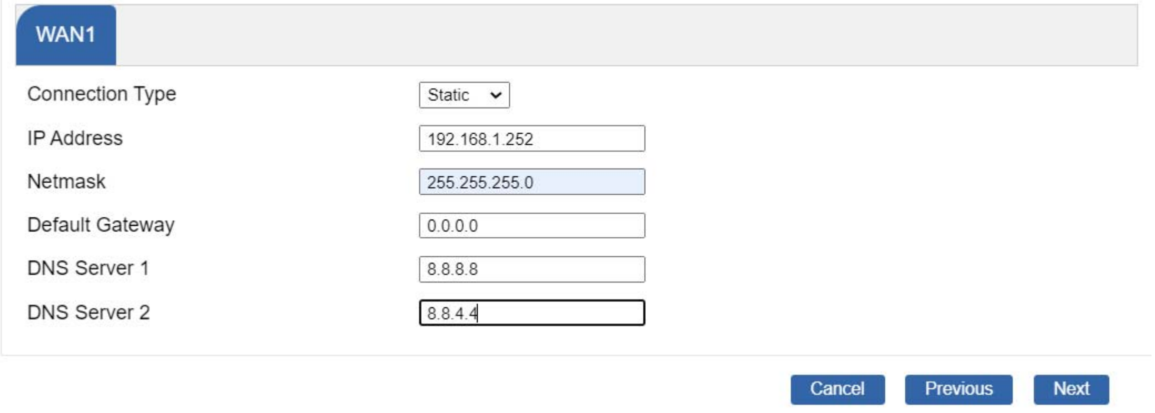
STEP 3 - Network Interface WAN

Connection Type	DHCP
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

Figure 4-8: 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 4-9.



Connection Type	Static
IP Address	192.168.1.252
Netmask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4

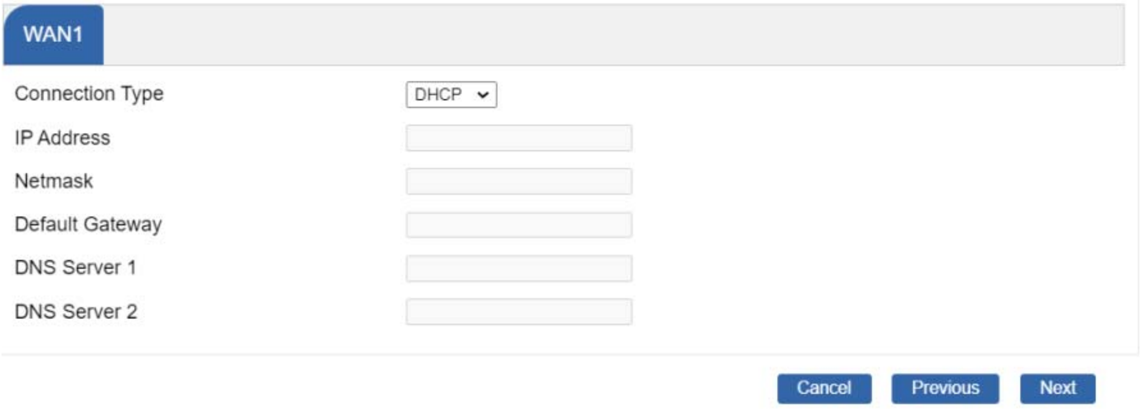
Figure 4-9: WAN Interface Setup – Static IP Setup

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 4-10.



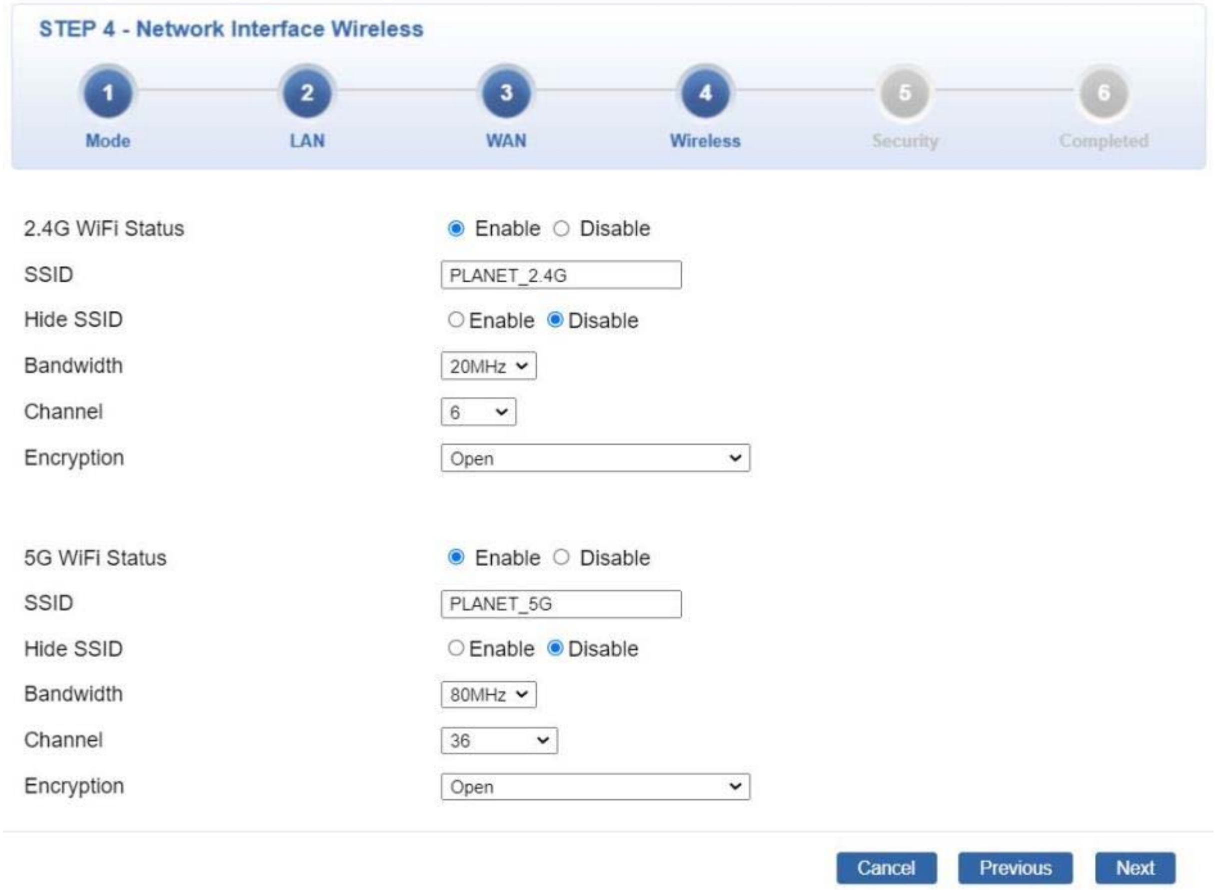
WAN1

Connection Type: DHCP
IP Address:
Netmask:
Default Gateway:
DNS Server 1:
DNS Server 2:

Figure 4-10: WAN Interface Setup – DHCP Setup

Step 4: Network Interface Wireless

Set up the Security Settings as shown in Figure 4-11.

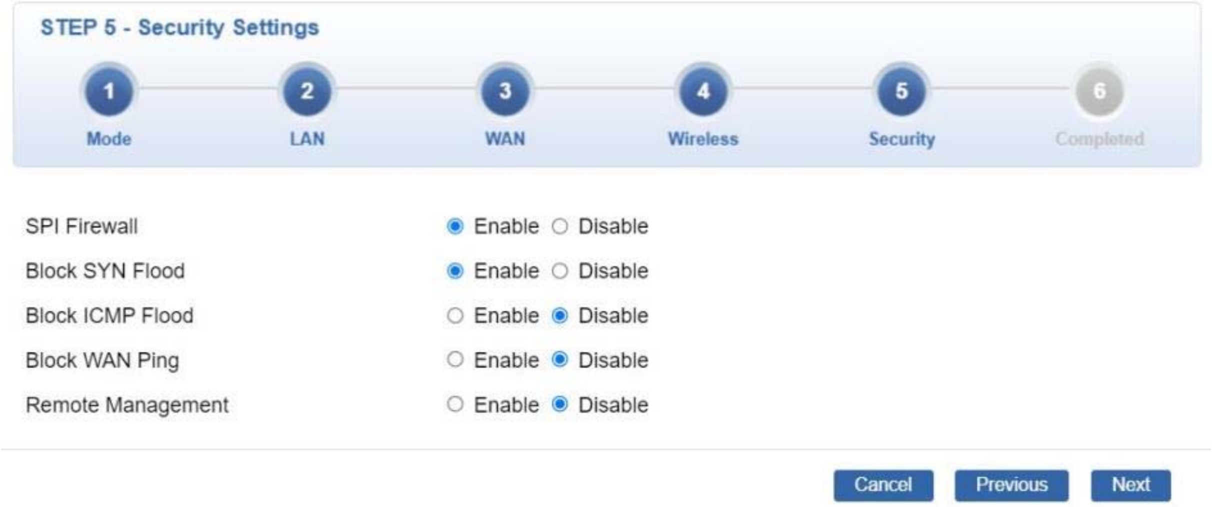


2.4G WiFi Status	● Enable ○ Disable
SSID	PLANET_2.4G
Hide SSID	○ Enable ● Disable
Bandwidth	20MHz
Channel	6
Encryption	Open
5G WiFi Status	● Enable ○ Disable
SSID	PLANET_5G
Hide SSID	○ Enable ● Disable
Bandwidth	80MHz
Channel	36
Encryption	Open

Figure 4-11: Network Setup

Step 5: Security Setting

Set up the Security Settings as shown in Figure 4-12.



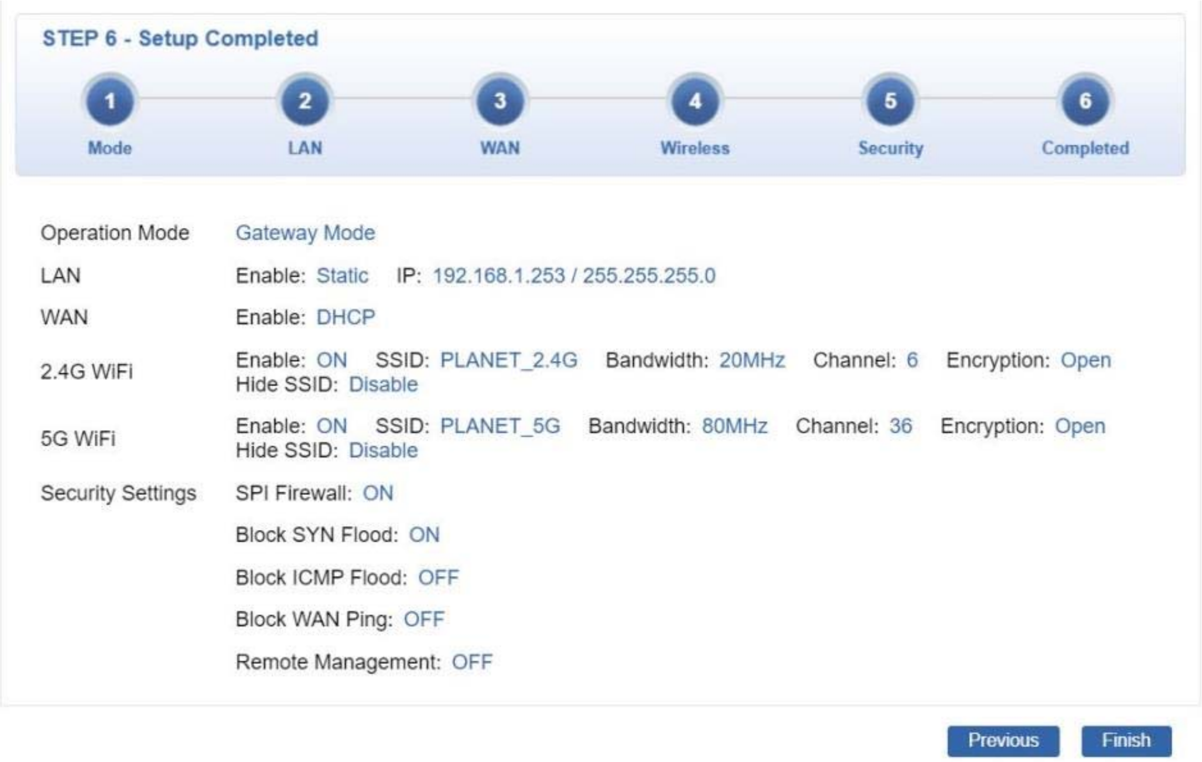
SPI Firewall	● Enable ○ Disable
Block SYN Flood	● Enable ○ Disable
Block ICMP Flood	○ Enable ● Disable
Block WAN Ping	○ Enable ● Disable
Remote Management	○ Enable ● Disable

Figure 4-12: 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 6: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in Figure 4-13.



Operation Mode: Gateway Mode

LAN: Enable: Static IP: 192.168.1.253 / 255.255.255.0

WAN: Enable: DHCP

2.4G WiFi: Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHz Channel: 6 Encryption: Open Hide SSID: Disable

5G WiFi: Enable: ON SSID: PLANET_5G Bandwidth: 80MHz Channel: 36 Encryption: Open Hide SSID: Disable

Security Settings: SPI Firewall: ON

Block SYN Flood: ON

Block ICMP Flood: OFF

Block WAN Ping: OFF

Remote Management: OFF

Figure 4-13: 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 4-14.

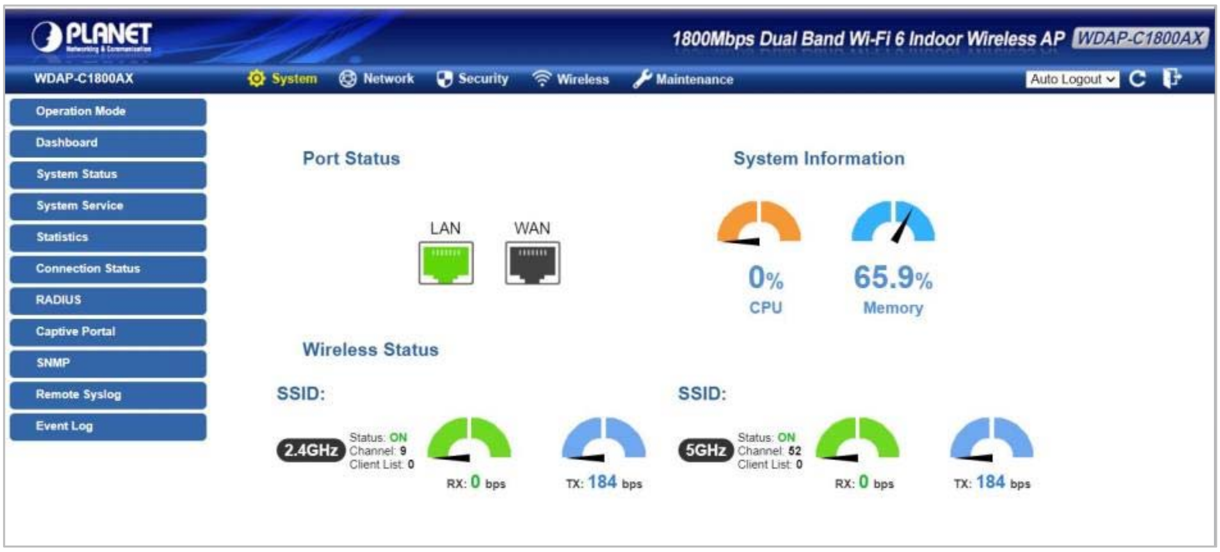


Figure 4-14: Dashboard

Port Status

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

Wireless Status

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

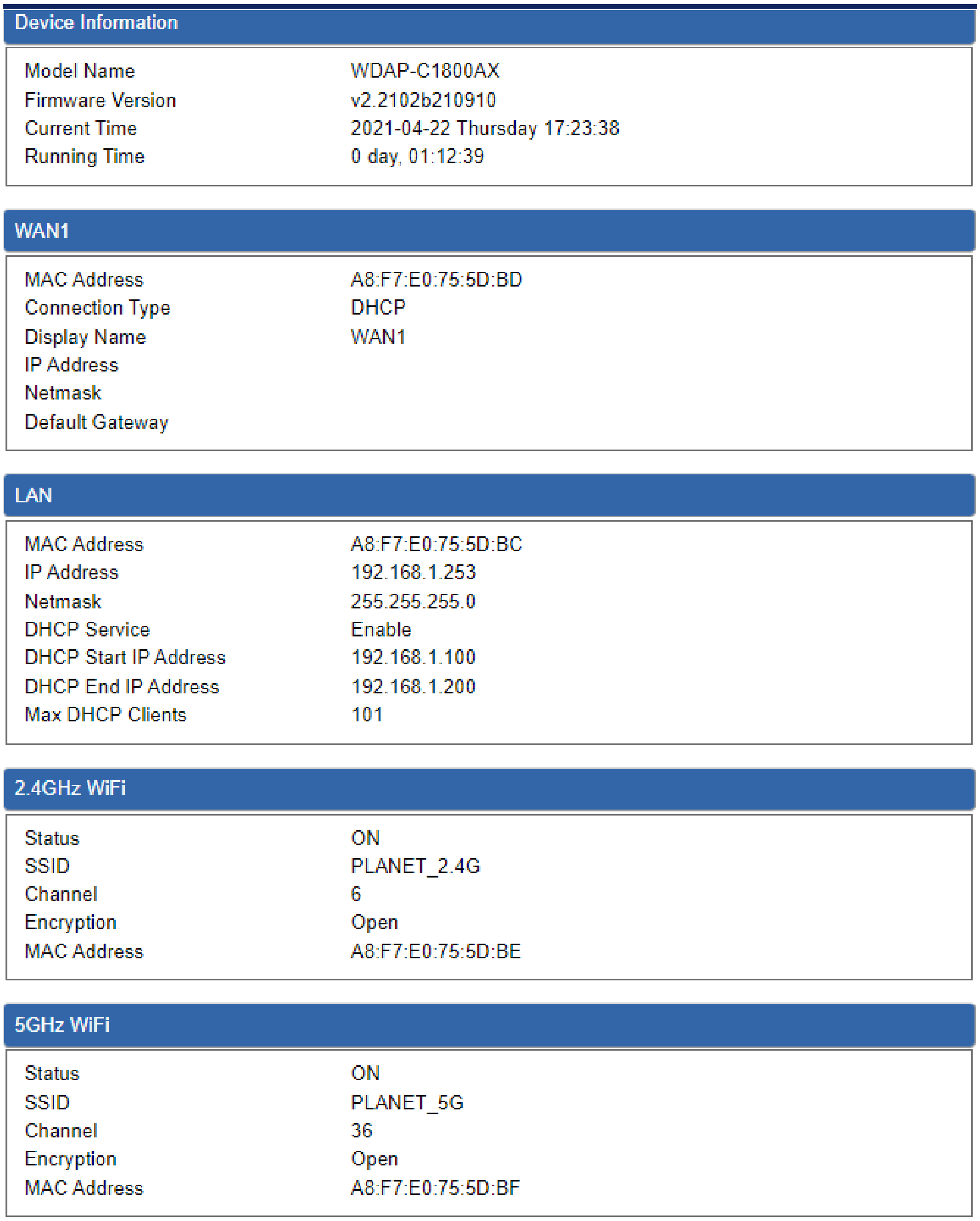
System Information

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 4-15.



Device Information

Model Name	WDAP-C1800AX
Firmware Version	v2.2102b210910
Current Time	2021-04-22 Thursday 17:23:38
Running Time	0 day, 01:12:39

WAN1

MAC Address	A8:F7:E0:75:5D:BD
Connection Type	DHCP
Display Name	WAN1
IP Address	
Netmask	
Default Gateway	

LAN

MAC Address	A8:F7:E0:75:5D:BC
IP Address	192.168.1.253
Netmask	255.255.255.0
DHCP Service	Enable
DHCP Start IP Address	192.168.1.100
DHCP End IP Address	192.168.1.200
Max DHCP Clients	101

2.4GHz WiFi

Status	ON
SSID	PLANET_2.4G
Channel	6
Encryption	Open
MAC Address	A8:F7:E0:75:5D:BE

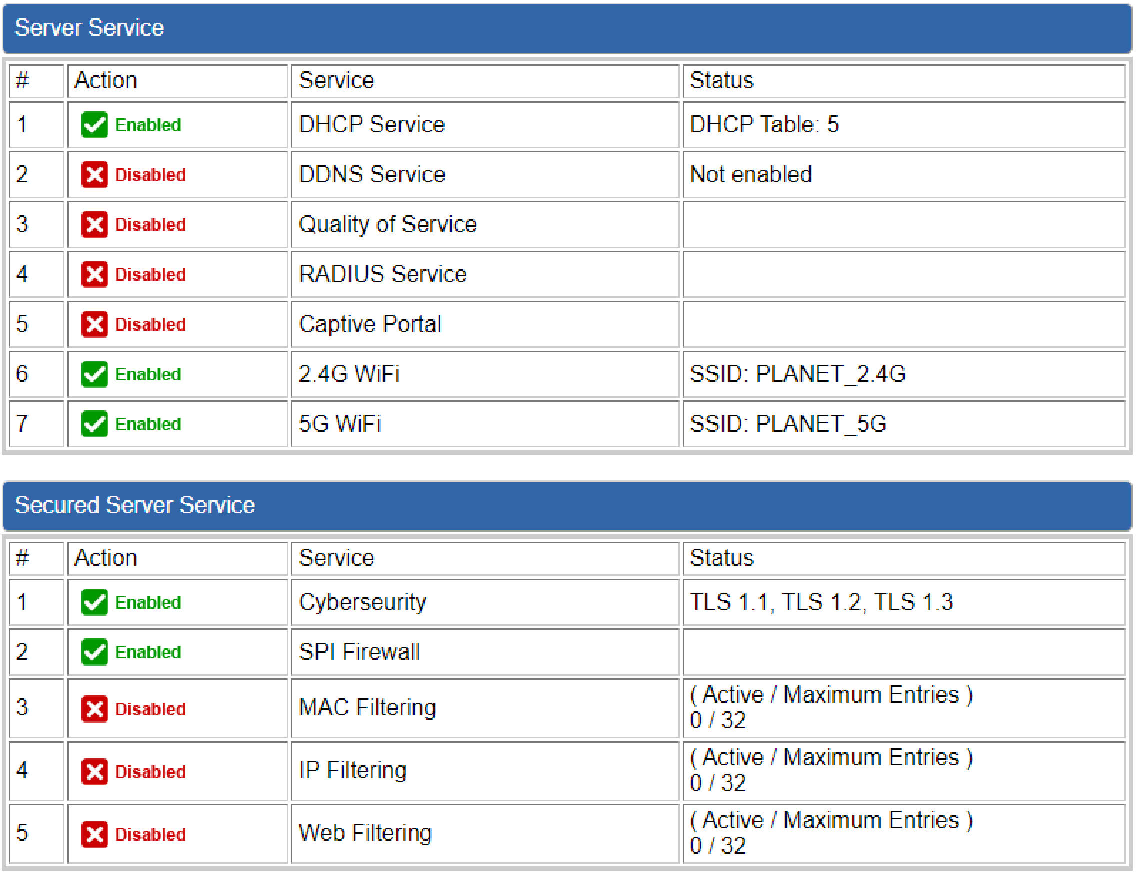
5GHz WiFi

Status	ON
SSID	PLANET_5G
Channel	36
Encryption	Open
MAC Address	A8:F7:E0:75:5D:BF

Figure 4-15: 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 4-16.



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 4-16: 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 4-17.

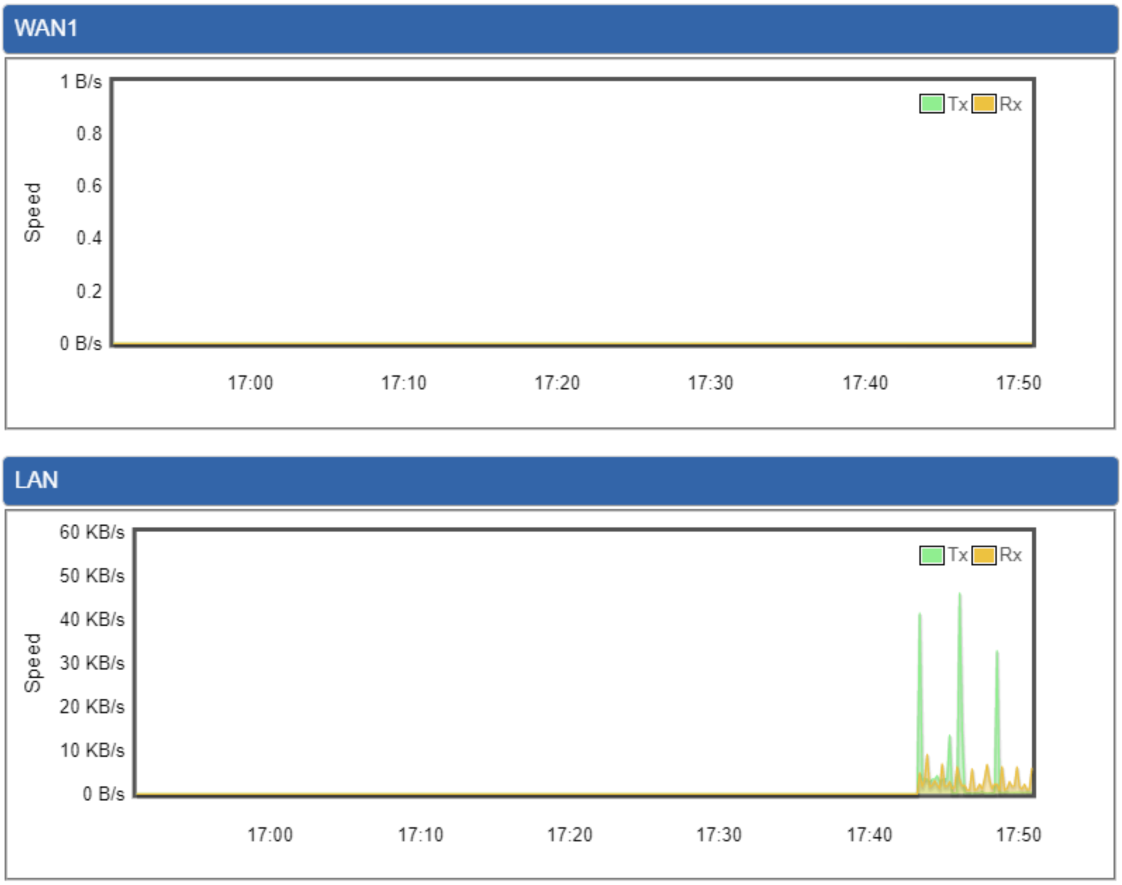
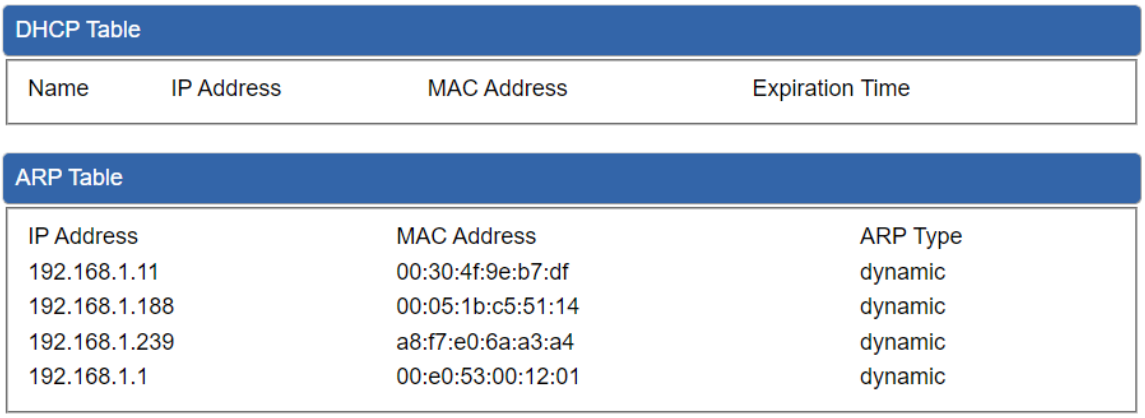


Figure 4-17: Statistics

4.1.7 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in Figure 4-18.



