

User's Manual

1200Mbps 802.11ac Wave 2 Dual Band
Ceiling-mount Wireless Access Point
w/802.3at PoE+ and 2 10/100/1000T
LAN Ports

▶ **WDAP-C7210E**



Copyright

Copyright © 2022 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

FC This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution:

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

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

- (1) This device may not cause harmful interference
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

FCC Radiation Exposure Statement

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

CE Compliance Statement

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

Safety

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

WEEE regulation



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

Revision

User Manual of PLANET 802.11ac Dual Band Ceiling-mount Wireless Access Point

Model: WDAP-C7210E

Rev: 2.0 (Dec. 2022)

Part No. EM-WDAP-C7210E_v2.0

CONTENTS

Chapter 1.Product Introduction	4
1.1 Package Contents.....	4
1.2 Product Description	5
1.3 Product Features	11
1.4 Product Specifications.....	12
Chapter 2.Hardware Installation.....	15
2.1 Product Outlook.....	15
Chapter 3.Preparation	18
3.1 System Requirements	18
3.2 Installing the AP.....	18
Chapter 4.Quick Installation Guide.....	20
4.1 Connecting to the AP	20
4.1.1 Configuring the IP Address Manually	21
4.2 Starting Setup in the Web UI	24
Chapter 5.Configuring the AP	25
5.1 System	27
5.1.1 Operation Mode.....	28
5.1.2 Gateway Mode (Router).....	29
5.1.3 Dashboard.....	35
5.1.4 System Status	36
5.1.5 System Service	37
5.1.6 Statistics	38
5.1.7 Connection Status	38
5.1.8 RADIUS.....	39
5.1.9 Captive Portal.....	39
5.1.10 SNMP	41
5.1.11 NMS.....	42
5.1.12 Remote Syslog	42
5.1.13 Event Log	43
5.2 Network.....	44
5.2.1 WAN	45
5.2.2 LAN.....	47
5.2.3 UPnP	48

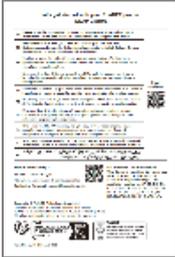
5.2.4	Routing	48
5.2.5	RIP.....	49
5.2.6	OSPF.....	49
5.2.7	IGMP	50
5.2.8	IPv6	50
5.2.9	DHCP	51
5.2.10	DDNS	53
5.3	Security.....	55
5.3.1	Firewall	55
5.3.2	MAC Filtering.....	58
5.3.3	IP Filtering	59
5.3.4	Web Filtering	60
5.3.5	Port Forwarding.....	61
5.3.6	QoS	62
5.3.7	DMZ.....	63
5.4	Wireless	64
5.4.1	Repeater.....	65
5.4.2	2.4G Wi-Fi	66
5.4.3	5G Wi-Fi	67
5.4.4	MAC ACL.....	68
5.4.5	Wi-Fi Advanced	69
5.4.6	Wi-Fi Statistics.....	70
5.4.7	Connection Status	70
5.5	Maintenance	71
5.5.1	Administrator	72
5.5.2	Date and Time	72
5.5.3	Saving/Restoring Configuration	73
5.5.4	Firmware Upgrading.....	73
5.5.5	Reboot / Reset	74
5.5.6	Auto Reboot	74
5.5.7	Diagnostics	75
5.5.8	LED.....	75
Chapter 6	Quick Connection to a Wireless Network.....	76
6.1	Windows XP (Wireless Zero Configuration).....	76
6.2	Windows 7/8/10 (WLAN AutoConfig)	78
6.3	Mac OS X 10.x	80
6.4	iPhone/iPod Touch/iPad	84

Appendix A: Planet Smart Discovery Utility	87
Appendix B: DDNS Application	88
Appendix C: FAQs	89
Appendix D: Troubleshooting	95
Appendix E: Glossary	97

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WDAP-C7210E Wireless AP. Before installing the AP, please verify the contents inside the package box.

Package Contents of WDAP-C7210E			
WDAP-C7210E	QR Code Sheet	Ethernet Cable	Mounting Kit
			



If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description

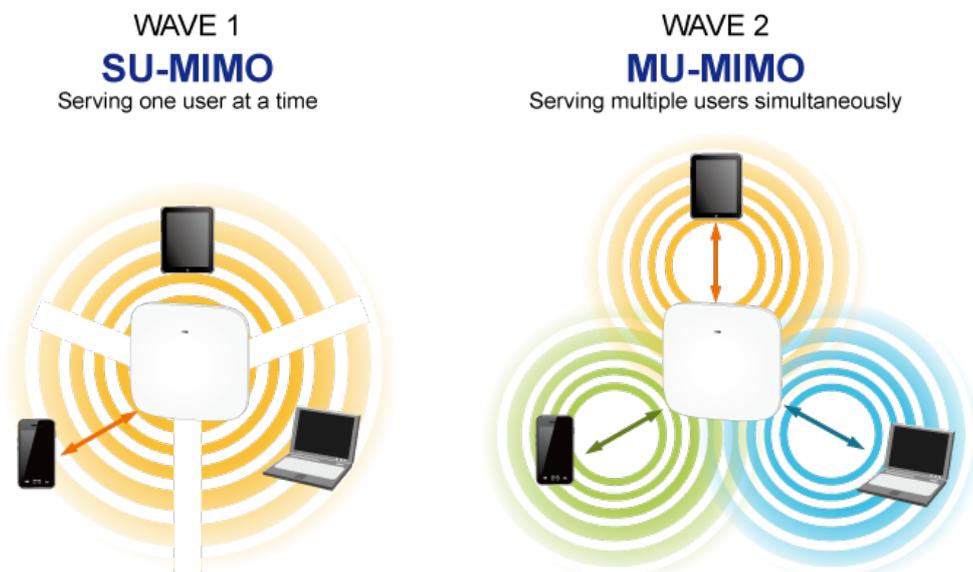
Ultra-high-speed, Wave 2 MU-MIMO Wireless LAN Solution

PLANET WDAP-C7210E 1200Mbps Wave 2 Dual Band 802.11ac Wireless AP supports central management through PLANET NMS controllers. With IEEE 802.11ac Wave 2 MU-MIMO 2T2R dual-band technology, the WDAP-C7210E provides a maximum wireless speed of 867Mbps at 5GHz and 300Mbps at 2.4GHz. The new version of the WDAP-C7210E not only has more powerful performance but also supports PLANET CloudViewer app for remotely monitoring devices from anywhere.



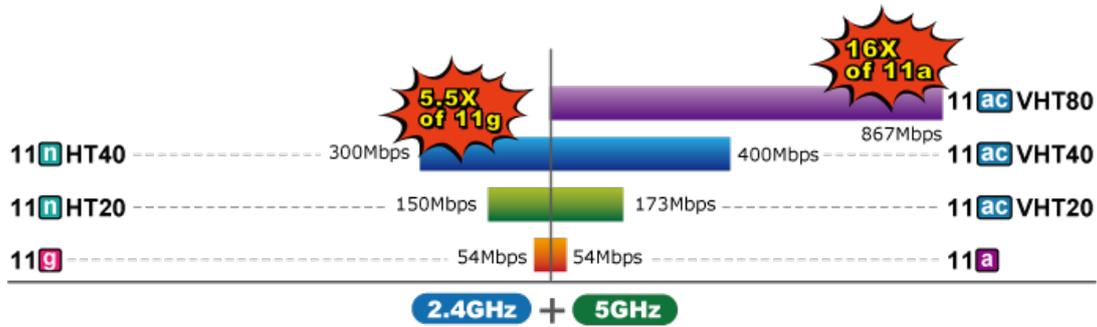
Benefits of MU-MIMO under 802.11ac Wave 2

With the MU-MIMO Wave 2 technology, the WDAP-C7210E, installed in public areas such as hotspots, airports and conferences, reduces the frustration that Wi-Fi users often experience in downloading web pages, e-mail file attachments and media contents. For cellular operators, the WDAP-C7210E provides a better Wi-Fi user experience, reducing the likelihood of users turning off Wi-Fi and putting more load on the cellular network. For enterprises, this technology also can solve Wi-Fi congestion issues in open work spaces and conference rooms.



Powerful Dual-band WLAN Solution

PLANET WDAP-C7210E, adopting the IEEE 802.11ac Wave 2 standard, provides a high-speed transmission of power and data, meaning two remote nodes in the **5GHz** frequency band can be bridged. The **2.4GHz** wireless connection can also be used simultaneously. Furthermore, the WDAP-C7210E adopts the high-class Mediatek SoC (System-on-a-Chip), which provides higher stability to meet the stringent requirements of the solution.

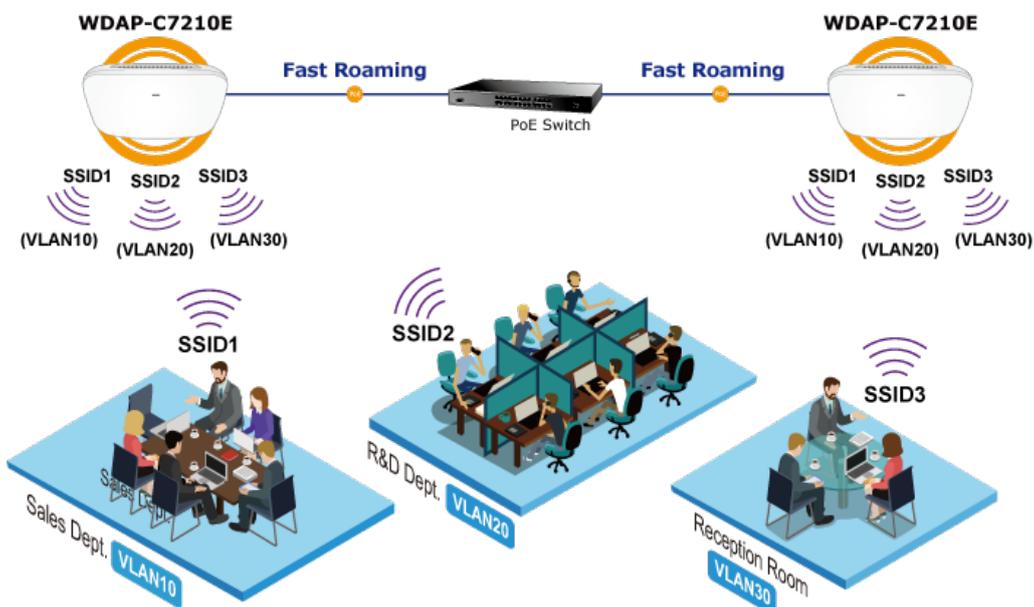


WDAP-C7210E Data Transmission Rates 1200Mbps

Enhanced Security and Rigorous Authentication

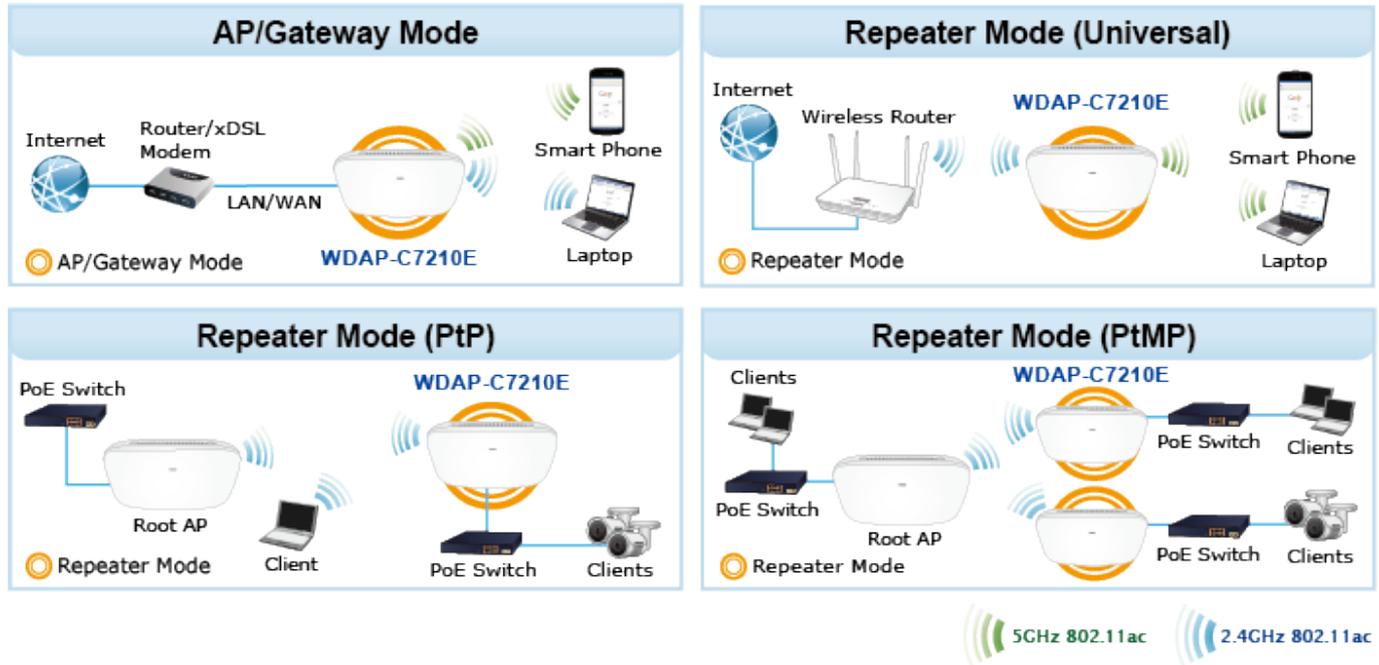
The WDAP-C7210E supports WPA / WPA2, WPA-PSK, WPA2-PSK and WPS3-PSK wireless encryptions, the advanced WPA2-AES mechanism and 802.1X RADIUS authentication, which can effectively prevent eavesdropping by unauthorized users or bandwidth occupied by unauthenticated wireless access. Furthermore, any users are granted or denied access to the wireless LAN network based on the ACL (Access Control List) that the administrator pre-established. For management purposes, the IEEE 802.1Q VLAN supported allows multiple VLAN tags to be mapped to multiple SSIDs to distinguish the wireless access.

Multi-SSID + VLAN + Fast Roaming



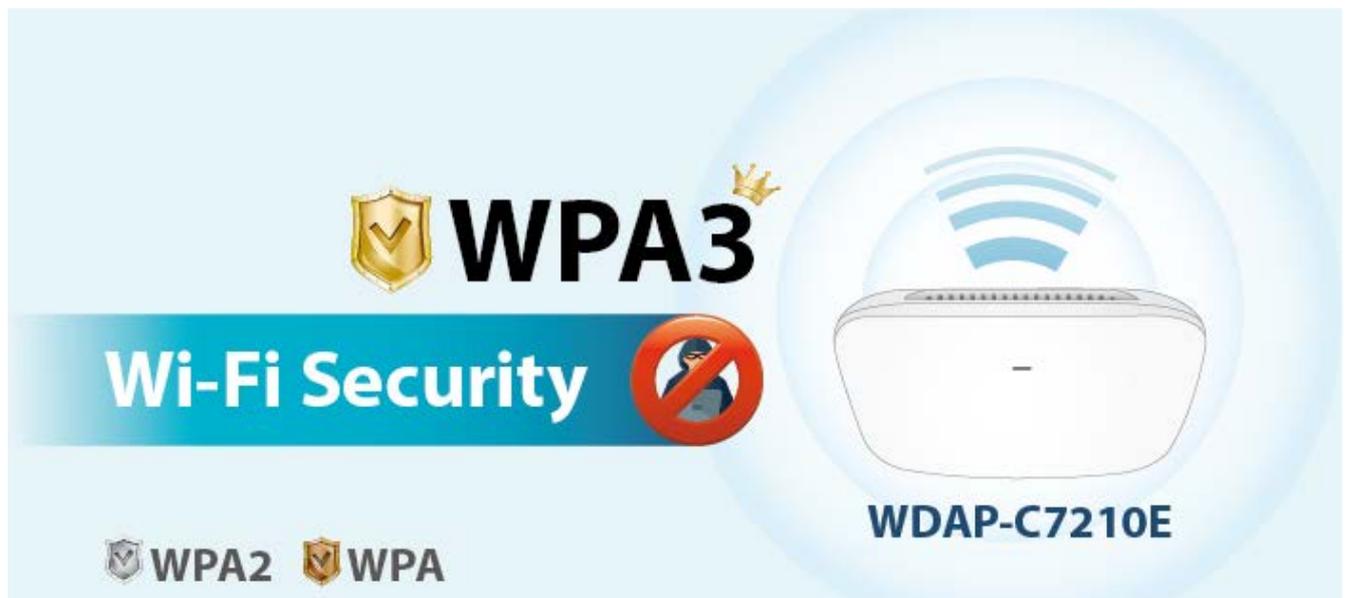
Multiple Operation Modes for Various Applications

The WDAP-C7210E supports AP, Gateway and Repeater mode, through which it provides more flexibility for users when wireless network is established. Compared with general wireless access points, the WDAP-C7210E offers more powerful and flexible capability for wireless clients.



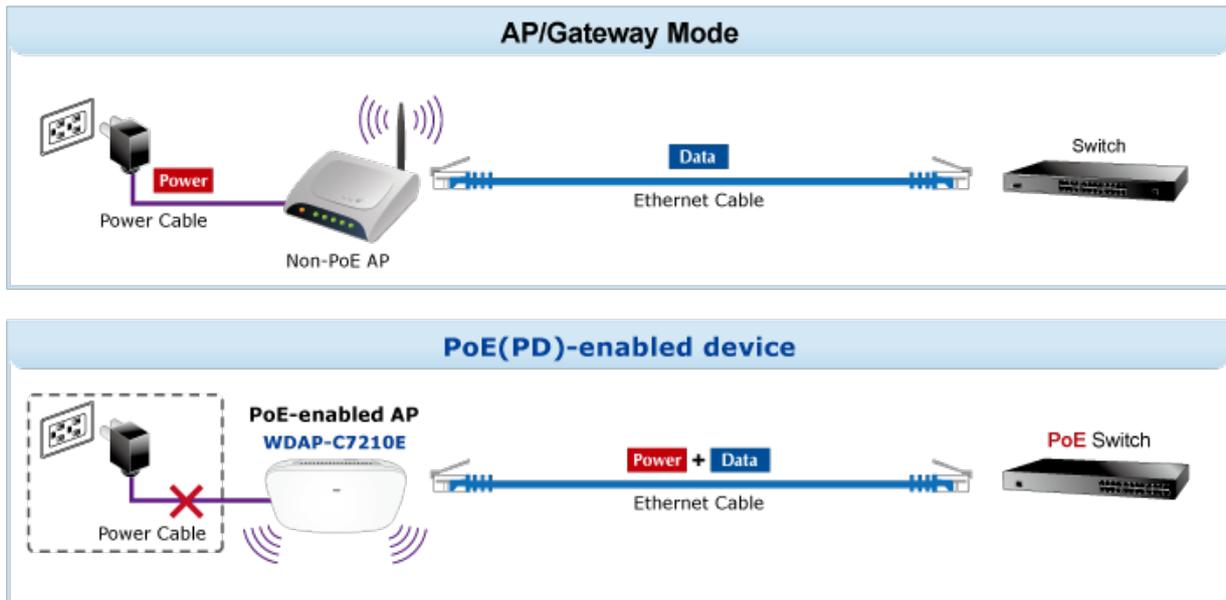
WPA3 Next Generation Security for Your WLAN Solution

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.



Ceiling-mount Design for Your Environment

With the standard IEEE802.3at Power over Ethernet (PoE) design, the WDAP-C7210E 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-C7210E 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-C7210E 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-C7210E 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 scheduled reboot setting, the WDAP-C7210E is easy for the administrator to deploy and manage without on-site maintenance. Moreover, you can use PLANET NMS controller series, WS switch series, VR series, ICG-2515 router series, and AP control function to deliver wireless profiles to multiple APs simultaneously, thus making the central management simple.

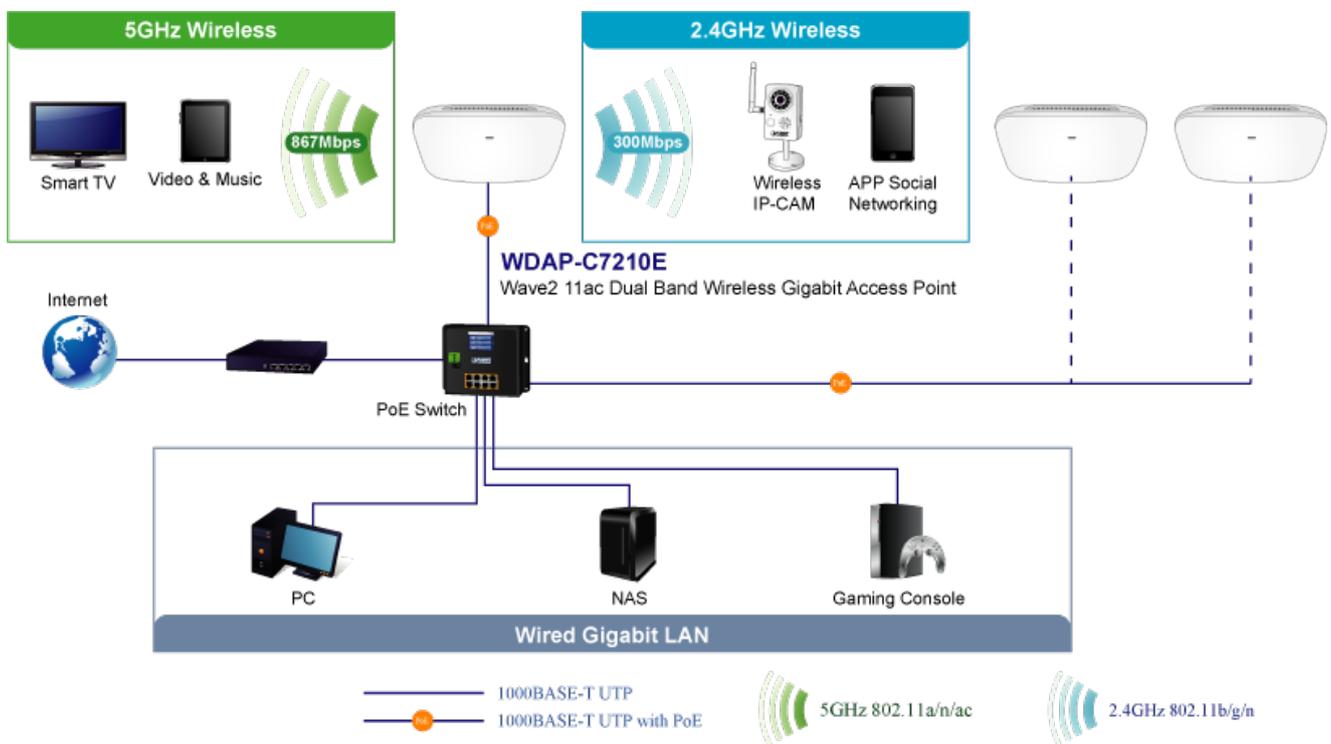
***Note:** The WDAP-C7210E and WDAP-C7210E (V2) are two different devices. Please make sure the model is right before setting it with NMS equipment. Check the model name from the label to make sure that the firmware is upgraded on the right version of the AP.

