

User's Manual

900Mbps 802.11ac Outdoor Wireless CPE

▶ **WBS-502AC**



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.

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 minimum distance **26cm** between the radiator & 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's Manual of PLANET 5GHz 900Mbps 802.11ac Outdoor Wireless CPE

Model: WBS-502AC

Rev: 1.0 (August, 2017)

Part No. EM-WBS-502AC_v1.0 (2081-E10680-000)

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	11
Chapter 2.Connecting to the AP	14
2.1 Preparation before Installation	14
2.1.1 Safety Precautions.....	14
2.2 Installation Precautions	14
2.3 Installing the AP	16
Chapter 3.Quick Installation Guide	18
3.1 Manual Network Setup -- TCP/IP Configuration	18
3.1.1 Configuring the IP Address Manually	18
3.2 Starting Setup in the Web UI	21
Chapter 4.Configuring the AP	23
4.1 Operation Mode	23
4.2 Overview	25
4.2.1 Device Status.....	25
4.2.2 Changes	27
4.2.3 Wireless Client List	27
4.2.4 WDS Link List	28
4.2.5 DHCP Client Table	29
4.2.6 Connection Status	29
4.3 Network	30
4.3.1 IP Settings.....	30
4.3.2 Spanning Tree Settings	32
4.4 Router (WISP Mode Only)	32
4.4.1 DHCP Server Settings	32
4.4.2 WAN Settings.....	33
4.4.2.1. DHCP.....	35
4.4.2.2. Static IP.....	35
4.4.2.3. PPPoE	36
4.4.2.4. PPTP	38
4.4.3 VPN Passthrough	39
4.4.4 Port Forwarding	39
4.4.5 DMZ Settings	41

4.4.6	Dos Protection	41
4.5	Wireless.....	42
4.5.1	Wireless Settings	42
4.5.2	WDS Link Settings.....	46
4.5.3	Security Settings.....	47
4.5.4	Wireless MAC Filter	56
4.5.5	Guest Network Settings.....	57
4.5.6	RSSI Threshold	57
4.5.7	Management VLAN	58
4.6	Management	60
4.6.1	Account (Password Settings)	60
4.6.2	SNMP Settings	60
4.6.3	CLI/SSH/HTTPS Settings.....	62
4.6.4	Email Alert.....	62
4.6.5	Backup/Restore Settings	63
4.6.6	WiFi Scheduler	64
4.6.6.1.	Auto Reboot Settings.....	64
4.6.6.2.	WiFi Scheduler.....	65
4.6.7	Firmware Upgrade	66
4.6.8	Time Settings	67
4.6.9	Log	69
4.6.10	Tools.....	69
4.6.11	Logout.....	71
Appendix A: Troubleshooting.....		72
Appendix B: Use Planet Smart Discovery to find AP		74

FIGURES

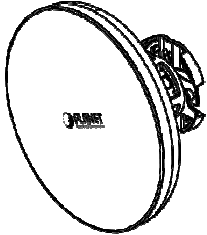
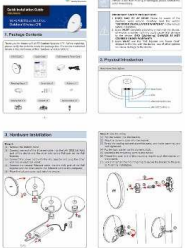
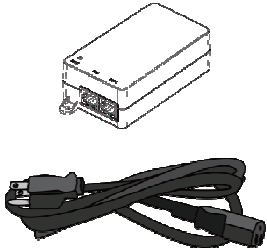
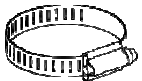
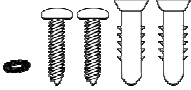


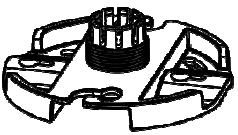

FIGURE 1-1 THREE-WAY VIEW	11
FIGURE 1-2 REAR PANEL	12
FIGURE 2-1 POE AND LAN PORT CONNECTION	16
FIGURE 2-2 FINISH INSTALLATION	16
FIGURE 2-3 POLE MOUNTING	17
FIGURE 2-4 WALL MOUNTING	17
FIGURE 3-1 TCP/IP SETTING	19
FIGURE 3-2 WINDOWS START MENU	20
FIGURE 3-3 SUCCESSFUL RESULT OF PING COMMAND	20
FIGURE 3-4 FAILED RESULT OF PING COMMAND	21
FIGURE 3-5 LOGIN BY DEFAULT IP ADDRESS	21
FIGURE 3-6 LOGIN WINDOW	21
FIGURE 3-7 WEB UI SCREENSHOT	22
FIGURE 4-1 WIRELESS – BASIC	23
FIGURE 4-2 SYSTEM MENU - RESET	25
FIGURE 4-3 SYSTEM MENU – LANGUAGE OPTION	25
FIGURE 4-4 MAIN STATUS	26
FIGURE 4-5 CHANGES	27
FIGURE 4-6 WIRELESS CLIENT LIST	28
FIGURE 4-7 WDS LINK STATUS	28
FIGURE 4-8 DHCP CLIENT LIST	29
FIGURE 4-9 CONNECTION STATUS	30
FIGURE 4-10 LAN IP SETTINGS	31
FIGURE 4-11 SPANNING TREE SETTINGS	32
FIGURE 4-12 DHCP SERVER SETTINGS	33
FIGURE 4-13 WAN SETTINGS – ALL	34
FIGURE 4-14 WAN SETTINGS – DHCP	35
FIGURE 4-15 WAN SETTINGS – STATIC IP	36
FIGURE 4-16 WAN SETTINGS – PPPoE	37
FIGURE 4-17 WAN SETTINGS – PPTP	38
FIGURE 4-18 VPN PASSTHROUGH	39
FIGURE 4-19 PORT FORWARDING	39
FIGURE 4-20 PORT FORWARDING	40
FIGURE 4-21 DMZ	41
FIGURE 4-22 DoS PROTECTION	42
FIGURE 4-23 WIRELESS SETTINGS – AP MODE	43
FIGURE 4-24 WIRELESS SETTINGS – WDS AP MODE	43
FIGURE 4-25 WIRELESS PROFILE – AP/WDS AP MODE	44
FIGURE 4-26 WIRELESS PROFILE – CB/WDS STA/CR MODE	45
FIGURE 4-27 WIRELESS SETTINGS – CB/WDS STA/CR MODE	46
FIGURE 4-28 WDS LINK SETTINGS – WDS AP MODE	46
FIGURE 4-29 WDS LINK SETTINGS – WDS BRIDGE MODE	47

FIGURE 4-30 SECURITY SETTINGS – AP/WDS AP MODE	48
FIGURE 4-31 SECURITY SETTINGS – CB/WDS STA/CR MODE	48
FIGURE 4-32 SECURITY SETTINGS – WDS BRIDGE MODE.....	49
FIGURE 4-33 SECURITY SETTINGS – WEP	50
FIGURE 4-34 SECURITY SETTINGS – WPA-PSK.....	50
FIGURE 4-35 SECURITY SETTINGS – WPA2-PSK.....	51
FIGURE 4-36 SECURITY SETTINGS – WPA-PSK MIXED.....	52
FIGURE 4-37 SECURITY SETTINGS – WPA (WPA ENTERPRISE).....	52
FIGURE 4-38 SECURITY SETTINGS – WPA2 (WPA2 ENTERPRISE)	53
FIGURE 4-39 SECURITY SETTINGS – WPA MIXED (WPA MIXED ENTERPRISE).....	55
FIGURE 4-40 WIRELESS MAC FILTER.....	56
FIGURE 4-41 WIRELESS - GUEST NETWORK SETTINGS	57
FIGURE 4-42 WIRELESS - RSSI THRESHOLD.....	58
FIGURE 4-43 WIRELESS – MANAGEMENT VLAN	58
FIGURE 4-44 ADMINISTRATION (PASSWORD SETTINGS).....	60
FIGURE 4-45 SNMP SETTINGS	61
FIGURE 4-46 CLI/SSH/HTTPS SETTINGS	62
FIGURE 4-47 EMAIL ALERT SETTINGS	63
FIGURE 4-48 BACKUP/RESTORE SETTINGS	64
FIGURE 4-49 AUTO REBOOT SETTINGS	65
FIGURE 4-50 WiFi SCHEDULER.....	65
FIGURE 4-51 FIRMWARE UPGRADE.....	66
FIGURE 4-52 TIME SETTINGS	68
FIGURE 4-53 SYSTEM LOG	69
FIGURE 4-54 TOOLS - PING.....	70
FIGURE 4-55 TOOLS - TRACEROUTE	70
FIGURE 4-56 TOOLS – SPEED TEST	71
FIGURE 4-57 LOGOUT.....	71

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WBS-502AC series. Before installing the CPE, please verify the contents inside the package box.

