



User's Manual

300Mbps 802.11n Wireless AP/CPE

▶ WAP-500N/WBS-500N



www.PLANET.com.tw




Copyright

Copyright © 2017 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 this company, 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, this company 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 (FCC) Interference Statement

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

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

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 limits set forth for an uncontrolled environment.
This equipment should be installed and operated with the minimum distance of **20cm** between the radiator and your body.

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 the guidelines must be followed 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; WEEE should be collected separately.



Revision

User Manual of PLANET 5GHz 300Mbps 802.11n Wireless AP/CPE

Model: WAP-500N/WBS-500N

Rev: 1.0 (August, 2017)

Part No. EM-WAP-500N_WBS-500N_v1.0

CONTENTS

Chapter 1.Product Introduction	7
1.1 Package Contents	7
1.2 Product Description	8
1.3 Product Features	9
1.4 Hardware Description	11
1.4.1 The Bottom Panel – Port	13
Chapter 2.Connecting to the AP	15
2.1 Preparation before Installation	15
2.1.1 Safety Precautions.....	15
2.2 Installation Precautions	15
2.3 Installing the AP	17
Chapter 3.Quick Installation Guide	19
3.1 Manual Network Setup -- TCP/IP Configuration	19
3.1.1 Configuring the IP Address Manually	19
3.2 Starting Setup in the Web UI	22
Chapter 4.Configuring the AP	24
4.1 Operation Mode	24
4.2 Status	25
4.2.1 Main	25
4.2.2 Save/Reload	27
4.2.3 Wireless Client List	28
4.2.4 WDS Link List	29
4.2.5 DHCP Client Table	29
4.2.6 Connection Status	30
4.2.7 System Log	31
4.3 System	32
4.3.1 IP Settings.....	32
4.3.2 Spanning Tree Settings	33
4.4 Router (WISP Mode Only)	34
4.4.1 DHCP Server Settings	34
4.4.2 WAN Settings.....	35
4.4.2.1. DHCP	36
4.4.2.2. Static IP.....	37
4.4.2.3. PPPoE	39
4.4.2.4. PPTP	41
4.4.3 VPN Passthrough	42
4.4.4 Port Forwarding	43

4.4.5	DMZ Settings	44
4.5	Wireless.....	46
4.5.1	Wireless Network	46
4.5.2	WDS Link Settings	49
4.5.3	Security Settings	50
4.5.4	Wireless MAC Filter	60
4.5.5	Wireless Advanced Settings	61
4.6	Management	63
4.6.1	Administration (Password Settings).....	63
4.6.2	Management VLAN	63
4.6.3	SNMP Settings	64
4.6.4	Backup/Restore Settings	65
4.6.5	Auto Reboot Settings.....	66
4.6.6	Firmware Upgrade	66
4.6.7	Time Settings	68
4.6.8	Wi-Fi Schedule	69
4.6.9	CLI Settings	70
4.6.10	Log	71
4.6.11	Diagnostics	71
4.6.12	Logout.....	73
Appendix A: Troubleshooting.....		74
Appendix B: Use Planet Smart Discovery to find AP		76

FIGURES

FIGURE 1-1 THREE-WAY VIEW (WAP-500N).....	11
FIGURE 1-2 REAR PANEL (WAP-500N)	12
FIGURE 1-3 BOTTOM PANEL (WAP-500N/WBS-500N).....	13
FIGURE 1-4 PoE WARNING LABEL	13
FIGURE 2-1 PoE AND LAN PORT CONNECTION.....	17
FIGURE 2-2 FINISH INSTALLATION AND CONNECT TO ANTENNAS (WAP-500N ONLY)	17
FIGURE 2-3 POLE MOUNTING	18
FIGURE 2-4 WALL MOUNTING	18
FIGURE 3-1 TCP/IP SETTING	20
FIGURE 3-2 WINDOWS START MENU	21
FIGURE 3-3 SUCCESSFUL RESULT OF PING COMMAND	21
FIGURE 3-4 FAILED RESULT OF PING COMMAND	22
FIGURE 3-5 LOGIN BY DEFAULT IP ADDRESS	22
FIGURE 3-6 LOGIN WINDOW	22
FIGURE 3-7 WEB UI SCREENSHOT.....	23
FIGURE 4-1 SYSTEM MENU - RESET	25
FIGURE 4-2 SYSTEM MENU – LANGUAGE OPTION	25
FIGURE 4-3 MAIN STATUS	26
FIGURE 4-4 SAVE/RELOAD	27
FIGURE 4-5 SAVE/RELOAD - DEFAULT	28
FIGURE 4-6 WIRELESS CLIENT LIST	28
FIGURE 4-7 KICK THE CLIENT.....	28
FIGURE 4-8 WDS LINK STATUS	29
FIGURE 4-9 DHCP CLIENT LIST	29
FIGURE 4-10 CONNECTION STATUS	30
FIGURE 4-11 SYSTEM LOG.....	31
FIGURE 4-12 LAN IP SETTINGS.....	32
FIGURE 4-13 SPANNING TREE SETTINGS.....	33
FIGURE 4-14 DHCP SERVER SETTINGS	34
FIGURE 4-15 WAN SETTINGS – ALL.....	35
FIGURE 4-16 WAN SETTINGS – DHCP.....	37
FIGURE 4-17 WAN SETTINGS – STATIC IP	38
FIGURE 4-18 WAN SETTINGS – PPPoE.....	39
FIGURE 4-19 WAN SETTINGS – PPTP	41
FIGURE 4-20 VPN PASSTHROUGH	42
FIGURE 4-21 PORT FORWARDING.....	43
FIGURE 4-22 PORT FORWARDING.....	44
FIGURE 4-23 DMZ	45
FIGURE 4-24 WIRELESS NETWORK – AP/WDS AP MODE	46
FIGURE 4-25 WIRELESS NETWORK – SSID PROFILE.....	47
FIGURE 4-26 WIRELESS NETWORK – CB/WDS STA/CR/REPEATER MODE	48
FIGURE 4-27 WDS LINK SETTINGS – WDS BRIDGE MODE	49

FIGURE 4-28 SECURITY SETTINGS – AP/WDS AP MODE	50
FIGURE 4-29 SECURITY SETTINGS – CB/WDS STA/CR/REPEATER MODE.....	51
FIGURE 4-30 SECURITY SETTINGS – WDS BRIDGE MODE.....	51
FIGURE 4-31 SECURITY SETTINGS – WEP	52
FIGURE 4-32 SECURITY SETTINGS – WPA-PSK.....	53
FIGURE 4-33 SECURITY SETTINGS – WPA2-PSK.....	54
FIGURE 4-34 SECURITY SETTINGS – WPA-PSK MIXED.....	54
FIGURE 4-35 SECURITY SETTINGS – WPA (WPA ENTERPRISE).....	55
FIGURE 4-36 SECURITY SETTINGS – WPA2 (WPA2 ENTERPRISE)	56
FIGURE 4-37 SECURITY SETTINGS – WPA MIXED (WPA MIXED ENTERPRISE).....	58
FIGURE 4-38 WIRELESS MAC FILTER.....	60
FIGURE 4-39 WIRELESS ADVANCED SETTINGS	61
FIGURE 4-40 ADMINISTRATION (PASSWORD SETTINGS).....	63
FIGURE 4-41 MANAGEMENT VLAN	63
FIGURE 4-42 SNMP SETTINGS	64
FIGURE 4-43 BACKUP/RESTORE SETTINGS	65
FIGURE 4-44 AUTO REBOOT SETTINGS	66
FIGURE 4-45 FIRMWARE UPGRADE.....	67
FIGURE 4-46 TIME SETTINGS	68
FIGURE 4-47 WI-FI SCHEDULE	69
FIGURE 4-48 CLI SETTINGS.....	70
FIGURE 4-49 LOG	71
FIGURE 4-50 DIAGNOSTICS.....	72
FIGURE 4-51 LOGOUT.....	73

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WAP-500N/WBS-500N series. Before installing the AP/CPE, please verify the contents inside the package box.

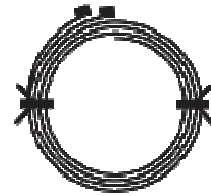
WBS-500N/WAP-500N



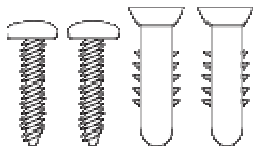
Quick Installation Guide



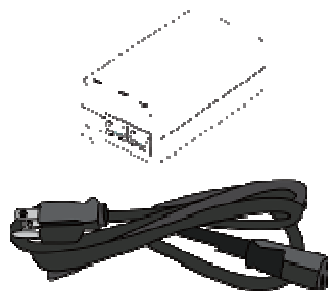
Mounting Strap x 2



Screw Set x 1



PoE Injector & Power Cord



Antenna x 2



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

1.2 Product Description

Cost-effective Wireless Solution with Superior Performance

PLANET WAP-500N/WBS-500N 300Mbps 802.11n Wireless AP/CPE offers a better range and excellent throughput. Via the WAP-500N/WBS-500N's RP-SMA antenna connectors, it is easy to build different point to multi-point applications with good diversity coverage and better noise immunity effect, thus heightening the performance and stability of a long-distance connectivity.

Designed for Various Requirements

The WAP-500N/WBS-500N is dedicatedly designed for WISP solution that provides CPE users with Internet access via the WISP provider in rural areas. Besides, it caters to various wireless communication connectivity, thus meeting users' application requirements.

Multiple SSIDs with VLAN Tagging

Multiple SSIDs can broadcast up to four wireless networks with different names. For management purposes, the **IEEE 802.1Q VLAN** supported allows multiple VLAN tags to be mapped to multiple SSIDs to distinguish the wireless access. This makes it possible for the WAP-500N/WBS-500N to work with managed Ethernet switches to have VLANs assigned for a different access level and authority.

Flexible and Reliable Characteristics

The WAP-500N/WBS-500N is definitely suitable for wireless IP surveillance, and bridge link of building to building and backbone of public service. Additionally, the self-healing capability keeps connection alive all the time. With the **IP55-rated** UV-resistant enclosure, the WAP-500N/WBS-500N can perform normally under rigorous weather conditions, meaning it can be installed in any harsh, environments. With the **proprietary Power over Ethernet (PoE)** design, the WAP-500N/WBS-500N can be easily installed in the areas where power outlets are not available.

Advanced Security and Rigorous Authentication

The WAP-500N/WBS-500N supports 152-bit WEP, WPA/WPA2, WPA-PSK and WPA2-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.

Easy Deployment and Management

With user-friendly Web UI and comprehensive management features including client limit control and **wireless traffic shaping**, the WAP-500N/WBS-500N is easy to limit the client access and inbound/outbound bandwidth control, even for users who have no experience in setting up a wireless network. Furthermore, with the **Planet Smart Discovery** Utility, **SNMP** and diagnostics tools, the WAP-500N/WBS-500N is convenient to be managed remotely.

1.3 Product Features

- **Industrial Compliant Wireless LAN and LAN**
 - Compliant with the IEEE 802.11a/n wireless technology
 - 2T2R architecture with data rate of up to 300Mbps
 - Equipped with two 10/100Mbps RJ45 ports, with auto MDI/MDI-X supported
- **Fixed Network Broadband Router**
 - Supported WAN connection types in WISP mode: DHCP, Static IP, PPPoE, PPTP
 - Supports Port Forwarding and DMZ for various networking applications
 - Supports DHCP server in WISP mode
- **RF Interface Characteristics**
 - Built-in RP-SMA connectors
 - High output power
- **Environmental Characteristics**
 - IP55 rating
 - Passive Power over Ethernet design
 - Operating temperature: -20~70°C
- **Multiple Operation Modes and Wireless Features**
 - Multiple operation modes: AP, WDS, WISP
 - WMM (Wi-Fi multimedia) provides higher priority to multimedia transmitting over wireless
 - Wireless Traffic Shaping to control the upload/download bandwidth
 - Wi-Fi scheduler allows to enable or disable based on predefined schedule
- **Secure Network Connection**
 - Full encryption supported: 64-/128-/152-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK and 802.1X RADIUS authentication
 - Supports 802.1Q VLAN pass-through over WDS and SSID-to-VLAN mapping
 - Supports up to 50 entries of MAC address filtering

➤ **Easy Installation and Management**

- IPv4/IPv6 dual-stack management networks
- Multilingual Web User Interface: English, Spanish, French, German, Portuguese, Russian, Simplified Chinese
- CLI command and SNMP-based management interface
- Self-healing mechanism through system auto reboot setting
- System status monitoring through remote Syslog Server and Device Discovery
- Diagnostic tools include Ping, Traceroute and Speed
- Planet Smart Discovery Utility allows administrator to discover and locate each AP

1.4 Hardware Description

- Dimensions (W x D x H): 100 x 29 x 186mm (without antennas)/100 x 29 x 380mm (with antennas)



Figure 1-1 Three-way View

Rear Panel – LED

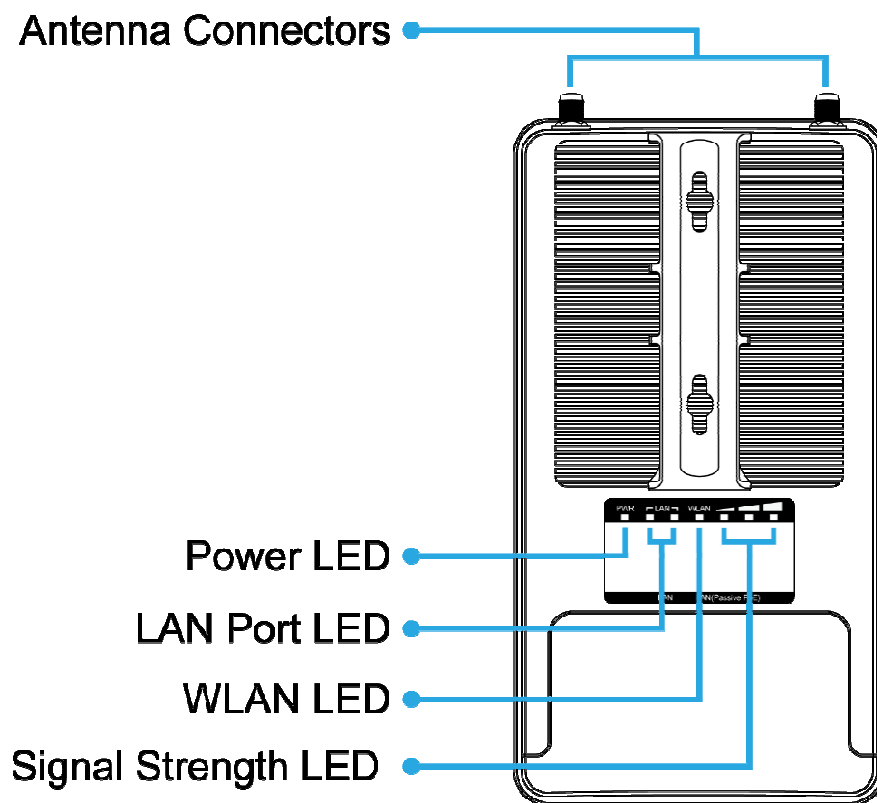


Figure 1-2 Rear Panel

LED Definition

LED	State	Meaning
Power	On	The device is powered on
	Off	The device is powered off
LAN Ports	On	Port linked
	Blinking	Data is transmitting or receiving data
	Off	No link
WLAN	On	The wireless radio is on
	Blinking	Data is transmitting or receiving over wireless
	Off	The wireless radio is off
Signal Strength (CB/WDS STA/CR only)	Green LED on	Signal is good
	Orange LED on	Signal is normal
	Red LED on	Signal is poor

Table 2-1 The LED indication

1.4.1 The Bottom Panel – Port

The Bottom panel provides the physical connectors connected to the power adapter and any other network device. **Figure 1-5** shows the bottom panel of the WAP-500N/WBS-500N.