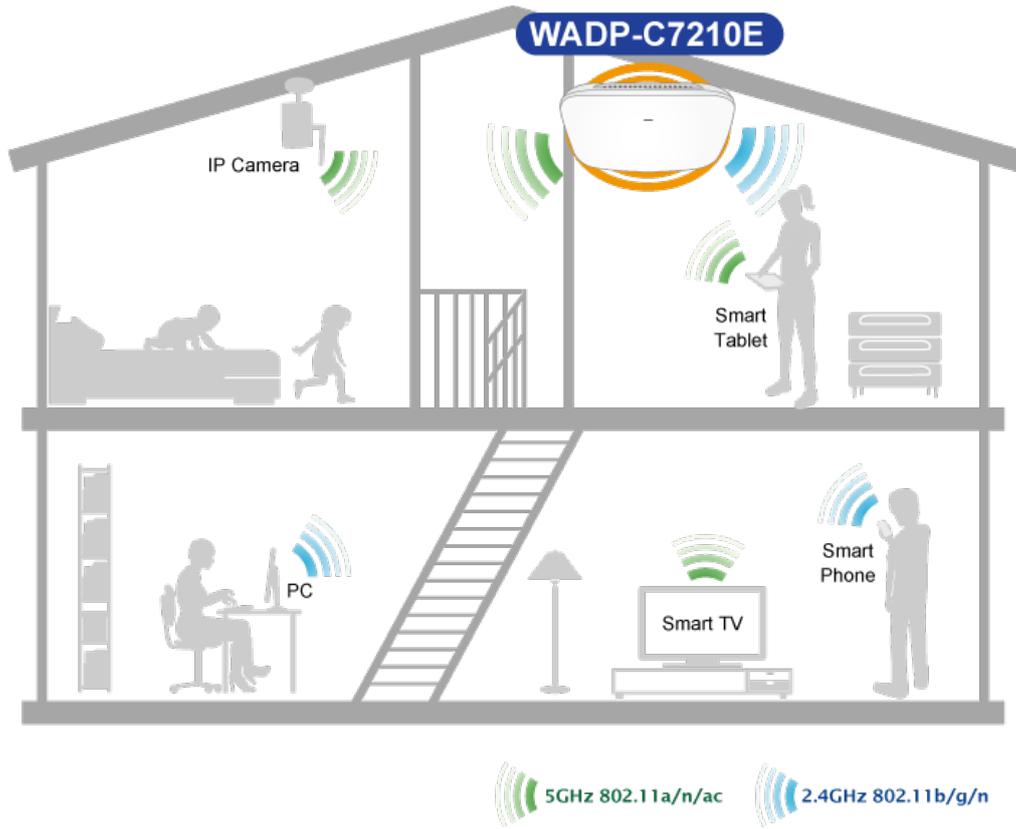


Applications

Extremely High-speed and Dual Band Make Wi-Fi Transmission More Powerful

The WDAP-C7210E delivers the dual band technology 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 high-definition (HD) video and any other multimedia application via 5GHz band. Moreover, the Gigabit Ethernet port of the WDAP-C7210E offers ultra-fast wired connections that utilize the maximum wireless bandwidth; therefore, users will have real wireless speed over 100Mbps. With outstanding stability of high-speed wireless transmission, the WDAP-C7210E can provide users with excellent experience in multimedia streaming with your mobile devices anywhere, anytime.





1.3 Product Features

Industrial Compliant Wireless LAN and LAN

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

RF Interface Characteristics

- 802.11ac Wave 2 2T2R MIMO architecture with data rate of up to 1200Mbps (300Mbps at 2.4GHz and 867Mbps at 5GHz)
- High output power with multiply-adjustable transmit power control

Multiple Operation Modes and Wireless Features

- Multiple operation modes: Access Point, Gateway, Repeater mode
- 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 Fast Roaming with 802.11k, 802.11v, and 802.11r

Secure Network Connection

- Full encryption supported: WAP-PSK/WPA2-PSK, WPA2-PSK, WPA2-PSK/ WPA3-PSK, WPA3-PSK, WPA/WPA2 Enterprise, WPA2 Enterprise and 802.1X RADIUS authentication
- Supports 802.1Q VLAN and SSID-to-VLAN mapping
- 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
- 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
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS system and CloudViewer for deployment management at the same time

1.4 Product Specifications

Product	WDAP-C7210E 1200Mbps 802.11ac Wave 2 Dual Band 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:	2 x 2.4GHz internal 5dBi antenna, 2 x 5GHz internal 4dBi antenna
Reset Button	Reset button on the rear side (Press over 7 seconds to reset the device to factory default)	
LED Indicators	SYS, 2.4GHz, 5GHz	
Dimensions (W x D x H)	186 x 186 x 35.8mm	
Weight	380 ±5g	
Power Requirements	48V DC IN, 0.5A, IEEE 802.3at PoE+ or 12V DC IN, 1.0A from DC Jack (5.5 x 2.1mm)	
Power Consumption	< 12W	
Mounting	Ceiling Mount	
Wireless Interface Specifications		
Standard	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	802.11ac: OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM) 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM) 802.11b: DSSS (DBPSK / DQPSK / CCK)	
Band Mode	2.4G / 5G concurrent mode	
Frequency Range	2.4GHz: FCC: 2.412~2.462GHz ETSI: 2.412~2.472GHz 5GHz: FCC: 5.180~5.32240GHz, 5.500745~5.825GHz ETSI: 5.180~5.320GHz, 5.500~5.180~5.700GHz	
Operating Channels	2.4GHz: FCC: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	

	<p>ETSI: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</p> <p>5GHz:</p> <p>FCC: 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)</p> <p>ETSI: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 (19 Channels)</p> <p>*5GHz channel list will vary in different countries according to their regulations.</p>																																																											
Max. Transmit Power (dBm)	<p>FCC: up to 22 ± 1dBm</p> <p>ETSI: < 20dBm (EIRP)</p>																																																											
Receive Sensitivity	<table border="1"> <thead> <tr> <th>Network Mode</th> <th>Data Rate</th> <th>Receive Sensitivity (dBm)</th> </tr> </thead> <tbody> <tr> <td colspan="3">2.4GHz</td> </tr> <tr> <td rowspan="2">802.11b</td> <td>1Mbps</td> <td>-99</td> </tr> <tr> <td>11Mbps</td> <td>-92</td> </tr> <tr> <td rowspan="2">802.11g</td> <td>6Mbps</td> <td>-95</td> </tr> <tr> <td>54Mbps</td> <td>-82</td> </tr> <tr> <td rowspan="2">802.11n HT20</td> <td>MCS0/MCS8</td> <td>-95</td> </tr> <tr> <td>MCS7/MCS15</td> <td>-77</td> </tr> <tr> <td rowspan="2">802.11n HT40</td> <td>MCS0/MCS8</td> <td>-93</td> </tr> <tr> <td>MCS7/MCS15</td> <td>-75</td> </tr> <tr> <td colspan="3">5GHz</td> </tr> <tr> <td rowspan="2">802.11a</td> <td>6Mbps</td> <td>-92</td> </tr> <tr> <td>54Mbps</td> <td>-75</td> </tr> <tr> <td rowspan="2">802.11n HT20</td> <td>MCS0/MCS8</td> <td>-91</td> </tr> <tr> <td>MCS7/MCS15</td> <td>-72</td> </tr> <tr> <td rowspan="2">802.11n HT40</td> <td>MCS0/MCS8</td> <td>-88</td> </tr> <tr> <td>MCS7/MCS15</td> <td>-70</td> </tr> <tr> <td rowspan="2">802.11ac VHT20</td> <td>MCS0</td> <td>-92</td> </tr> <tr> <td>MCS8</td> <td>-70</td> </tr> <tr> <td rowspan="2">802.11ac VHT40</td> <td>MCS0</td> <td>-89</td> </tr> <tr> <td>MCS9</td> <td>-65</td> </tr> <tr> <td rowspan="2">802.11ac VHT80</td> <td>MCS0</td> <td>-87</td> </tr> <tr> <td>MCS9</td> <td>-61</td> </tr> </tbody> </table>	Network Mode	Data Rate	Receive Sensitivity (dBm)	2.4GHz			802.11b	1Mbps	-99	11Mbps	-92	802.11g	6Mbps	-95	54Mbps	-82	802.11n HT20	MCS0/MCS8	-95	MCS7/MCS15	-77	802.11n HT40	MCS0/MCS8	-93	MCS7/MCS15	-75	5GHz			802.11a	6Mbps	-92	54Mbps	-75	802.11n HT20	MCS0/MCS8	-91	MCS7/MCS15	-72	802.11n HT40	MCS0/MCS8	-88	MCS7/MCS15	-70	802.11ac VHT20	MCS0	-92	MCS8	-70	802.11ac VHT40	MCS0	-89	MCS9	-65	802.11ac VHT80	MCS0	-87	MCS9	-61
	Network Mode	Data Rate	Receive Sensitivity (dBm)																																																									
	2.4GHz																																																											
	802.11b	1Mbps	-99																																																									
		11Mbps	-92																																																									
	802.11g	6Mbps	-95																																																									
		54Mbps	-82																																																									
	802.11n HT20	MCS0/MCS8	-95																																																									
		MCS7/MCS15	-77																																																									
	802.11n HT40	MCS0/MCS8	-93																																																									
		MCS7/MCS15	-75																																																									
	5GHz																																																											
	802.11a	6Mbps	-92																																																									
		54Mbps	-75																																																									
	802.11n HT20	MCS0/MCS8	-91																																																									
		MCS7/MCS15	-72																																																									
	802.11n HT40	MCS0/MCS8	-88																																																									
		MCS7/MCS15	-70																																																									
	802.11ac VHT20	MCS0	-92																																																									
MCS8		-70																																																										
802.11ac VHT40	MCS0	-89																																																										
	MCS9	-65																																																										
802.11ac VHT80	MCS0	-87																																																										
	MCS9	-61																																																										
Software Features																																																												
LAN	<p>Static IP / Dynamic IP</p> <p>Supports IP-MAC binding</p>																																																											
WAN	<ul style="list-style-type: none"> ▪ Static IP ▪ Dynamic IP ▪ PPPoE ▪ PPTP ▪ L2TP 																																																											

Wireless Mode	<ul style="list-style-type: none"> ▪ Access Point ▪ Gateway ▪ Repeater
Channel Width	20MHz, 40MHz, 80MHz
Encryption Security	WPA, WPA-PSK, WPA2, WPA2-PSK, WPA3-PSK, 802.1X
Wireless Security	Enable/Disable SSID Broadcast
	Wireless max. 32 MAC addresses filtering
	User Isolation
Max. SSIDs	8 (4 per radio)
Max. Clients	64 per radio
Max. WDS Peers	4
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
	Fast Roaming
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 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
	SNMP v1/v2c/v3 support, MIB I/II, Private MIB
Central Management	Applicable controllers: NMS-500, NMS-1000V
Environment & Certification	
Temperature	Operating: 0 ~ 40 degrees C
	Storage: -40 ~ 70 degrees C
Humidity	Operating: 10 ~ 90% (non-condensing)
	Storage: 5 ~ 90% (non-condensing)
Regulatory	CE, RoHS

Chapter 2. Hardware Installation

2.1 Product Outlook

WDAP-C7210E

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

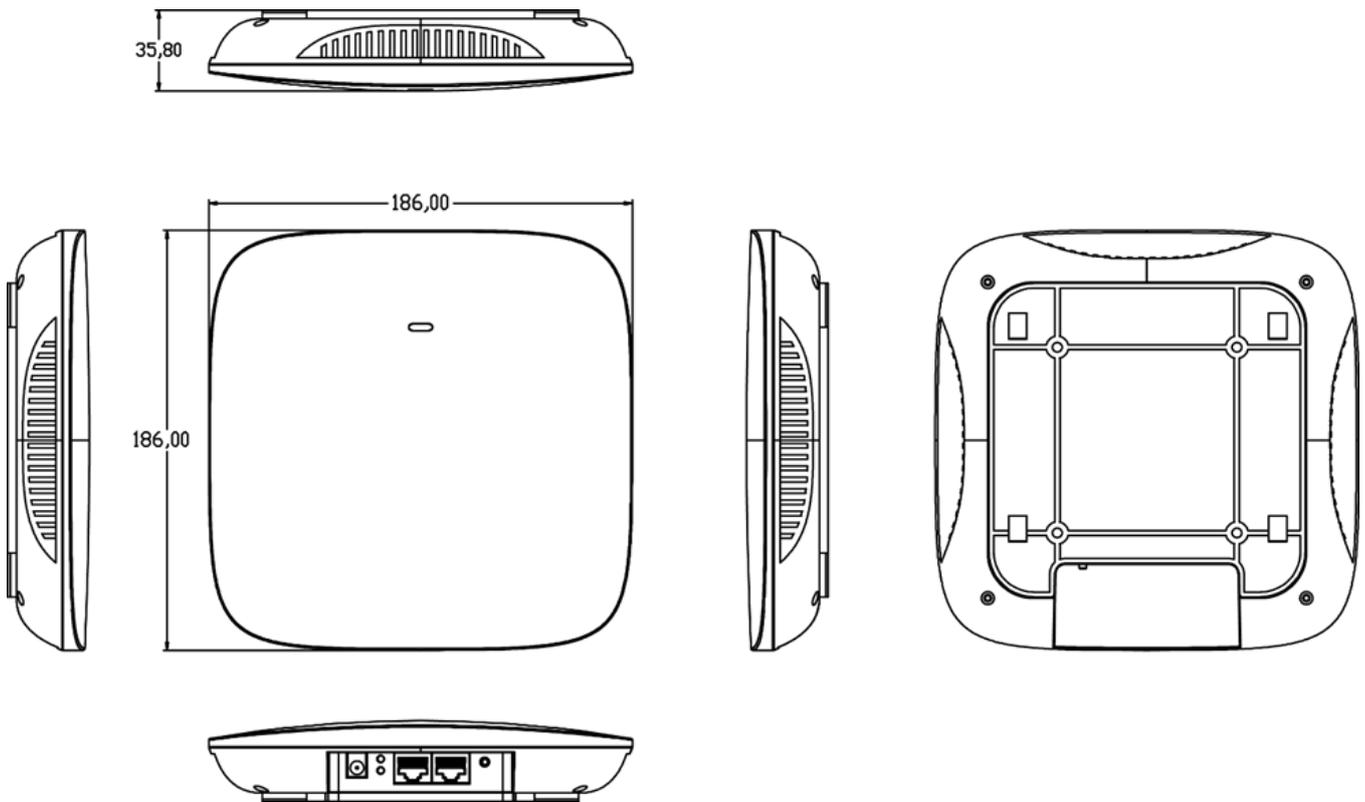


Figure 2-1 WDAP-C7210E Triple Viewing

■ Front Panel

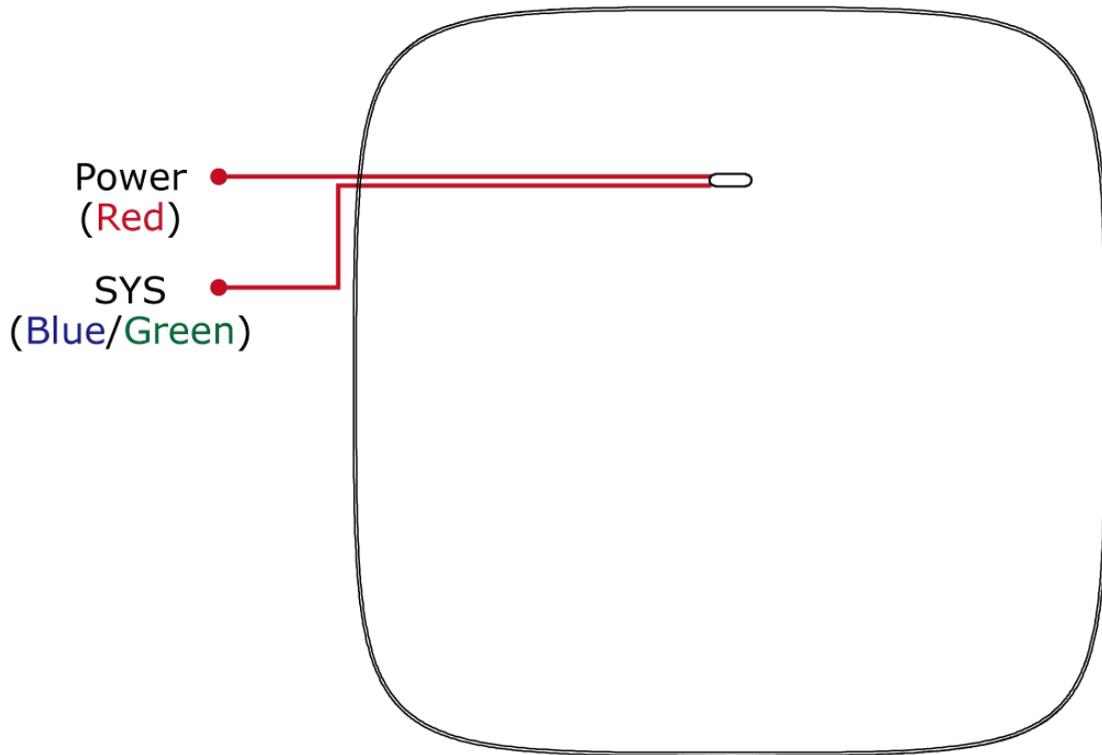


Figure 2-2 WDAP-C7210E Front Panel

LED Definition

LED	STATUS	FUNCTION
PWR	On (Red)	The access point is on.
	Off	System is operating.
SYS	On (Green)	Wireless LAN is working. 5GHz enabled.
	On (Blue)	Wireless LAN is working. 2.4GHz enabled. 5GHz disabled.
	Off	Wireless LAN disabled or LED status disabled.



Dual Band 802.11ax 1800Mbps Ceiling-mount Wireless Access Point w/802.3at PoE+ & 2 10/100/1000T LAN Ports

» [WDAP-C1800AX](#)



■ Rear Panel

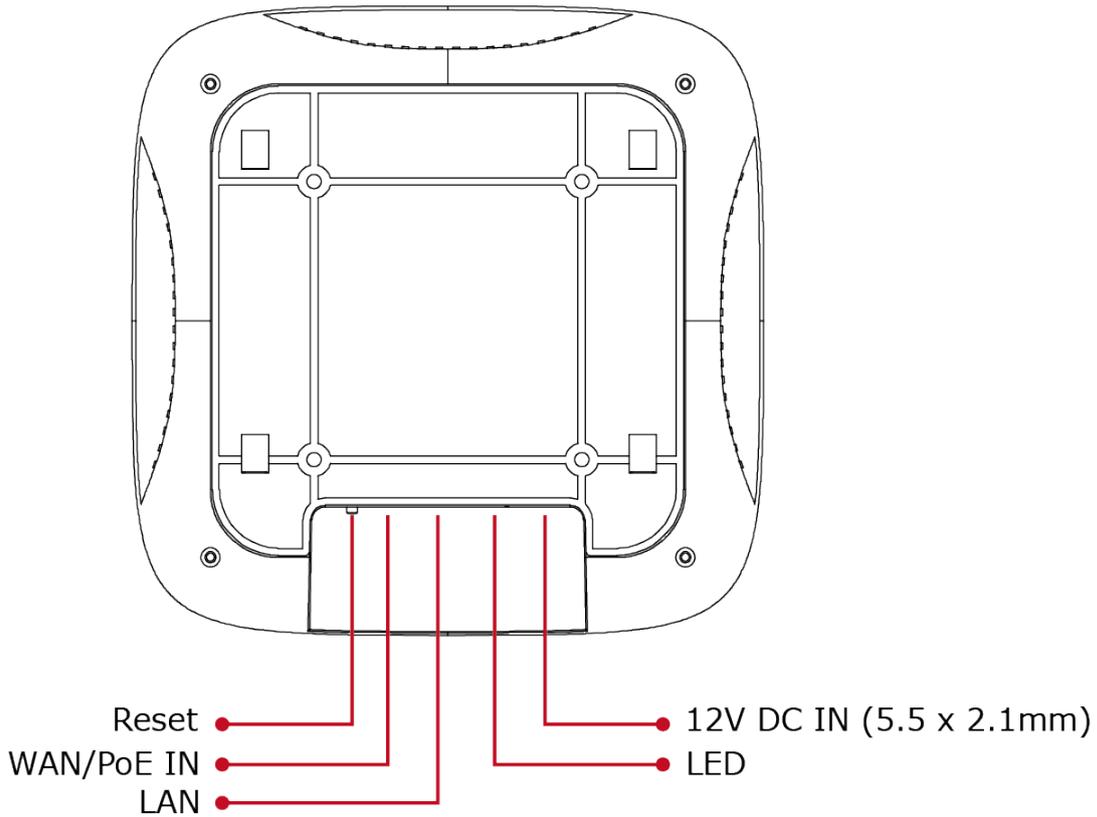


Figure 2-3 WDAP-C7210E Rear Panel

■ Bottom Panel

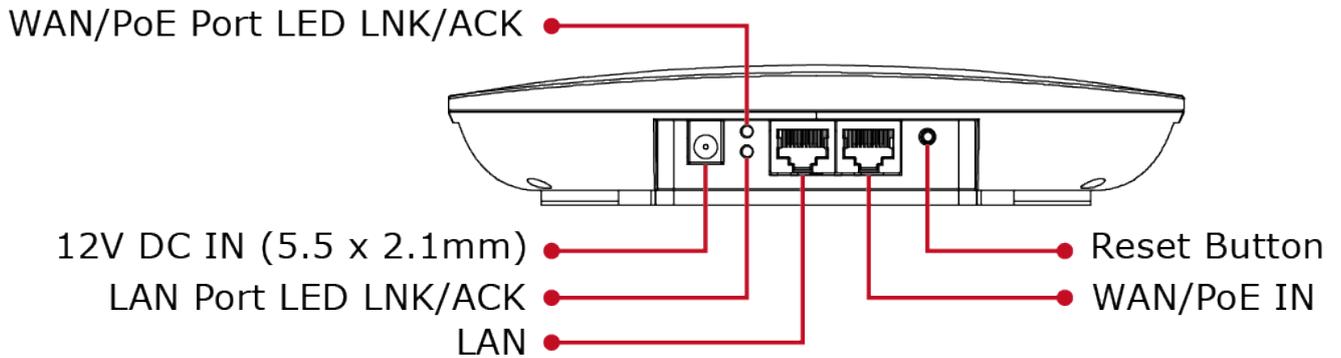


Figure 2-4 WDAP-C7210E Bottom Panel

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.
LAN	LAN port connecting to the network equipment.
PoE/WAN	LAN/WAN port with Power over Ethernet (PoE) IN
Reset	To restore to the factory default setting, press and hold the Reset Button for about 7 seconds, and then release it.