WBS-502AC	Quick Installation Guide	PoE Injector & Power Cord
		
Mounting Ring x 1	Screw Set x 1	Rubber x 1
		
Sealing Nut x 1	Bracket x 1	Dynamic Stick x 1
		

格式化: 間距 套用前: 0.5 行

格式化: 間距 套用前: 0.5 行

格式化: 間距 套用前: 0.5 行

格式化: 間距 套用前: 0.5 行

格式化: 間距 套用前: 0.5 行

格式化: 間距 套用前: 0.5 行



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

1.2 Product Description

Ultra-high-speed Enterprise Outdoor Wireless Solution

PLANET WBS-502AC 5GHz 900Mbps 802.11ac Outdoor Wireless CPE supports **IEEE 802.11ac** standard with 2T2R MIMO mechanism, which brings the latest wireless technology into outdoor infrastructure. The WBS-502AC supports standard **IEEE 802.3at Power over Ethernet (PoE)** and features **IEEE 802.3af PoE pass-through** going to the secondary LAN port, which is able to supply power to the PoE IP camera or other PoE PD equipment. With excellent performance and concentrated antenna beamwidth, the WBS-502AC is definitely ideal for long-distance outdoor surveillance.

Bringing Superior 11ac Performance to Outdoor

To provide extremely high-speed user experience, the WBS-502AC adopts IEEE 802.11ac technology to extend the 802.11n 40MHz channel binding to 80MHz and the implementation of 256-QAM modulation where higher transmitting/receiving rates go up to 867Mbps in 5GHz frequency band with less interference. Equipped with **Gigabit LAN** ports, the WBS-502AC allows 11ac wireless traffic to directly access high-speed connection without the bottleneck of 100Mbps uplink wired connection, thus offering a better range and superior throughput than those of the 802.11a/n wireless outdoor CPE.

Multiple SSIDs with VLAN Tagging

Multiple SSIDs can broadcast up to 8 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 or allows VLAN tags to pass through over WDS link. This makes it possible for the WBS-502AC to work with managed Ethernet switches to have VLAN assigned for a different access level and authority.

Value-added Outdoor Characteristics

The WBS-502AC is definitely suitable for wireless IP surveillance, and bridge link of building to building and backbone of public service. With standard IEEE 802.3at Power over Ethernet (PoE) design, the WBS-502AC can be powered by the remote PoE switch through the 100m Cat5e UTP cable and is able to supply power to the IP camera supporting IEEE 802.3af standard through the secondary LAN port. With the IP55-rated outdoor UV-resistant enclosure, the WBS-502AC can perform normally under rigorous weather conditions, meaning it can be installed in any harsh, outdoor environments.

Completely Secure Wireless Network

The WBS-502AC 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. To provide the secure Wi-Fi access for visitors, **Guest Network** feature allows you to create a temporary network with an individual SSID, security setting and DHCP settings to isolate the guest network to a separate network segment, thus preventing guests from being able to access files on intranet and also ensuring the guest's internet connectivity.

Deployment and Alignment within Minutes

In order to provide accurate antenna alignment, the WBS-502AC is equipped with a **360-degree** 3D array of mounting brackets, greatly reducing deployment effort to easily achieve high-performance backhaul links over long distance through the built-in higher gain antenna.

Smart Management Features Meeting High Expectations

With user-friendly Web UI and comprehensive management features like **RSSI threshold**, **Client Limit** Control and **Wireless Traffic Shaping**, the WBS-502AC is easy to limit the client access and control the bandwidth, 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 WBS-502AC is convenient to be managed remotely.

1.3 Product Features

- **Industrial Compliant Wireless LAN and LAN**
 - Compliant with the IEEE 802.11a/n/ac wireless technology
 - 2T2R architecture with data rate of up to 900Mbps
 - Equipped with two 10/100/1000Mbps RJ45 ports with auto MDI/MDI-X supported
 - IPv4 and IPv6 dual-stack management networks
- **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
 - Supports Guest Network in AP mode
- **RF Interface Characteristics**
 - Built-in dual-polarization antenna
 - High output power for outdoor usage

➤ **Outdoor Environmental Characteristics**

- IP55 rating
- IEEE 802.3at PoE design, IEEE 802.3af PoE pass-through going to the secondary LAN port
- 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 32 entries of MAC address filtering

➤ **Easy Deployment and Management**

- 360-degree 3D array of mounting brackets design
- Multilingual Web User Interface: English, Spanish, French, German, Portuguese, Russian, Simplified Chinese
- CLI command and SNMP-based management interface
- Supports SSH/HTTPS secure connection
- Self-healing mechanism through system auto reboot setting
- System status monitoring through remote Syslog Server and Device Discovery
- Diagnostic tools includes Ping, Traceroute, Speed
- Planet Smart Discovery Utility allows administrator to discover and locate each AP

1.4 Hardware Description

- Dimensions (Φ x H): 190 x 38mm

← 格式化: 間距 套用後: 0.5 行



Figure 1-1 Three-way View

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 1-2](#) shows the bottom panel of the WBS-502AC.

Bottom/Side Panel

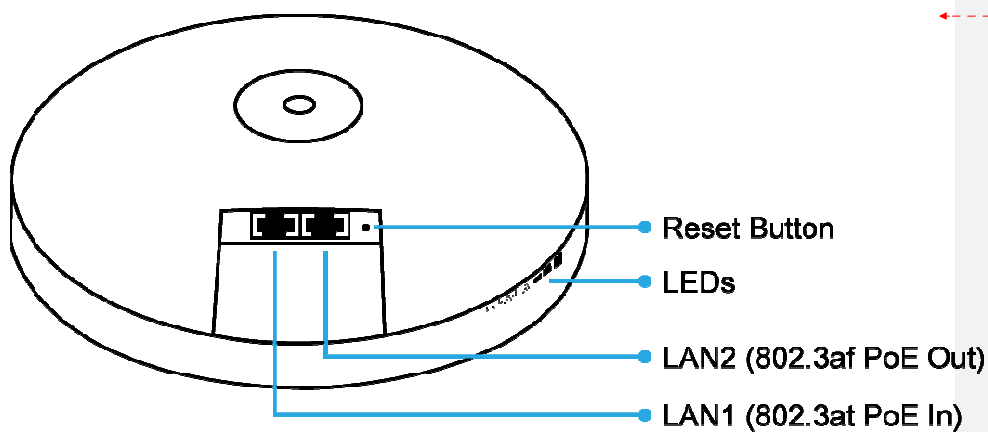


Figure 1-2 Rear Panel

格式化: 间距 套用後: 0.5 行

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)	Good	On	Signal is good
	Normal	On	Signal is normal
	Poor	On	Signal is poor

Table 2-1 The LED indication

Hardware Interface Definition

Object	Description
PoE LAN Port	10/100/1000Mbps RJ45 port, auto MDI/MDI-X IEEE 802.3at PoE PD supported, 54VDC In
LAN2 Port	10/100/1000Mbps RJ45 port, auto MDI/MDI-X, IEEE 802.3af PoE PSE
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

← 格式化: 间距 套用前: 0.2 行, 套用后: 0.2 行

← 格式化: 间距 套用前: 0.2 行, 套用后: 0.2 行

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-502AC for the first time, for your safety as well as others', please seek assistance from an 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-502AC, 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 arrester and grounding kit with the WBS-502AC; otherwise, a random lightning could easily cause fatal damage to the WBS-502AC. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
- Users **MUST** use the "Power cord and PoE Injector" shipped in the box with the WBS-502AC. Use of other options will cause damage to the WBS-502AC.

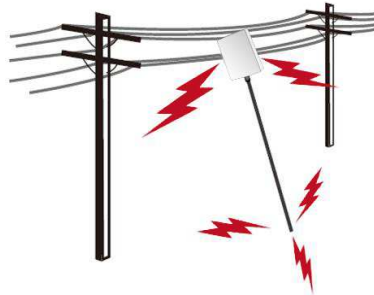


OUTDOOR INSTALLATION WARNING

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.

格式化: 間距 套用後: 0.5 行

格式化: 間距 套用後: 0.5 行

格式化: 間距 套用後: 0.5 行

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 (802.3at 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.
- (5) Place the bottom cover back into the device.