DHCP Table

Name	IP Address	MAC Address	Expiration Time

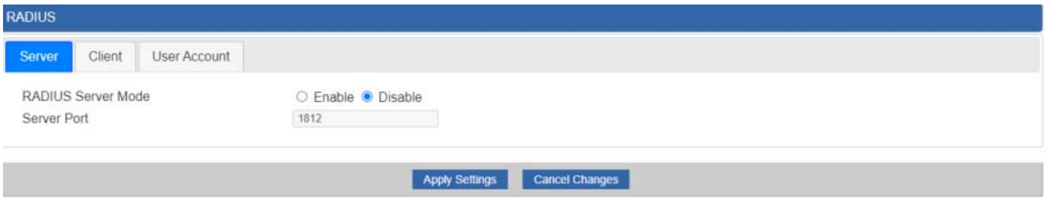
ARP Table

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 4-18: 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 4-19.



RADIUS Server Mode ○ Enable ● Disable

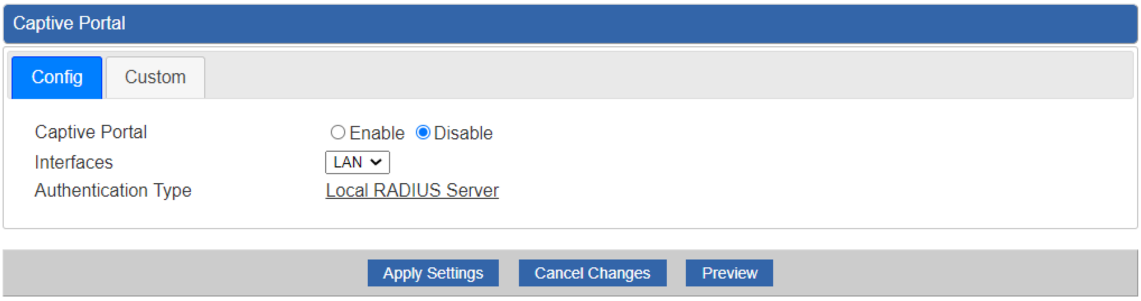
Server Port 1812

Figure 4-19: 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 4-20.



Captive Portal ○ Enable ● Disable

Interfaces LAN

Authentication Type Local RADIUS Server

Figure 4-20: Captive Portal

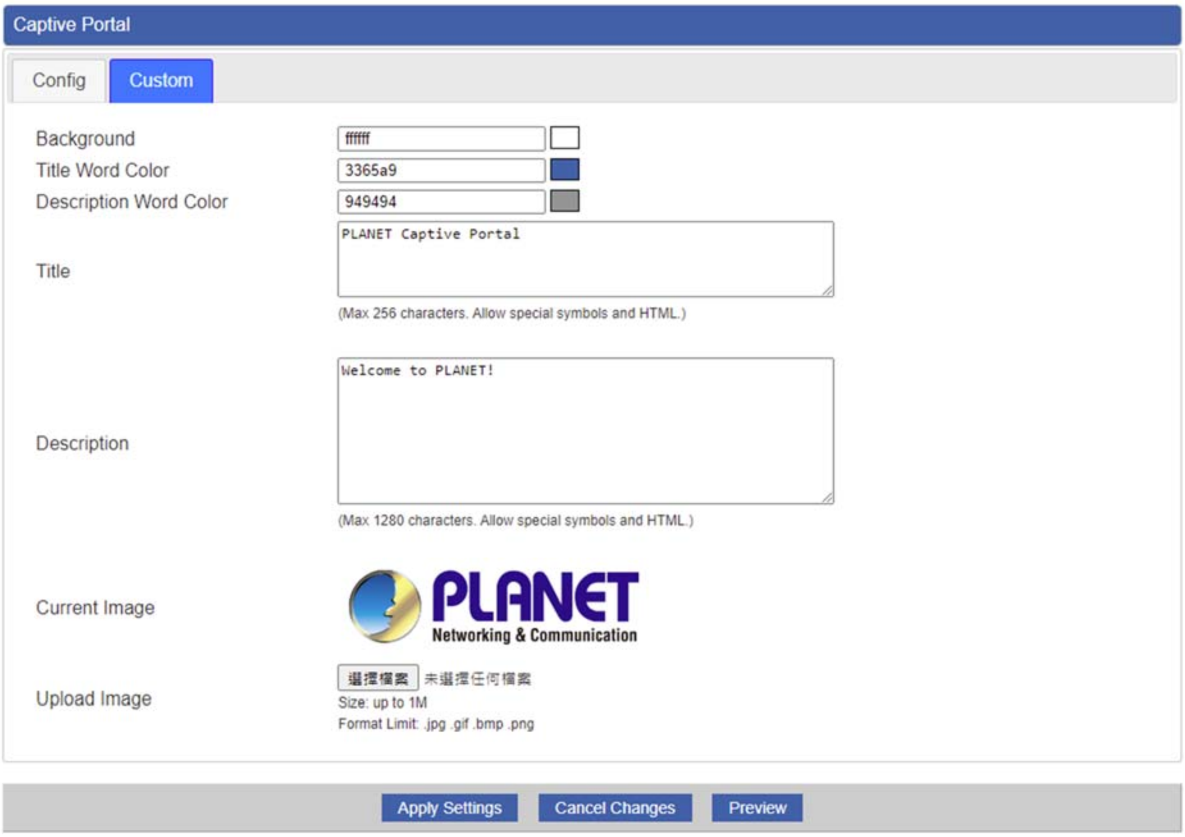
Object	Description
Captive Portal	Disable or enable the Captive Portal function. The default configuration is disabled.

Note

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

Customizing the Custom Captive Portal Web Page

1. Click **Custom**

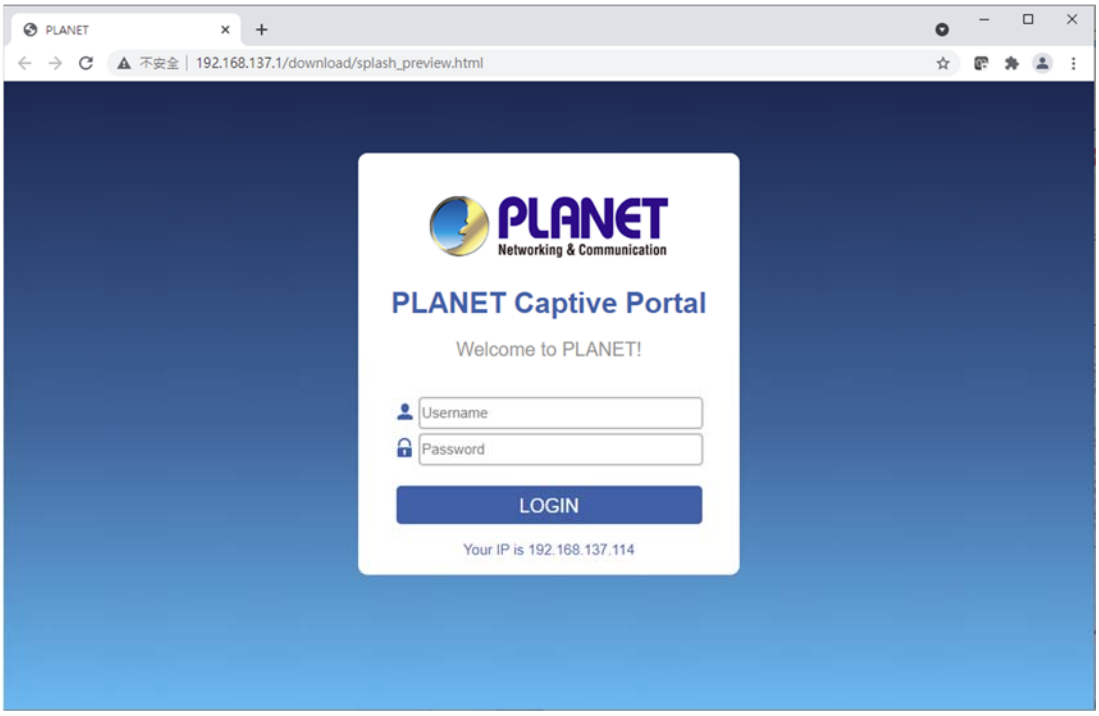


Captive Portal

Config | Custom

Background	ffffff
Title Word Color	3365a9
Description Word Color	949494
Title	PLANET Captive Portal (Max 256 characters. Allow special symbols and HTML.)
Description	Welcome to PLANET! (Max 1280 characters. Allow special symbols and HTML.)
Current Image	
Upload Image	選擇檔案 未選擇任何檔案 Size: up to 1M Format Limit: .jpg .gif .bmp .png

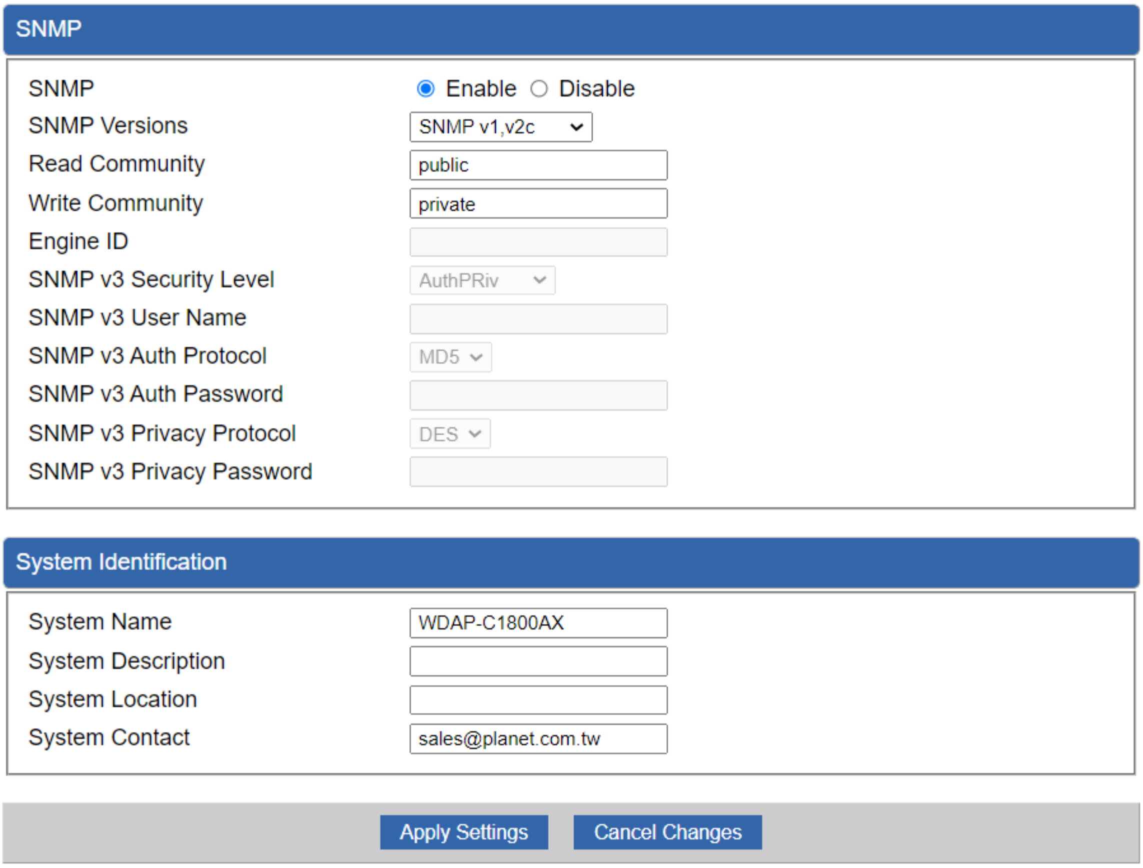
2. After configure and upload image, click **Apply Settings** button
3. Click **Preview** to check the Captive Portal login page



PLANET
不安全 | 192.168.137.1/download/splash_preview.html
PLANET Captive Portal
Welcome to PLANET!
Username
Password
LOGIN
Your IP is 192.168.137.114

4.1.10 SNMP

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



SNMP

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

System Identification

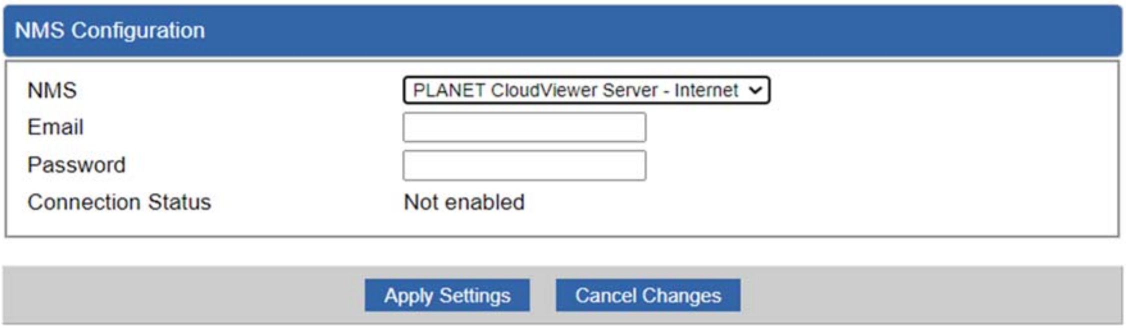
System Name	WDAP-C1800AX
System Description	
System Location	
System Contact	sales@planet.com.tw

Figure 4-21: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the 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 CloudViewer Server – Internet screens – is shown in Figure 4-22.


NMS Configuration

NMS: PLANET CloudViewer Server - Internet

Email:

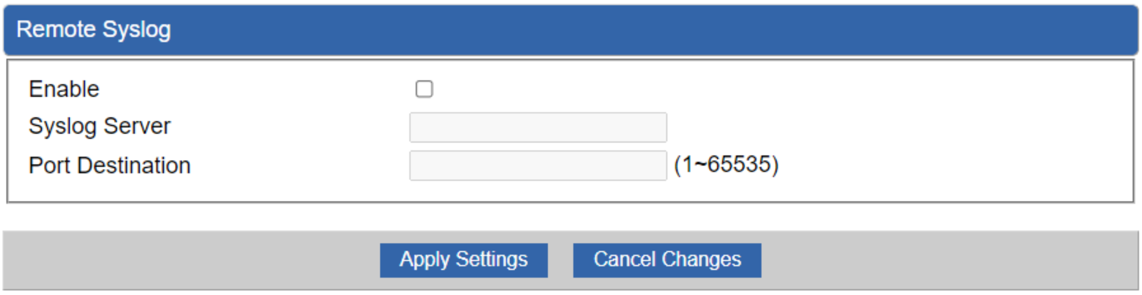
Password:

Connection Status: Not enabled

Figure 4-22: CloudViewer Server

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

4.1.12 Remote Syslog


Remote Syslog

Enable: □

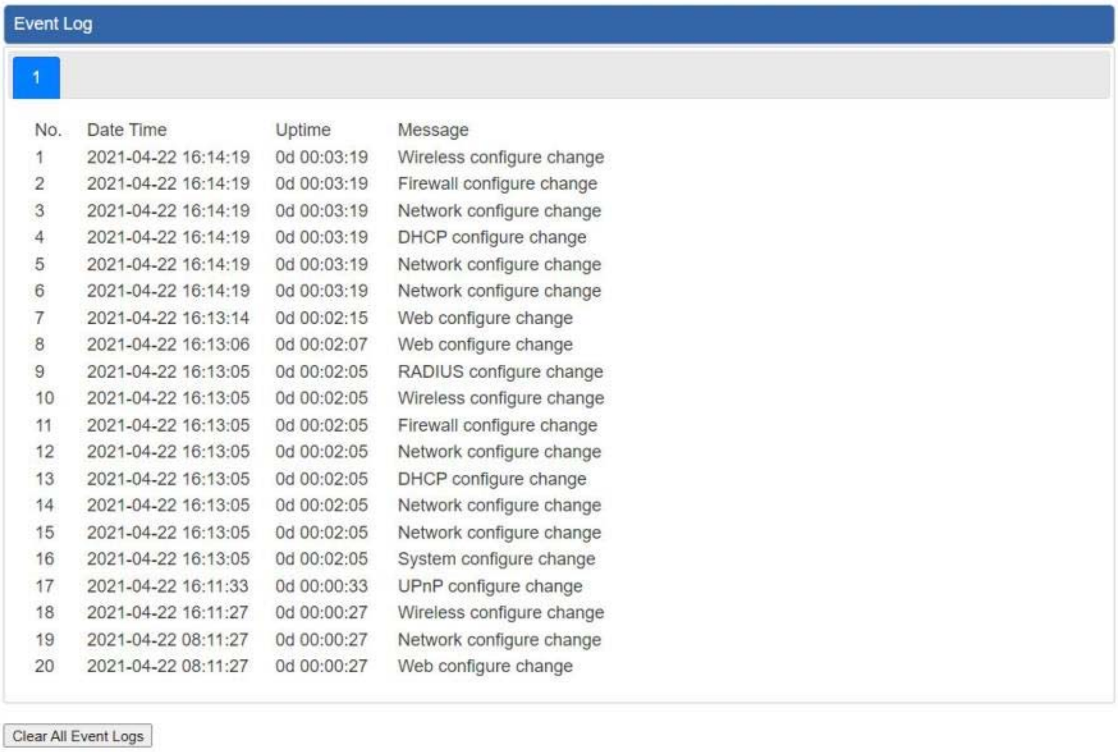
Syslog Server:

Port Destination: (1~65535)

Figure 4-23: Remote Syslog

Object	Description
Enable Remote Syslog	Enable Captive Portal on routers

4.1.13 Event Log



No.	Date Time	Uptime	Message
1	2021-04-22 16:14:19	0d 00:03:19	Wireless configure change
2	2021-04-22 16:14:19	0d 00:03:19	Firewall configure change
3	2021-04-22 16:14:19	0d 00:03:19	Network configure change
4	2021-04-22 16:14:19	0d 00:03:19	DHCP configure change
5	2021-04-22 16:14:19	0d 00:03:19	Network configure change
6	2021-04-22 16:14:19	0d 00:03:19	Network configure change
7	2021-04-22 16:13:14	0d 00:02:15	Web configure change
8	2021-04-22 16:13:06	0d 00:02:07	Web configure change
9	2021-04-22 16:13:05	0d 00:02:05	RADIUS configure change
10	2021-04-22 16:13:05	0d 00:02:05	Wireless configure change
11	2021-04-22 16:13:05	0d 00:02:05	Firewall configure change
12	2021-04-22 16:13:05	0d 00:02:05	Network configure change
13	2021-04-22 16:13:05	0d 00:02:05	DHCP configure change
14	2021-04-22 16:13:05	0d 00:02:05	Network configure change
15	2021-04-22 16:13:05	0d 00:02:05	Network configure change
16	2021-04-22 16:13:05	0d 00:02:05	System configure change
17	2021-04-22 16:11:33	0d 00:00:33	UPnP configure change
18	2021-04-22 16:11:27	0d 00:00:27	Wireless configure change
19	2021-04-22 08:11:27	0d 00:00:27	Network configure change
20	2021-04-22 08:11:27	0d 00:00:27	Web configure change

Figure 4-24: 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 4-25.

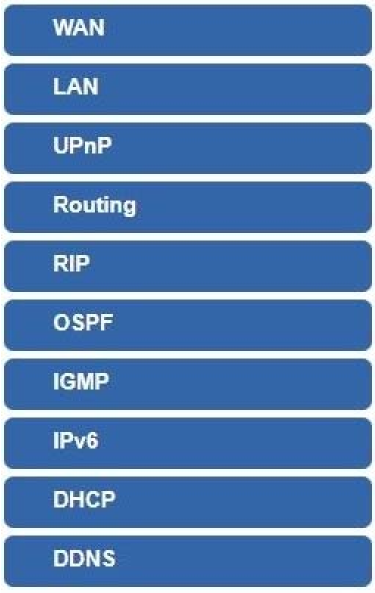
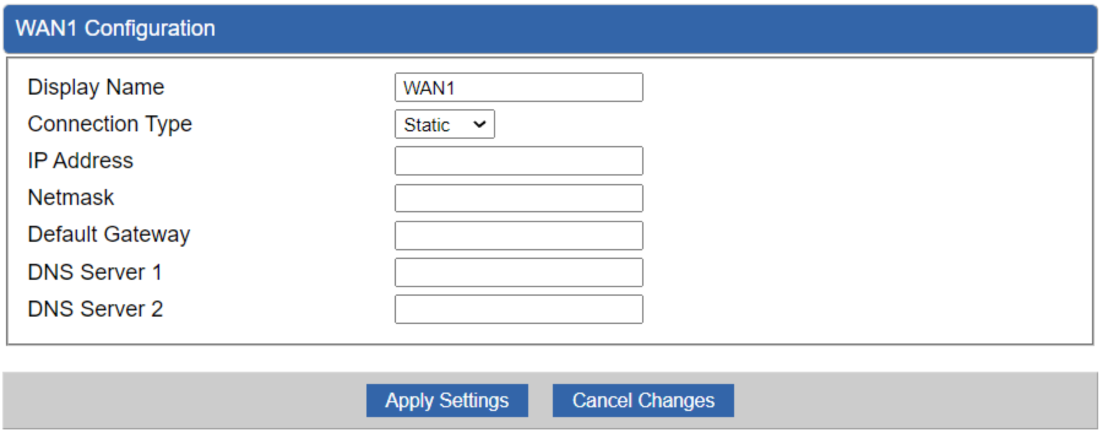


Figure 4-25: Network Menu

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.

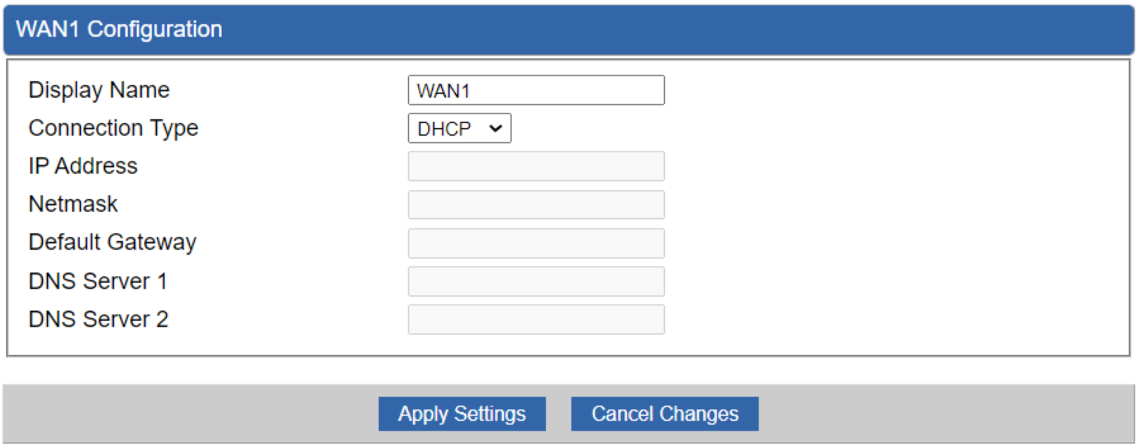
4.2.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the router as shown in Figure 4-26. Here you may select the access method by clicking the item value of WAN access type.