Bottom Panel

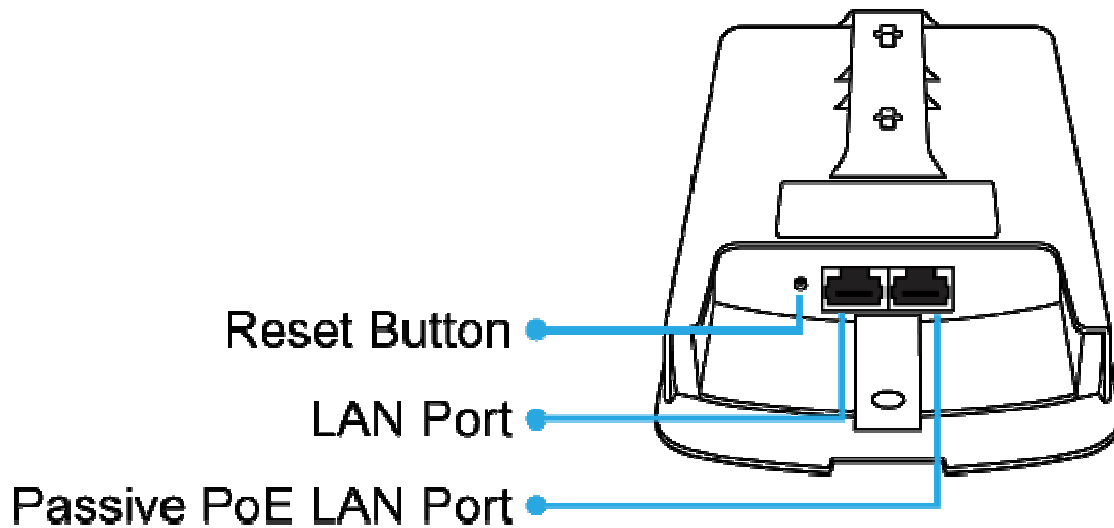


Figure 1-3 Bottom Panel (WAP-500N/WBS-500N)

PoE Warning Label

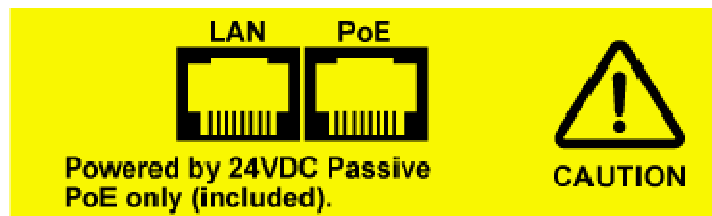


Figure 1-4 PoE Warning Label

Hardware Interface Definition

Object	Description
Antenna Connectors	2 RP-SMA (Female) antenna connectors
Passive PoE LAN Port	10/100Mbps RJ45 port, auto MDI/MDI-X Passive PoE/PD supported, 24VDC In Pin assignment: Pin 4, 5 (+) Pin 7, 8 (-) NOTE: Please use the 24VDC Passive PoE only (included).

LAN Port	10/100Mbps RJ45 port, auto MDI/MDI-X
Reset Button	Press and hold the Reset button on the device for over 10 seconds to return to the factory default setting.

Table 2-2 Hardware Interface Definition

Chapter 2. Connecting to the AP

2.1 Preparation before Installation

2.1.1 Safety Precautions

1. To keep you safe and install the hardware properly, please read and follow these safety precautions.
2. If you are installing the WBS-500N or WAP-500N for the first time, for your safety as well as others', please seek assistance from a installer who has received safety training on the hazards involved.
3. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.
4. When installing the WBS-500N or WAP-500N, please note the following things:
 - ◆ Do not use a metal ladder;
 - ◆ Do not work on a wet or windy day;
 - ◆ Wear shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.
5. When the system is operational, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

2.2 Installation Precautions

- Users **MUST** use a proper and well-installed surge arrestor and grounding kit with the WBS-500N or WAP-500N; otherwise, a random lightning could easily cause fatal damage to the WBS-500N or WAP-500N. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
- Users **MUST** use the "Power cord and PoE Injector" shipped in the box with the WBS-500N or WAP-500N. Use of other options will cause damage to the WBS-500N or WAP-500N.



INSTALLATION WARNING

IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK! Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

CONTACTING POWER LINES CAN BE LETHAL. Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these lines. People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines. Make sure that equipment or personnel do not come in contact directly or indirectly with power lines.



The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination.

This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING, USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

- Select equipment locations that will allow safe, simple equipment installation.
- Don't work alone. A friend or co-worker can save your life if an accident happens.
- Use approved non-conducting ladders and other safety equipment. Make sure all equipment is in good repair.
- If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.
- If anything such as a wire or mast does come in contact with a power line, **DON'T TOUCH IT OR ATTEMPT TO MOVE IT.** Instead, save your life by calling the power company.
- Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS. This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

- The base of the antenna mast or tower must be connected directly to the building protective ground or to one or more approved grounding rods, using 1 OAWG ground wire and corrosion-resistant connectors.
- Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE:

- **DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.**
- Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.

Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

2.3 Installing the AP

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. PoE and LAN port connection:

- (1) Remove the bottom cover.
- (2) Connect one end of the Ethernet cable into the LAN (Passive PoE) port of the device and the other end to the PoE port on the PoE Injector.
- (3) Connect the power cord with the PoE Injector and plug the other end into an electrical outlet.
- (4) Connect the second Ethernet cable into the LAN port of the PoE Injector and the other end to the Ethernet port on the computer.

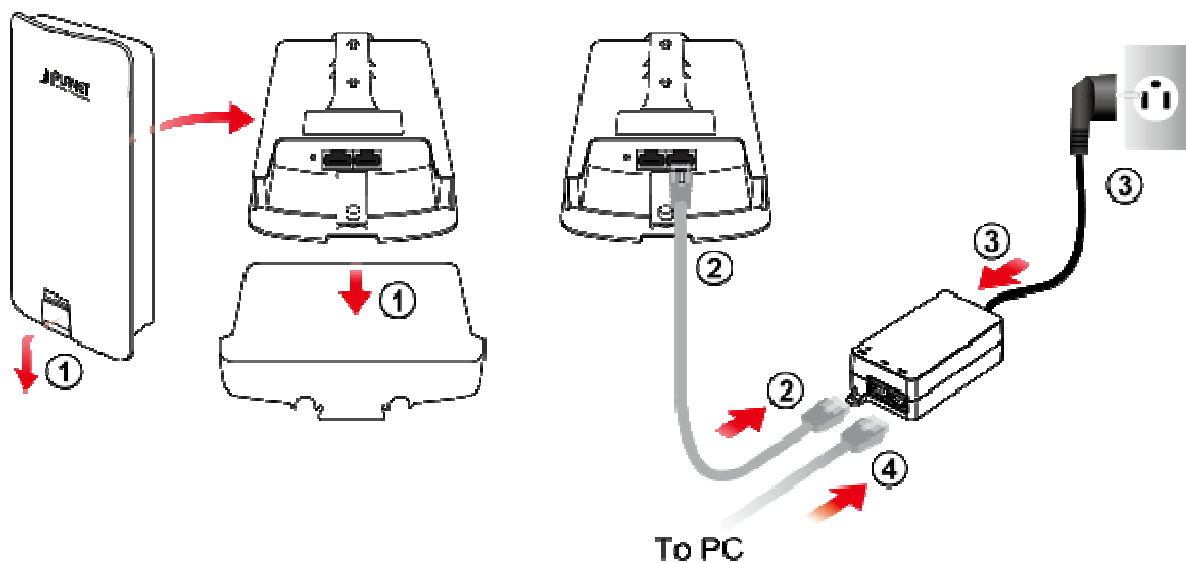


Figure 2-1 PoE and LAN port connection

Step 2. Attach the antennas onto the antenna connectors of the device and place the bottom cover back into the device to finish the installation.

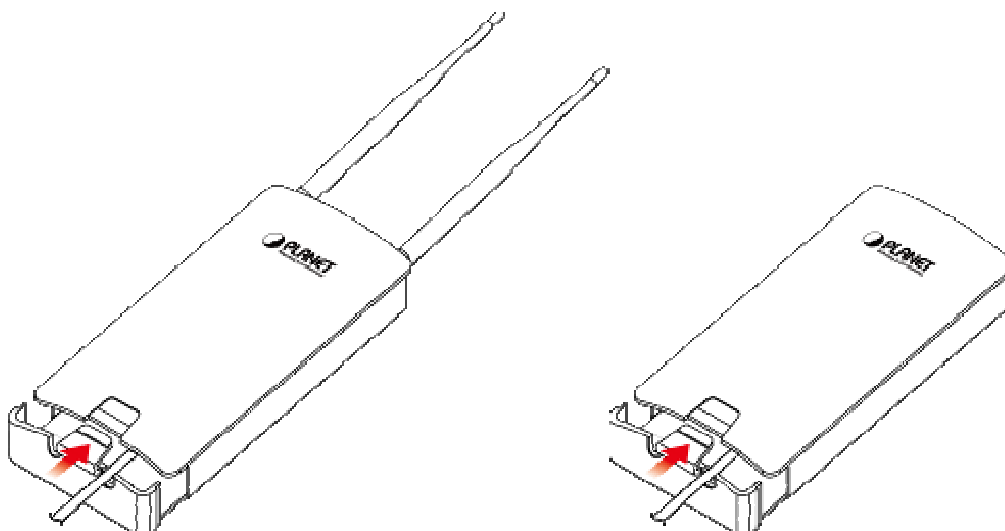


Figure 2-2 Finish installation and connect to antennas

Step 3. Pole Mounting:

- (1) Thread two mounting straps through the mounting bracket on the back of the device.
- (2) Position the device on a pole and secure both mounting straps to finish the installation.

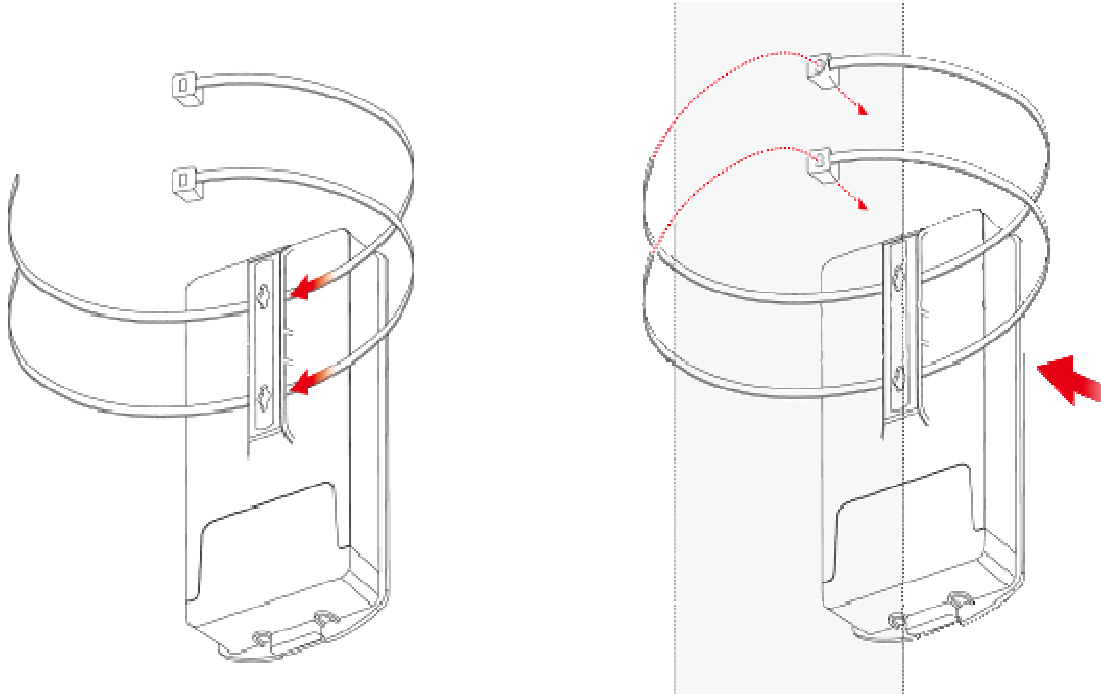


Figure 2-3 Pole Mounting

Step 4. Wall Mounting:

- (1) Secure the adhesive label to a position on the wall where you would like to install the device.
- (2) Follow the plotting sticker to drill two holes and secure the plastic anchors.
- (3) Align the screw holes on the mounting bracket with the screws and then install the device on the wall to finish the installation.