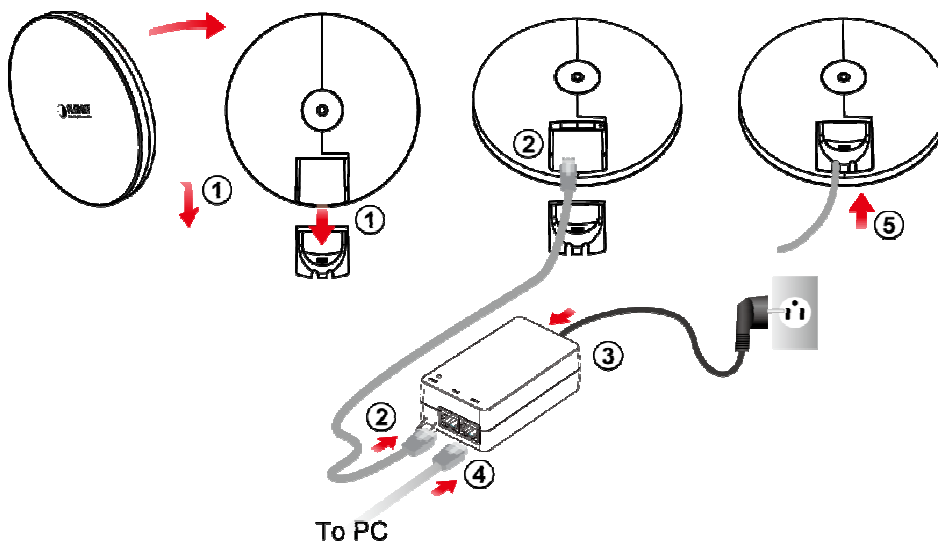


Figure 2-1 PoE and LAN port connection

Figure 2-2 Finish installation

Step 2. Pole Mounting:

- (1) Put the rubber into the bracket.
- (2) Plug the dynamic stick into the bracket.
- (3) Screw the sealing nut and assemble parts, and make sure they are well tightened.
- (4) Put the lock washer on the dynamic stick.
- (5) Assemble the mounting parts to the device.
- (6) Thread the open end of the mounting ring through the two tabs on the bracket.
- (7) Lock and tighten the mounting ring to secure the bracket to the pole to finish the installation.

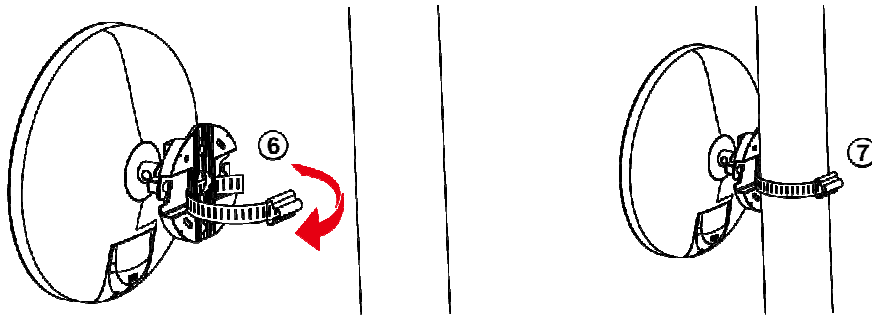


Figure 2-3 Pole Mounting

格式化: 间距 套用前: 0.5 行

格式化: 间距 套用前: 0.5 行

Step 4. Wall Mounting:

- (1) Put the rubber into the bracket.
- (2) Plug the dynamic stick into the bracket.
- (3) Screw the sealing nut and assemble parts, and make sure they are well tightened.
- (4) Put the lock washer on the dynamic stick.
- (5) Assemble the mounting parts to the device.
- (6) Mark and drill two pilot holes aligning to the screw holes of the bracket.
- (7) Put wall anchors into the holes and insert screw into the wall anchor.
- (8) Screw and secure the bracket in place to finish the installation.

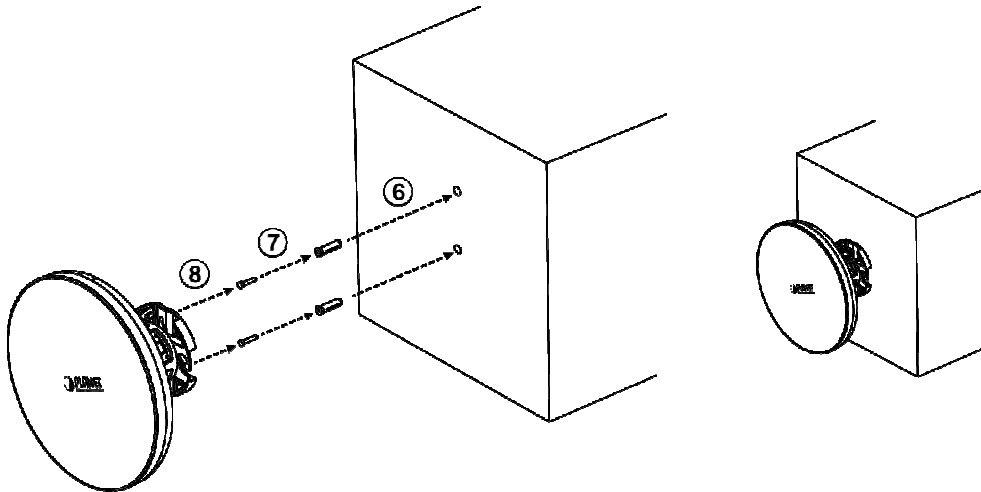


Figure 2-4 Wall Mounting

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-502AC 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-502AC 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-502AC 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

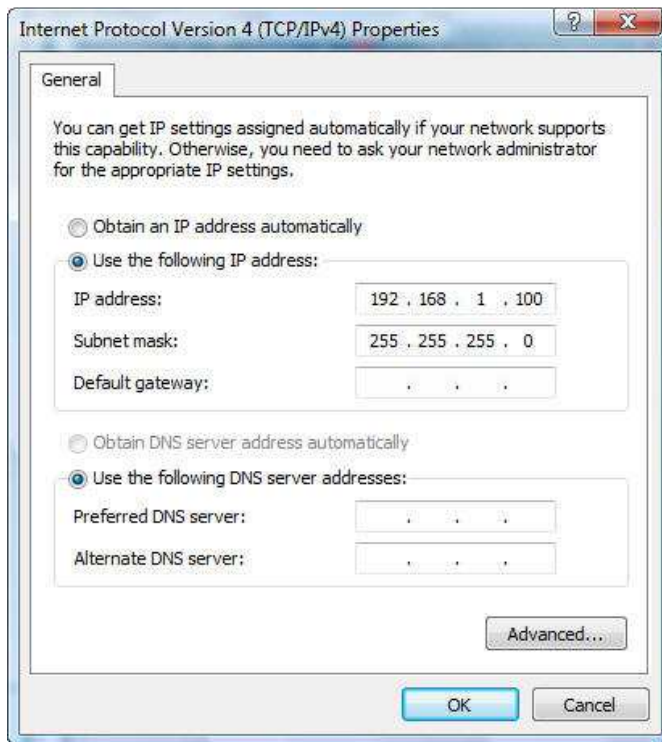


Figure 3-1 TCP/IP Setting

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.

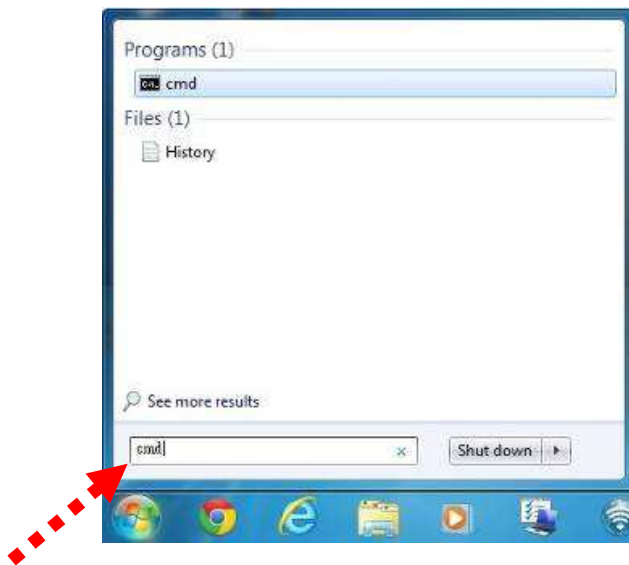


Figure 3-2 Windows Start Menu

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.

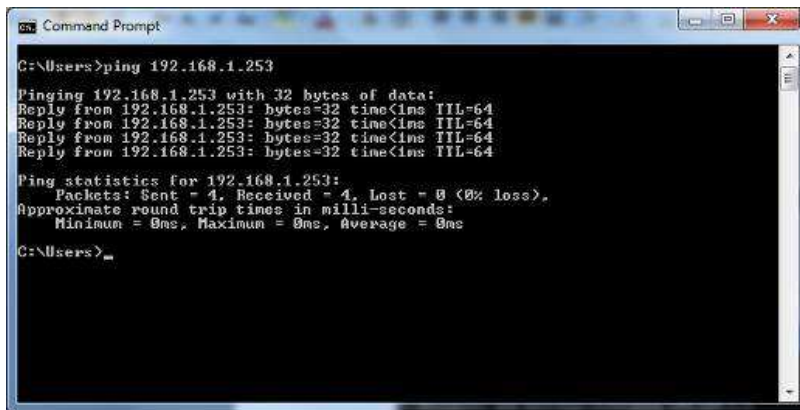


Figure 3-3 Successful result of Ping command

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

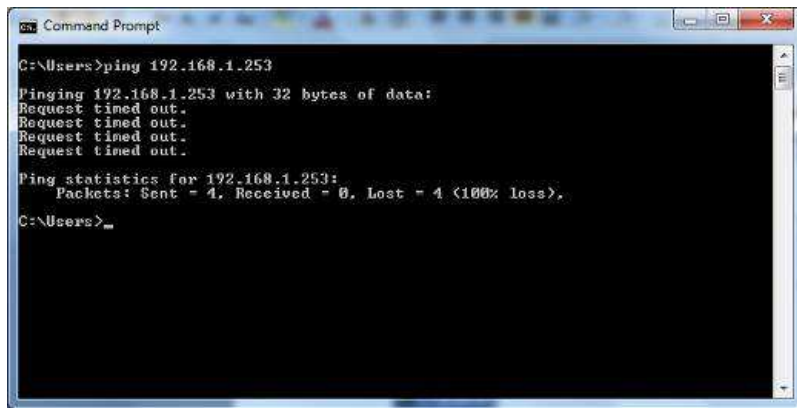


Figure 3-4 Failed result of Ping command

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-502AC 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.

