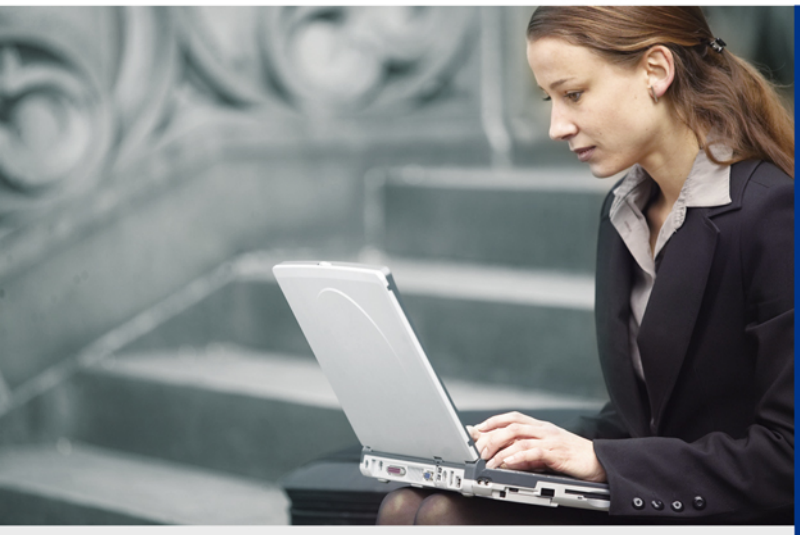
PLANET
Networking & Communication

# User's Manual

## 900Mbps 802.11ac Outdoor Wireless CPE

► **WBS-502AC**



www.PLANET.com.tw

## Copyright

Copyright © 2017 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

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

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

## Federal Communication Commission (FCC) Interference Statement

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

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

**FCC Caution:**

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

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

(1) This device may not cause harmful interference

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

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

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

## FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with 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** ..... **11**
**1.4 Product Specifications** ..... **13**
**Chapter 2.Hardware Installation** ..... **16**
**2.1 Hardware Description** ..... **16**
2.1.1 The Bottom Panel – Port ..... 16
**Chapter 3.Connecting to the AP** ..... **19**
**3.1 Preparation before Installation** ..... **19**
3.1.1 Professional Installation Required ..... 19
3.1.2 Safety Precautions ..... 19
**3.2 Installation Precautions** ..... **19**
**3.3 Installing the AP** ..... **21**
**Chapter 4.Quick Installation Guide** ..... **23**
**4.1 Manual Network Setup -- TCP/IP Configuration** ..... **23**
4.1.1 Configuring the IP Address Manually ..... 23
**4.2 Starting Setup in the Web UI** ..... **26**
**Chapter 5.Configuring the AP** ..... **28**
**5.1 Operation Mode** ..... **28**
5.1.1 Access Point (AP) ..... 31
5.1.2 Client Bridge (CB) ..... 32
5.1.3 WDS Access Point (WDS AP) ..... 33
5.1.4 WDS Station (WDS STA) ..... 34
5.1.5 WDS Bridge (WDS PtP/WDS PtMP) ..... 35
5.1.6 Client Router (CR/WISP) ..... 40
**5.2 Overview** ..... **46**
5.2.1 Device Status ..... 46
5.2.2 Changes ..... 48
5.2.3 Wireless Client List ..... 48
5.2.4 WDS Link List ..... 49
5.2.5 DHCP Client Table ..... 50
5.2.6 Connection Status ..... 50
**5.3 Network** ..... **51**
5.3.1 IP Settings ..... 51
5.3.2 Spanning Tree Settings ..... 53
**5.4 Router (WISP Mode Only)** ..... **53**

5.4.1 DHCP Server Settings ..... 53
5.4.2 WAN Settings ..... 54
5.4.2.1. DHCP ..... 56
5.4.2.2. Static IP ..... 56
5.4.2.3. PPPoE ..... 57
5.4.2.4. PPTP ..... 59
5.4.3 VPN Passthrough ..... 60
5.4.4 Port Forwarding ..... 60
5.4.5 DMZ Settings ..... 62
5.4.6 Dos Protection ..... 62
**5.5 Wireless ..... 63**
5.5.1 Wireless Settings ..... 63
5.5.2 WDS Link Settings ..... 67
5.5.3 Security Settings ..... 68
5.5.4 Wireless MAC Filter ..... 77
5.5.5 Guest Network Settings ..... 78
5.5.6 RSSI Threshold ..... 79
5.5.7 Management VLAN ..... 79
**5.6 Management ..... 81**
5.6.1 Account (Password Settings) ..... 81
5.6.2 SNMP Settings ..... 81
5.6.3 CLI/SSH/HTTPS Settings ..... 83
5.6.4 Email Alert ..... 83
5.6.5 Backup/Restore Settings ..... 84
5.6.6 WiFi Scheduler ..... 85
5.6.6.1. Auto Reboot Settings ..... 85
5.6.6.2. WiFi Scheduler ..... 86
5.6.7 Firmware Upgrade ..... 87
5.6.8 Time Settings ..... 88
5.6.9 Log ..... 90
5.6.10 Tools ..... 90
5.6.11 Logout ..... 92
**Appendix A: Troubleshooting ..... 93**
**Appendix B: Use Planet Smart Discovery to find AP ..... 95**
**Appendix C: FAQ ..... 96**
**Q1: How to set up the AP Client Connection ..... 96**
**Q2: How to set up the WDS Connection ..... 103**

# FIGURES

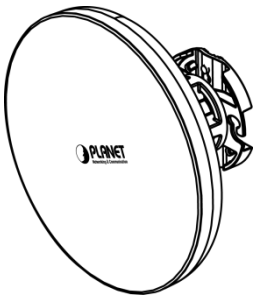
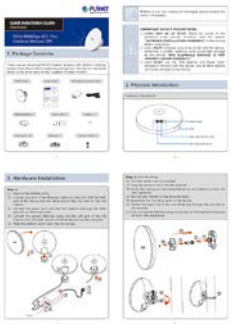
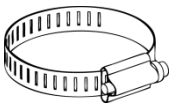
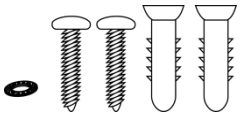
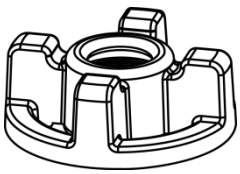
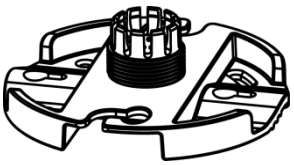
**FIGURE 2-1** THREE-WAY VIEW ..... 16
**FIGURE 2-2** REAR PANEL ..... 17
**FIGURE 3-1** POE AND LAN PORT CONNECTION ..... 21
**FIGURE 3-2** FINISH INSTALLATION AND CONNECT TO ANTENNAS (WBS-502AC ONLY) ..... 21
**FIGURE 3-3** POLE MOUNTING ..... 22
**FIGURE 3-4** WALL MOUNTING ..... 22
**FIGURE 4-1** TCP/IP SETTING ..... 24
**FIGURE 4-2** WINDOWS START MENU ..... 25
**FIGURE 4-3** SUCCESSFUL RESULT OF PING COMMAND ..... 25
**FIGURE 4-4** FAILED RESULT OF PING COMMAND ..... 26
**FIGURE 4-5** LOGIN BY DEFAULT IP ADDRESS ..... 26
**FIGURE 4-6** LOGIN WINDOW ..... 26
**FIGURE 4-7** WEB UI SCREENSHOT ..... 27
**FIGURE 5-1** WIRELESS – BASIC ..... 29
**FIGURE 5-2** OPERATION MODE – ALL ..... 29
**FIGURE 5-3** OPERATION MODE – AP ..... 31
**FIGURE 5-4** OPERATION MODE – CLIENT BRIDGE ..... 32
**FIGURE 5-5** OPERATION MODE – WDS AP ..... 33
**FIGURE 5-6** OPERATION MODE – WDS STATION ..... 34
**FIGURE 5-7** OPERATION MODE – WDS BRIDGE ..... 35
**FIGURE 5-8** OPERATION MODE – CLIENT ROUTER (WISP) ..... 40
**FIGURE 5-9** SYSTEM MENU - RESET ..... 46
**FIGURE 5-10** SYSTEM MENU – LANGUAGE OPTION ..... 46
**FIGURE 5-11** MAIN STATUS ..... 47
**FIGURE 5-12** CHANGES ..... 48
**FIGURE 5-13** WIRELESS CLIENT LIST ..... 49
**FIGURE 5-14** WDS LINK STATUS ..... 49
**FIGURE 5-15** DHCP CLIENT LIST ..... 50
**FIGURE 5-16** CONNECTION STATUS ..... 51
**FIGURE 5-17** LAN IP SETTINGS ..... 52
**FIGURE 5-18** SPANNING TREE SETTINGS ..... 53
**FIGURE 5-19** DHCP SERVER SETTINGS ..... 54
**FIGURE 5-20** WAN SETTINGS – ALL ..... 55
**FIGURE 5-21** WAN SETTINGS – DHCP ..... 56
**FIGURE 5-22** WAN SETTINGS – STATIC IP ..... 57
**FIGURE 5-23** WAN SETTINGS – PPPOE ..... 58
**FIGURE 5-24** WAN SETTINGS – PPTP ..... 59
**FIGURE 5-25** VPN PASSTHROUGH ..... 60
**FIGURE 5-26** PORT FORWARDING ..... 60
**FIGURE 5-27** PORT FORWARDING ..... 61
**FIGURE 5-28** DMZ ..... 62
**FIGURE 5-29** DOS PROTECTION ..... 63

**FIGURE 5-30** WIRELESS SETTINGS – AP MODE ..... 64
**FIGURE 5-31** WIRELESS SETTINGS – WDS AP MODE ..... 64
**FIGURE 5-32** WIRELESS PROFILE – AP/WDS AP MODE ..... 65
**FIGURE 5-33** WIRELESS PROFILE – CB/WDS STA/CR MODE ..... 66
**FIGURE 5-34** WIRELESS SETTINGS – CB/WDS STA/CR MODE ..... 67
**FIGURE 5-35** WDS LINK SETTINGS – WDS AP MODE ..... 67
**FIGURE 5-36** WDS LINK SETTINGS – WDS BRIDGE MODE ..... 68
**FIGURE 5-37** SECURITY SETTINGS – AP/WDS AP MODE ..... 69
**FIGURE 5-38** SECURITY SETTINGS – CB/WDS STA/CR MODE ..... 69
**FIGURE 5-39** SECURITY SETTINGS – WDS BRIDGE MODE ..... 70
**FIGURE 5-40** SECURITY SETTINGS – WEP ..... 71
**FIGURE 5-41** SECURITY SETTINGS – WPA-PSK ..... 71
**FIGURE 5-42** SECURITY SETTINGS – WPA2-PSK ..... 72
**FIGURE 5-43** SECURITY SETTINGS – WPA-PSK MIXED ..... 73
**FIGURE 5-44** SECURITY SETTINGS – WPA (WPA ENTERPRISE) ..... 73
**FIGURE 5-45** SECURITY SETTINGS – WPA2 (WPA2 ENTERPRISE) ..... 74
**FIGURE 5-46** SECURITY SETTINGS – WPA MIXED (WPA MIXED ENTERPRISE) ..... 76
**FIGURE 5-47** WIRELESS MAC FILTER ..... 77
**FIGURE 5-48** WIRELESS - GUEST NETWORK SETTINGS ..... 78
**FIGURE 5-49** WIRELESS - RSSI THRESHOLD ..... 79
**FIGURE 5-50** WIRELESS – MANAGEMENT VLAN ..... 79
**FIGURE 5-51** ADMINISTRATION (PASSWORD SETTINGS) ..... 81
**FIGURE 5-52** SNMP SETTINGS ..... 82
**FIGURE 5-53** CLI/SSH/HTTPS SETTINGS ..... 83
**FIGURE 5-54** EMAIL ALERT SETTINGS ..... 84
**FIGURE 5-55** BACKUP/RESTORE SETTINGS ..... 85
**FIGURE 5-56** AUTO REBOOT SETTINGS ..... 86
**FIGURE 5-57** WI-FI SCHEDULER ..... 86
**FIGURE 5-58** FIRMWARE UPGRADE ..... 87
**FIGURE 5-59** TIME SETTINGS ..... 89
**FIGURE 5-60** SYSTEM LOG ..... 90
**FIGURE 5-61** TOOLS - PING ..... 91
**FIGURE 5-62** TOOLS - TRACEROUTE ..... 91
**FIGURE 5-63** TOOLS – SPEED TEST ..... 92
**FIGURE 5-64** LOGOUT ..... 92

# 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 |
|  |  | |

Note

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

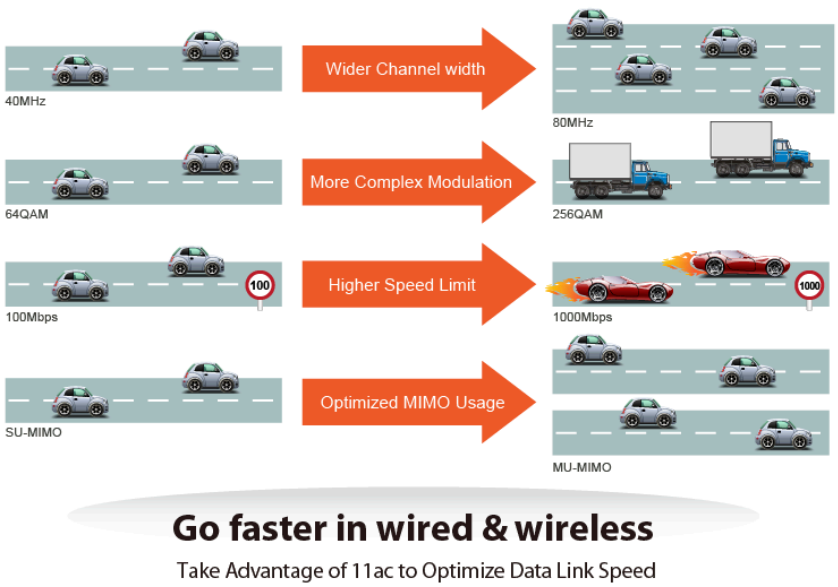
## 1.2 Product Description

### 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 – be it PtP or PtMP application.

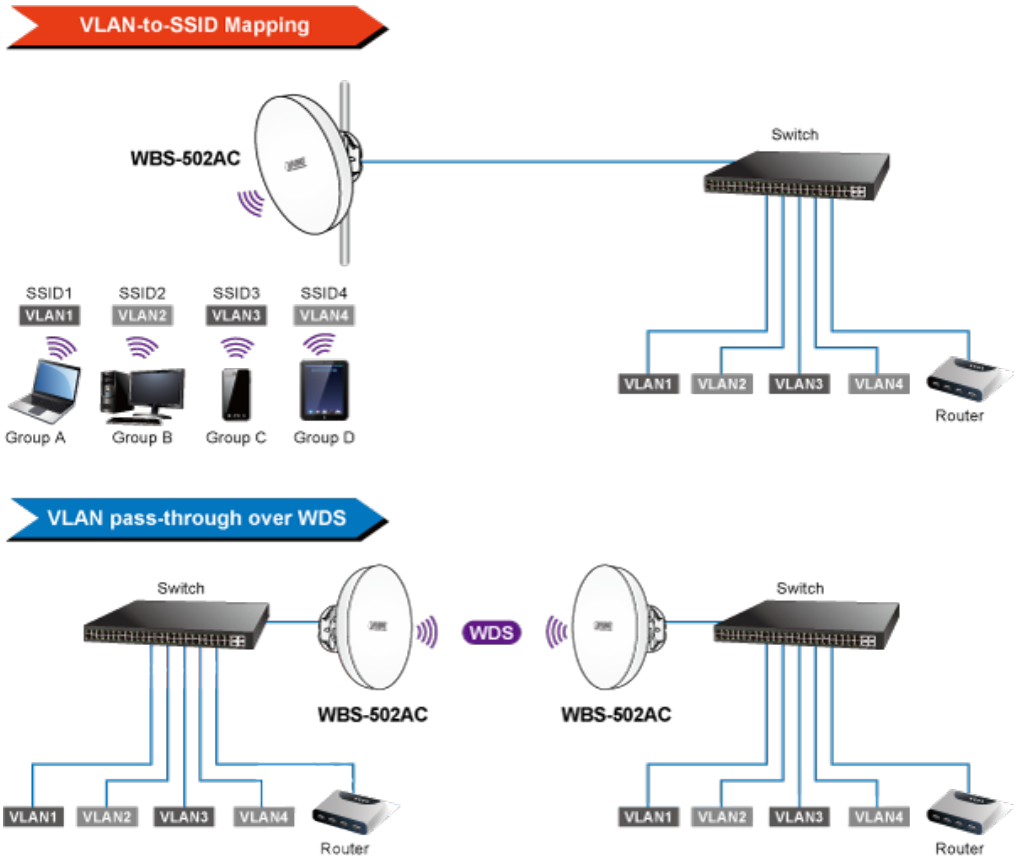
### Bringing Superior 11ac Performance to Outdoor

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.



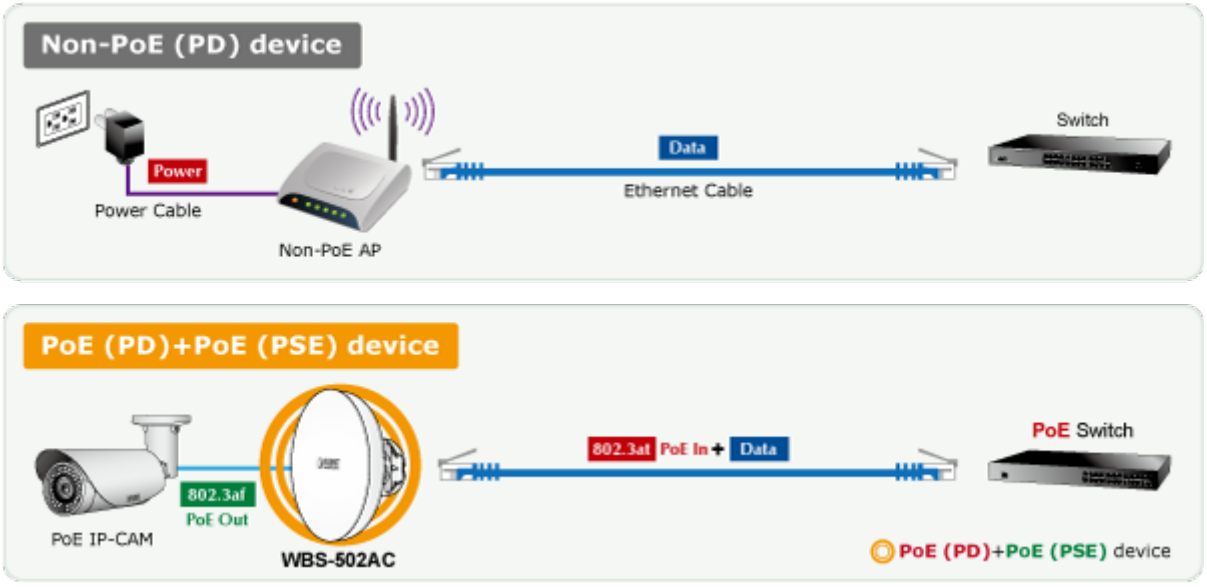

### Multiple SSIDs with VLAN Tagging

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 19dBi 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 19dBi 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, Client Bridge, Client Router (WISP), WDS
  - 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 Product Specifications

| | | | |
|---|---|---|---|
| **Product** | **WBS-502AC** | | |
| | 5GHz 900Mbps 802.11ac Outdoor Wireless CPE | | |
| **Hardware** | | | |
| **Standard Support** | IEEE 802.11a/n/ac<br>IEEE 802.11i<br>IEEE 802.3 10BASE-T<br>IEEE 802.3u 100BASE-TX<br>IEEE 802.3ab 1000BASE-T<br>IEEE 802.3x flow control | | |
| **Memory** | 64 Mbytes DDR SDRAM<br>16 Mbytes Flash | | |
| **Power Requirements** | IEEE 802.3at PoE+ | | |
| **Interface** | Wireless IEEE802.11a/n/ac, 2T2R<br>PoE LAN (LAN 1): 1 x 10/100/1000BASE-TX, auto-MDI/MDIX, 54V 802.3at PoE in<br>LAN 2: 1 x 10/100/1000BASE-TX, auto-MDI/MDIX, 802.3af PoE pass-through out | | |
| **Button** | Reset button | | |
| **LED** | PWR, LAN, WLAN, Signal Strength | | |
| **Dimensions (Φ x H)** | 190 x 38mm | | |
| **Weight** | 527g | | |
| **Antenna** | Built-in 19dBi directional antenna with dual polarization | | |
| | **Beam-width** | **Port1** | **Port2** |
| | **HPBW Horizontal** | 30° | 18° |
| | **HPBW Vertical** | 18° | 30° |
| **Data Rate** | IEEE 802.11a: up to 54Mbps<br>IEEE 802.11n (20MHz): up to 150Mbps<br>IEEE 802.11n (40MHz): up to 300Mbps<br>802.11ac (VHT20, Nss2-MCS8): Up to 173.3Mbps<br>802.11ac (VHT40, Nss2-MCS9): Up to 400Mbps<br>802.11ac (VHT80, Nss2-MCS9): Up to 867Mbps | | |
| **Media Access Control** | CSMA/CA | | |
| **Modulation** | Transmission/Emission type: OFDM<br>Data Modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM | | |
| **Frequency Band** | FCC: 5.180~5.580GHz, 5.660~5.825GHz<br>ETSI: 5.180~5.240GHz | | |
| **Operating Channels** | United States -- FCC:<br>36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116,<br>132, 136, 140, 149, 153, 157, 161, 165 (21 channels)<br><br>Europe -- ETSI: 36, 40, 44, 48 (4 channels)<br>**5GHz channel list will vary in different countries according to their regulations.** | | |

| | | | |
|---|---|---|---|
| **Max. Transmit Power (dBm)** | FCC : up to 26 ± 2dBm<br>ETSI : < 20dBm (EIRP) | | |
| **Receiver Sensitivity (dBm)** | **Network Mode** | **Data Rate** | **Receive Sensitivity (dBm)** |
| | **802.11a** | 6Mbps | -93 |
| | | 54 Mbps | -76 |
| | **802.11n HT20** | MCS0/MCS8 | -92 |
| | | MCS7/MCS15 | -73 |
| | **802.11n HT40** | MCS0/MCS8 | -89 |
| | | MCS7/MCS15 | -72 |
| | **802.11ac VHT20** | MCS0_1SS/2SS | -92 |
| | | MCS8_1SS/2SS | -69 |
| | **802.11ac VHT40** | MCS0_1SS/2SS | -89 |
| | | MCS9_1SS/2SS | -65 |
| | **802.11ac VHT80** | MCS0_1SS/2SS | -86 |
| | | MCS9_1SS/2SS | -62 |
| **Power Consumption** | Maximum 24W (with PSE) | | |
| **Power Requirements** | LAN1: IEEE 802.3at PoE+, 48~56V DC in-line power | | |
| **Environment and Certification** | | | |
| **Operating Temperature** | -20~70 degrees C | | |
| **Operating Humidity** | 10~90% (non-condensing) | | |
| **IP Level** | IP55 | | |
| **Regulatory** | CE, FCC, RoHS | | |
| **Software** | | | |
| **LAN** | ■ Static IP<br>■ Dynamic IP<br>■ DHCP server in WISP mode | | |
| | Supports 802.1d STP (Spanning Tree Protocol) | | |
| **WAN Connection Type (WISP Mode only)** | ■ Static IP<br>■ Dynamic IP<br>■ PPPoE<br>■ PPTP | | |
| **Firewall** | Offers DoS protection to guard user's content network against DoS attacks | | |
| | Built-in DMZ and Port Forwarding | | |
| | VPN Pass-through:<br>■ PPTP Pass-through<br>■ L2TP Pass-through<br>■ IPSec Pass-through | | |
| **Wireless Modes** | ■ Access Point<br>■ Client Bridge<br>■ WDS (AP/Bridge/Station)<br>■ Client Router (WISP)/Client AP Router (WISP+AP) | | |

| | |
|---|---|
| **Channel Width** | 20MHz, 40MHz, 80MHz |
| **Encryption Type** | 64-/128-/152-bit WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X |
| **Wireless Security** | Enable/Disable SSID Broadcast |
| | Wireless MAC address filtering up to 32 entries per SSID |
| | VAP Separation, Station Separation |
| **Max. SSIDs** | Up to 8 |
| **Max. Wireless Clients** | 127 per radio (32 suggested, depending on usage) |
| **Max. WDS Peers** | Up to 8 in WDS Bridge mode |
| **Wireless QoS** | Supports Wi-Fi Multimedia (WMM) |
| | Supports Wireless Traffic Shaping per Radio |
| **Wireless Advanced Control** | Auto Channel Selection |
| | Auto Transmit Power by Regular Domains |
| | Client Limit Control, RSSI Threshold |
| | Distance Control (Auto Ack Timeout) |
| | Wi-Fi Schedule |
| **Status Monitoring** | Connection Status |
| | Device Discovery, PLANET Smart Discovery |
| | Wireless Client List/WDS Link List |
| | DHCP Client Table |
| | System Log supports remote syslog server |
| | Signal Strength LEDs in Client Bridge and WDS Station modes |
| **VLAN** | VLAN pass-through over WDS, |
| | SSID-to-VLAN mapping |
| | Management VLAN (VID: 1~4094) |
| **Self-healing** | Supports auto reboot settings |
| **NTP** | Network Time Management |
| **Management** | Web-based UI, HTTPS, SSH, CLI (Command Line Interface) supported |
| | Configuration backup and restore |
| | Email alert |
| | SNMP v1/v2c/v3 support, MIB I/II, Private MIB |
| **Diagnostic Tools** | Built-in Ping, Trace Route, Speed Test Tools |

# Chapter 2. Hardware Installation

## 2.1 Hardware Description

- **Dimensions (Φ x H):** 190 x 38mm

**Figure 2-1** Three-way View

### 2.1.1 The Bottom Panel – Port

The Bottom panel provides the physical connectors connected to the power adapter and any other network device. **Figure 2-2** shows the bottom panel of the WBS-502AC.

## Bottom/Side Panel

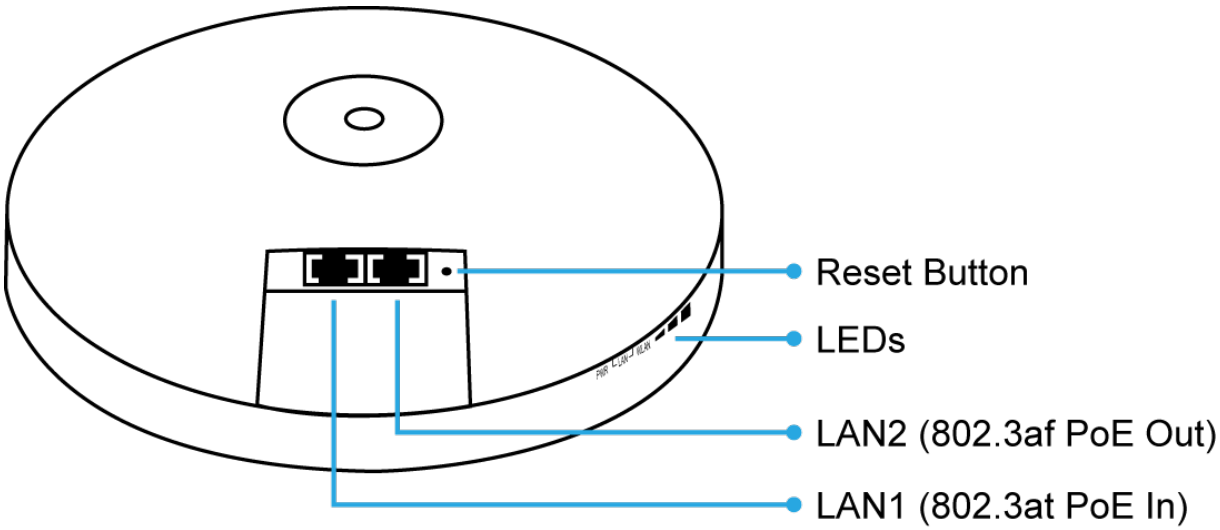



**Figure 2-2** Rear Panel

## LED Definition

| LED | | State | Meaning |
|---|---|---|---|
| **Power** | | On | The device is powered on |
| | | Off | The device is powered off |
| **LAN Ports** | | On | Port linked |
| | | Blinking | Data is transmitting or receiving data |
| | | Off | No link |
| **WLAN** | | On | The wireless radio is on |
| | | Blinking | Data is transmitting or receiving over wireless |
| | | Off | The wireless radio is off |
| **Signal Strength (Client Bridge/WDS Station/Client Router mode 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<br>IEEE 802.3at PoE PD supported, 54VDC In |
| **LAN2 Port** | 10/100/1000Mbps RJ45 port, auto MDI/MDI-X,<br>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

# Chapter 3. Connecting to the AP

## 3.1 Preparation before Installation

### 3.1.1 Professional Installation Required

Please seek assistance from a professional installer who is well trained in the RF installation and knowledgeable in the local regulations.

### 3.1.2 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 a professional 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.

## 3.2 Installation Precautions

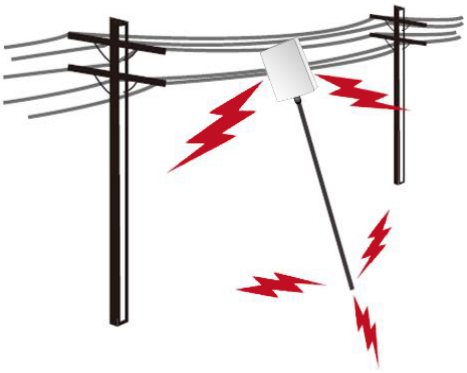
- Users **MUST** use a proper and well-installed surge arrestor and grounding kit with the WBS-502AC; otherwise, a random lightning could easily cause fatal damage to the WBS-502AC. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**
- Users **MUST** use the "Power cord and PoE Injector" shipped 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 lasers 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.