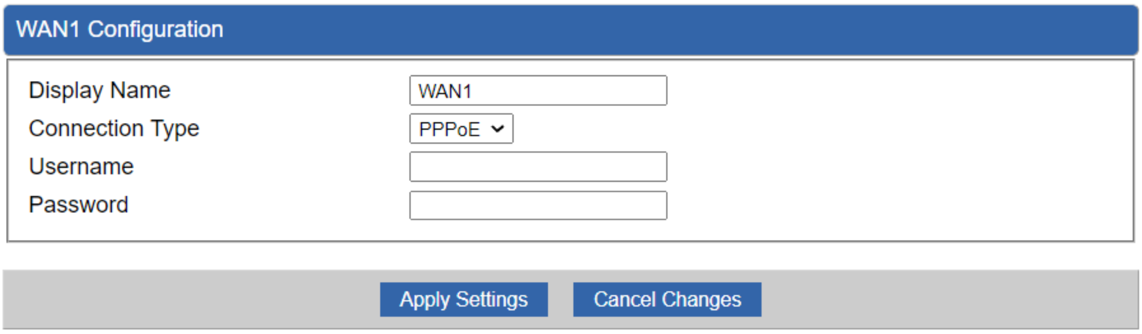
WAN1 Configuration

Display Name	WAN1
Connection Type	Static
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	



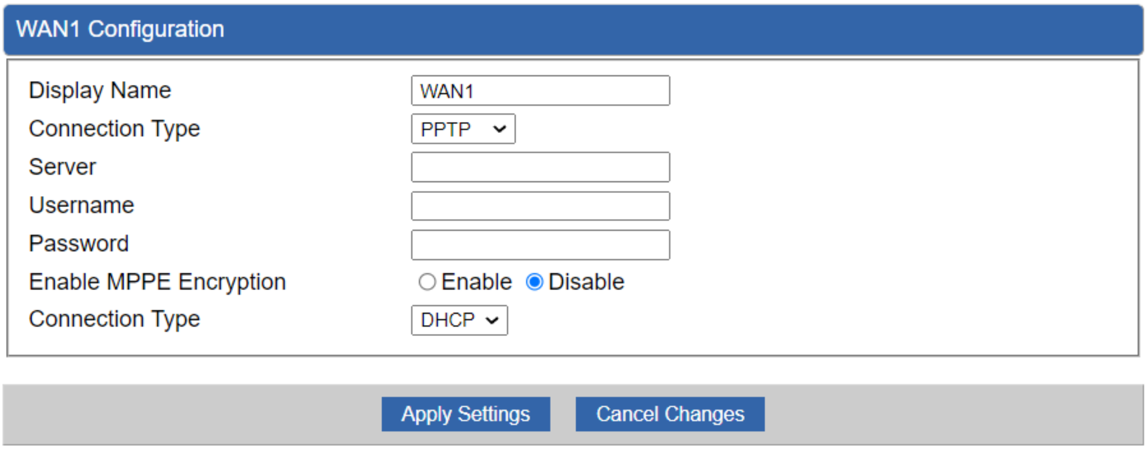
WAN1 Configuration

Display Name	WAN1
Connection Type	DHCP
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	



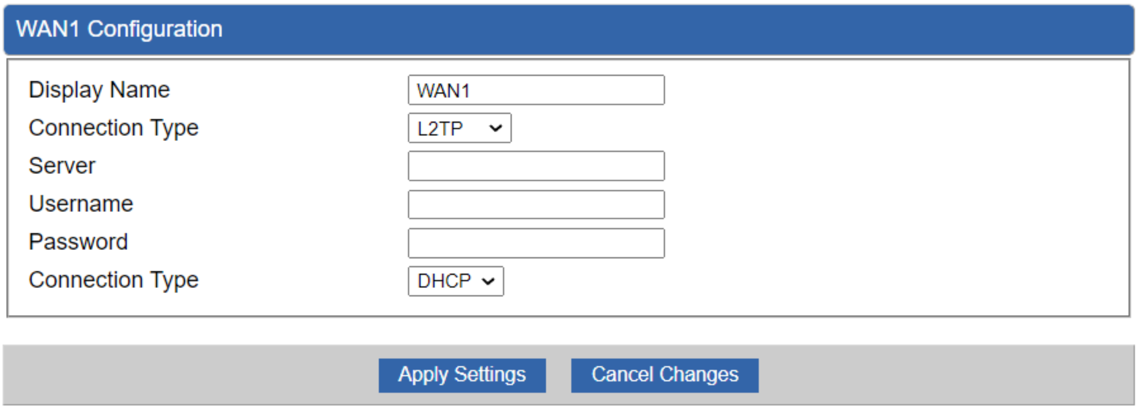
WAN1 Configuration

Display Name	WAN1
Connection Type	PPPoE
Username	
Password	



WAN1 Configuration

Display Name	WAN1
Connection Type	PPTP
Server	
Username	
Password	
Enable MPPE Encryption	○ Enable ● Disable
Connection Type	DHCP



WAN1 Configuration

Display Name	WAN1
Connection Type	L2TP
Server	
Username	
Password	
Connection Type	DHCP

Figure 4-26: WAN

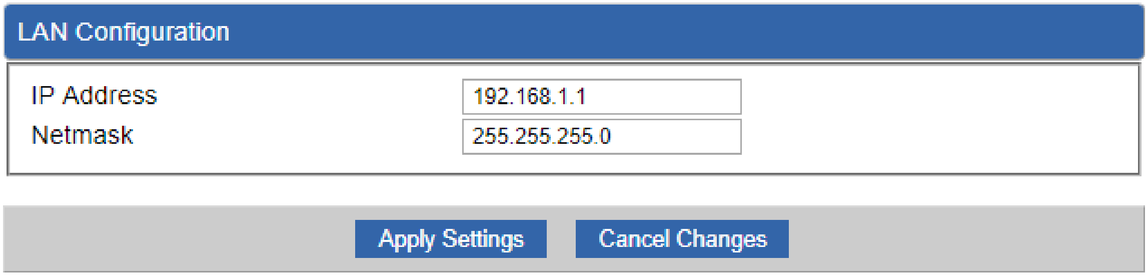
Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.	
	Static	Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet 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**

Object	Description	
		Enter the Gateway assigned by your ISP. **DNS Server** The DNS server information will be supplied by your ISP.
	DHCP	Select DHCP Client to obtain IP Address information automatically from your ISP.
	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 4-27. Here you may change the settings for IP address, subnet mask, DHCP, etc.



LAN Configuration

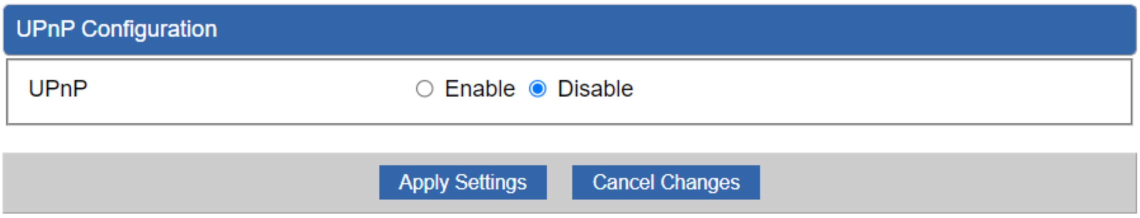
IP Address: 192.168.1.1

Netmask: 255.255.255.0

Figure 4-27: 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


UPnP Configuration

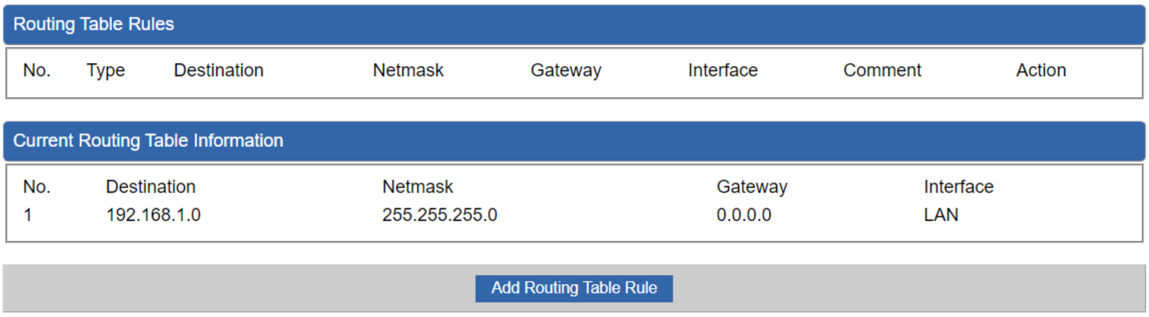
UPnP	○ Enable ● Disable

Figure 4-28: 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 4-30 and 31.

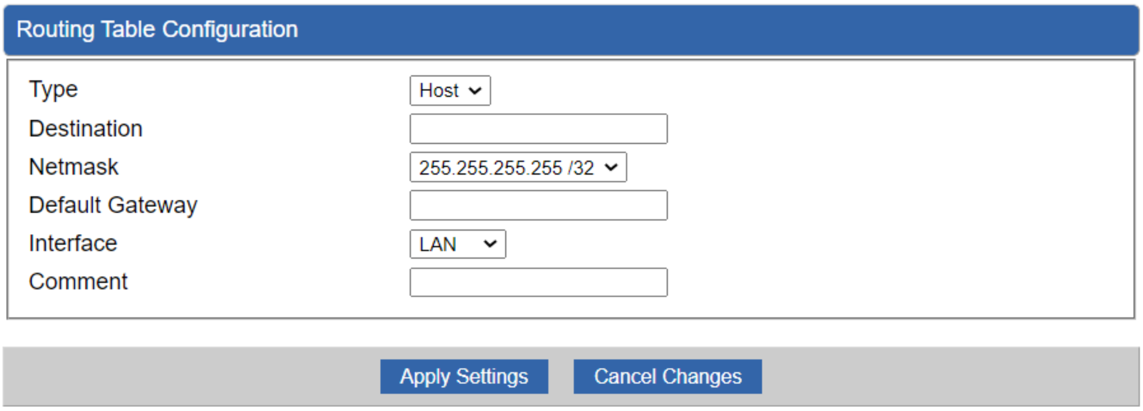

Routing Table Rules

No.	Type	Destination	Netmask	Gateway	Interface	Comment	Action

Current Routing Table Information

No.	Destination	Netmask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	LAN

Figure 4-29: Routing table


Routing Table Configuration

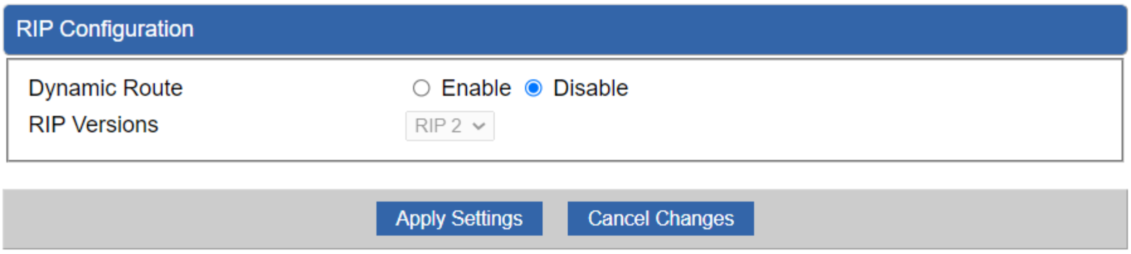
Type	Host
Destination	
Netmask	255.255.255.255 /32
Default Gateway	
Interface	LAN
Comment	

Figure 4-30: 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



RIP Configuration

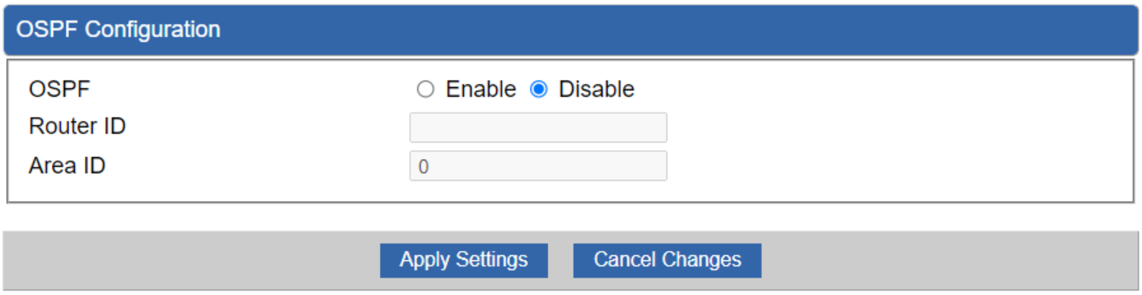
Dynamic Route ○ Enable ● Disable

RIP Versions RIP 2

Figure 4-31 RIP

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

4.2.6 OSPF



OSPF Configuration

OSPF ○ Enable ● Disable

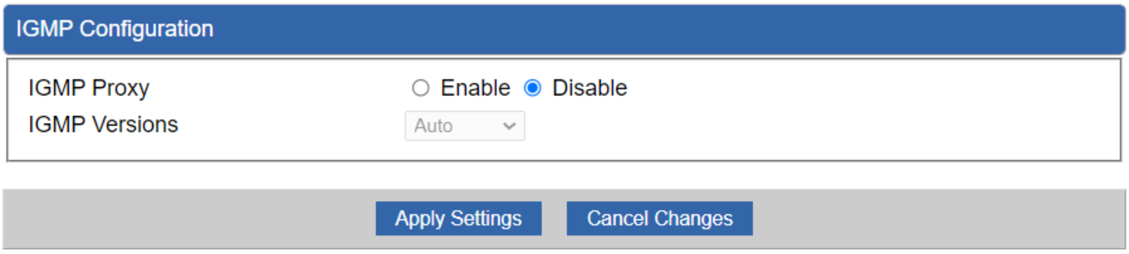
Router ID

Area ID 0

Figure 4-32: OSPF

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

4.2.7 IGMP



IGMP Configuration

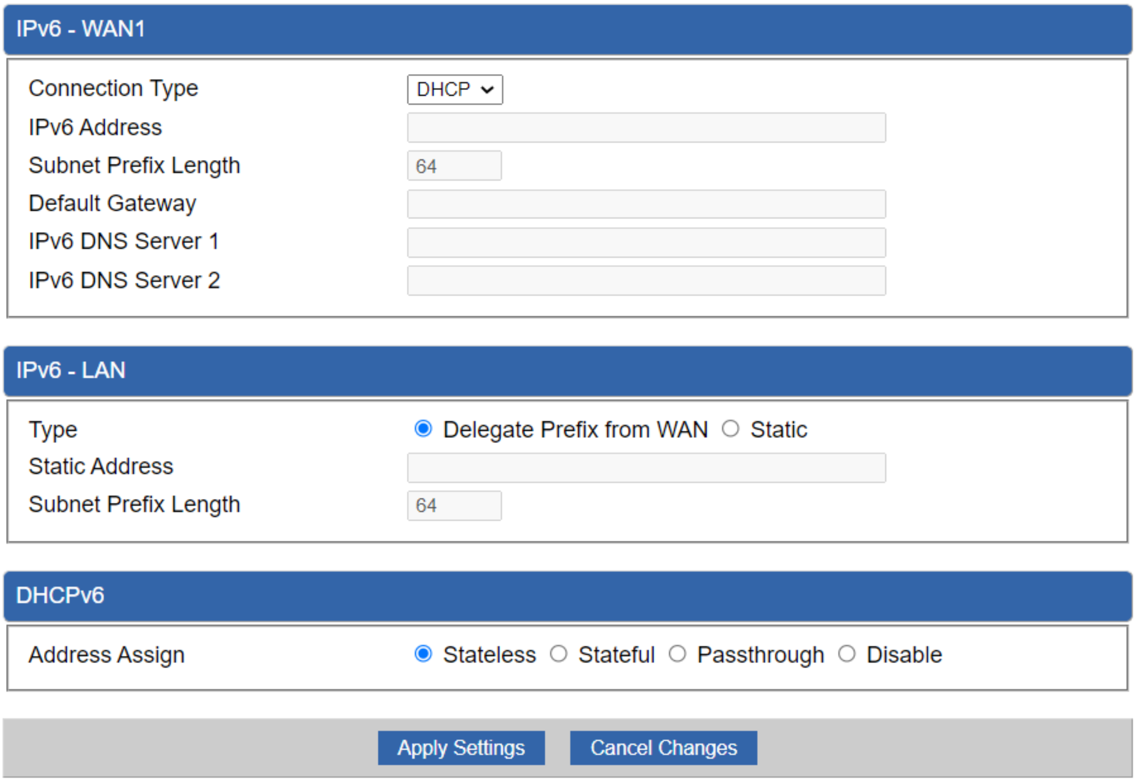
IGMP Proxy	○ Enable ● Disable
IGMP Versions	Auto

Figure 4-33: 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 4-35. It allows you to enable IPv6 function and set up the parameters of the router’s WAN. In this setting you may change WAN connection type and other settings.



IPv6 - WAN1

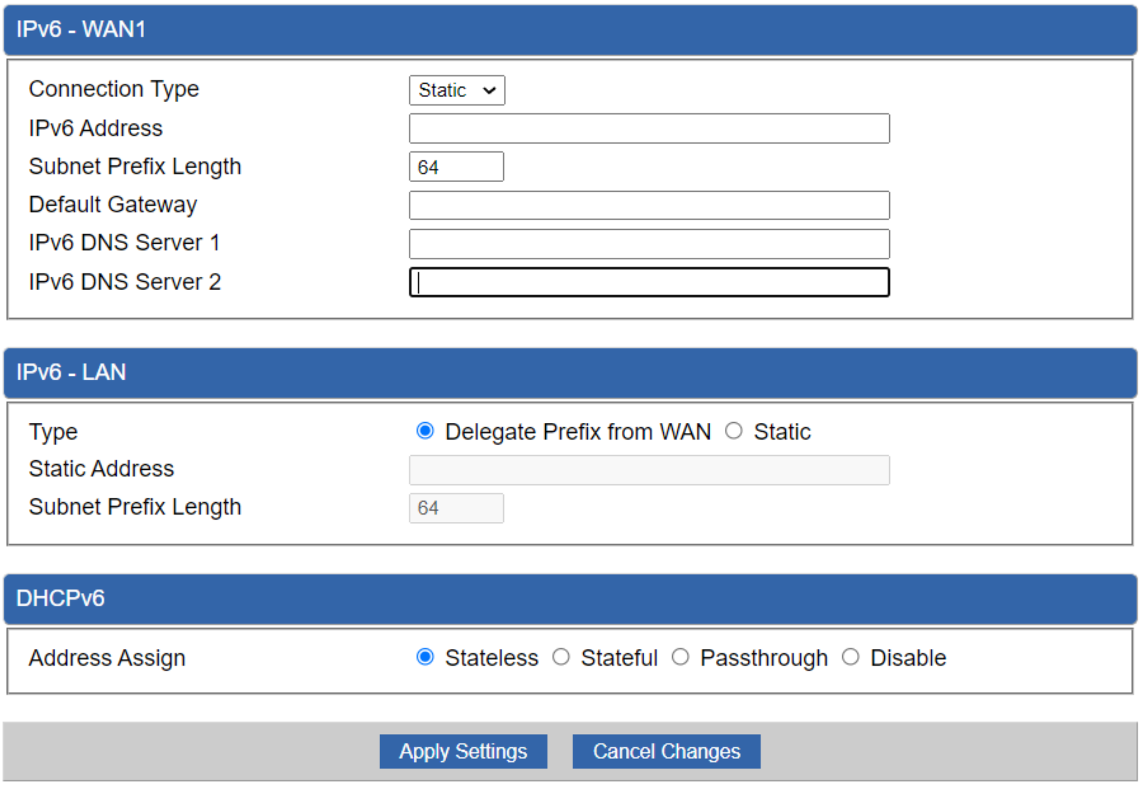
Connection Type	DHCP
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	
IPv6 DNS Server 1	
IPv6 DNS Server 2	

IPv6 - LAN

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

DHCPv6

Address Assign	● Stateless ○ Stateful ○ Passthrough ○ Disable



IPv6 - WAN1

Connection Type	Static
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	
IPv6 DNS Server 1	
IPv6 DNS Server 2	

IPv6 - LAN

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

DHCPv6

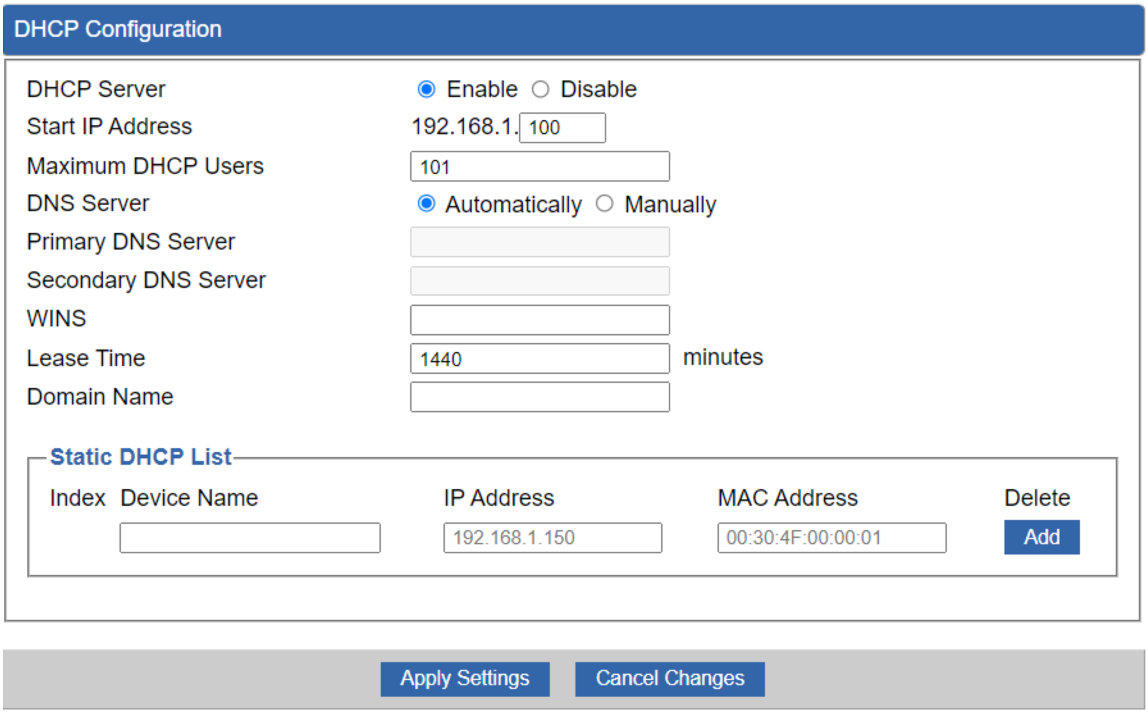
Address Assign	● Stateless ○ Stateful ○ Passthrough ○ Disable

Figure 4-34: 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 4-35.



DHCP Configuration

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

Static DHCP List

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

Figure 4-35: 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.
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.

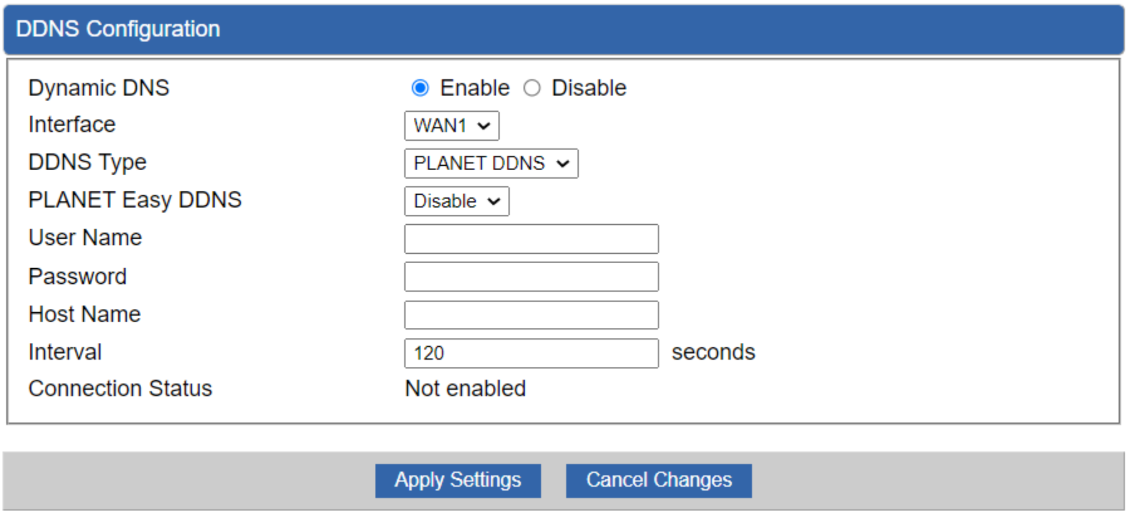
PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in Figure 4-36.

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)



DDNS Configuration

Dynamic DNS	● Enable ○ Disable
Interface	WAN1
DDNS Type	PLANET DDNS
PLANET Easy DDNS	Disable
User Name	
Password	
Host Name	
Interval	120 seconds
Connection Status	Not enabled

Figure 4-36: 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 4-37. Please refer to the following sections for the details.

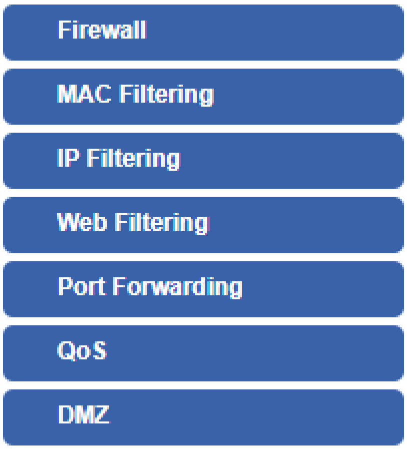
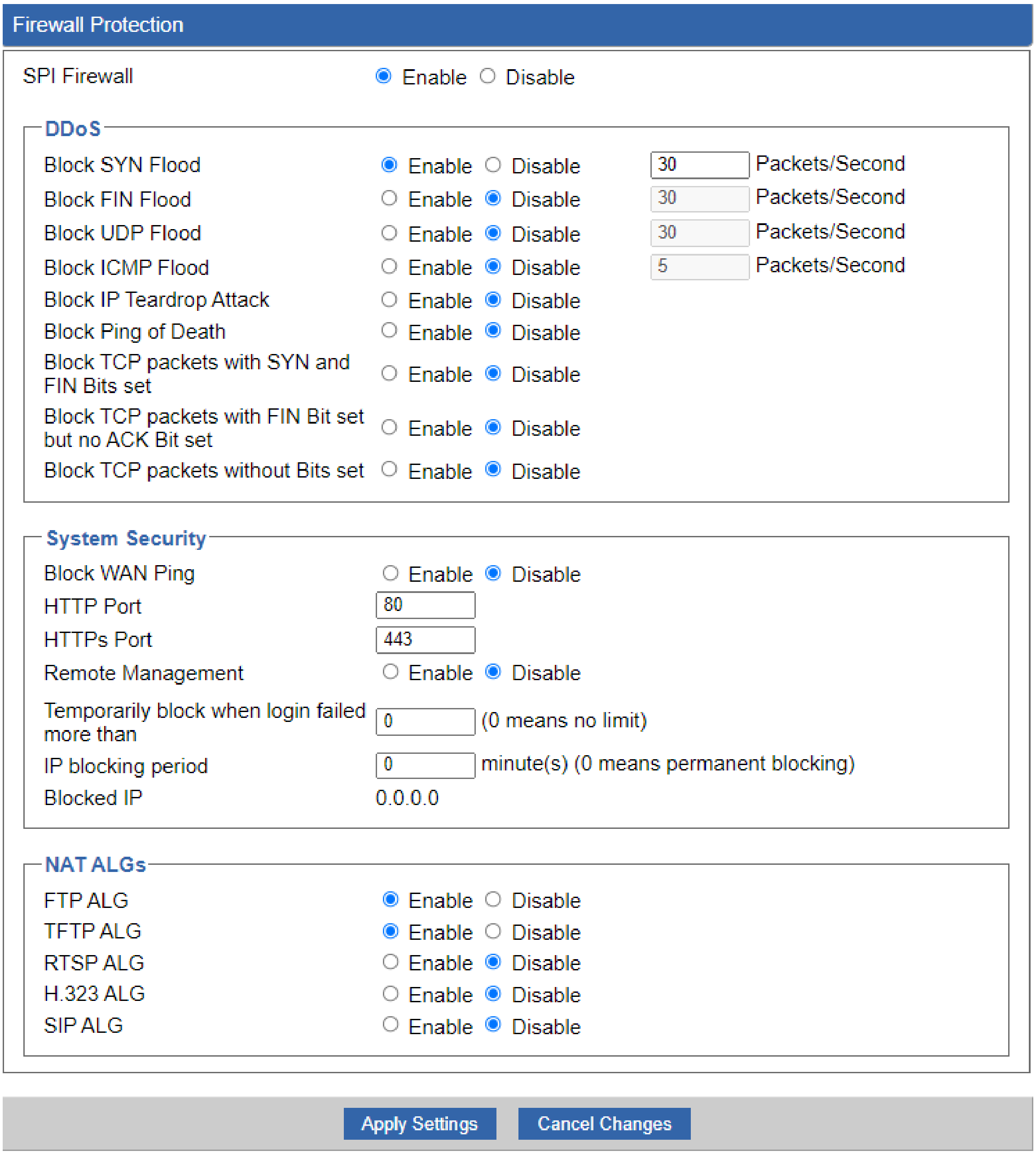


Figure 4-37: Security menu

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 4-38.