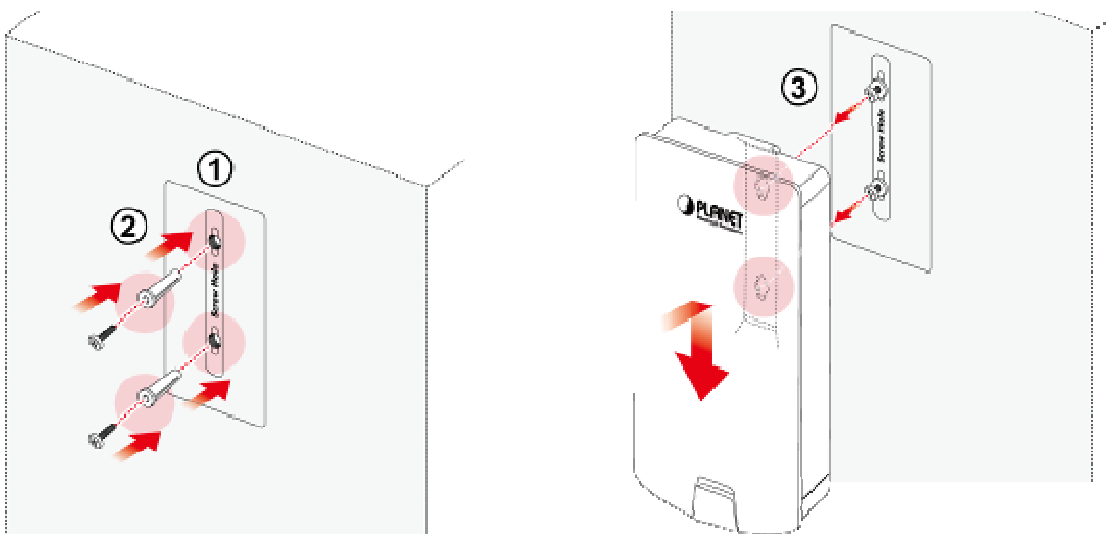


Figure 2-4 Wall Mounting

Chapter 3. 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.

3.1 Manual Network Setup -- TCP/IP Configuration

The default IP address of the WBS-500N and WAP-500N is **192.168.1.253**. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the WBS-500N or WAP-500N with your PC via an Ethernet cable which is then plugged into a LAN port of the PoE injector with one end and into a LAN port of the PC with the other end. Then power on the WBS-500N and WAP-500N via PoE injector or PoE switch.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 7**. And the procedures in other operating systems are similar. First, make sure your Ethernet adapter is working, and refer to the Ethernet adapter's manual if needed.

3.1.1 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 ("xxx" is any number from 2 to 252); subnet mask is 255.255.255.0.

- 1 Select **Use the following IP address** radio button.
- 2 If the AP's LAN IP address is 192.168.1.253, enter IP address 192.168.1.x (x is from 2 to 254 except 192.168.1.253), and **subnet mask** 255.255.255.0.
- 3 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field, you can enter the DNS server IP address which has been provided by your ISP

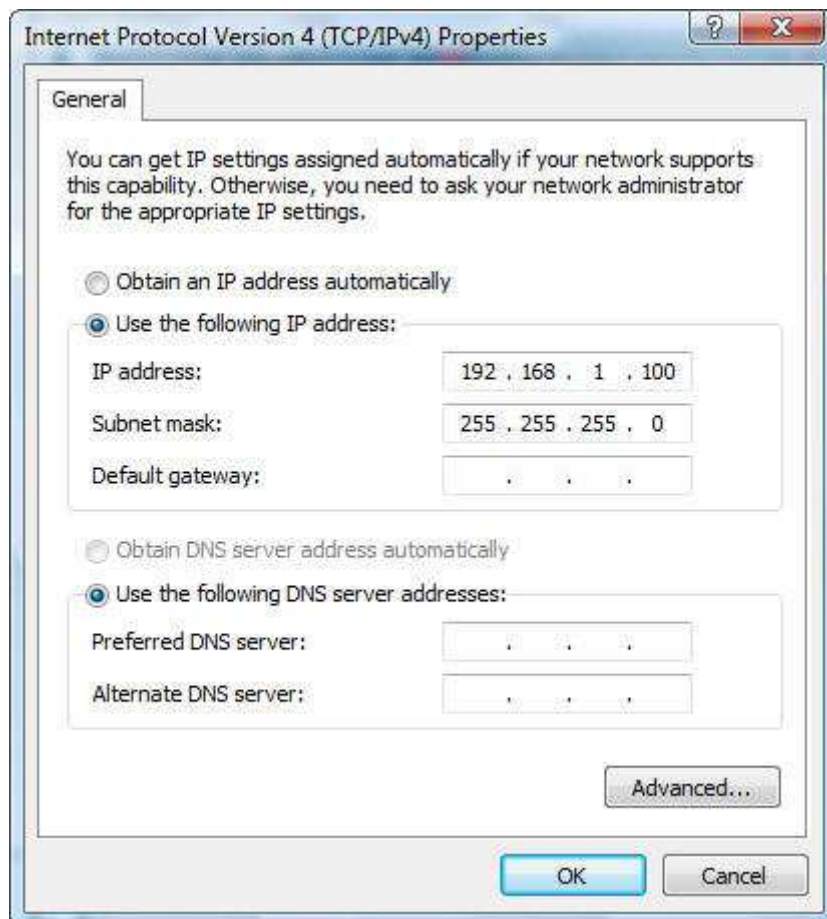


Figure 3-1 TCP/IP Setting

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 7** OS. Please follow the Steps below:

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

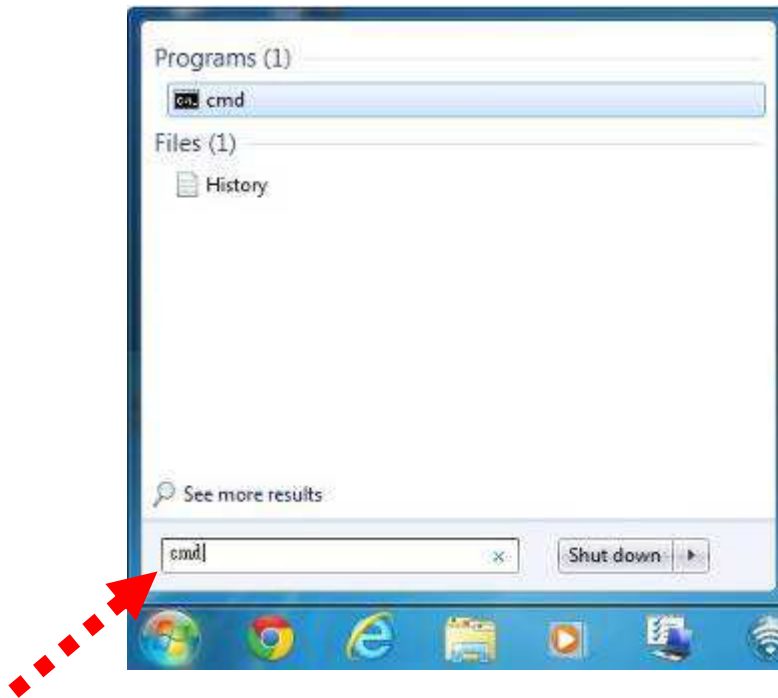


Figure 3-2 Windows Start Menu

3. Open a command prompt and 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.

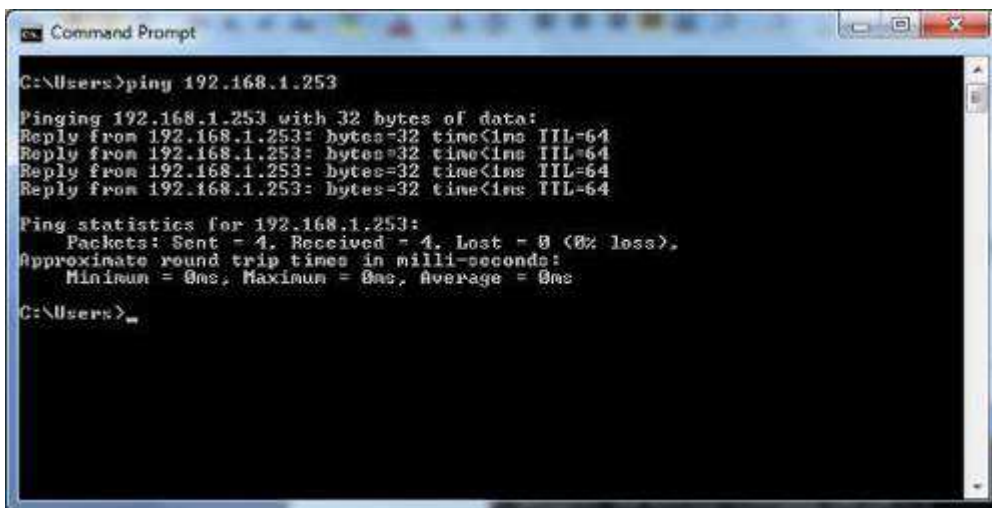


Figure 3-3 Successful result of Ping command

If the result displayed is similar to [Figure 4-4](#), it means the connection between your PC and the AP has failed.

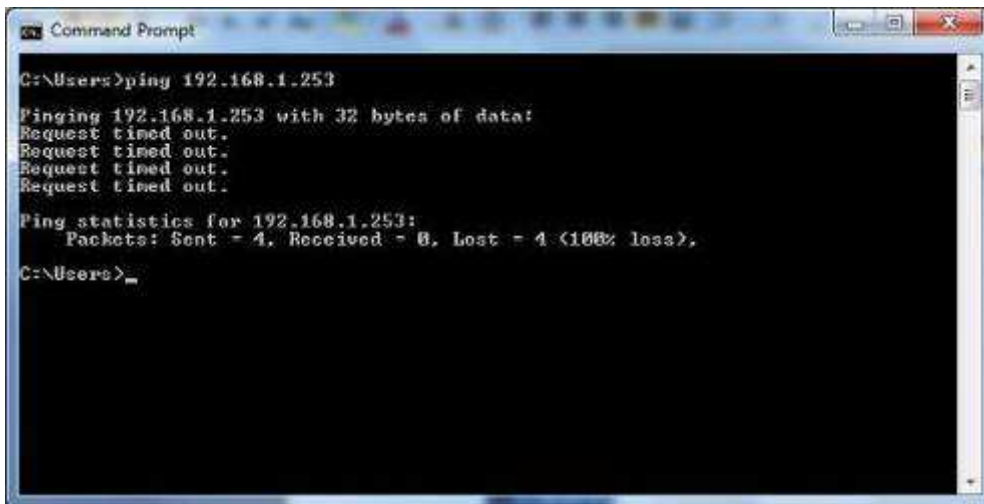


Figure 3-4 Failed result of Ping command

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.

3.2 Starting Setup in the Web UI

It is easy to configure and manage the WBS-500N or WAP-500N with the web browser.

Step 1. To access the configuration page, open a web browser and enter the default IP address <http://192.168.1.253> in the web address field of the browser.

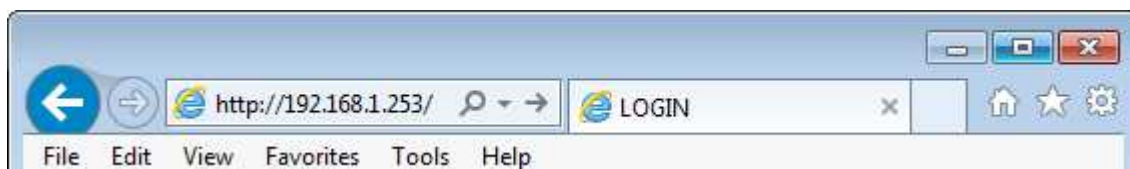


Figure 3-5 Login by default IP address

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.



Figure 3-6 Login Window

Default IP Address: **192.168.1.253**

Default User Name: **admin**

Default Password: **admin**



Note

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

After you enter into the Web User Interface, click **Operation Mode** on the left hand side of the screen to configure the wireless connection. Once the basic configuration of the device is done, go to the **Save/Reload** page to save and apply the changes.

The screenshot displays the Planet 300Mbps 802.11n Outdoor Wireless AP/CPE Web UI. The top header includes the Planet logo and the device model. The main content area is titled 'System Properties' and features a 'Home' and 'Reset' button. Below the title, there are two main sections: 'System Properties' and 'Operation Mode'. The 'System Properties' section contains a 'Device Name' field with the value 'PLANET' and a character count '(1 to 32 characters)'. The 'Operation Mode' section has five radio button options: 'Access Point' (selected), 'Client Bridge', 'WDS', 'Client Router', and 'Repeater'. At the bottom of the 'System Properties' section, there are 'Save & Apply' and 'Cancel' buttons. On the left side, there is a navigation menu with three main categories: 'Status' (containing 'Save/Reload:0', 'Main', 'Wireless Client List', and 'System Log'), 'System' (containing 'Operation Mode', 'IP Settings', and 'Spanning Tree Settings'), and 'Wireless' (containing 'Wireless Network', 'Wireless MAC Filter', and 'Wireless Advanced Settings').

Figure 3-7 Web UI Screenshot

You can choose an Operation Mode according to your application. Please refer to the instructions in the next chapter for configuring different Operation Modes.

Chapter 4. Configuring the AP

This chapter instructs you how to quickly configure the AP/CPE in different operation modes.

4.1 Operation Mode

Go to the “**System → Operation Mode**” page to configure the device in the operation mode which is suitable to your application. Then go to “**Wireless → Wireless Network**” to configure the related wireless settings of each mode.

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Device Name 	Enter a name for the device (1-32 characters). The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices.
<ul style="list-style-type: none"> • Operation Mode 	Select an operation mode for your application.
<ul style="list-style-type: none"> • Save & Apply 	Click Save & Apply to save changes.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the unsaved changes and revert to the previous settings.