## 3.3 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.

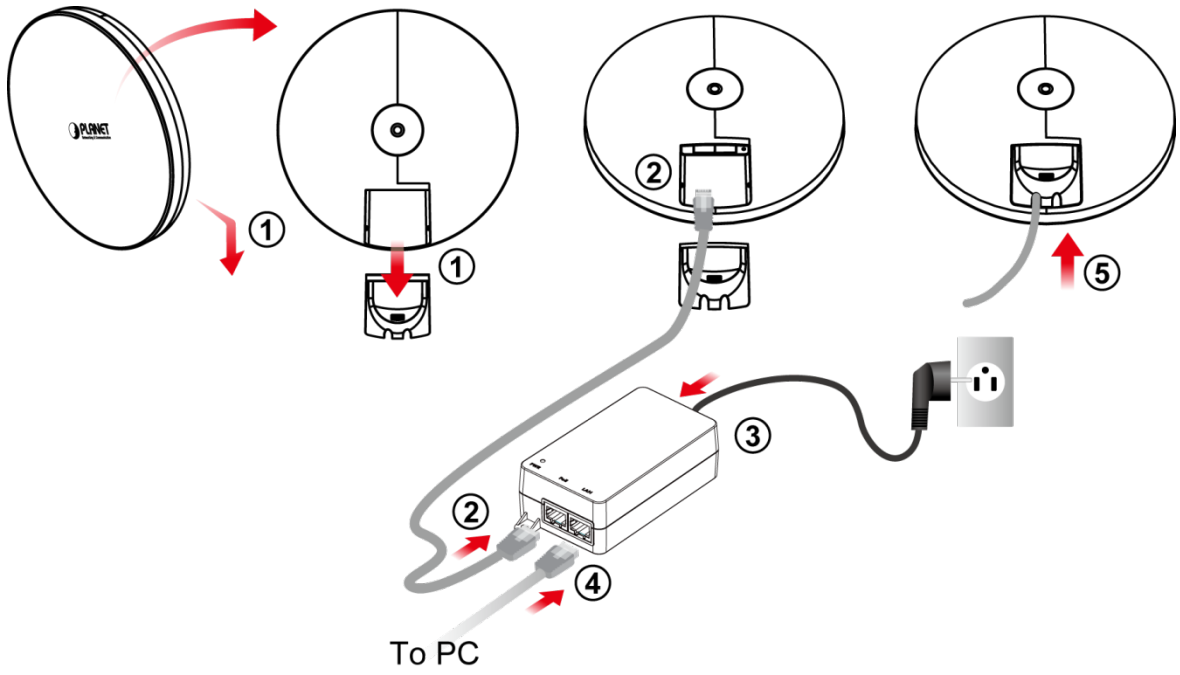



**Figure 3-1** PoE and LAN port connection

**Figure 3-2** Finish installation and connect to antennas (WBS-502AC only)

**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.

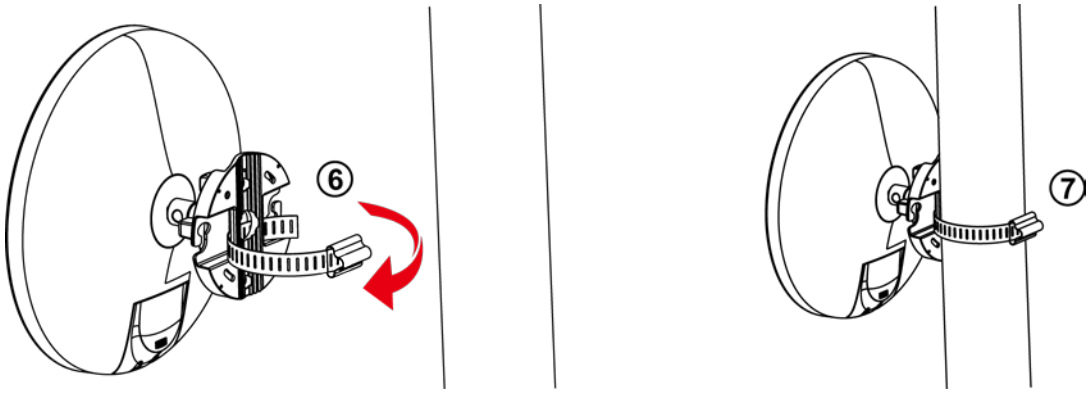



**Figure 3-3** Pole Mounting

**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.

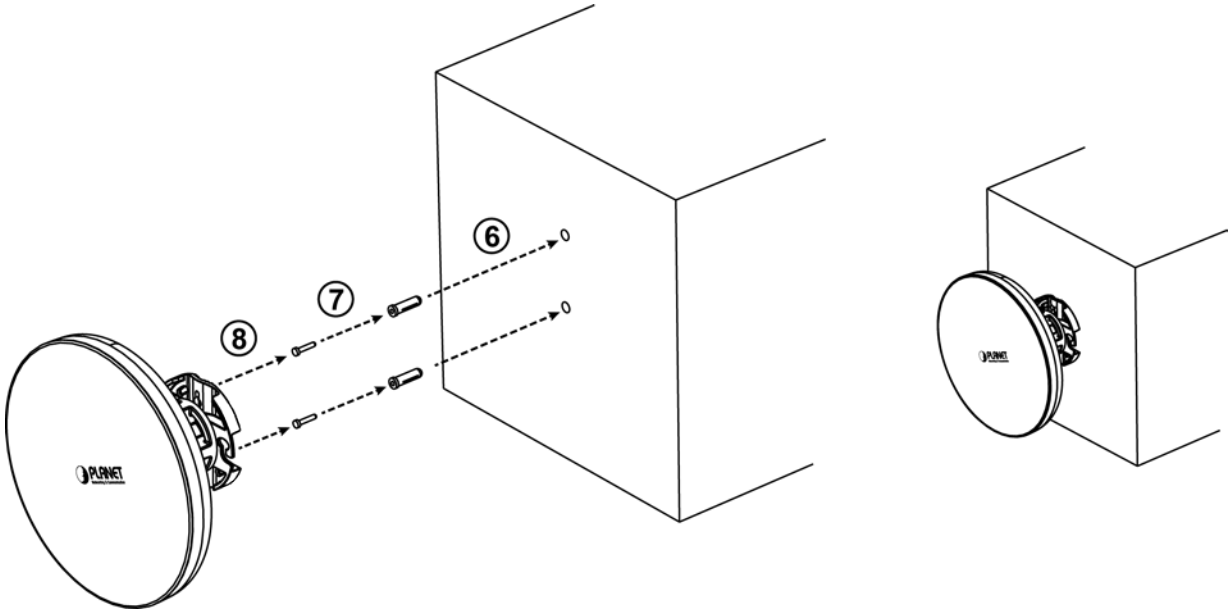



**Figure 3-4** Wall Mounting

# Chapter 4. Quick Installation Guide

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

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

## 4.1 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.

### 4.1.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx ("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

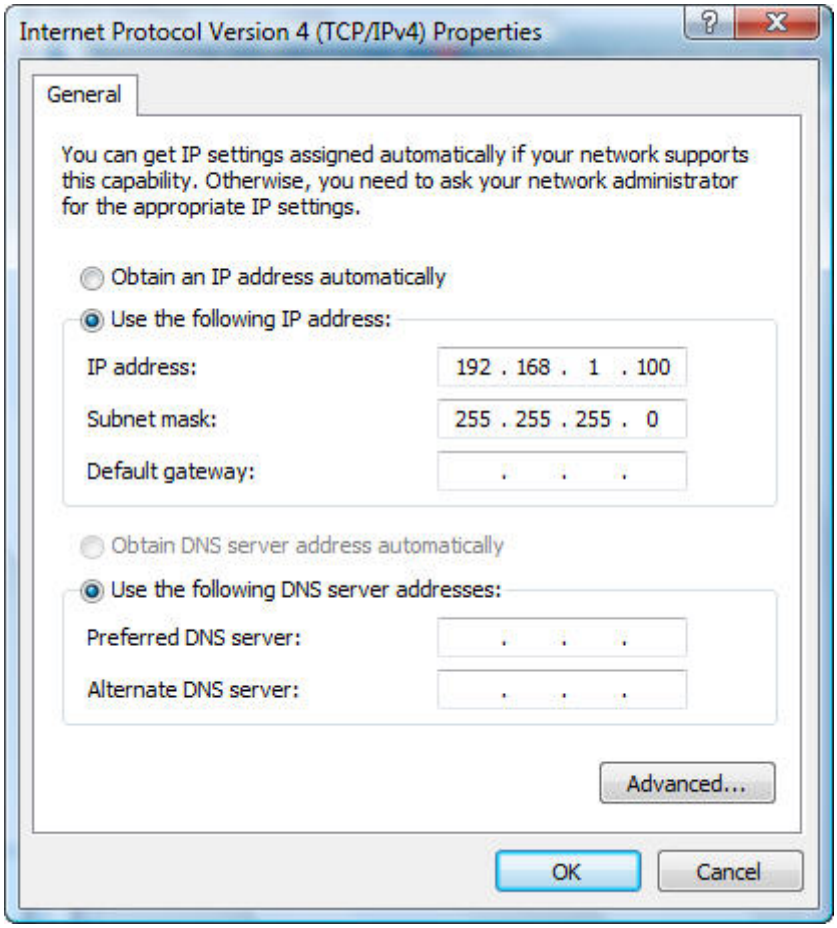



**Figure 4-1** TCP/IP Setting

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

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 7** OS. Please follow the Steps below:

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

2. Type "**cmd**" in the Search box.

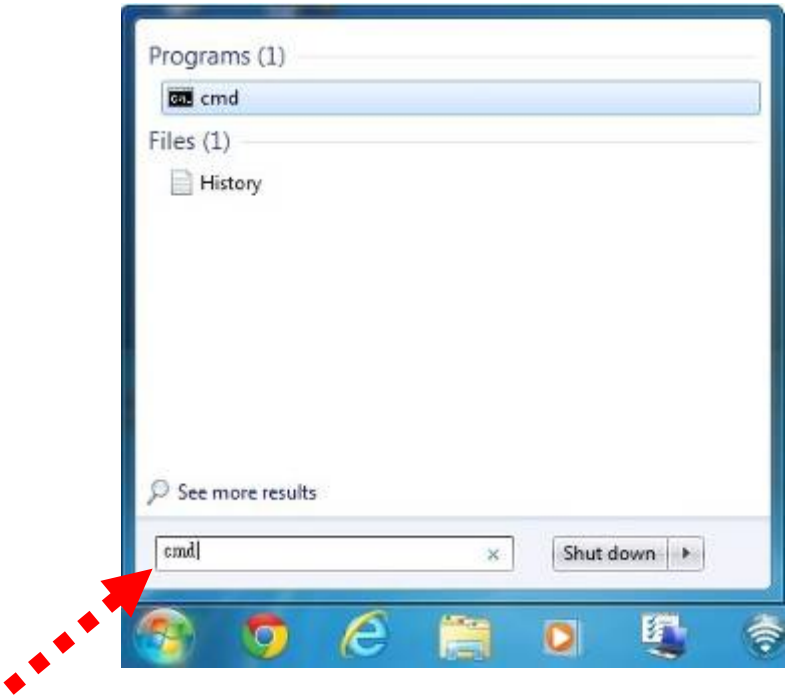



**Figure 4-2** Windows Start Menu

3. Open a command prompt 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.

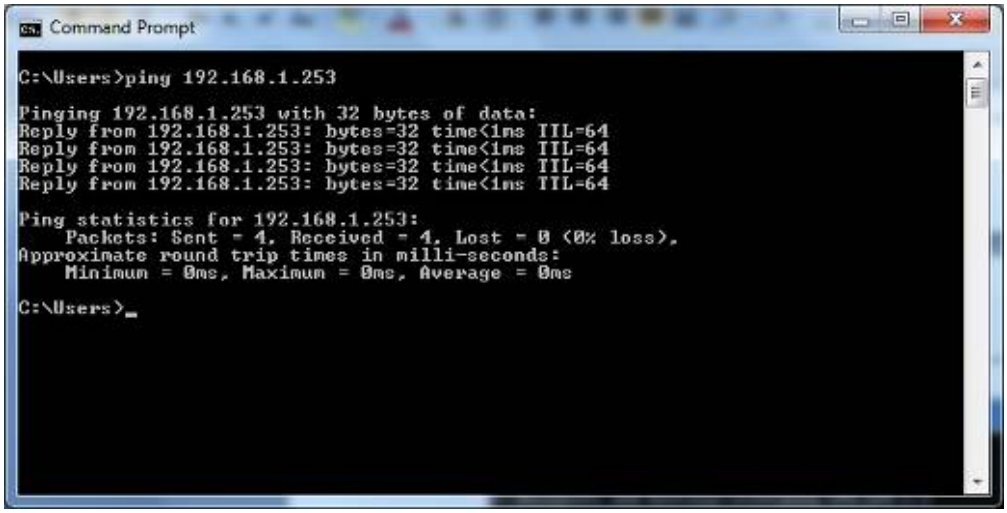



**Figure 4-3** Successful result of Ping command

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

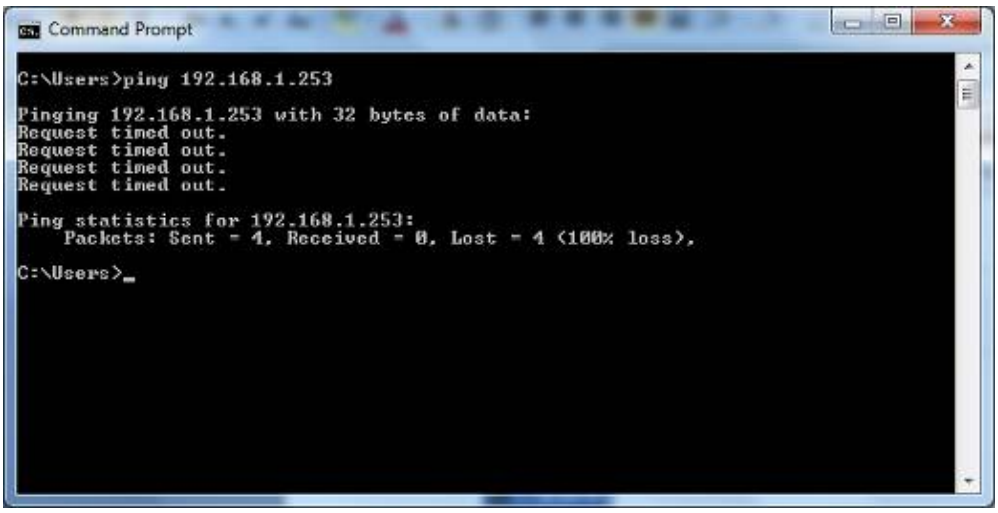



**Figure 4-4** Failed result of Ping command

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

## 4.2 Starting Setup in the Web UI

It is easy to configure and manage the 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.

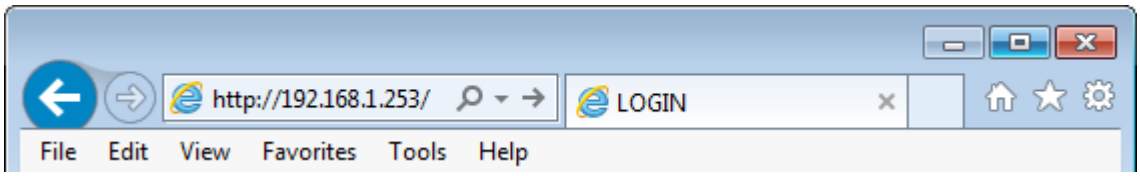



**Figure 4-5** Login by default IP address

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 4-6** 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.

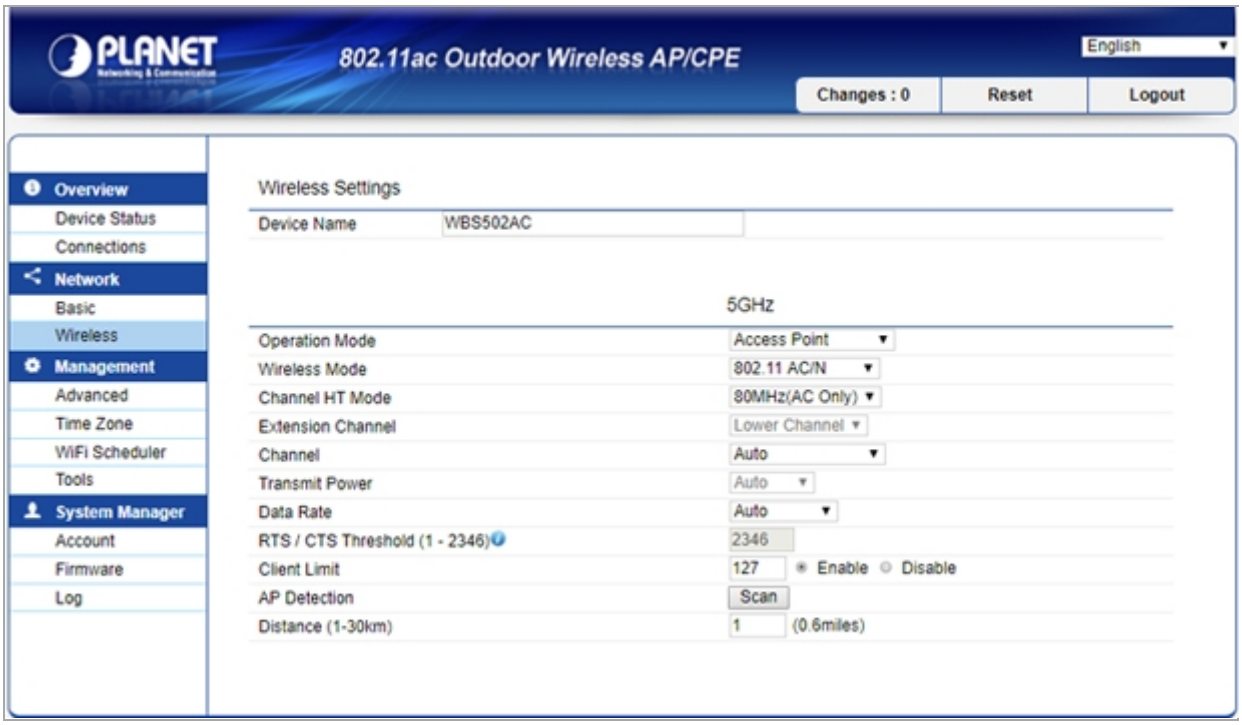



**Figure 4-7** Web UI Screenshot

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 5. Configuring the AP

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

## 5.1 Operation Mode

On this page, you can select the following different operation modes of the AP depending on your application:

| Operation Modes | Description |
|---|---|
| ■ **Access Point** | Access Point mode is used to provide wireless connectivity to wireless clients. This mode is compatible with general wireless clients. |
| ■ **Client Bridge** | Client Bridge mode allows the Access Point to become a wireless client to be able to be associated with another AP, thus enabling the wireless capability of wired clients. |
| ■ **WDS Access Point** | In WDS Access Point mode, the device functions as a WDS bridge in the Access Point mode. For WDS Access Point, it can be connected by the same series of devices in the WDS station mode. In this mode, the setting is the same as the Access Point mode. |
| ■ **WDS Bridge** | In the WDS Bridge mode, the device can bridge with remote LAN networks through MAC address. This application can create two individual networks for two groups of users sharing one Internet. The advantage of WDS is the Layer 2 transparent bridging and broadcasting across wireless connections so that all connected network devices form one common broadcast domain.<br><br>**NOTE: The WDS mode is a non-standard extension to the IEEE 802.11 standard, which is implemented differently in wireless driver and firmware making them incompatible with each other. In order to use WDS, the same model of devices should be used.** |
| ■ **WDS Station** | In the WDS Station mode, the device functions as a wireless client which can bridge the remote WDS Access Point with SSID. In this mode, the setting is the same as the Client Bridge mode. |
| ■ **Client Router** | In the Client Router (Wireless ISP) mode, the device can connect to a wireless network and share the Internet connection to the WISP subscribers. On the LAN side, the device acts like a wired router for IP sharing function. In this mode, the wireless interface acts as WAN side. |

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

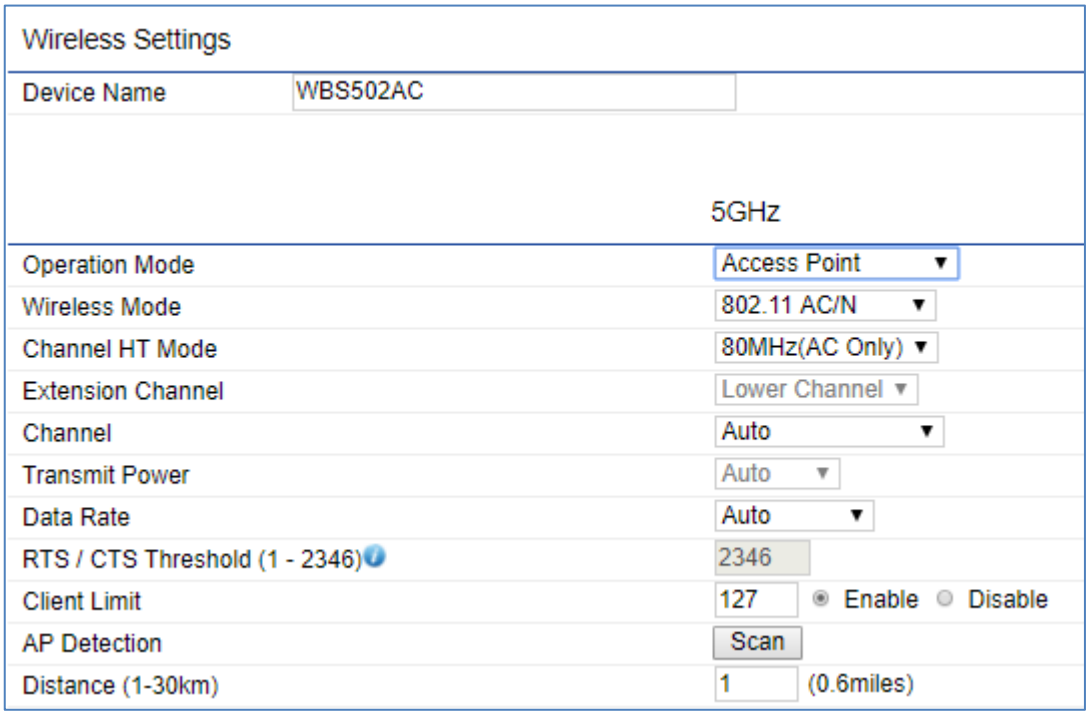



**Figure 5-1** Wireless – Basic

There are 6 operation modes supported in the WBS-502AC. Choose the suitable one and start to configure the wireless basic setting of the operation mode you chose in this page.

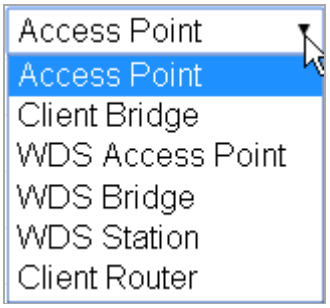



**Figure 5-2** Operation Mode – All

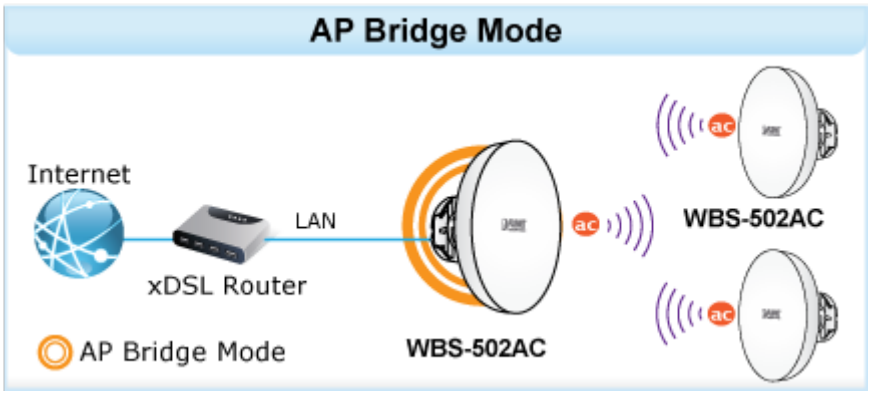
The page includes the following settings:

| Object | Description |
|---|---|
| • **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. |
| • **Operation Mode** | Use the radio button to select an operation mode. |
| • **Wireless Mode** | The wireless mode supports the following 5GHz modes:<br>● 802.11AC/N mixed mode<br>● 802.11A/N mixed mode<br>● 802.11A<br>● 802.11N (5GHz) |
| • **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:<br>● 80MHz (AC only)<br>● 40MHz<br>● 20MHz |
| • **Extension Channel** | Select upper or lower channel. Your selection may affect the Auto channel function. |
| • **Channel** | Select the appropriate channel and frequency.<br>Select Auto to enable auto-channel selection. |
| • **Transmit Power** | The transmission power of the device (value: auto).<br>To meet the regional regulation, this option is not allowed to be configured through the user interface. |
| • **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**". |
| • **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. |
| • **Client Limit** | Specify the maximum clients allowed to connect to the radio interface. |
| • **AP Detection** | AP Detection can select the best channel to use by scanning nearby areas for Access Points. |
| • **Distance (1-30km)** | Specify the distance between the master AP and slave AP. Longer distances may drop high-speed connections. |
| • **Save** | Click **Save** to save changes. |

### 5.1.1 Access Point (AP)

This section allows you to configure the AP Bridge mode to provide wireless connectivity for wireless clients.




Go to the "**Network → Wireless**" page to configure the device as "**Access Point**" and then configure the related wireless settings in the bottom of this page.

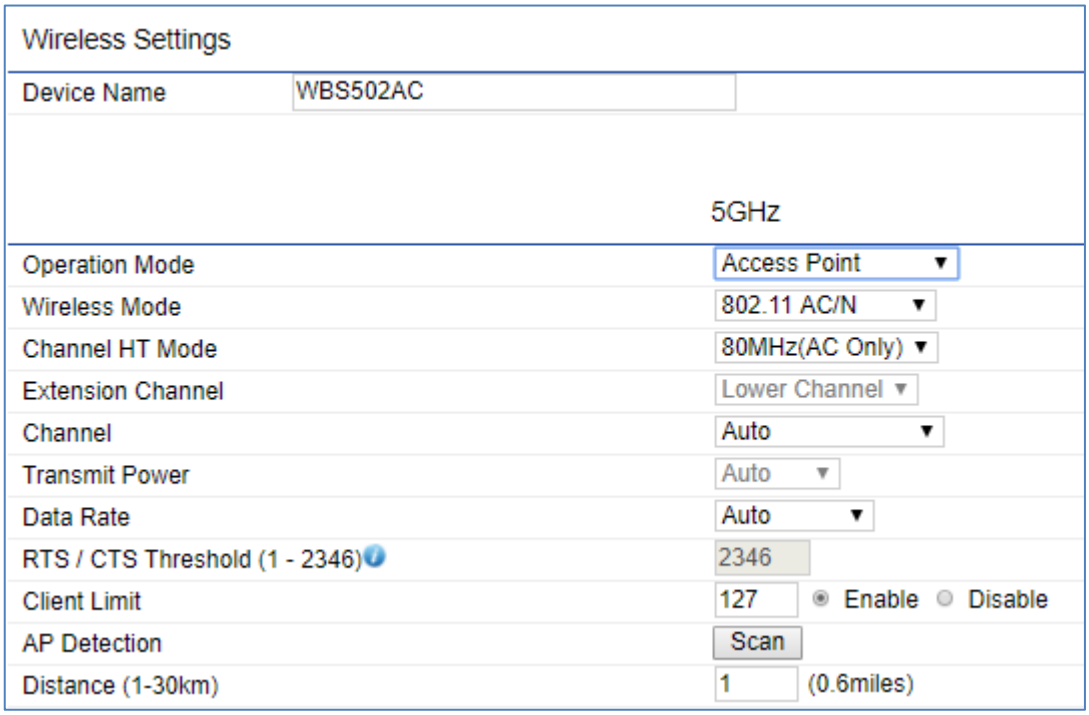
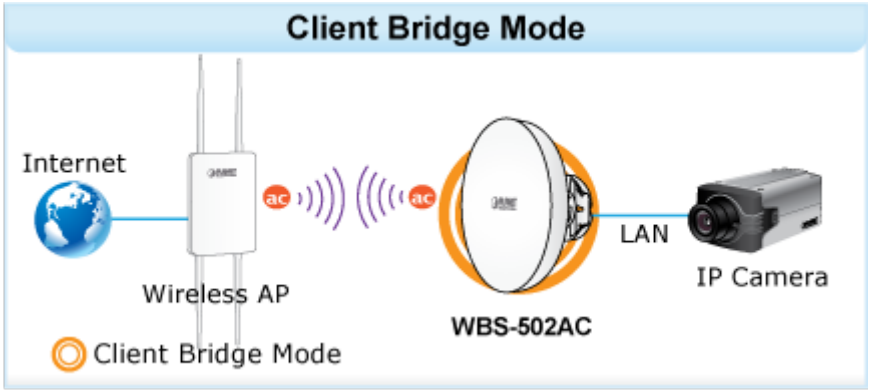



**Figure 5-3** Operation Mode – AP

For the configuration example, please refer to the section "**Appendix C: FAQ, Q1**".

### 5.1.2 Client Bridge (CB)

This section allows you to configure the Client Bridge mode. In this mode, the device enables the wired client to connect to the central site through wireless interface.




Go to the "**Network → Wireless**" page to configure the device as "**Client Bridge**" and then configure the related wireless settings in the bottom of this page.