Firewall Protection

SPI Firewall ● Enable ○ Disable

DDoS

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

System Security

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

NAT ALGs

FTP ALG	● Enable ○ Disable
TFTP ALG	● Enable ○ Disable
RTSP ALG	○ Enable ● Disable
H.323 ALG	○ Enable ● Disable
SIP ALG	○ Enable ● Disable

Figure 4-38: Firewall

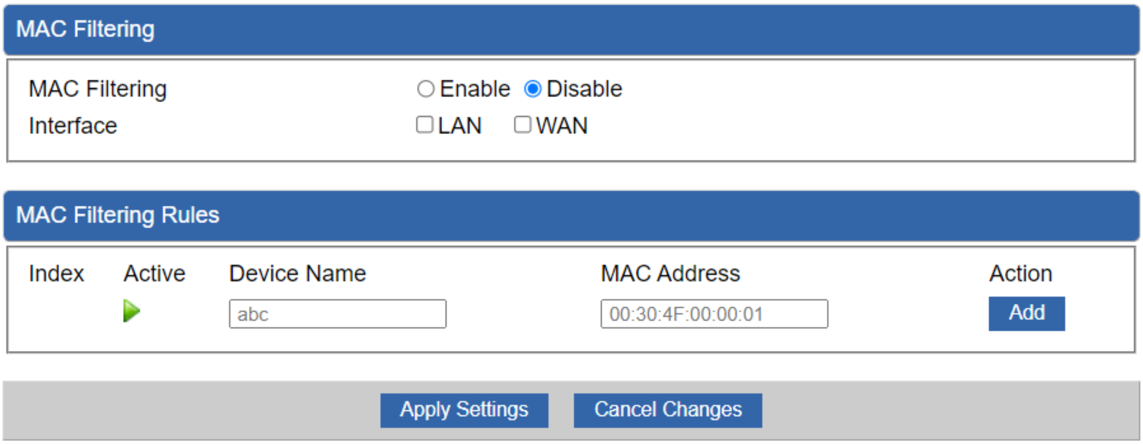
Object	Description

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 4-39.



MAC Filtering

MAC Filtering ○ Enable ● Disable

Interface □ LAN □ WAN

MAC Filtering Rules

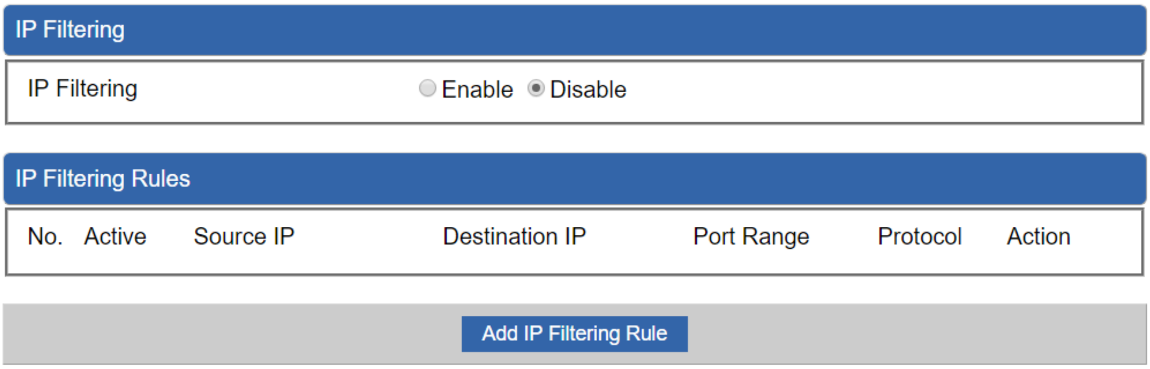
Index	Active	Device Name	MAC Address	Action
	▶	abc	00:30:4F:00:00:01	Add

Figure 4-39: 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.

4.3.4 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in Figure 4-40. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.



IP Filtering

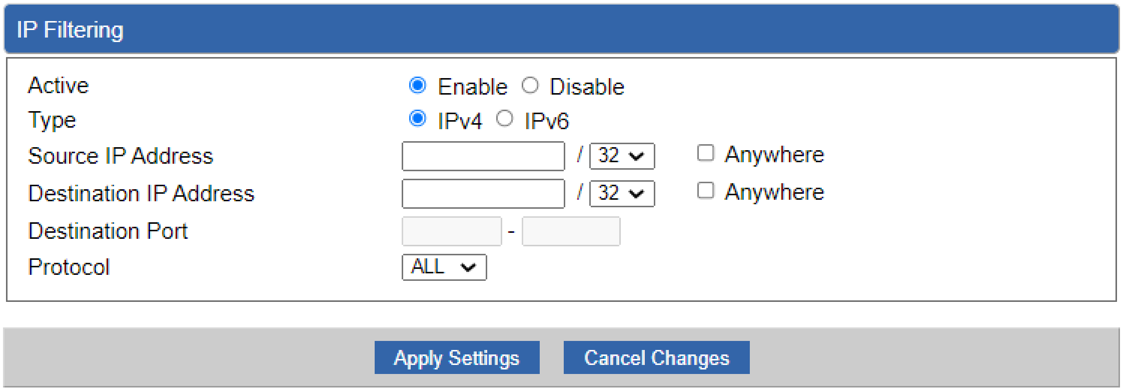
IP Filtering ○ Enable ● Disable

IP Filtering Rules

No.	Active	Source IP	Destination IP	Port Range	Protocol	Action

Figure 4-40: IP Filtering

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



IP Filtering

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

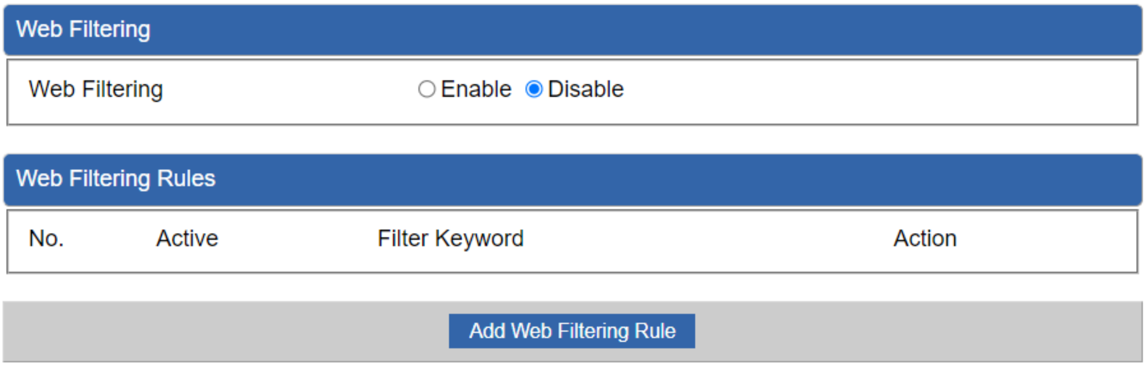
Figure 4-41: IP Filter Rule Setting

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.

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

4.3.6 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-43. Block those URLs which contain keywords listed below.



Web Filtering

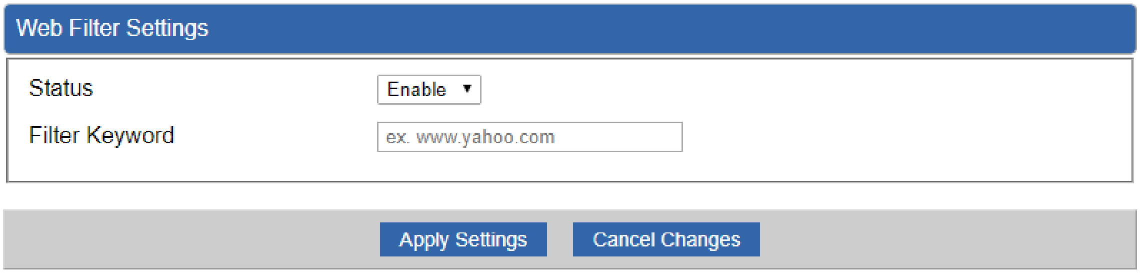
Web Filtering ○ Enable ● Disable

Web Filtering Rules

No.	Active	Filter Keyword	Action

Figure 4-41: Web Filtering

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



Web Filter Settings

Status: Enable ▾

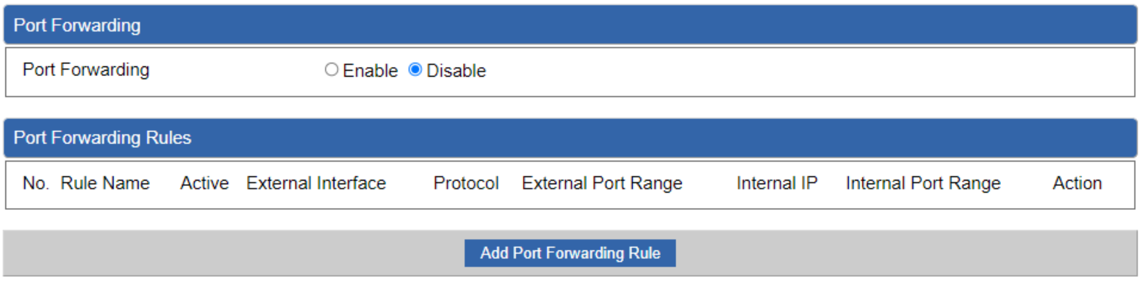
Filter Keyword: ex. www.yahoo.com

Figure 4-42: 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.

4.3.8 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 4-43. 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.



Port Forwarding

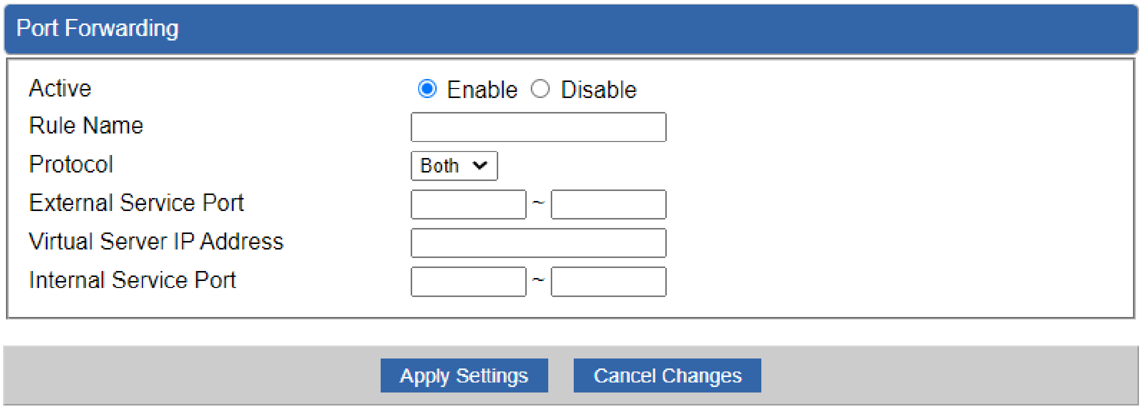
Port Forwarding ○ Enable ● Disable

Port Forwarding Rules

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

Figure 4-43: Port Forwarding

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



Port Forwarding

Active ● Enable ○ Disable

Rule Name

Protocol Both

External Service Port ~

Virtual Server IP Address

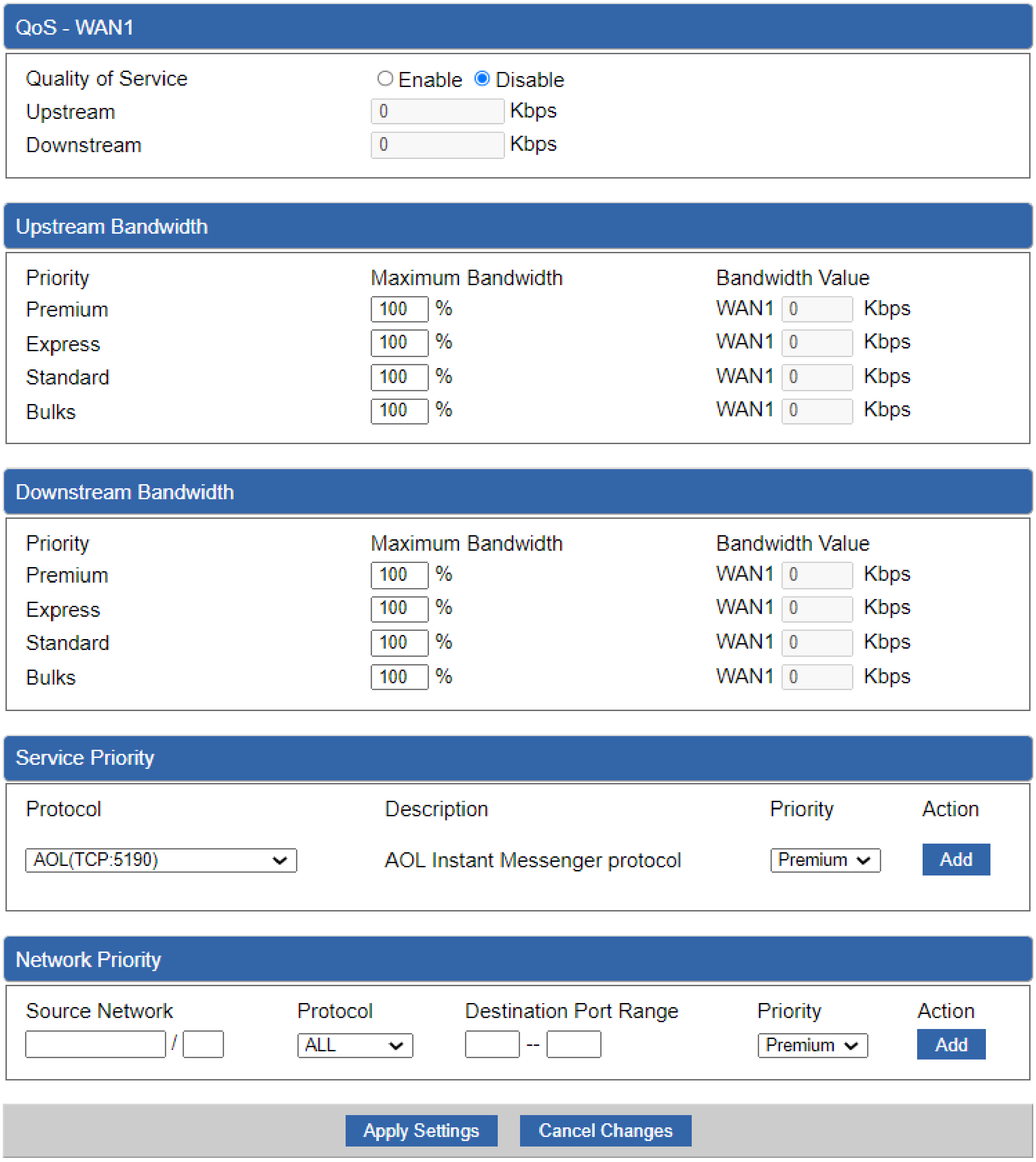
Internal Service Port ~

Figure 4-44: 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

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

4.3.10 QoS



QoS - WAN1

Quality of Service	○ Enable ● Disable
Upstream	0 Kbps
Downstream	0 Kbps

Upstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	100 %	WAN1 0 Kbps
Express	100 %	WAN1 0 Kbps
Standard	100 %	WAN1 0 Kbps
Bulks	100 %	WAN1 0 Kbps

Downstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	100 %	WAN1 0 Kbps
Express	100 %	WAN1 0 Kbps
Standard	100 %	WAN1 0 Kbps
Bulks	100 %	WAN1 0 Kbps

Service Priority

Protocol	Description	Priority	Action
AOL(TCP:5190)	AOL Instant Messenger protocol	Premium	Add

Network Priority

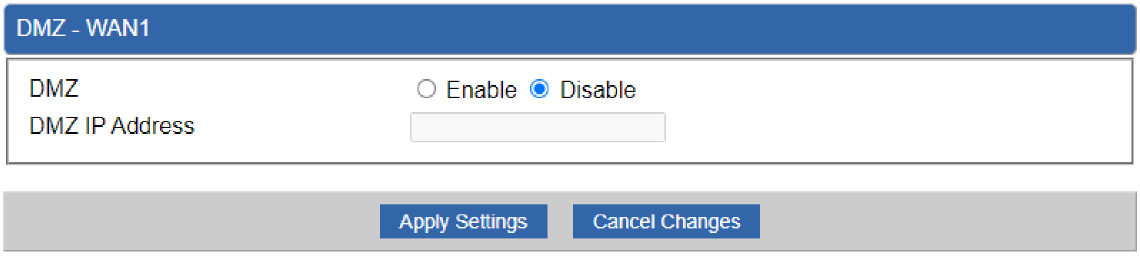
Source Network	Protocol	Destination Port Range	Priority	Action
/	ALL	--	Premium	Add

Figure 4-45: 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

4.3.11 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in Figure 4-46.Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.


DMZ - WAN1

DMZ ○ Enable ● Disable

DMZ IP Address

Figure 4-46: 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

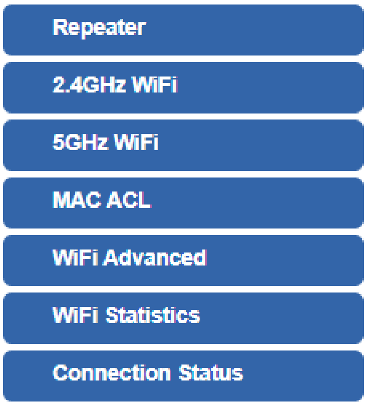
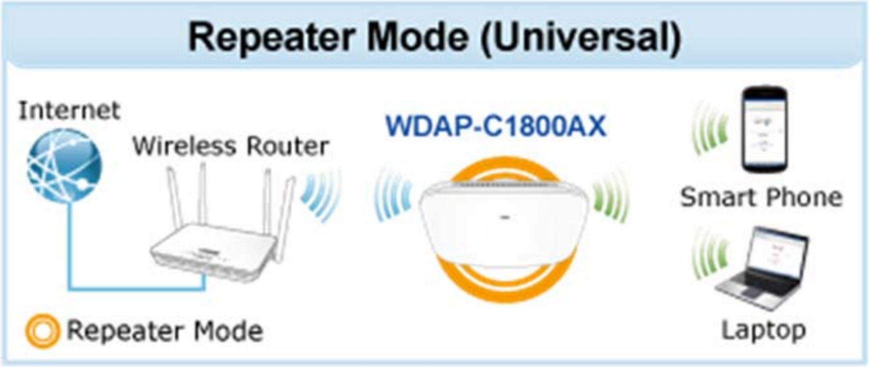


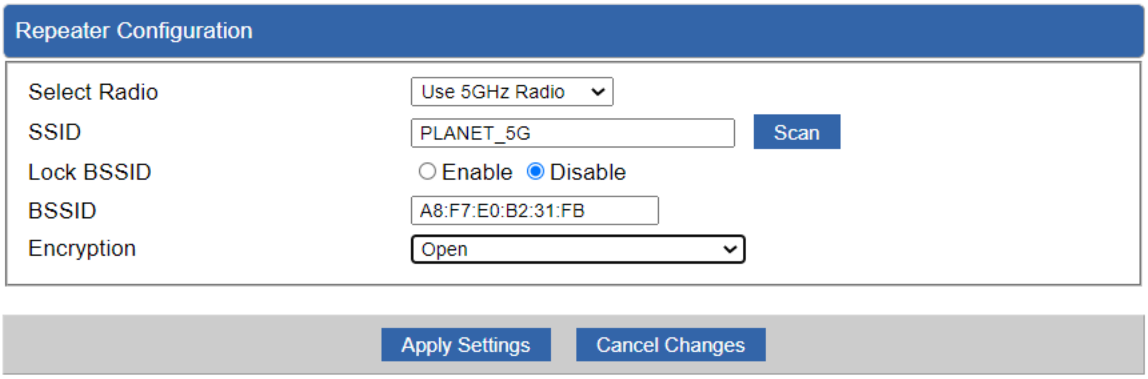
Figure 4-47: Wireless Menu

Object	Description
Repeater	Allow to configure Repeater.
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



Repeater Configuration

Select Radio: Use 5GHz Radio

SSID: PLANET_5G

Lock BSSID: ○ Enable ● Disable

BSSID: A8:F7:E0:B2:31:FB

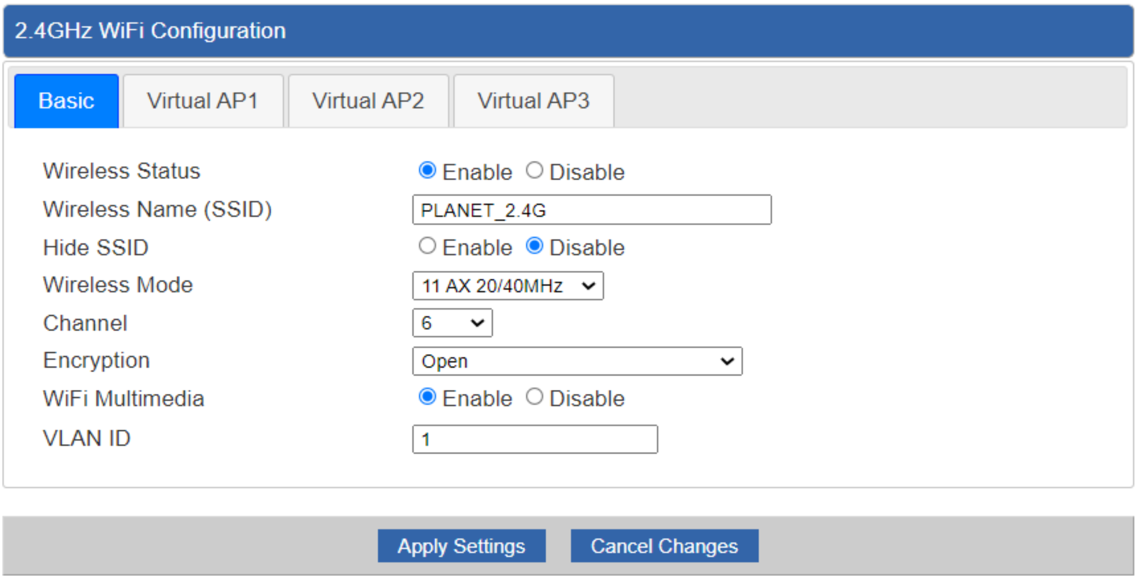
Encryption: Open

Figure 4-48: 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.



2.4GHz WiFi Configuration

Wireless Status: ● Enable ○ Disable

Wireless Name (SSID): PLANET_2.4G

Hide SSID: ○ Enable ● Disable

Wireless Mode: 11 AX 20/40MHz

Channel: 6

Encryption: Open

WiFi Multimedia: ● Enable ○ Disable

VLAN ID: 1

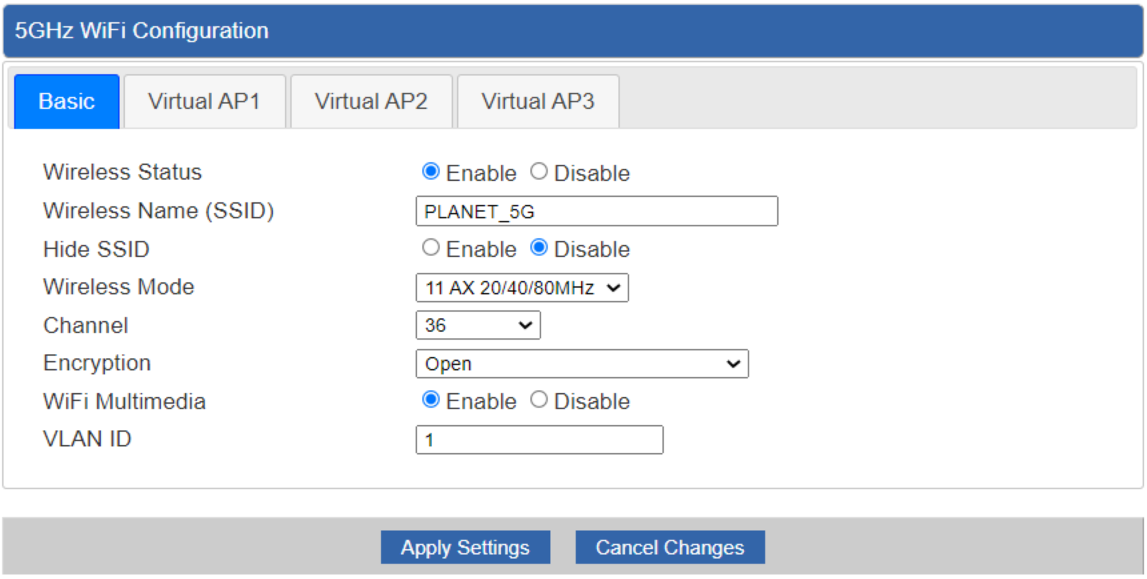
Figure 4-49: 2.4G Wi-Fi

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 VLAD ID

4.4.3 5G Wi-Fi

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



Wireless Status ● Enable ○ Disable

Wireless Name (SSID) PLANET_5G

Hide SSID ○ Enable ● Disable

Wireless Mode 11 AX 20/40/80MHz

Channel 36

Encryption Open

WiFi Multimedia ● Enable ○ Disable

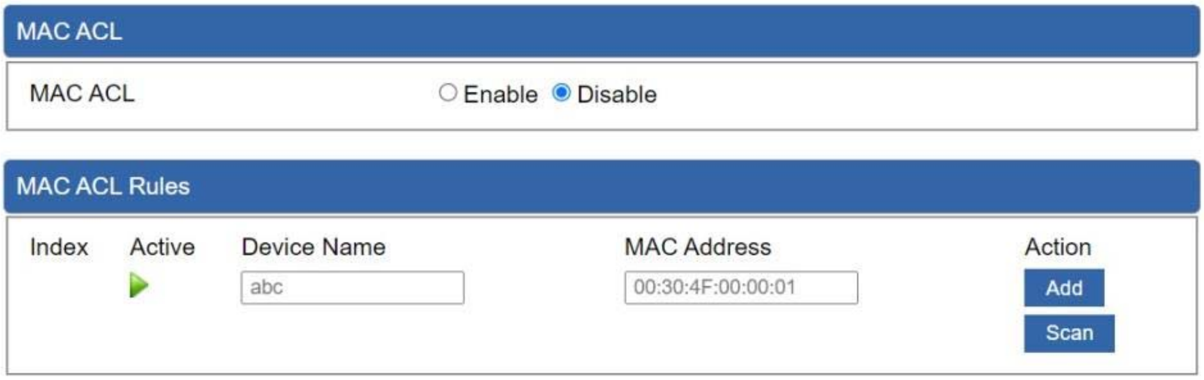
VLAN ID 1

Figure 4-50: 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 VLAD ID

4.4.4 MAC ACL

This page allows the user to define MAC ACL.