4.2 Status

This section provides the current system summary, system log and connection status including Wireless Client List, WDS Link List, DHCP Client Table and Connection Status to assist the administrator in viewing the network status.

In the upper-right corner of each function page, you can click “**Home**” to go back to the **Main** page to view the current system status and click “**Reset**” to force the system reboot or reset the device to factory defaults.

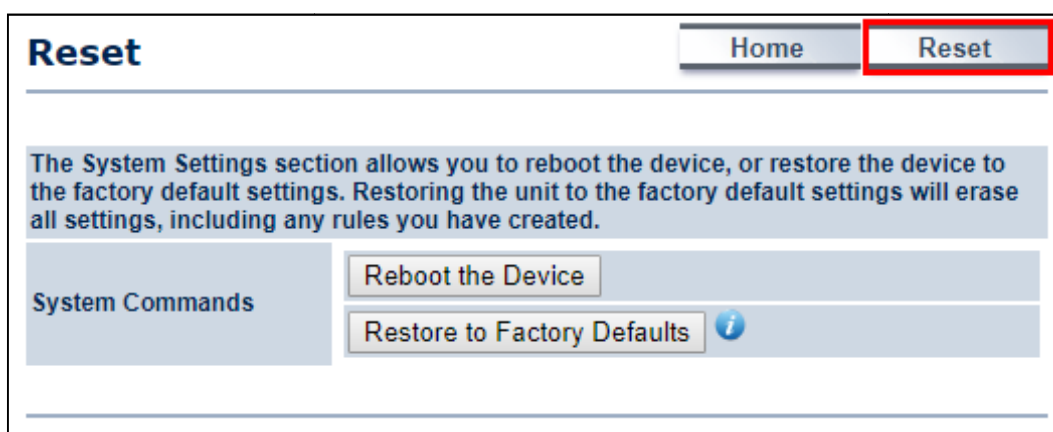


Figure 4-1 System Menu - Reset

In the upper-right corner of each function page, you can choose the **Language** supported in the system from the drop-down list for better user experience. Once a language is chosen, the whole web page will be translated into the language that you preferred.



Figure 4-2 System Menu – Language option

4.2.1 Main

Click “**Status → Main**” to view the current system summary.

Main		Home	Reset
System Information			
Device Name	WBS-500N		
Ethernet Main MAC Address	A8:F7:E0:58:E9:73		
Ethernet Secondary MAC Address	A8:F7:E0:58:E9:73		
Wireless MAC Address	A8:F7:E0:58:E9:72		
Country	N/A		
Current Time	Wed Apr 26 18:09:46 UTC 2017		
Firmware Version	1.0.0		
LAN Settings			
IP Address	192.168.1.251		
Subnet Mask	255.255.255.0		
DHCP Server	Enabled		
RX(Packets)	184.158 KB (2072 PKts.)		
TX(Packets)	2.94403 MB (2918 PKts.)		
WAN Settings			
MAC Address	A8:F7:E0:58:E9:72		
Connection Type	DHCP		
Connection Status	Up		
IP Address	192.168.100.131		
IP Subnet Mask	255.255.255.0		
Primary DNS	192.168.100.1		
Secondary DNS			
RX(Packets)	9.13184 KB (54 PKts.)		
TX(Packets)	7.24023 KB (123 PKts.)		
Current Wireless Settings			
Operation Mode	Client Router		
Wireless Mode	IEEE 802.11 A/N Mixed		
Channel Bandwidth	20/40 MHz		
Frequency/Channel	5.18 GHz(Channel 36)		
Wireless Network Name (SSID)	PLANET 1		
Security	WPA2-PSK AES		
Distance	1 km		
RX(Packets)	9.13184 KB (54 PKts.)		
TX(Packets)	7.24023 KB (123 PKts.)		
Refresh			

Figure 4-3 Main Status

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • System Information 	Shows the general system information such as device name, MAC address, country, current time, and firmware version.
<ul style="list-style-type: none"> • LAN Settings 	Shows Local Area Network settings such as the LAN IP address, subnet mask, DHCP server, and Rx/Tx packets.
<ul style="list-style-type: none"> • WAN Settings 	Shows Wide Area Network settings such as the MAC address, connection type, connection status, IP address, subnet mask, primary and secondary DNS, and Rx/Tx packets.
<ul style="list-style-type: none"> • Current Wireless Settings 	Shows wireless information such as operation mode, wireless mode, channel bandwidth, frequency, channel, information about each SSID, security settings, and Rx/Tx packets.

4.2.2 Save/Reload

Click "**Status → Save/Reload**" and the following page will be displayed.

The screenshot displays the 'Save/Reload' page of the Access Point web interface. The left sidebar contains a navigation menu with the following items: Status, **Save/Reload:16** (highlighted in red), Main, Wireless Client List, System Log, System, Operation Mode, IP Settings, Spanning Tree Settings, Wireless, Wireless Network, Wireless MAC Filter, Wireless Advanced Settings, and Management. The main content area features a 'Save/Reload' title, 'Home' and 'Reset' buttons, and an 'Unsaved changes list' section. The list contains the following configuration parameters:

```
-network.1.ifname
-network.3.ifname
network.lan.ifname=eth0
-network.4.ifname
-network.2.ifname
network.sys.ManagementVLANID=4096
wireless.cfg039f7e.wps_configured=1
wireless.cfg039f7e.key=12345678
wireless.cfg039f7e.encryption=psk2 aes
wireless.cfg039f7e.WLANWpaRadiusAccSrvIP=...
wireless.cfg039f7e.hidden=0
wireless.cfg039f7e.server=...
wireless.wifi0.WLANHTMode=40
wireless.wifi0.WLANExtChannel=0
wireless.wifi0.channel=36
wireless.cfg09feac.WLANVLANEnable=0
```

At the bottom of the page, the 'Save & Apply' button is highlighted in red, along with a 'Revert' button.

Figure 4-4 Save/Reload

Click **Save & Apply** to save and apply all configurations.

Click **Revert** to cancel the unsaved changes and revert to the previous settings that have been saved.

It's not necessary to save and apply the settings if unsaved changes list is empty.

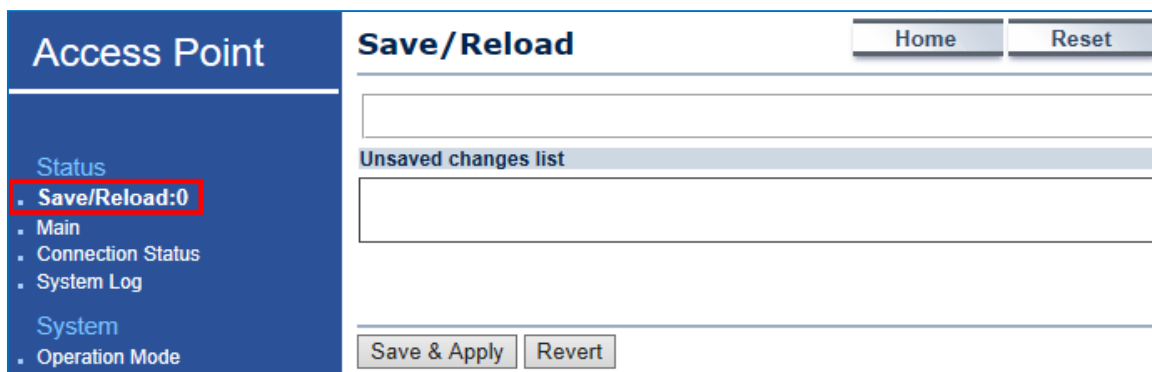


Figure 4-5 Save/Reload - Default

4.2.3 Wireless Client List

Click “Status → Wireless Client List” to view the current associated client.

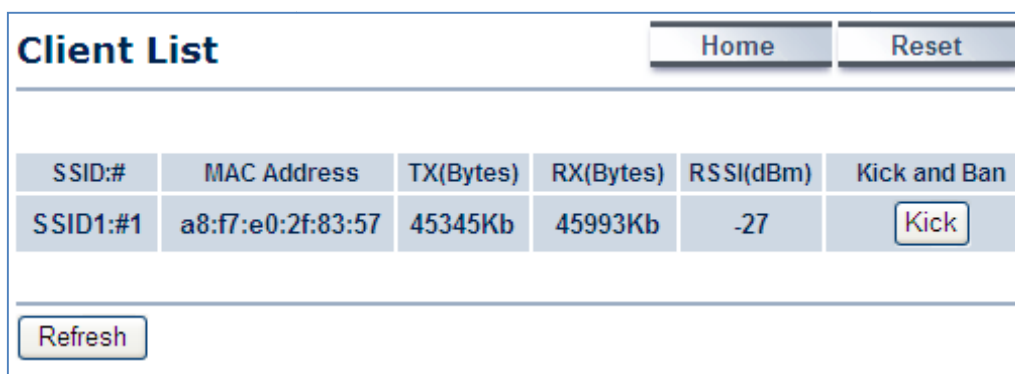


Figure 4-6 Wireless Client List

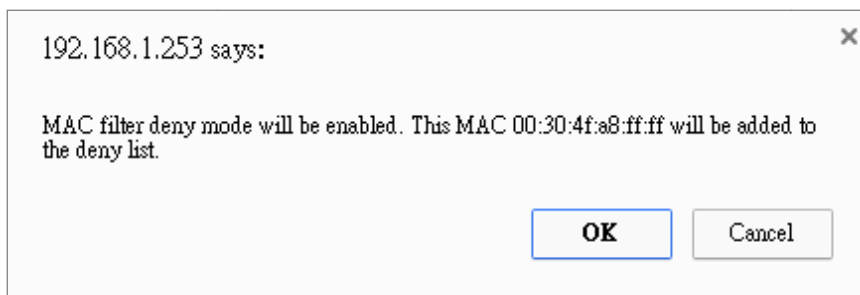


Figure 4-7 Kick the client

The page includes the following settings:

Object	Description
• SSID:#	The SSID number that the client is associated with.
• MAC Address	The MAC address of the associated client.
• Tx (Bytes)	The current transmit packet of the associated client.
• Rx (Bytes)	The current received packet of the associated client.
• RSSI (dBm)	The current signal strength of the associated client.

<ul style="list-style-type: none"> • Kick and Ban 	Click Kick to add the client to the wireless mac filtering deny list.
---	--

4.2.4 WDS Link List

Click “**Status → WDS Link List**” to view the current WDS link client.

The **WDS Link List** is only available in WDS Bridge mode.

WDS Link Status			
		Home	Reset
WDS Link ID	MAC Address	Link Status	RSSI (dBm)
1	a8:f7:e0:2f:83:57	UP	-35
Refresh			

Figure 4-8 WDS Link Status

The page includes the following settings:

Object	Description
• WDS Link ID	The sequence number of the WDS link.
• MAC Address	The MAC Address of the associated remote node.
• Link Status	The current link status.
• RSSI (dBm)	The current signal strength of the associated remote node.
• Refresh	Click Refresh to update the current list.

4.2.5 DHCP Client Table

Click “**Status → DHCP Client Table**” to view the current DHCP client.

The **DHCP Client Table** is only available in WISP mode.

DHCP Client List					
		Home	Reset		
MAC Address	IP	Host Name	Expires	Revoke	Reserve
00:16:d4:ff:d2:e3	192.168.1.107	ENM-2-PC	23h 53min 48s	Revoke	Reserve
Refresh					

Figure 4-9 DHCP Client List

The page includes the following settings:

Object	Description
• MAC Address	The MAC Address of the DHCP client.
• IP	The IP assigned to the DHCP client.
• Host Name	The Host Name of the DHCP client.
• Expires	The Expired time of the DHCP client.
• Revoke	Click Revoke to revoke the DHCP lease of the client.
• Reserve	Click Reserve to reserve the IP to the client.
• Refresh	Click Refresh to update the client list.

4.2.6 Connection Status

Click “**Status → Connection Status**” to view the current DHCP client.

Connection Status		Home	Reset
Network Type	WDS Station		
SSID	PLANET1		
BSSID	A8:F7:E0:42:12:83		
Connection Status	Associated		
Wireless Mode	IEEE 802.11n/a Mixed		
Current Channel	5.18 GHz(Channel 36)		
Security	WPA2-PSK AES		
Tx Data Rates(Mbps)	300 Mbps		
Current noise level	-95 dBm		
Signal strength	-60 dBm		
Refresh			

Figure 4-10 Connection Status

The page includes the following settings:

Object	Description
• Network Type	The current operation mode of the device.
• SSID	The SSID of the connected AP.
• BSSID	The MAC Address of the connected AP.
• Connection Status	The status of the connection.

• Wireless Mode	The current wireless mode of the AP.
• Current Channel	The current channel used of this connection.
• Security	The encryption method of the AP.
• Tx Data Rates (Mbps)	The current data rates of the connection.
• Current Noise Level	The current noise level of the connection
• Signal Strength	The current signal strength of the connected AP.
• Refresh	Click Refresh to update the current data.

4.2.7 System Log

Click “**Status → System Log**” to view the system log.