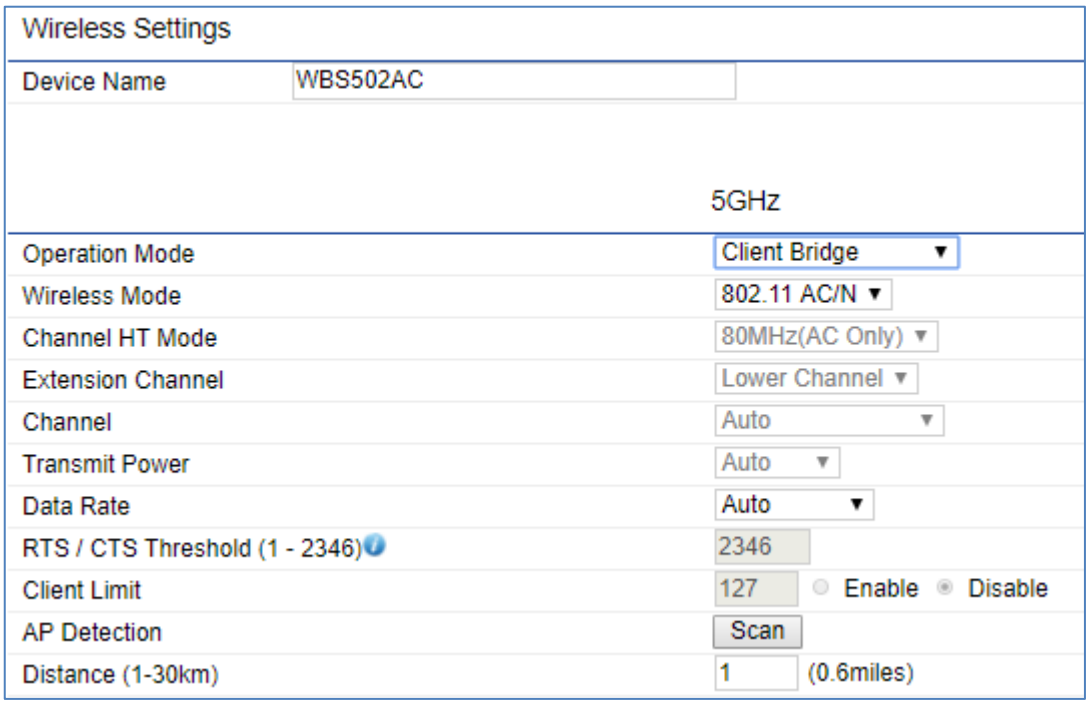
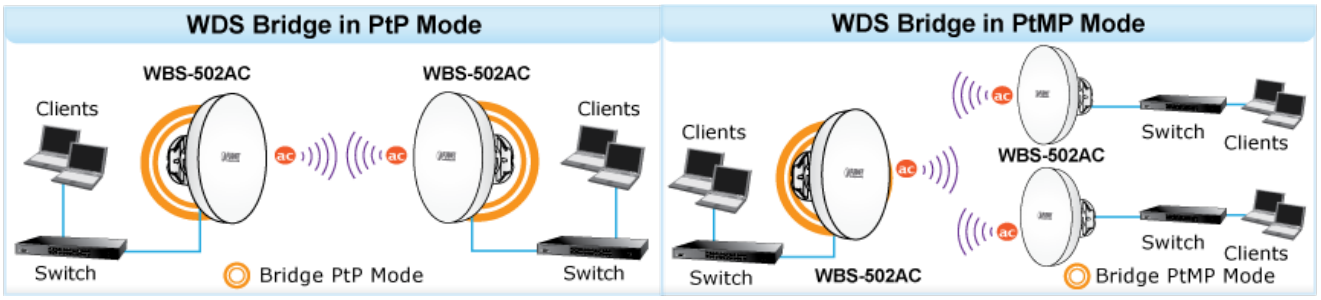



**Figure 5-4** Operation Mode – Client Bridge

For the configuration example, please refer to the section "**Appendix C: FAQ, Q1**".

### 5.1.3 WDS Access Point (WDS AP)

This section allows you to configure the WDS AP mode. In this mode, the device is acting as master AP in the WDS connection.




Go to the "**Network → Wireless**" page to configure the device as "**WDS Access Point**" and then configure the related wireless settings in the bottom of this page.

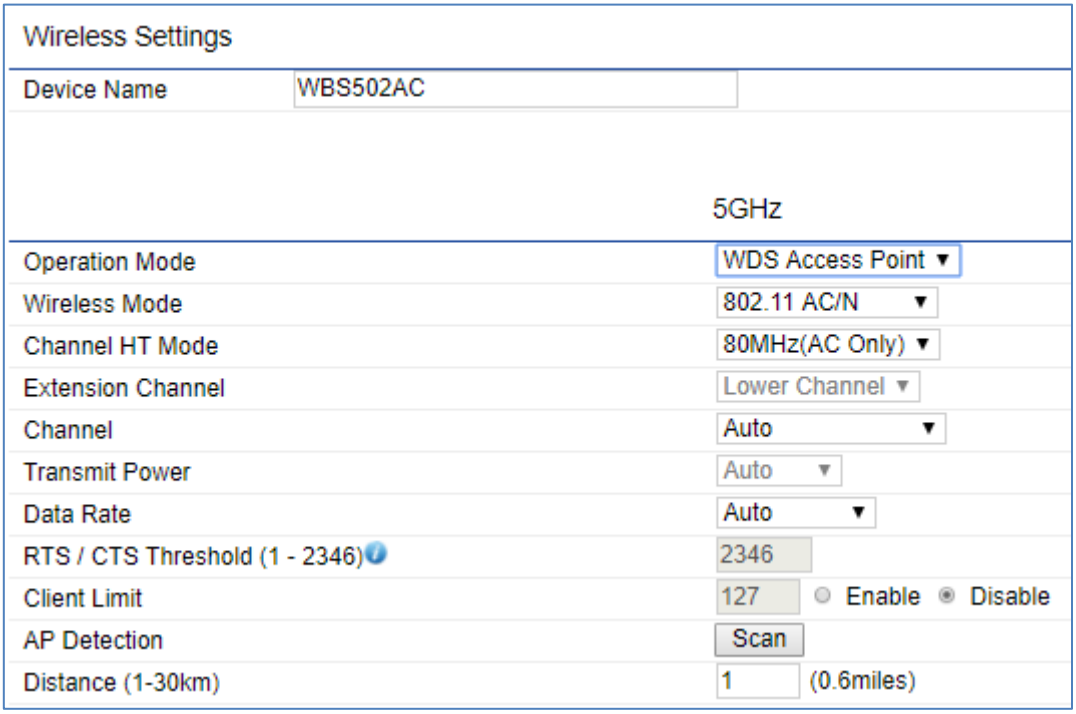
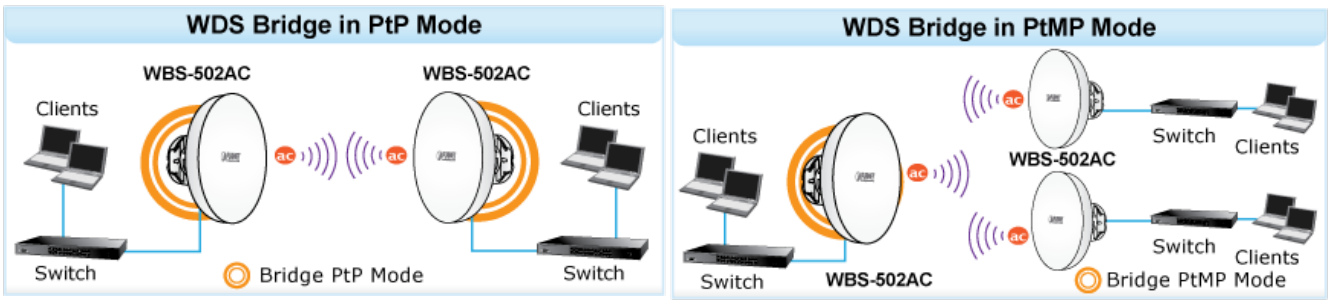



**Figure 5-5** Operation Mode – WDS AP

For the configuration example, please refer to the section "**Appendix C: FAQ, Q2**".

### 5.1.4 WDS Station (WDS STA)

This section allows you to configure the WDS Station mode. In this mode, the device is acting as slave AP in the WDS connection.




Go to the "**Network → Wireless**" page to configure the device as "**WDS Station**" and then configure the related wireless settings in the bottom of this page.

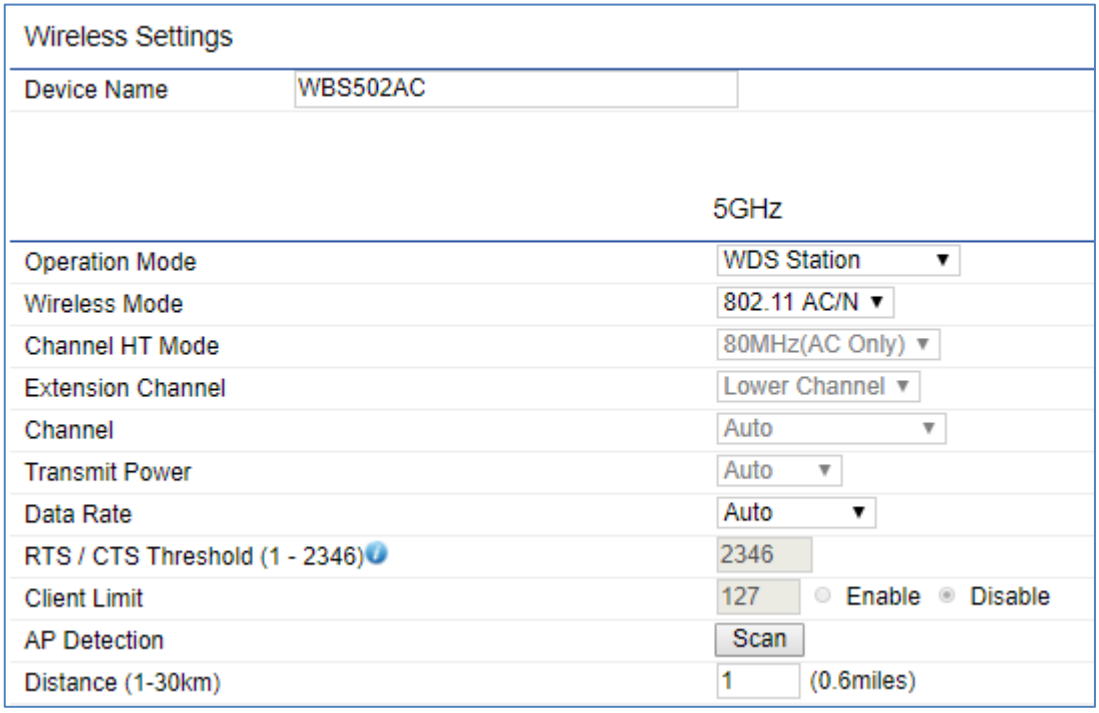
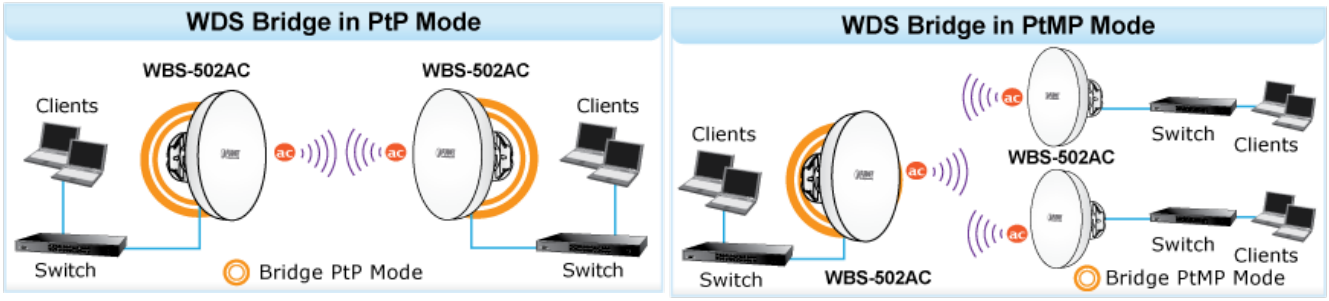



**Figure 5-6** Operation Mode – WDS Station

For the configuration example, please refer to the section "**Appendix C: FAQ, Q2**".

### 5.1.5 WDS Bridge (WDS PtP/WDS PtMP)

This section allows you to configure the WDS Bridge mode. In this mode, the device is bridging to remote node through wireless MAC address.




Go to the "**Network → Wireless**" page to configure the device as "**WDS Bridge**" and then configure the related wireless settings in the bottom of this page.

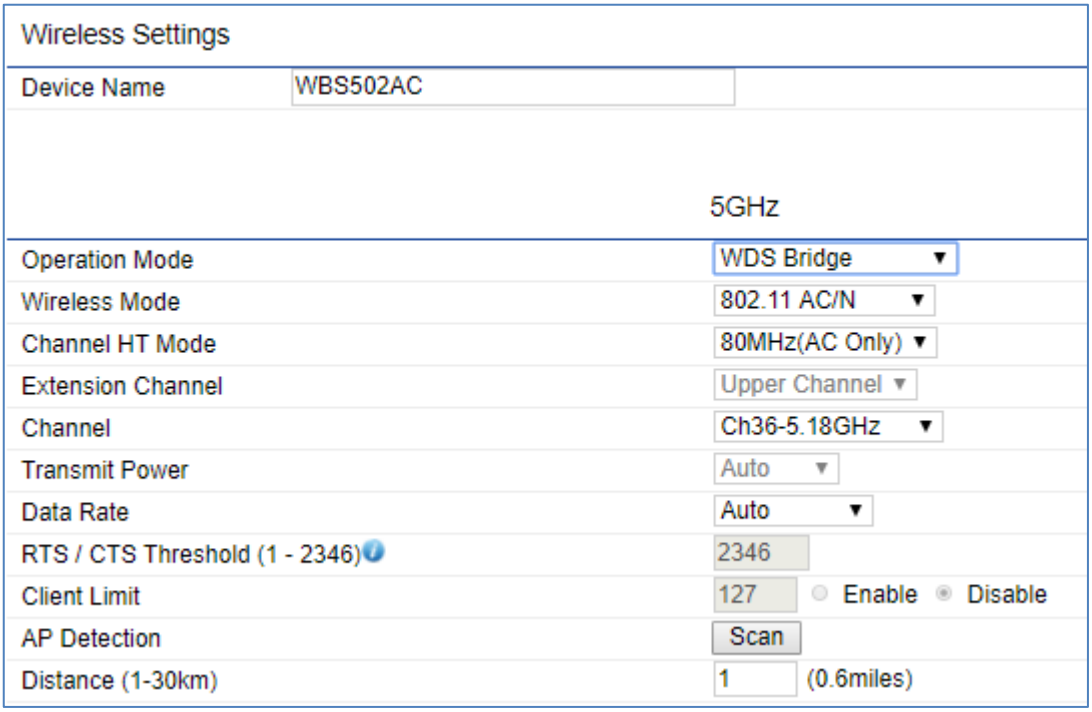
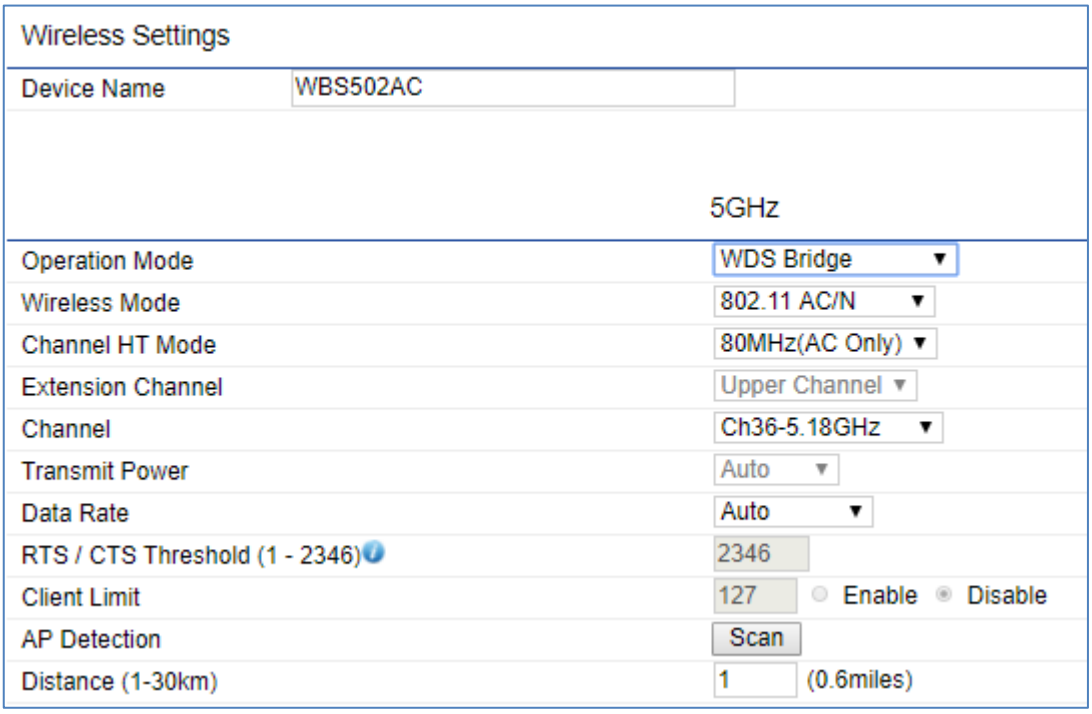



**Figure 5-7** Operation Mode – WDS Bridge

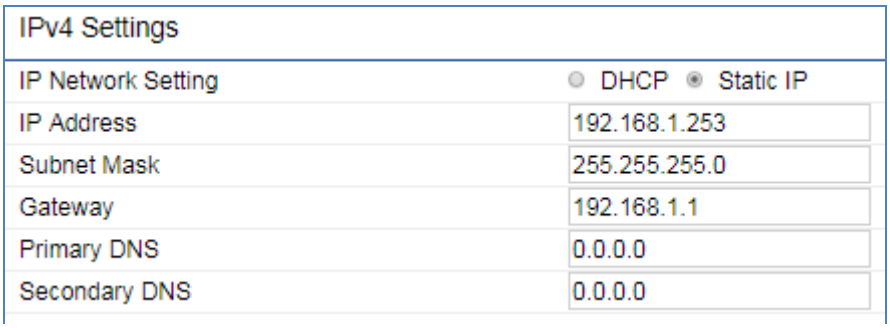
*Configuration Example*

The following procedure will guide you to how to establish WDS connection.

**Step 1**. Go to the "**Network → Wireless**" page to configure the device as "**WDS Bridge**".




**Step 2**. Go to the "**Network → Basic**" page to configure LAN IP of central site and remote site. The LAN IP must be different at both sites. In this example, the master AP at central site is configured to 192.168.1.252 and the slave AP at remote site is configured to 192.168.1.253.




**Step 3**. Go to the "**Network → Wireless**" page to configure the wireless parameters of the WDS link.
In this example, we fixed the channel to 36 and channel width to 80MHz.

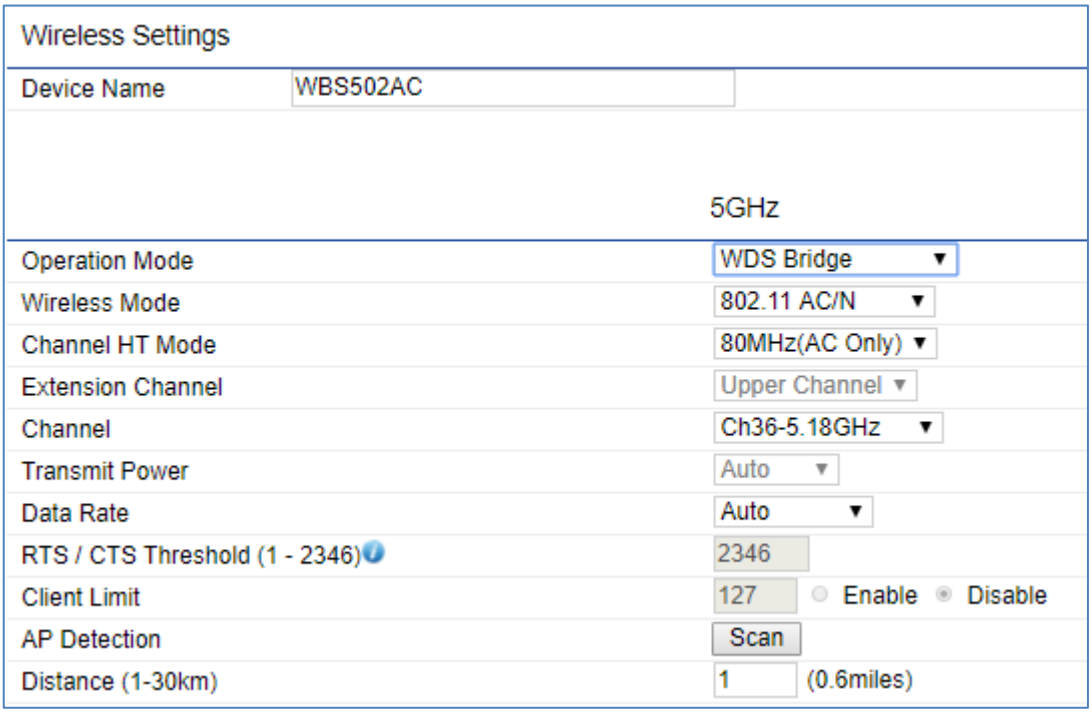
(1) Channel HT Mode: Set to 80MHz for wider bandwidth to optimize performance

(2) Channel/Frequency: Set to a fixed channel for the WDS link.

(3) Distance:

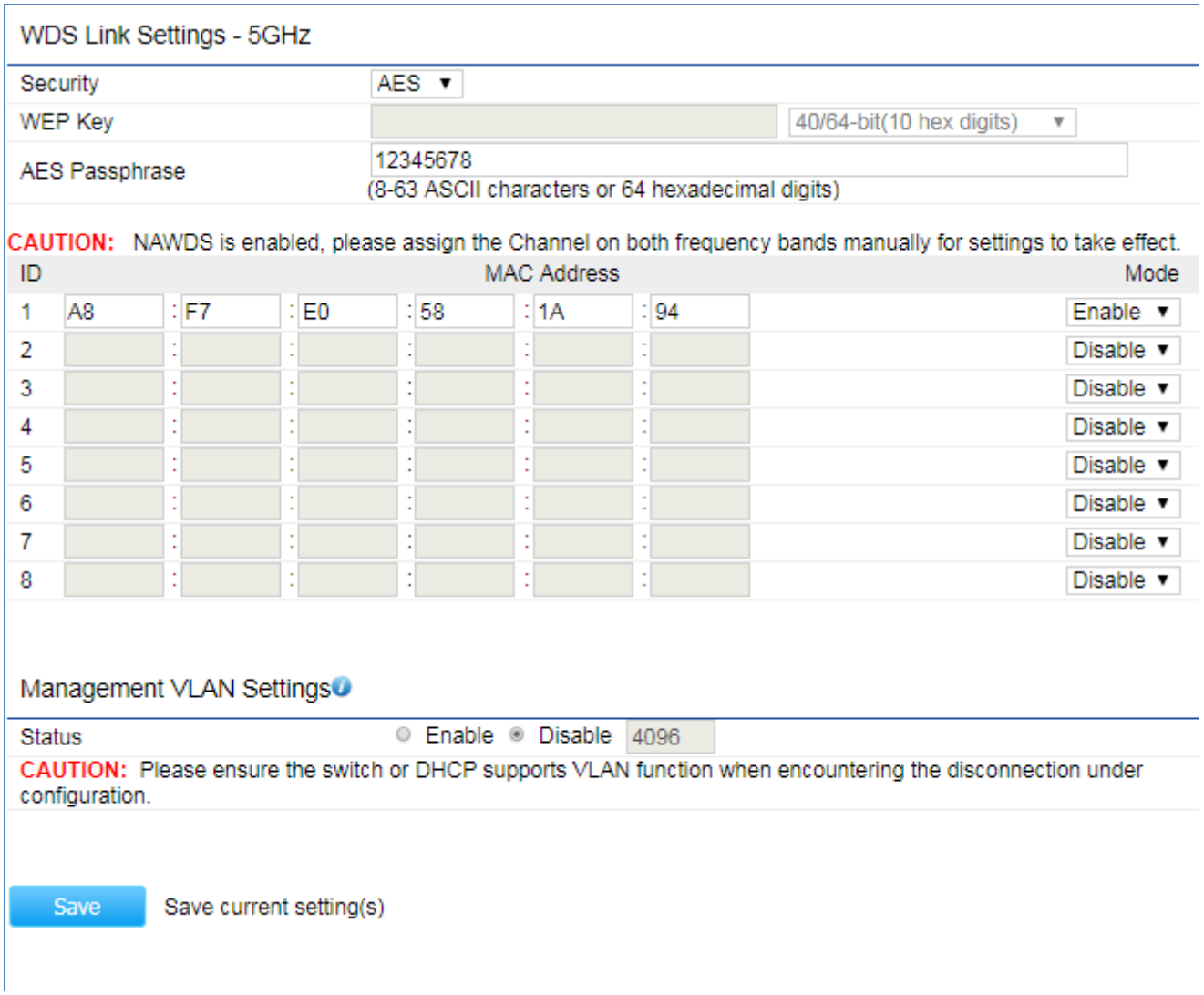
a. In PtP: The distance must be configured to the same at both sites.

b. In PtMP: The distance at each slave node must be configured to the actual distance from each slave node to the master node. The master node should be configured to the value of the farthest node. In PtMP application, the distance from each node to master node should not have too much deviation to ensure the connection stability.

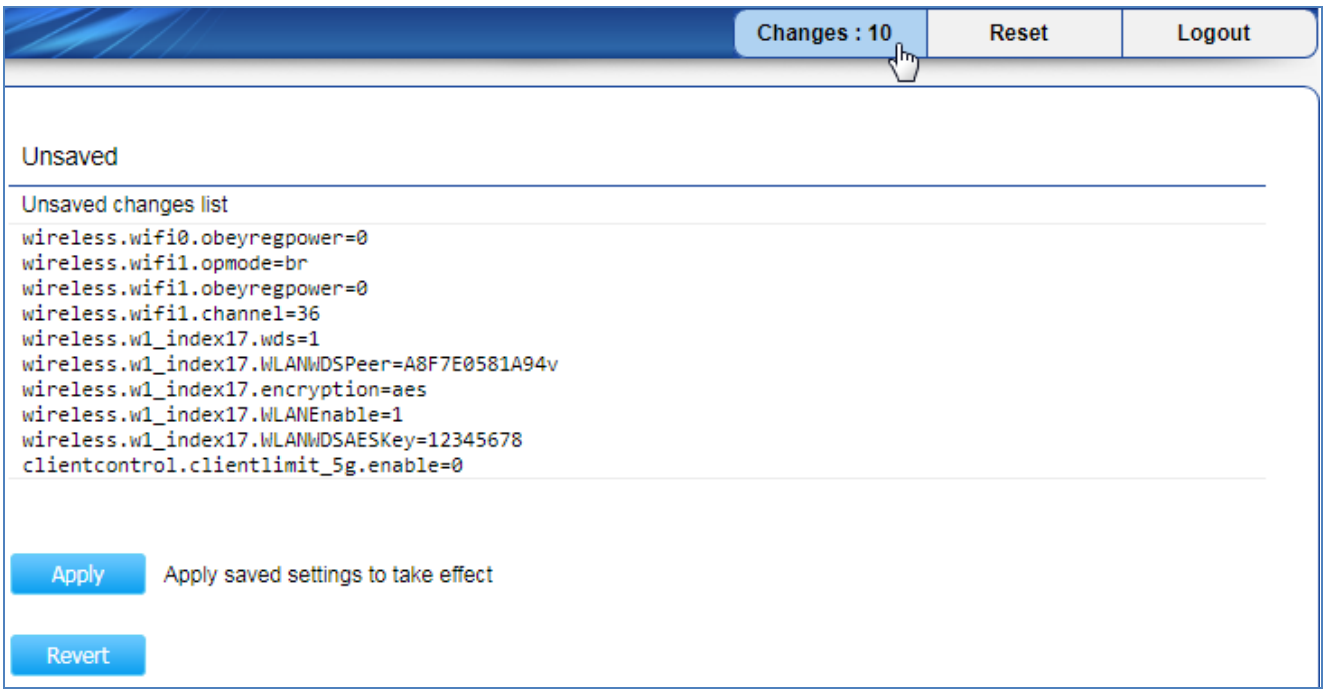



**Step 4**. In the "**WDS Link Settings**" section, select the mode of ID1 to enable it and enter the wireless MAC of the remote node. Then, add encryption to protect the WDS link. Click **Save** to save the changes.

※ In PtMP of the master node: Enter the wireless MAC of each remote slave node (up to 8 entries).

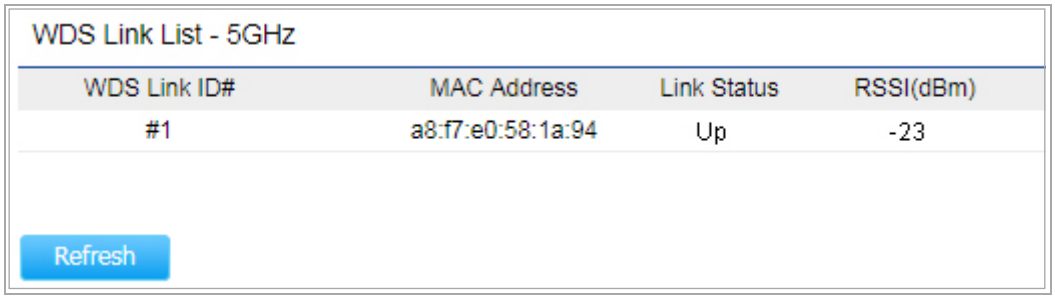



**Step 5**. In the upper-right corner of the page, click "**Changes**" to apply settings.



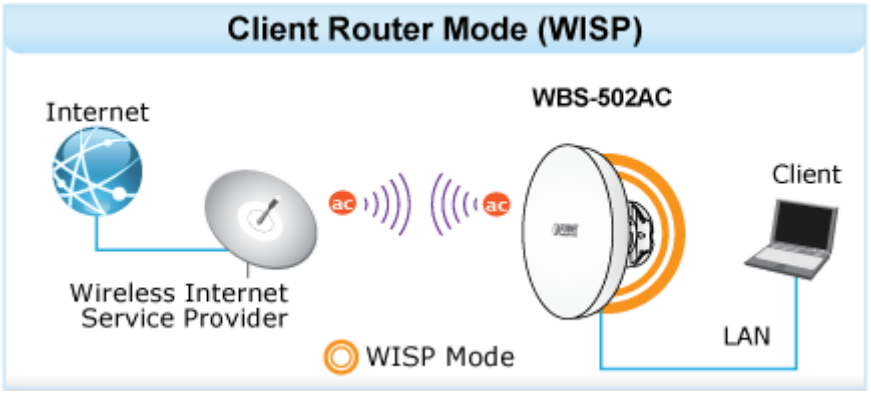
**Step 6**. Repeat Step1 to 5 for each node.

**Step 7**. Go to the "**Overview -> Connections**" page to check the connection status.



### 5.1.6 Client Router (CR/WISP)

This section allows you to configure the Client Router (Wireless ISP) mode to enable clients to access Internet through remote wireless AP provided by ISP. In this mode, the DHCP server is enabled and able to assign IP address to local clients after the device is connected to remote wireless AP provided by ISP.




Go to the "**Network → Wireless**" page to configure the device as "**Client Router**" and then configure the related wireless settings in the bottom of this page.