MAC ACL

MAC ACL ○ Enable ● Disable

MAC ACL Rules

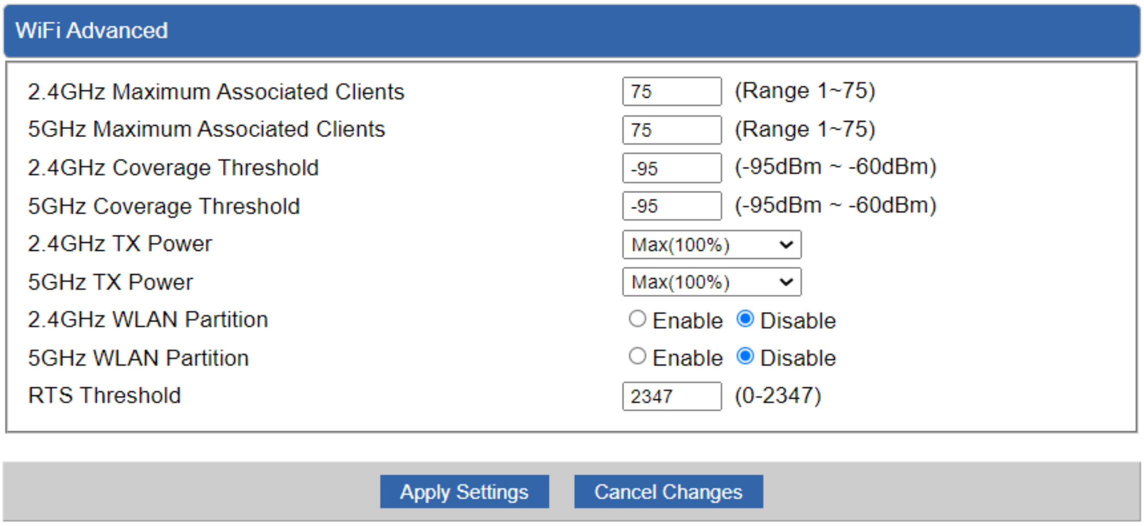
Index	Active	Device Name	MAC Address	Action
	▶	abc	00:30:4F:00:00:01	Add Scan

Figure 4-51: 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.


WiFi Advanced

2.4GHz Maximum Associated Clients	75 (Range 1~75)
5GHz Maximum Associated Clients	75 (Range 1~75)
2.4GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
5GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
2.4GHz TX Power	Max(100%)
5GHz TX Power	Max(100%)
2.4GHz WLAN Partition	○ Enable ● Disable
5GHz WLAN Partition	○ Enable ● Disable
RTS Threshold	2347 (0-2347)

Figure 4-52: 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.

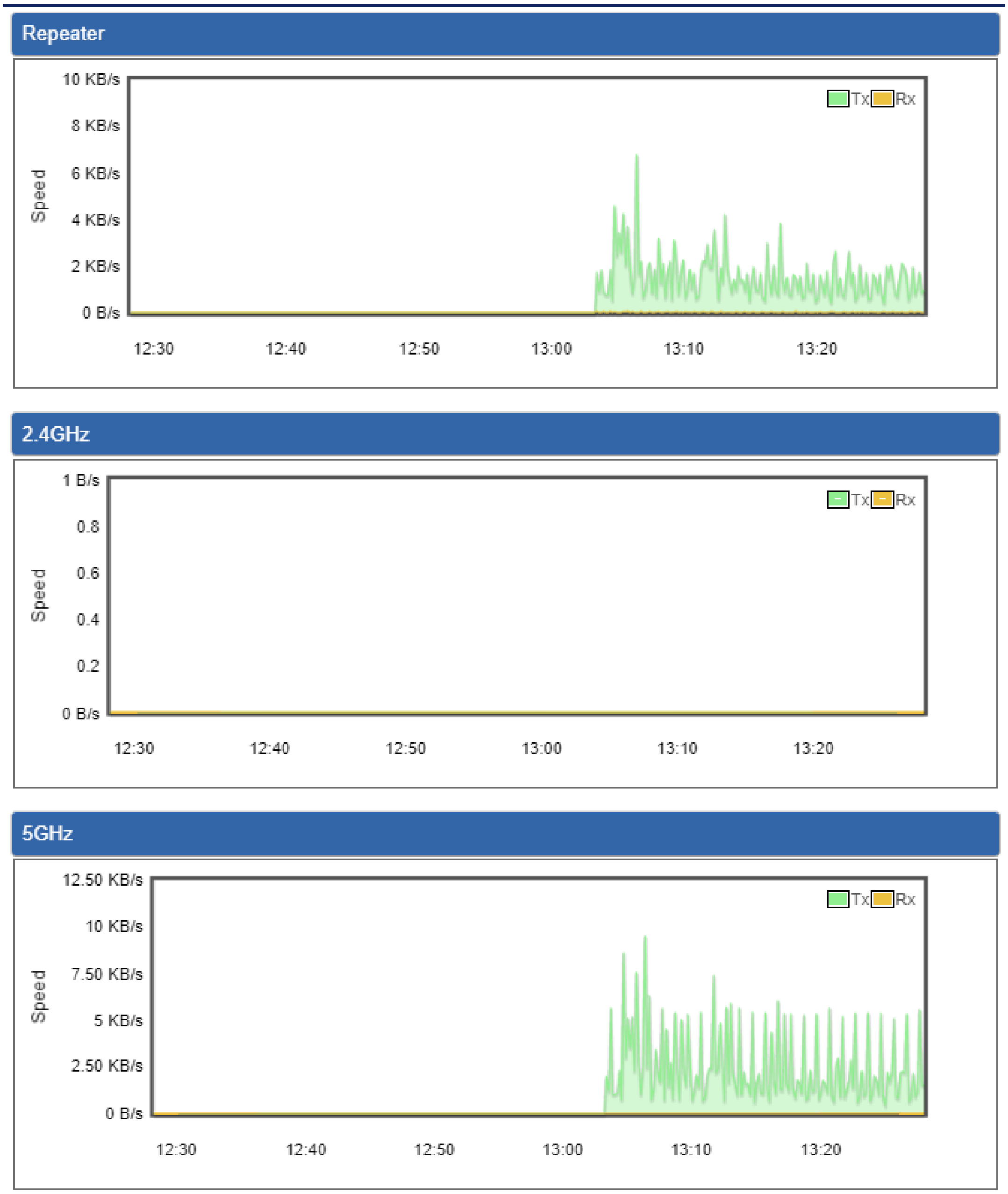
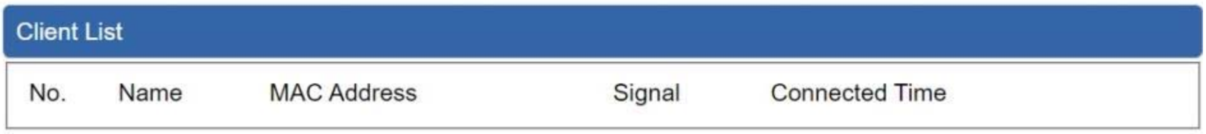


Figure 4-53: Wi-Fi Statistics

4.4.7 Connection Status

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



Client List

No.	Name	MAC Address	Signal	Connected Time

Figure 4-54: 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

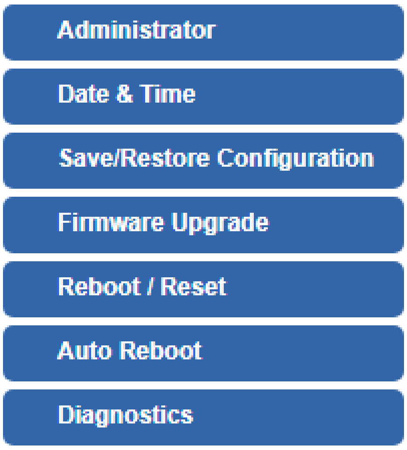
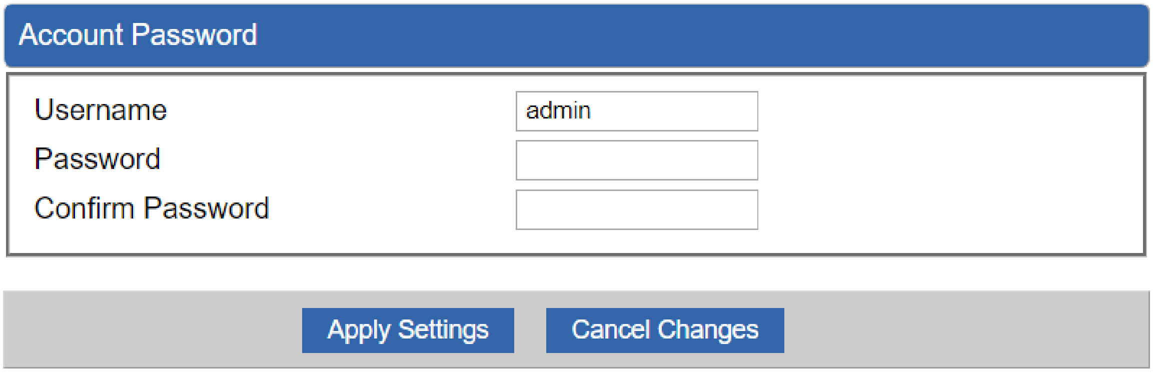


Figure 4-55: Maintenance

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 4-56.



Account Password

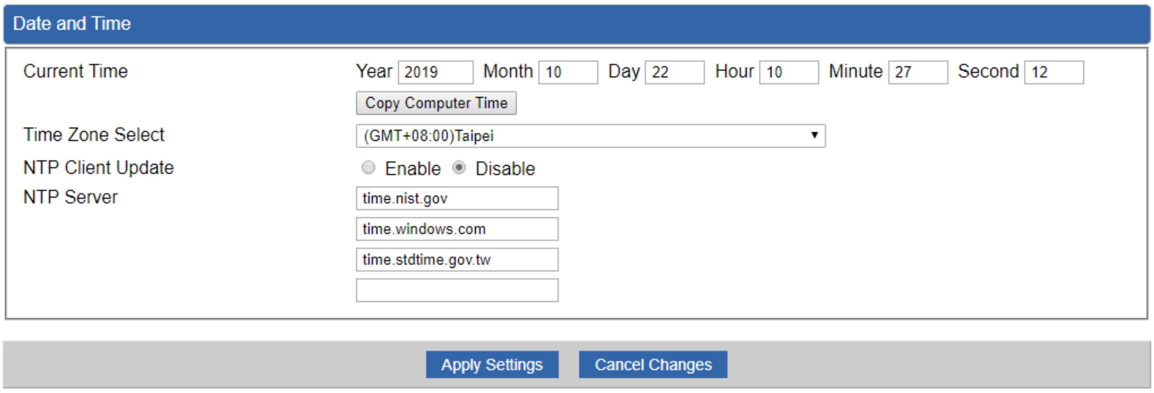
Username	admin
Password	
Confirm Password	

Figure 4-56: 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 4-57.



Date and Time

Current Time	Year 2019 Month 10 Day 22 Hour 10 Minute 27 Second 12
Time Zone Select	(GMT+08:00)Taipei
NTP Client Update	○ Enable ● Disable
NTP Server	time.nist.gov time.windows.com time.stdtime.gov.tw

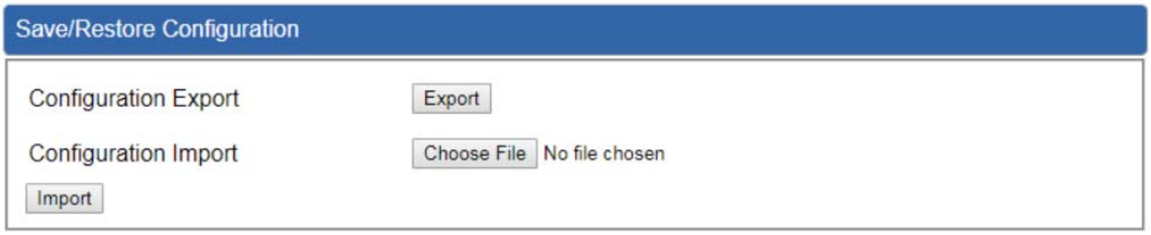
Figure 4-57: Date and Time

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 4-58 is shown below:



Save/Restore Configuration

Configuration Export Export

Configuration Import Choose File No file chosen

Import

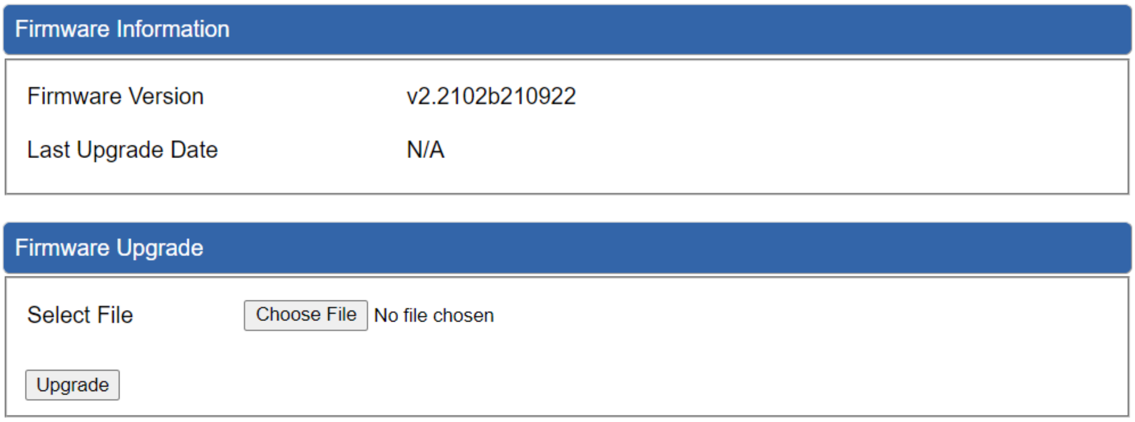
Figure 4-58: Save/Restore Configuration

■ **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 4-59.



Firmware Information

Firmware Version	v2.2102b210922
Last Upgrade Date	N/A

Firmware Upgrade

Select File [Choose File] No file chosen

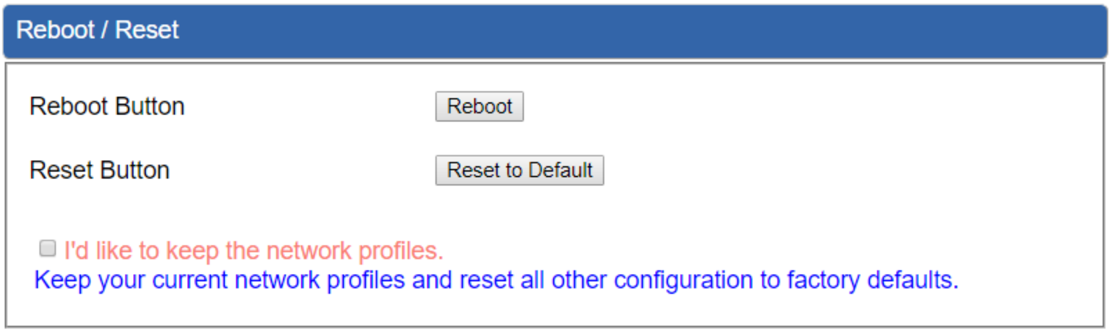
[Upgrade]

Figure 4-59: 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 4-60 is shown below:



Reboot / Reset

Reboot Button [Reboot]

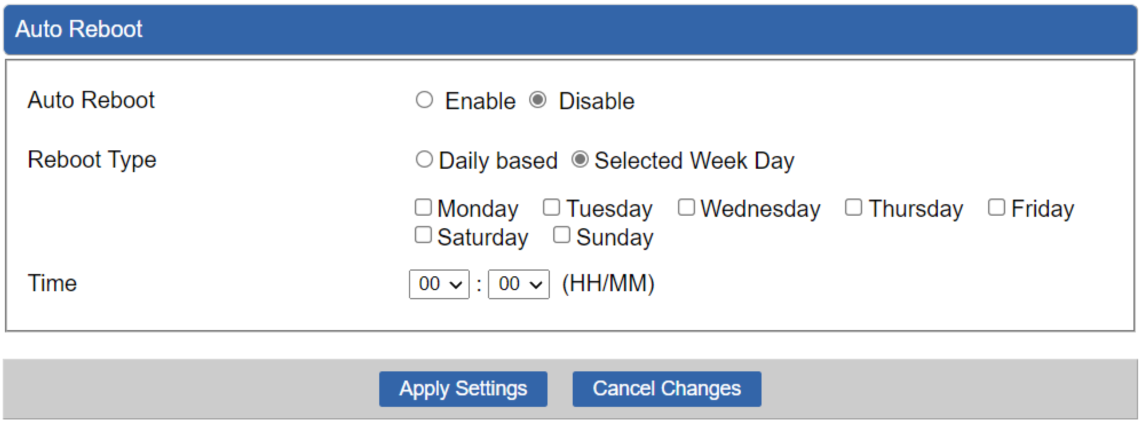
Reset Button [Reset to Default]

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

Figure 4-60: 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



Auto Reboot

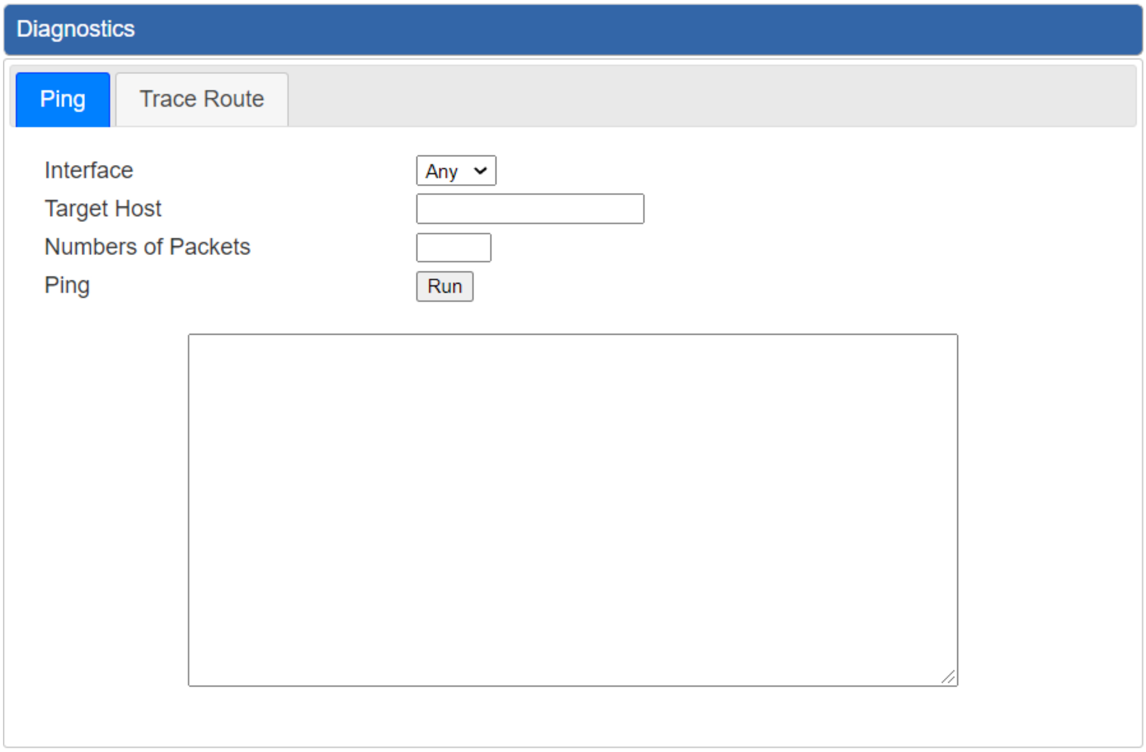
Auto Reboot	○ Enable ● Disable
Reboot Type	○ Daily based ● Selected Week Day
	□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday
Time	00 : 00 (HH/MM)

Figure 4-61: 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 4-62.



Diagnostics

Interface: Any

Target Host:

Numbers of Packets:

Ping: Run

Figure 4-62: 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.

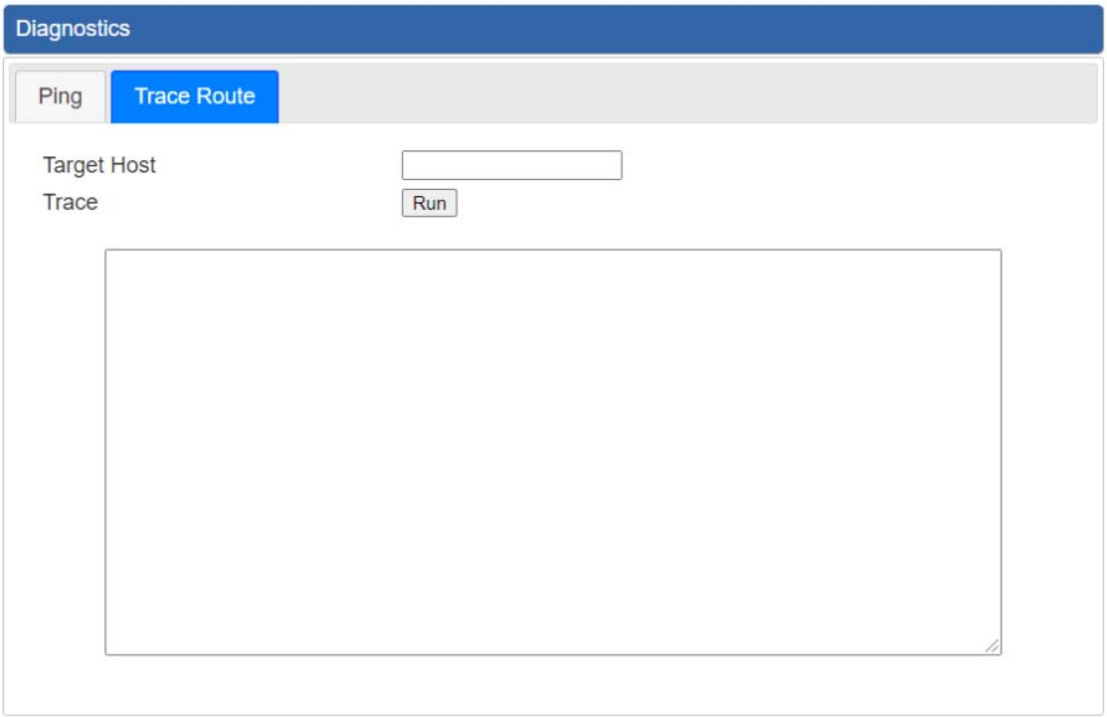


Figure 4-63: Trace Route

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

Note

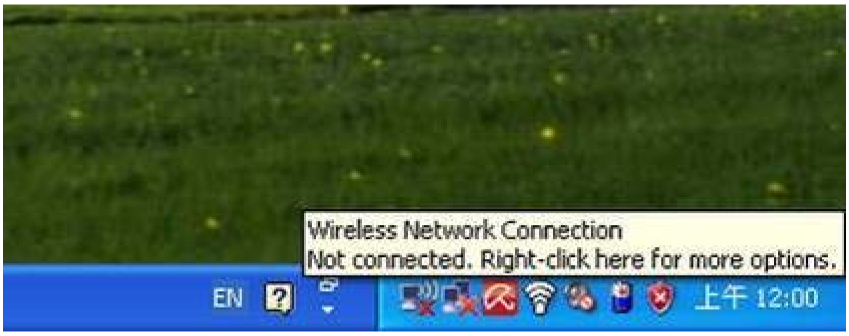
Be sure the target IP address is within the same network subnet of the router, or you have to set up the correct gateway IP address.

Chapter 5. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WDAP-C1800AX is configured to "**default**".

5.1 Windows XP (Wireless Zero Configuration)

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



Wireless Network Connection
Not connected. Right-click here for more options.