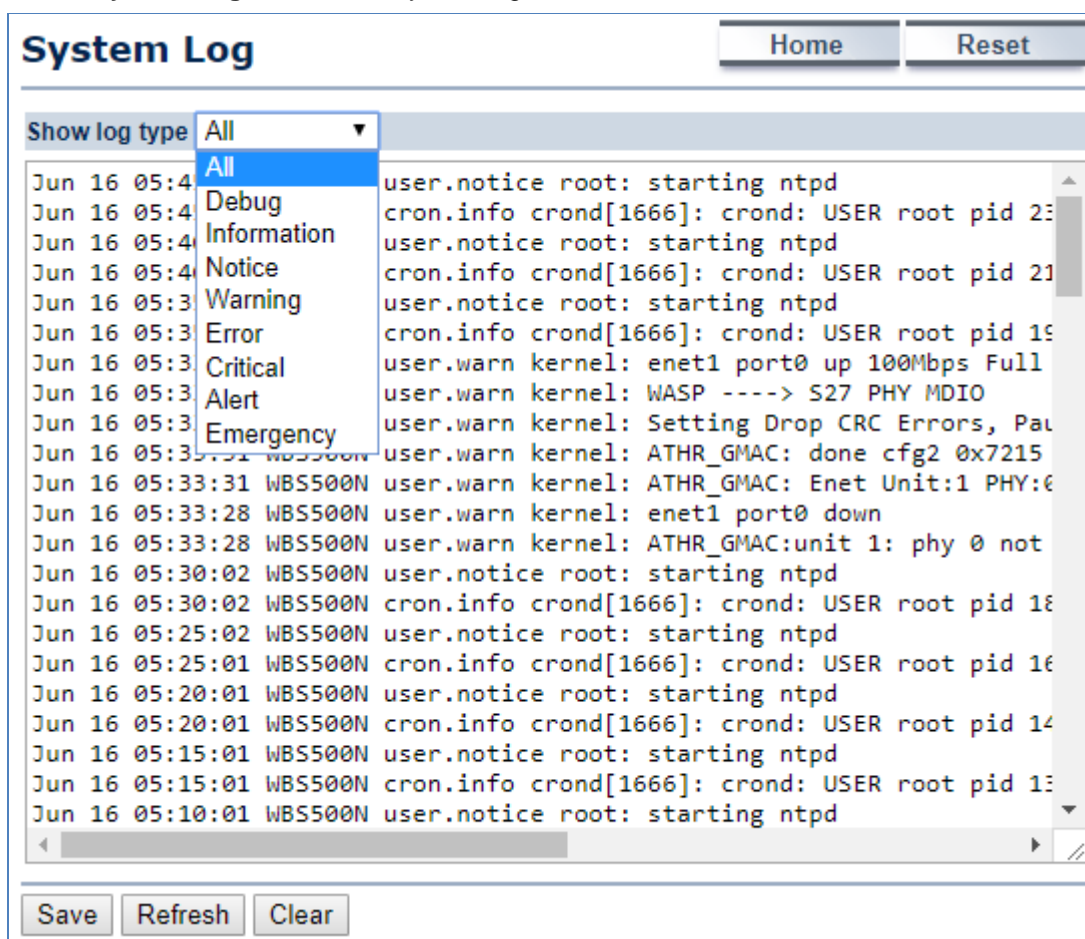


Figure 4-11 System Log

The page includes the following settings:

Object	Description
• Show log type	Select log type to filter the records.
• Save	Click Save to save the records.
• Refresh	Click Refresh to update the current data.
• Clear	Click Clear to erase the records.

4.3 System

4.3.1 IP Settings

Click "**System → IP Settings**" to configure the LAN IP address.

IP Settings Home Reset

System Information

IP Network Setting Obtain an IP address automatically (DHCP)
 Specify an IP address

IP Address . . .

IP Subnet Mask . . .

Default Gateway . . .

Primary DNS . . .

Secondary DNS . . .

Use Link-Local Address

IPv6 IP Address

IPv6 Subnet Prefix Length

IPv6 Default Gateway

IPv6 Primary DNS

IPv6 Secondary DNS

Accept Cancel

Figure 4-12 LAN IP Settings

The page includes the following settings:

Object	Description
• IP Network Setting	Select Obtain an IP address automatically (DHCP) to receive the IP from DHCP server. Select Specify an IP address to configure the AP to use static IP.

• IP Address	The LAN IP of the AP. The default is 192.168.1.253 . You can change it according to your needs.
• IP Subnet Mask	The LAN subnet mask of the AP.
• Default Gateway	Enter the Gateway IP address of the AP.
• Primary DNS	Enter the primary DNS server of the AP.
• Secondary DNS	Enter the secondary DNS server of the AP.
• Use Link-Local Address	Click to enable a link-local address for the AP.
• IPv6 IP Address	Enter the IPv6 LAN IP of the AP.
• IPv6 Subnet Prefix Length	Enter the secondary DNS server of the AP.
• IPv6 Default Gateway	Enter the IPv6 Gateway IP address of the AP.
• IPv6 Primary DNS	Enter the IPv6 primary DNS server of the AP.
• IPv6 Secondary DNS	Enter the IPv6 secondary DNS server of the AP.
• Accept	Click Accept to apply the new settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

4.3.2 Spanning Tree Settings

The Spanning Tree Protocol (STP) allows network to provide a redundant link in the event of a link failure. It is advised to turn on this option for multi-point bridge network to avoid network loop.

Click "**System → Spanning Tree Settings**" to enable/disable Spanning Tree Settings.

Spanning Tree Settings ⓘ		Home	Reset
Spanning Tree Status	<input type="radio"/> ON <input checked="" type="radio"/> OFF		
Bridge Hello Time	2	seconds	(1-10)
Bridge Max Age	20	seconds	(6-40)
Bridge Forward Delay	4	seconds	(4-30)
Priority	32768		(0-65535)
<input type="button" value="Accept"/> <input type="button" value="Cancel"/>			

Figure 4-13 Spanning Tree Settings

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> Spanning Tree Status 	Click ON to enable or click OFF to disable the option.
<ul style="list-style-type: none"> Bridge Hello Time 	Specify Bridge Hello Time in seconds. This value determines how often the AP sends hello packets to communicate information about the topology throughout the entire Bridged Local Area Network.
<ul style="list-style-type: none"> Bridge Max Age 	Specify Bridge Max Age in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be dead.
<ul style="list-style-type: none"> Bridge Forward Delay 	Specify Bridge Forward Delay in seconds. Forwarding delay time is the time spent in each of the Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it looks at some traffic before participating.
<ul style="list-style-type: none"> Priority 	Specify the Priority number. Smaller numbers have greater priority.
<ul style="list-style-type: none"> Accept 	Click Accept to apply the setting.
<ul style="list-style-type: none"> Cancel 	Click Cancel to cancel the setting.

4.4 Router (WISP Mode Only)

4.4.1 DHCP Server Settings

Go to the “**Operation Mode**” page to configure the device as “**WISP**” and then go to “**Router → LAN Settings**” to configure the device’s LAN IP settings.

On this page, enable the DHCP server to assign IP address to local wired/wireless clients after the device is connected to the remote AP supplied by wireless ISP.

LAN Settings

Home
Reset

LAN IP Setup

IP Address	192 . 168 . 1 . 253
IP Subnet Mask	255 . 255 . 255 . 0

Use Router As DHCP Server

Starting IP Address	192 . 168 . 1 . 100
Ending IP Address	192 . 168 . 1 . 200
WINS Server IP	0 . 0 . 0 . 0

Accept
Cancel

Figure 4-14 DHCP Server Settings

The page includes the following settings:

Object	Description
• IP Address	The LAN IP of the AP.
• IP Subnet Mask	The LAN subnet mask of the AP.
• Use Router As DHCP Server	Select it to enable DHCP server. In here the device is acting as a router.
• Starting IP Address	Specify the starting IP address for the DHCP range.
• Ending IP Address	Specify the ending IP address for the DHCP range.
• WINS Server IP	Enter the IP address of the WINS server.
• Accept	Click Accept to apply the setting.
• Cancel	Click Cancel to cancel the setting.

4.4.2 WAN Settings

Go to the “Operation Mode” page to configure the device as “WISP” and then go to “Router → WAN Settings” to configure the device’s WAN settings. The WAN settings should be provided by the ISP.

WAN Settings Home Reset

Internet Connection Type: DHCP

Options:

Account Name (if required):

Domain Name (if required):

MTU: Auto 1500 (576 - 1500)

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN:

Accept Cancel

Figure 4-15 WAN Settings – All

The page includes the following common settings in each Internet Connection Type:

Object	Description
<ul style="list-style-type: none"> Internet Connection Type 	<ul style="list-style-type: none"> DHCP: Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. Static IP: Setting a static IP address allows an administrator to set a specific IP address for the router and guarantees that it cannot be assigned a different address. PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet. PPTP: The Point-to-Point Tunneling Protocol (PPTP) is used in association with virtual private networks (VPNs).
<p>Option: This section may vary depending on the Internet Connection Type. Refer to settings of each corresponding section from 5.4.2.1 to 5.4.2.4</p>	
<p>Domain Name Server (DNS) Address</p>	
<ul style="list-style-type: none"> Get Automatically From ISP 	Select it to obtain the DNS automatically from the DHCP server.
<ul style="list-style-type: none"> Use These DNS Servers 	Select it to set up the Primary DNS and Secondary DNS servers manually.
<ul style="list-style-type: none"> Primary DNS 	Enter the primary DNS server address.
<ul style="list-style-type: none"> Secondary DNS 	Enter the secondary DNS server address.
<p>WAN Ping</p>	
<ul style="list-style-type: none"> Discard Ping on WAN 	Check it to enable pings on the WAN interface or disable to block pings on the WAN interface.
<ul style="list-style-type: none"> Accept 	Click Accept to apply the setting.
<ul style="list-style-type: none"> Cancel 	Click Cancel to cancel the setting.

4.4.2.1. DHCP

Select **DHCP** and the device will automatically obtain IP addresses, subnet masks and gateway addresses from the ISP.

Figure 4-16 WAN Settings – DHCP

The page includes the following specific settings in DHCP type:

Object	Description
<ul style="list-style-type: none"> Account Name (if required) 	Enter the account name provided by your ISP.
<ul style="list-style-type: none"> Domain Name (if required) 	Enter the domain name provided by your ISP.
<ul style="list-style-type: none"> MTU 	The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for DHCP is 1500. The MTU size can be set between 576 and 1500.
<ul style="list-style-type: none"> Accept 	Click Accept to apply the setting.
<ul style="list-style-type: none"> Cancel 	Click Cancel to cancel the setting.

4.4.2.2. Static IP

If your ISP offers you static IP Internet connection type, select **Static IP** and then enter IP address, subnet mask, primary DNS and secondary DNS information provided by ISP in the corresponding fields.

WAN Settings Home Reset

Internet Connection Type: Static IP ▼

Options

Account Name (if required):

Domain Name (if required):

MTU: Auto ▼ 1500 (576 - 1500)

Internet IP Address

IP Address: 192 . 168 . 10 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN:

Accept Cancel

Figure 4-17 WAN Settings – Static IP

The page includes the following specific settings in Static IP type:

Object	Description
• Account Name (if required)	Enter the account name provided by your ISP.
• Domain Name (if required)	Enter the domain name provided by your ISP.
• MTU	The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for static IP is 1500. The MTU size can be set between 576 and 1500.
• IP Address	Enter the device's WAN IP address provided by ISP.
• IP Subnet Mask	Enter the device's WAN IP subnet mask provided by ISP.
• Gateway IP Address	Enter the device's WAN Gateway IP provided by ISP.
• Accept	Click Accept to apply the setting.
• Cancel	Click Cancel to cancel the setting.

4.4.2.3. PPPoE

Select **PPPOE** if ISP is using a PPPoE connection and provide you with PPPoE user name and password.

WAN Settings Home Reset

Internet Connection Type: PPPoE

Options

MTU: Auto 1492 (576 - 1492)

PPPoE Options

Login: admin

Password: *****

Service Name (if required):

Connect on Demand: Max idle Time 1 Minutes

Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN:

Accept Cancel

Figure 4-18 WAN Settings – PPPOE

The page includes the following specific settings in PPPoE type:

Object	Description
• MTU	The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for PPPoE is 1492. The MTU size can be set between 576 and 1492.
• Login	Enter the username provided by ISP.
• Password	Enter the password provided by ISP.
• Service Name (if required)	Enter the service name of an ISP (optional).

<ul style="list-style-type: none">• Connect on Demand	Select it to specify the maximum idle time. Internet connection will disconnect when it reaches the maximum idle time, but it will automatically connect when user tries to access the network.
<ul style="list-style-type: none">• Keep Alive	Select whether to keep the Internet connection always on, or enter a redial period once the internet loses connection.
<ul style="list-style-type: none">• Accept	Click Accept to apply the setting.
<ul style="list-style-type: none">• Cancel	Click Cancel to cancel the setting.

4.4.2.4. PPTP

Select **PPTP** if ISP is using a PPTP connection.

WAN Settings Home Reset

Internet Connection Type: PPTP

Options

MTU: Auto (1200 - 1400)

PPTP Options

IP Address: 192 . 168 . 10 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

PPTP Server: 0 . 0 . 0 . 0

Username: admin

Password: ****

Connect on Demand: Max idle Time 15 Minutes

Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

WAN Ping

Discard Ping on WAN:

Accept Cancel

Figure 4-19 WAN Settings – PPTP

The page includes the following specific settings in PPTP type:

Object	Description
• MTU	The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for PPTP is 1400. The MTU size can be set between 1200 and 1400.
• IP Address	Enter the device's WAN IP address provided by ISP.

• Subnet Mask	Enter the device's WAN IP subnet mask provided by ISP.
• Default Gateway	Enter the device's WAN Gateway IP provided by ISP.
• PPTP Server	Enter the IP address of the PPTP server.
• Username	Enter the username provided by ISP.
• Password	Enter the password provided by ISP.
• Connect on Demand	Select it to specify the maximum idle time. Internet connection will disconnect when it reaches the maximum idle time, but it will automatically connect when user tries to access the network.
• Keep Alive	Select whether to keep the Internet connection always on, or enter a redial period once the internet loses connection.
• Accept	Click Accept to apply the setting.
• Cancel	Click Cancel to cancel the setting.

4.4.3 VPN Passthrough

VPN Passthrough allows a secure virtual private network (VPN) connection between two sites. Enabling the options on this page opens a VPN port and enables connections to pass through the AP without interruption.

Go to the “**Operation Mode**” page to configure the device as “**WISP**” and then go to “**Router → VPN Pass Through**” to enable VPN passthrough you required.

Figure 4-20 VPN Passthrough

The page includes the following settings:

Object	Description
• PPTP Passthrough	Check this option to enable PPTP pass-through mode.
• L2TP Passthrough	Check this option to enable L2TP pass-through mode.
• IPSec Passthrough	Check this option to enable IPSec pass-through mode.
• Accept	Click Accept to apply the setting.