Chapter 3. Preparation

3.1 System Requirements

- Broadband Internet Access Service (Cable/xDSL/Ethernet connection)
- One IEEE 802.3at PoE switch (supply power to the WDAP-C7210E)
- PCs with a working Ethernet adapter and an Ethernet cable with RJ45 connectors
- PCs running Windows 7/10/11, MAC OS 10 or later, Linux, UNIX or other platforms compatible with TCP/IP protocols



1. The AP in the following instructions refers to PLANET WDAP-C7210E.
2. It is recommended to use Internet Explorer 11, Firefox or Chrome to access the AP.

3.2 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.

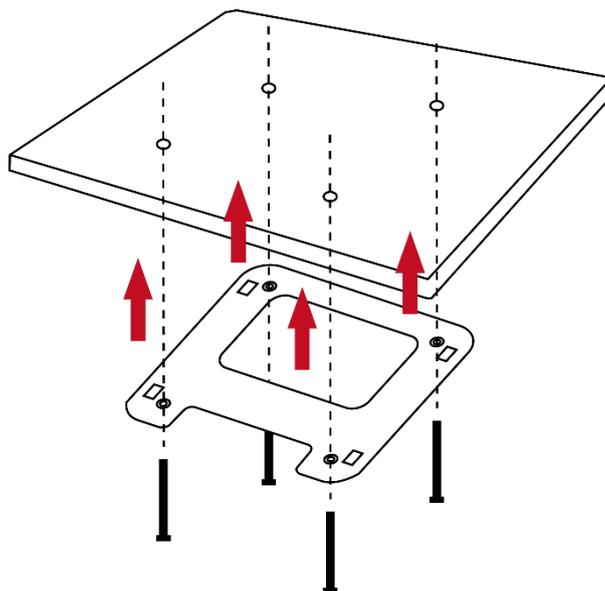


Figure 3-1 Mounting the Bracket

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-C7210E.

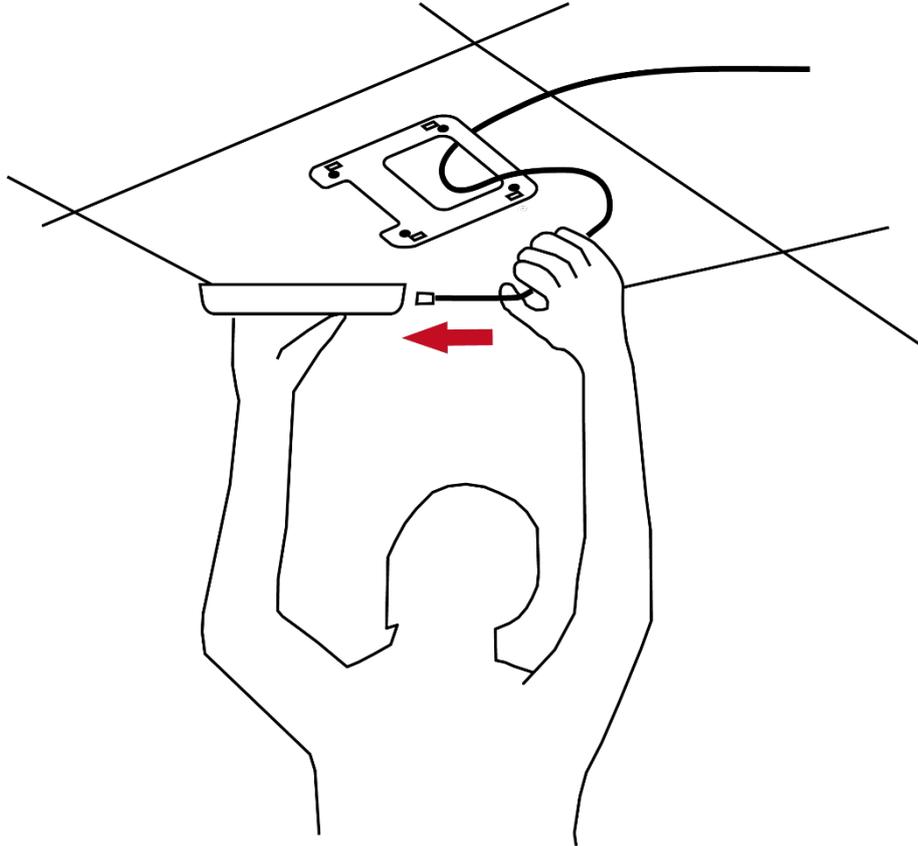


Figure 3-2 Connecting the Ethernet Cable

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

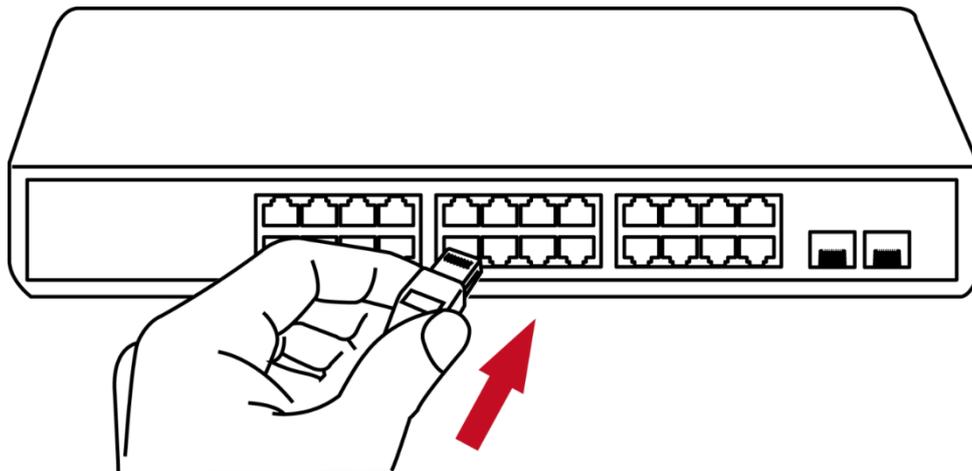


Figure 3-3 Connecting the PoE Injector

Chapter 4. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AP within minutes.

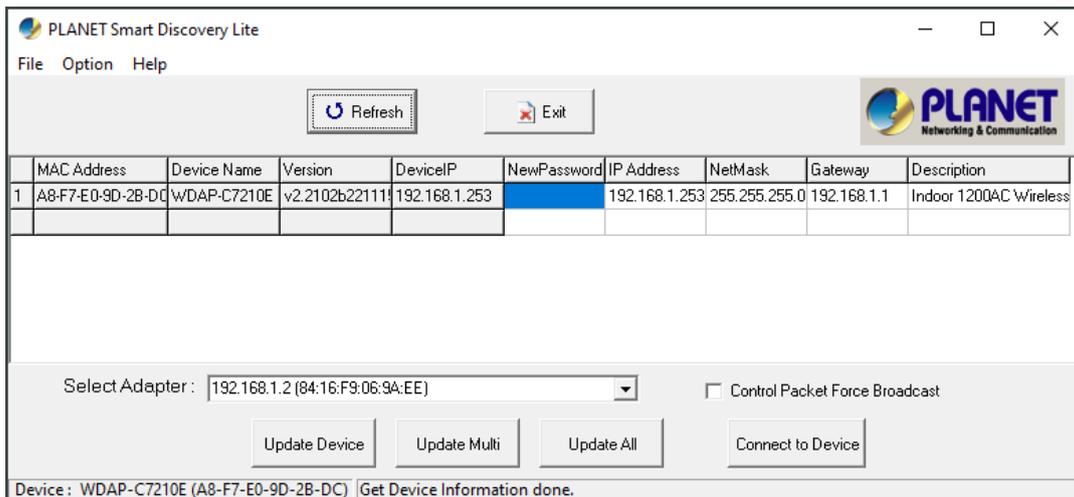


A computer with wired Ethernet connection to the Wireless AP is required for the first-time configuration.

4.1 Connecting to the AP

As the default setting of connection type of WDAP-C7210E(V2) is DHCP, your computer's IP address has to be the same network segment as the wireless AP. To find the IP address of the AP, use the utility of "Smart Discovery Lite", which can be found on PLANET official website.

1. Launch the utility from your computer after you have downloaded and decompressed it.
2. Select your adapter to connect the AP.
3. Click the "Refresh" button.
4. The AP model and its IP address are shown.
5. Check whether the IP address of your adapter and the IP address of the AP are the same.
6. If yes, click "Connect to Devices" for the AP setting.
7. If no, go to the next page to set your wired or wireless setting.
8. If there is no DHCP server in the local network, the IP will go back to 192.168.1.253 by default after 60 seconds.



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.

4.1.1 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-C7210E 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-C7210E is 192.168.1.253 and the DSL router is 192.168.1.254, or you may choose from 192.168.1.1 to 192.168.1.252.

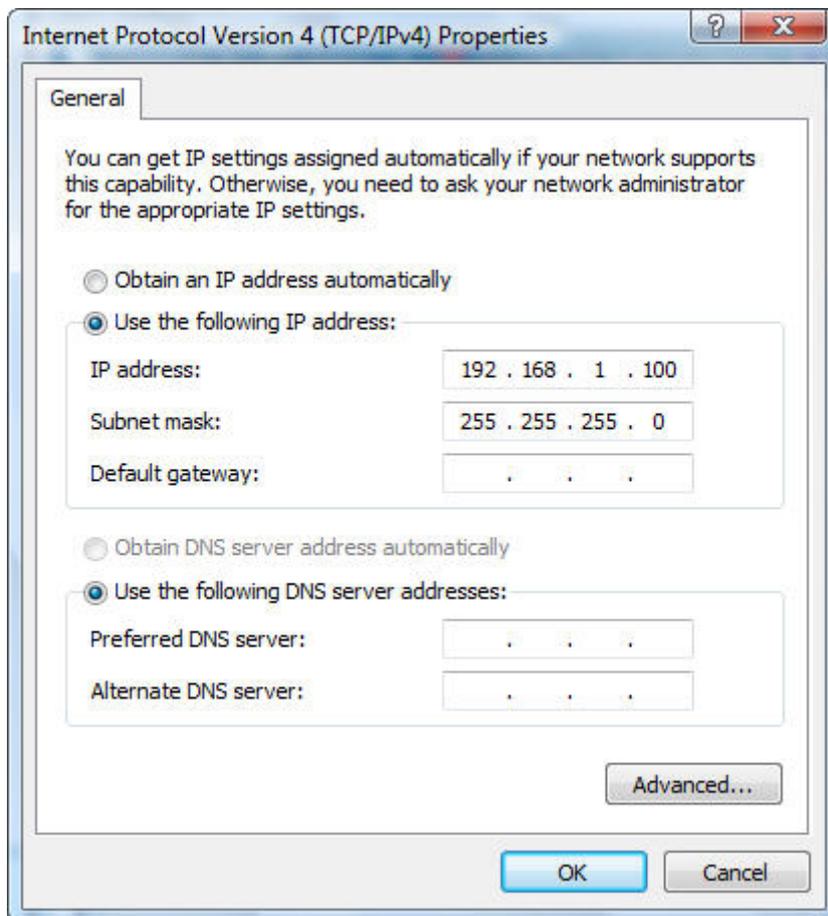


Figure 4-1 TCP/IP Setting

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.

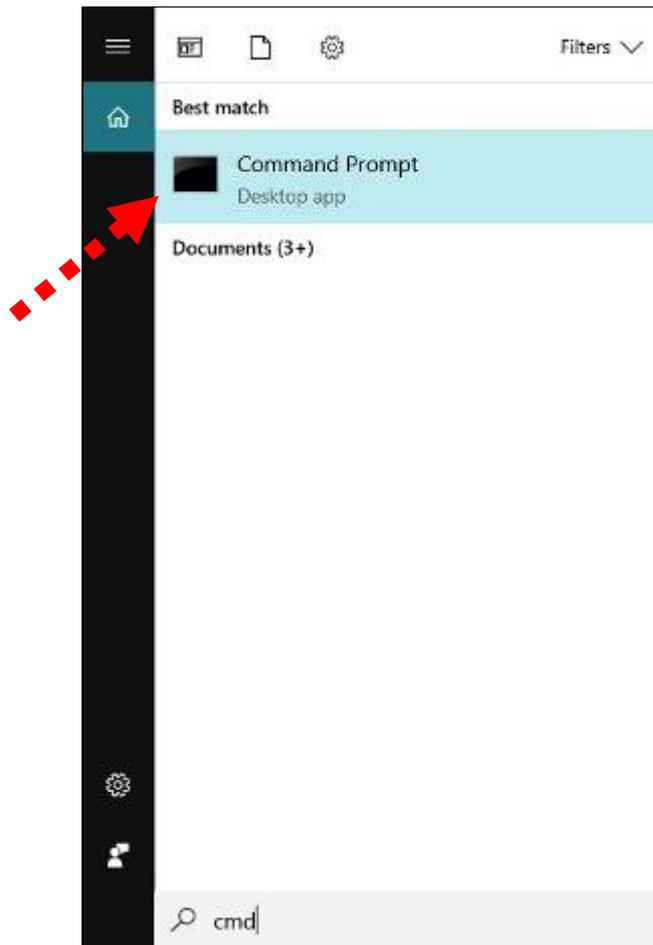


Figure 4-2 Windows Start Menu

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.

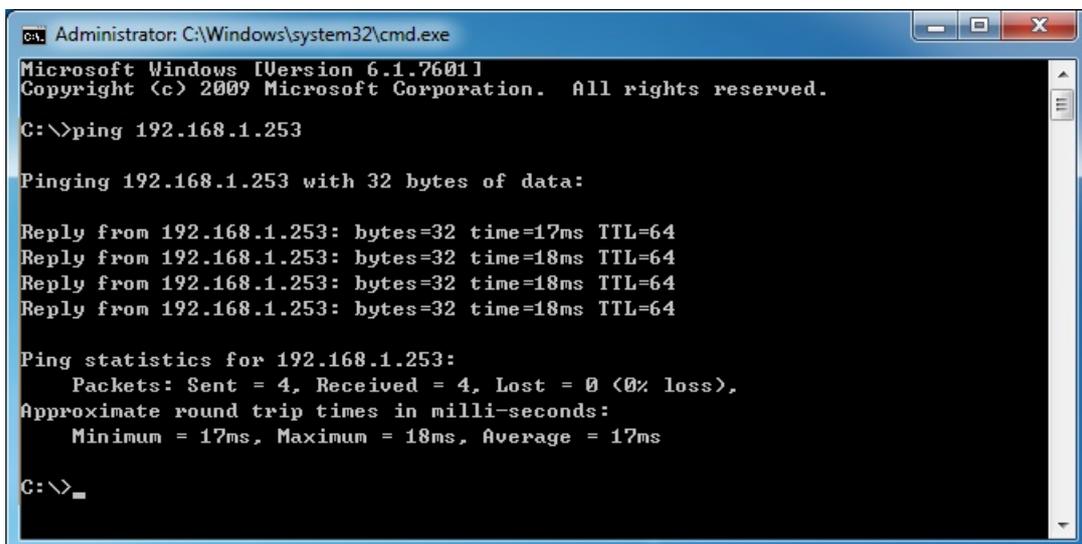
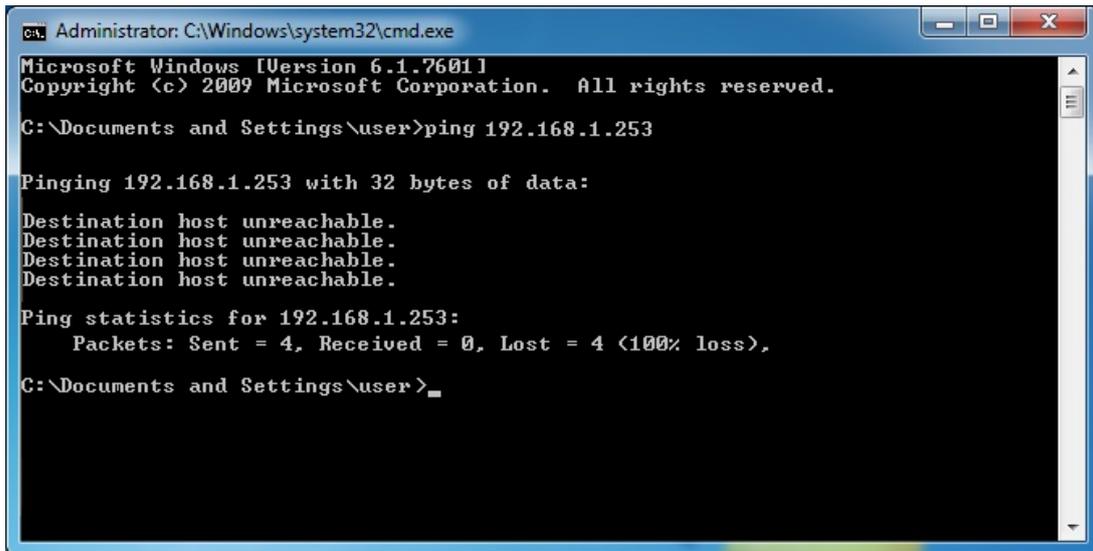