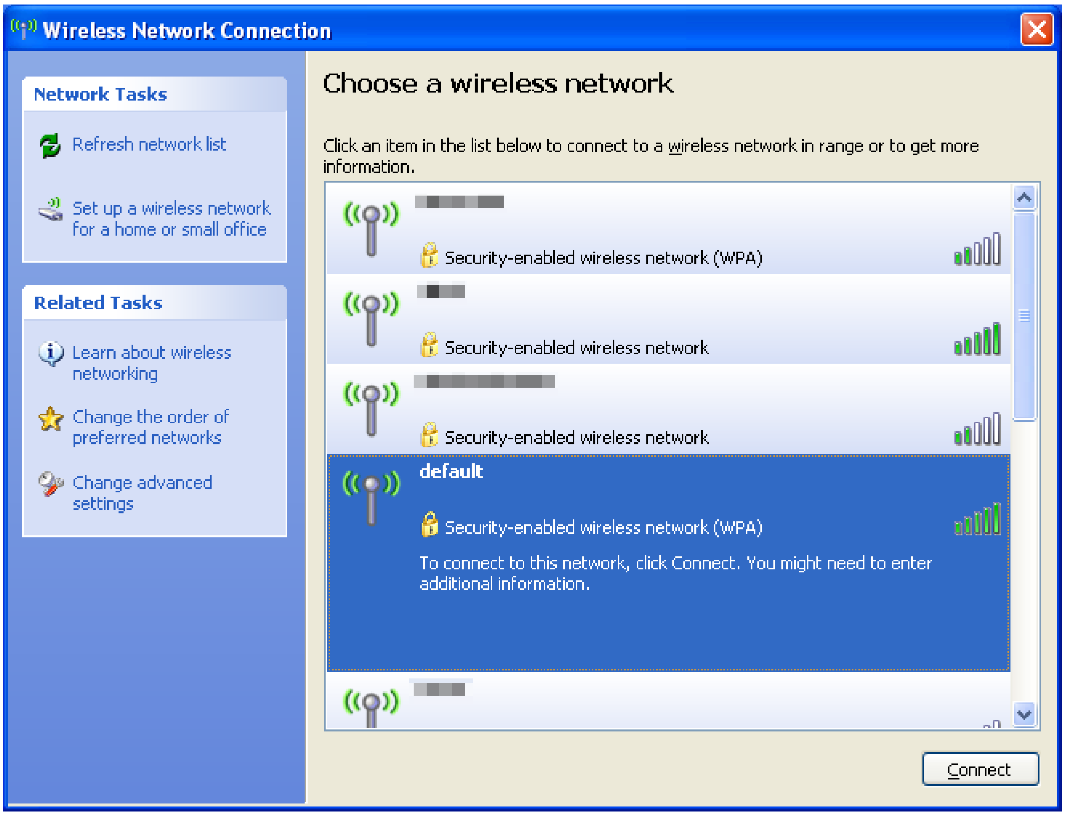
Figure 5-1 System Tray – Wireless Network Icon

Step 2: Select [**View Available Wireless Networks**]

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [default]

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


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

[redacted]
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network

[redacted]
Security-enabled wireless network

default
Security-enabled wireless network (WPA)
To connect to this network, click Connect. You might need to enter additional information.

[redacted]

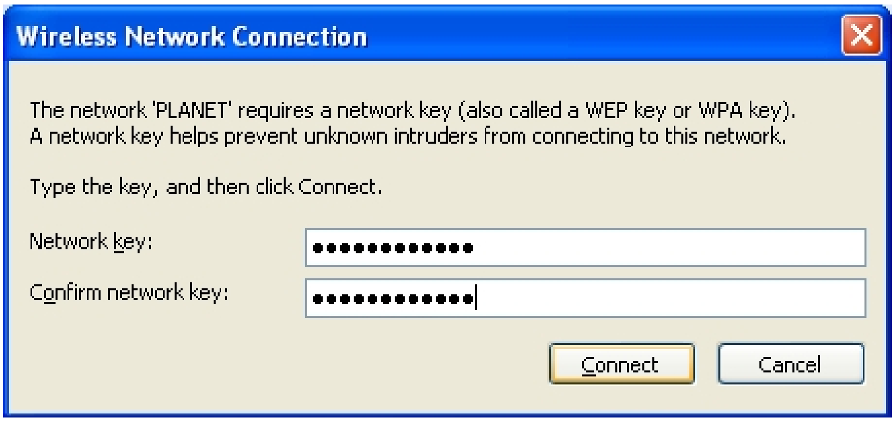
Figure 5-1 Choosing a Wireless Network

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

(1) The Wireless Network Connection box will appear

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

(3) Click the [Connect] button



The network 'PLANET' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

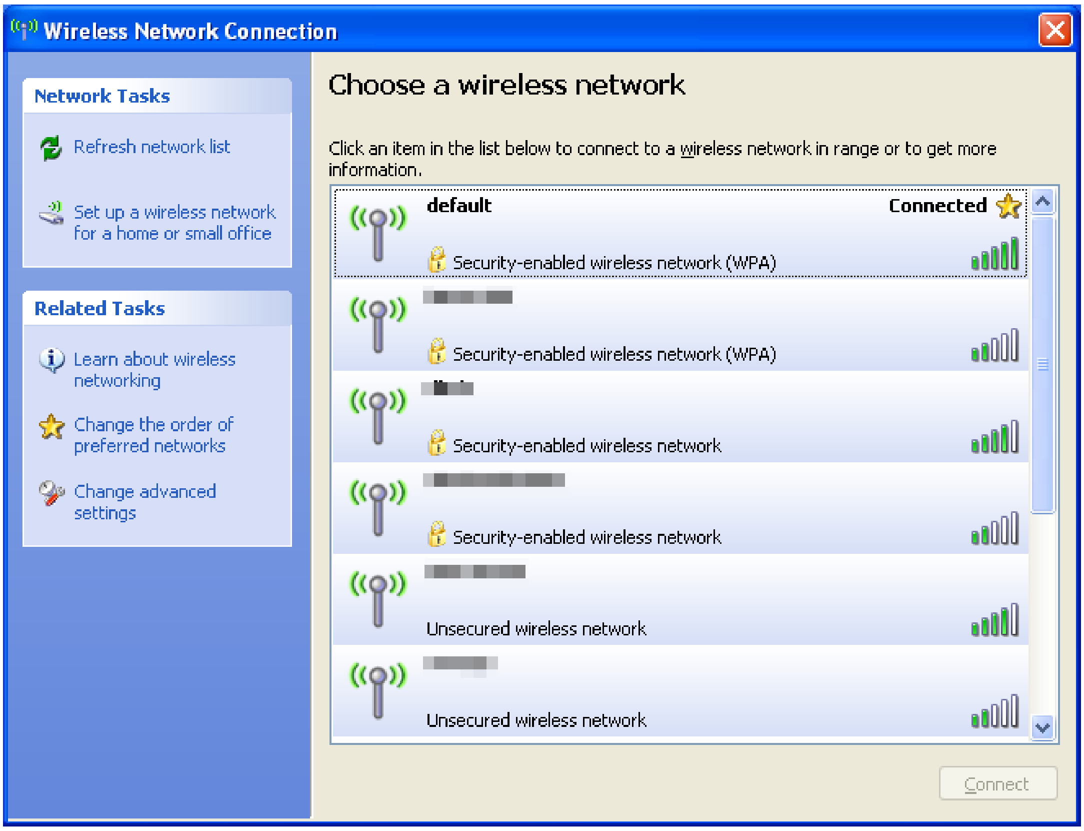
Type the key, and then click Connect.

Network key: •••••••••••••

Confirm network key: •••••••••••••

Figure 5-2 Entering the Network Key

Step 5: Check if "**Connected**" is displayed



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

default Connected
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network

[redacted]
Security-enabled wireless network

[redacted]
Unsecured wireless network

[redacted]
Unsecured wireless network

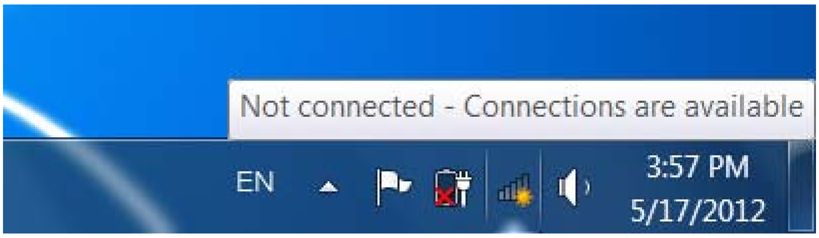
Figure 5-3 Choosing a Wireless Network -- Connected

Some laptops are equipped with a “Wireless ON/OFF” switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to “ON” position.

5.2 Windows 7/8/10 (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



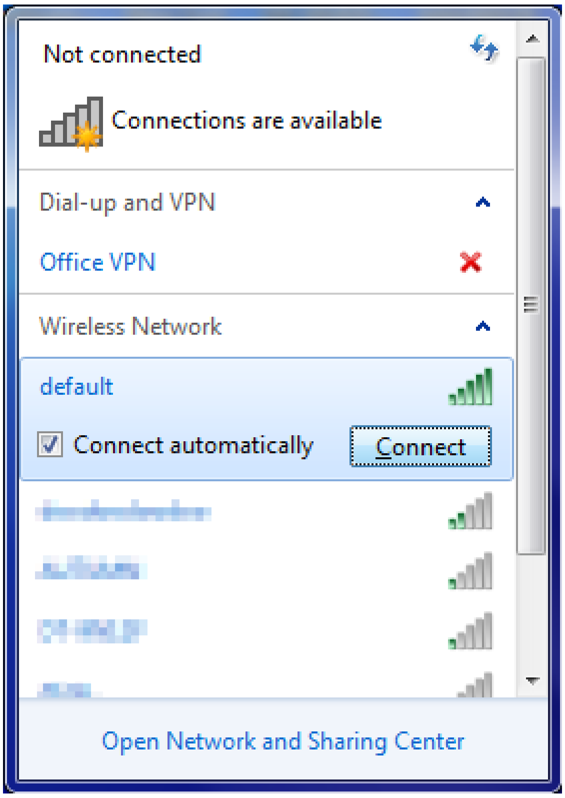
Not connected - Connections are available

Figure 5-4 Network Icon

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

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

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



Not connected

Connections are available

Dial-up and VPN

Office VPN

Wireless Network

default

☑ Connect automatically

Figure 5-5 WLAN AutoConfig

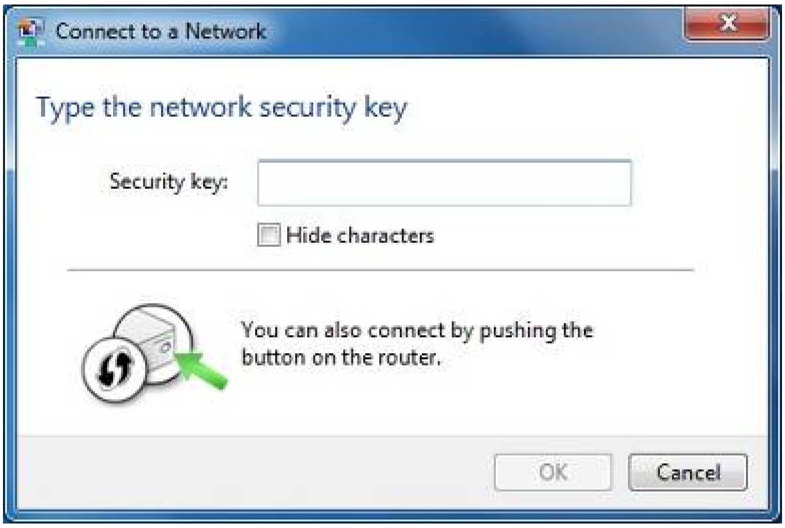
If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

Step 4: 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.



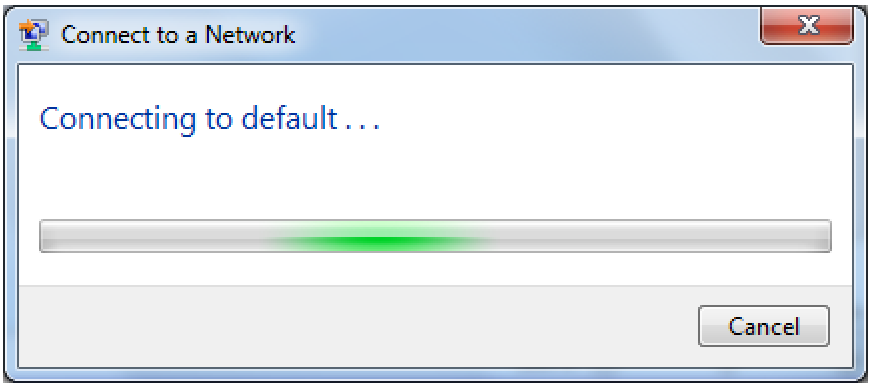
Type the network security key

Security key:

□ Hide characters

You can also connect by pushing the button on the router.

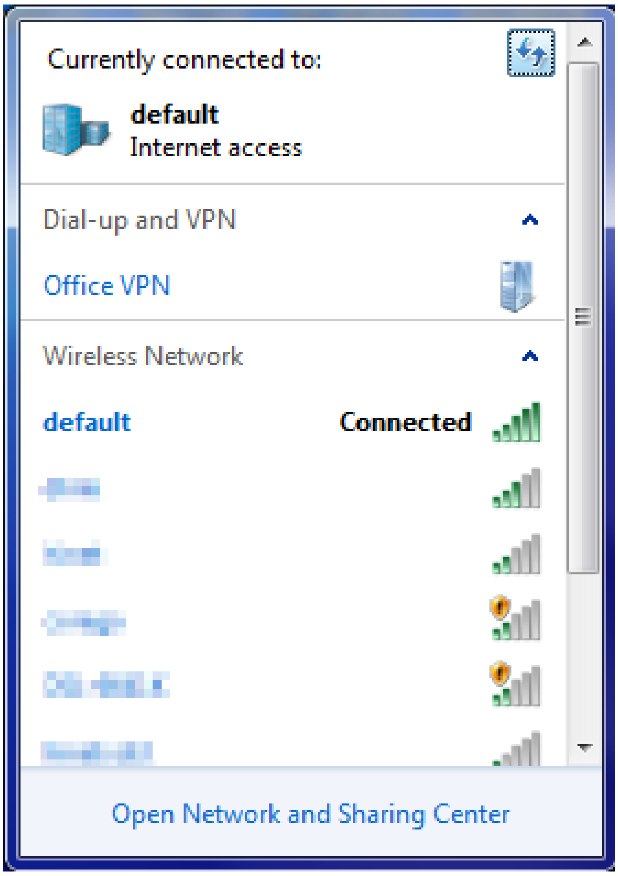
Figure 5-6 Typing the Network Key



Connecting to default . . .

Figure 5-7 Connecting to a Network

Step 5: Check if “**Connected**” is displayed.



Currently connected to:

default
Internet access

Dial-up and VPN

Office VPN

Wireless Network

default **Connected**

Open Network and Sharing Center

Figure 5-8 Connected to a Network

5.3 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.

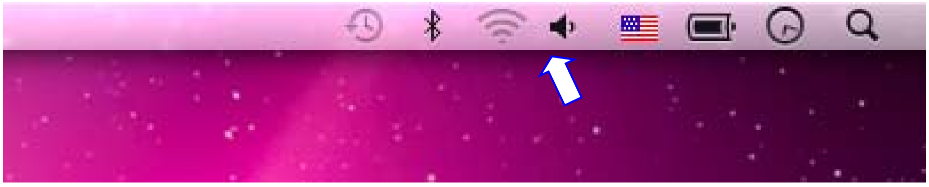


Figure 5-9 Mac OS – Network Icon

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

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

(2) Double-click on the selected SSID.

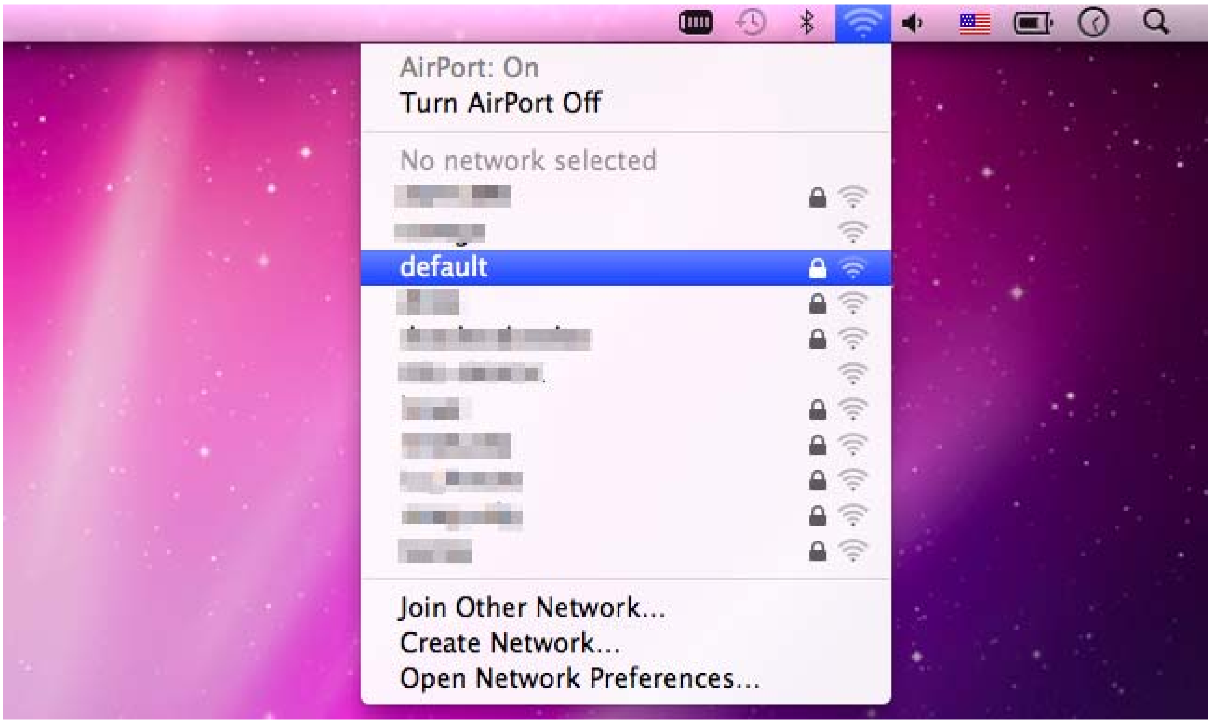
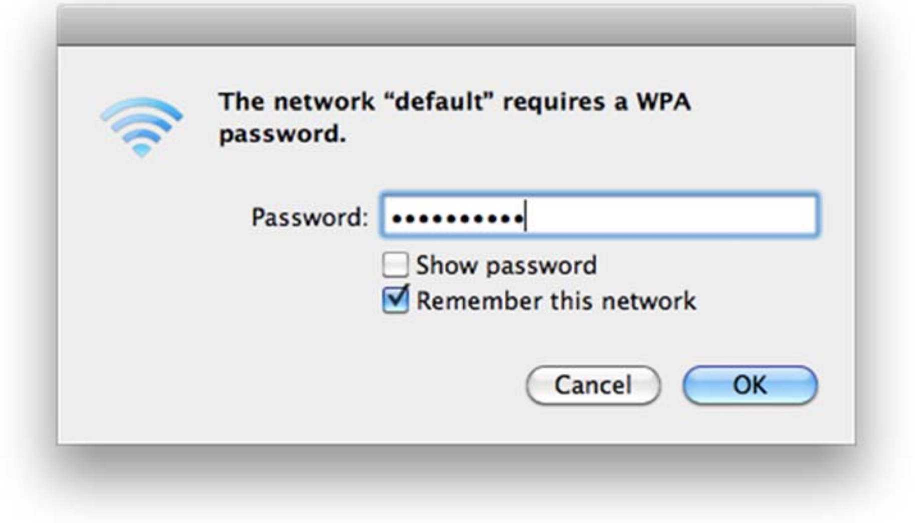


Figure 5-10 Highlighting and Selecting the Wireless Network

Step 4: 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.



The network "default" requires a WPA password.

Password: ••••••••••

□ Show password

☑ Remember this network

Figure 5-11 Enter the Password

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

Step 5: 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.