<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the setting.
---	--

4.4.4 Port Forwarding

Go to the “**Operation Mode**” page to configure the device as “**WISP**” and then go to “**Router → Port Forwarding**” to enable VPN passthrough you required.

Figure 4-21 Port Forwarding

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • # 	Displays the sequence number of the forwarded port.
<ul style="list-style-type: none"> • Name 	Displays the name of the forwarded port.
<ul style="list-style-type: none"> • Protocol 	Displays the protocol to use for mapping from the following: TCP, UDP or Both.
<ul style="list-style-type: none"> • Start Port 	Displays the LAN port number that WAN client packets will be forward to.
<ul style="list-style-type: none"> • End Port 	Displays the port number that the WAN client packets are received.
<ul style="list-style-type: none"> • Server IP Address 	Displays the IP address of the server for the forwarded port.
<ul style="list-style-type: none"> • Enable 	Click to enable or disable the forwarded port profile.
<ul style="list-style-type: none"> • Modify 	Click to modify the forwarded port profile.
<ul style="list-style-type: none"> • Delete 	Click to delete the forwarded port profile.
<ul style="list-style-type: none"> • Add Entry 	Click Add Entry to add the new forwarding rule.
<ul style="list-style-type: none"> • Accept 	Click Accept to apply the setting.

When clicking **Add Entry**, the following window pops up and fill in the fields required to add a new forwarding rule.

Figure 4-22 Port Forwarding

The page includes the following settings:

Object	Description
• Service Name	Enter a name for the port forwarding rule.
• Protocol	Select a protocol for the application: Choices are TCP or UDP, or both.
• Starting Port (1~65535)	Enter a starting port number.
• Ending Port (1~65535)	Enter an ending port number. All ports numbers between the starting and ending ports will forward users to the IP address specified in the IP Address field.
• IP Address	Enter the IP address of the server computer on the LAN network where users will be redirected.
• Save	Click Save to save the new forwarding rule.
• Cancel	Click Cancel to cancel the setting.

4.4.5 DMZ Settings

The DMZ function allows the device to redirect all packets going to the WAN port IP address to a particular IP address on the LAN. The difference between the virtual server and the DMZ function is that a virtual server redirects a particular service or Internet application, such as FTP, to a particular LAN client or server, whereas a DMZ redirects all packets, regardless of the service, going to the WAN IP address to a particular LAN client or server.

Go to the “**Operation Mode**” page to configure the device as “**WISP**” and then go to “**Router → DMZ Settings**” to enable/configure DMZ.

DMZ Home Reset

DMZ Hosting

DMZ Address . . .

Accept Cancel

Figure 4-23 DMZ

The page includes the following settings:

Object	Description
• DMZ Hosting	Select Enable DMZ to activate DMZ functionality.
• DMZ Address	Enter an IP address of a device on the LAN.
• Accept	Click Accept to apply the setting.
• Cancel	Click Cancel to cancel the setting.

4.5 Wireless

In this section, wireless related settings in different operation modes are provided.

4.5.1 Wireless Network

Click “**Wireless** → **Wireless Network**” to configure the wireless basic settings. The wireless settings on this page may vary according to the selected operation mode.

Wireless Network

Home
Reset

Wireless Mode	802.11 A/N Mixed ▾
Channel HT Mode	20/40MHz ▾
Extension Channel	Upper Channel ▾
Channel / Frequency	Ch36-5.18GHz ▾ <input checked="" type="checkbox"/> Auto
AP Detection	Scan

Current Profiles

SSID	Security	Isolation <small> </small>	VID	Enable	Edit
PLANET1	None	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	Edit
PLANET2	None	<input type="checkbox"/>	2	<input type="checkbox"/>	Edit
PLANET3	None	<input type="checkbox"/>	3	<input type="checkbox"/>	Edit
PLANET4	None	<input type="checkbox"/>	4	<input type="checkbox"/>	Edit

Accept
Cancel

Figure 4-24 Wireless Network – AP/WDS AP Mode

In the AP/WDS AP mode, click the **Edit** button on the “**Wireless Network**” page to enter the “**SSID Profile**” page to configure the SSID profile for the wireless network.

SSID Profile

Wireless Setting

SSID	<input type="text" value="PLANET1"/>	(1 to 32 characters)
VLAN ID	<input type="text" value="1"/>	(1~4094)
Suppressed SSID	<input type="checkbox"/>	
Station Separation ?	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Wireless Security

Security Mode	<input type="text" value="Disabled"/>
---------------	---------------------------------------

Figure 4-25 Wireless Network – SSID Profile

The page includes the following settings:

Object	Description
• Wireless Mode	Wireless mode supports 802.11a/n mixed modes.
• Channel HT Mode	The default channel bandwidth is 20/40MHz. The larger the channel, the better the transmission quality and speed.
• Extension Channel	Select upper or lower channel. Your selection may affect the Auto channel function.
• Channel / Frequency	Select the channel and frequency that apply to your country's regulations.
• Auto	Check this option to enable auto-channel selection.
• AP Detection	AP Detection can select the best channel to use by scanning nearby areas for Access Points.
• Current Profile	Configure up to four different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click Edit to configure the profile and check whether you want to enable extra SSIDs.
SSID Profile	
• SSID	Specify the SSID for the current profile.
• VLAN ID	Specify the VLAN tag for the current profile.
• Suppressed SSID	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
• Station Separation	Click the appropriate radio button to allow or prevent communication between client devices.
• Wireless Security	Refer to section 5.5.3 Security Setting .
• Save	Click Save to save changes.

<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the unsaved changes and revert to the previous settings.
---	--

In the CB/WDS STA/CR/Repeater mode, select **Security Mode** on the “**Wireless Network**” page to configure the wireless security similar to the root AP’s security settings.

Figure 4-26 Wireless Network – CB/WDS STA/CR/Repeater Mode

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Wireless Mode 	Wireless mode supports 802.11a/n mixed modes.
<ul style="list-style-type: none"> • SSID 	Specify the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.
<ul style="list-style-type: none"> • Site Survey 	Scans nearby locations for Access Points. You can select a discovered Access Point to establish a connection.
<ul style="list-style-type: none"> • Prefer BSSID 	Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.
<ul style="list-style-type: none"> • Wireless Security 	Refer to section 5.5.3 Security Setting .
<ul style="list-style-type: none"> • Accept 	Click Accept to apply the setting.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the unsaved changes and revert to the previous settings.

4.5.2 WDS Link Settings

Go to the “**Operation Mode**” page to configure the device as “**WDS Bridge**” and then go to “**Wireless → WDS Link Settings**” to configure the WDS link settings.

WDS Link Settings

Home
Reset

Security	<input style="width: 90%;" type="text" value="AES"/>				
WEP Key	<input style="width: 95%;" type="text"/>				<input type="text" value="40/64-bit(10 hex digits)"/>
AES Passphrase	<input style="width: 95%;" type="text" value="12345678"/>				
	(8-63 ASCII characters or 64 hexadecimal digits)				

CAUTION: WDS was enabled, you need to assign Wifi Channel manually later.

ID	MAC Address	Mode
1	<input type="text" value="A8"/> : <input type="text" value="F7"/> : <input type="text" value="E0"/> : <input type="text" value="58"/> : <input type="text" value="1A"/> : <input type="text" value="94"/>	<input type="text" value="Enable"/>
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/>
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/>
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/>

Accept
Cancel

Figure 4-27 WDS Link Settings – WDS Bridge Mode

The page includes the following settings:

Object	Description
• Security	Select the type of WDS security: None, WEP, or AES.
• WEP Key	Enter the WEP key if security is selected as WEP.
• AES Passphrase	Enter the AES passphrase if security is selected as AES.
• MAC Address	Enter the wireless MAC address of the AP to which you want to extend wireless connectivity.
• Mode	Select Disable or Enable to disable or enable WDS.
• Accept	Click Accept to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

**NOTE:**

1. The WDS link settings is only available in WDS Bridge mode and is communicating through wireless MAC address each other by using non-standard protocol which may not be compatible with other brands or models. Use the same model for full compatibility as required.
2. The security setting in each site of WDS link must be the same.
3. The wireless channel must be fixed and must be the same in each site of WDS link.

4.5.3 Security Settings

Go to the “**Wireless → Wireless Network**” page to configure the security settings.

In the AP/WDS AP mode, click the **Edit** button on the “**Wireless Network**” page to enter the “**SSID Profile**” page and configure the wireless security for the wireless network.

SSID Profile	
Wireless Setting	
SSID	PLANET1 (1 to 32 characters)
VLAN ID	1 (1~4094)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Security	
Security Mode	Disabled ▼
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 4-28 Security Settings – AP/WDS AP Mode

In the CB/WDS STA/CR/Repeater mode, select **Security Mode** on the “**Wireless Network**” page to configure the wireless security similar to the root AP’s security settings.

Figure 4-29 Security Settings – CB/WDS STA/CR/Repeater Mode

In the WDS Bridge mode, select **Security Mode** on the “WDS Link Settings” page to configure the wireless security settings. The security settings in each site of the WDS link must be configured to the same.

Figure 4-30 Security Settings – WDS Bridge Mode

The option includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Security Mode 	Select the suitable security mode from the drop-down list to encrypt the wireless network. The options include Disabled, WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed . The latest WPA2-PSK mode is strongly recommended.



1. The WEP and WPA/WPA2 with TKIP does not support in the 802.11n mode and these options are not available in the 802.11n mode.
2. In the 802.11a/n mixed mode, if the security is configured to WEP and WPA/WPA2 with TKIP, the connection mode/speed will be changed from 802.11n to 802.11a.

■ Disabled

Authentication is disabled and no password/key is required to connect to the access point.

■ WEP

WEP (Wired Equivalent Privacy) is a basic encryption. For a higher level of security consider using the WPA encryption.

Wireless Security	
Security Mode	WEP ▼
Auth Type	Open System ▼
Input Type	Hex ▼
Key Length	40/64-bit (10 hex digits or 5 ASCII char) ▼
	40/64-bit (10 hex digits or 5 ASCII char)
	104/128-bit (26 hex digits or 13 ASCII char)
	128/152-bit (32 hex digits or 16 ASCII char)
Default Key	
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 4-31 Security Settings – WEP

The security mode includes the following settings:

Object	Description
<ul style="list-style-type: none"> Security Mode 	Select WEP from the drop-down list to configure the wireless network using WEP encryption method.
<ul style="list-style-type: none"> Auth Type 	Select Open System or Shared.
<ul style="list-style-type: none"> Input Type 	Select an input type of Hex or ASCII.
<ul style="list-style-type: none"> Key Length 	Level of WEP encryption is applied to all WEP keys. Select a 64-/128-/152-bit password length. <ul style="list-style-type: none"> 40/64-bit: enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F and null key is not permitted) or 5 ASCII characters. 104/128-bit: enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F and null key is not permitted) or 13 ASCII characters. 128/152-bit: enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F and null key is not permitted) or 16 ASCII characters.
<ul style="list-style-type: none"> Default Key 	Select 1 – 4 to specify which of the four WEP keys the device uses as its default.

• Key1 – Key4	Specify a password for the security key index. For security, each typed character is masked by a dot.
• Save	Click Save to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

■ WPA-PSK

The screenshot shows the 'Wireless Security' configuration window. It contains the following fields and controls:

- Security Mode:** A dropdown menu set to 'WPA-PSK'.
- Encryption:** A dropdown menu set to 'Both(TKIP+AES)'.
- Passphrase:** A text input field containing '12345678'. Below the field, it specifies '(8 to 63 characters) or (64 Hexadecimal characters)'.
- Group Key Update Interval:** A text input field containing '3600', followed by the label 'seconds(30~3600, 0: disabled)'.
- Buttons:** 'Save' and 'Cancel' buttons are located at the bottom left of the window.

Figure 4-32 Security Settings – WPA-PSK

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA-PSK from the drop-down list to configure the wireless network using WPA-PSK encryption method.
• Encryption	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES. ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
• Passphrase	Specify the security password. For security, each typed character is masked by a dot.
• Group Key Update Interval	Specify how often, in seconds, the group key changes.
• Save	Click Save to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

■ WPA2-PSK

The latest WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.

Wireless Security	
Security Mode	WPA2-PSK ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 4-33 Security Settings – WPA2-PSK

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA2-PSK from the drop-down list to configure the wireless network using WPA2-PSK encryption method.
• Encryption	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES. ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
• Passphrase	Specify the security password. For security, each typed character is masked by a dot.
• Group Key Update Interval	Specify how often, in seconds, the group key changes.
• Save	Click Save to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

■ WPA-PSK Mixed

Wireless Security	
Security Mode	WPA-PSK Mixed ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 4-34 Security Settings – WPA-PSK Mixed

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA-PSK Mixed from the drop-down list to configure the wireless network using WPA-PSK Mixed encryption method.
• Encryption	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES. ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
• Passphrase	Specify the security password. For security, each typed character is masked by a dot.
• Group Key Update Interval	Specify how often, in seconds, the group key changes.
• Save	Click Save to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

■ WPA (WPA Enterprise)

Wireless Security

Security Mode	WPA
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable
Radius Accounting Server	. . .
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 Seconds(60~600)

Save
Cancel

Figure 4-35 Security Settings – WPA (WPA Enterprise)

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA from the drop-down list to configure the wireless network using WPA encryption method.
• Encryption	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES.