Figure 4-3 Successful Result of Ping Command

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



```
cs: Administrator: C:\Windows\system32\cmd.exe
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 4-4 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.

4.2 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.

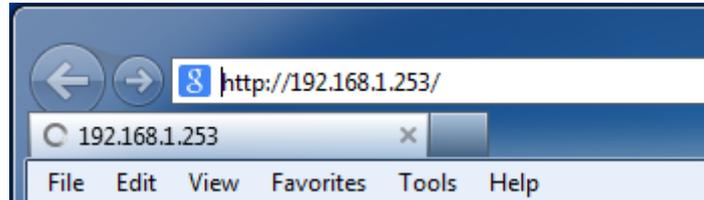


Figure 4-5 Login by Default IP Address

After a moment, a login window will appear. Enter **admin** for the password in lower case letters. Then click **LOGIN** or press the **Enter** key.



Figure 4-6 Login Window

Default Username: **admin**

Default Password: **admin**



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.

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and allows you to manage the AP with ease.

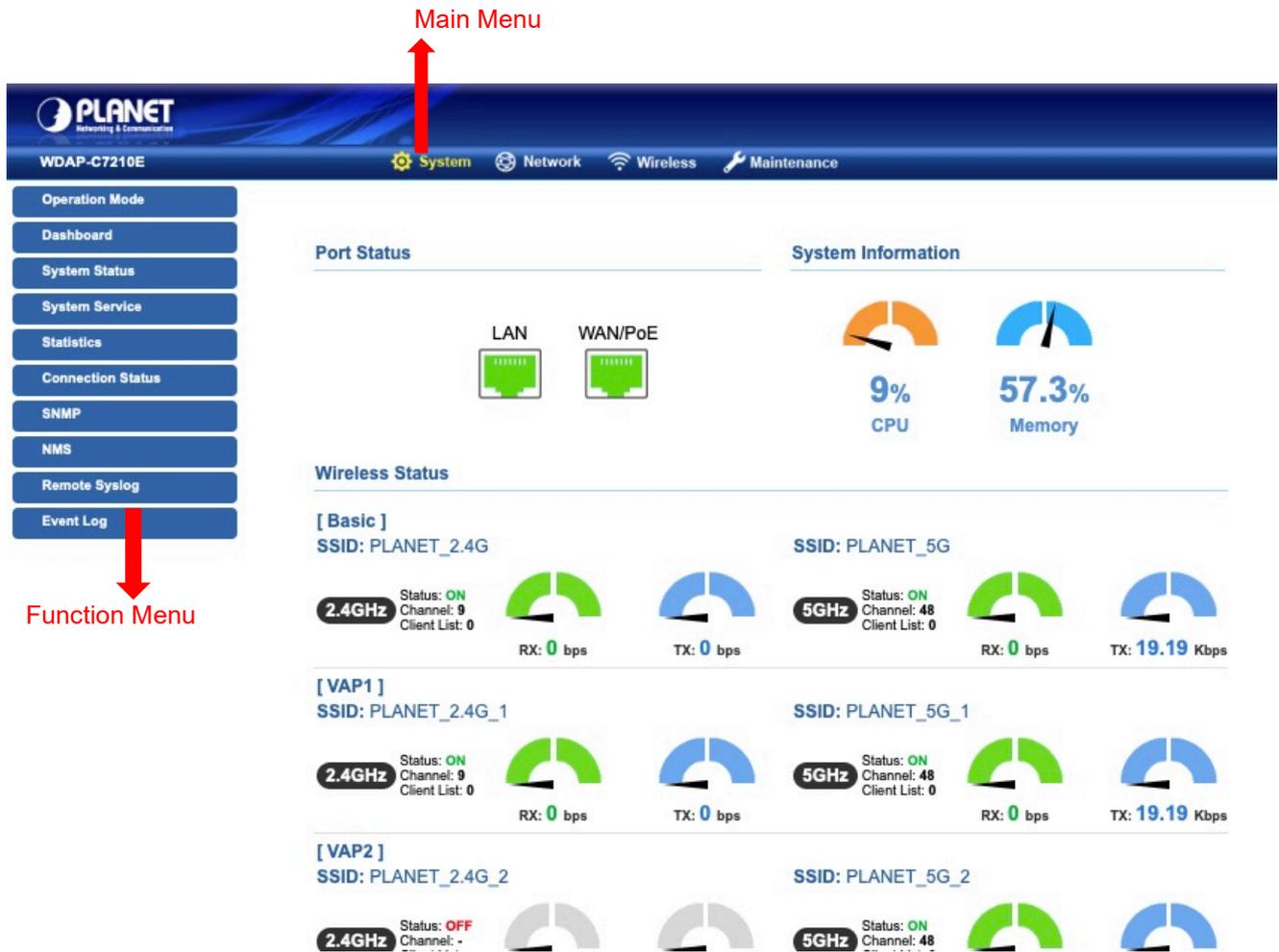


Figure 5-1 Main Web Page

■ 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 5-2 and 5-3.



Figure 5-2: 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 5-3: 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.

5.1 System

Use the system menu items to display and configure basic administrative details of the router. The System menu shown in [Figure 5-4](#) provides the following features to configure and monitor system.



Figure 5-4: 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

5.1.1 Operation Mode

The Wizard guides you to configuring the WDAP-C7210E in a different mode, including AP, gateway and repeater modes.

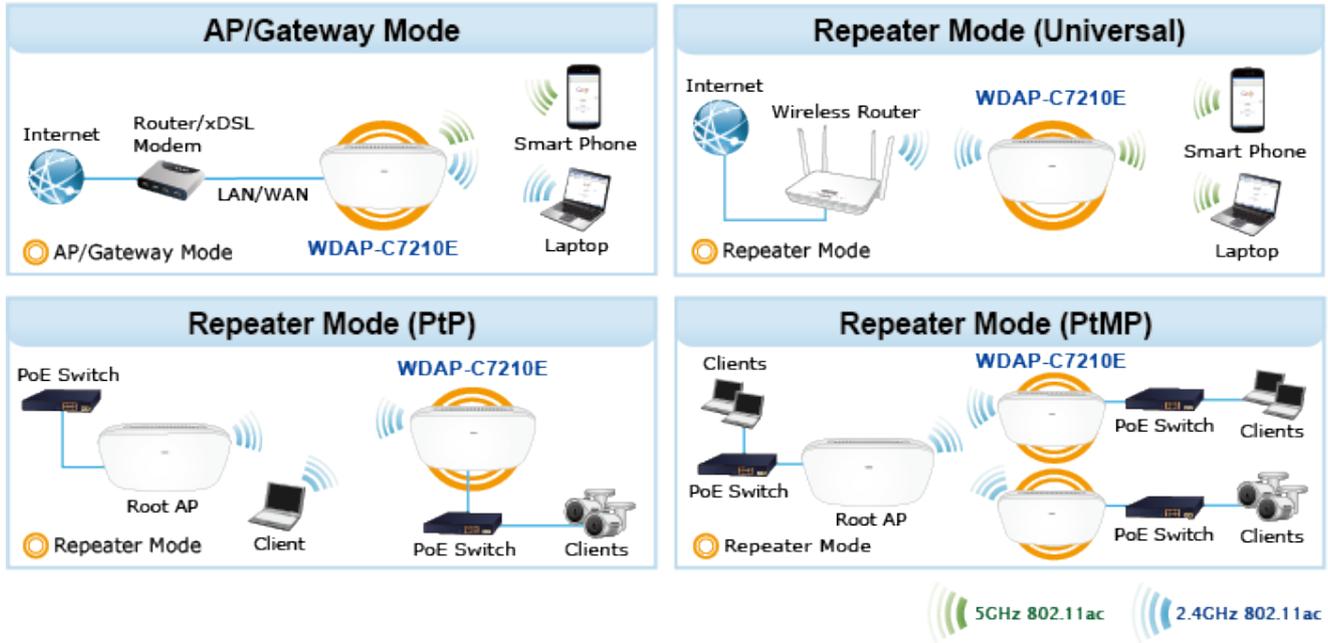


Figure 5-5 Operation Mode



The default operation mode is AP Mode.

5.1.2 Gateway Mode (Router)

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

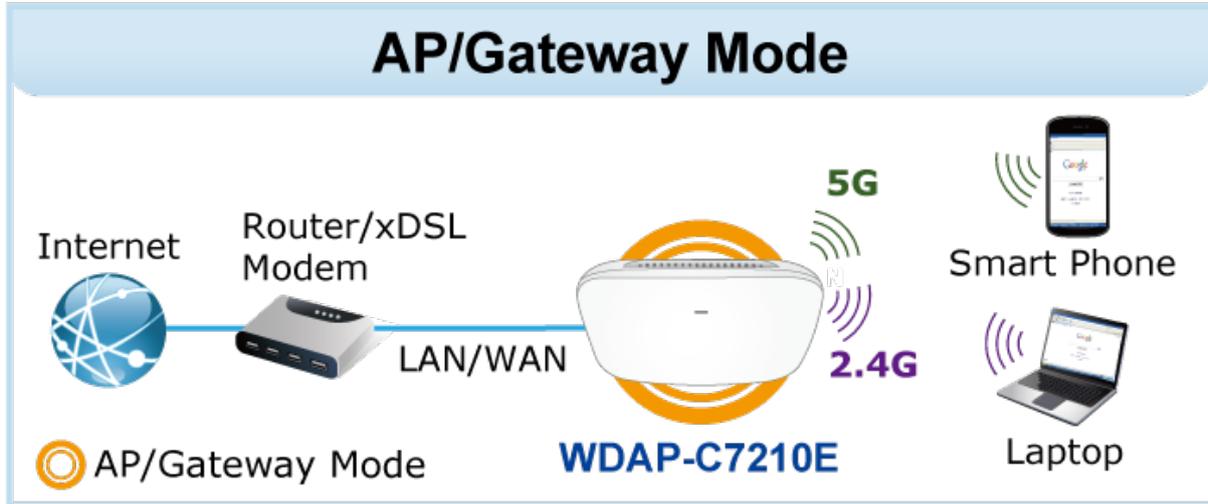


Figure 5-6: Setup Wizard

Step 1: Operation Mode

Select operation mode.

STEP 1 - Operation Mode

1 Mode 2 LAN 3 WAN 4 Wireless 5 Security 6 Completed

▼ Current Mode

Gateway Mode

AP Mode

Repeater 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.

Cancel Next

Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in [Figure 5-7](#).

STEP 2 - Network Interface LAN

1 Mode 2 LAN 3 WAN 4 Wireless 5 Security 6 Completed

IP Address: 192.168.1.253

Netmask: 255.255.255.0

DHCP Server:

Start IP Address: 192.168.1.100

Maximum DHCP Users: 101

Cancel Previous Next

Figure 5-7: Setup Wizard – LAN Configuration

STEP 2 - Network Interface LAN

1 Mode 2 LAN 3 Wireless 4 Completed

Connection Type: DHCP

DHCP Fallback: Enable Disable

Fallback Seconds: 60 (30~300)

IP Address: 192.168.1.253

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

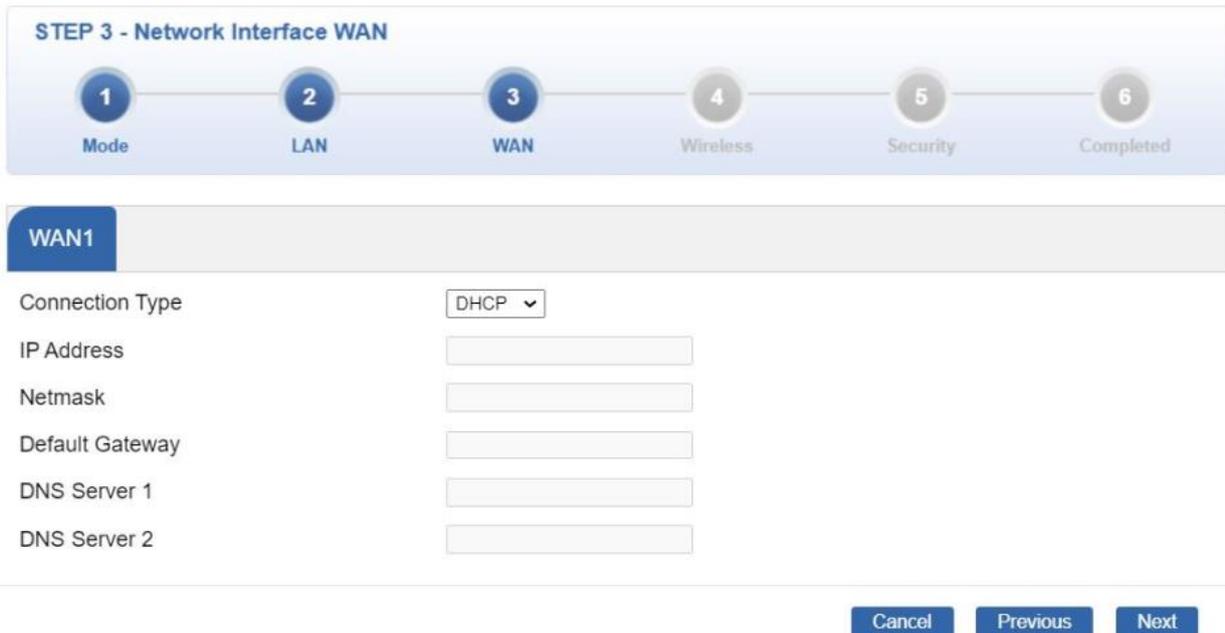
Cancel Previous Next

Figure 5-7-1: Setup Wizard – LAN Configuration for AP mode

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.
DHCP Fallback (AP mode only)	The IP address of your AP will be assigned from DHCP Server. If there is no DHCP Server in the local network, the IP will be set to 192.168.1.253.
Fallback Seconds (AP mode only)	By default is 60
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 5-8](#)



STEP 3 - Network Interface WAN

1 Mode 2 LAN 3 WAN 4 Wireless 5 Security 6 Completed

WAN1

Connection Type:

IP Address:

Netmask:

Default Gateway:

DNS Server 1:

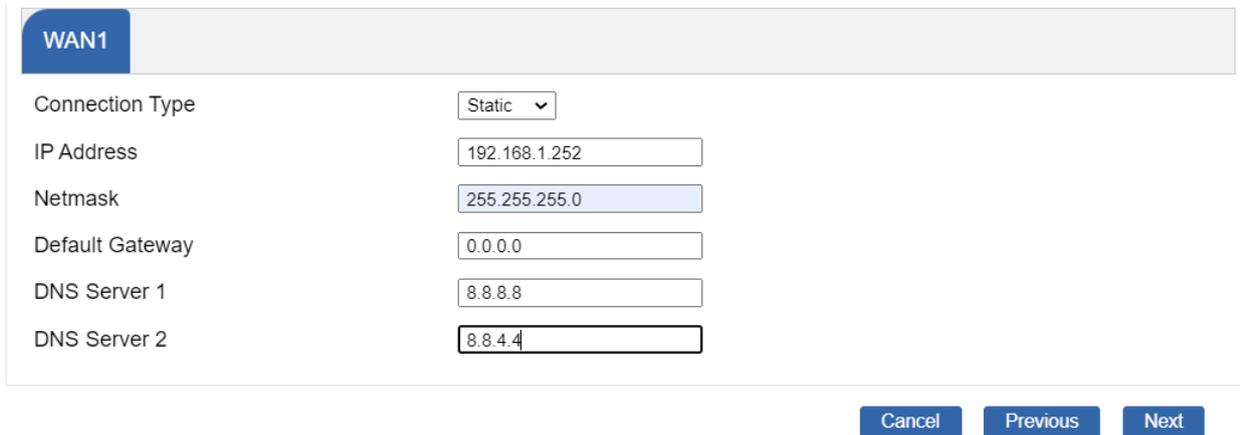
DNS Server 2:

Cancel Previous Next

Figure 5-8: 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 5-9](#).



The screenshot shows the WAN1 configuration page with the following fields:

- Connection Type: Static (dropdown)
- 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

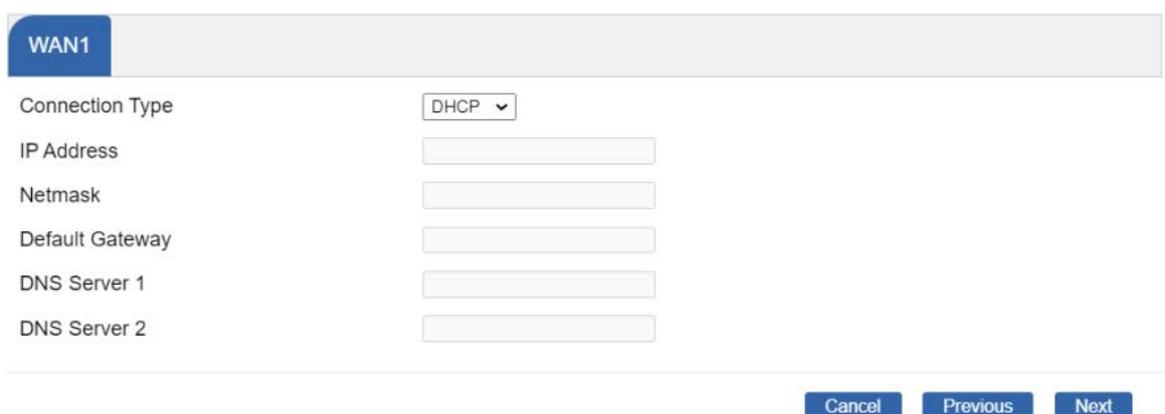
Buttons at the bottom: Cancel, Previous, Next.

Figure 5-9: 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 5-10](#).



The screenshot shows the WAN1 configuration page with the following fields:

- Connection Type: DHCP (dropdown)
- IP Address: (empty field)
- Netmask: (empty field)
- Default Gateway: (empty field)
- DNS Server 1: (empty field)
- DNS Server 2: (empty field)

Buttons at the bottom: Cancel, Previous, Next.

Figure 5-10: WAN Interface Setup – DHCP Setup

Step 4: Network Interface Wireless

Set up the Security Settings as shown in [Figure 5-11](#).

STEP 4 - Network Interface Wireless

1 Mode 2 LAN 3 WAN 4 **Wireless** 5 Security 6 Completed

2.4G WIFI Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

5G WIFI Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

Figure 5-11: Network Setup

Step 5: Security Setting

Set up the Security Settings as shown in [Figure 5-12](#).

STEP 5 - Security Settings

1 Mode 2 LAN 3 WAN 4 Wireless 5 **Security** 6 Completed

SPI Firewall Enable Disable

Block SYN Flood Enable Disable

Block ICMP Flood Enable Disable

Block WAN Ping Enable Disable

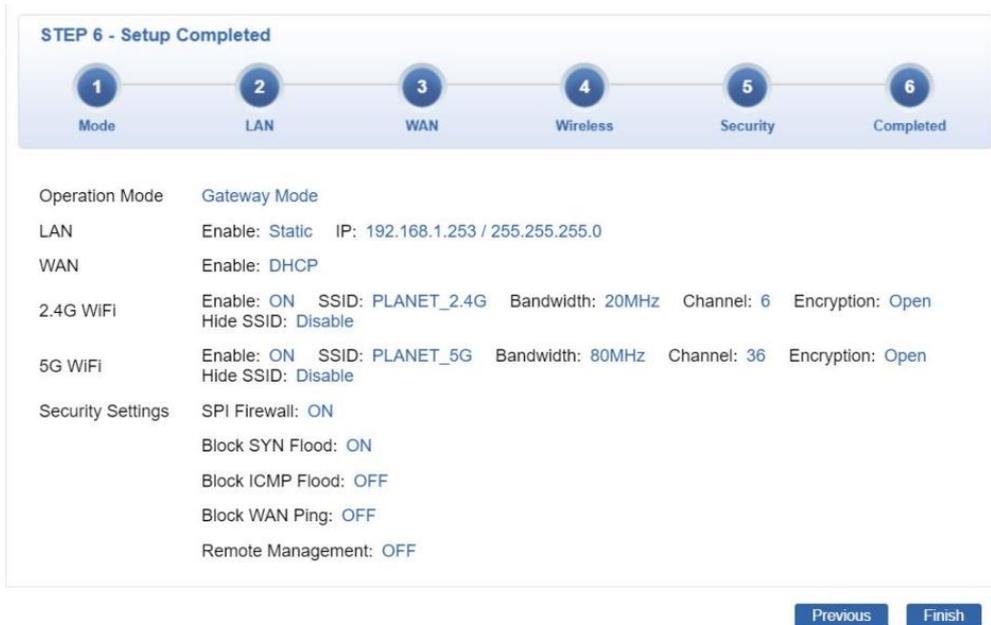
Remote Management Enable Disable

Figure 5-12: 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 shows the summary of LAN, WAN and Security settings as shown in [Figure 5-13](#).



STEP 6 - Setup Completed

1 Mode 2 LAN 3 WAN 4 Wireless 5 Security 6 Completed

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

Previous Finish

Figure 5-13: Setup Wizard – Setup Completed

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

5.1.3 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 5-14.



Figure 5-14: Dashboard

Port Status

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

Wireless Status

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

System Information

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

5.1.4 System Status

This page displays system information as shown in [Figure 5-15](#).

Device Information	
Model Name	WDAP-C7210E
Firmware Version	v2.2102b221115
Region	ETSI
Current Time	2022-11-30 Wednesday 10:52:49
Running Time	0 day, 00:38:37

WAN1	
MAC Address	A8:F7:E0:00:18:AD
Connection Type	DHCP
Display Name	WAN1
IP Address	
Netmask	
Default Gateway	

LAN	
MAC Address	A8:F7:E0:00:18:AC
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	WPA2/WPA3 Personal
MAC Address	A8:F7:E0:00:18:AE

5GHz WiFi	
Status	ON
SSID	PLANET_5G
Channel	36
Encryption	WPA2/WPA3 Personal
MAC Address	A8:F7:E0:00:18:AF

Figure 5-15: Status

5.1.5 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 5-16](#).

Service			
#	State	Service	Detail
1	✔ Enabled	DHCP Service	DHCP Table: 0
2	✘ Disabled	DDNS Service	Not enabled
3	✔ Enabled	SNMP Service	
4	✘ Disabled	Quality of Service	
5	✘ Disabled	RADIUS Service	
6	✘ Disabled	Captive Portal	
7	✔ Enabled	2.4GHz WiFi	SSID: PLANET_2.4G
8	✔ Enabled	5GHz WiFi	SSID: PLANET_5G

Secured Service			
#	State	Service	Detail
1	✔ Enabled	Cybersecurity	TLS 1.2, TLS 1.3
2	✔ Enabled	SPI Firewall	
3	✘ Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	✘ Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	✘ Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32

Figure 5-16: Service

5.1.6 Statistics

This page displays the number of packets that passes through the router on the WAN and LAN. The statistics are shown in [Figure 5-17](#).

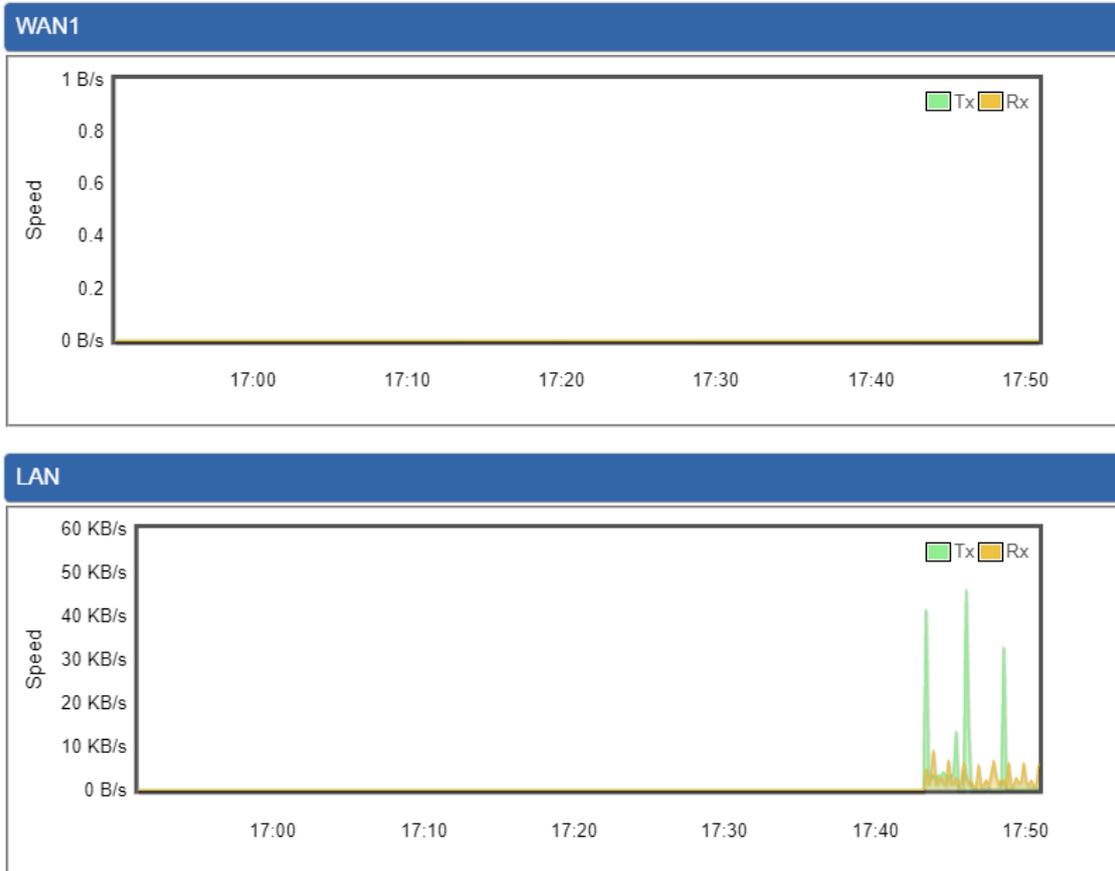


Figure 5-17: Statistics

5.1.7 Connection Status

The page shows the DHCP table and ARP table where statuses are shown in [Figure 5-18](#).

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 5-18: Connection Status

5.1.8 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 5-19](#).

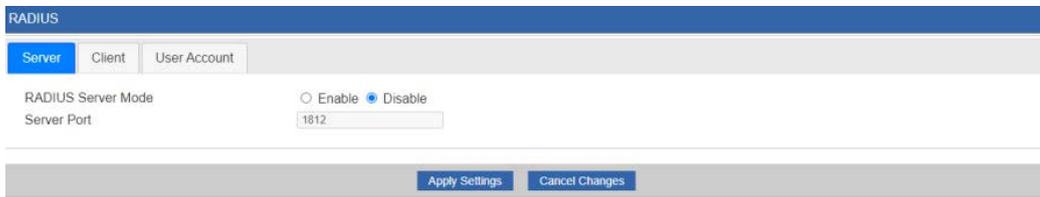


Figure 5-19: RADIUS

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

5.1.9 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 5-20](#).

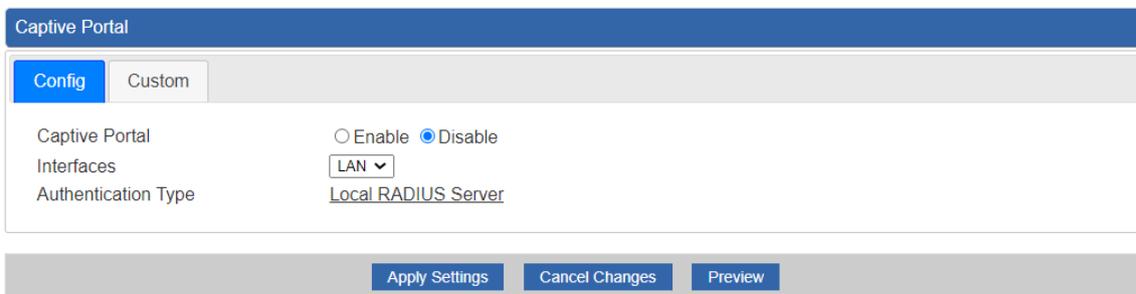
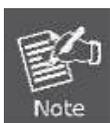


Figure 5-20: Captive Portal

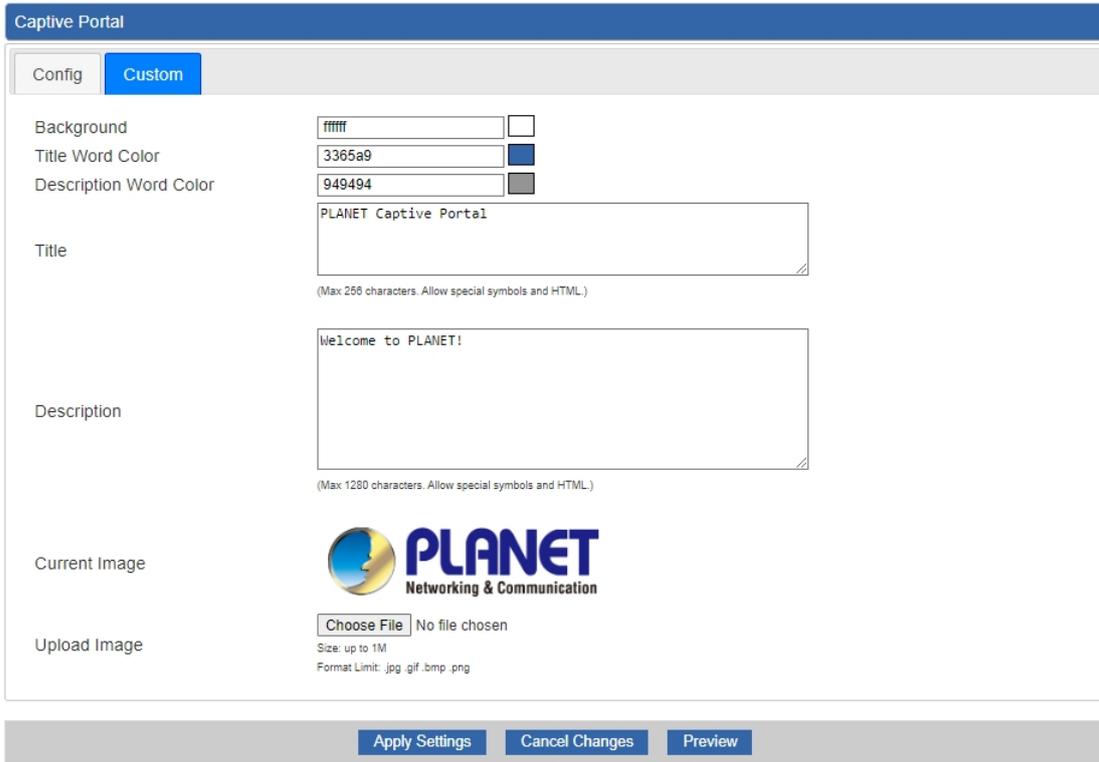
Object	Description
Captive Portal	Disable or enable the Captive Portal function. The default configuration is disabled.



Captive Portal function can be only configured in **Gateway Mode**.

■ Customizing the Custom Captive Portal Web Page

1. Click **Custom**

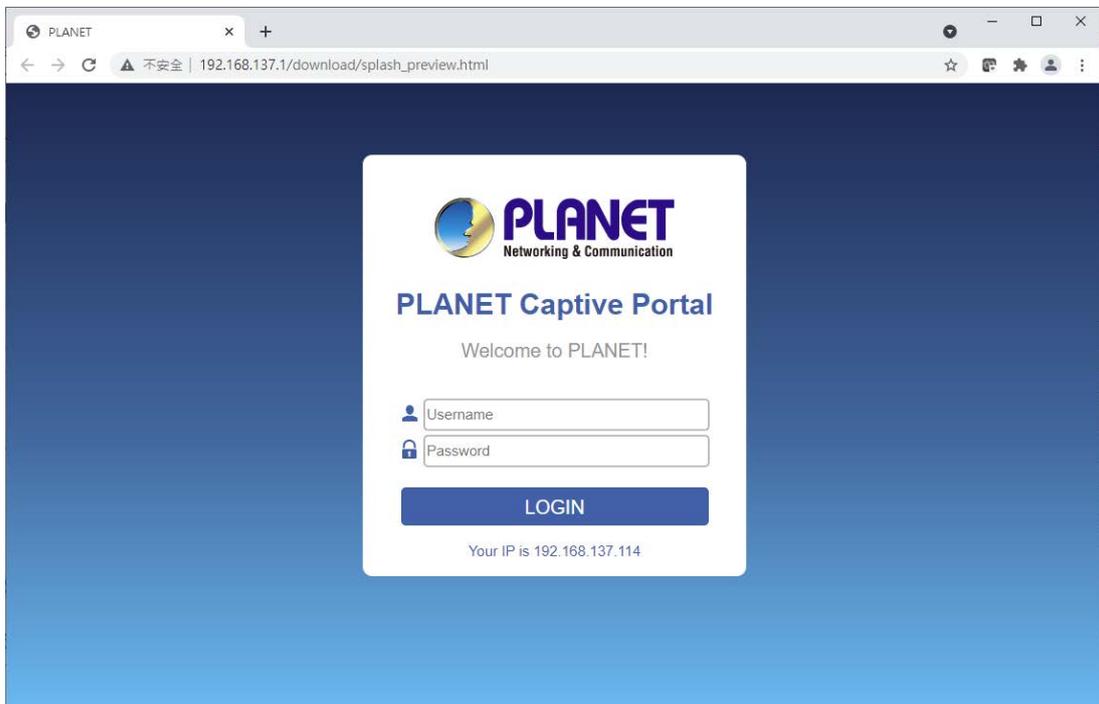


The screenshot shows the 'Captive Portal' configuration window with the 'Custom' tab selected. The interface includes the following fields and options:

- Background:** A text input field containing 'ffffff' and a color selection icon.
- Title Word Color:** A text input field containing '3365a9' and a color selection icon.