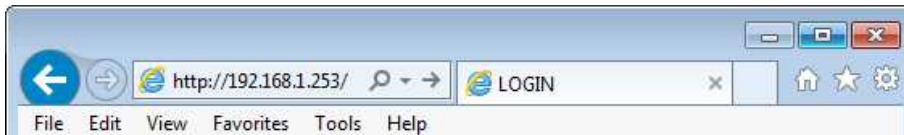


Figure 3-5 Login by default IP address

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**



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 **Wireless** 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 **Changes** page to save and apply the changes.



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 CPE in different operation modes.

4.1 Operation Mode

Go to the "Network → Wireless" page to configure the operation mode which is suitable to your application.

Wireless Settings	
Device Name	WBS502AC
	5GHz
Operation Mode	Access Point ▼
Wireless Mode	802.11 AC/N ▼
Channel HT Mode	80MHz(AC Only) ▼
Extension Channel	Lower Channel ▼
Channel	Auto ▼
Transmit Power	Auto ▼
Data Rate	Auto ▼
RTS / CTS Threshold (1 - 2346)	2346
Client Limit	127 <input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Detection	Scan
Distance (1-30km)	1 (0.6miles)

Figure 4-1 Wireless – Basic

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"> • Wireless Mode 	The wireless mode supports the following 5GHz modes: <ul style="list-style-type: none"> • 802.11AC/N mixed mode • 802.11A/N mixed mode • 802.11A • 802.11N (5GHz)
<ul style="list-style-type: none"> • Channel HT Mode 	The channel HT mode is the channel bandwidth and default is 80MHz (AC only). The larger the channel bandwidth, the better the transmission quality and speed. The Channel HT Mode includes: <ul style="list-style-type: none"> • 80MHz (AC only) • 40MHz

	<ul style="list-style-type: none"> ● 20MHz
<ul style="list-style-type: none"> ● Extension Channel 	Select upper or lower channel. Your selection may affect the Auto channel function.
<ul style="list-style-type: none"> ● Channel 	Select the appropriate channel and frequency. Select Auto to enable auto-channel selection.
<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"> ● 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"> ● RTS/CTS Threshold (1-2346) 	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.
<ul style="list-style-type: none"> ● Client Limit 	Specify the maximum clients allowed to connect to the radio interface.
<ul style="list-style-type: none"> ● AP Detection 	AP Detection can select the best channel to use by scanning nearby areas for Access Points.
<ul style="list-style-type: none"> ● Distance (1-30km) 	Specify the distance between the master AP and slave AP. Longer distances may drop high-speed connections.
<ul style="list-style-type: none"> ● Save 	Click Save to save changes.

4.2 Overview

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.

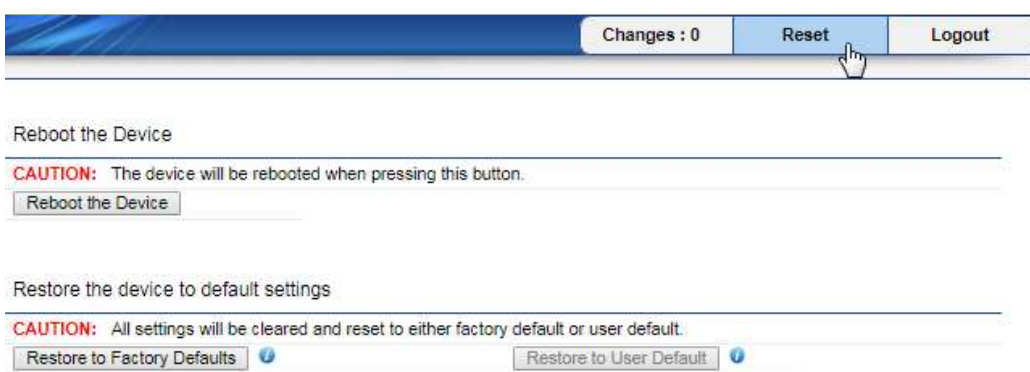


Figure 4-2 System Menu - Reset

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.

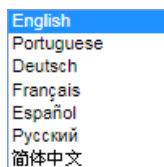


Figure 4-3 System Menu – Language option

4.2.1 Device Status

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

Device Information			
Device Name	WBS502AC		
MAC Address			
- LAN	A8:F7:E0:56:7C:87		
- Wireless WAN - 5GHz	A8:F7:E0:56:7C:89		
Country	USA		
Current Local Time	Tue Aug 8 08:50:44 UTC 2017		
Firmware Version	1.0.0		
Management VLAN ID	Untagged		
Wireless WAN Information - 5GHz			
Operation Mode	Client Router		
Wireless Mode	802.11 AC/N		
Channel Bandwidth	80 MHz		
Channel	5.745 GHz (Channel 149)		
Distance	1000 M		
WAN			
MAC Address	A8:F7:E0:56:7C:89		
Connection Type	DHCP		
Connection Status	UP		
IP Address	192.168.0.172		
IP Subnet Mask	255.255.255.0		
Primary DNS	192.168.0.254		
Secondary DNS			
Statistics			
SSID	MAC	RX(Packets)	TX(Packets)
Ethernet	A8:F7:E0:56:7C:87	1214.858KB(6724 PKts.)	3873.184KB(5666 PKts.)
Miki_5G	A8:F7:E0:56:7C:89	7.111KB(61 PKts.)	1.362KB(9 PKts.)
<input type="button" value="Refresh"/>			

Figure 4-4 Main Status

The page includes the following settings:

Object	Description
• Device Information	Shows the general system information such as device name, MAC address, country, current time, and firmware version.
• LAN Information	Shows Local Area Network settings such as the LAN IP address, subnet mask, DHCP server, and Rx/Tx packets.
• WAN Information	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.
• Wireless LAN Information / Wireless WAN Information (WISP)	Shows wireless information such as operation mode, wireless mode, channel bandwidth, frequency, channel, information about each SSID, security settings, and Rx/Tx packets.
• Statistics	Shows the current traffic statistic of each interface.

4.2.2 Changes

Click “Changes” and the following page will be displayed.

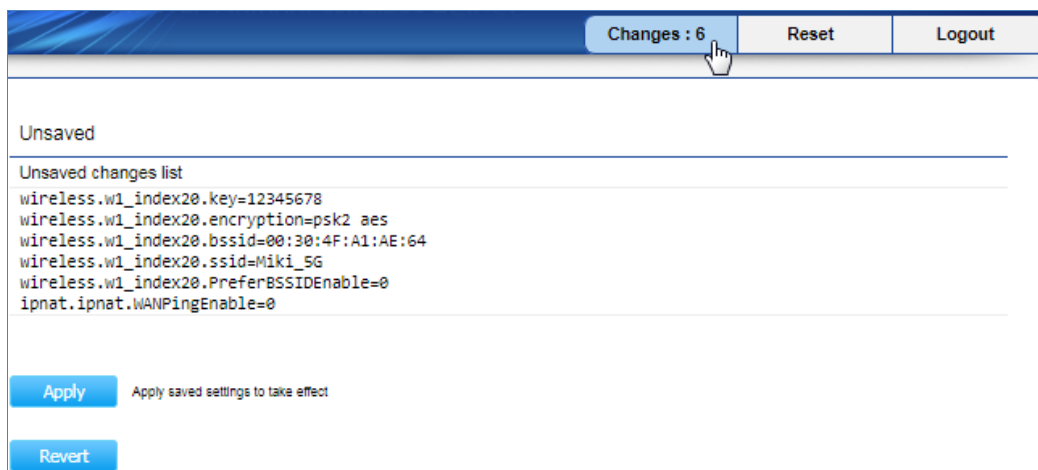


Figure 4-5 Changes

Click **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.

4.2.3 Wireless Client List

Click “Overview → Connections” to view the current associated client.