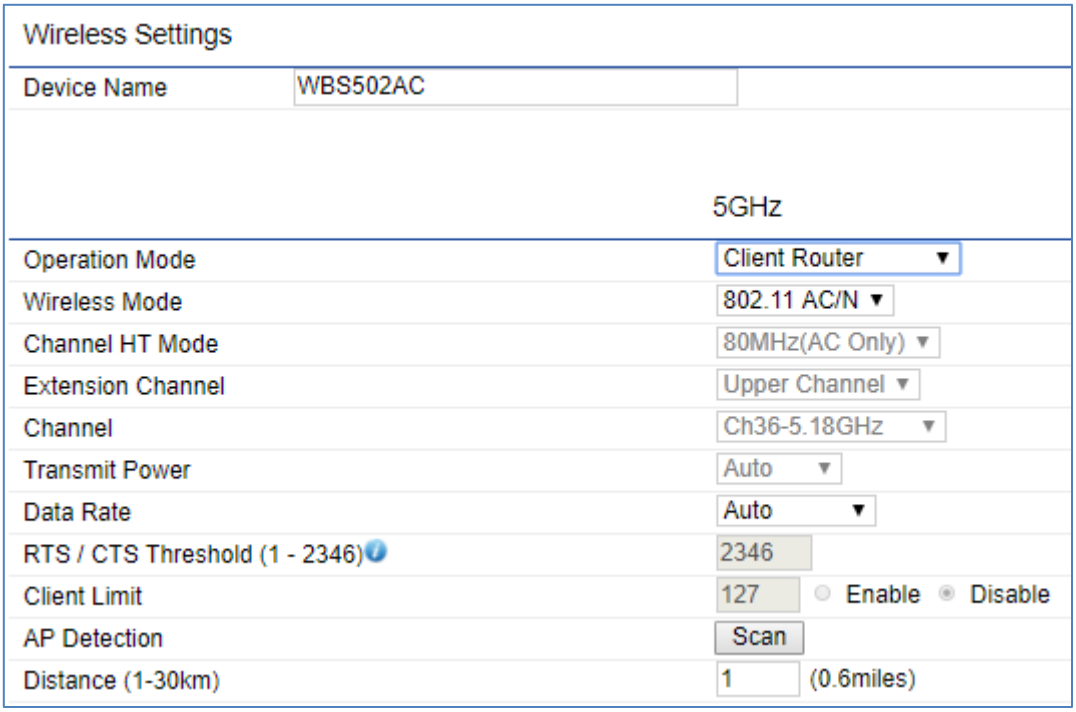
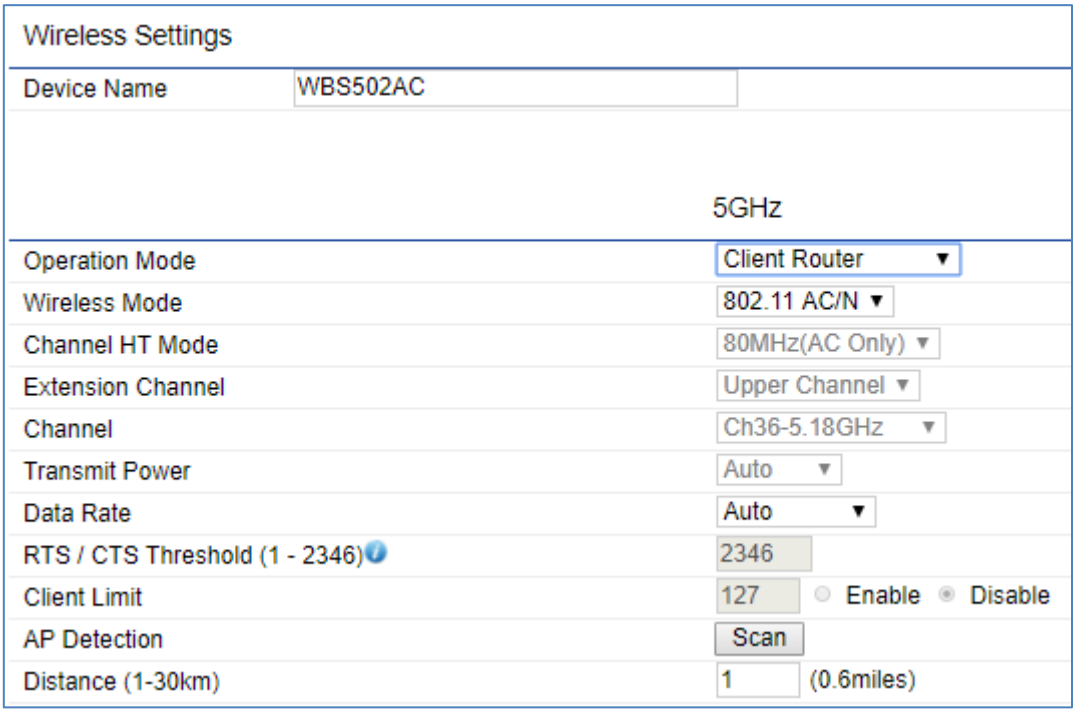



**Figure 5-8** Operation Mode – Client Router (WISP)

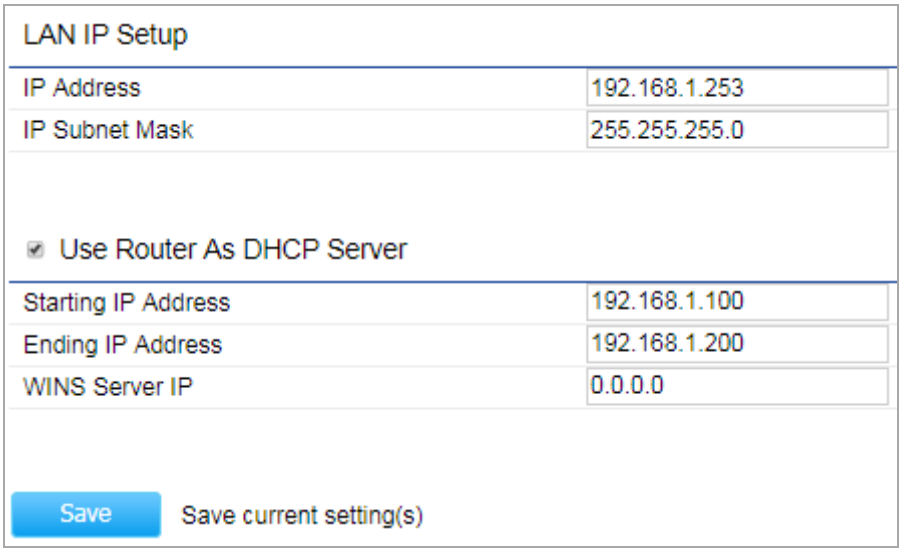
*Configuration Example*

The following procedure will guide you to how to establish WISP connection.

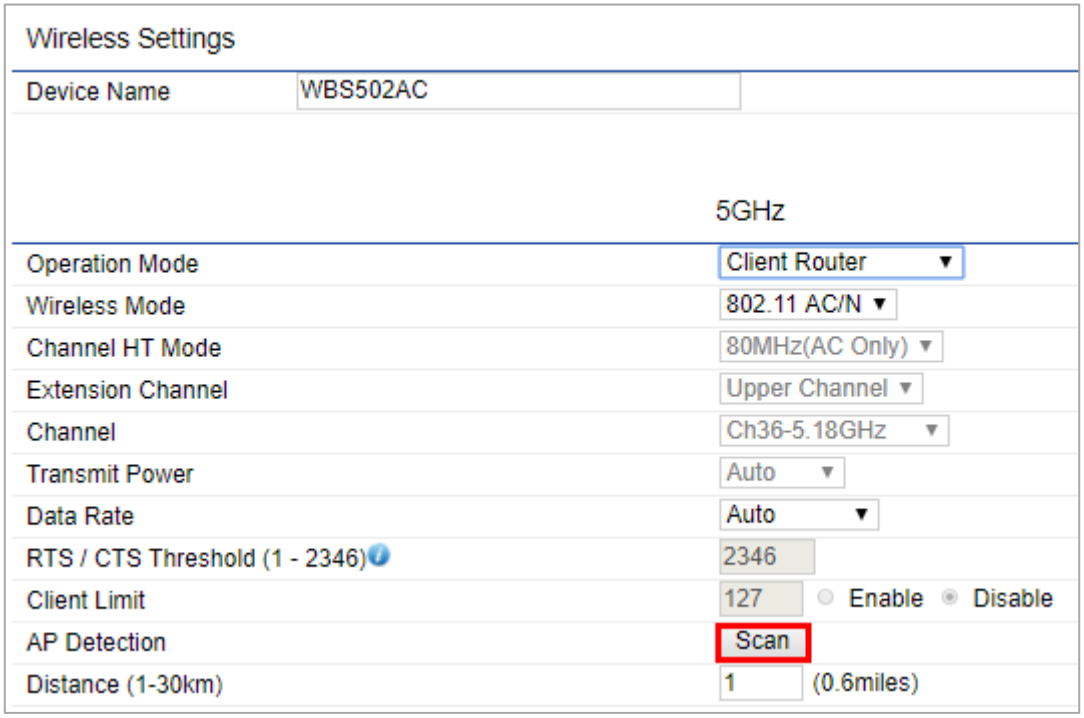
**Step 1**. Go to the "**Network → Wireless**" page to configure the device as "**Client Router**".



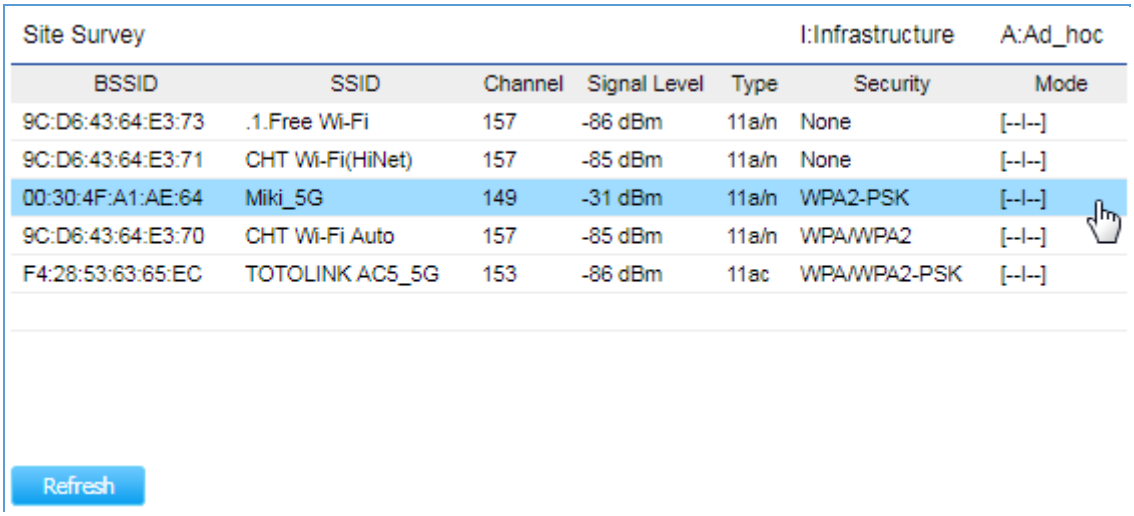

**Step 2**. Go to the "**Router → LAN Settings**" page to configure LAN IP and enable the DHCP server. The LAN IP must be a different subnet from the remote wireless AP provided by ISP.



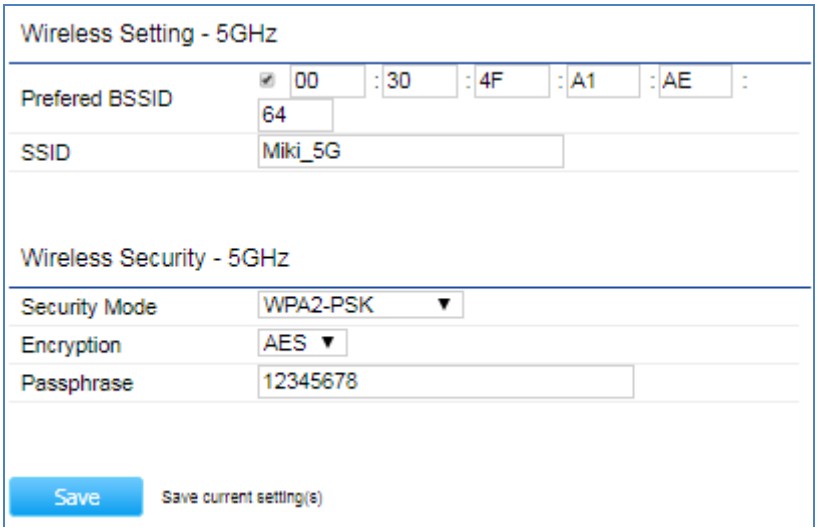

**Step 3**. Go to the "**Network → Wireless**" page and click the **Scan** button to discover the root AP.



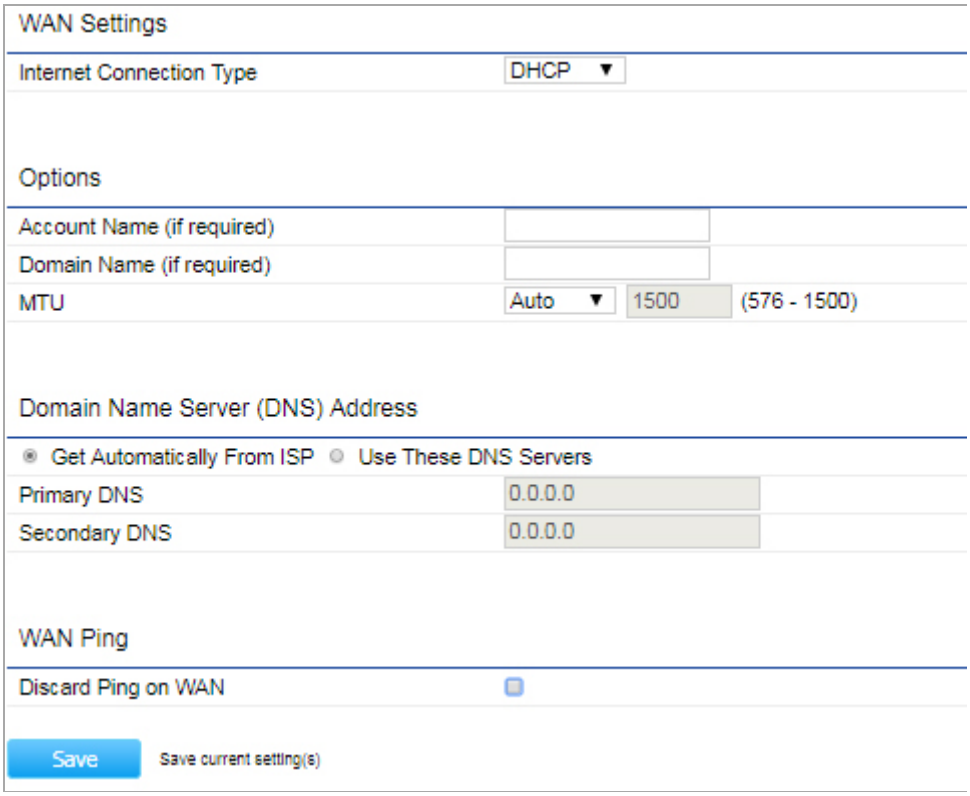

**Step 4**. Click the **root AP** as shown below and it will go back to the previous wireless network page.



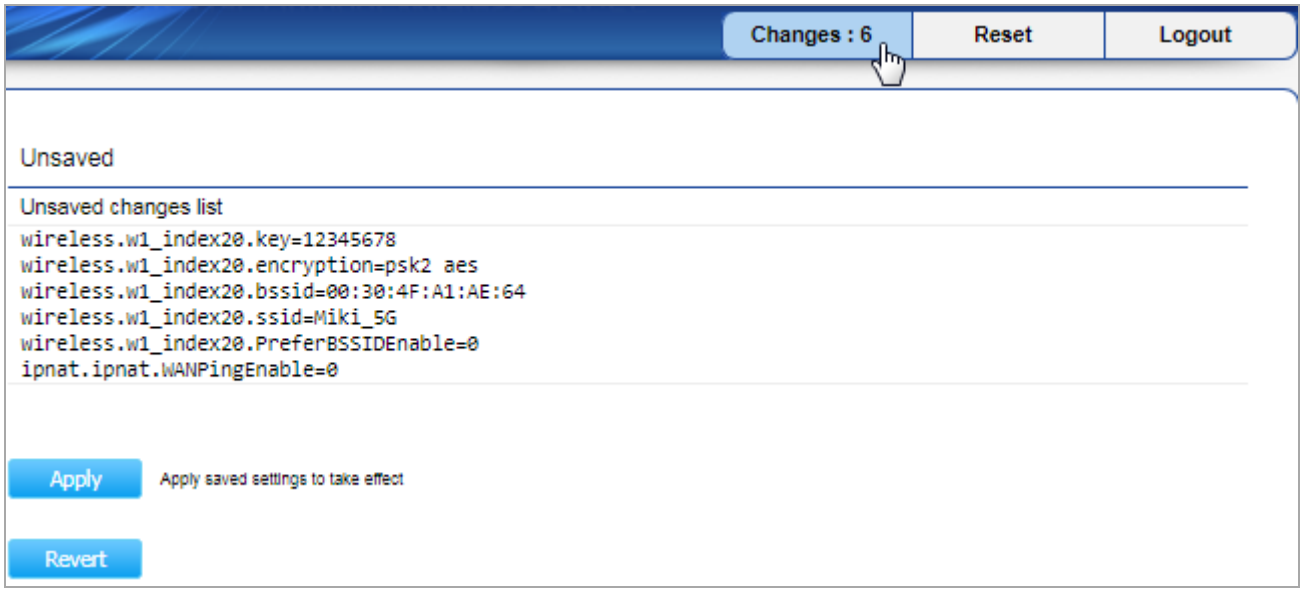

**Step 5**. Click the check box of the preferred BSSID and configure the encryption same as the root AP. Then, click "**Save**" to save the configurations.



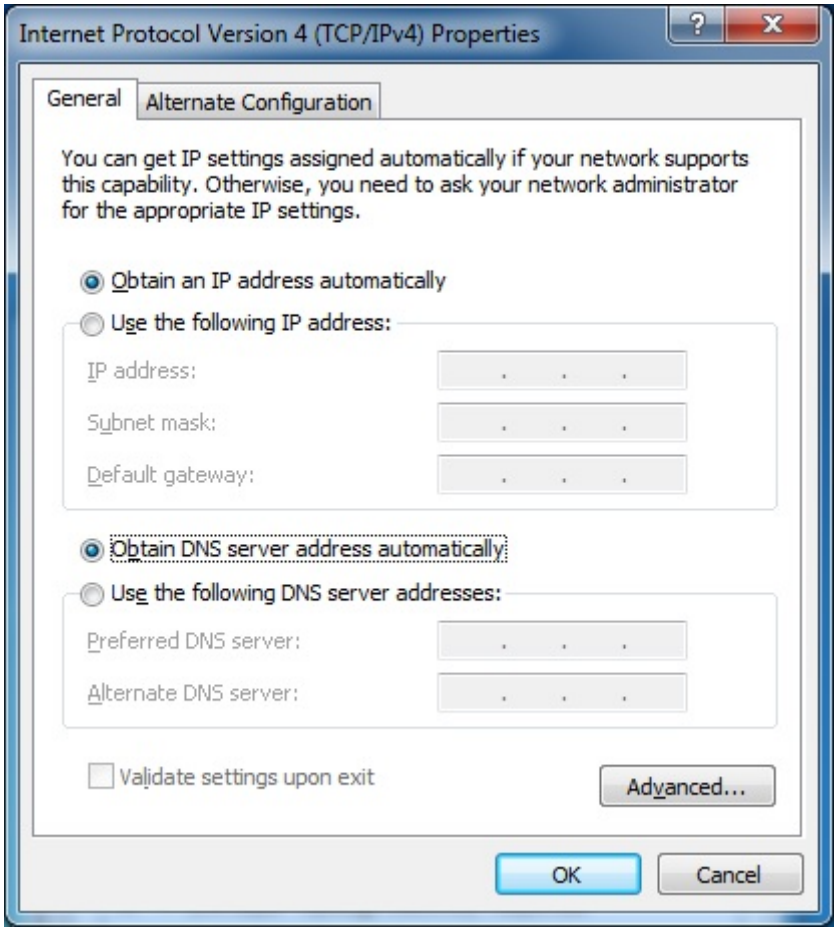

**Step 6**. Go to the "**Router -> WAN Settings**" page to configure WAN settings. The Internet connection type is provided by your ISP and should be configured properly. Disable "**Discard Ping on WAN**" and then you'll be able to use ping test tool of Diagnostics page to ping DNS to ensure the WAN connection is established properly in WISP mode.



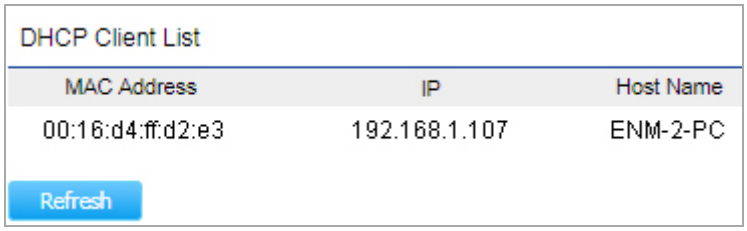
**Step 7**. In the upper-right corner of the page, click "**Changes**" to apply settings.




**Step 8**. Modify your PC/laptop connected to the LAN port of this client router to "**Obtain an IP address automatically**".



**Step 9**. Go to "**Overview -> DHCP Client Table**" to ensure your PC/laptop received the IP automatically.

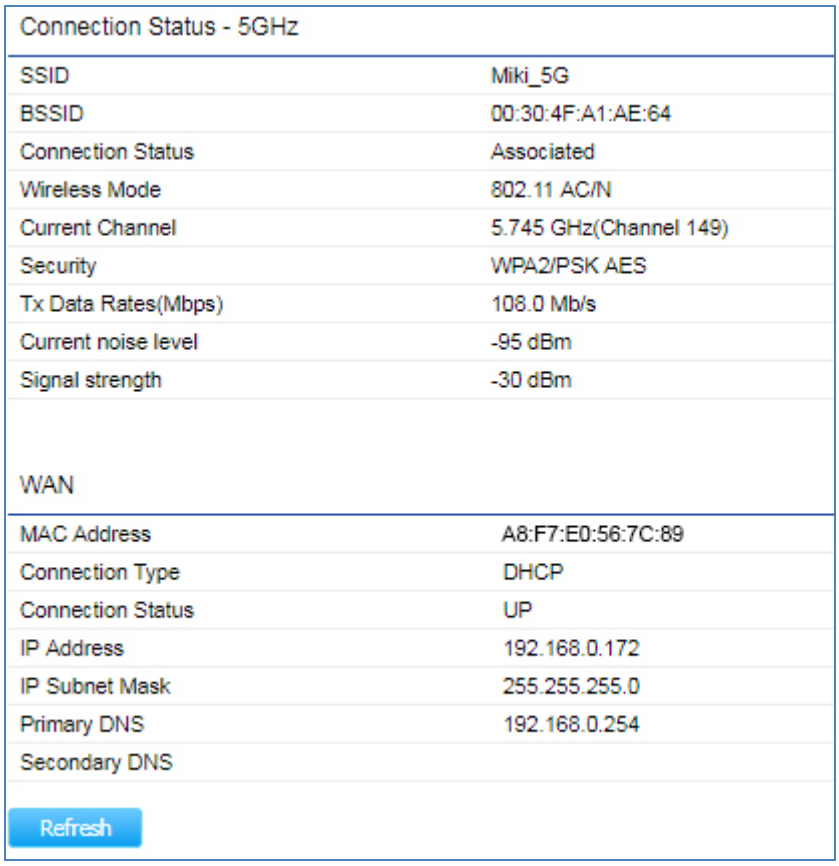


DHCP Client List

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

Refresh

**Step 10.** Go to "**Overview -> Connections**" to check whether the connection is established successfully.



Connection Status - 5GHz

| | |
|---|---|
| SSID | Miki_5G |
| BSSID | 00:30:4F:A1:AE:64 |
| Connection Status | Associated |
| Wireless Mode | 802.11 AC/N |
| Current Channel | 5.745 GHz(Channel 149) |
| Security | WPA2/PSK AES |
| Tx Data Rates(Mbps) | 108.0 Mb/s |
| Current noise level | -95 dBm |
| Signal strength | -30 dBm |

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 | |

Refresh

## 5.2 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.

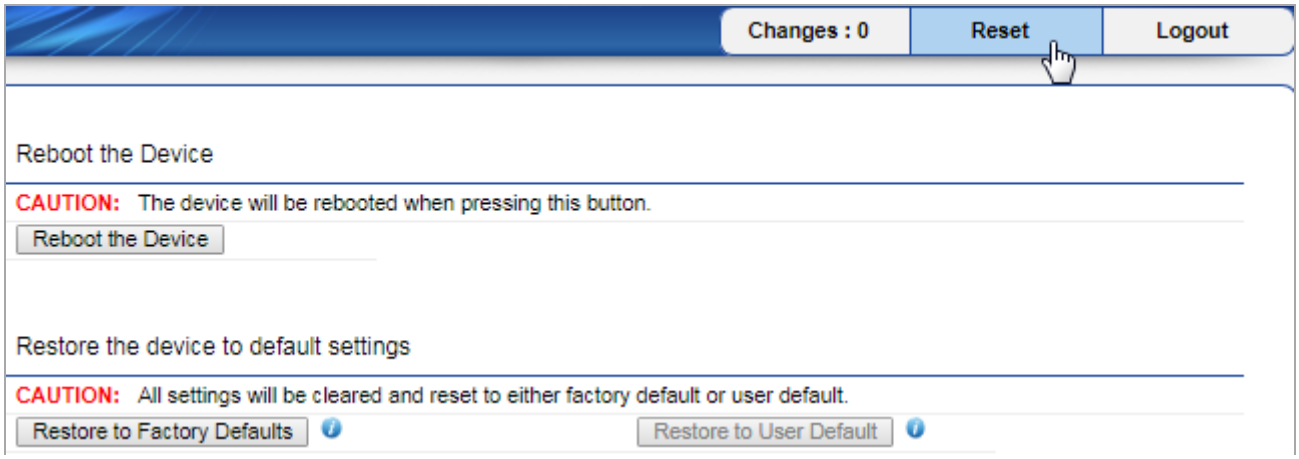



**Figure 5-9** System Menu - Reset

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.

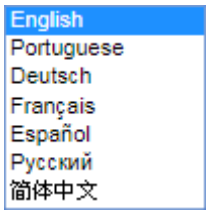



**Figure 5-10** System Menu – Language option

### 5.2.1 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.) |

Refresh

**Figure 5-11** 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. |

### 5.2.2 Changes

Click "**Changes**" and the following page will be displayed.

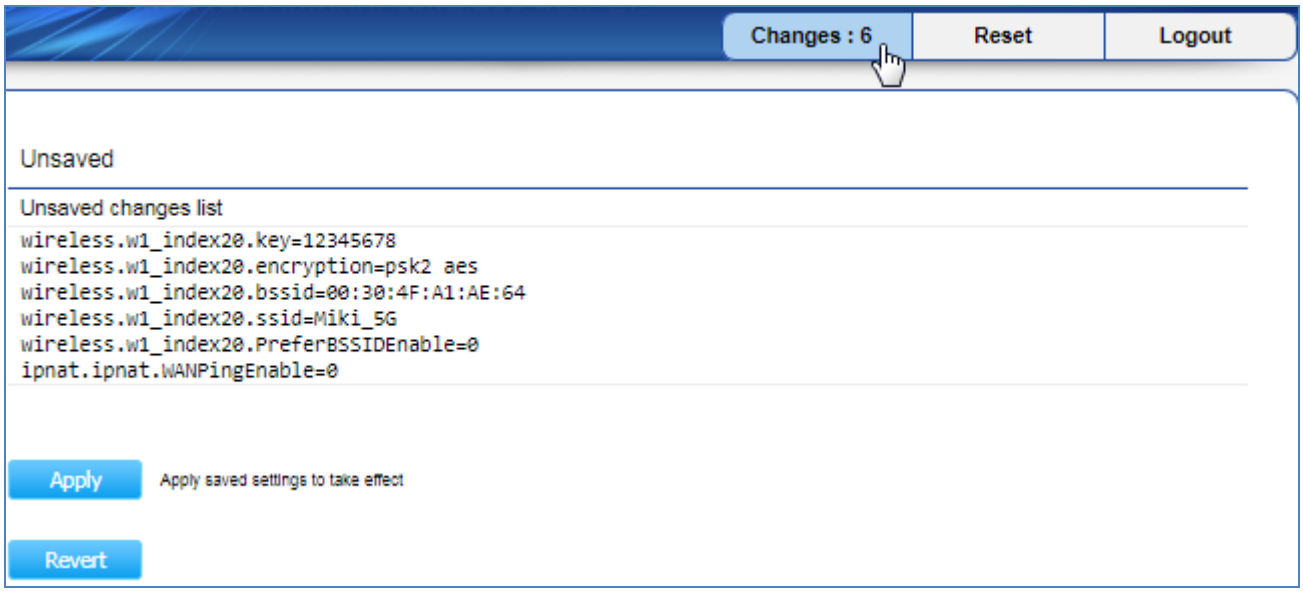



**Figure 5-12** Changes

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.

### 5.2.3 Wireless Client List

Click "**Overview → Connections**" to view the current associated client.

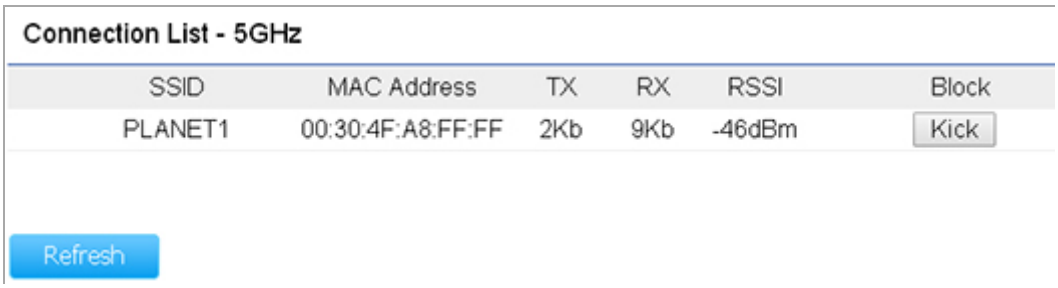



**Figure 5-13** Wireless Client List

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. |

### 5.2.4 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.

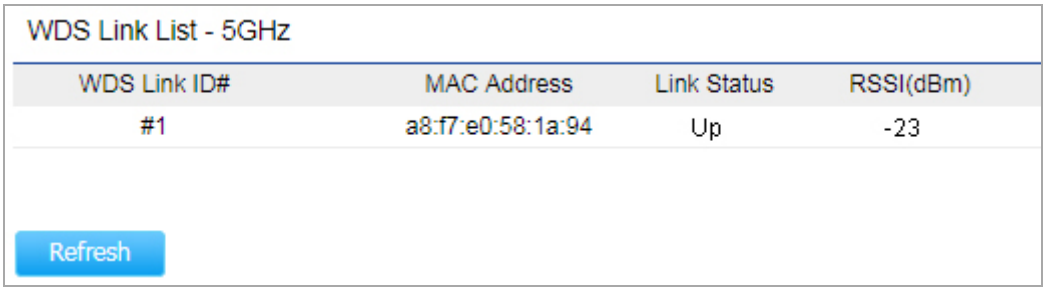



**Figure 5-14** WDS Link Status

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. |

### 5.2.5 DHCP Client Table

Click "**Overview -> DHCP Client Table**" to view the current DHCP client.