- Description Word Color:** A text input field containing '949494' and a color selection icon.
- Title:** A text area containing 'PLANET Captive Portal' with a character limit of 256.
- Description:** A text area containing 'Welcome to PLANET!' with a character limit of 1280.
- Current Image:** A preview of the PLANET logo.
- Upload Image:** A 'Choose File' button, 'No file chosen' text, and format restrictions (Size: up to 1M, Format Limit: .jpg .gif .bmp .png).

At the bottom of the window are three buttons: 'Apply Settings', 'Cancel Changes', and 'Preview'.

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



5.1.10 SNMP

This page provides SNMP setting of the router as shown in [Figure 5-21](#).

SNMP

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> 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-C7210E
System Description	
System Location	Default Location
System Contact	Default Contact

SNMP Trap Receiver Configuration

SNMP Trap	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SNMP Trap Destination 1	
SNMP Trap Destination 2	

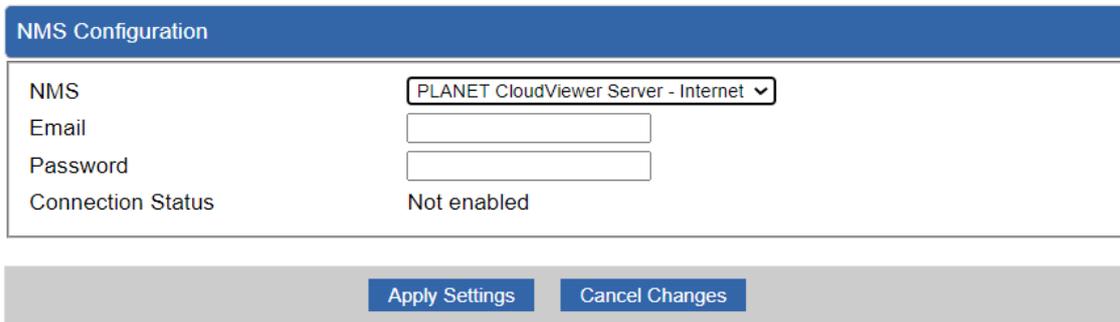
Apply Settings
Cancel Changes

Figure 5-21: 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.

5.1.11 NMS

The CloudViewer Server – Internet screens – is shown in Figure 5-22.



The screenshot shows the 'NMS Configuration' window. It contains the following fields and controls:

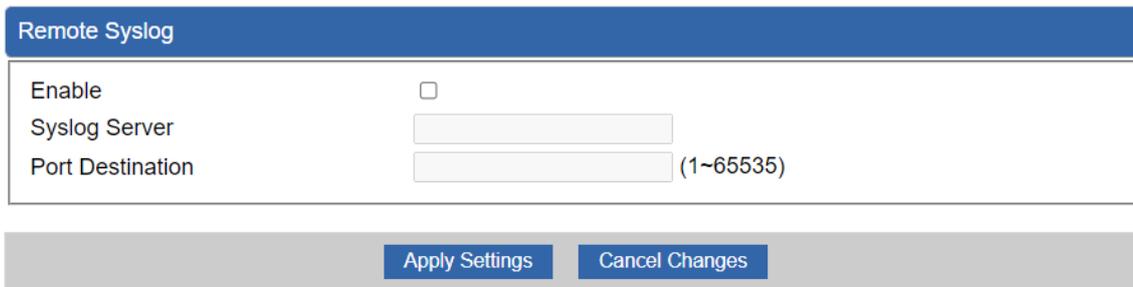
- NMS:** A dropdown menu currently showing 'PLANET CloudViewer Server - Internet'.
- Email:** An empty text input field.
- Password:** An empty text input field.
- Connection Status:** A label indicating 'Not enabled'.

At the bottom of the window, there are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 5-22: 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

5.1.12 Remote Syslog



The screenshot shows the 'Remote Syslog' configuration window. It contains the following fields and controls:

- Enable:** A checkbox that is currently unchecked.
- Syslog Server:** An empty text input field.
- Port Destination:** A text input field containing '(1~65535)'.

At the bottom of the window, there are two buttons: 'Apply Settings' and 'Cancel Changes'.

Figure 5-23: Remote Syslog

Object	Description
Enable Remote Syslog	Enable Captive Portal on routers

5.1.13 Event Log

Event Log

1

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 5-24: Event Log

Object	Description
Event Log	Display Event Log information

5.2 Network

The Network function provides WAN, LAN and network configuration of the router as shown in [Figure 5-25](#).



Figure 5-25: 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.

5.2.1 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 5-26](#). Here you may select the access method by clicking the item value of WAN access type.

WAN1 Configuration	
Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="Static"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Apply Settings

Cancel Changes

WAN1 Configuration	
Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="DHCP"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
Default Gateway	<input type="text"/>
DNS Server 1	<input type="text"/>
DNS Server 2	<input type="text"/>

Apply Settings

Cancel Changes

WAN1 Configuration	
Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="PPPoE"/>
Username	<input type="text"/>
Password	<input type="text"/>

Apply Settings

Cancel Changes

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="PPTP"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Enable MPPE Encryption	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Type	<input type="text" value="DHCP"/>

WAN1 Configuration

Display Name	<input type="text" value="WAN1"/>
Connection Type	<input type="text" value="L2TP"/>
Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Connection Type	<input type="text" value="DHCP"/>

Figure 5-26: WAN

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

Object	Description
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.



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.

5.2.2 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 5-27](#). Here you may change the settings for IP address, subnet mask, DHCP, etc.

LAN Configuration

IP Address	<input type="text" value="192.168.1.253"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.1.1"/>
Primary DNS	<input type="text" value="8.8.8.8"/>
Secondary DNS	<input type="text" value="8.8.4.4"/>

Figure 5-27: LAN Setup

Object	Description
IP Address	The LAN IP address of the router and default is 192.168.1.253
Net Mask	Default is 255.255.255.0 .

5.2.3 UPnP

UPnP Configuration

UPnP Enable Disable

Apply Settings
Cancel Changes

Figure 5-28: UPnP

Object	Description
UPnP	Set the function as enable or disable

5.2.4 Routing

Please refer to the following sections for the details as shown in [Figures 5-30 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

Add Routing Table Rule

Figure 5-29: Routing table

Routing Table Configuration

Type	<input type="text" value="Host"/>
Destination	<input type="text"/>
Netmask	<input type="text" value="255.255.255.255 /32"/>
Default Gateway	<input type="text"/>
Interface	<input type="text" value="LAN"/>
Comment	<input type="text"/>

Apply Settings
Cancel Changes

Figure 5-30: 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.

5.2.5 RIP

RIP Configuration

Dynamic Route

RIP Versions

Enable
 Disable

RIP 2 ▾

Apply Settings
Cancel Changes

Figure 5-31 RIP

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

5.2.6 OSPF

OSPF Configuration

OSPF

Router ID

Area ID

Enable
 Disable

Apply Settings
Cancel Changes

Figure 5-32: OSPF

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

5.2.7 IGMP

IGMP Configuration

IGMP Proxy Enable Disable

IGMP Versions Auto

Apply Settings
Cancel Changes

Figure 5-33: IGMP

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

5.2.8 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the router as shown in [Figure 5-35](#). 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

Apply Settings
Cancel Changes

IPv6 - WAN1

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

IPv6 - LAN

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

DHCPv6

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

Figure 5-34: 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

5.2.9 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 5-35](#).

DHCP Configuration

DHCP Server Enable Disable

Start IP Address 192.168.1.

Maximum DHCP Users

DNS Server Automatically Manually

Primary DNS Server

Secondary DNS Server

WINS

Lease Time minutes

Domain Name

Static DHCP List

Index	Device Name	IP Address	MAC Address	Delete
	<input style="width: 150px;" type="text"/>	<input style="width: 100px;" type="text" value="192.168.1.150"/>	<input style="width: 100px;" type="text" value="00:30:4F:00:00:01"/>	<input type="button" value="Add"/>

Figure 5-35: 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.

5.2.10 DDNS

The router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS** (<http://www.planetddns.com>) and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in [Figure 5-36](#).

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	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interface	WAN1 ▾
DDNS Type	PLANET DDNS ▾
PLANET Easy DDNS	Disable ▾
User Name	<input type="text"/>
Password	<input type="text"/>
Host Name	<input type="text"/>
Interval	<input type="text" value="120"/> seconds
Connection Status	Not enabled

Figure 5-36: 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: <ol style="list-style-type: none"> 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NoIP: Activate NoIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account.
User Name	The user name is used to log into DDNS service.
Password	The password is used to log into DDNS service.
Host Name	The host name as registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Connection Status	Show the connection status of the DDNS function.

5.3 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in [Figure 5-37](#). Please refer to the following sections for the details.



Figure 5-37: 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.