Connection List - 5GHz						
SSID	MAC Address	TX	RX	RSSI	Block	
PLANET1	00:30:4F:A8:FF:FF	2Kb	9Kb	-46dBm	<input type="button" value="Kick"/>	

Figure 4-6 Wireless Client List

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.
• Kick	Click Kick to add the client to the MAC ACL denied list.

4.2.4 WDS Link List

Click "Overview → Connections" to view the current WDS link client.

The **WDS Link List** is only available in WDS AP and WDS Bridge modes.

WDS Link List - 5GHz			
WDS Link ID#	MAC Address	Link Status	RSSI(dBm)
#1	a8:f7:e0:58:1a:94	Up	-23

Figure 4-7 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 “**Overview -> DHCP Client Table**” to view the current DHCP client.

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

DHCP Client List		
MAC Address	IP	Host Name
00:16:d4:ff:d2:e3	192.168.1.107	ENM-2-PC

Refresh

Figure 4-8 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 “**Overview → Connections**” to view the current association status.

Connection Status - 5GHz	
SSID	PLANET1
BSSID	A8:F7:E0:56:7C:89
Connection Status	Associated
Wireless Mode	802.11 AC/N
Current Channel	5.18 GHz(Channel 36)
Security	WPA2/PSK AES
Tx Data Rates(Mbps)	866.7 Mb/s
Current noise level	-95 dBm
Signal strength	-22 dBm
<input type="button" value="Refresh"/>	

Figure 4-9 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.

4.3 Network

4.3.1 IP Settings

Click "**Network** → **Basic**" to configure the LAN IP address.

IPv4 Settings	
IP Network Setting	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	192.168.1.253
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
IPv6 Settings	
	<input checked="" type="checkbox"/> Link-Local Address
IP Address	
Subnet Prefix Length	
Gateway	
Primary DNS	
Secondary DNS	

Figure 4-10 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.
• Save	Click Save to apply the new 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. Click **"Network → Basic"** to enable/disable Spanning Tree Settings.

Spanning Tree Protocol (STP) Settings		
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Hello Time	2	seconds (1-10)
Max Age	20	seconds (6-40)
Forward Delay	15	seconds (4-30)
Priority	32768	(0-65535)
<input type="button" value="Save"/> Save current setting(s)		

Figure 4-11 Spanning Tree Settings

The page includes the following settings:

Object	Description
• Spanning Tree Status	Click Enable to enable or click Disable to disable the option.
• Hello Time	Specify 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.
• Max Age	Specify 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.
• Forward Delay	Specify 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.
• Priority	Specify the Priority number. Smaller numbers have greater priority.
• Save	Click Save to save the setting.

4.4 Router (WISP Mode Only)

4.4.1 DHCP Server Settings

Go to the **"Network → Wireless"** 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 IP Setup	
IP Address	192.168.1.253
IP Subnet Mask	255.255.255.0
<input checked="" type="checkbox"/> 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
<input type="button" value="Save"/> Save current setting(s)	

Figure 4-12 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.
• Save	Click Save to save the setting.

4.4.2 WAN Settings

Go to the “**Network → Wireless**” 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	
Internet Connection Type	DHCP ▼
Options	
Account Name (if required)	<input type="text"/>
Domain Name (if required)	<input type="text"/>
MTU	Auto ▼ 1500 (576 - 1500)
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP <input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text" value="0.0.0.0"/>
Secondary DNS	<input type="text" value="0.0.0.0"/>
WAN Ping	
Discard Ping on WAN	<input checked="" type="checkbox"/>

Figure 4-13 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>	
Domain Name Server (DNS) Address	
<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.
WAN Ping	

<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.
--	---

4.4.2.1. DHCP

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

格式化: 間距 套用前: 0.5 行

Figure 4-14 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.

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	
Internet Connection Type	Static IP ▼
Options	
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

Figure 4-15 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.

4.4.2.3. PPPoE

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

格式化: 間距 套用前: 0.5 行

WAN Settings	
Internet Connection Type	PPPoE ▼
Options	
MTU	Auto ▼ 1492 (576 - 1492)
PPPoE Options	
Login	admin
Password
Service Name (if required)	
<input type="radio"/> Connect on Demand: Max idle Time 1 Minutes	
<input checked="" type="radio"/> Keep Alive: Redial Period 30 Seconds	
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP <input type="radio"/> Use These DNS Servers	

Figure 4-16 WAN Settings – PPPOE

格式化: 间距 套用前: 0.5 行

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).
• 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.

4.4.2.4. PPTP

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

WAN Settings	
Internet Connection Type	PPTP ▼
Options	
MTU	Auto ▼ 1400 (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	*****
<input type="radio"/> Connect on Demand: Max idle Time 15 Minutes	
<input checked="" type="radio"/> Keep Alive: Redial Period 30 Seconds	

Figure 4-17 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.

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 “**Network → Wireless**” page to configure the device as “**WISP**” and then go to “**Router → VPN Pass Through**” to enable VPN passthrough you required in WISP mode.

格式化: 间距 套用前: 0.5 行

Figure 4-18 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.
• Save	Click Save to save the setting.

4.4.4 Port Forwarding

Go to the “**Network → Wireless**” page to configure the device as “**WISP**” and then go to “**Router → Port Forwarding**” to configure the port forwarding rule.

Figure 4-19 Port Forwarding

The page includes the following settings:

Object	Description
--------	-------------

• #	Displays the sequence number of the forwarded port.
• Name	Displays the name of the forwarded port.
• Protocol	Displays the protocol to use for mapping from the following: TCP, UDP or Both.
• Start Port	Displays the LAN port number that WAN client packets will be forward to.
• End Port	Displays the port number that the WAN client packets are received.
• Server IP Address	Displays the IP address of the server for the forwarded port.
• Enable	Click to enable or disable the forwarded port profile.
• Modify	Click to modify the forwarded port profile.
• Delete	Click to delete the forwarded port profile.
• Add Entry	Click Add Entry to add the new forwarding rule.
• Save	Click Save to save the setting.

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

Figure 4-20 Port Forwarding

格式化: 间距 套用前: 0.5 行

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.

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

Figure 4-21 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.
• Save	Click Save to save the setting.

4.4.6 Dos Protection

The DoS Protection function can protect the device from being attacked by TCP-SYN Flood, UDP Flood and ping attack.

Go to the “**Network → Wireless**” page to configure the device as “**WISP**” and then go to “**Management → Dos Protection**” to enable DoS protection.

格式化: 间距 套用前: 0.5 行

Figure 4-22 DoS Protection

The page includes the following settings:

Object	Description
• SYN Flood Attack Protection	Enter a value between 1 ~ 10000. When the current TCP-SYN-Flood Packets numbers is beyond the set value, the Router will start up the blocking function immediately.
• Use TCP SYN Cookies Protection	Select it to use TCP SYN Cookies Protection.
• UDP Flood Attack Protection	Enter a value between 1 ~ 10000. When the current UDP-Flood Packets number is beyond the set value, the Router will start up the blocking function immediately.
• Ping Attack Protection	Select Enable to ignore/forbid ping packet.
• Save	Click Save to save the setting.

4.5 Wireless

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

4.5.1 Wireless Settings

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

格式化: 间距 套用前: 0.5 行

Wireless Settings - 5GHz								
No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	<input checked="" type="checkbox"/>	PLANET1	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	51
2	<input type="checkbox"/>	PLANET2	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	52
3	<input type="checkbox"/>	PLANET3	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	53
4	<input type="checkbox"/>	PLANET4	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	54
5	<input type="checkbox"/>	PLANET5	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	55
6	<input type="checkbox"/>	PLANET6	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	56
7	<input type="checkbox"/>	PLANET7	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	57
8	<input type="checkbox"/>	PLANET8	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	58

Figure 4-23 Wireless Settings – AP Mode

Wireless Settings - 5GHz								
No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	<input checked="" type="checkbox"/>	PLANET1	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	51
2	<input type="checkbox"/>	PLANET2	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	52
3	<input type="checkbox"/>	PLANET3	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	53
4	<input type="checkbox"/>	PLANET4	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	54

WDS Link Settings - 5GHz	
Security	None ▼
AES Passphrase	<input type="text"/> (8-63 ASCII characters or 64 hexadecimal digits)
ID	MAC Address
1	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
	Mode
	Disable ▼
	Disable ▼
	Disable ▼
	Disable ▼

Figure 4-24 Wireless Settings – WDS AP Mode

In the AP/WDS AP mode, click the **Edit** button on the “Wireless Settings – 5GHz” section to enter the “SSID Profile” page to configure the SSID profile includes the wireless security and wireless traffic shaping for the wireless network.