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

**Figure 5-15** 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. |

### 5.2.6 Connection Status

Click "**Overview → Connections**" to view the current association status.

The **Connection Status** is only available in the following operation modes:

(1) Client Bridge

(2) Client Router

(3) WDS Station

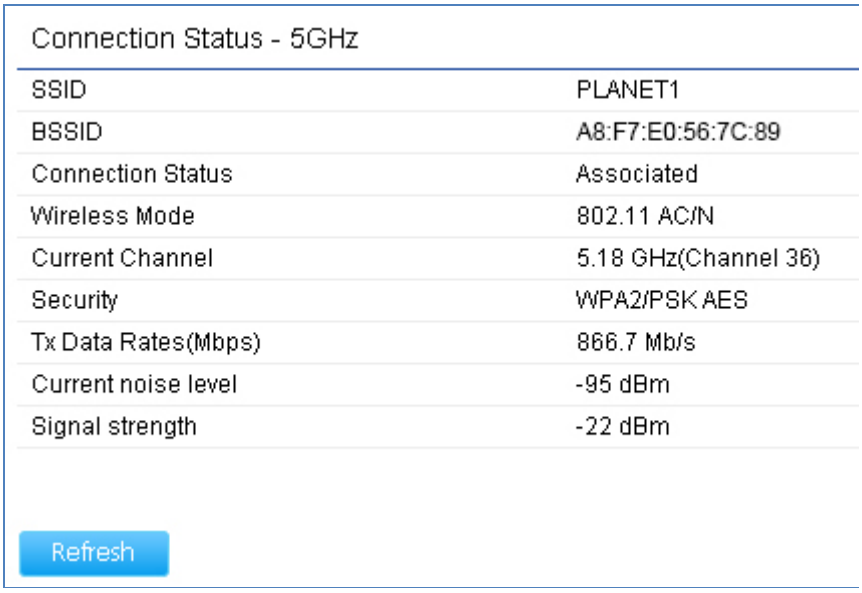



**Figure 5-16** Connection Status

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. |

## 5.3 Network

### 5.3.1 IP Settings

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

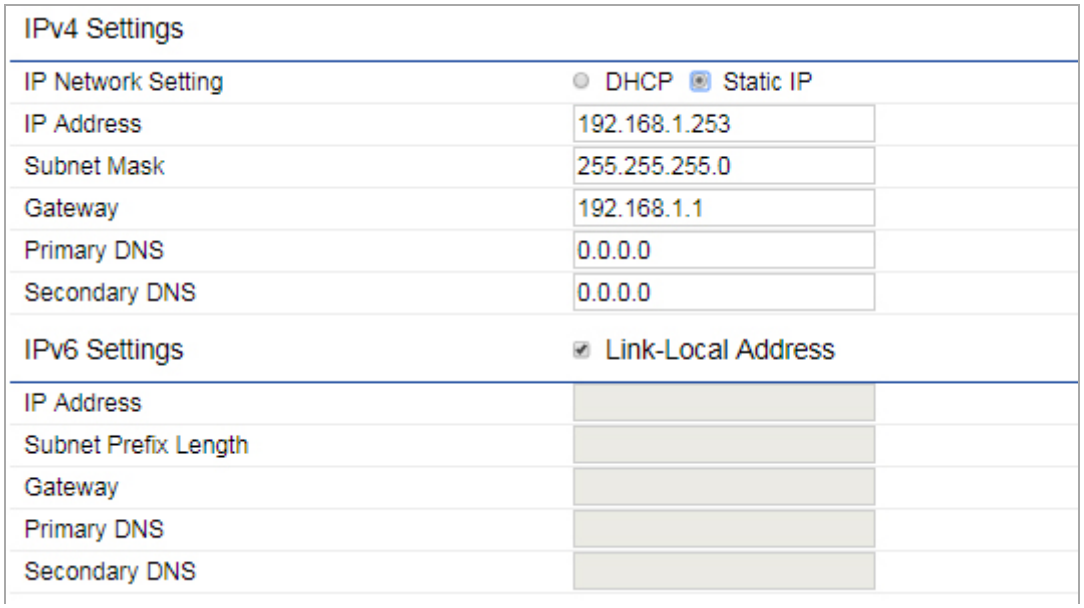



**Figure 5-17** LAN IP Settings

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.<br>Select **Specify an IP address** to configure the AP to use static IP. |
| • **IP Address** | The LAN IP of the AP.<br>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. |

### 5.3.2 Spanning Tree Settings

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

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

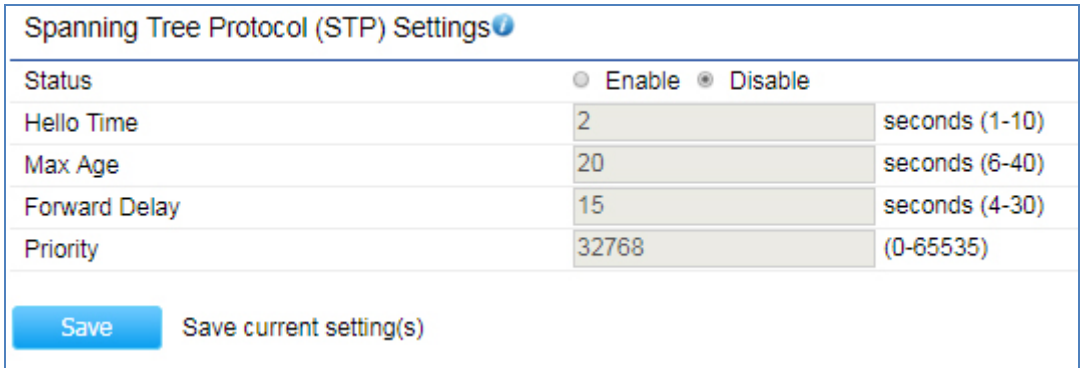



**Figure 5-18** Spanning Tree Settings

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. |

## 5.4 Router (WISP Mode Only)

### 5.4.1 DHCP Server Settings

Go to the "**Network → Wireless**" page to configure the device as "**Client Router**" and then go to "**Router → LAN Settings**" to configure the device's LAN IP settings in client router mode.

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.

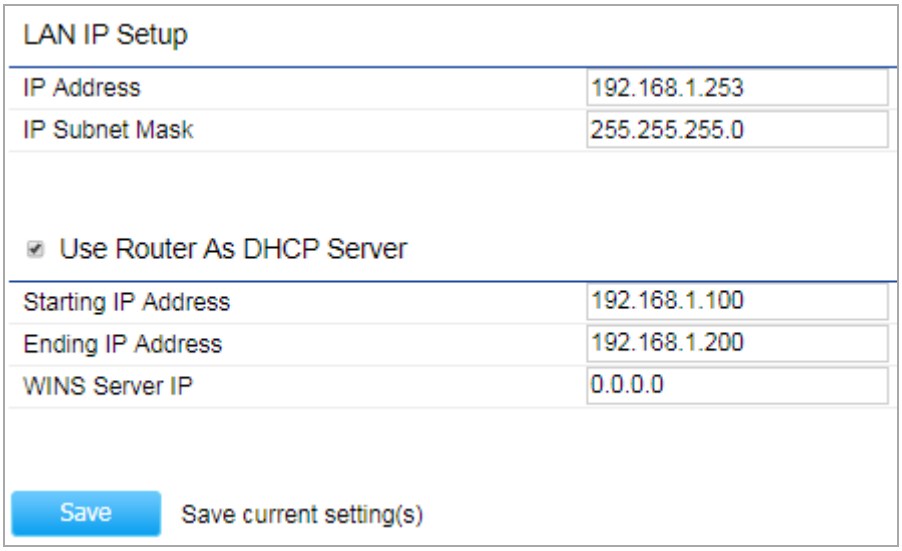



**Figure 5-19** DHCP Server Settings

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. |

### 5.4.2 WAN Settings

Go to the "**Network → Wireless**" page to configure the device as "**Client Router**" and then go to "**Router → WAN Settings**" to configure the device's WAN settings in client router mode. The WAN settings should be provided by the ISP.

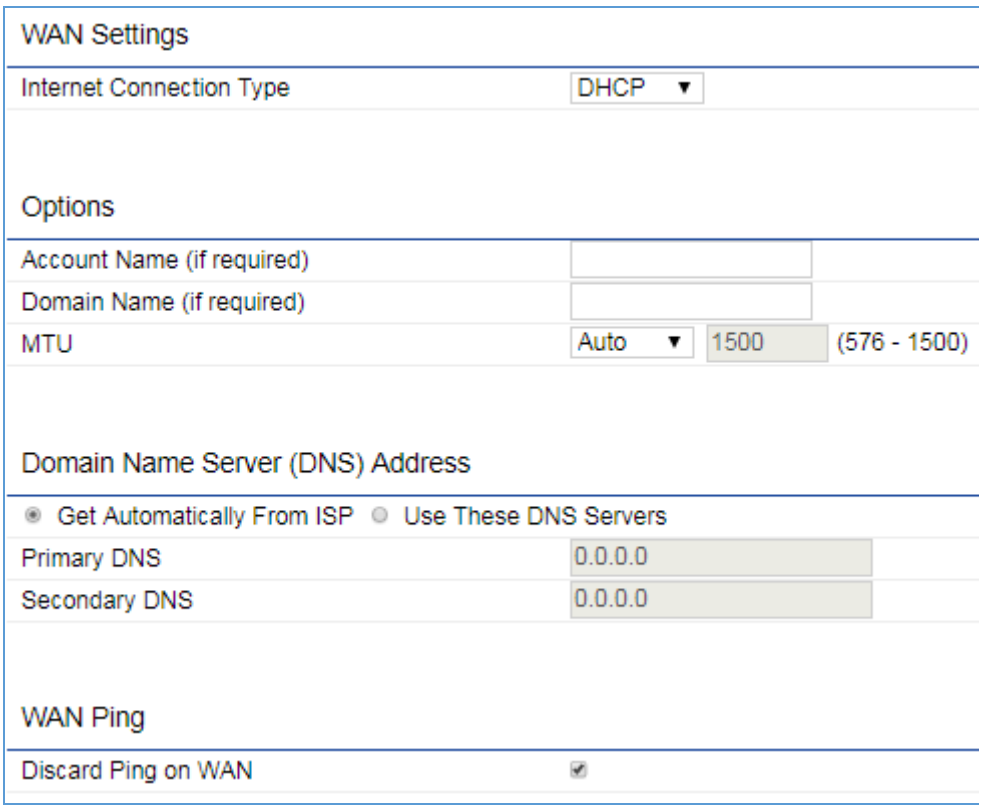



**Figure 5-20** WAN Settings – All

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

| Object | Description |
|---|---|
| • **Internet Connection Type** | • **DHCP:** Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider.<br>• **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.<br>• **PPPoE:** Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet.<br>• **PPTP:** The Point-to-Point Tunneling Protocol (PPTP) is used in association with virtual private networks (VPNs). |
| **Option:** This section may vary depending on the Internet Connection Type.<br>Refer to settings of each corresponding section from 5.4.2.1 to 5.4.2.4 | |
| **Domain Name Server (DNS) Address** | |
| • **Get Automatically From ISP** | Select it to obtain the DNS automatically from the DHCP server. |
| • **Use These DNS Servers** | Select it to set up the Primary DNS and Secondary DNS servers manually. |
| • **Primary DNS** | Enter the primary DNS server address. |
| • **Secondary DNS** | Enter the secondary DNS server address. |
| **WAN Ping** | |

| | |
|---|---|
| • **Discard Ping on WAN** | Check it to enable pings on the WAN interface or disable to block pings on the WAN interface. |

#### 5.4.2.1. DHCP

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

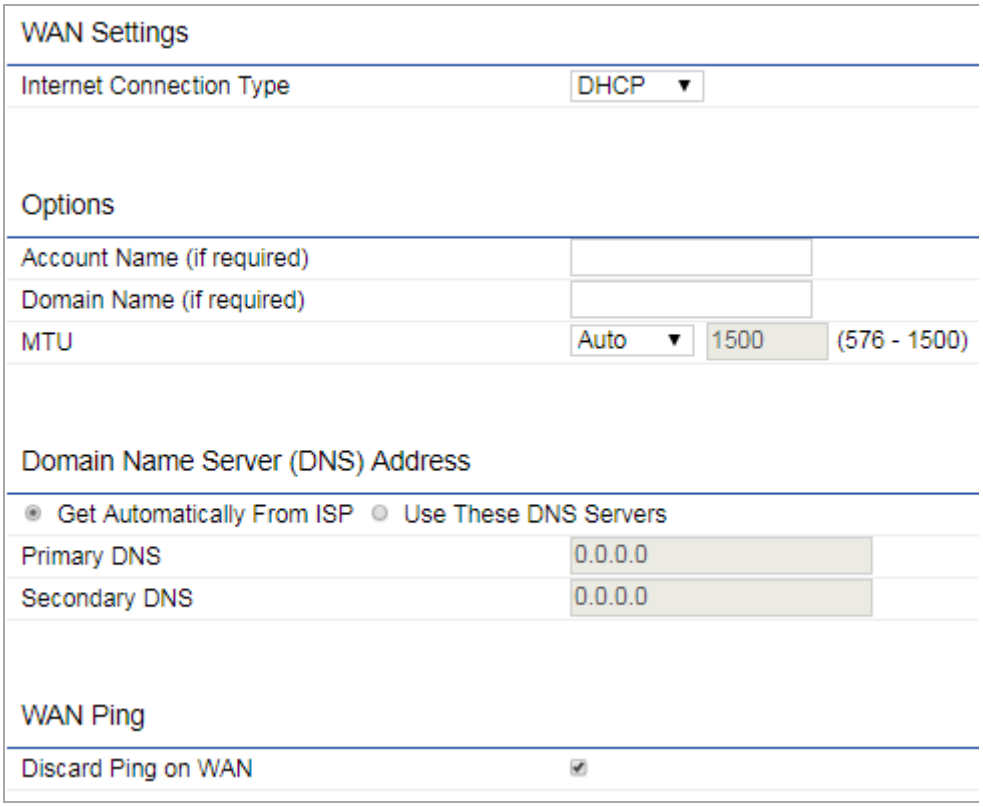



**Figure 5-21** WAN Settings – DHCP

The page includes the following specific settings in DHCP 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 DHCP is 1500. The MTU size can be set between 576 and 1500. |

#### 5.4.2.2. 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.

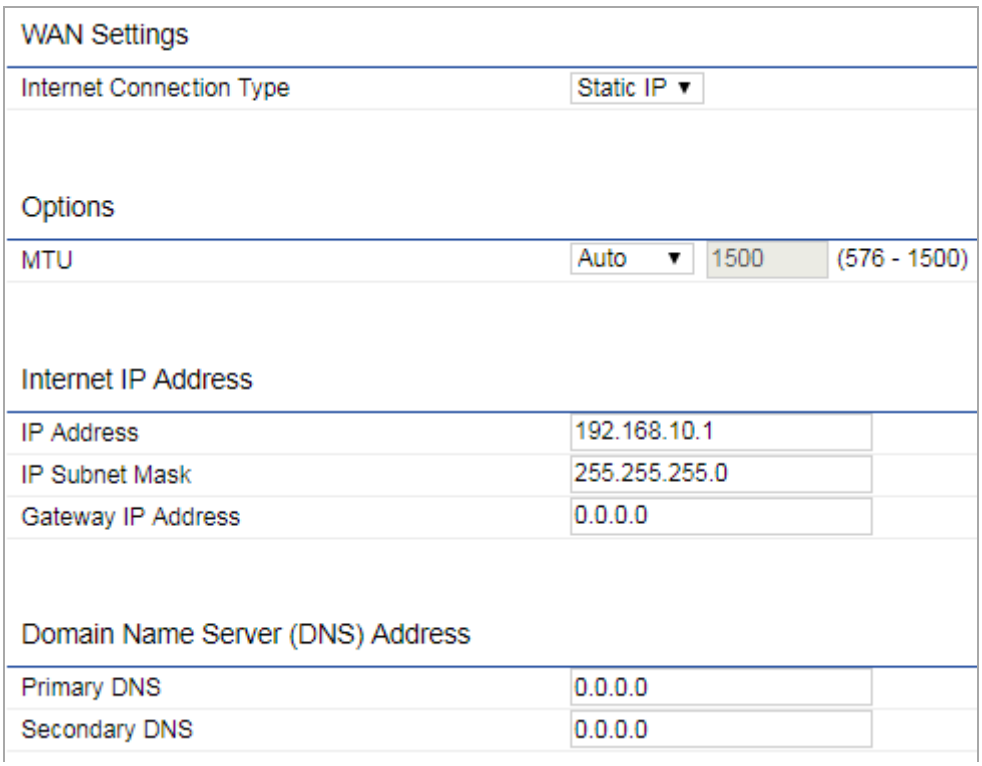



**Figure 5-22** WAN Settings – Static IP

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. |

#### 5.4.2.3. PPPoE

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

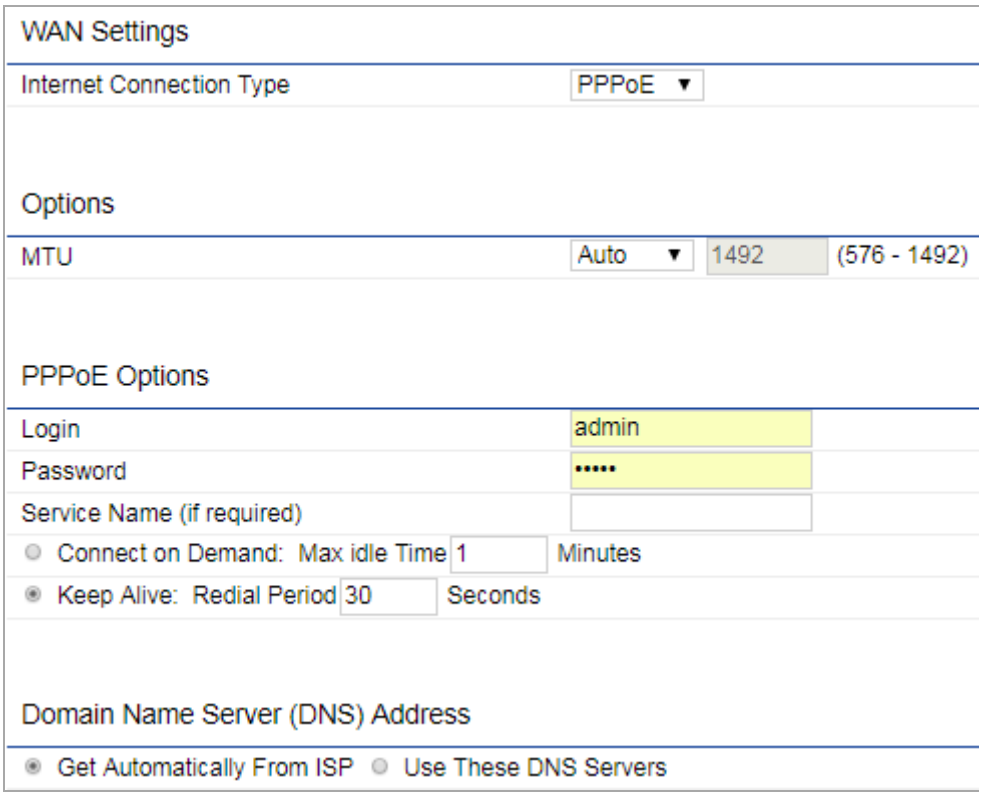



**Figure 5-23** WAN Settings – PPPOE

The page includes the following specific settings in PPPoE type:

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

#### 5.4.2.4. PPTP

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

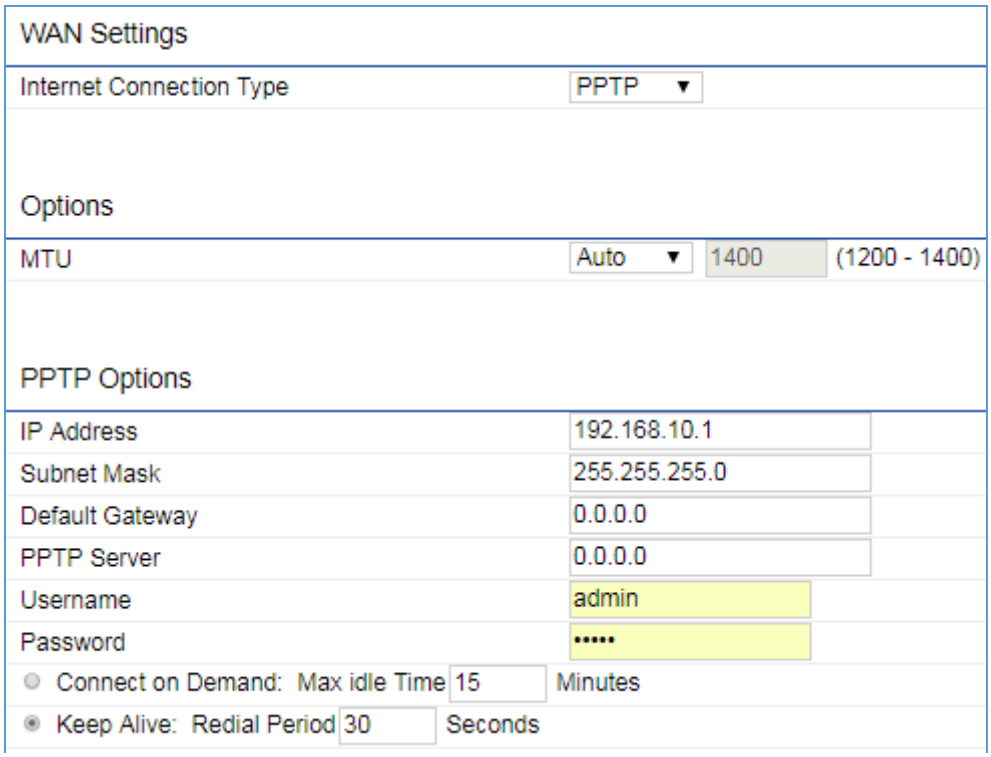



**Figure 5-24** WAN Settings – PPTP

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. |

### 5.4.3 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 "**Client Router**" and then go to "**Router → VPN Pass Through**" to enable VPN passthrough you required in client router mode.

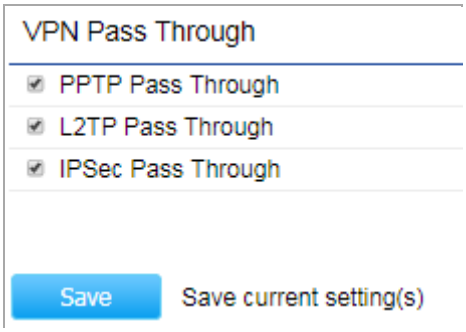



**Figure 5-25** VPN Passthrough

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. |

### 5.4.4 Port Forwarding

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

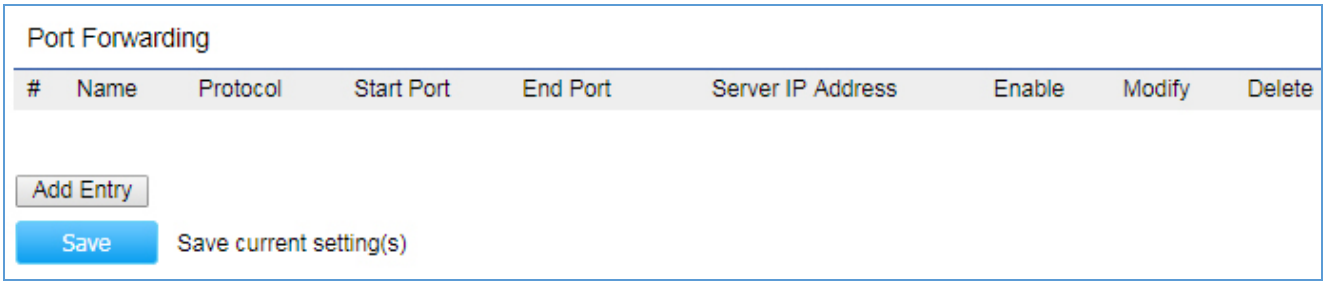



**Figure 5-26** Port Forwarding

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.

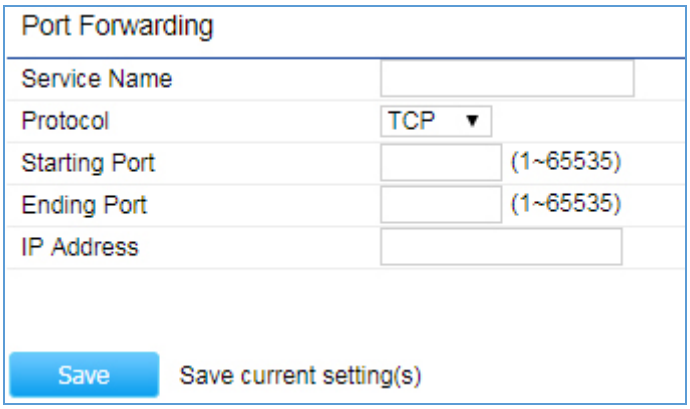



**Figure 5-27** Port Forwarding

The page includes the following settings:

| Object | Description |
|---|---|
| • **Service Name** | Enter a name for the port forwarding rule. |
| • **Protocol** | Select a protocol for the application: Choices are TCP or UDP, or both. |
| • **Starting Port (1~65535)** | Enter a starting port number. |
| • **Ending Port (1~65535)** | Enter an ending port number.<br>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. |

### 5.4.5 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 "**Client Router**" and then go to "**Router → DMZ Settings**" to enable/configure DMZ in client router mode.

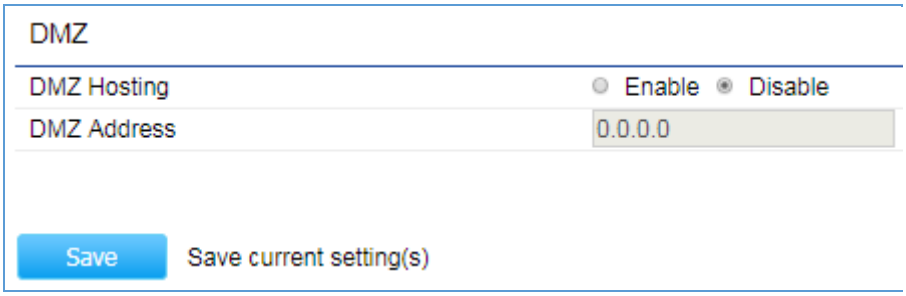



**Figure 5-28** DMZ

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. |

### 5.4.6 Dos Protection

The DoS Protection function can protect the device from being attacked by TCP-SYN Flood, UDP Flood and ping attack when acting as Client Router mode.

Go to the "**Network → Wireless**" page to configure the device as "**Client Router**" and then go to "**Management → Dos Protection**" to enable DoS protection in client router mode.