5.3.1 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 5-38](#).

Firewall Protection

SPI Firewall Enable Disable

DDoS

Block SYN Flood Enable Disable Packets/Second

Block FIN Flood Enable Disable Packets/Second

Block UDP Flood Enable Disable Packets/Second

Block ICMP Flood Enable Disable 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

HTTPs Port

Remote Management Enable Disable

Temporarily block when login failed more than (0 means no limit)

IP blocking period 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

Apply Settings
Cancel Changes

Figure 5-38: Firewall

Object	Description
SPI Firewall	<p>The SPI Firewall prevents attack and improper access to network resources.</p> <p>The default configuration is enabled.</p>
Block SYN Flood	<p>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.</p> <p>The default configuration is enabled.</p>
Block FIN Flood	<p>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.</p> <p>The default configuration is disabled.</p>

Block UDP Flood	<p>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.</p> <p>The default configuration is disabled.</p>
Block ICMP Flood	<p>ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.</p> <p>The default configuration is disabled.</p>
IP TearDrop	<p>If the function is enabled, the router will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.</p>
Ping Of Death	<p>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.</p>
TCP packets with SYN and FIN Bits set	<p>Set the function as enable or disable</p>
TCP packets with FIN Bit set but no ACK Bit set	<p>Set the function as enable or disable</p>
TCP packets without Bits set	<p>Set the function as enable or disable</p>
Block WAN Ping	<p>Enable the function to allow the Ping access from the Internet network.</p> <p>The default configuration is disabled.</p>
HTTP Port	<p>The default is 80.</p>
HTTPs Port	<p>The default is 443.</p>
Remote Management	<p>Enable the function to allow the web server access of the router from the Internet network.</p> <p>The default configuration is disabled.</p>
Temporarily block when login failed	<p>The default is 0. (0 means no limit)</p>
IP blocking period	<p>The default is 0. (0 means permanent blocking)</p>
Blocked IP	<p>0.0.0.0</p>
FTP ALG	<p>Set the function as enable or disable</p>
TFTP ALG	<p>Set the function as enable or disable</p>
RTSP ALG	<p>Set the function as enable or disable</p>
H.323 ALG	<p>Set the function as enable or disable</p>
SIP ALG	<p>Set the function as enable or disable</p>

5.3.2 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 5-39](#).

MAC Filtering

MAC Filtering Enable Disable
 Interface LAN WAN

MAC Filtering Rules

Index	Active	Device Name	MAC Address	Action
		<input type="text" value="abc"/>	<input type="text" value="00:30:4F:00:00:01"/>	<input type="button" value="Add"/>

Figure 5-39: 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 to the list.

5.3.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in [Figure 5-40](#). To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.



Figure 5-40: 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.

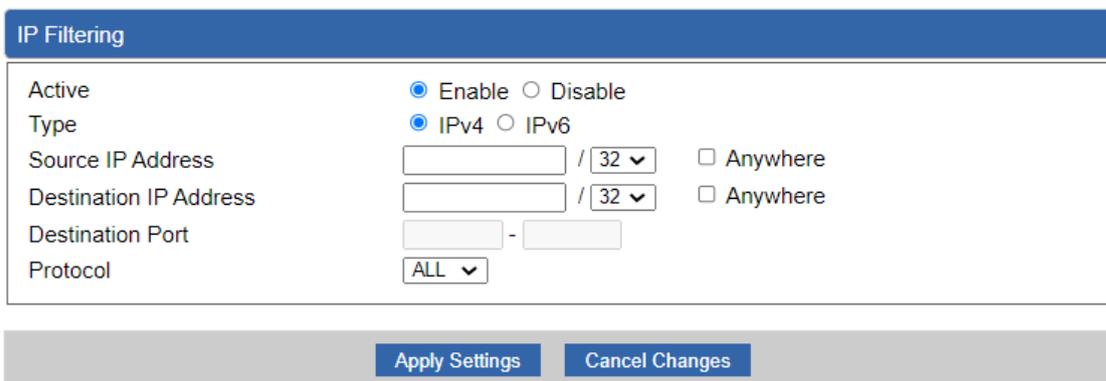


Figure 5-41: IP Filter Rule Setting

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.
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 all the default protocols.

5.3.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in [Figure 5-43](#). Block those URLs which contain keywords listed below.

Web Filtering

Web Filtering Enable Disable

Web Filtering Rules

No.	Active	Filter Keyword	Action
<input type="button" value="Add Web Filtering Rule"/>			

Figure 5-41: 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

Filter Keyword

Figure 5-42: 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.

5.3.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in Figure 5-43. 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.

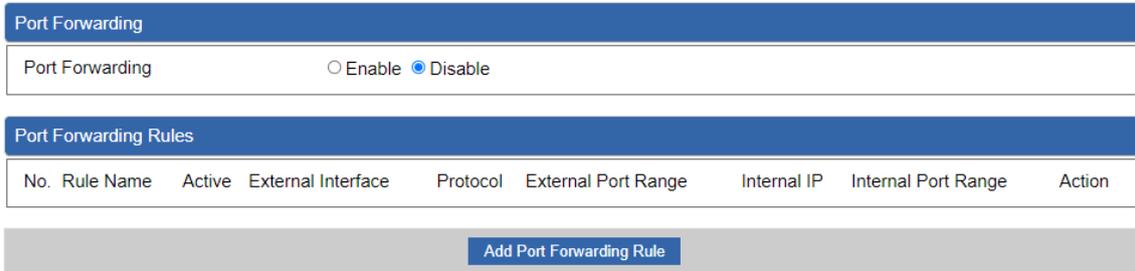


Figure 5-43: Port Forwarding

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.

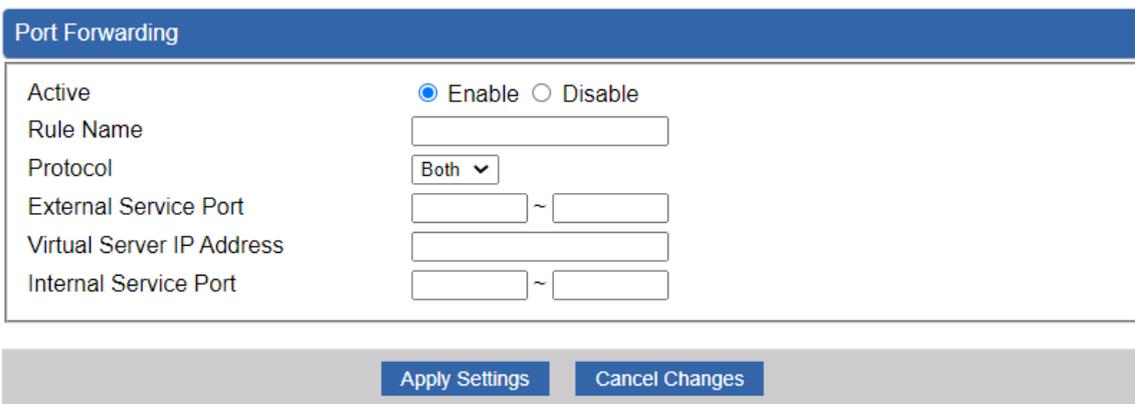


Figure 5-44: Port Forwarding Rule Setting

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

5.3.6 QoS

QoS - WAN1

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

Upstream Bandwidth

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

Downstream Bandwidth

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

Service Priority

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

Network Priority

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

Figure 5-45: 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

5.3.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in [Figure 5-46](#). Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

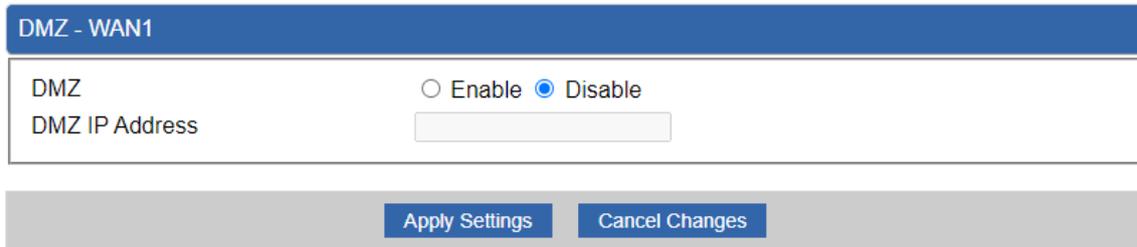


Figure 5-46: DMZ

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.

5.4 Wireless

The Wireless menu provides the following features for managing the system

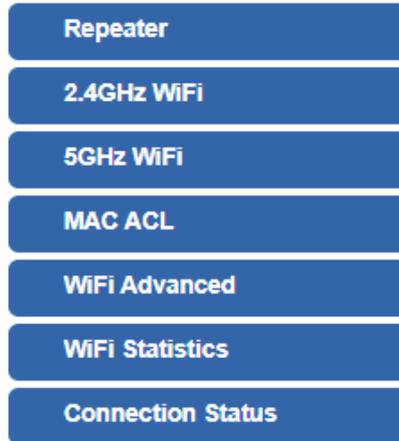
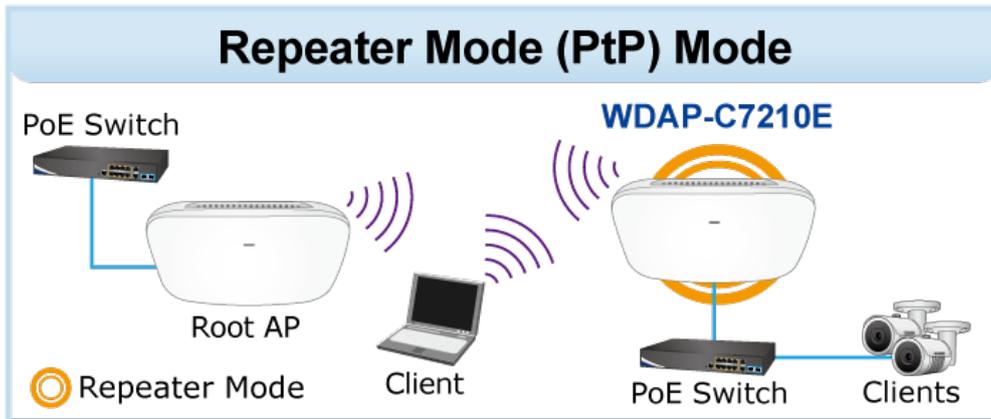


Figure 5-47: Wireless Menu

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.

5.4.1 Repeater



This page allows the user to define Repeater

Repeater Configuration

Select Radio	Use 5GHz Radio <input type="button" value="v"/>	
SSID	PLANET_5G <input type="button" value="Scan"/>	
Lock BSSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
BSSID	A8:F7:E0:B2:31:FB	
Encryption	Open <input type="button" value="v"/>	

Figure 5-48: 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"

5.4.2 2.4G Wi-Fi

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

2.4GHz WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Wireless Mode

Channel

Encryption

WiFi Multimedia Enable Disable

VLAN ID

Apply Settings
Cancel Changes

Figure 5-49: 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

5.4.3 5G Wi-Fi

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

5GHz WiFi Configuration

Basic

Virtual AP1

Virtual AP2

Virtual AP3

Wireless Status Enable Disable

Wireless Name (SSID)

Hide SSID Enable Disable

Wireless Mode

Channel

Encryption

WiFi Multimedia Enable Disable

VLAN ID

Apply Settings

Cancel Changes

Figure 5-50: 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

5.4.4 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	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; background-color: #0056b3; color: white; margin-bottom: 5px;">Add</div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; background-color: #0056b3; color: white;">Scan</div>

Figure 5-51: 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

5.4.5 Wi-Fi Advanced

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

WiFi Advanced

2.4GHz Maximum Associated Clients	<input type="text" value="75"/> (Range 1~75)
5GHz Maximum Associated Clients	<input type="text" value="75"/> (Range 1~75)
2.4GHz Coverage Threshold	<input type="text" value="-95"/> (-95dBm ~ -60dBm)
5GHz Coverage Threshold	<input type="text" value="-95"/> (-95dBm ~ -60dBm)
2.4GHz TX Power	<input type="button" value="Max(100%)"/>
5GHz TX Power	<input type="button" value="Max(100%)"/>
2.4GHz WLAN Partition	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5GHz WLAN Partition	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RTS Threshold	<input type="text" value="2347"/> (0-2347)

Figure 5-52: 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	<p>Enable or Disable RTS/CTS protocol. It can be used in the following scenarios and used by Stations or Wireless AP.</p> <p>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.</p> <p>2) In mixed mode, the hidden node problem can be avoided.</p> <p>The default value is 2347</p>

5.4.6 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

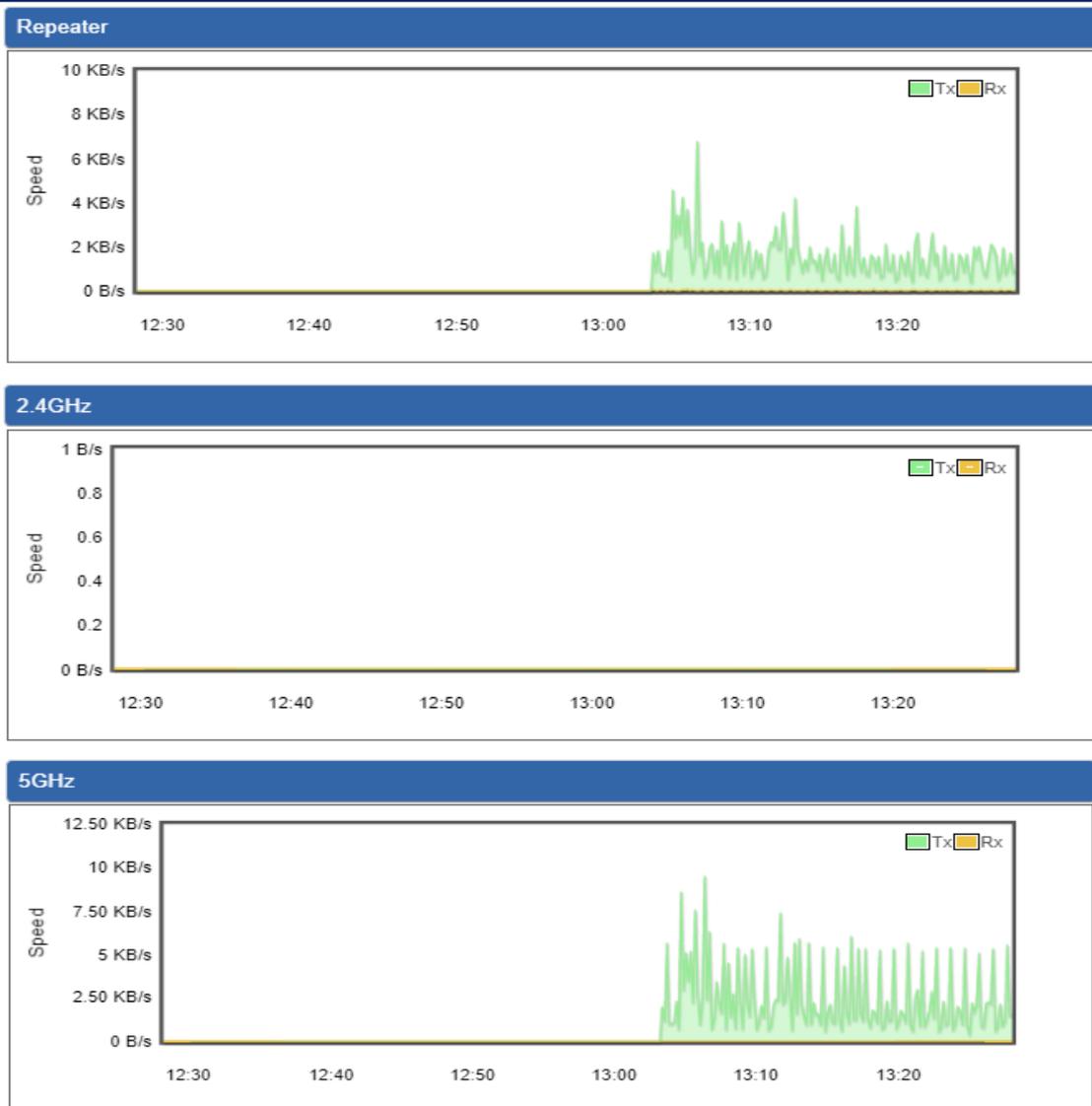


Figure 5-53: Wi-Fi Statistics

5.4.7 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 5-54: 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.

5.5 Maintenance

The Maintenance menu provides the following features for managing the system



Figure 5-55: 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.
LED	Allows you to set the LED status

5.5.1 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 5-56](#).

Account Password