格式化: 间距 套用前: 0.5 行

Figure 4-25 Wireless Profile – AP/WDS AP Mode

格式化: 间距 套用前: 0.5 行

The wireless settings of AP or WDS AP mode include the following settings:

Object	Description
Wireless Settings – 5GHz	
• No.	Displays the sequence number of the entries. In the AP mode, up to 8 SSIDs can be configured as different VAPs. In the WDS AP mode, up to 4 SSIDs can be configured as different VAPs.
• Enable	Click it to enable the SSID interface.
• SSID	Specify the SSID for the current profile.
• Edit	Click the Edit button of the selected SSID to enter the “ SSID Profile ” page to configure the SSID profile includes the wireless security and wireless traffic shaping for the wireless network.
• Security	Displays the current wireless security of the specific SSID.
• Hidden SSID	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
• Client Isolation	Click this option to prevent communication between client devices.
• VLAN Isolation	Enable it to restrict clients communicating with different VLANs by selecting the radio button.
• VLAN ID	Specify the VLAN tag for the SSID.

Wireless Profile Settings (Security, MAC ACL, Wireless Traffic Shaping)	
• 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.
• 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.
MAC Address	Displays the MAC Address that will be denied/allowed access to this device.
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.
Enable Traffic Shaping	Enable or disable the regulation of packet flow leaving an interface for improved QoS.
• Download Limit	Specify the wireless transmission speed used for downloading.
• Upload Limit	Specify the wireless transmission speed used for uploading.
• Save	Click Save to save changes.

In the CB/WDS STA/CR mode, click **Scan** in the “**AP Detection**” field to associate to the AP. Then, you can configure the wireless profile settings as following page.

The screenshot shows the 'Wireless Setting - 5GHz' configuration interface. It includes the following fields and values:

- Preferred BSSID:** A8 : F7 : E0 : 00 : 01 : 9D
- SSID:** PLANET
- Wireless Security - 5GHz:**
 - Security Mode:** WPA2-PSK
 - Encryption:** AES
 - Passphrase:** 12345678
- Buttons:** A blue 'Save' button and a text link 'Save current setting(s)' are located at the bottom left.

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

After click Save, the wireless configuration can be observed in the **Wireless Settings – 5GHz** section.

No.	SSID	Edit	Security
AP SSID	PLANET	Edit	WPA2/PSK AES

Save Save current setting(s)

格式化: 間距 套用前: 0.5 行

Figure 4-27 Wireless Settings – CB/WDS STA/CR Mode

格式化: 間距 套用前: 0.5 行

The page includes the following settings:

Object	Description
• Prefer BSSID	Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.
• SSID	Specify the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.
• 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.
• No.	Displays the sequence number of the entries.
• SSID	Displays the SSID for the current profile.
• Edit	Click the Edit button to modify the wireless security of associated AP.
• Security	Displays the current wireless security of the specific SSID.
• Save	Click Save to save changes.

4.5.2 WDS Link Settings

Go to the “**Network → Wireless**” page to configure the device as “**WDS Access Point**” or “**WDS Bridge**” and then you can configure the WDS link settings.

WDS Link Settings - 5GHz

Security: AES ▼

AES Passphrase: 12345678 (8-63 ASCII characters or 64 hexadecimal digits)

CAUTION: NAWDS is enabled, please assign the Channel on both frequency bands manually for settings to take effect.

ID	MAC Address						Mode
1	A8	F7	E0	58	1A	94	Enable ▼
2							Disable ▼
3							Disable ▼
4							Disable ▼

Figure 4-28 WDS Link Settings – WDS AP Mode

WDS Link Settings - 5GHz

Security	AES ▼	
WEP Key	<input type="text"/>	40/64-bit(10 hex digits) ▼
AES Passphrase	12345678 (8-63 ASCII characters or 64 hexadecimal digits)	

CAUTION: NAWDS is enabled, please assign the Channel on both frequency bands manually for settings to take effect.

ID	MAC Address						Mode
1	A8	F7	E0	58	1A	94	Enable ▼
2							Disable ▼
3							Disable ▼
4							Disable ▼
5							Disable ▼
6							Disable ▼
7							Disable ▼
8							Disable ▼

Figure 4-29 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.
• ID	Displays the sequence number of the entries. In the WDS AP mode, up to 4 nodes can be configured to use WDS link. In the WDS Bridge mode, up to 8 nodes can be configured to use WDS link.
• 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.
• Save	Click Save to save changes.



NOTE:

1. The WDS link settings is only available in WDS AP or 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 "Network → Wireless" page to configure the security settings.

In the AP/WDS AP mode, click the **Edit** button in the “**Wireless Settings – 5GHz**” section to enter the “**SSID Profile**” page and configure the wireless security for the wireless network.

Figure 4-30 Security Settings – AP/WDS AP Mode

In the CB/WDS STA/CR mode, click **Edit** button in the “**Wireless Settings – 5GHz**” section to modify the wireless security of the associated AP.

Figure 4-31 Security Settings – CB/WDS STA/CR Mode

In the WDS AP or WDS Bridge mode, select **Security** in the “**WDS Link Settings – 5GHz**” section to configure the WDS security settings. The security settings in each site of the WDS link must be configured to the same.

WDS Link Settings - 5GHz												
Security	AES ▼											
WEP Key							40/64-bit(10 hex digits) ▼					
AES Passphrase	12345678 (8-63 ASCII characters or 64 hexadecimal digits)											
CAUTION: NAWDS is enabled, please assign the Channel on both frequency bands manually for settings to take effect.												
ID	MAC Address						Mode					
1	A8	:	F7	:	E0	:	58	:	1A	:	94	Enable ▼
2		:		:		:		:		:		Disable ▼
3		:		:		:		:		:		Disable ▼
4		:		:		:		:		:		Disable ▼
5		:		:		:		:		:		Disable ▼
6		:		:		:		:		:		Disable ▼
7		:		:		:		:		:		Disable ▼
8		:		:		:		:		:		Disable ▼

Figure 4-32 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.



- 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.
- In the 802.11AC/N or 802.11A/N mixed mode, if the security is configured to WEP and WPA/WPA2 with TKIP, the connection mode/speed will be changed to 802.11a.

格式化: 間距 套用前: 0.25 行

格式化: 間距 套用後: 0.5 行

■ 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 - 5GHz	
Security Mode	WEP ▼
Auth Type	Open System ▼
Input Type	Hex ▼
Key Length	40/64-bit (10 hex digits or 5 ASCII char) ▼
Default Key	40/64-bit (10 hex digits or 5 ASCII char)
Key1	104/128-bit (26 hex digits or 13 ASCII char)
Key2	128/152-bit (32 hex digits or 16 ASCII char)
Key3	
Key4	

Figure 4-33 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 	<p>Level of WEP encryption is applied to all WEP keys. Select a 64-/128-/152-bit password length.</p> <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.
<ul style="list-style-type: none"> • Key1 – Key4 	Specify a password for the security key index. For security, each typed character is masked by a dot.
<ul style="list-style-type: none"> • Save 	Click Save to save the settings.

■ **WPA-PSK**

Wireless Security - 5GHz	
Security Mode	WPA-PSK ▼
Encryption	Both(TKIP+AES) ▼
Passphrase	12345678
Group Key Update Interval	3600

Figure 4-34 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.

■ **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 - 5GHz	
Security Mode	WPA2-PSK ▼
Encryption	Both(TKIP+AES) ▼
Passphrase	12345678
Group Key Update Interval	3600

Figure 4-35 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.

■ WPA-PSK Mixed

Wireless Security - 5GHz	
Security Mode	WPA-PSK Mixed ▼
Encryption	Both(TKIP+AES) ▼
Passphrase	12345678
Group Key Update Interval	3600

Figure 4-36 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.

■ WPA (WPA Enterprise)

Wireless Security - 5GHz	
Security Mode	WPA-Enterprise ▼
Encryption	Both(TKIP+AES) ▼
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable ▼
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Figure 4-37 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. ■ 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.

■ WPA2 (WPA2 Enterprise)

The screenshot shows the 'Wireless Security - 5GHz' configuration window. The 'Security Mode' is set to 'WPA2-Enterprise'. The 'Encryption' is set to 'Both(TKIP+AES)'. The 'Group Key Update Interval' is set to 3600. The 'Radius Port' is set to 1812. The 'Radius Accounting' is set to 'Disable'. The 'Interim Accounting Interval' is set to 600. Other fields like 'Radius Server', 'Radius Secret', 'Radius Accounting Server', and 'Radius Accounting Secret' are present but their values are obscured by grey boxes.

Figure 4-38 Security Settings – WPA2 (WPA2 Enterprise)

The security mode includes the following settings:

Object	Description
• Security Mode	Select WPA2 from the drop-down list to configure the wireless network using WPA2 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.

	<ul style="list-style-type: none"> ■ 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.

■ WPA Mixed (WPA Mixed Enterprise)

Wireless Security - 5GHz	
Security Mode	WPA Mixed-Enterprise ▼
Encryption	Both(TKIP+AES) ▼
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable ▼
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Figure 4-39 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.
• Interim Accounting Interval	Specify the interim accounting interval (60 - 600 seconds).
• Save	Click Save to save the 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.