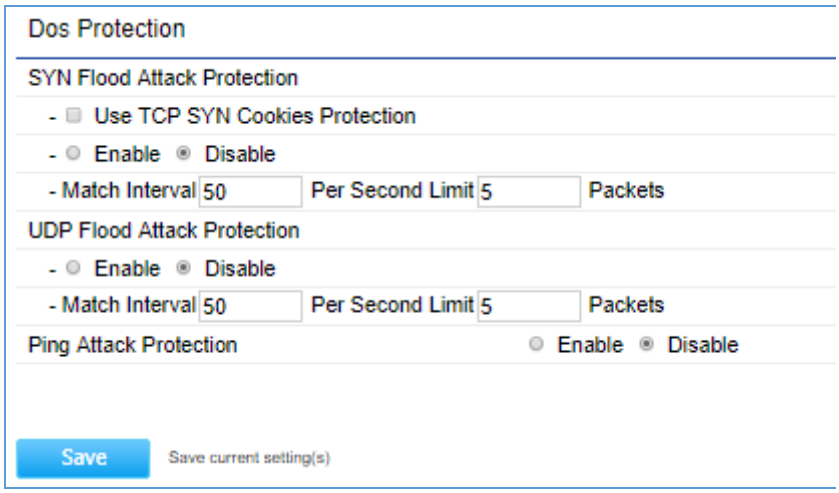



**Figure 5-29** DoS Protection

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. |

## 5.5 Wireless

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

### 5.5.1 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.

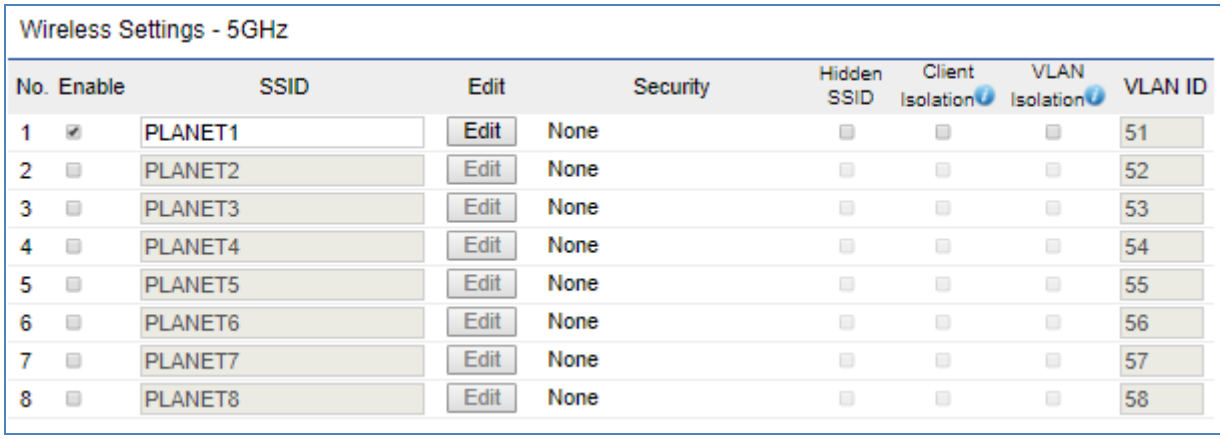



**Figure 5-30** Wireless Settings – AP Mode

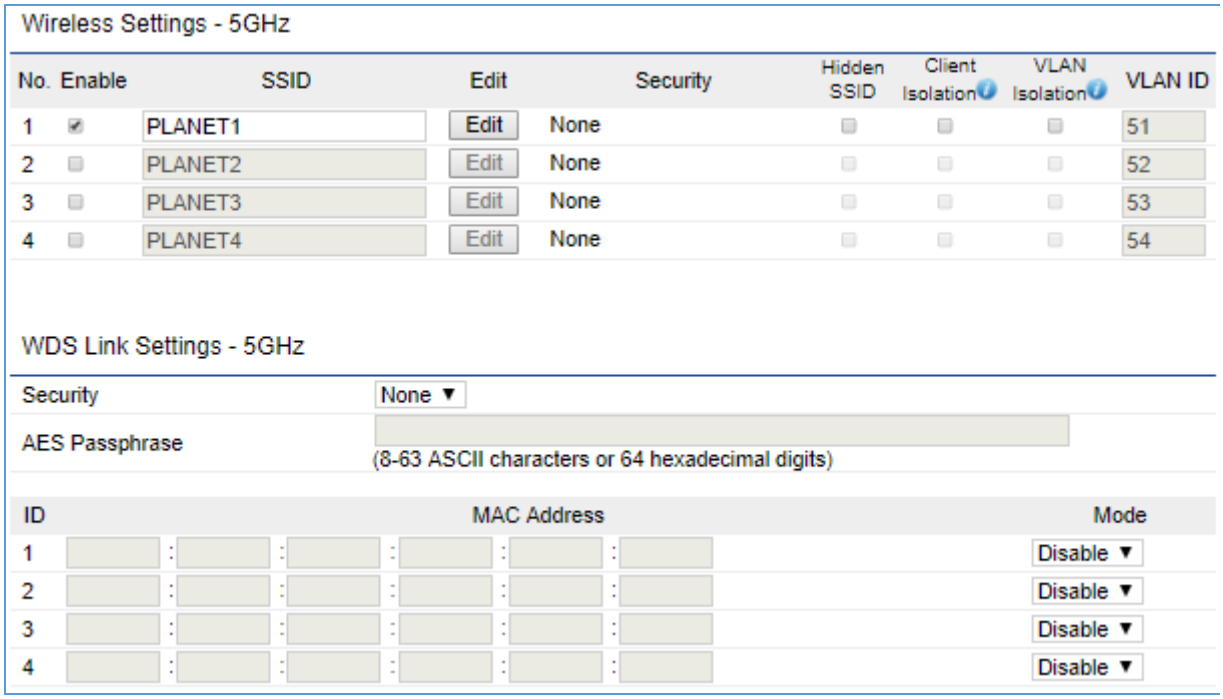



**Figure 5-31** Wireless Settings – WDS AP Mode

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.

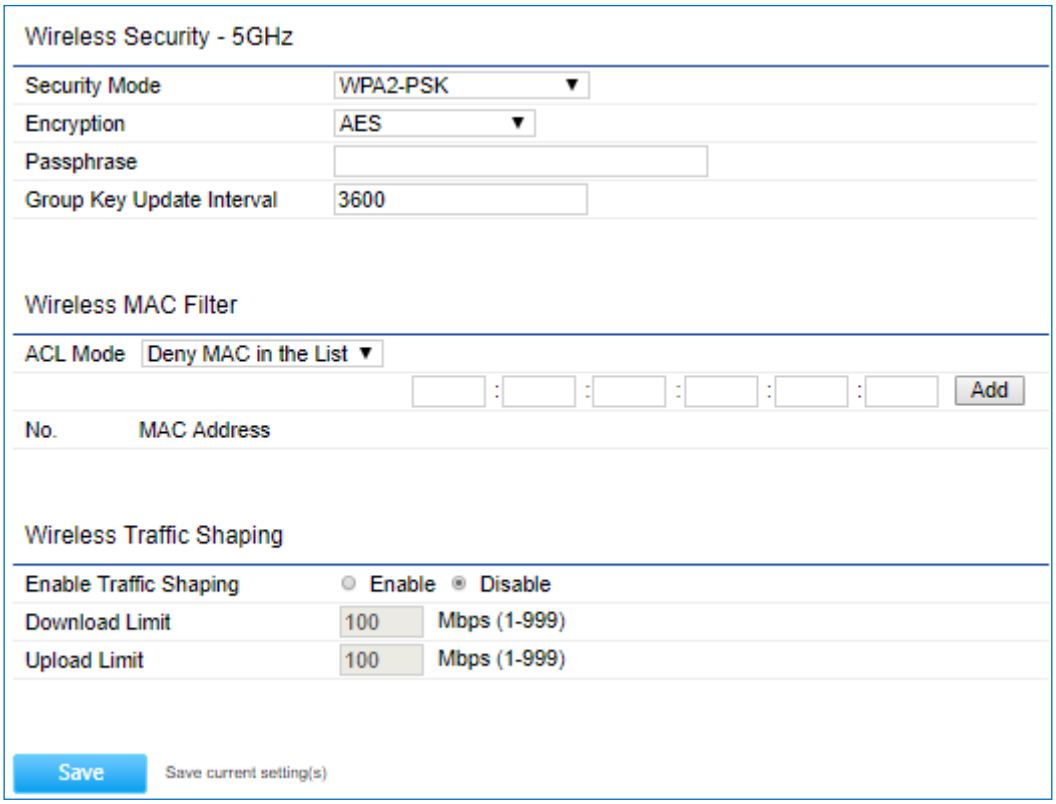



**Figure 5-32** Wireless Profile – AP/WDS AP Mode

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.<br>In the AP mode, up to 8 SSIDs can be configured as different VAPs.<br>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 VIDs 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.

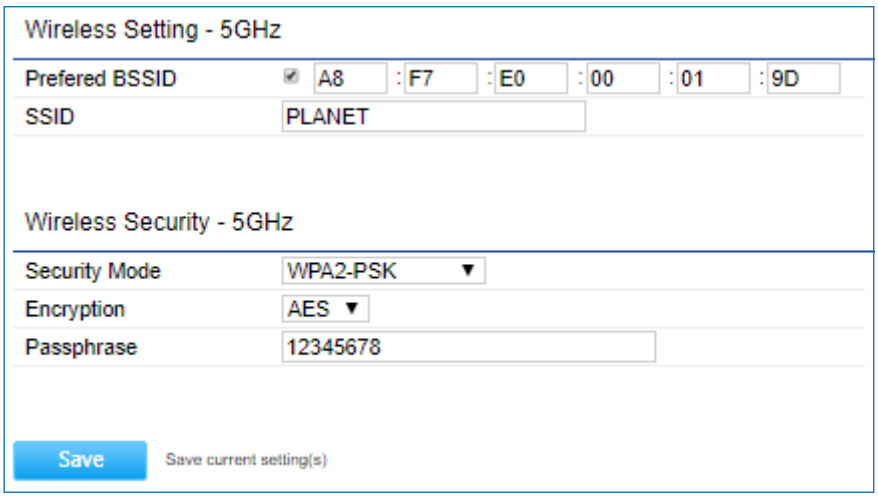



**Figure 5-33** Wireless Profile – CB/WDS STA/CR Mode

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

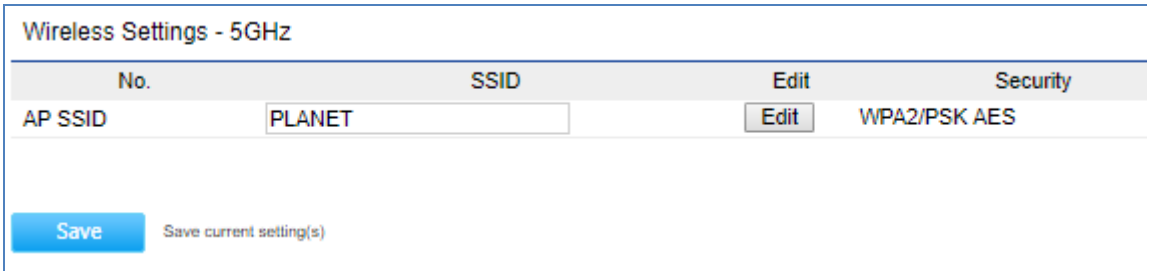



**Figure 5-34** Wireless Settings – CB/WDS STA/CR Mode

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. |

## 5.5.2 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 including PtP (Point to Point) or PtMP (Point to Multiple Points) applications.

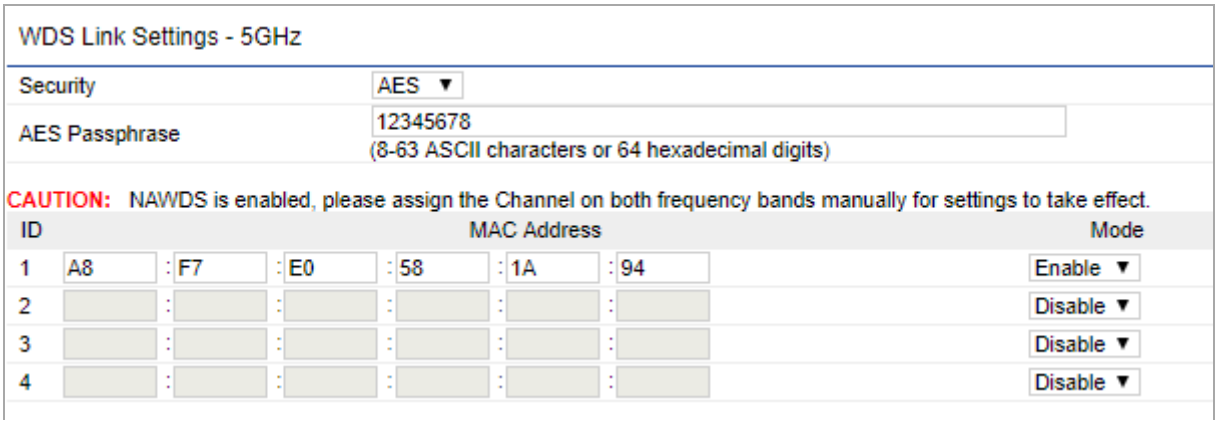



**Figure 5-35** WDS Link Settings – WDS AP Mode

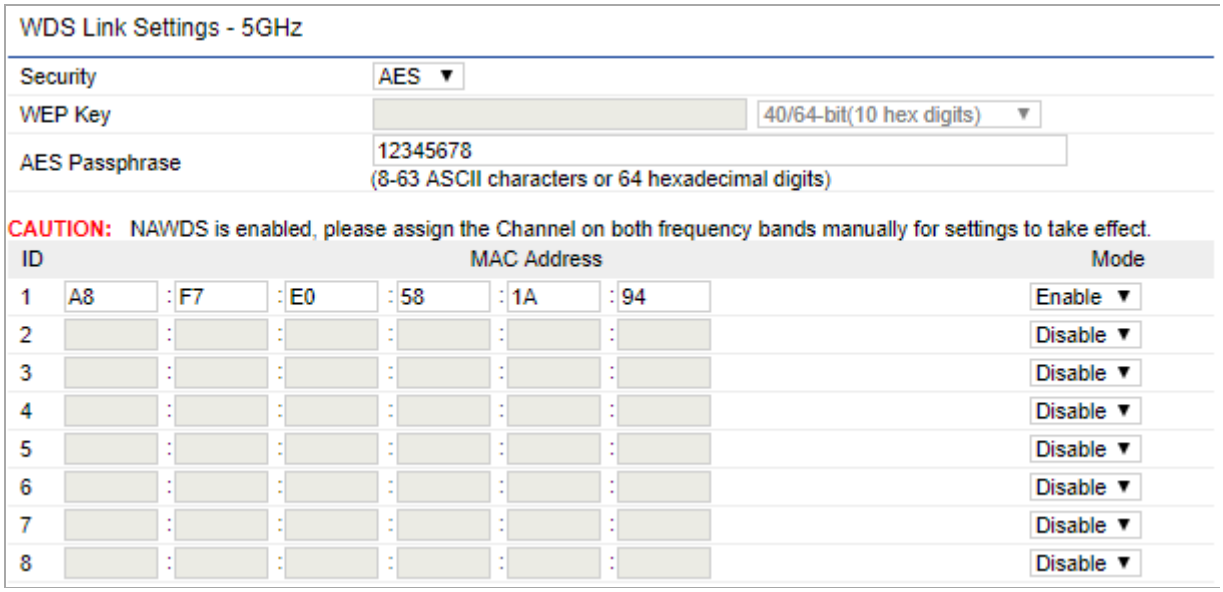



**Figure 5-36** WDS Link Settings – WDS Bridge Mode

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.<br>In the WDS AP mode, up to 4 nodes can be configured to use WDS link.<br>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.

### 5.5.3 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.

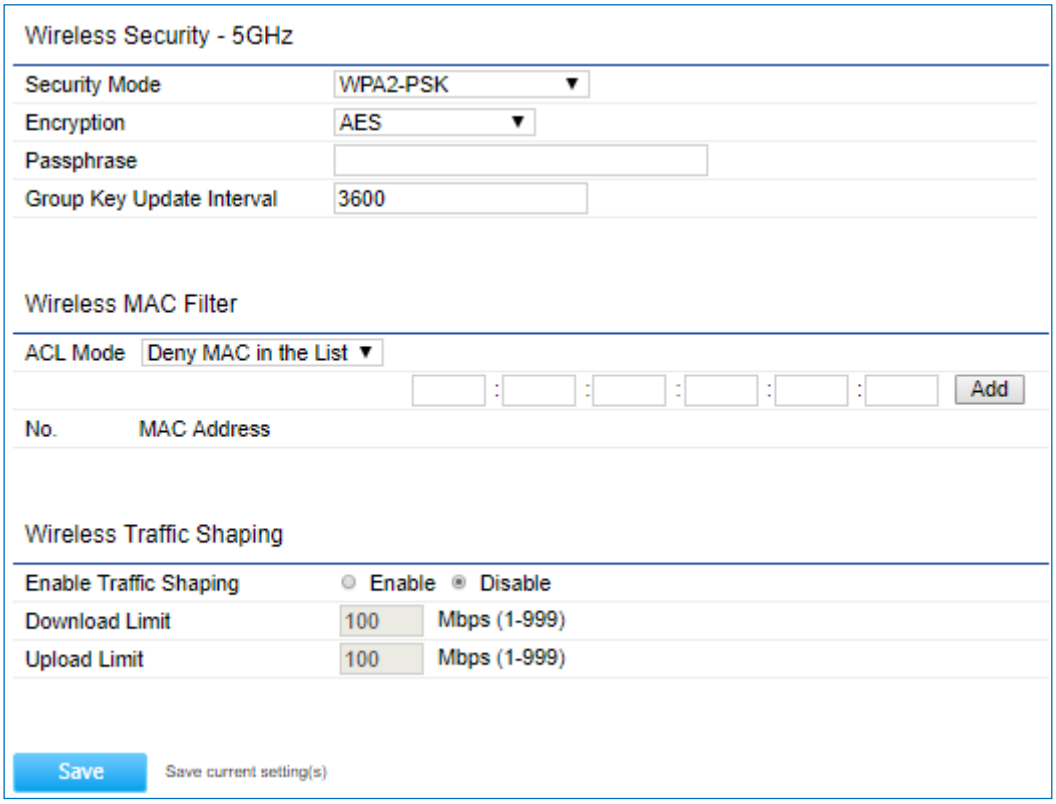



**Figure 5-37** Security Settings – AP/WDS AP Mode

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.

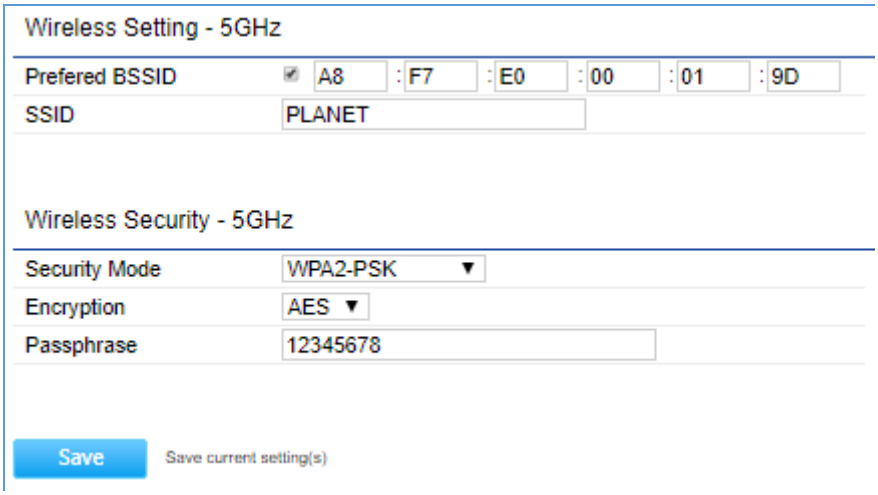



**Figure 5-38** Security Settings – CB/WDS STA/CR Mode

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.

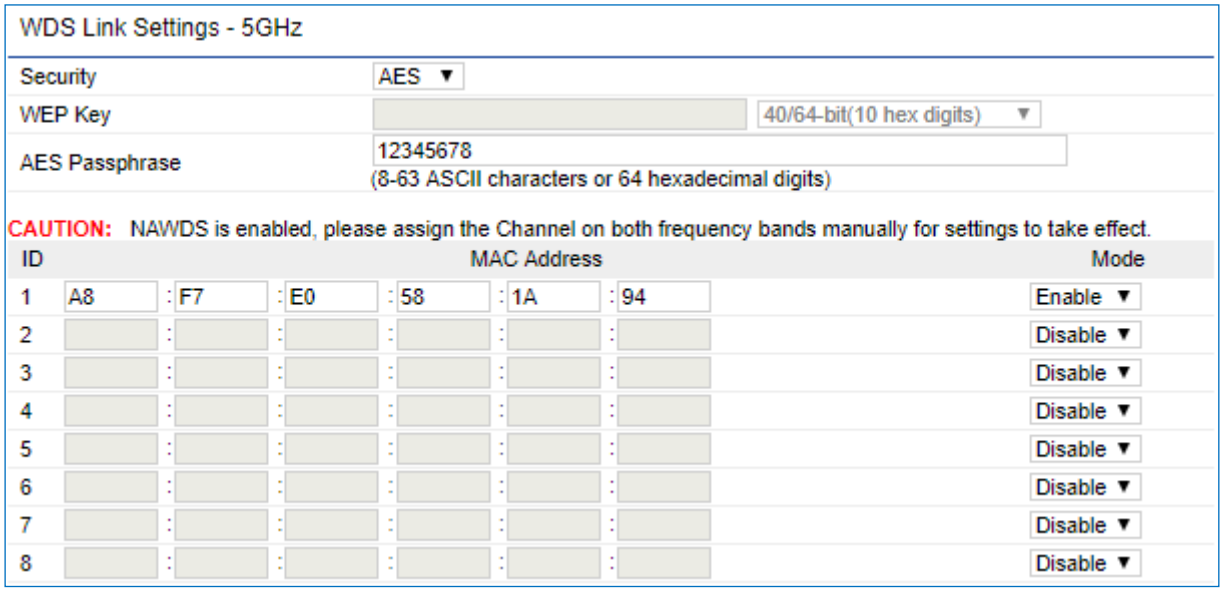



**Figure 5-39** Security Settings – WDS Bridge Mode

The option includes the following settings:

| Object | Description |
|---|---|
| • **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. |

Note

1. The WEP and WPA/WPA2 with TKIP does not support in the 802.11n mode and these options are not available in the 802.11n mode.
2. In the 802.11AC/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.

### ■ 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.

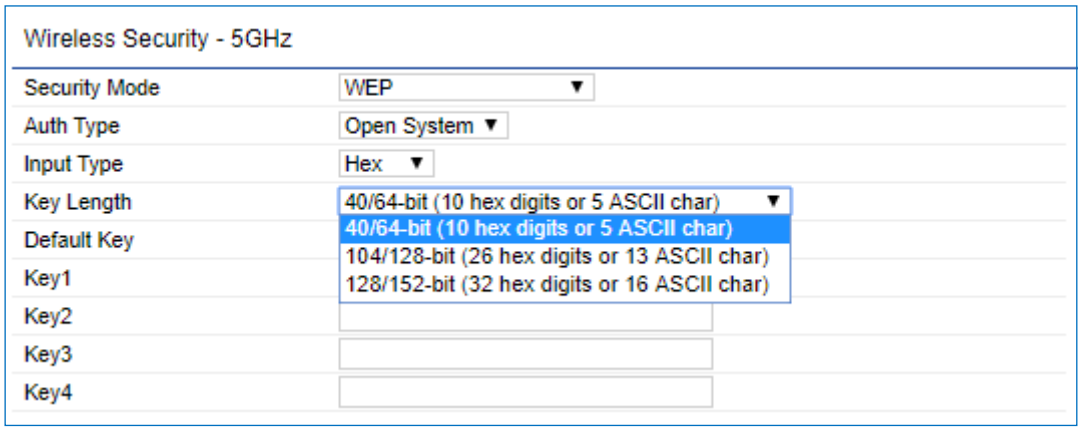



**Figure 5-40** Security Settings – WEP

The security mode includes the following settings:

| Object | Description |
|---|---|
| • **Security Mode** | Select WEP from the drop-down list to configure the wireless network using WEP encryption method. |
| • **Auth Type** | Select Open System or Shared. |
| • **Input Type** | Select an input type of Hex or ASCII. |
| • **Key Length** | Level of WEP encryption is applied to all WEP keys.<br>Select a 64-/128-/152-bit password length.<br>■ **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.<br>■ **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.<br>■ **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. |
| • **Default Key** | Select 1 – 4 to specify which of the four WEP keys the device uses as its default. |
| • **Key1 – Key4** | Specify a password for the security key index. For security, each typed character is masked by a dot. |
| • **Save** | Click **Save** to save the settings. |

■ **WPA-PSK**

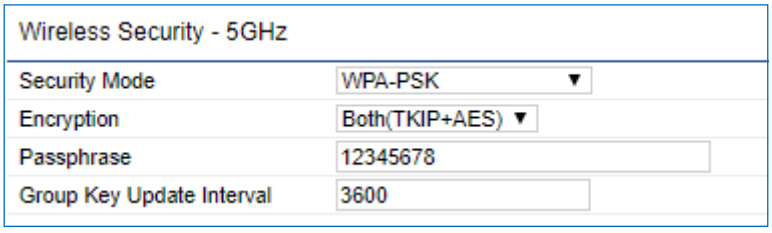



**Figure 5-41** Security Settings – WPA-PSK

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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.

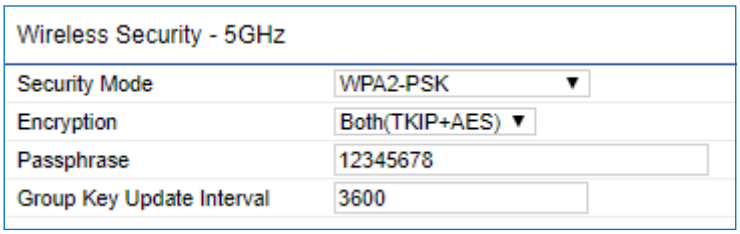



**Figure 5-42** Security Settings – WPA2-PSK

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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**

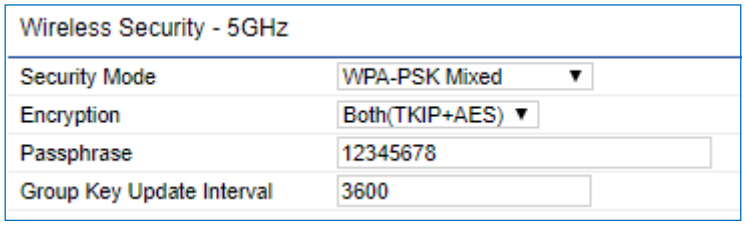



**Figure 5-43** Security Settings – WPA-PSK Mixed

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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)**

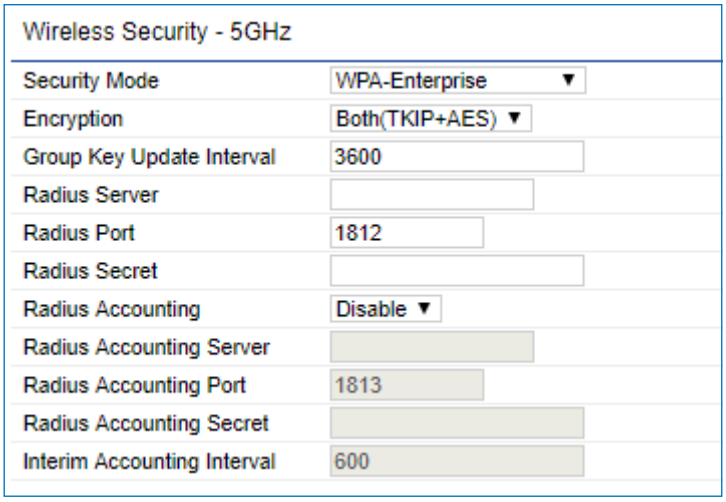



**Figure 5-44** Security Settings – WPA (WPA Enterprise)

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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)**

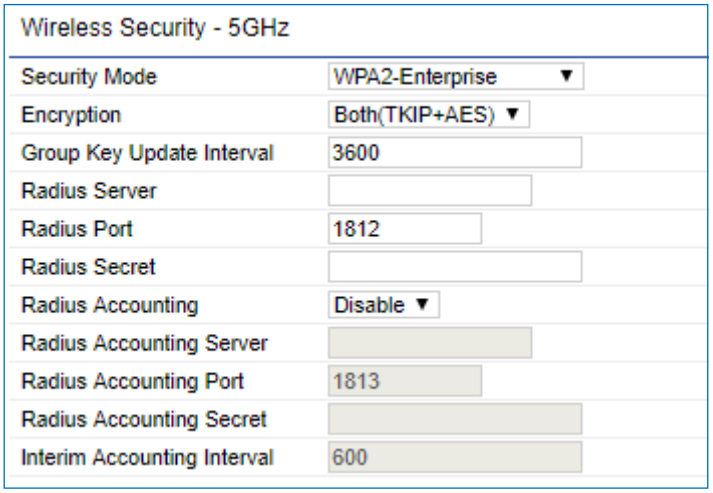



**Figure 5-45** Security Settings – WPA2 (WPA2 Enterprise)

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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)**

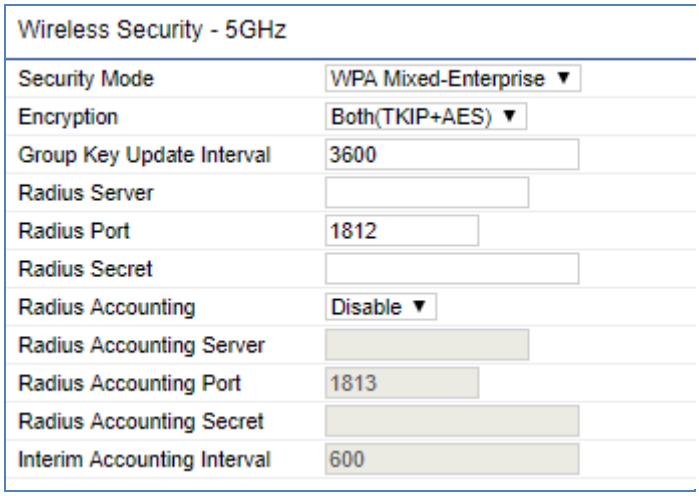



**Figure 5-46** Security Settings – WPA Mixed (WPA Mixed Enterprise)

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.<br>■ **Both:** uses TKIP and AES.<br>■ **TKIP:** automatic encryption with WPA-PSK; requires passphrase.<br>■ **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. |

### 5.5.4 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.

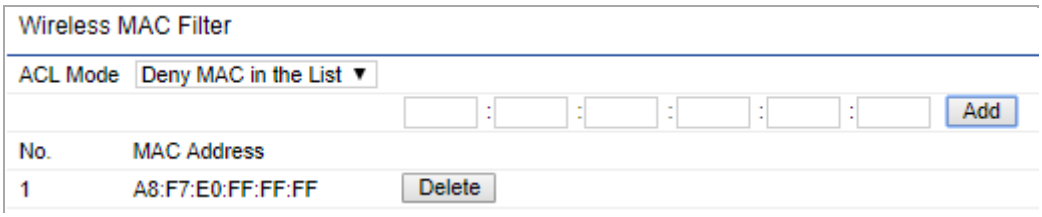



**Figure 5-47** Wireless MAC Filter

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. |

### 5.5.5 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.

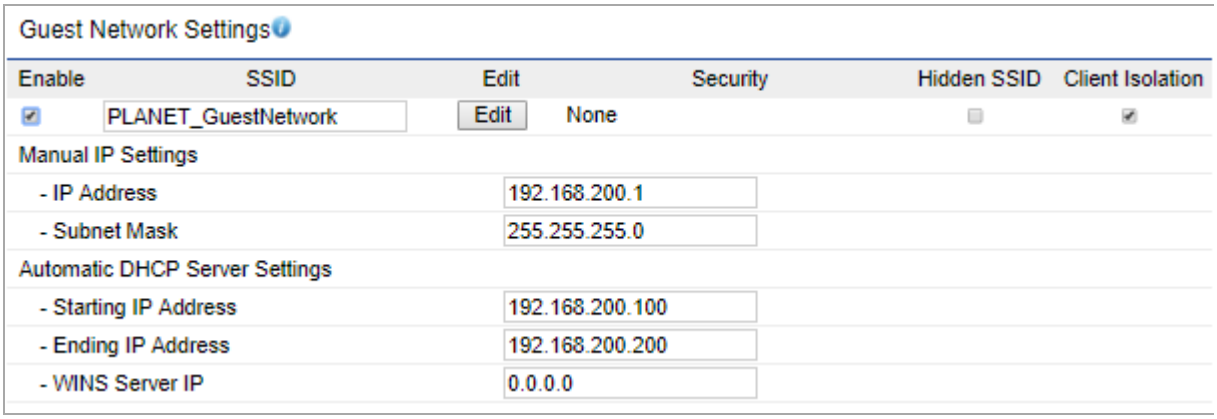



**Figure 5-48** Wireless - Guest Network Settings

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. |

### 5.5.6 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.

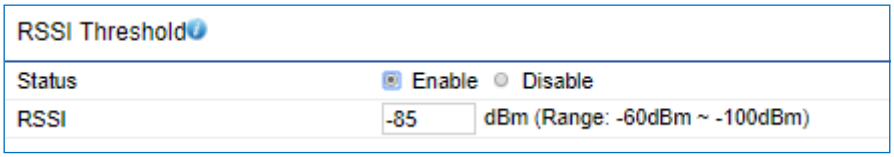



**Figure 5-49** Wireless - RSSI Threshold

The page includes the following settings:

| Object | Description |
|---|---|
| • **Status** | Click **Enable** to enable the RSSI Threshold. |
| • **RSSI (Received Signal Strength Index)** | Specifies the RSSI value to limit the client access.<br>Range: -60dBm ~ -100dBm<br><br>RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal. |