Username	<input type="text" value="admin"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Apply Settings
Cancel Changes

Figure 5-56: Administrator

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

5.5.2 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 5-57](#).

Date and Time

Current Time	Year <input type="text" value="2019"/> Month <input type="text" value="10"/> Day <input type="text" value="22"/> Hour <input type="text" value="10"/> Minute <input type="text" value="27"/> Second <input type="text" value="12"/>
	<input type="button" value="Copy Computer Time"/>
Time Zone Select	<input type="text" value="(GMT+08:00)Taipei"/>
NTP Client Update	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
NTP Server	<input type="text" value="time.nist.gov"/> <input type="text" value="time.windows.com"/> <input type="text" value="time.stdtime.gov.tw"/> <input type="text"/>

Apply Settings
Cancel Changes

Figure 5-57: 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.

5.5.3 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 5-58](#) is shown below:

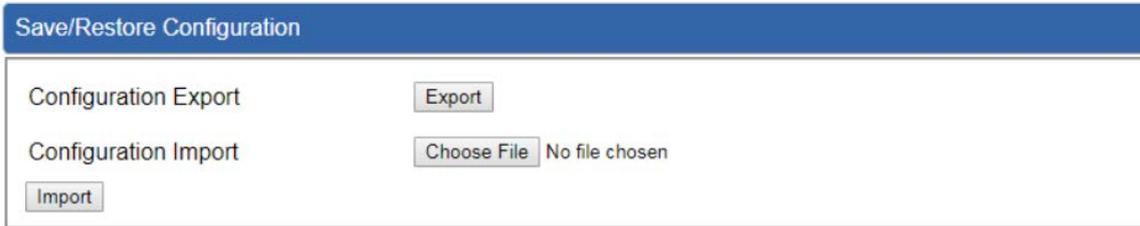
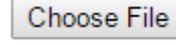


Figure 5-58: Save/Restore Configuration

■ Save Setting to PC

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

5.5.4 Firmware Upgrading

This page provides the firmware upgrade of the router as shown in [Figure 5-59](#).



Figure 5-59: Firmware upgrade

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

5.5.5 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 5-60](#) is shown below:

Reboot / Reset

Reboot Button

Reset Button

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

Figure 5-60: 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 <input type="button" value="Reset to Default"/> button to keep the current network profiles and reset all other configurations to factory defaults.

5.5.6 Auto Reboot

Auto Reboot

Auto Reboot Enable Disable

Reboot Type Daily based Selected Week Day

Monday Tuesday Wednesday Thursday Friday
 Saturday Sunday

Time : (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

5.5.7 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 5-62](#).

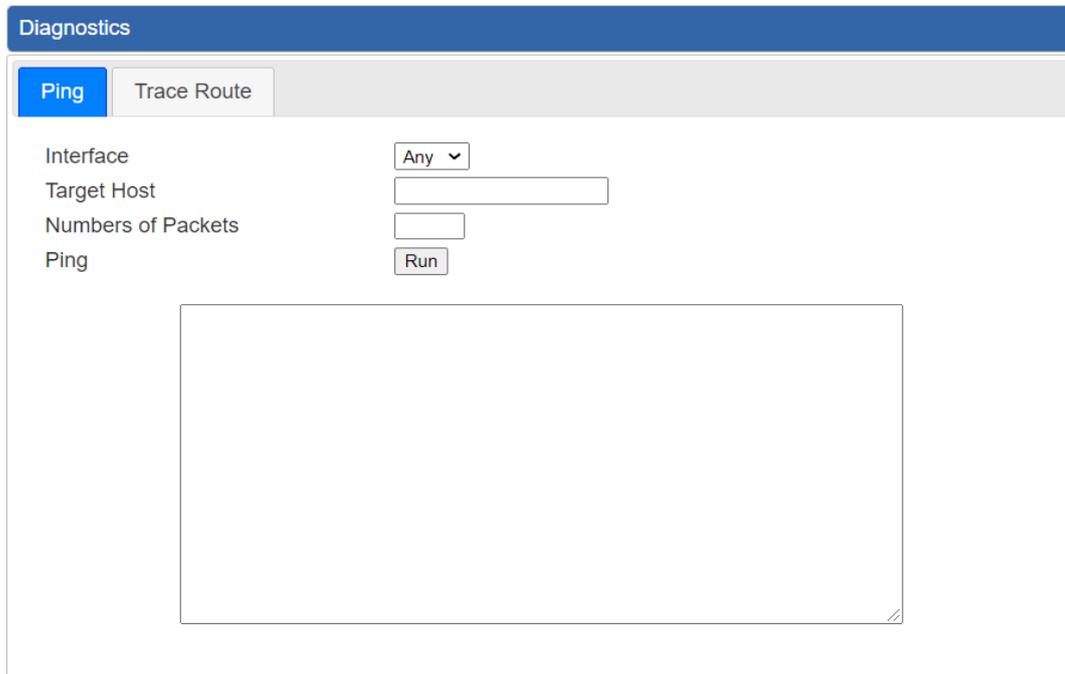


Figure 5-62: Ping

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.

5.5.8 LED

The page allows you to set the status of LED by enabling or disabling it. The LED status is shown in [Figure 5-63](#).

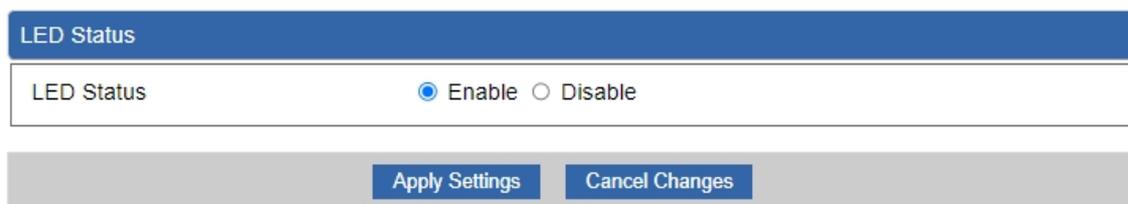


Figure 5-63: LED

Object	Description
Enable	The LED will be turned on if Wi-Fi is enabled.
Disable	The LED will be turned off if it is disabled.

Chapter 6. Quick Connection to a Wireless Network

6.1 Windows XP (Wireless Zero Configuration)

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



Figure 6-1 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

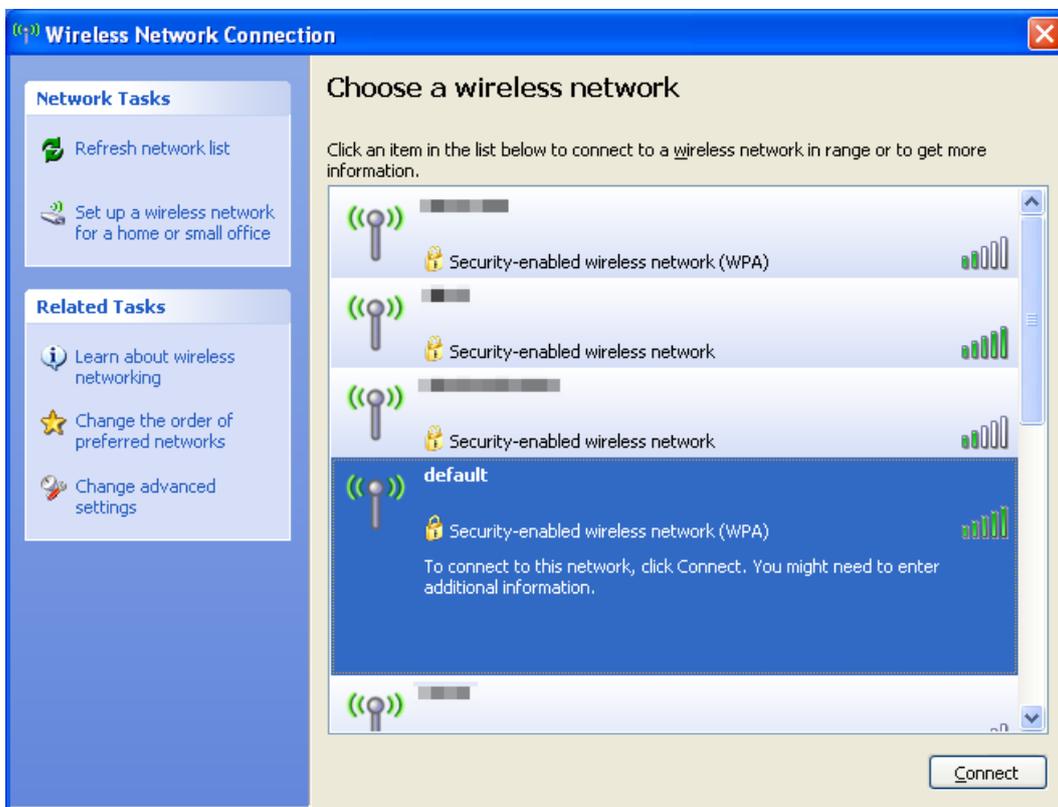


Figure 6-2 Choosing a Wireless Network

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



Figure 6-3 Entering the Network Key

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

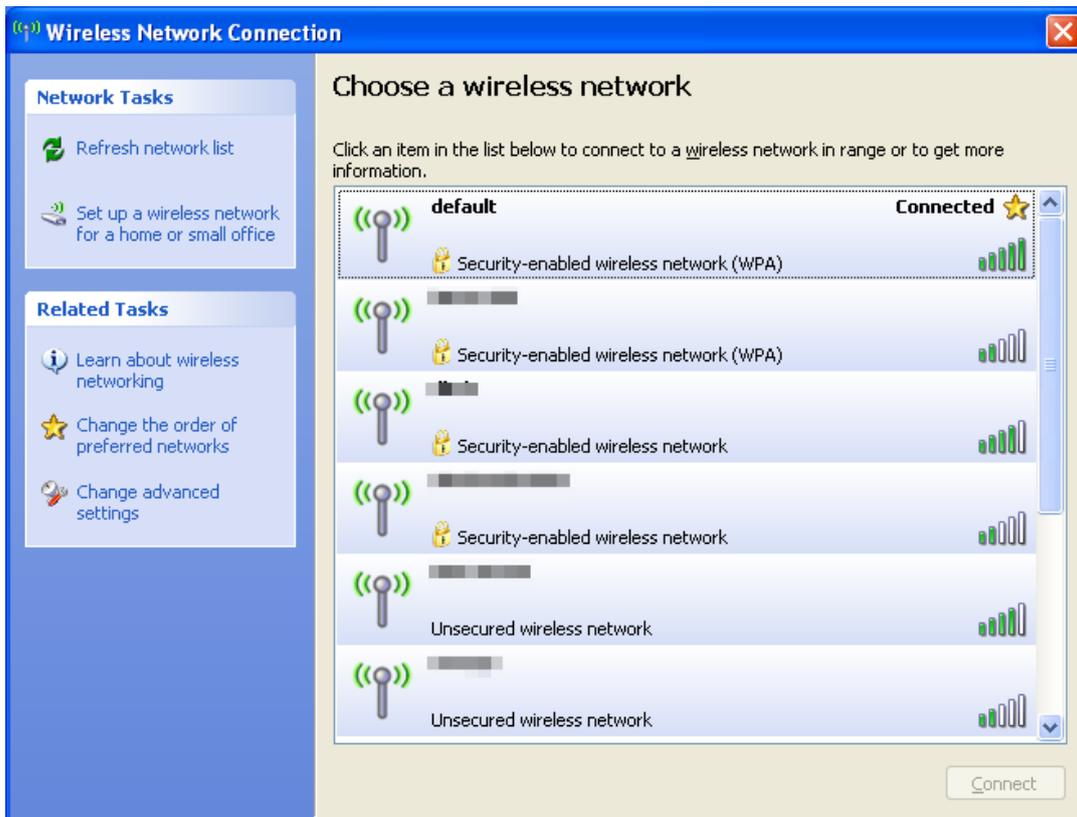


Figure 6-4 Choosing a Wireless Network -- Connected



Note

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.

6.2 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



Figure 6-5 Network Icon

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

- (1) Select SSID [**default**]
- (2) Click the [**Connect**] button

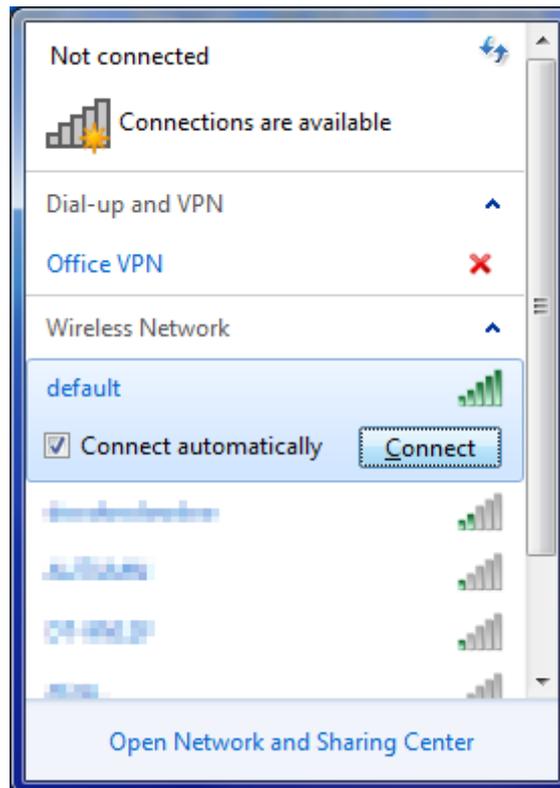


Figure 6-6 WLAN AutoConfig



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

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

- (1) The Connect to a Network box will appear.
- (2) Enter the encryption key that is configured in [section 5.7.2.1](#)
- (3) Click the [OK] button.

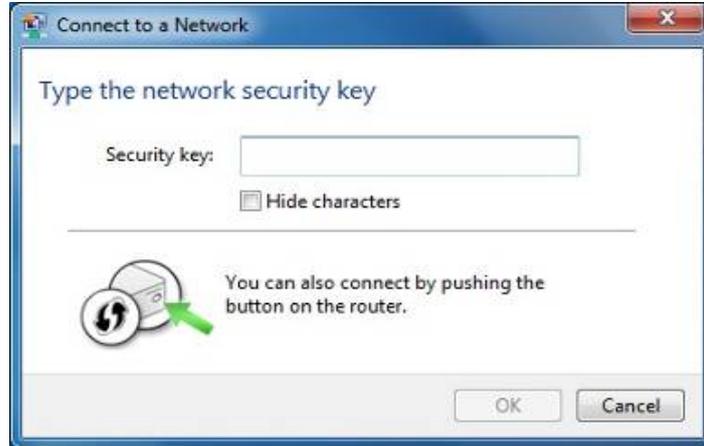


Figure 6-7 Typing the Network Key

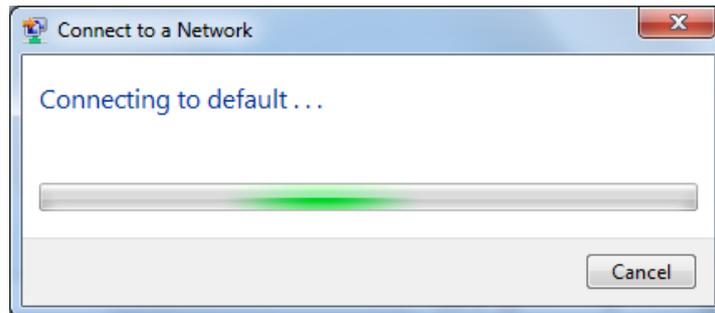


Figure 6-8 Connecting to a Network

Step 4: Check if **“Connected”** is displayed.

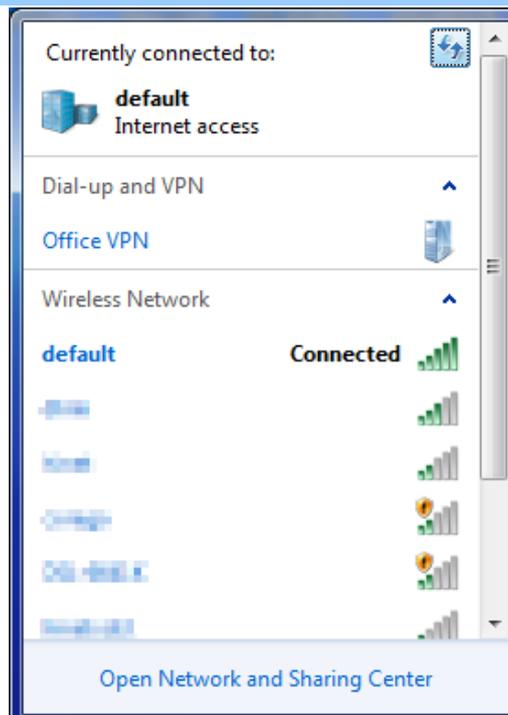


Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the WDAP-C7210E 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 6-10 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 6-11 Highlighting and Selecting the Wireless Network

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

- (1) Enter the encryption key that is configured in [section 5.7.2.1](#)
- (2) Click the [OK] button.



Figure 6-12 Enter the Password



Note

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

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

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

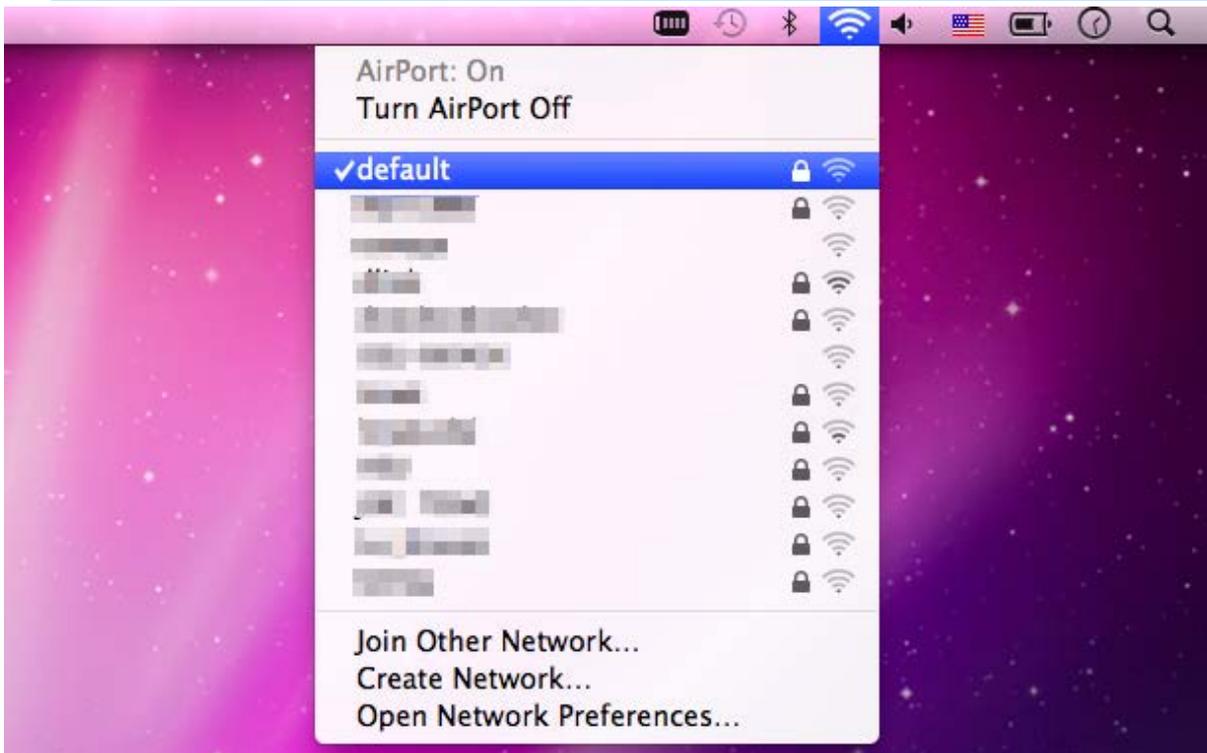


Figure 6-13 Connected to the Network

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**

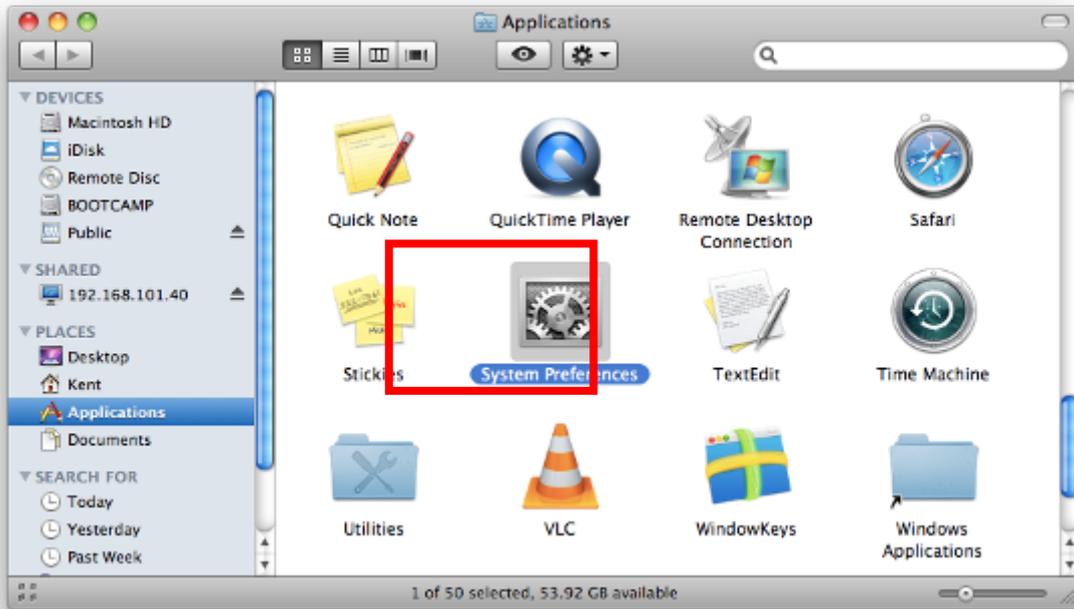


Figure 6-14 System Preferences

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

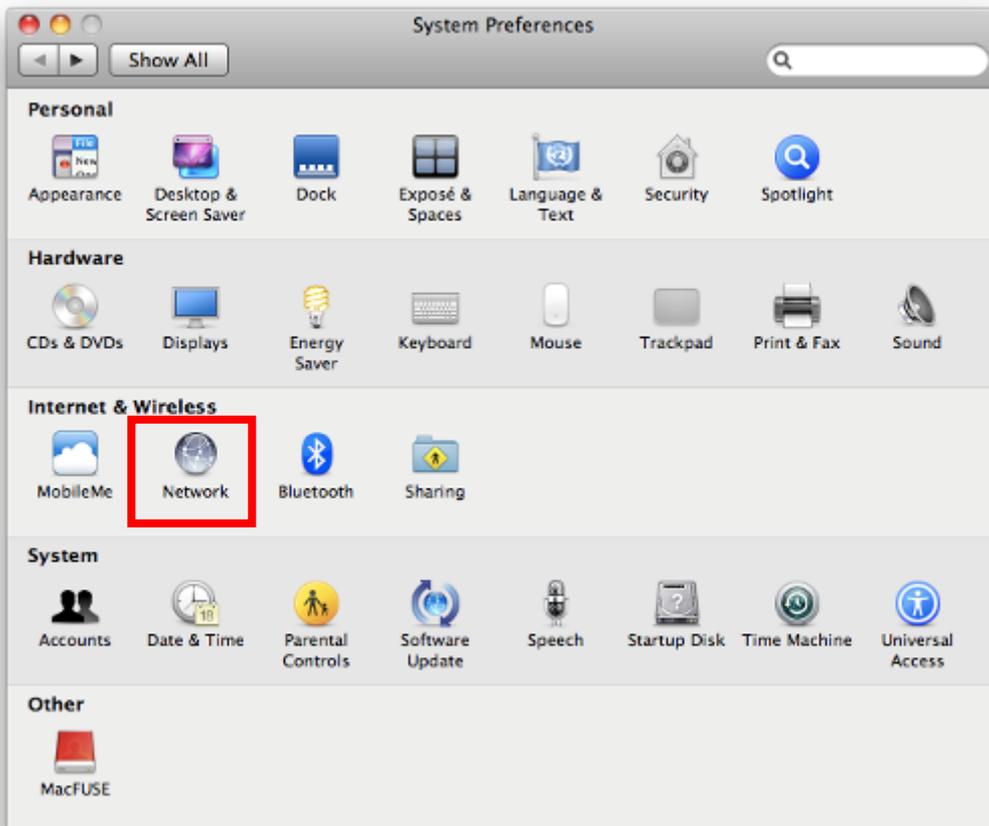


Figure 6-15 System Preferences -- Network

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

- (1) Choose the **AirPort** on the left menu (make sure it is ON)
- (2) Select Network Name [**default**] here

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

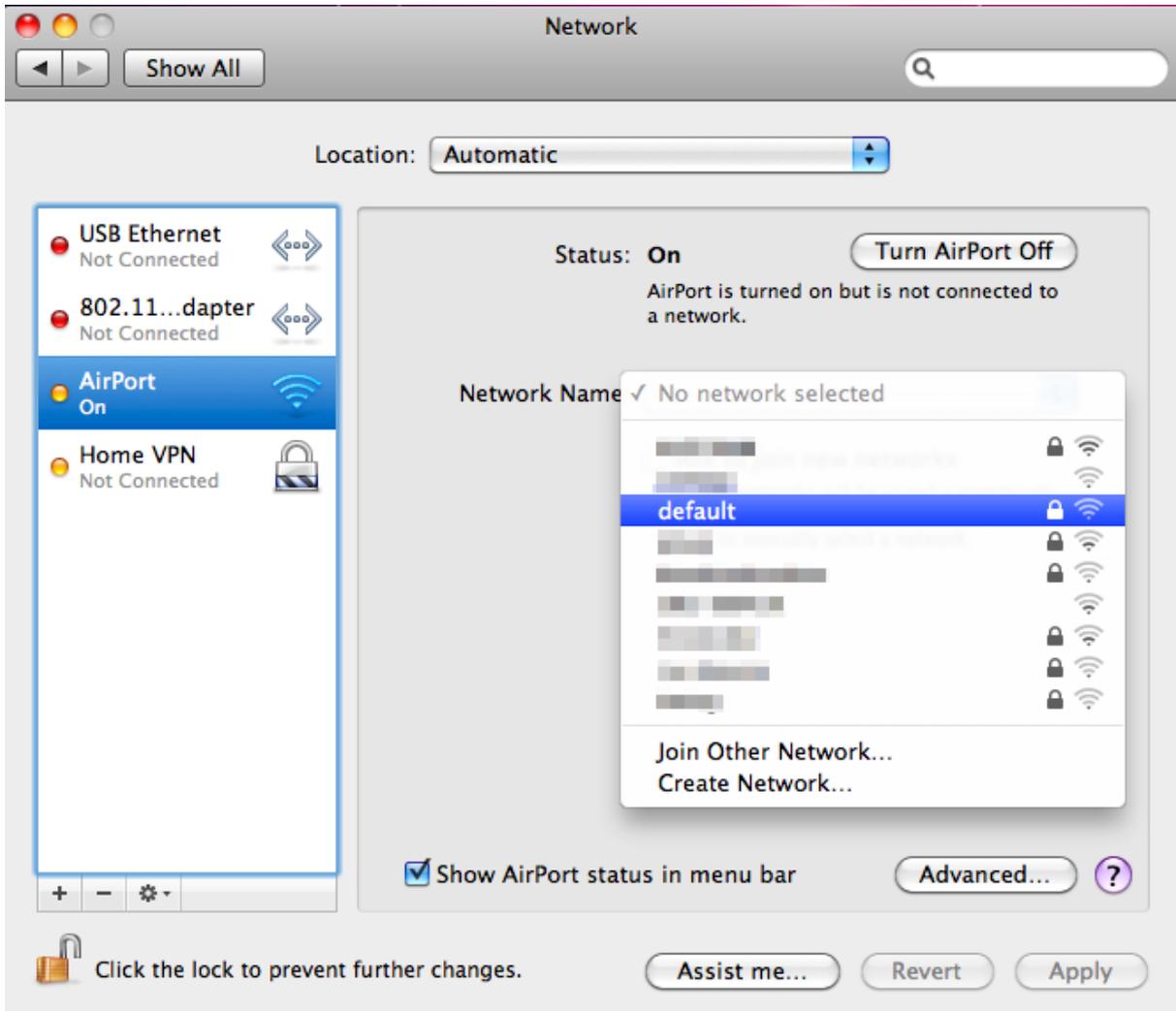


Figure 6-16 Selecting the Wireless Network

6.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the WDAP-C7210E is configured to “**default**”.

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

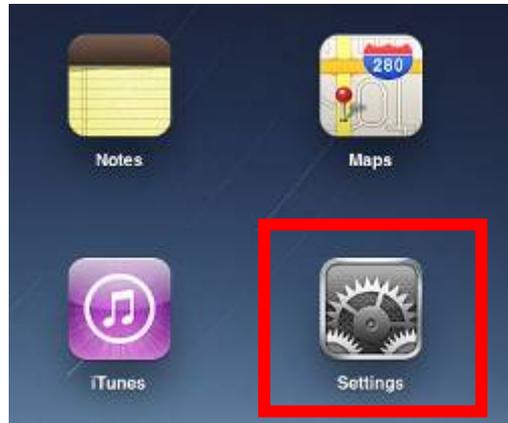


Figure 6-17 iPhone – Settings icon

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

(1) Tap [General] \ [Network]

(2) Tap [Wi-Fi]

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



Figure 6-18 Wi-Fi Setting



Figure 6-19 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in “Choose a Network...”

- (1) Turn on Wi-Fi by tapping “Wi-Fi”
- (2) Select SSID [default]



Figure 6-20 Turning on Wi-Fi

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

- (1) The password input screen will be displayed.
- (2) Enter the encryption key that is configured in [section 5.7.2.1](#)
- (3) Tap the **[Join]** button.

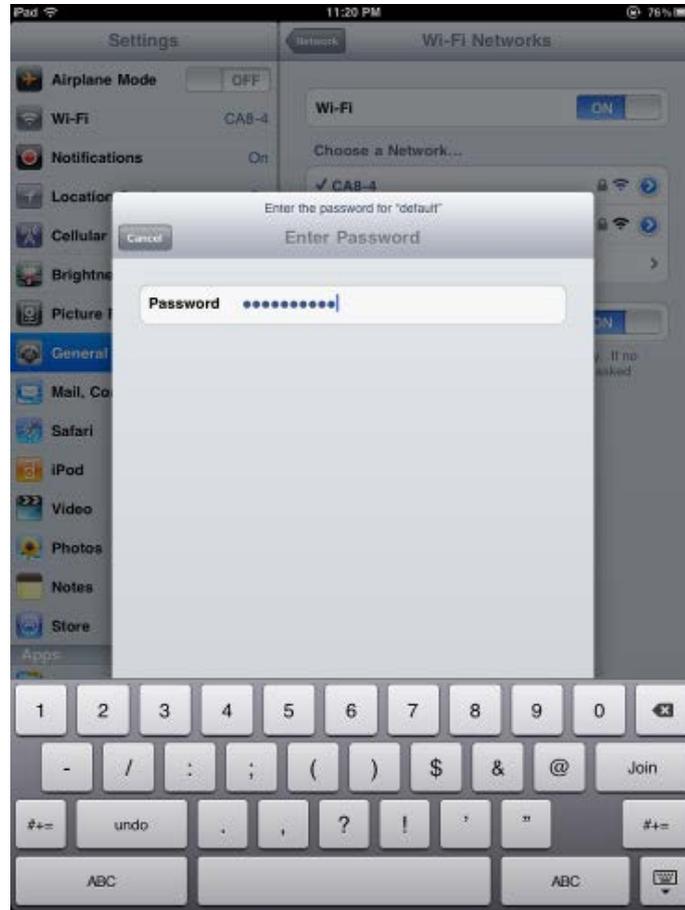


Figure 6-21 iPhone -- Entering the Password

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

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



Figure 6-22 iPhone -- Connected to the Network

Appendix A: Planet Smart Discovery Utility

To easily list the WDAP-C7210E in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution.

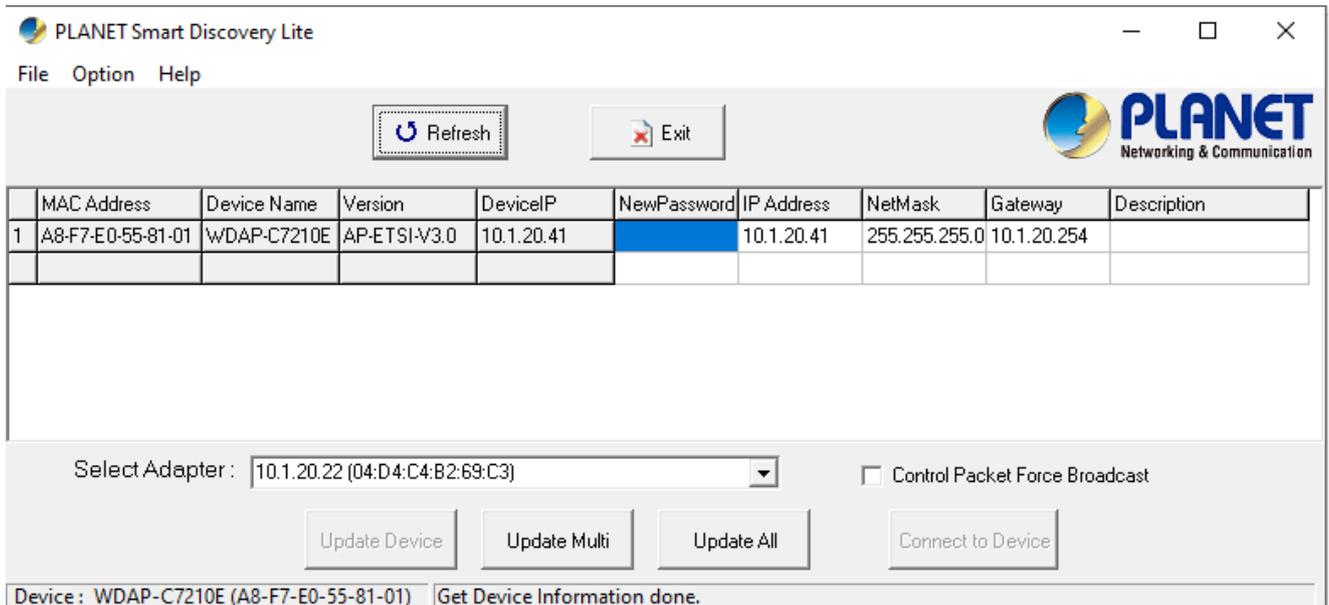
The following installation instructions guide you to running the Planet Smart Discovery Utility.

Step 1: Upload the **Planet Smart Discovery Utility** from the administrator PC.

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



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



Step 3: Press **“Connect to Device”** and then the Web login screen appears.



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

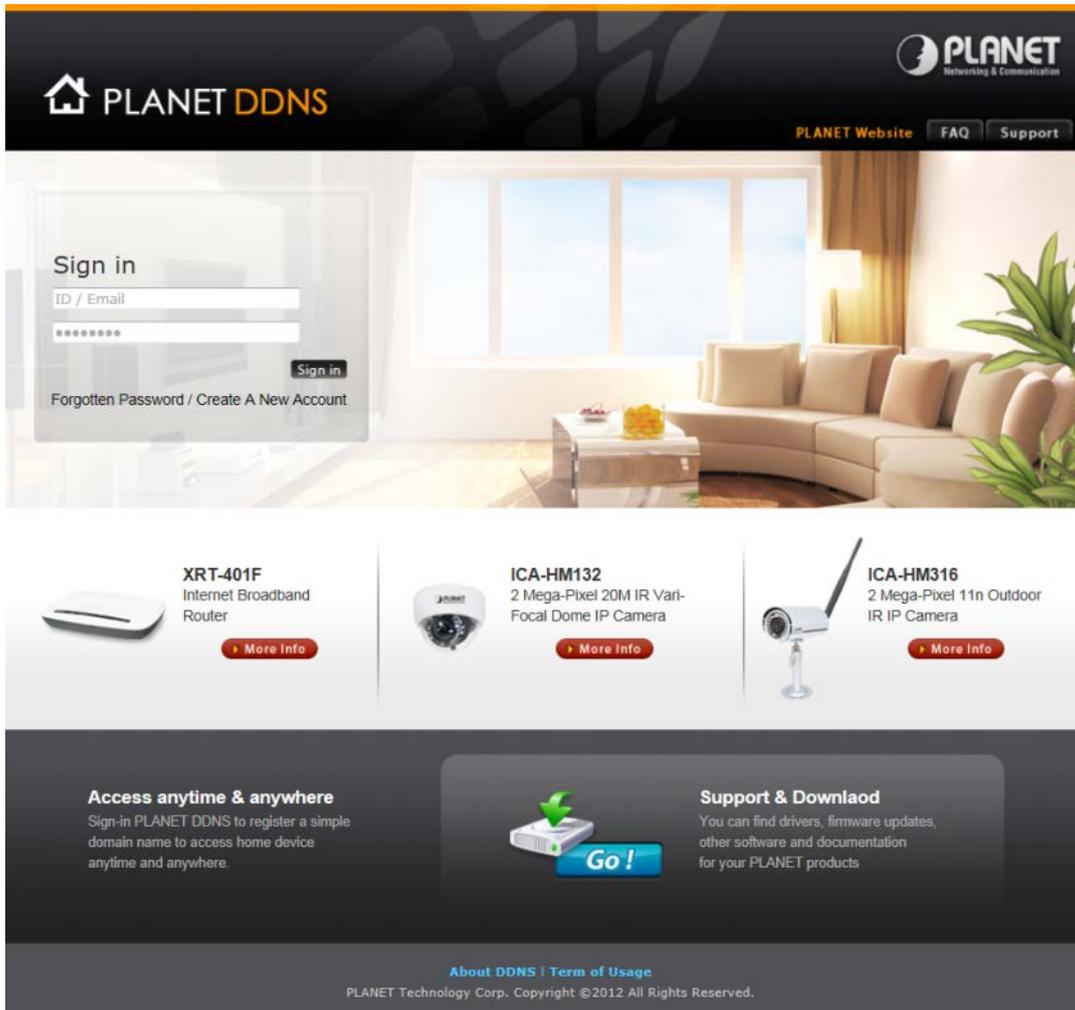
Appendix B: DDNS Application

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.

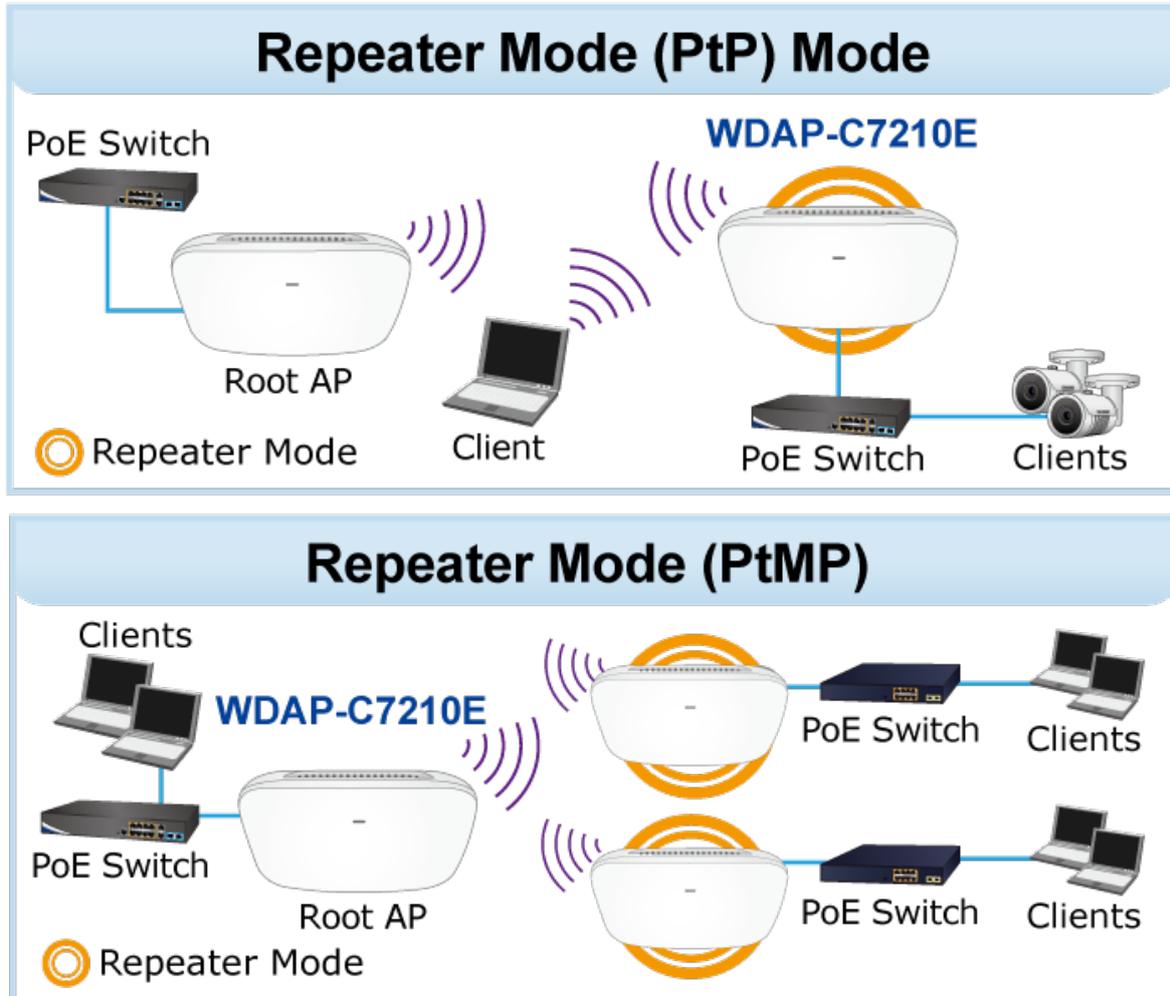
Step 3: Input all DDNS settings.



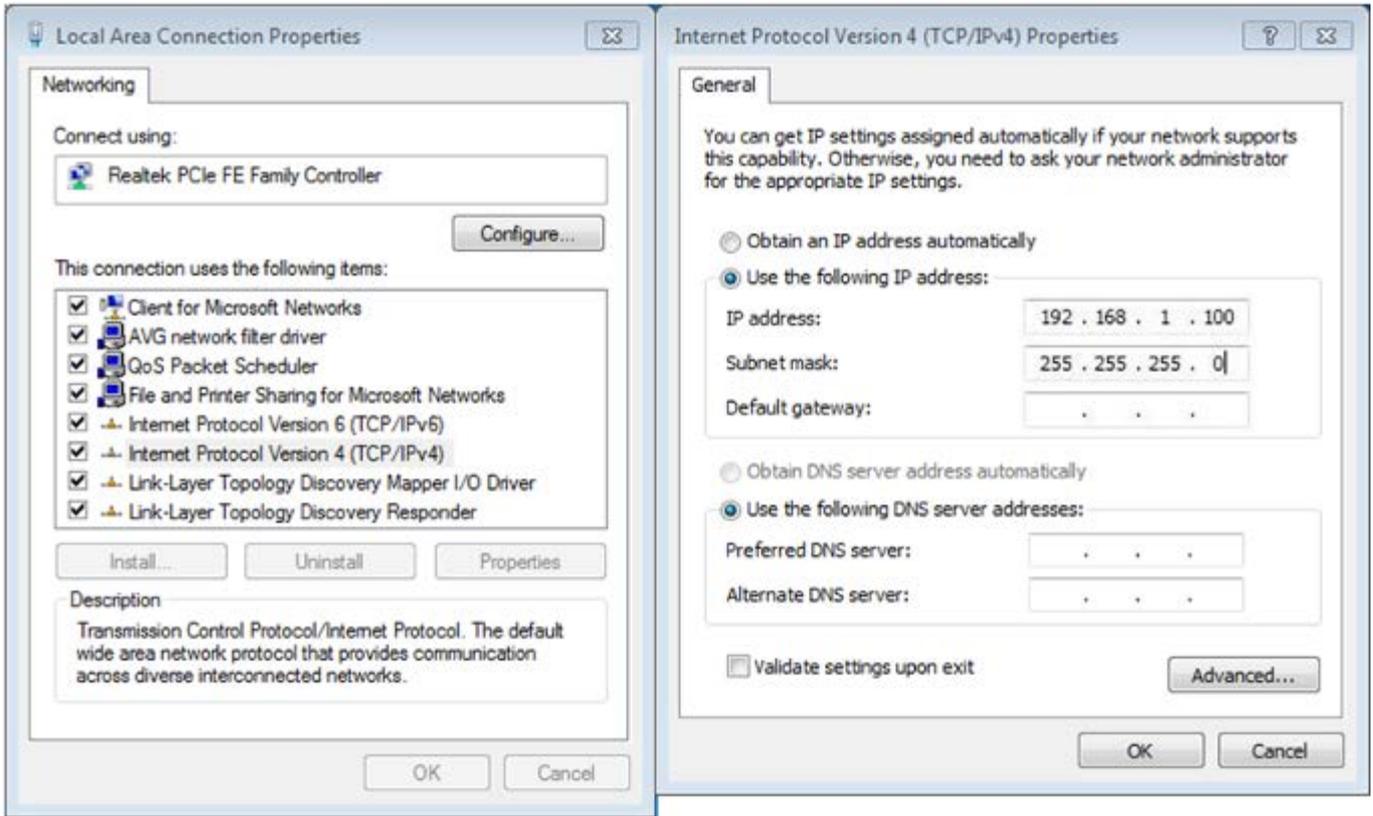
Appendix C: FAQs

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”.



Step 2. For AP-1, go to “Operation Mode” to configure it to **AP Mode**. For AP-2, configure it to **Repeater Mode**.

AP-1

Note: Set a fixed channel for the root AP (AP-1), please don't set auto channel.

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

STEP 1 - Operation Mode

1
Mode

2
LAN

3
Wireless

4
Completed



Gateway Mode

Current Mode



AP Mode



Repeater Mode



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

Cancel Next

AP-2

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

STEP 1 - Operation Mode

1 Mode 2 LAN 3 Wireless Connection 4 Wireless 5 Completed



Gateway Mode



AP Mode



Repeater Mode

▼ Current Mode



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.

Cancel
Next

Step 3. For AP-2, change the default IP to the same IP range but different from AP-1. In this case, the IP of AP-2 is changed to **192.168.1.252** and the IP of AP-1 is set to 192.168.1.253.