Wireless MAC Filter	
ACL Mode	Deny MAC in the List ▼
	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value="Add"/>
No.	MAC Address
1	A8:F7:E0:FF:FF:FF <input type="button" value="Delete"/>

Figure 4-40 Wireless MAC Filter

The page includes the following settings:

Object	Description
• 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.
• 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.
• No.	Displays the sequence number of the entries.
• MAC Address	Displays the MAC Address that will be denied/allowed access to this device.
• Delete	Click Delete to remove the entry from the list.

4.5.5 Guest Network Settings

Go to the “**Network → Wireless**” page to configure the device as “**Access Point**” or “**WDS Access Point**” mode and then you can configure the **Guest Network Settings** in the bottom of the page.

The Guest Network allows segregate temporary guest wifi usage with individual SSID, security and DHCP settings. Click **Edit** to configure the security for the guest network.

Guest Network Settings					
Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
<input checked="" type="checkbox"/>	PLANET_GuestNetwork	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manual IP Settings					
- IP Address		<input type="text" value="192.168.200.1"/>			
- Subnet Mask		<input type="text" value="255.255.255.0"/>			
Automatic DHCP Server Settings					
- Starting IP Address		<input type="text" value="192.168.200.100"/>			
- Ending IP Address		<input type="text" value="192.168.200.200"/>			
- WINS Server IP		<input type="text" value="0.0.0.0"/>			

Figure 4-41 Wireless - Guest Network Settings

The page includes the following settings:

Object	Description
• Enable	Click Enable to enable the guest network wifi.
• SSID	Specifies the SSID for the current profile.
• Edit	Click Edit to configure the wireless security of the guest network wifi.
• Security	Displays the current security setting of the guest network wifi.
• Hidden SSID	Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.
• Client Isolation	Check this option to prevent communication between client devices.
• IP Address	IP address of this device when enabled the guest network.
• Subnet Mask	Subnet mask of this device when enabled the guest network.
• Starting IP Address	The first IP Address in the range of the addresses by the DHCP server.
• Ending IP Address	The last IP Address in the range of addresses assigned by the DHCP server.
• WINS Server IP	Enter the IP address of the WINS server.

4.5.6 RSSI Threshold

Go to the “**Network → Wireless**” page to configure the device as “**Access Point**” or “**WDS Access Point**” mode

and then you can configure the **Guest Network Settings** in the bottom of the page.

and then you can configure the **RSSI Threshold** in the bottom of the page.

The RSSI Threshold is used when a weakening wireless link between AP and client is detected below the specific RSSI, the AP will encourage client to access the nearby AP with stronger signal, thus ensure stable wireless connectivity.

Figure 4-42 Wireless - RSSI Threshold

The page includes the following settings:

Object	Description
<ul style="list-style-type: none"> Status 	Click Enable to enable the RSSI Threshold.
<ul style="list-style-type: none"> RSSI (Received Signal Strength Index) 	<p>Specifies the RSSI value to limit the client access. Range: -60dBm ~ -100dBm</p> <p>RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.</p>

4.5.7 Management VLAN

Go to the **“Network → Wireless”** page to configure the device as **“Access Point”** or **“WDS Access Point”** mode and then you can configure the **Management VLAN Settings** in the bottom of the page.

If your network includes VLANs and if tagged packets need to pass through the Access Point, enable the management VLAN settings and enter the VLAN ID. Otherwise, keep it disabled.

Figure 4-43 Wireless – Management VLAN

The page includes the following settings:

Object	Description
--------	-------------

• Status	Click Enable to enable the Management VLAN.
• Management VLAN ID	Specifies the management VLAN ID for the wireless network. Range: 1 ~ 4094

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 Account (Password Settings)

Click **“System Manager → Account”** to configure username and password of the login account.

Figure 4-44 Administration (Password Settings)

The page includes the following settings:

Object	Description
• Administrator Username	Enter a new username for logging in to the Web page.
• Current Password	Enter the current password.
• New Password	Enter a new password for logging in to the Web page.
• Verify Password	Re-enter the new password for confirmation.
• Apply	Click Apply to apply all changes.
Remote Management: WISP mode only	
• Remote Management	Click Enable to enable remote access through WAN.
• Remote Management Port	Enter the remote access port number.

4.6.2 SNMP Settings

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

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

SNMP Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Port	<input type="text" value="161"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read Write)	<input type="text" value="private"/>
Trap Destination	
- Port	<input type="text" value="162"/>
- IP Address	<input type="text"/>
- Community Name	<input type="text" value="public"/>
SNMPv3 Settings	
- Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
- Username	<input type="text" value="admin"/> (1-31 Characters)
- Authorized Protocol	<input type="text" value="MD5"/> ▼
- Authorized Key	<input type="text" value="12345678"/> (8-32 Characters)
- Private Protocol	<input type="text" value="DES"/> ▼

Figure 4-45 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.

4.6.3 CLI/SSH/HTTPS Settings

Click “**Management → Advanced**” to configure CLI/SSH/HTTPS settings.

CLI Setting	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH Setting	
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
HTTPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTPS forward	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Figure 4-46 CLI/SSH/HTTPS Settings

The page includes the following settings:

Object	Description
• CLI	Enable or disable the device management via a command line interface.
• SSH	Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.
• HTTPS	Enable HTTPS to transfer and Displays web content securely. The Hypertext Transfer Protocol over SSL (Secure Socket Layer) is a TCP/IP protocol used by web servers to transfer and Displays web content securely.
• Apply	Click Apply to apply all changes.

4.6.4 Email Alert

You can use the Email Alert feature to send messages to the configured email address when particular system events occur. Click “**Management → Advanced**” to configure email alert settings.

Figure 4-47 Email Alert Settings

The page includes the following settings:

Object	Description
• Status	Click Enable to use email alert.
• From	Enter the email address to show the sender of the email.
• To	Enter the address to receive email alerts.
• Subject	Enter the text to appear in the email subject line.
• Username	Enter the username for the email account that will be used to send emails.
• Password	Enter the password for the email account that will be used to send emails.
• SMTP Server	Enter the IP address or hostname of the outgoing SMTP server.
• Port	Enter the SMTP port number to use for outbound emails.
• Security Mode	Select the security mode of the SMTP server. SSL/TLS: default port number is 465 STARTTLS: default port number is 587
• Apply	Click Apply to apply all changes.

4.6.5 Backup/Restore Settings

Click “System Manager → Firmware” and refer to the “Backup/Restore Settings” section.

Backup/Restore Settings	
Factory Setting	
- Backup Setting	<input type="button" value="Export"/>
- Restore New Setting	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/>
- Reset to Default	<input type="button" value="Reset"/>
User Setting	
- Back Up Setting as Default	<input type="button" value="Backup"/>
- Restore to User Default	<input type="button" value="Restore"/>
- CAUTION: Please write down your account and password before saving. The user settings will now become the new default settings at the next successful login.	

Figure 4-48 Backup/Restore Settings

The page includes the following settings:

Object	Description
Factory Setting	
• Backup Setting	Click Export to save the current configured settings.
• Restore New Setting	To restore settings that have been previously backed up, click Choose File to select the file, and click Import .
• Revert to Factory Default Settings	Click Reset to restore the device to its factory default settings.
User Setting	
• Backup Setting as Default	Click Backup to backup the user settings you would like to save to the device's memory for the default settings.
• Restore to User Default	Click Restore to restore user settings to the factory standard settings.

4.6.6 WiFi Scheduler

4.6.6.1. Auto Reboot Settings

Click "**Management → WiFi Scheduler**" 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.

Auto Reboot Settings

Status Enable Disable

Timer Sunday Monday Tuesday Wednesday Thursday Friday Saturday

: 23 : 59

Save current setting(s)

Figure 4-49 Auto Reboot Settings

The page includes the following settings:

Object	Description
• Auto Reboot Settings	Select Enable to set up this function.
• Timer	Select the day and enter the time you would like to reboot automatically.
• Save	Click Save to save all changes.

4.6.6.2. WiFi Scheduler

Click “Management → WiFi Scheduler” and the following page will be displayed.

This page allows you to configure wireless on/off schedule rule. The device can regularly enable/disable wireless radio according to the specific scheduling rule.

WiFi Scheduler

Status Enable Disable
NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.

Wireless Radio

SSID Selection

Schedule Templates

Schedule Table	Day	Availability	Duration					
			00	:	00	~ 24	:	00
	Sunday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Monday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Tuesday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Wednesday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Thursday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Friday	<input type="text" value="available"/>	00	:	00	~ 24	:	00
	Saturday	<input type="text" value="available"/>	00	:	00	~ 24	:	00

Save current setting(s)

Figure 4-50 WiFi scheduler

The page includes the following settings:

Object	Description
• Status	Select Enable to set up this function.
• Wireless Radio	Select frequency from the drop-down list for the preferred band type.
• SSID Selection	Select the SSID that you want to configure the wifi schedule.
• Schedule Templates	Select a schedule template from the drop-down list.
• Schedule Table	Choose "available" or "unavailable" on the specific day.
• Duration	Configure the wifi radio on/off according to the duration time you planned. The format is [HH:MM ~ HH:MM] (Start Time ~ End Time). HH: range from 0-24 MM: range from 0-59
• Save	Click Save to save all changes.