### 5.5.7 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.

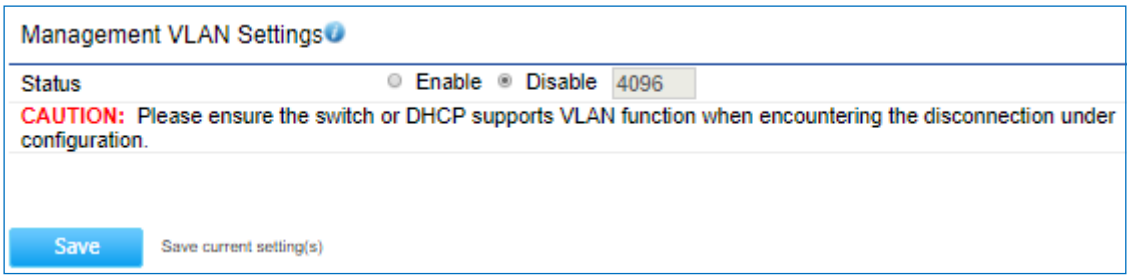



**Figure 5-50** Wireless – Management VLAN

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.<br>Range: 1 ~ 4094 |

## 5.6 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.

### 5.6.1 Account (Password Settings)

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

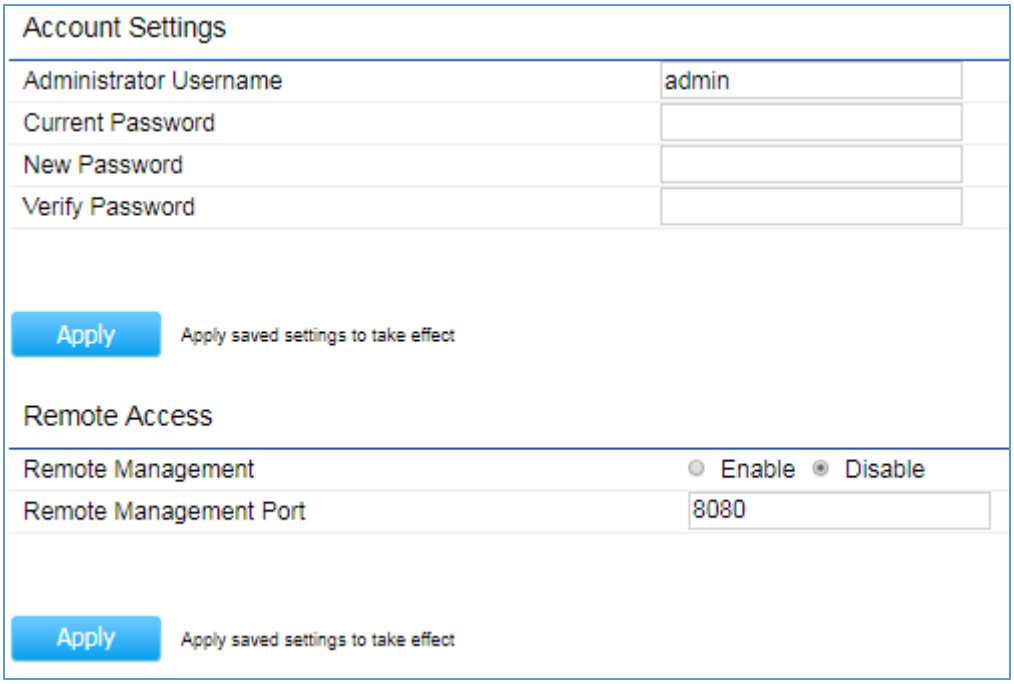



**Figure 5-51** Administration (Password Settings)

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: Client Router (WISP) mode only** | |
| • **Remote Management** | Click **Enable** to enable remote access through WAN. |
| • **Remote Management Port** | Enter the remote access port number. |

### 5.6.2 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.

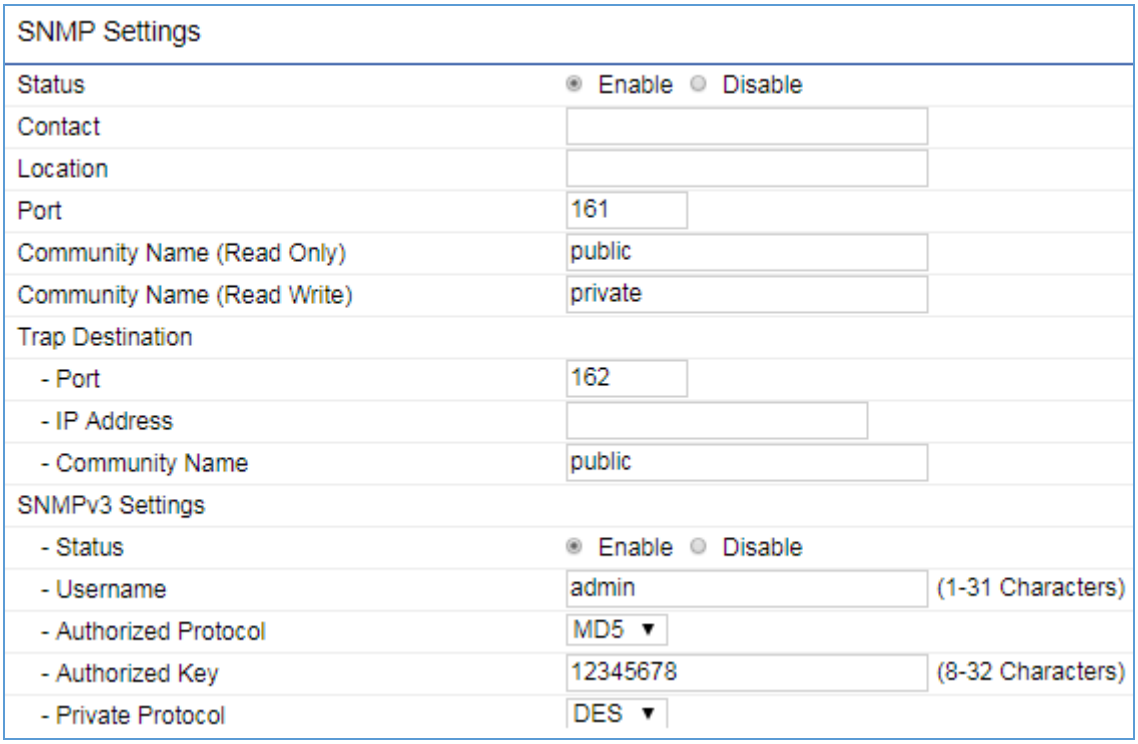



**Figure 5-52** SNMP Settings

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. |

### 5.6.3 CLI/SSH/HTTPS Settings

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

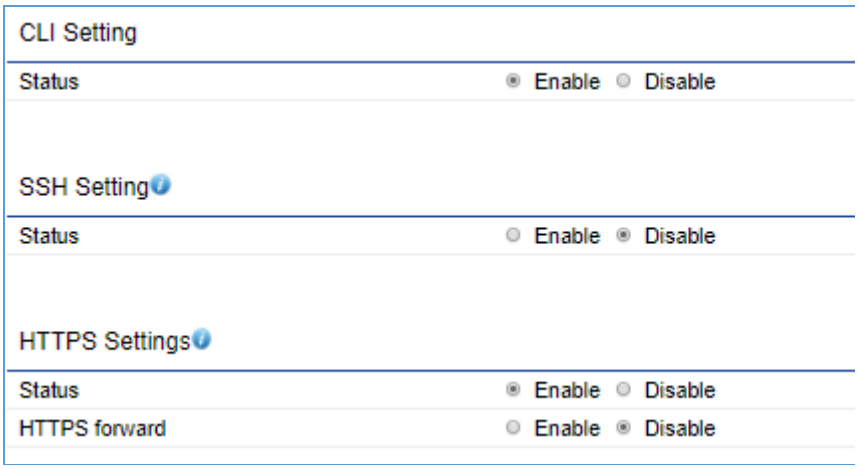



**Figure 5-53** CLI/SSH/HTTPS Settings

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. |

### 5.6.4 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.

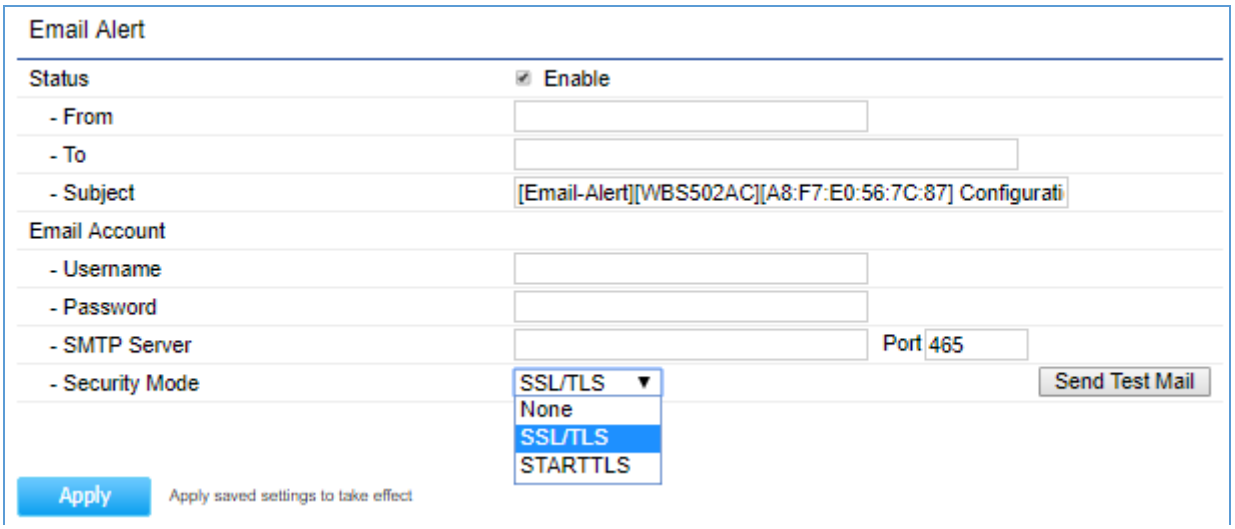



**Figure 5-54** Email Alert Settings

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.<br>SSL/TLS: default port number is 465<br>STARTTLS: default port number is 587 |
| • **Apply** | Click **Apply** to apply all changes. |

### 5.6.5 Backup/Restore Settings

Click "**System Manager → Firmware**" and refer to the "**Backup/Restore Settings**" section.

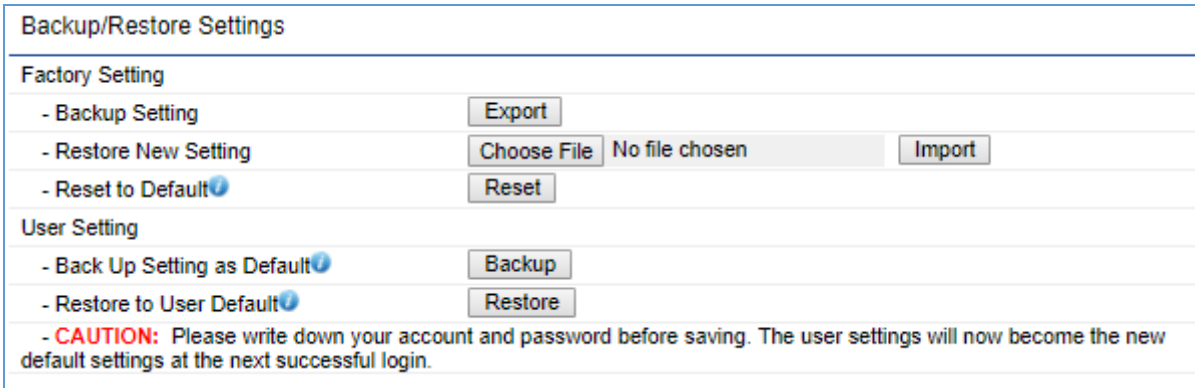



**Figure 5-55** Backup/Restore Settings

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. |

## 5.6.6 WiFi Scheduler

### 5.6.6.1. 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.

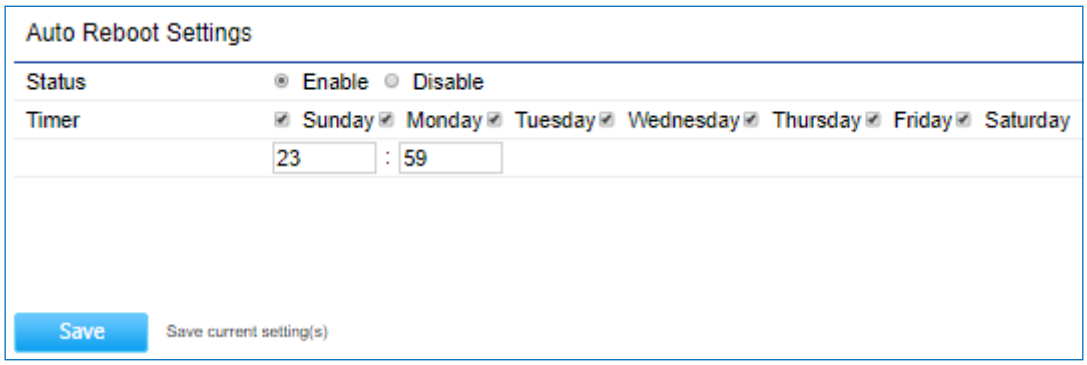



**Figure 5-56** Auto Reboot Settings

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. |

### 5.6.6.2. 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.

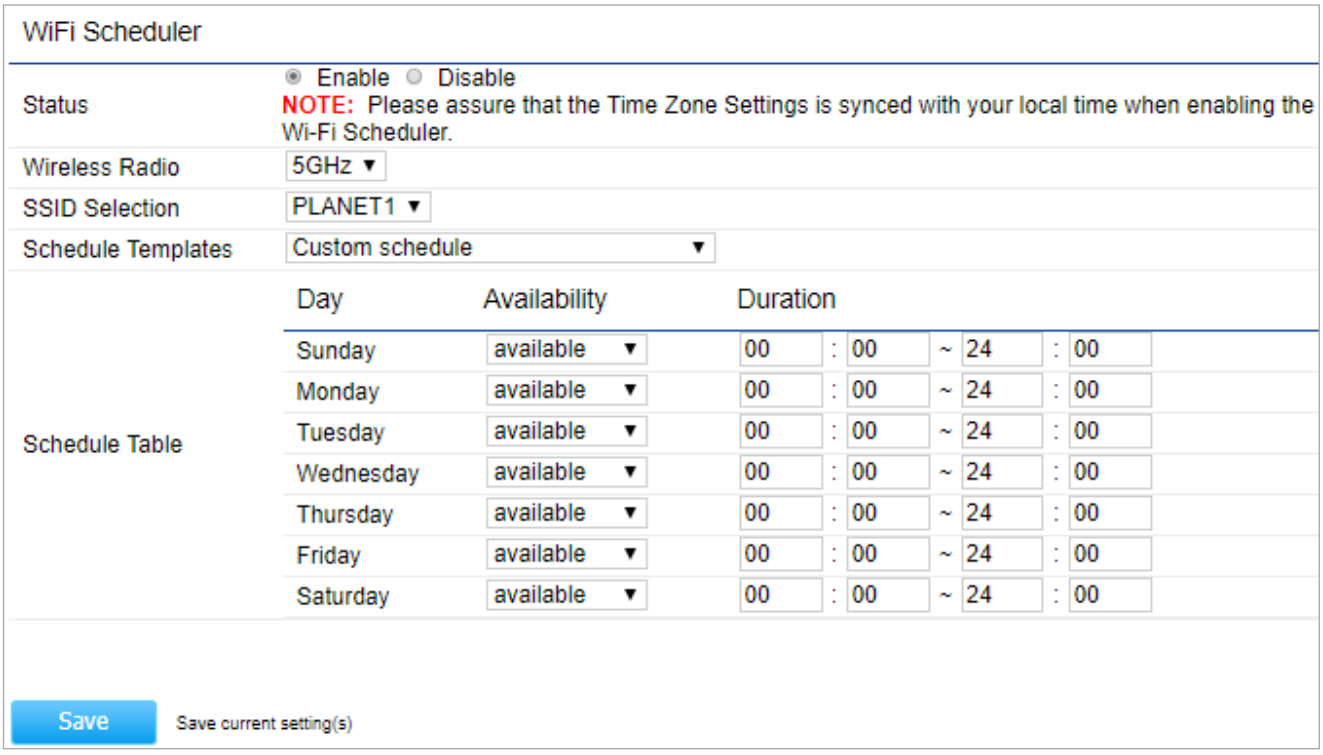



**Figure 5-57** WiFi scheduler

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.<br>The format is [HH:MM ~ HH:MM] (Start Time ~ End Time).<br>HH: range from 0-24<br>MM: range from 0-59 |
| • **Save** | Click **Save** to save all changes. |

### 5.6.7 Firmware Upgrade

Click “**System Manager → Firmware**” and refer to the “**Firmware Upgrade**” section to upgrade the device’s firmware.

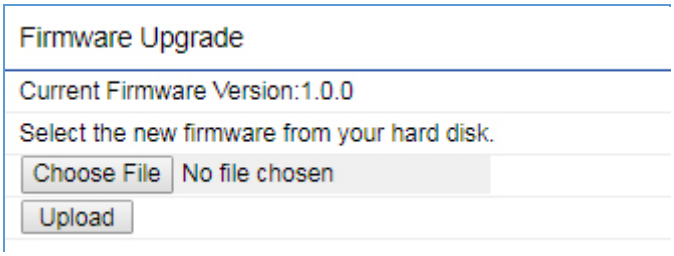



**Figure 5-58** Firmware Upgrade

The page includes the following settings:

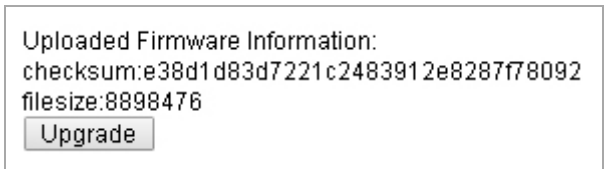
| Object | Description |
|---|---|
| • **Current Firmware Version** | Displays the current firmware version. |
| • **Choose File** | Click **Choose File** to locate and select the upgrade file from your local hard disk. |
| • **Upload** | Click **Upload** to upgrade the firmware. |

*Firmware Upgrade Procedure*

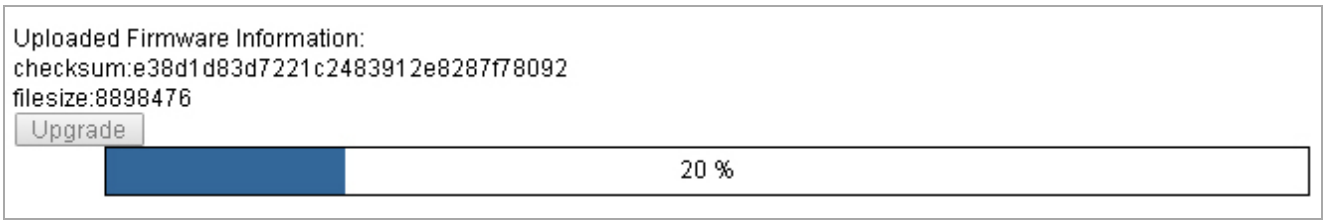
The following procedure will guide you to how to upgrade the firmware.

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

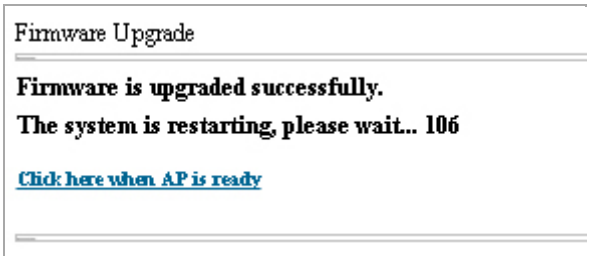
**Step 2**. The firmware checksum information appears to help you confirm whether the file is correct. Once confirmed, click the **Upgrade** button to begin the upgrade process.




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




**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.




### 5.6.8 Time Settings

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

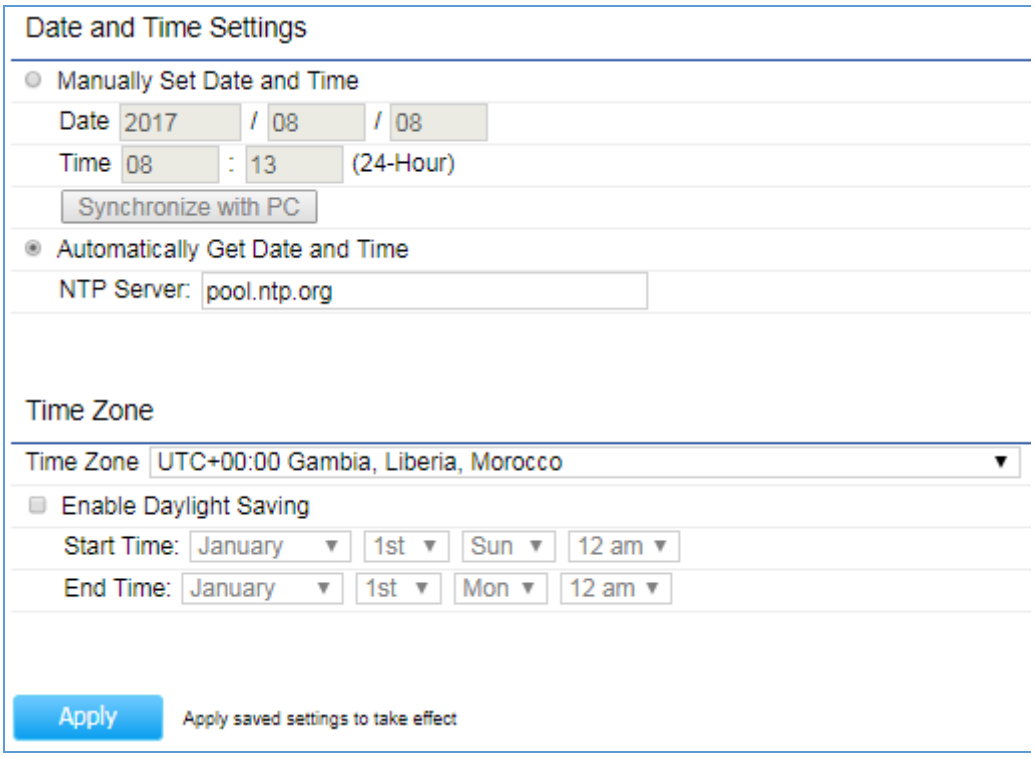



**Figure 5-59** Time Settings

The page includes the following settings:

| Object | Description |
|---|---|
| • **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. |
| • **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. |
| • **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. |
| • **Apply** | Click **Apply** to apply all changes. |

### 5.6.9 Log

Click "**System Manager → Log**" to view the system log.

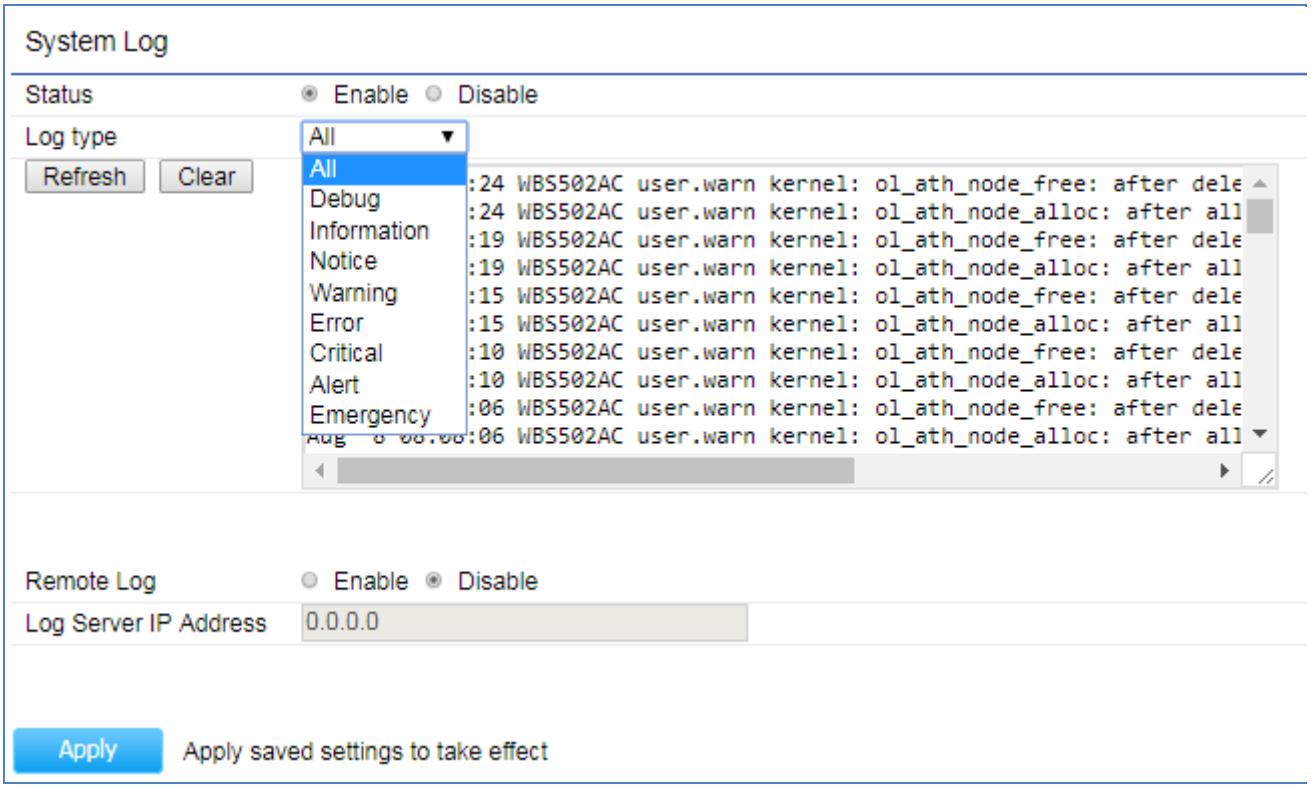



**Figure 5-60** System Log

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. |

### 5.6.10 Tools

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

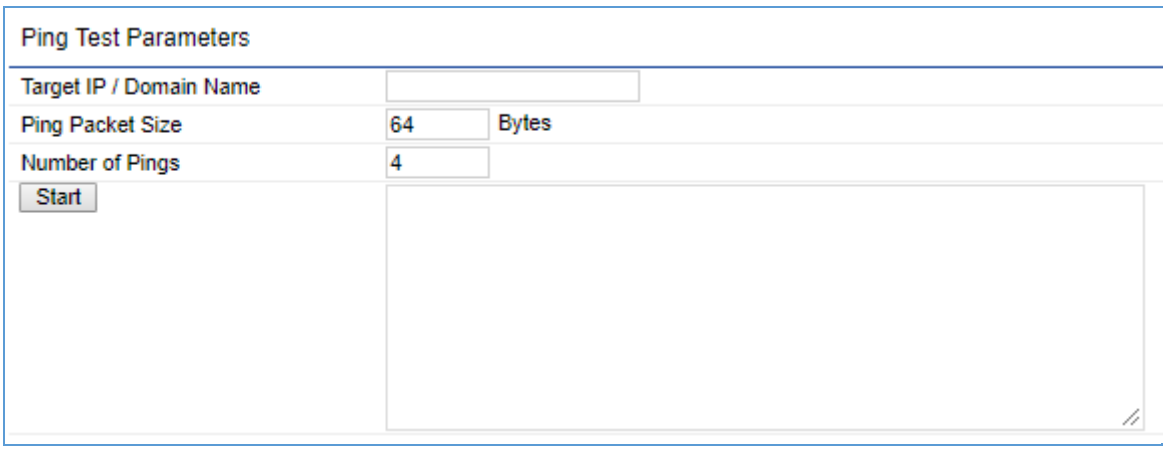



**Figure 5-61** Tools - Ping

The section includes the following settings:

| Object | Description |
|---|---|
| • **Target IP / Domain Name** | Enter the IP address you would like to ping. |
| • **Ping Packet Size** | Enter the packet size of each ping. |
| • **Number of Pings** | Enter the number of times you want to ping. |
| • **Start** | Click **Start** to begin pinging. |

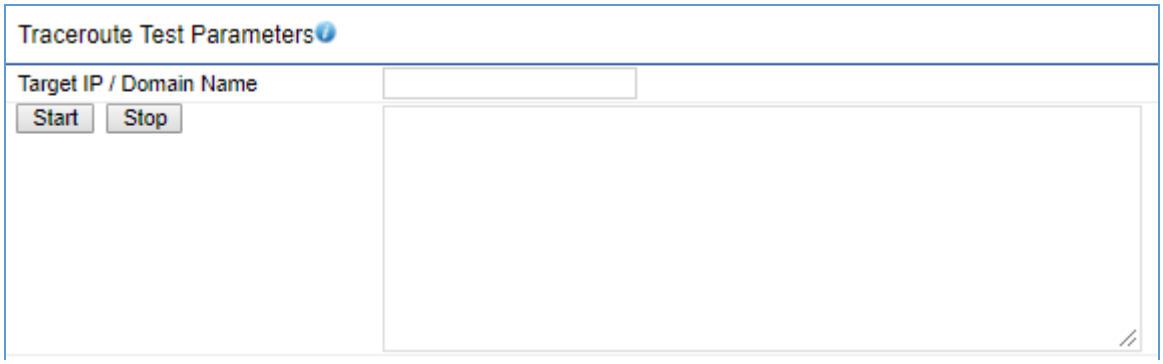



**Figure 5-62** Tools - Traceroute

The section includes the following settings:

| Object | Description |
|---|---|
| • **Trace route target** | Enter an IP address or domain name you want to trace. |
| • **Start** | Click **Start** to begin the traceroute operation. |
| • **Stop** | Click **Stop** to terminate the traceroute operation. |

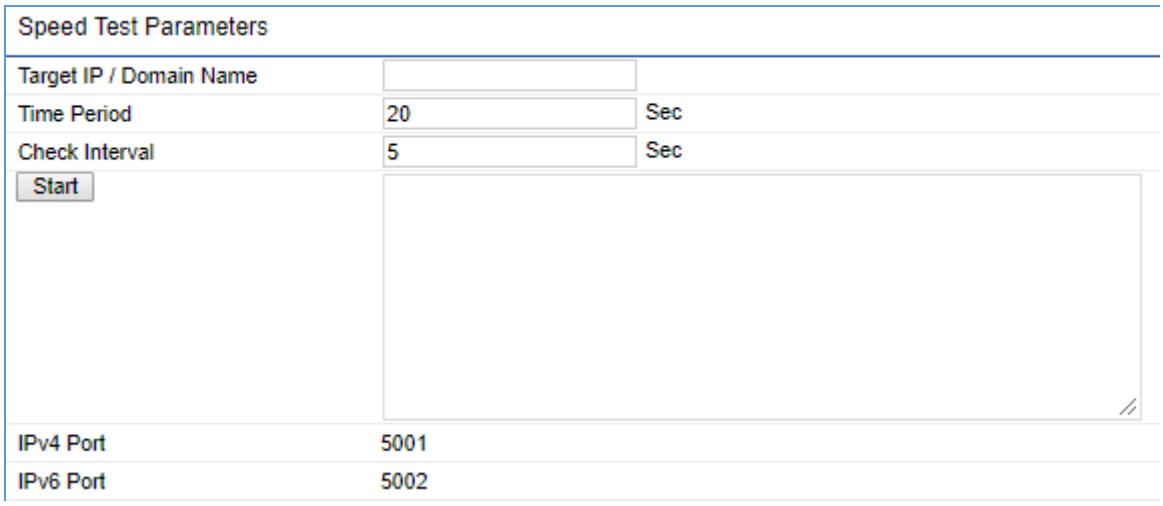



**Figure 5-63** Tools – Speed Test

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. |

### 5.6.11 Logout

Click "**Logout**" on the upper-right corner of the page to log out the system.