	<ul style="list-style-type: none"> ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
• Radius Server	Specify the IP address of the RADIUS server.
• Radius Port	Specify the port number that your RADIUS server uses for authentication. Default port is 1812.
• Radius Secret	Specify RADIUS secret furnished by the RADIUS server.
• Group Key Update Interval	Specify how often, in seconds, the group key changes.
• Radius Accounting	Select to enable or disable RADIUS accounting.
• Radius Accounting Server	Specify the IP address of the RADIUS accounting server.
• Radius Accounting Port	Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.
• Radius Accounting Secret	Specify RADIUS accounting secret furnished by the RADIUS server.
• Interim Accounting Interval	Specify the interim accounting interval (60 - 600 seconds).
• Save	Click Save to save the settings.
• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

■ **WPA2 (WPA2 Enterprise)**

Wireless Security

Security Mode	WPA2
Encryption	Both(TKIP+AES)
Radius Server	. . .
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 <small>seconds(30~3600, 0: disabled)</small>
Radius Accounting	Enable
Radius Accounting Server	. . .
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 <small>Seconds(60~600)</small>

Figure 4-36 Security Settings – WPA2 (WPA2 Enterprise)

The security mode includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Security Mode 	Select WPA2 from the drop-down list to configure the wireless network using WPA2 encryption method.
<ul style="list-style-type: none"> • Encryption 	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES. ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
<ul style="list-style-type: none"> • Radius Server 	Specify the IP address of the RADIUS server.
<ul style="list-style-type: none"> • Radius Port 	Specify the port number that your RADIUS server uses for authentication. Default port is 1812.
<ul style="list-style-type: none"> • Radius Secret 	Specify RADIUS secret furnished by the RADIUS server.
<ul style="list-style-type: none"> • Group Key Update Interval 	Specify how often, in seconds, the group key changes.
<ul style="list-style-type: none"> • Radius Accounting 	Select to enable or disable RADIUS accounting.
<ul style="list-style-type: none"> • Radius Accounting Server 	Specify the IP address of the RADIUS accounting server.
<ul style="list-style-type: none"> • Radius Accounting Port 	Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.
<ul style="list-style-type: none"> • Radius Accounting Secret 	Specify RADIUS accounting secret furnished by the RADIUS server.
<ul style="list-style-type: none"> • Interim Accounting Interval 	Specify the interim accounting interval (60 - 600 seconds).
<ul style="list-style-type: none"> • Save 	Click Save to save the settings.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the unsaved changes and revert to the previous settings.

WPA Mixed (WPA Mixed Enterprise)

Wireless Security	
Security Mode	WPA Mixed
Encryption	Both(TKIP+AES)
Radius Server	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Radius Port	1812
Radius Secret	<input type="text"/>
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable
Radius Accounting Server	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Radius Accounting Port	1813
Radius Accounting Secret	<input type="text"/>
Interim Accounting Interval	600 Seconds(60~600)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 4-37 Security Settings – WPA Mixed (WPA Mixed Enterprise)

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA Mixed from the drop-down list to configure the wireless network using WPA Mixed encryption method.
• Encryption	Select TKIP or AES, or both as the encryption type. <ul style="list-style-type: none"> ■ Both: uses TKIP and AES. ■ TKIP: automatic encryption with WPA-PSK; requires passphrase. ■ AES: automatic encryption with WPA2-PSK; requires passphrase.
• Radius Server	Specify the IP address of the RADIUS server.
• Radius Port	Specify the port number that your RADIUS server uses for authentication. Default port is 1812.
• Radius Secret	Specify RADIUS secret furnished by the RADIUS server.
• Group Key Update Interval	Specify how often, in seconds, the group key changes.
• Radius Accounting	Select to enable or disable RADIUS accounting.
• Radius Accounting Server	Specify the IP address of the RADIUS accounting server.
• Radius Accounting Port	Specify the port number that your RADIUS accounting server uses for authentication. Default port is 1813.
• Radius Accounting Secret	Specify RADIUS accounting secret furnished by the RADIUS server.

<ul style="list-style-type: none">• Interim Accounting Interval	Specify the interim accounting interval (60 - 600 seconds).
<ul style="list-style-type: none">• Save	Click Save to save the settings.
<ul style="list-style-type: none">• Cancel	Click Cancel to cancel the unsaved changes and revert to the previous settings.

4.5.4 Wireless MAC Filter

Wireless MAC Filters are used to allow or deny network access to wireless clients according to their MAC addresses. You can manually add a MAC address to restrict the permission to access the device or refer to [section 5.2.3](#) to kick the associated client from the wireless client list.

Click "**Wireless** → **Wireless MAC Filter**" to configure the wireless access control settings.

The screenshot shows the 'Wireless MAC Filter' configuration interface. At the top, there are 'Home' and 'Reset' buttons. The 'ACL Mode' is set to 'Deny MAC in the List'. Below this, there is a form to add a new MAC address, consisting of six input fields for the hexadecimal digits and an 'Add' button. A table below the form lists existing entries. The table has three columns: '#', 'MAC Address', and a 'Delete' button. The first entry has the number '1' in the first column and the MAC address '00:30:4F:A8:FF:FF' in the second column. At the bottom of the page, there is an 'Accept' button.

Figure 4-38 Wireless MAC Filter

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • ACL Mode 	Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. The option includes Disable, Deny MAC in the list, or Allow MAC in the list.
<ul style="list-style-type: none"> • Add 	Enter the wireless MAC address of the client in front of the Add button and then click Add to add the new entry to the MAC filtering list.
<ul style="list-style-type: none"> • # 	Displays the sequence number of the entries.
<ul style="list-style-type: none"> • MAC Address 	Displays the MAC Address that will be denied/allowed access to this device.
<ul style="list-style-type: none"> • Delete 	Click Delete to remove the entry from the list.
<ul style="list-style-type: none"> • Accept 	Click Accept to apply the setting.

4.5.5 Wireless Advanced Settings

Click “Wireless → Wireless Advanced Settings” to configure the wireless advanced settings.

This section allows you to configure the wireless related settings to optimize the wireless network.

Wireless Advanced Settings

Home
Reset

Data Rate	<input type="text" value="Auto"/>
Transmit Power	<input type="text" value="Auto"/>
RTS/CTS Threshold (1 - 2346)	<input type="text" value="2346"/> Bytes
Distance (1-30km)	<input type="text" value="1"/> km (0.6 miles) <div style="border: 1px solid gray; width: 100%; height: 10px; margin-top: 2px;"></div>
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="text" value="32"/> Frames <input type="text" value="50000"/> Bytes(Max)

Wireless Traffic Shaping

Enable Traffic Shaping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Upload Limit	<input type="text" value="1000"/> kbit/s (512-99999999)
Download Limit	<input type="text" value="180000"/> kbit/s (512-99999999)

Client Limit

Frequency	Enable	Max Client
2.4G	<input checked="" type="checkbox"/>	<input type="text" value="64"/>

Accept
Cancel

Figure 4-39 Wireless Advanced Settings

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Data Rate 	Select a data rate from the drop-down list. The data rate affects throughput. If you select a low data rate value, for example, the throughput is reduced but the transmission distance increases. The default is “Auto”.
<ul style="list-style-type: none"> • Transmit Power 	The transmission power of the device (value: auto). To meet the regional regulation, this option is not allowed to be configured through the user interface.
<ul style="list-style-type: none"> • RTS/CTS Threshold 	When the length of a data packet exceeds this value, the device will send an RTS frame to the destination wireless node, and the latter will reply with a CTS frame, and thus they are ready to communicate. The default value is 2346. A small number causes RTS/CTS packets to be sent more

	often and consumes more bandwidth.
• Distance	Specify the distance between the master AP and slave AP. Longer distances may drop high-speed connections.
• Aggregation	A part of the 802.11n standard that allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source, destination end points, and traffic class (QoS) into one large frame with a common MAC header. This option reduces the number of packets, but increases packet sizes.

Wireless Traffic Shaping

• Enable Traffic Shaping	Enable or disable the regulation of packet flow leaving an interface for improved QoS.
• Incoming Traffic Limit	Specify the wireless transmission speed used for downloading.
• Outgoing Traffic Limit	Specify the wireless transmission speed used for uploading.
• Total Percentage	Specify the total percentage of the wireless traffic that is shaped.
• SSID1 to SSID4	Specify the percentage of the wireless traffic that is shaped for a specific SSID.

Client Limit: This option is only available in AP and WDS AP modes.

• Frequency	Display the frequency of the device's radio interface.
• Enable	Click to enable the client limit function.
• Max Client	Specify the maximum clients allowed to connect to the radio interface.
• Accept	Click Accept to apply all changes.
• Cancel	Click Cancel to cancel the settings.

4.6 Management

On this page, you can configure the system settings for management purpose, including Management VLAN settings, Time settings, Password settings, SNMP settings, CLI settings, Wi-Fi schedule, Firmware upgrade, Configuration backup and restore, Factory default, and Auto reboot.

4.6.1 Administration (Password Settings)

Click “Management → Administration” to configure username and password of the login account.

Figure 4-40 Administration (Password Settings)

The page includes the following settings:

Object	Description
• New Name	Enter a new username for logging in to the Web page.
• New Password	Enter a new password for logging in to the Web page.
• Confirm Password	Re-enter the new password for confirmation.
• Save/Apply	Click Save/Apply to apply all changes.
• Cancel	Click Cancel to cancel the settings.

4.6.2 Management VLAN

Click “Management → Management VLAN” to configure the management VLAN settings.

Figure 4-41 Management VLAN

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Management VLAN ID 	If your network includes VLANs and if tagged packets need to pass through the Access Point, enter the VLAN ID. Otherwise, select No VLAN tag .
<ul style="list-style-type: none"> • Accept 	Click Accept to apply the changes.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the settings.

4.6.3 SNMP Settings

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Click “**Management → SNMP Settings**” to configure SNMP settings.

SNMP Settings

Home
Reset

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read Write)	<input type="text" value="private"/>
Trap Destination Address	<input type="text"/>
Trap Destination Community Name	<input type="text" value="public"/>
SNMPv3	<input checked="" type="radio"/> v3Enable <input type="radio"/> v3Disable
User Name (1-31 Characters)	<input type="text" value="admin"/>
Auth Protocol	<input type="text" value="MD5"/>
Auth Key (8-32 Characters)	<input type="text" value="12345678"/>
Priv Protocol	<input type="text" value="DES"/>
Priv Key (8-32 Characters)	<input type="text" value="12345678"/>
Engine ID	<input type="text"/>

Save/Apply
Cancel

Figure 4-42 SNMP Settings

The page includes the following settings:

Object	Description
• SNMP	Enable or disable the SNMP service.
• Contact	Enter the contact details of the device.
• Location	Enter the location of the device.
• Community Name (Read Only)	Enter the password for accessing the SNMP community for read-only access.
• Community Name (Read/Write)	Enter the password for accessing the SNMP community for read and write access.
• Trap Destination Address	Enter the IP address where SNMP traps are to be sent.
• Trap Destination Community Name	Enter the password of the SNMP trap community.
• SNMPv3	Enable or Disable the SNMPv3 feature.
• User Name	Specify the username for SNMPv3.
• Auth Protocol	Select the authentication protocol type: MD5 or SHA.
• Auth Key (8-32 Characters)	Specify the authentication key for authentication.
• Priv Protocol	Select the privacy protocol type: DES.
• Priv Key (8-32 Characters)	Specify the privacy key for privacy.
• Engine ID	Specify the engine ID for SNMPv3.
• Save/Apply	Click Save/Apply to apply all changes.
• Cancel	Click Cancel to cancel the settings.

4.6.4 Backup/Restore Settings

Click "**Management → Backup/Restore Settings**" and the following page will be displayed.

The screenshot shows the 'Backup/Restore Settings' interface. At the top right, there are 'Home' and 'Reset' buttons. The main content area is divided into three sections:

- Save A Copy of Current Settings:** A light blue bar containing a 'Backup' button.
- Restore Saved Settings from A File:** A light blue bar containing a 'Choose File' button (which displays 'No file chosen'), and a 'Restore' button.
- Revert to Factory Default Settings:** A light blue bar containing a 'Factory Default' button.

Figure 4-43 Backup/Restore Settings

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Save A Copy of Current Settings 	Click Backup to save the current configured settings.
<ul style="list-style-type: none"> • Restore Saved Settings from A File 	To restore settings that have been previously backed up, click Choose File to select the file, and click Restore .
<ul style="list-style-type: none"> • Revert to Factory Default Settings 	Click Factory Default to restore the device to its factory default settings.

4.6.5 Auto Reboot Settings

Click “**Management → Auto Reboot Settings**” and the following page will be displayed.

This page allows you to enable and configure system auto reboot interval. The device can regularly reboot according to the frequency in different time formats of interval.

Figure 4-44 Auto Reboot Settings

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Auto Reboot Settings 	Select Enable from the drop-down menu to set up this function.
<ul style="list-style-type: none"> • Frequency of Auto Reboot 	Select the frequency interval using the drop-down menu. The interval supported is in different time formats: <ul style="list-style-type: none"> • Min: 10/20/30/40/50/60 mins • Hour: 1~24 hours • Day: 1~31 days • Week: 1~5 weeks
<ul style="list-style-type: none"> • Save/Apply 	Click Save/Apply to apply all changes.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the settings.

4.6.6 Firmware Upgrade

Click “**Management → Firmware Upgrade**” to upgrade the device’s firmware.

Firmware Upgrade Home Reset

Current Firmware Version: 1.0.0

Locate and select the upgrade file from your hard disk:

Choose File No file chosen

Upload

Figure 4-45 Firmware Upgrade

The page includes the following settings:

Object	Description
• Current Firmware Version	Click ON to enable or click OFF to disable the option.
• Choose File	Click Choose File to locate and select the upgrade file from your local hard disk.
• Upload	Click Upload to upgrade the firmware.

Firmware Upgrade Procedure

The following procedure will guide you to how to upgrade the firmware.

Step 1. Click the **Choose File** button to locate the firmware file path. Then, click the **Upload** button.

Step 2. The firmware checksum information appears to help you confirm whether the file is correct. Once confirmed, click the **Upgrade** button to begin the upgrade process.

Firmware Upgrade Home Reset

Uploaded Firmware Information:
checksum:ff0583a58fe42000e2a54764f19e6f73
filesize:6264449

Upgrade

Step 3. Wait for the process until it is finished.

Firmware Upgrade

Home
Reset

Uploaded Firmware Information:
checksum:ff0583a58fe42000e2a54764f19e6f73
filesize:6264449

Upgrade

Note: This (upgrading) process will take about 1 minute. Please wait...

44 %

Step 4. When the upgrade is finished, the system will auto reboot and you can click the hyperlink “[Click here when AP is ready](#)” after the system restarts.