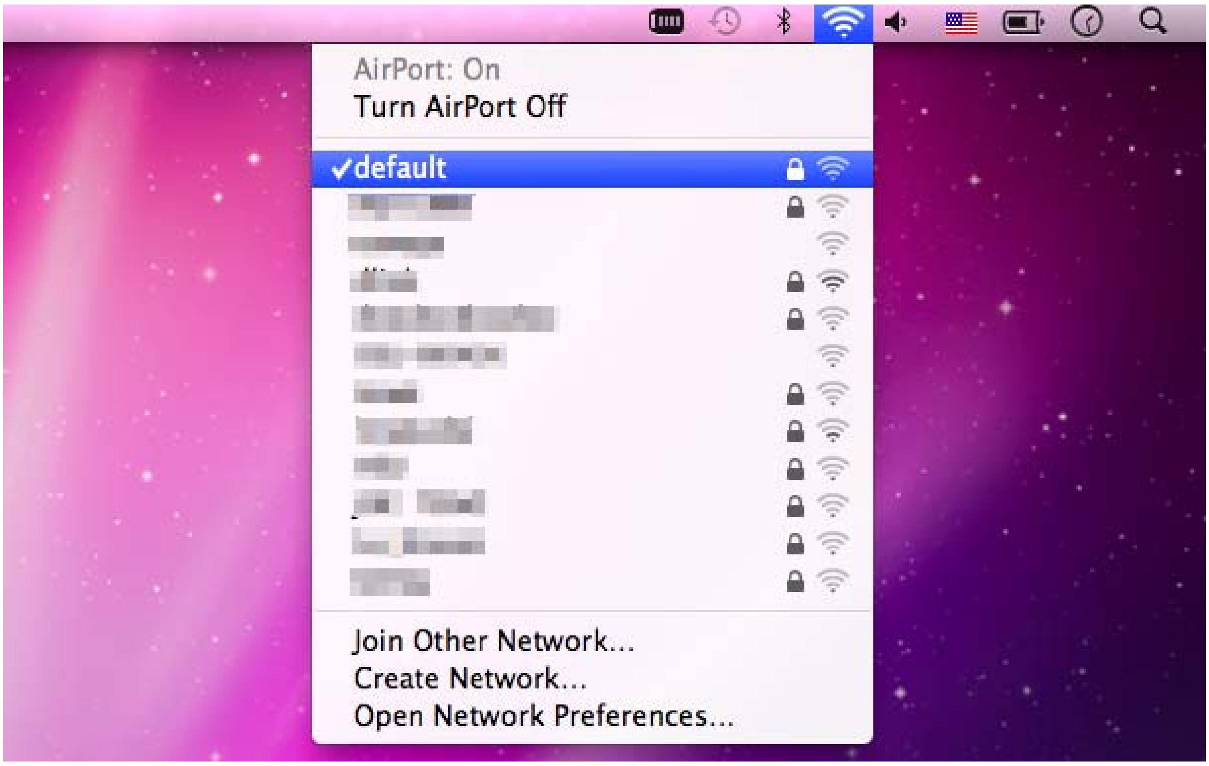


Figure 5-12 Connected to the Network

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**

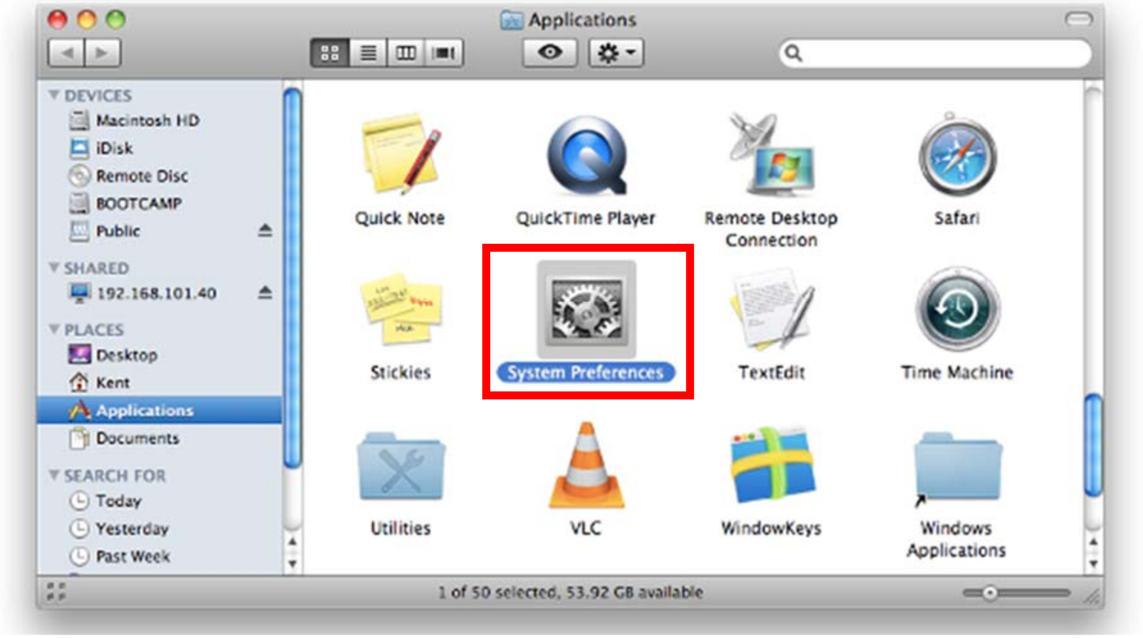


Figure 5-13 System Preferences

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

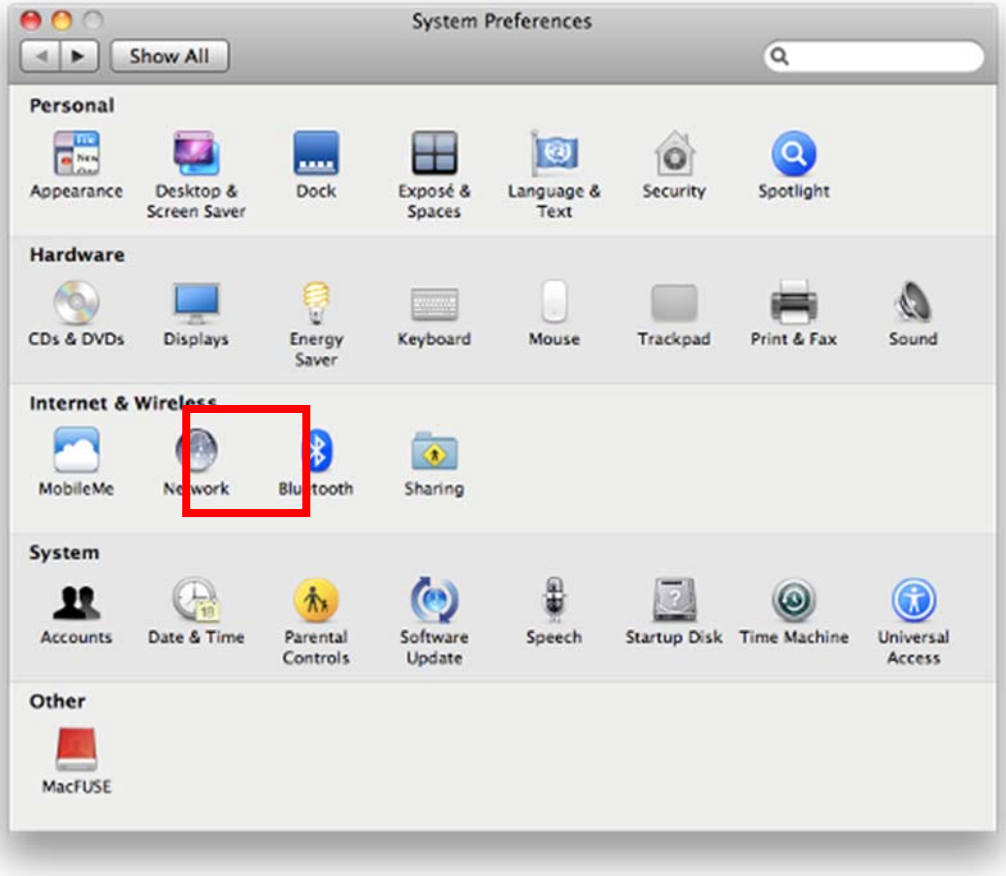


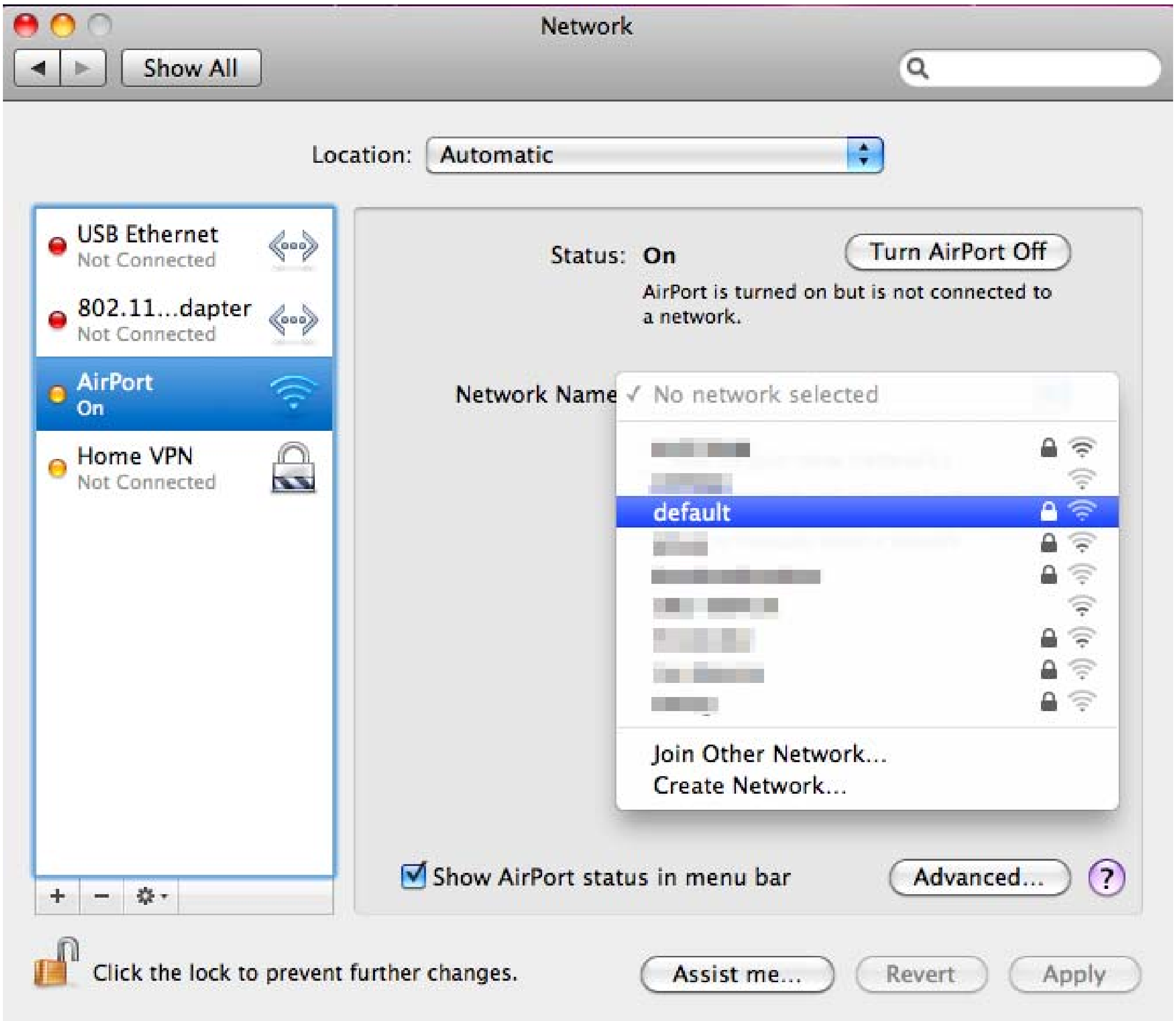
Figure 5-14 System Preferences -- Network

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”.



Location: Automatic

Status: On

AirPort is turned on but is not connected to a network.

Network Name ✓ No network selected

default

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

Figure 5-15 Selecting the Wireless Network

5.4 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

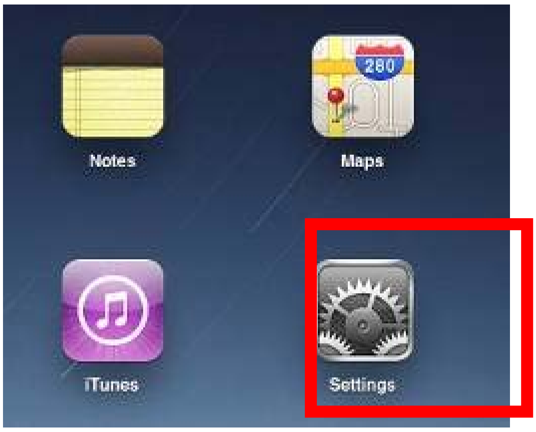


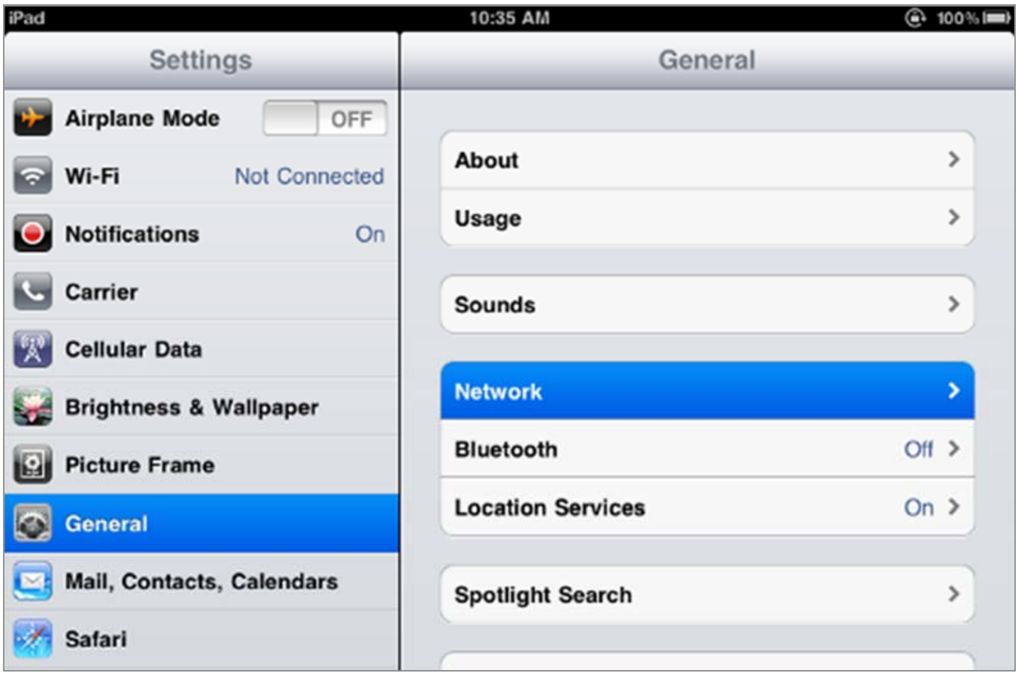
Figure 5-16 iPhone – Settings icon

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".



iPad 10:35 AM 100%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Carrier

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Mail, Contacts, Calendars

Safari

General

About >

Usage >

Sounds >

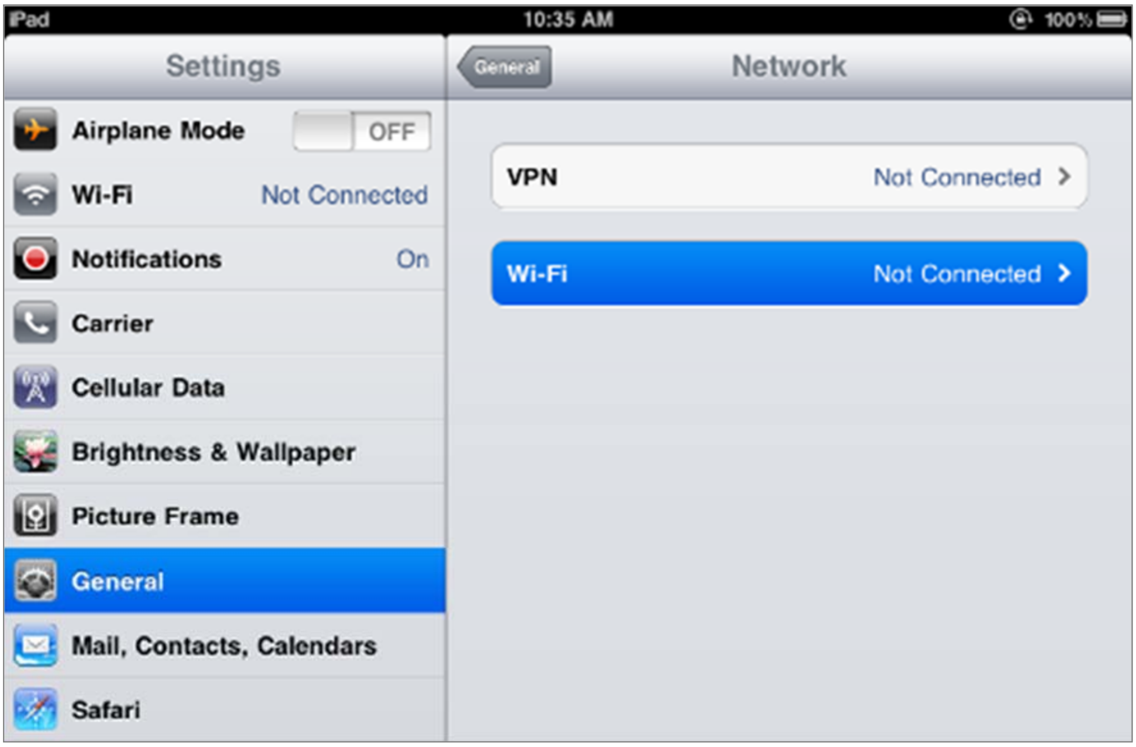
Network >

Bluetooth Off >

Location Services On >

Spotlight Search >

Figure 5-17 Wi-Fi Setting



iPad 10:35 AM 100%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Carrier

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Mail, Contacts, Calendars

Safari

General Network

VPN Not Connected

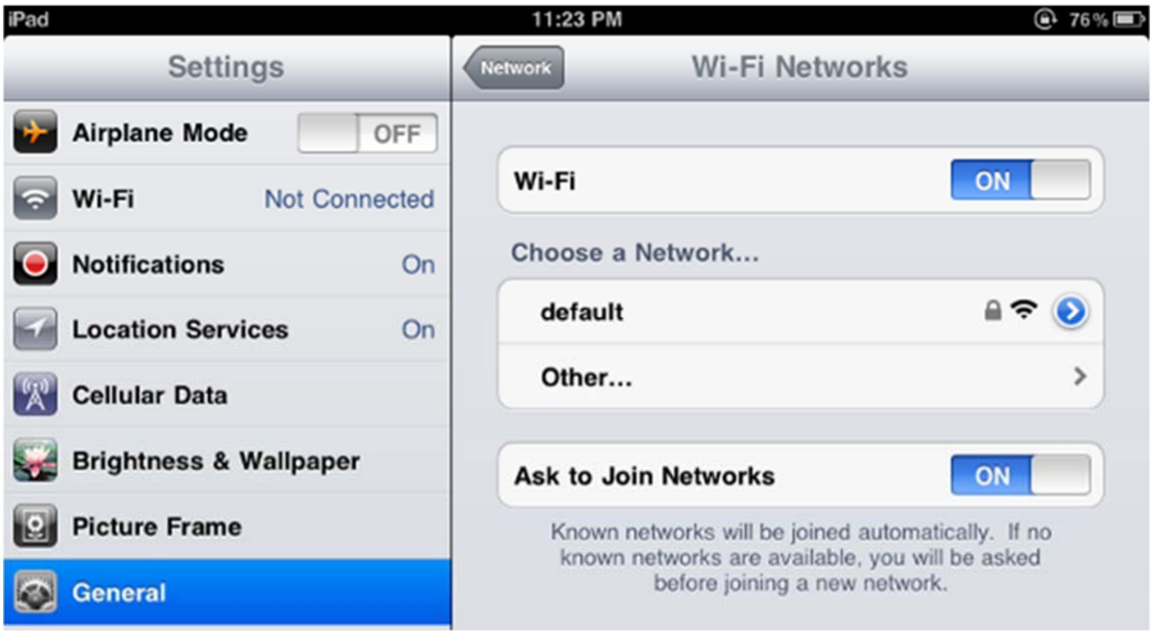
Wi-Fi Not Connected

Figure 5-18 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**]



iPad 11:23 PM 76%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Location Services On

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Network Wi-Fi Networks

Wi-Fi ON

Choose a Network...

default

Other...

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

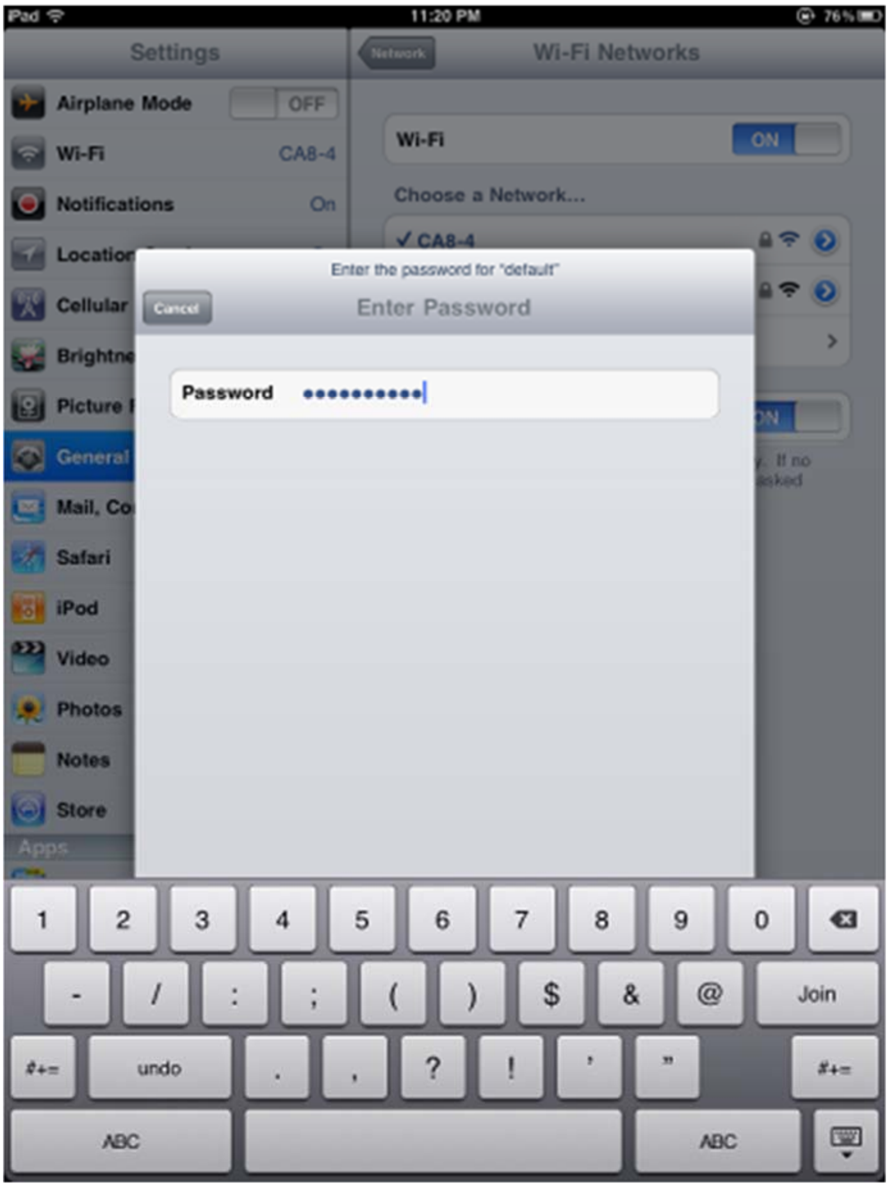
Figure 5-19 Turning on Wi-Fi

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.



Enter the password for "default"

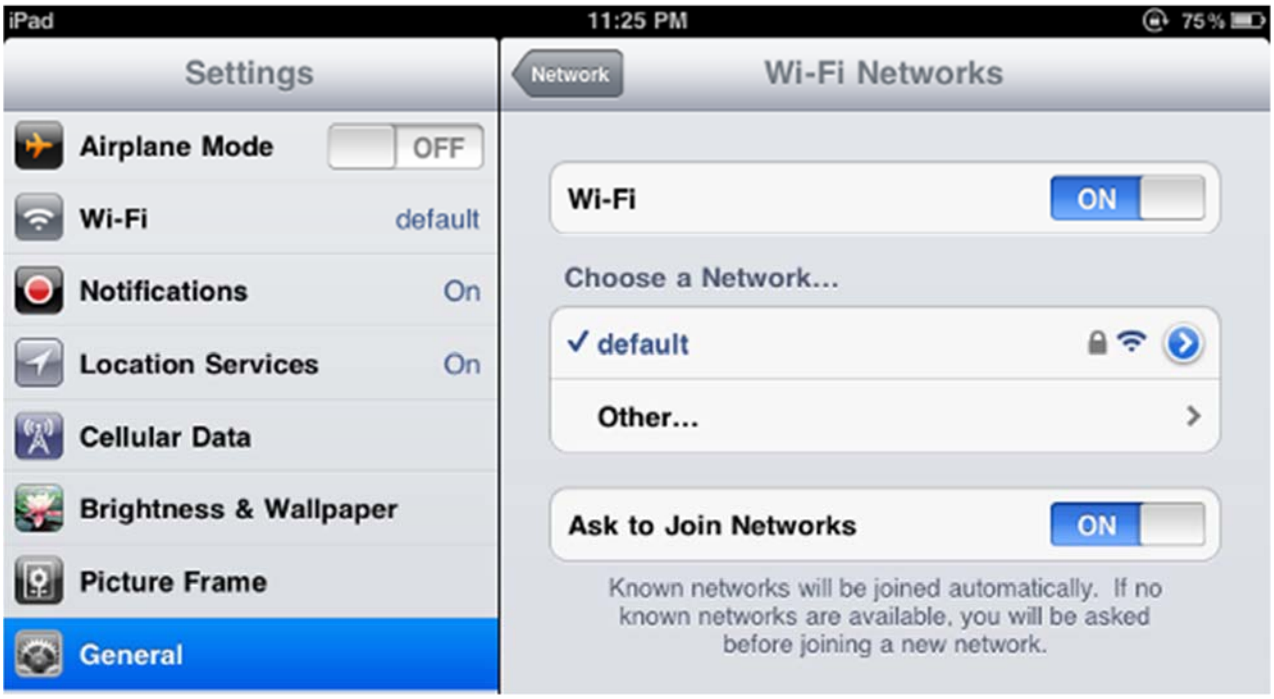
Enter Password

Password ●●●●●●●●●●●

Figure 5-20 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.



iPad 11:25 PM 75%

Settings

Airplane Mode OFF

Wi-Fi default

Notifications On

Location Services On

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Network

Wi-Fi Networks

Wi-Fi ON

Choose a Network...

✓ default

Other...

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Figure 5-21 iPhone -- Connected to the Network

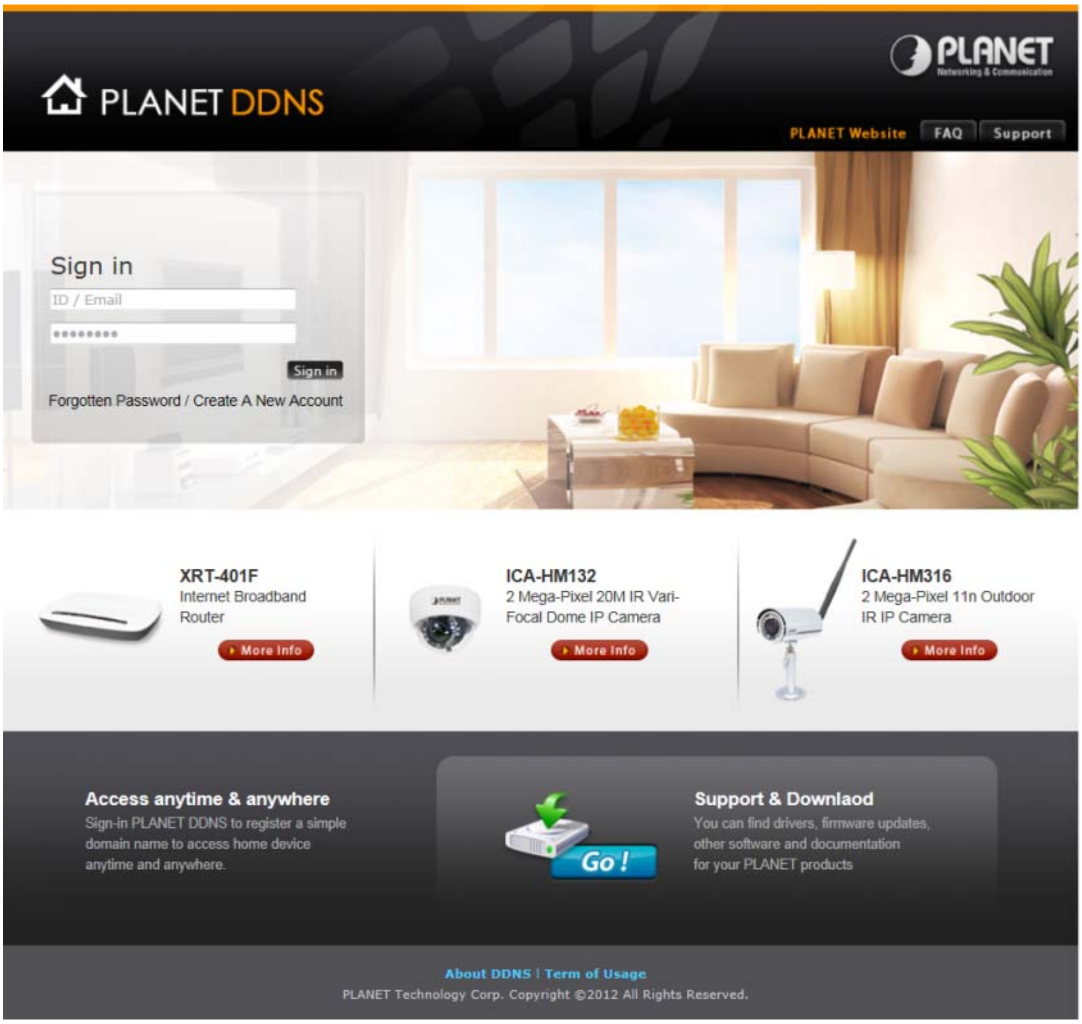
Appendix A: DDNS Application

Configuring PLANET DDNS steps:

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

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

Step 3: Input all DDNS settings.


PLANET DDNS
PLANET Networking & Communication
PLANET Website
FAQ
Support
Sign in
ID / Email
••••••••
Sign in
Forgotten Password / Create A New Account
XRT-401F
Internet Broadband Router
More Info
ICA-HM132
2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera
More Info
ICA-HM316
2 Mega-Pixel 11n Outdoor IR IP Camera
More Info
Access anytime & anywhere
Go !
Support & Downlaod
About DDNS | Term of Usage

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

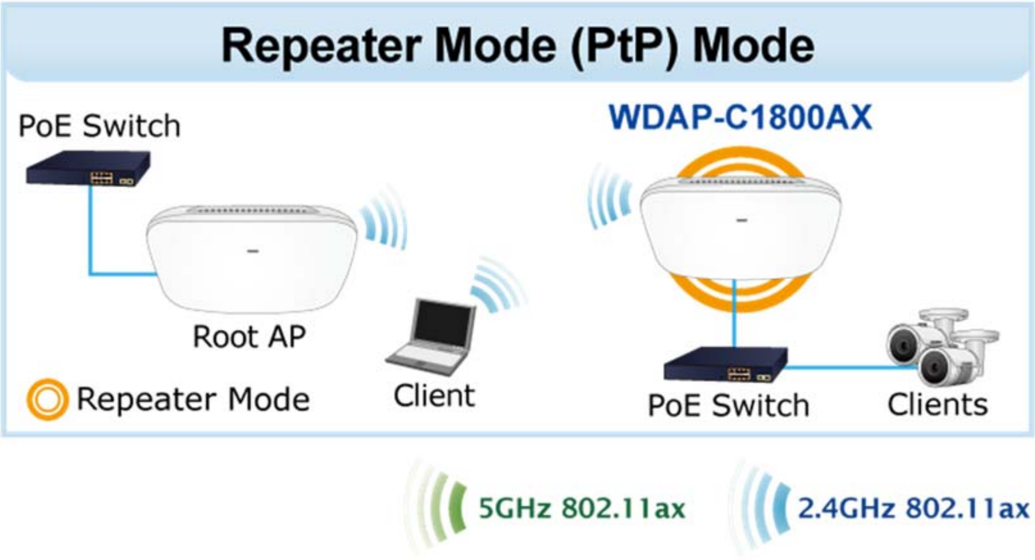
You can find drivers, firmware updates, other software and documentation for your PLANET products

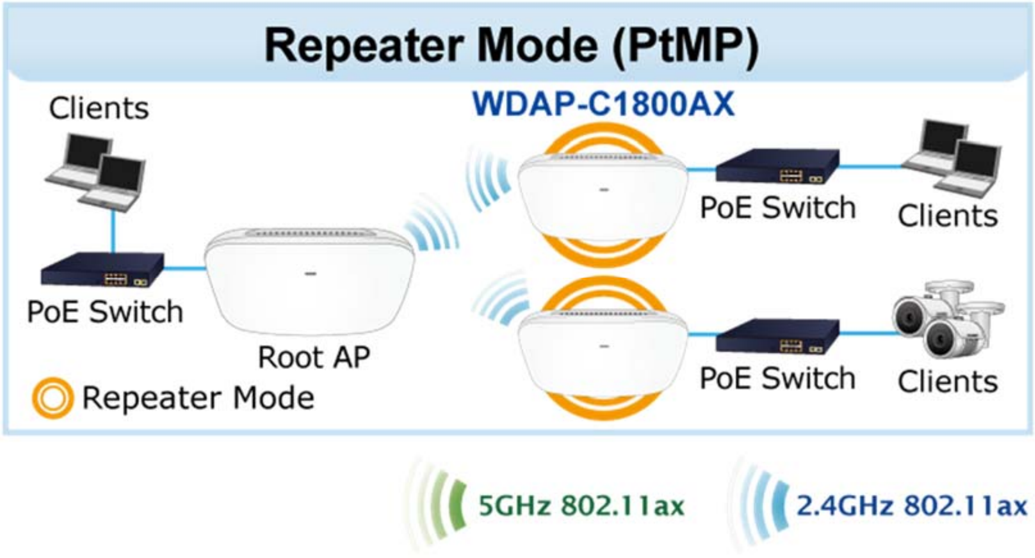
PLANET Technology Corp. Copyright ©2012 All Rights Reserved.