4.6.7 Firmware Upgrade

Click "**System Manager → Firmware**" and refer to the "**Firmware Upgrade**" section to upgrade the device's firmware.

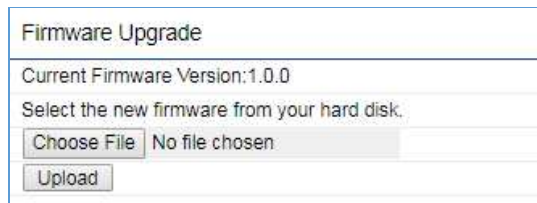


Figure 4-51 Firmware Upgrade

The page includes the following settings:

Object	Description
• Current Firmware Version	Displays the current firmware version.
• 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.

Uploaded Firmware Information:
checksum:e38d1d83d7221c2483912e8287f78092
filesize:8898476

格式化: 间距 套用前: 0.5 行

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

Uploaded Firmware Information:
checksum:e38d1d83d7221c2483912e8287f78092
filesize:8898476

20 %

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... 106

[Click here when AP is ready](#)

4.6.8 Time Settings

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

Date and Time Settings

Manually Set Date and Time

Date / /

Time : (24-Hour)

Automatically Get Date and Time

NTP Server:

Time Zone

Time Zone

Enable Daylight Saving

Start Time:

End Time:

Apply saved settings to take effect

Figure 4-52 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"> Apply 	Click Apply to apply all changes.

4.6.9 Log

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

The screenshot shows the 'System Log' configuration page. At the top, the title is 'System Log'. Below it, there are two radio buttons for 'Status': 'Enable' (selected) and 'Disable'. Underneath is a 'Log type' dropdown menu currently set to 'All', with a 'Refresh' and 'Clear' button to its left. A scrollable list of log entries follows, showing details like time, IP address, user, and message. Below the list, there are two radio buttons for 'Remote Log': 'Enable' and 'Disable' (selected). A text input field for 'Log Server IP Address' contains '0.0.0.0'. At the bottom left, there is an 'Apply' button, and to its right, the text 'Apply saved settings to take effect'.

Figure 4-53 System Log

The page includes the following settings:

Object	Description
• Status	Select Enable to enable the system log.
• 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.
• Remote Log	Select Enable to enable the remote log function.
• Log Server IP Address	Enter the remote log server IP address to record the system log.
• Apply	Click Apply to apply all changes.

4.6.10 Tools

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

Figure 4-54 Tools - Ping

The section includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Target IP / Domain Name 	Enter the IP address you would like to ping.
<ul style="list-style-type: none"> • Ping Packet Size 	Enter the packet size of each ping.
<ul style="list-style-type: none"> • Number of Pings 	Enter the number of times you want to ping.
<ul style="list-style-type: none"> • Start 	Click Start to begin pinging.

Figure 4-55 Tools - Traceroute

The section includes the following settings:

Object	Description
<ul style="list-style-type: none"> • Trace route target 	Enter an IP address or domain name you want to trace.
<ul style="list-style-type: none"> • Start 	Click Start to begin the traceroute operation.
<ul style="list-style-type: none"> • Stop 	Click Stop to terminate the traceroute operation.

Speed Test Parameters	
Target IP / Domain Name	<input type="text"/>
Time Period	<input type="text" value="20"/> Sec
Check Interval	<input type="text" value="5"/> Sec
<input type="button" value="Start"/>	<div style="border: 1px solid gray; height: 80px; width: 100%;"></div>
IPv4 Port	5001
IPv6 Port	5002

Figure 4-56 Tools – Speed Test

The section includes the following settings:

Object	Description
• Target IP / Domain Name	Enter the IP address you would like to test.
• Time period	Enter time period for the speed test.
• Check Interval	Enter the interval for the speed test.
• Start	Click Start 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.

4.6.11 Logout

Click “Logout” on the upper-right corner of the page to log out the system.

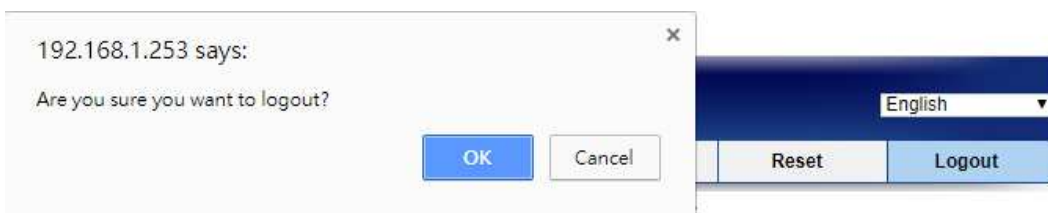


Figure 4-57 Logout

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.	<ul 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.	<ul 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.	<ul style="list-style-type: none"> ● 'Broadcast ESSID' set to off? ● The antenna is properly secured.

	<ul style="list-style-type: none">● Are you too far from your AP? Try to get closer.● Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	<ul style="list-style-type: none">● Are you using QoS function? Try to disable it and try again.● Internet is slow sometimes; try to be patient.● Try to reset the AP and see if it's better after that.● Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow.● If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; the password is wrong.	<ul style="list-style-type: none">● Make sure you're connecting to the correct IP address of the AP.● Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated.● If you really forget the password, do a hard reset.
The AP becomes hot.	<ul style="list-style-type: none">● This is not a malfunction if you can keep your hand on the AP's case.● 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 WBS-502AC 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.

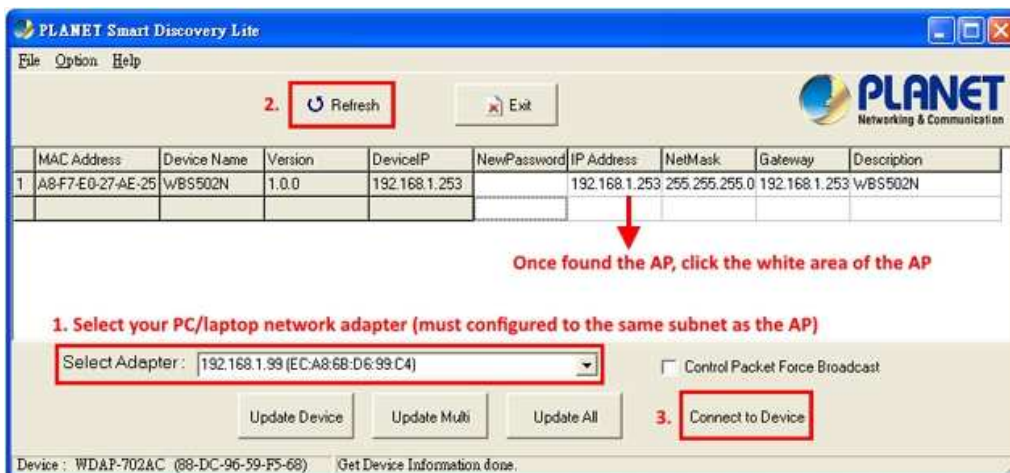


Figure B-1 PLANET Smart Discovery

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 900Mbps 802.11ac Wireless Outdoor CPE is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	Lietuviškai	Šiuo PLANET Technology Corporation ., skelbia, kad 900Mbps 802.11ac Wireless Outdoor CPE tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation , tímto prohlašuje, že tato 900Mbps 802.11ac Wireless Outdoor CPE splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	Magyar	A gyártó PLANET Technology Corporation , kijelenti, hogy ez a 900Mbps 802.11ac Wireless Outdoor CPE megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation , erklærer herved, at følgende udstyr 900Mbps 802.11ac Wireless Outdoor CPE overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	Malti	Hawnhekk, PLANET Technology Corporation , jiddikjara li dan 900Mbps 802.11ac Wireless Outdoor CPE jikkonforma mal-ħitġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt PLANET Technology Corporation , dass sich dieses Gerät 900Mbps 802.11ac Wireless Outdoor CPE in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW)	Nederlands	Hierbij verklaart, PLANET Technology Corporation , dat 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor CPE vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation , oświadcza, że 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor CPE ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ</i>	Português	PLANET Technology Corporation , declara que este 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor 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 900Mbps 802.11ac Wireless Outdoor CPE skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente, PLANET Technology Corporation , dichiara che questo 900Mbps 802.11ac Wireless Outdoor CPE è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	Suomi	PLANET Technology Corporation , vakuuttaa täten että 900Mbps 802.11ac Wireless Outdoor CPE tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo PLANET Technology Corporation , apliecinu, ka šī 900Mbps 802.11ac Wireless Outdoor CPE atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation , att denna 900Mbps 802.11ac Wireless Outdoor CPE står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