Suggestion: It is better to set to static IP for those APs. It could avoid you to unable to find and control those APs by NMS series or AP controller function, especially when an AP gets a new IP from DHCP server.

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

STEP 2 - Network Interface LAN

1 Mode 2 LAN 3 Wireless Connection 4 Wireless 5 Completed

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

Cancel
Previous
Next

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

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

STEP 3 - Network Interface Wireless Connection

1 Mode 2 LAN 3 Wireless Connection 4 Wireless 5 Completed

Select Radio	Use 5GHz Radio
SSID	PLANET_5G
Lock BSSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	A8:F7:E0:00:12:AF
Encryption	WPA2/WPA3 Personal
Passphrase	12345678

Cancel
Previous
Next

Step 5. Click “Next” to set the wireless setting of AP-2, and then Finish the setting of AP-2.

STEP 4 - Network Interface Wireless

1
Mode

2
LAN

3
Wireless Connection

4
Wireless

5
Completed

2.4G WiFi Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

Encryption

5G WiFi Status Enable Disable

SSID

Hide SSID Enable Disable

Bandwidth

Channel

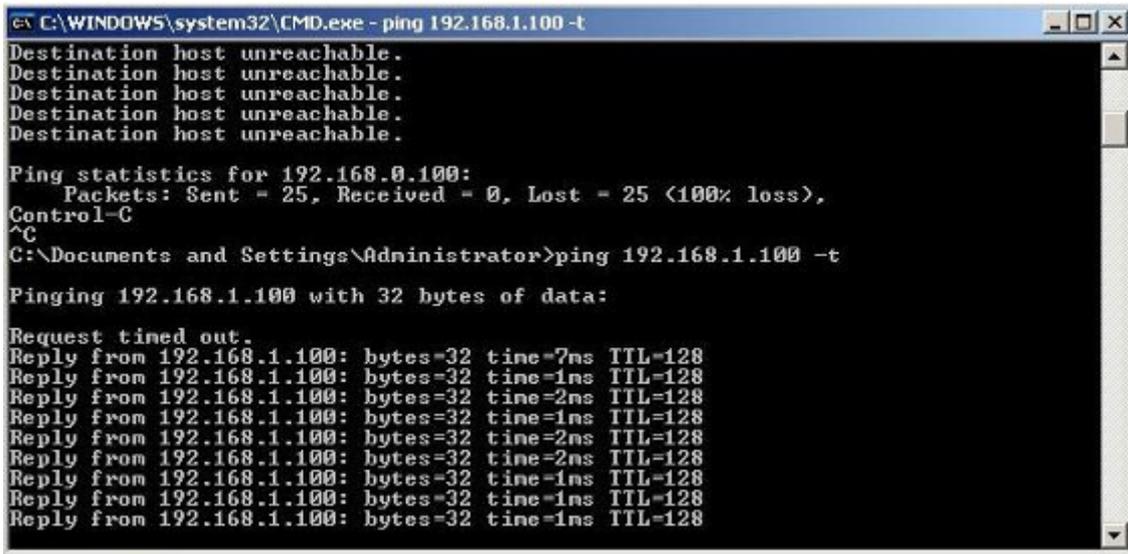
Encryption

Step 6. Click “System Status” to check connection status.

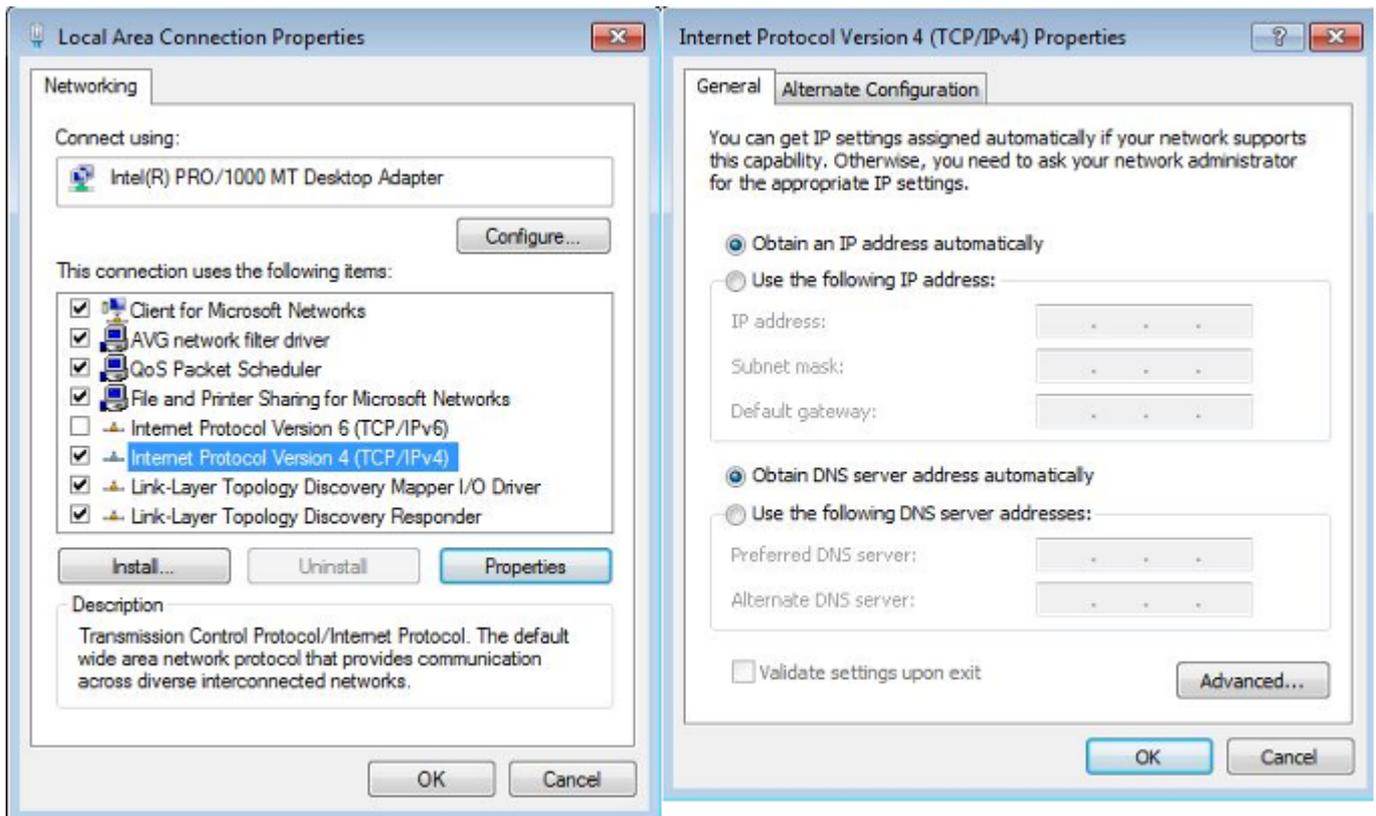
<ul style="list-style-type: none"> Operation Mode Dashboard System Status System Service Statistics Connection Status SNMP NMS Remote Syslog Event Log 	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Device Information</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Model Name</td><td>WDAP-C7210E</td></tr> <tr><td>Firmware Version</td><td>v2.2102b221115</td></tr> <tr><td>Region</td><td>ETSI</td></tr> <tr><td>Current Time</td><td>2022-12-12 Monday 10:00:58</td></tr> <tr><td>Running Time</td><td>0 day, 00:01:11</td></tr> </table> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>LAN</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>MAC Address</td><td>A8:F7:E0:00:18:AC</td></tr> <tr><td>Connection Type</td><td>Static</td></tr> <tr><td>IP Address</td><td>192.168.1.252</td></tr> <tr><td>Netmask</td><td>255.255.255.0</td></tr> <tr><td>Gateway</td><td>192.168.1.1</td></tr> </table> </div> <div style="border: 2px solid red; padding: 5px; margin-bottom: 5px;"> <p>Repeater</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Status</td><td>ON</td></tr> <tr><td>SSID</td><td>PLANET_5G_AP-1</td></tr> <tr><td>Channel</td><td>149</td></tr> <tr><td>Encryption</td><td>WPA2 Personal (TKIP+AES)</td></tr> <tr><td>BSSID</td><td>A8:F7:E0:A1:B2:C9</td></tr> <tr><td>Signal</td><td>-28 dBm</td></tr> <tr><td>Link Quality</td><td>100%</td></tr> </table> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>2.4GHz WiFi</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Status</td><td>ON</td></tr> <tr><td>SSID</td><td>PLANET_2.4G</td></tr> <tr><td>Channel</td><td>6</td></tr> <tr><td>Encryption</td><td>Open</td></tr> <tr><td>MAC Address</td><td>A8:F7:E0:00:18:AE</td></tr> </table> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>5GHz WiFi</p> <table style="width: 100%; border-collapse: collapse;"> <tr><td>Status</td><td>ON</td></tr> <tr><td>SSID</td><td>PLANET_5G</td></tr> <tr><td>Channel</td><td>36</td></tr> <tr><td>Encryption</td><td>Open</td></tr> <tr><td>MAC Address</td><td>A8:F7:E0:00:18:AF</td></tr> </table> </div>	Model Name	WDAP-C7210E	Firmware Version	v2.2102b221115	Region	ETSI	Current Time	2022-12-12 Monday 10:00:58	Running Time	0 day, 00:01:11	MAC Address	A8:F7:E0:00:18:AC	Connection Type	Static	IP Address	192.168.1.252	Netmask	255.255.255.0	Gateway	192.168.1.1	Status	ON	SSID	PLANET_5G_AP-1	Channel	149	Encryption	WPA2 Personal (TKIP+AES)	BSSID	A8:F7:E0:A1:B2:C9	Signal	-28 dBm	Link Quality	100%	Status	ON	SSID	PLANET_2.4G	Channel	6	Encryption	Open	MAC Address	A8:F7:E0:00:18:AE	Status	ON	SSID	PLANET_5G	Channel	36	Encryption	Open	MAC Address	A8:F7:E0:00:18:AF
Model Name	WDAP-C7210E																																																						
Firmware Version	v2.2102b221115																																																						
Region	ETSI																																																						
Current Time	2022-12-12 Monday 10:00:58																																																						
Running Time	0 day, 00:01:11																																																						
MAC Address	A8:F7:E0:00:18:AC																																																						
Connection Type	Static																																																						
IP Address	192.168.1.252																																																						
Netmask	255.255.255.0																																																						
Gateway	192.168.1.1																																																						
Status	ON																																																						
SSID	PLANET_5G_AP-1																																																						
Channel	149																																																						
Encryption	WPA2 Personal (TKIP+AES)																																																						
BSSID	A8:F7:E0:A1:B2:C9																																																						
Signal	-28 dBm																																																						
Link Quality	100%																																																						
Status	ON																																																						
SSID	PLANET_2.4G																																																						
Channel	6																																																						
Encryption	Open																																																						
MAC Address	A8:F7:E0:00:18:AE																																																						
Status	ON																																																						
SSID	PLANET_5G																																																						
Channel	36																																																						
Encryption	Open																																																						
MAC Address	A8:F7:E0:00:18:AF																																																						

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

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



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



Appendix D: 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> a. Go to 'Status' -> 'Internet Connection' menu on the router connected to the AP, and check Internet connection status. b. Please be patient. Sometimes Internet is just that slow. c. If you've connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password entered in the router's settings again. e. Call your Internet service provider and check if there's something wrong with their service. f. If you just can't connect to one or more website, but you can still use other internet services, please check 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,

Scenario	Solution
	but can't use host name, please check DNS setting.
I can't locate my AP by my wireless device.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 E: Glossary

- **802.11ac** - 802.11ac is a wireless networking standard in the 802.11 family (which is marketed under the brand name Wi-Fi), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5 GHz 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 2.4GHz, 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 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - 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 (Domain Name System)** - 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 (Digital Subscriber Line)** - 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 (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - 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 **I**dentification 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 (Wired Equivalent Privacy)** - 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 (Wireless Local Area Network)** - 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-ftiġġiet 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". (BMW)	Nederlands	Hierbij verklaart PLANET Technology Corporation , 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	<i>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ</i> , PLANET Technology Corporation , <i>ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ 11ac Wireless AP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU</i>	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 .