Firmware Upgrade

Firmware is upgraded successfully.
The system is restarting, please wait...94

Click here when AP is ready

4.6.7 Time Settings

Click “**Management → Time Settings**” to configure time zone and NTP server settings to be in sync with the device’s time.

Time Settings

Home
Reset

Time

Manually Set Date and Time
2017 / 04 / 26 09 : 52 Synchronize with PC

Automatically Get Date and Time
Time Zone: UTC+00:00 Gambia, Liberia, Morocco ▼
 User defined NTP Server: 209.81.9.7

Enable Daylight Saving
Start Time: January ▼ 1st ▼ Sun ▼ 12 am ▼
End Time: January ▼ 1st ▼ Mon ▼ 12 am ▼

Save/Apply
Cancel

Figure 4-46 Time Settings

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Manually Set Date and Time 	Enter the date and time values in the date and time fields or click the Synchronize with PC to get the date and time values from the administrator's PC.
<ul style="list-style-type: none"> • Automatically Get Date and Time 	Select a time zone from the drop-down list and check whether you want to enter the IP address of an NTP server or use the default NTP server.
<ul style="list-style-type: none"> • Enable Daylight Saving 	Click to enable or disable daylight savings time. Select the start and stop times from the Start Time and Stop Time drop-down lists.
<ul style="list-style-type: none"> • Save/Apply 	Click Save/Apply to apply all changes.
<ul style="list-style-type: none"> • Cancel 	Click Cancel to cancel the settings.

4.6.8 Wi-Fi Schedule

This page allows you to configure wireless schedule. The device can regularly enable/disable Wi-Fi function according to the pre-defined schedule rules.

Click "**Management → Auto Reboot Settings**" and the following page will be displayed.

Wifi Schedule

Home
Reset

Wifi Schedule
Disable ▾

Schedule Name

Service

 Wireless Power ON
 Wireless Power OFF

Day
Mon ▾

Time of day

 : **All Day (use 24-hour clock)**

Add
Cancel

Schedule Table

#	Name	Service	Schedule	Select
Delete Selected Delete All Reset				

Accept
Cancel

Figure 4-47 Wi-Fi Schedule

The page includes the following settings:

Object	Description
• Schedule Name	Enter the description of the schedule service.
• Service	Select the type of schedule service, either Wireless Power ON or Wireless Power OFF.
• Day	Select the days of the week to enable the schedule service.
• Time of Day	Set the start time that the service is active.
• Add	Click Add to append the schedule service to the schedule service table
• Cancel	Click Cancel to discard changes.

4.6.9 CLI Settings

The command line interface (CLI) allows user to access the device through a command console, modem or Telnet connection for configuration.

Click "**Management → CLI Settings**" to enable/disable CLI.

Figure 4-48 CLI Settings

The page includes the following settings:

Object	Description
• CLI	Select ON/OFF to enable or disable the ability to modify the device via a command line interface.
• Save/Apply	Click Save/Apply to apply all changes.
• Cancel	Click Cancel to cancel the settings.

4.6.10 Log

Click “**Management → Log**” to enable/disable system log.

Figure 4-49 Log

The page includes the following settings:

Object	Description
• Syslog	Enable or disable the syslog function.
• Log Server IP Address	Enter the IP address of the log server.
• Local Log	Enable or disable the local log service.
• Save/Apply	Click Save/Apply to apply all changes.
• Cancel	Click Cancel to cancel the settings.

4.6.11 Diagnostics

Click “**Management → Diagnostics**” to test the connection and performance through the built-in diagnostics utilities.

Diagnostics

Home
Reset

Ping Test Parameters

Target IP / Domain Name	<input style="width: 90%;" type="text"/>
Ping Packet Size	<input style="width: 40%;" type="text" value="64"/> Bytes
Number of Pings	<input style="width: 40%;" type="text" value="4"/>

Traceroute Test Parameters ?

Traceroute target	<input style="width: 90%;" type="text"/>
-------------------	--

Speed Test

Target Address	<input style="width: 90%;" type="text"/>
Time Period	<input style="width: 40%;" type="text" value="20"/> Sec
Check Interval	<input style="width: 40%;" type="text" value="5"/> Sec
IPv4 Port	5001
IPv6 Port	5002

Figure 4-50 Diagnostics

The page includes the following settings:

Object	Description
• Target IP / Domain Name	Enter the IP address you would like to search.
• Ping Packet Size	Enter the packet size of each ping.
• Number of Pings	Enter the number of times you want to ping.
• Start Ping	Click Start Ping to begin pinging.
• Trace route target	Enter an IP address or domain name you want to trace.
• Start Traceroute	Click Start Traceroute to begin the traceroute operation.
• Target Address	Enter the IP address of the target PC.
• Time period	Enter time period for the speed test.
• Check Interval	Enter the interval for the speed test.
• Start Speed Test	Click Start Speed Test to begin the speed test operation.
• IPv4 Port	Displays the IPv4 port number of the device.

• IPv6 Port	Displays the IPv6 port number of the device.
--------------------	--

4.6.12 Logout

Click "**Management → Logout**" to log out the system.

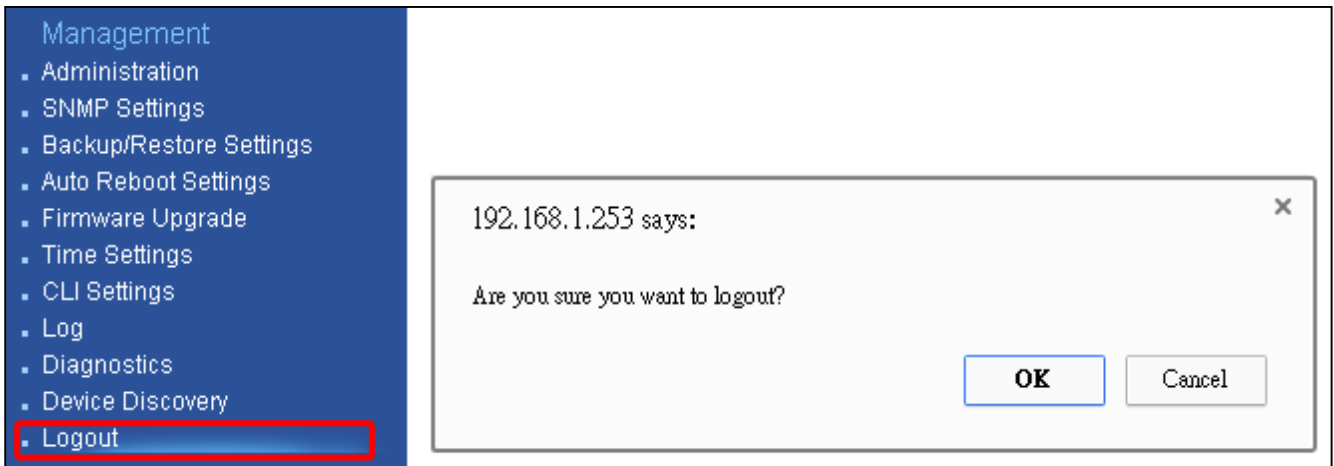


Figure 4-51 Logout

The page includes the following settings:

Object	Description
• OK	Click OK to log out the system.
• Cancel	Click Cancel to cancel the operation.

Appendix A: Troubleshooting

If you find the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the Planet Tech Support 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.	<ol style="list-style-type: none"> 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 to the AP. If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered. You must use the same IP address section that AP uses. 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 (Press the 'reset' button for over 10 seconds). Set your computer to static IP address, and see if the Planet Smart Discovery can find the AP or not. If you did a firmware upgrade and this happens, contact the Planet Tech Support for help. If all the solutions above don't work, contact the Planet Tech Support for help.
I can't get connected to the Internet.	<ol style="list-style-type: none"> Check the Internet connection status from the router that is connected with the AP. Please be patient. Sometimes Internet is just that slow. If you have 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. Check PPPoE / L2TP / PPTP user ID and password in your router again. Call your Internet service provider and check if there's something wrong with their service. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. Try to reset the AP and try again later. Reset the device provided by your Internet service provider. Try to use IP address instead of hostname. If you can use IP address to communicate with a remote server, but can't use hostname, please check DNS setting.
I can't locate my AP by my wireless device.	<ol style="list-style-type: none"> 'Broadcast ESSID' set to off? The antenna is properly secured.

	<ul style="list-style-type: none"> 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.
<p>File downloading is very slow or breaks frequently.</p>	<ul style="list-style-type: none"> a. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes; try to be patient. c. Try to reset the AP and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. e. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
<p>I can't log into the web management interface; the password is wrong.</p>	<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.
<p>The AP becomes hot.</p>	<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 A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer for help.

Appendix B: Use Planet Smart Discovery to find AP

To easily discover the WAP-500N/WBS-500N in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution. The utility is available at: http://www.planet.com.tw/en/product/images/48590/Planet_Utility.zip

The following instructions will guide you to how to use the Planet Smart Discovery Utility.

Step 1. Deposit the **Planet Smart Discovery Utility** in administrator PC.

Step 2. Execute this utility.



Step 3. Click the “**Refresh**” button as shown below to update the list of the currently connected devices.

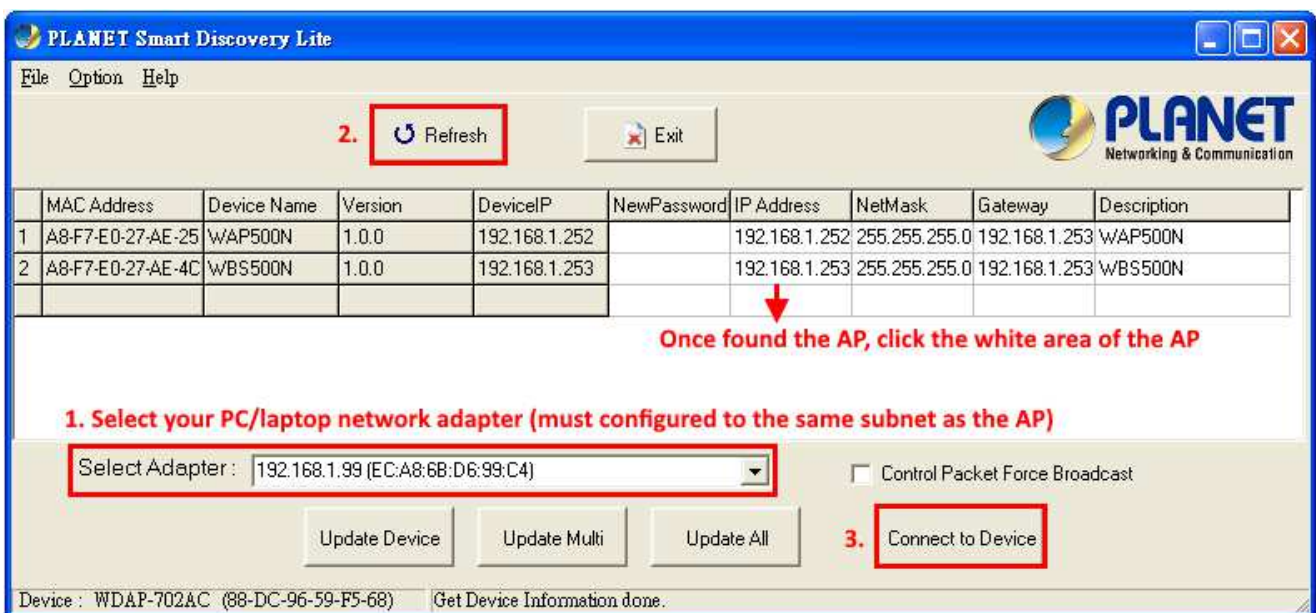


Figure B-1 PLANET Smart Discovery

Step 4. Select the AP from the list and then click the “**Connect to Device**” button to link to the Web Management Configuration Page.



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

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation , declares that this 300Mbps 802.11n Wireless AP/CPE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	Lietuviškai	Šiuo PLANET Technology Corporation , skelbia, kad 300Mbps 802.11n Wireless AP/CPE tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation , tímto prohlašuje, že tato 300Mbps 802.11n Wireless AP/CPE splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	Magyar	A gyártó PLANET Technology Corporation , kijelenti, hogy ez a 300Mbps 802.11n Wireless AP/CPE megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation , erklærer herved, at følgende udstyr 300Mbps 802.11n Wireless AP/CPE overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	Malti	Hawnhekk, PLANET Technology Corporation , jiddikjara li dan 300Mbps 802.11n Wireless AP/CPE jikkonforma mal-htiġijiet essenzjali u ma provvediment i oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt PLANET Technology Corporation , dass sich dieses Gerät 300Mbps 802.11n Wireless AP/CPE in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW i)	Nederlands	Hierbij verklaart, PLANET Technology Corporation , dat 300Mbps 802.11n Wireless AP/CPE in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eestikeeles	Käesolevaga kinnitab PLANET Technology Corporation , et see 300Mbps 802.11n Wireless AP/CPE vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation , oświadcza, że 300Mbps 802.11n Wireless AP/CPE spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC”.
Ελληνικά	<i>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ, PLANET Technology Corporation, ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ 300Mbps 802.11n Wireless AP/CPE ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK</i>	Português	PLANET Technology Corporation , declara que este 300Mbps 802.11n Wireless AP/CPE está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, PLANET Technology Corporation , declara que 300Mbps 802.11n Wireless AP/CPE cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	Slovensky	Výrobca PLANET Technology Corporation , týmto deklaruje, že táto 300Mbps 802.11n Wireless AP/CPE je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, PLANET Technology Corporation , déclare que les appareils du 300Mbps 802.11n Wireless AP/CPE sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	Slovensko	PLANET Technology Corporation , s tem potrjuje, da je ta 300Mbps 802.11n Wireless AP/CPE skladden/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente, PLANET Technology Corporation , dichiara che questo 300Mbps 802.11n Wireless AP/CPE è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	Suomi	PLANET Technology Corporation , vakuuttaa täten että 300Mbps 802.11n Wireless AP/CPE tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo PLANET Technology Corporation , apliecina, ka šī 300Mbps 802.11n Wireless AP/CPE atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation , att denna 300Mbps 802.11n Wireless AP/CPE står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