Appendix B: FAQs

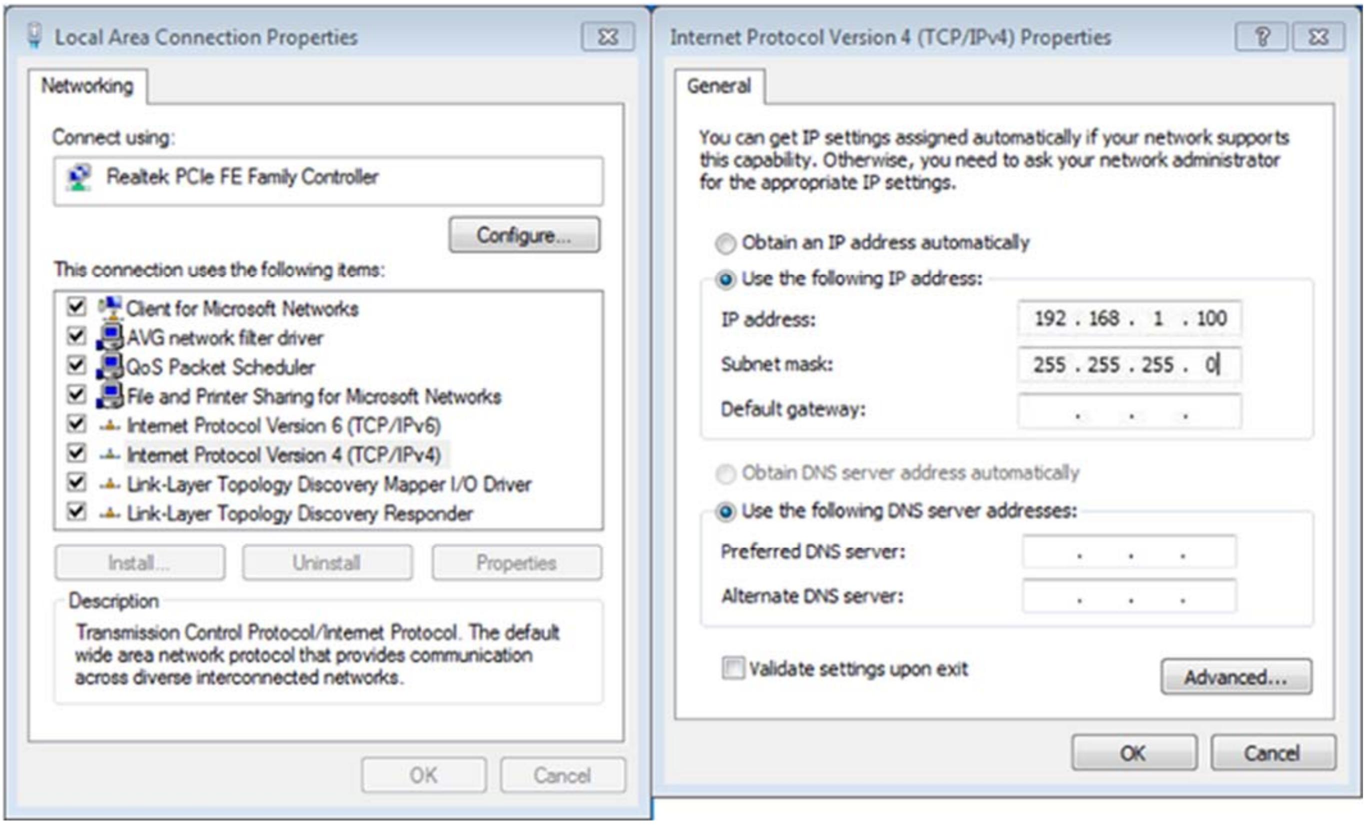
Q1: How to Set Up the AP Client Connection

Topology:





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**”.



Local Area Connection Properties

Networking

Connect using:

Realtek PCIe FE Family Controller

This connection uses the following items:

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

Description

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

Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

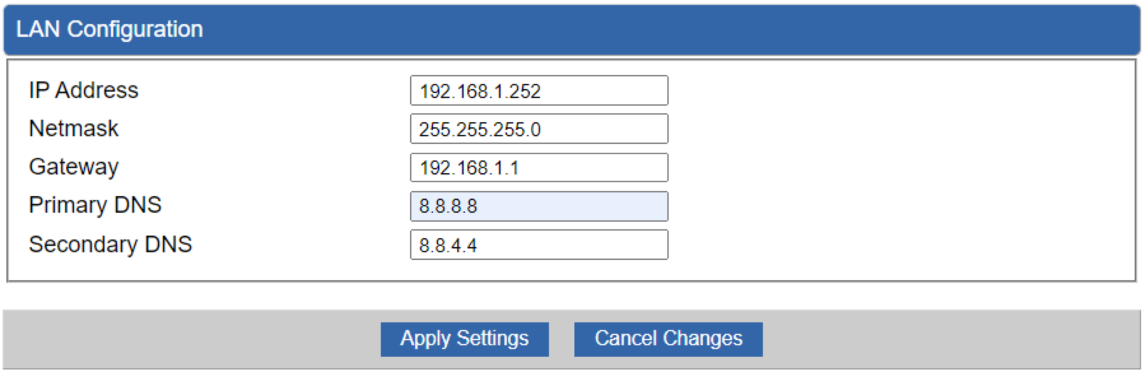
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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**.

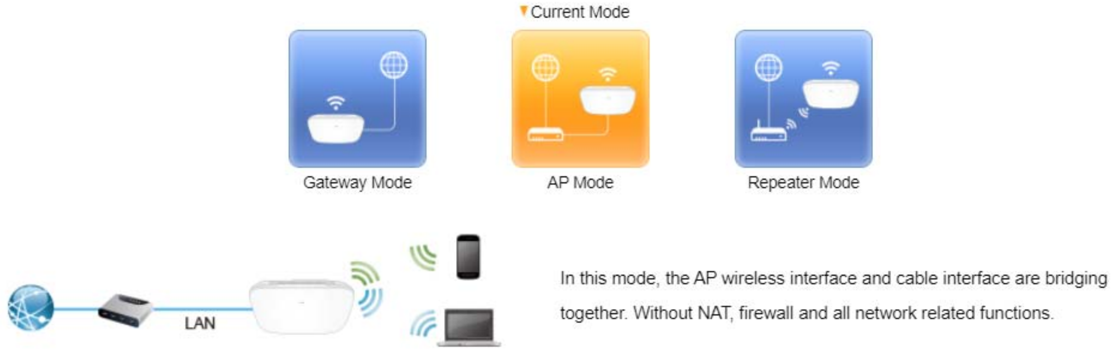


LAN Configuration

IP Address	192.168.1.252
Netmask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4

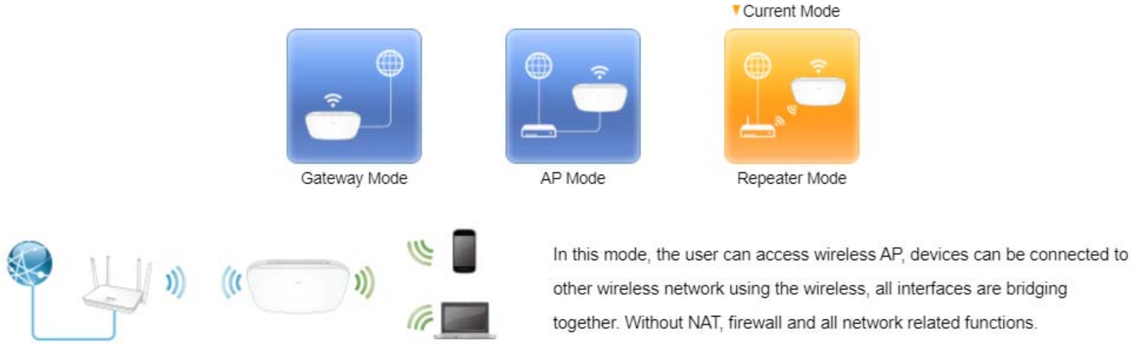
Step 3. In AP-1, go to “**Wizard**” to configure it to **AP Mode**. In AP-2, configure it to **Repeater Mode**.

AP-1



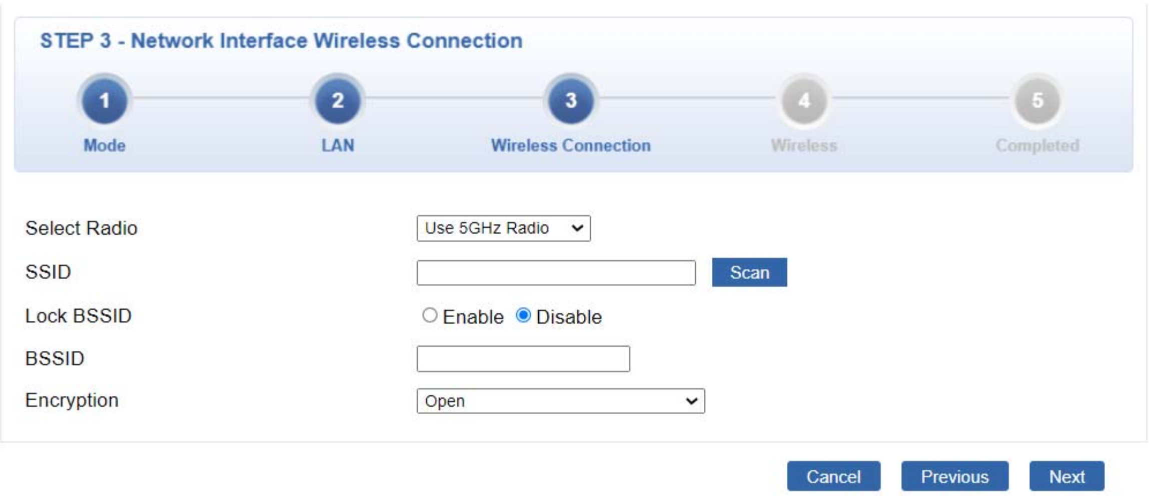
In this mode, the AP wireless interface and cable interface are bridging together. Without NAT, firewall and all network related functions.

AP-2



In this mode, the user can access wireless AP, devices can be connected to other wireless network using the wireless, all interfaces are bridging together. Without NAT, firewall and all network related functions.

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.

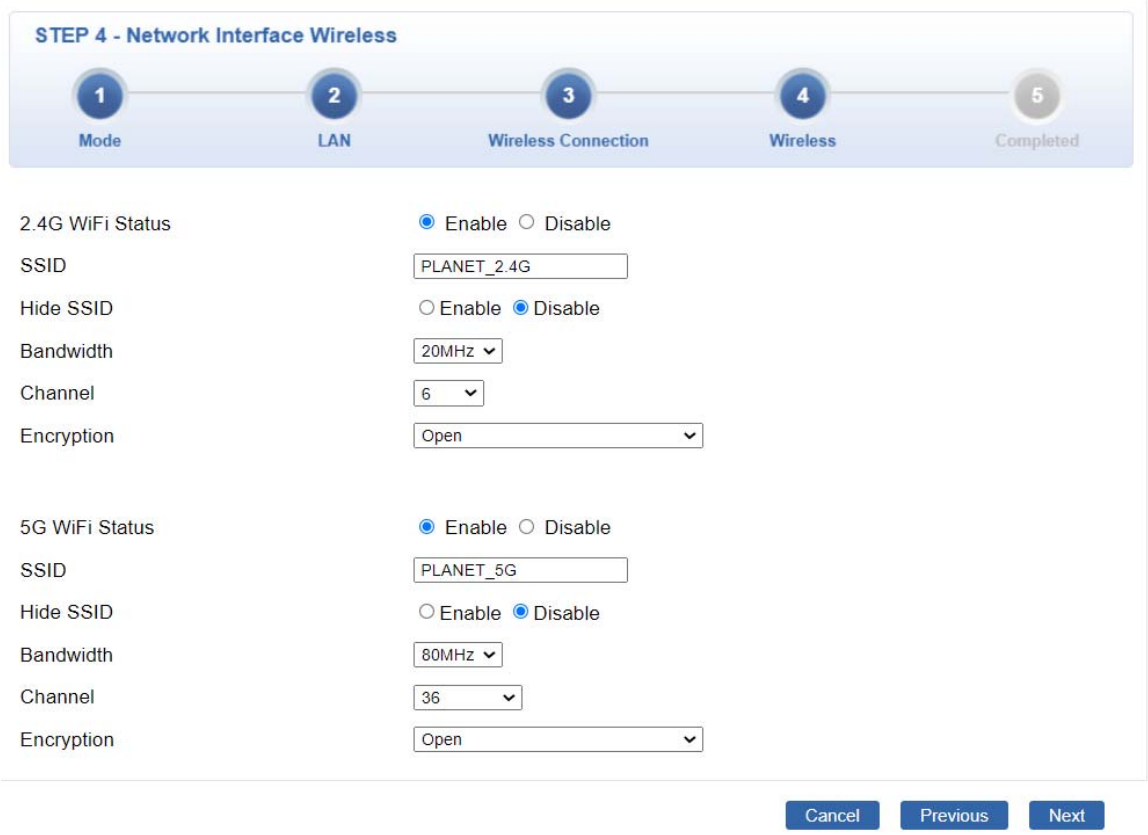


STEP 3 - Network Interface Wireless Connection

1 Mode — 2 LAN — 3 Wireless Connection — 4 Wireless — 5 Completed

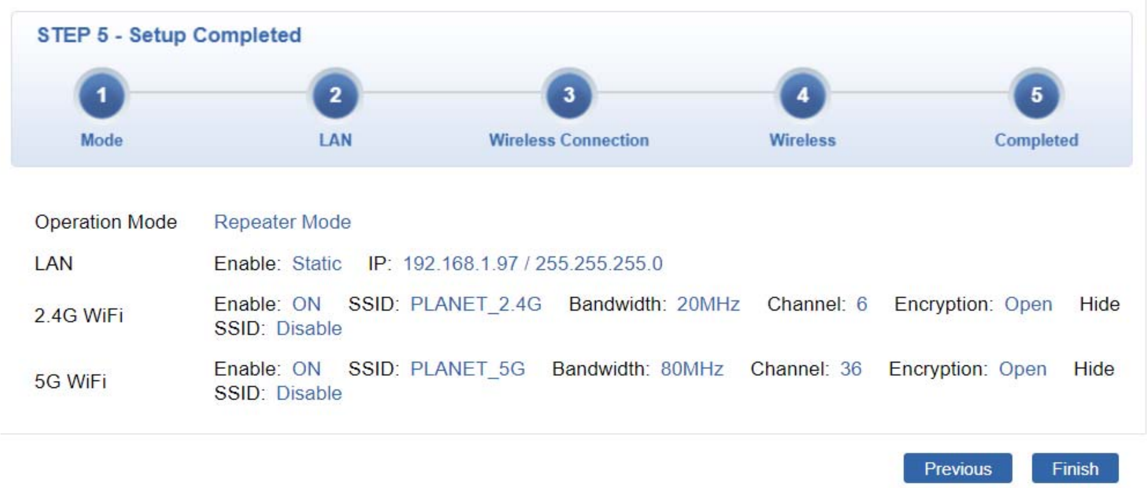
Select Radio	Use 5GHz Radio
SSID	
Lock BSSID	○ Enable ● Disable
BSSID	
Encryption	Open

Step 5. Click “**Next**” to finish the setting.



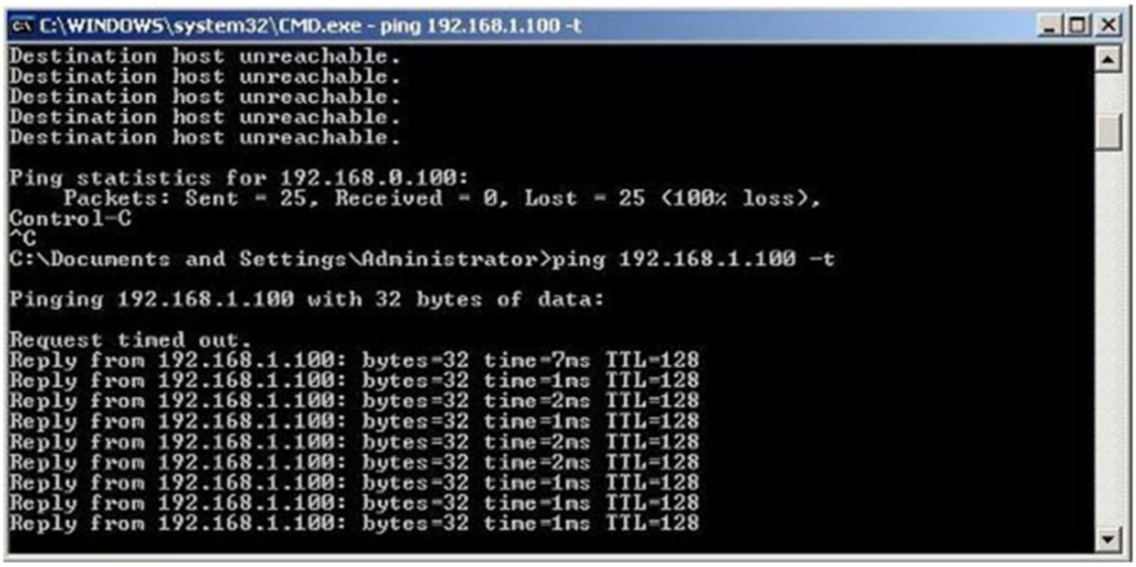
2.4G WiFi Status	● Enable ○ Disable
SSID	PLANET_2.4G
Hide SSID	○ Enable ● Disable
Bandwidth	20MHz
Channel	6
Encryption	Open
5G WiFi Status	● Enable ○ Disable
SSID	PLANET_5G
Hide SSID	○ Enable ● Disable
Bandwidth	80MHz
Channel	36
Encryption	Open

Step 6. Setup Completed



Operation Mode	Repeater Mode
LAN	Enable: Static IP: 192.168.1.97 / 255.255.255.0
2.4G WiFi	Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHz Channel: 6 Encryption: Open Hide SSID: Disable
5G WiFi	Enable: ON SSID: PLANET_5G Bandwidth: 80MHz Channel: 36 Encryption: Open Hide SSID: Disable

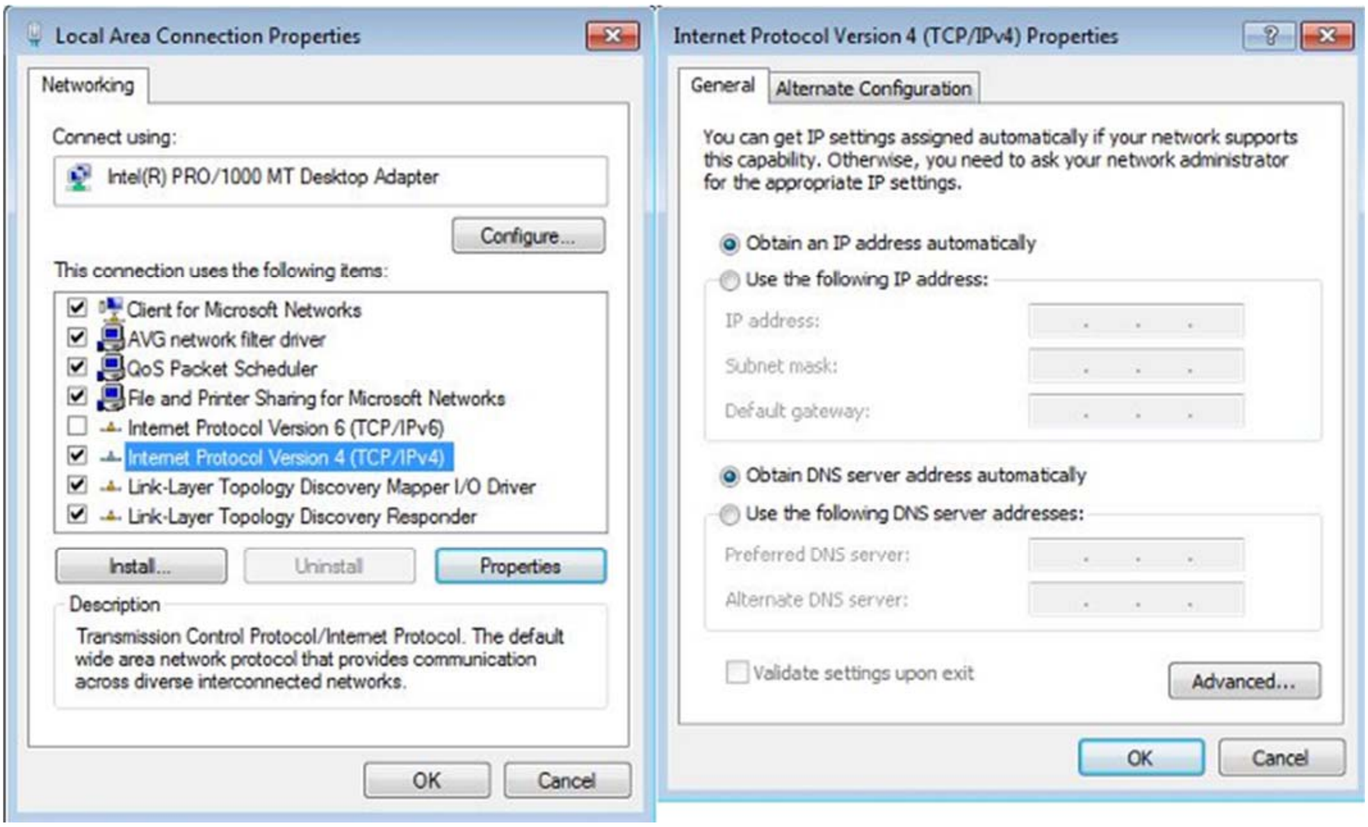
Step 7. Use command line tool to ping each other to ensure the link is successfully established. From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.100.



C:\WINDOWS\system32\CMD.exe - ping 192.168.1.100 -t

```
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

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

Description

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

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

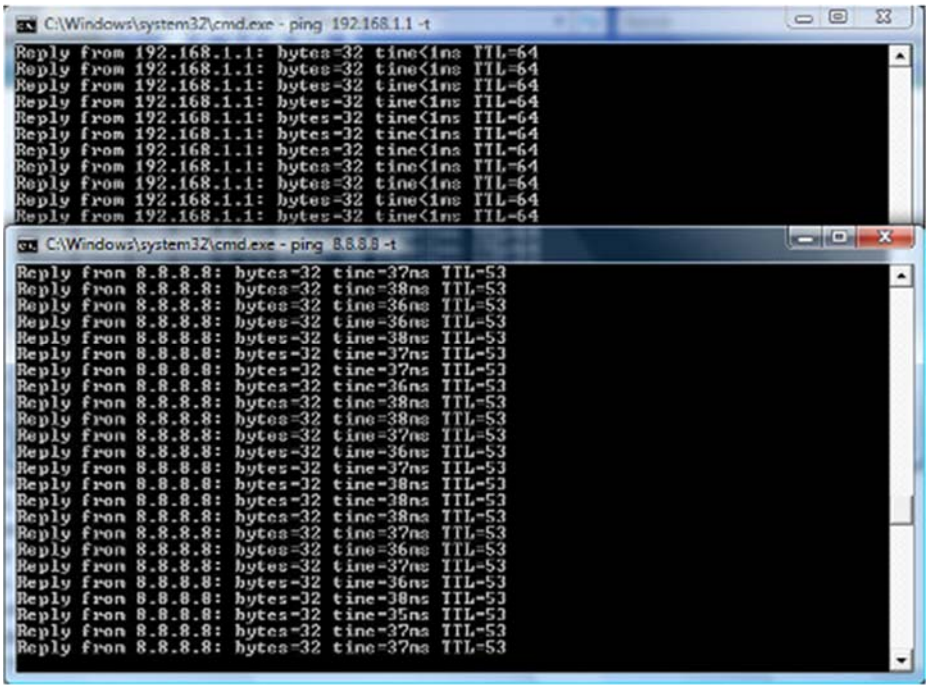
Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

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

wireless connection.



C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t

```
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=35ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
```

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

Scenario	Solution
	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 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 **11ac 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 **11ac Wireless AP** tenkina visus svarbiausius 2014/53/EU direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **11ac Wireless AP** splňuje základní požadavky a další příslušná ustanovení směrnice 2014/53/EU.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **11ac Wireless AP** megfelel az 2014/53/EU irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **11ac Wireless AP** overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **11ac 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 **11ac 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 **11ac 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 **11ac Wireless AP** vastab Euroopa Nõukogu direktiivi 2014/53/EU põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **11ac 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* **11ac Wireless AP***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ* 2014/53/EU	**Português**	**PLANET Technology Corporation**, declara que este **11ac 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 **11ac 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 **11ac 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 **11ac 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 **11ac Wireless AP** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive **2014/53/EU**
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **11ac 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 **11ac 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 **11ac Wireless AP** atbilst Direktīvas 2014/53/EU pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **11ac Wireless AP** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv **2014/53/EU**.