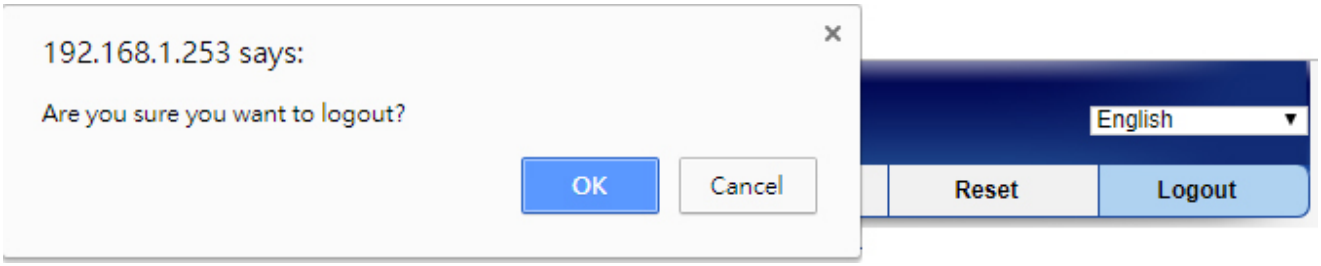



**Figure 5-64** Logout

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. | ● 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.<br>● If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered.<br>● You must use the same IP address section that AP uses.<br>● 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).<br>● Set your computer to static IP address, and see if the Planet Smart Discovery can find the AP or not.<br>● If you did a firmware upgrade and this happens, contact the Planet Tech Support for help.<br>● If all the solutions above don't work, contact the Planet Tech Support for help. |
| I can't get connected to the Internet. | ● Check the Internet connection status from the router that is connected with the AP.<br>● Please be patient. Sometimes Internet is just that slow.<br>● 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.<br>● Check PPPoE / L2TP / PPTP user ID and password in your router again.<br>● Call your Internet service provider and check if there's something wrong with their service.<br>● If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter.<br>● Try to reset the AP and try again later.<br>● Reset the device provided by your Internet service provider.<br>● 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. | ● 'Broadcast ESSID' set to off?<br>● The antenna is properly secured. |

| | |
|---|---|
| | ● Are you too far from your AP? Try to get closer.<br>● 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. | ● Are you using QoS function? Try to disable it and try again.<br>● Internet is slow sometimes; try to be patient.<br>● Try to reset the AP and see if it's better after that.<br>● Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow.<br>● 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. | ● Make sure you're connecting to the correct IP address of the AP.<br>● Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated.<br>● If you really forget the password, do a hard reset. |
| The AP becomes hot. | ● This is not a malfunction if you can keep your hand on the AP's case.<br>● 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.

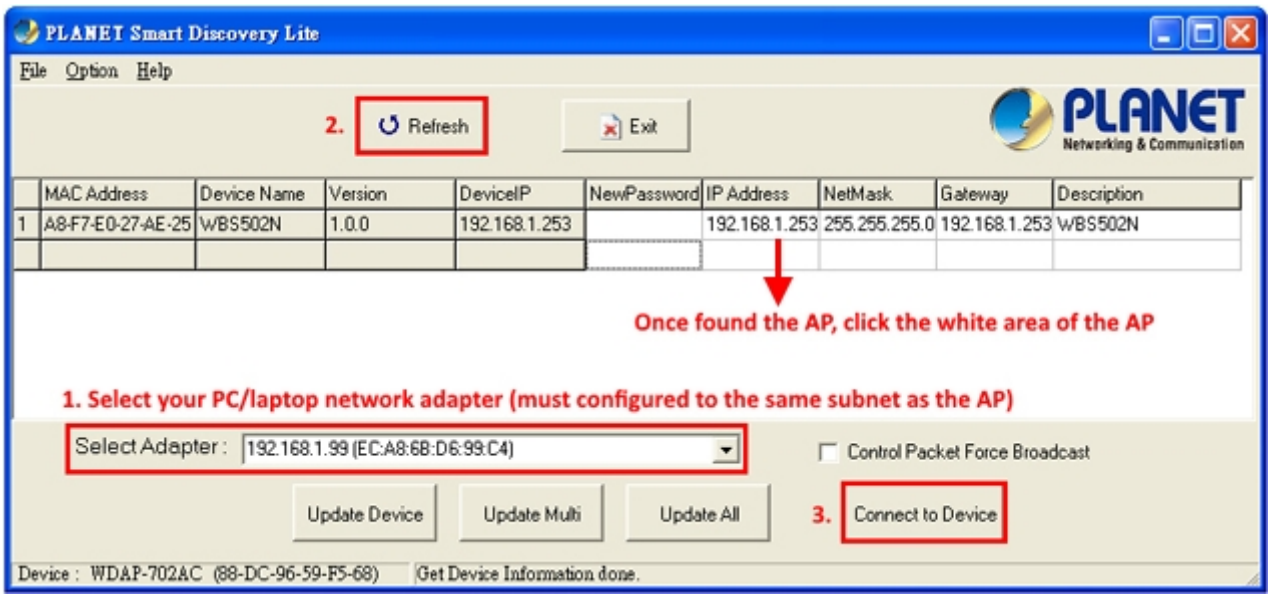



**Figure B-1** PLANET Smart Discovery

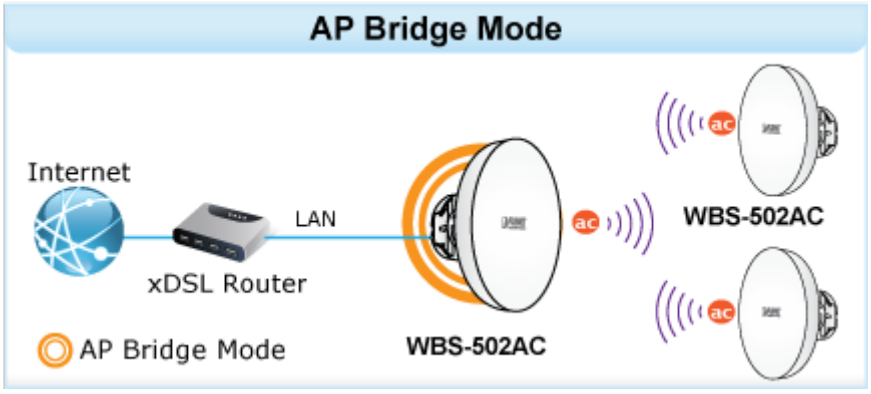
**Step 4.** Select the AP from the list and then click the **"Connect to Device"** button to link to the Web Management Configuration Page.

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

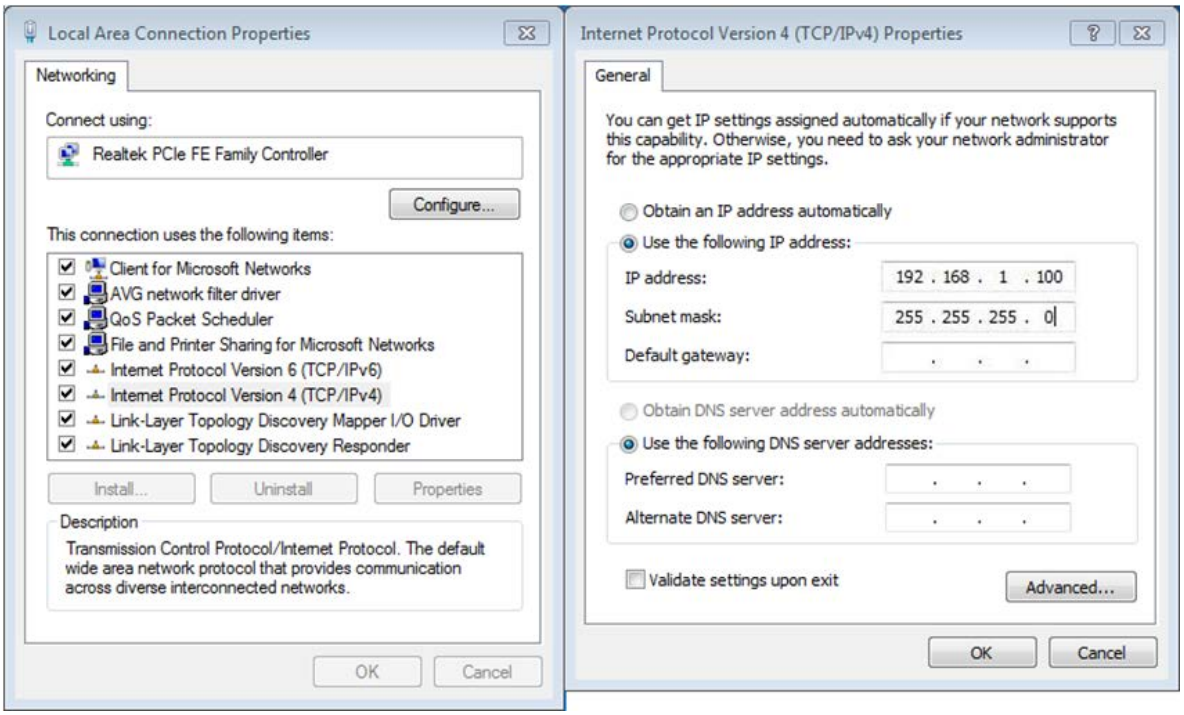
# Appendix C: FAQ

## Q1: How to set up the AP Client Connection

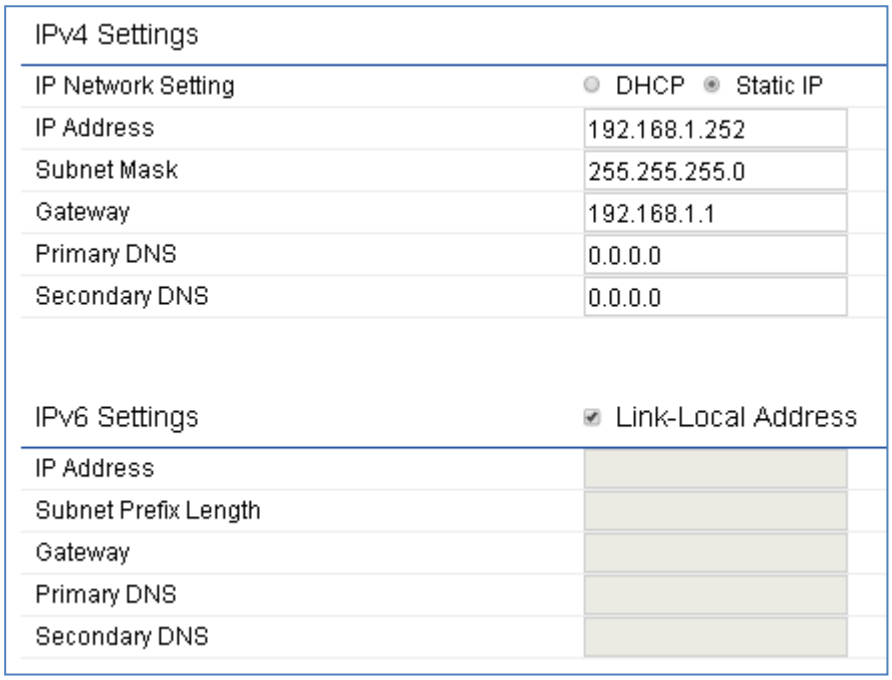
**Topology:**



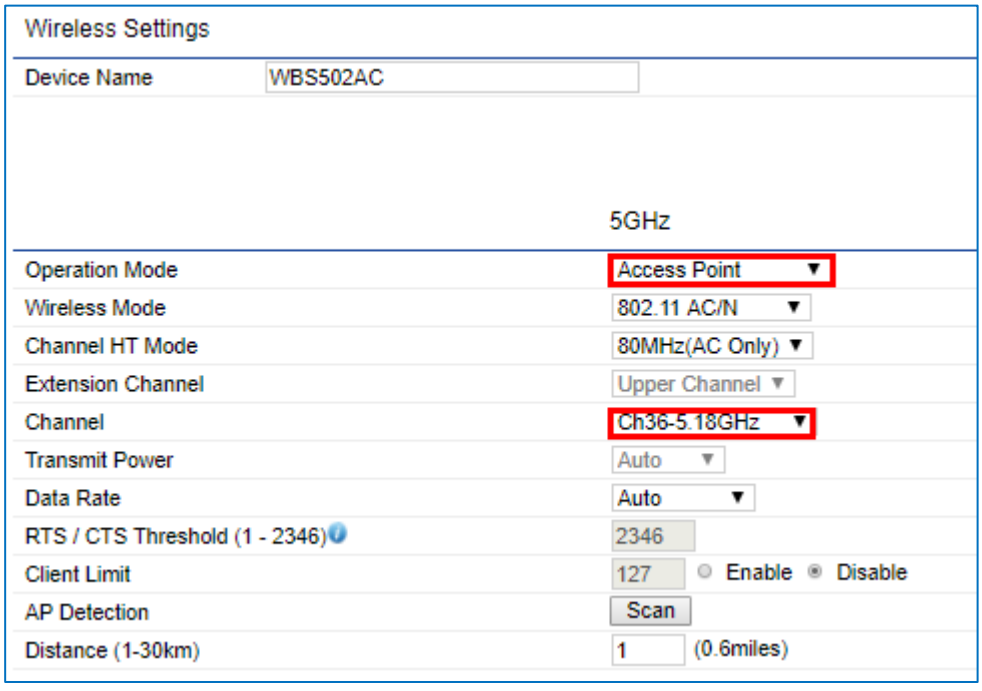

1. Use static IP in the PCs that are connected with AP-1 (Site-1) and AP-2 (Site-2). In this case, Site-1 is "192.168.1.100", and Site-2 is "192.168.1.200".



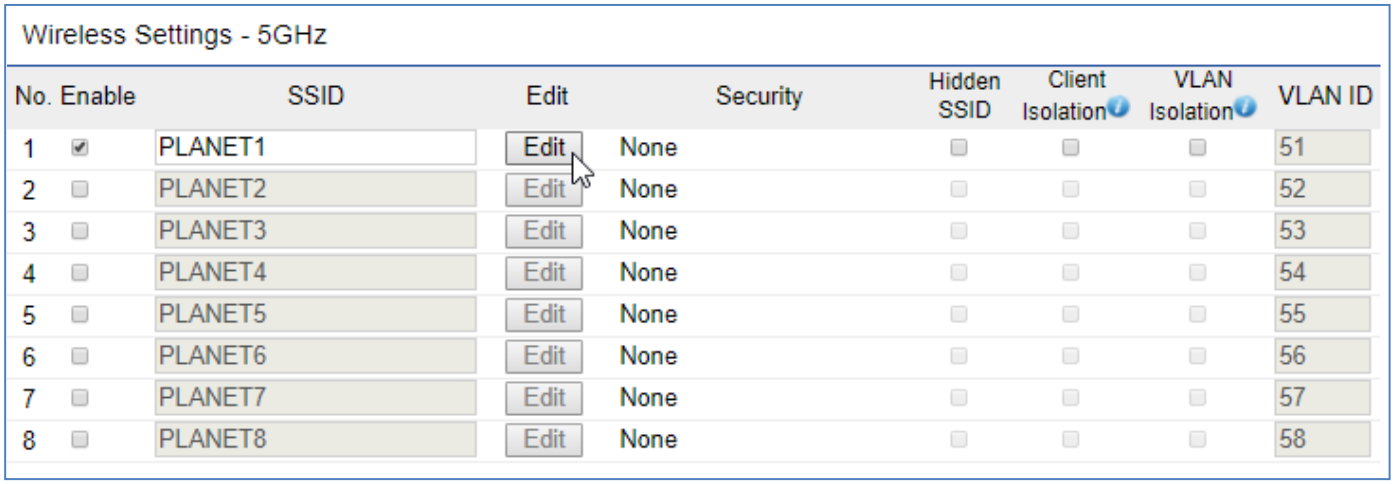

2. In the AP-1, go to "**Network-> Basic**" to configure the IP address to static and must different from the AP-2.



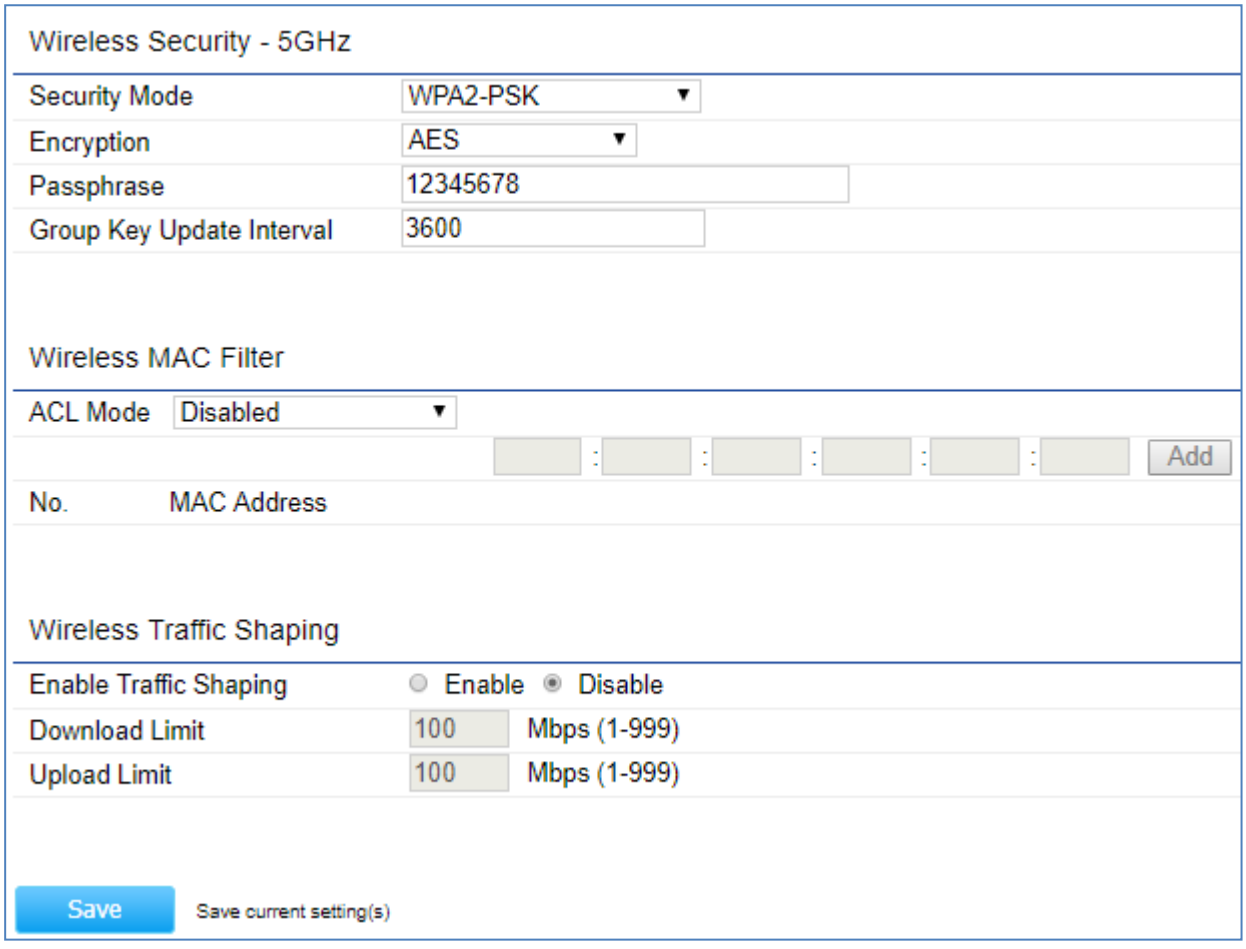

3. In the AP-1, go to "**Network-> Wireless**" page and configure the following wireless parameters:
   (1) Operation Mode: set to "**Access Point**" mode.
   (2) Channel: set to a fixed channel (e.g. channel 36)



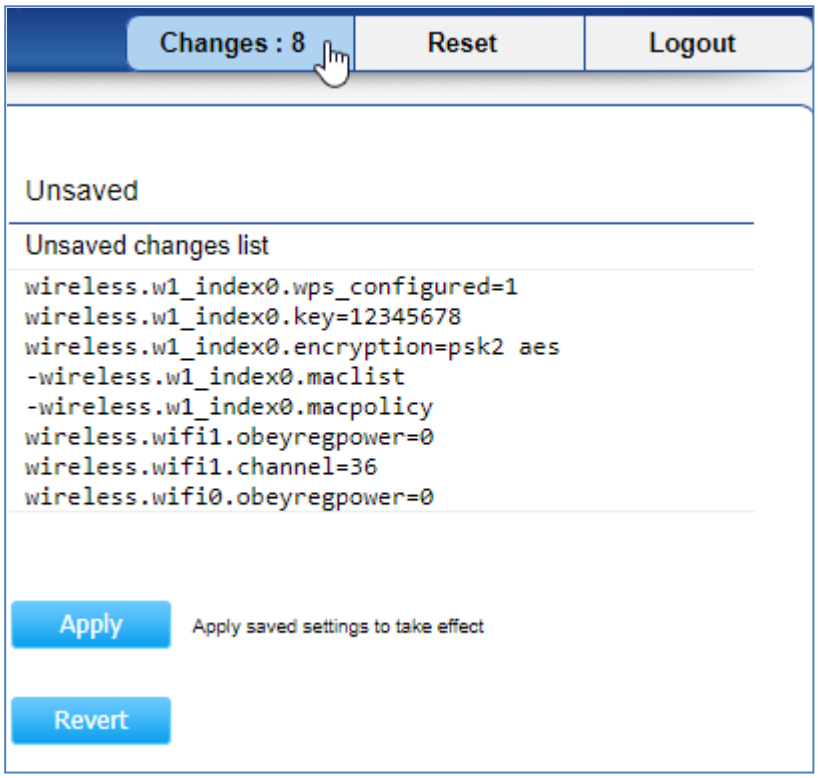

4. Click "**Edit**" in the wireless settings section.



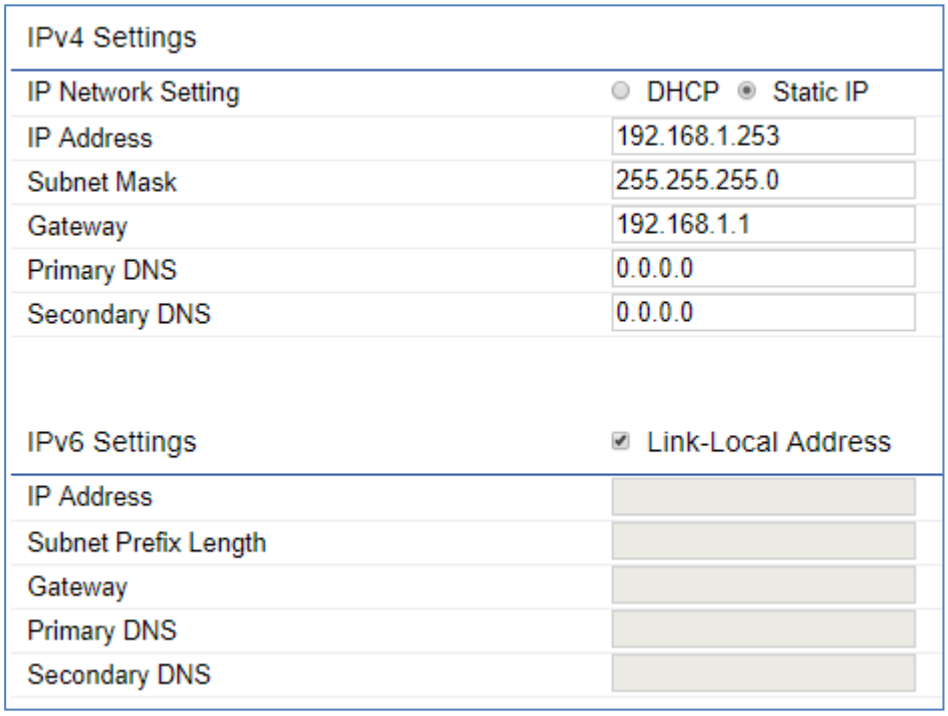

5. In the wireless security section, configure the encryption and passphrase (WPA2-PSK/AES is suggested). Then, click "**Save**" to go back to the main page.



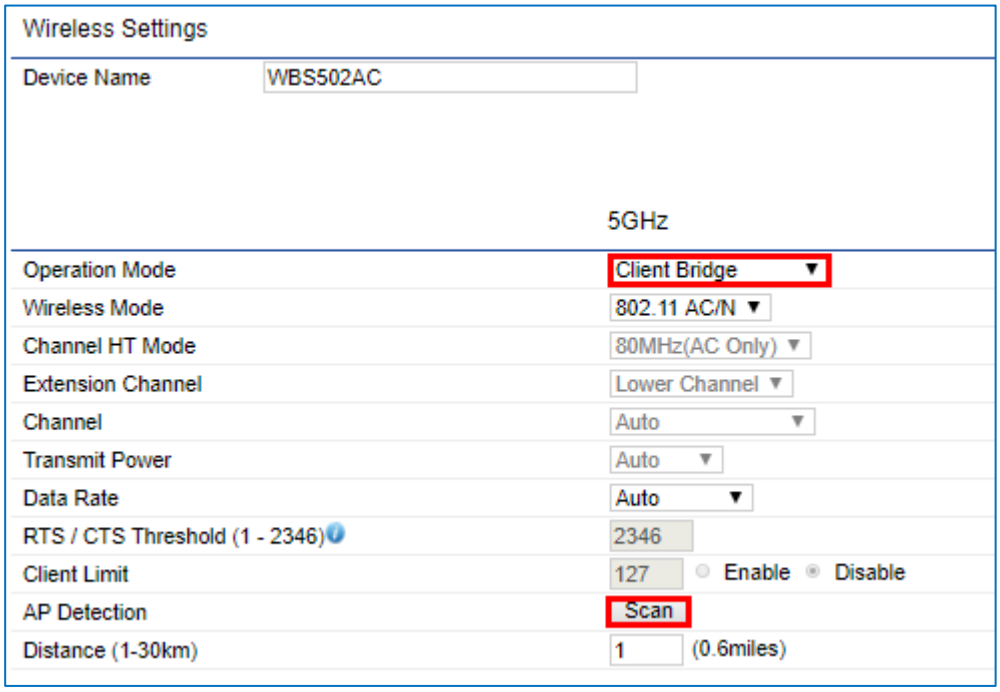

6. In the wireless main page, click "**Save**" to save the configurations.
7. Go to the "**Changes**" page to click "**Apply**" to apply the saved settings to take effect.



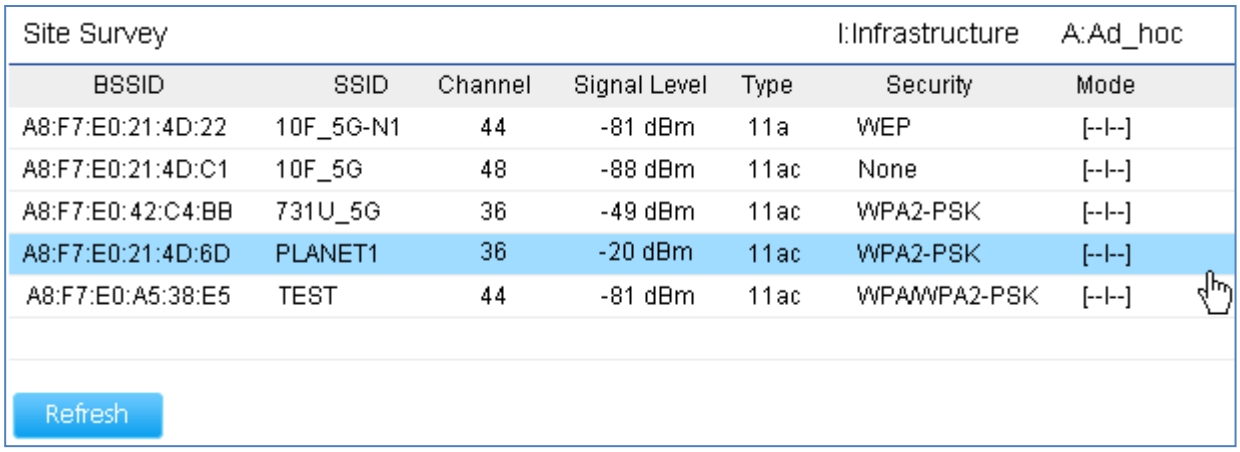

8. In the AP-2, go to "**Network-> Basic**" to ensure the IP address is static and different from the AP-1.



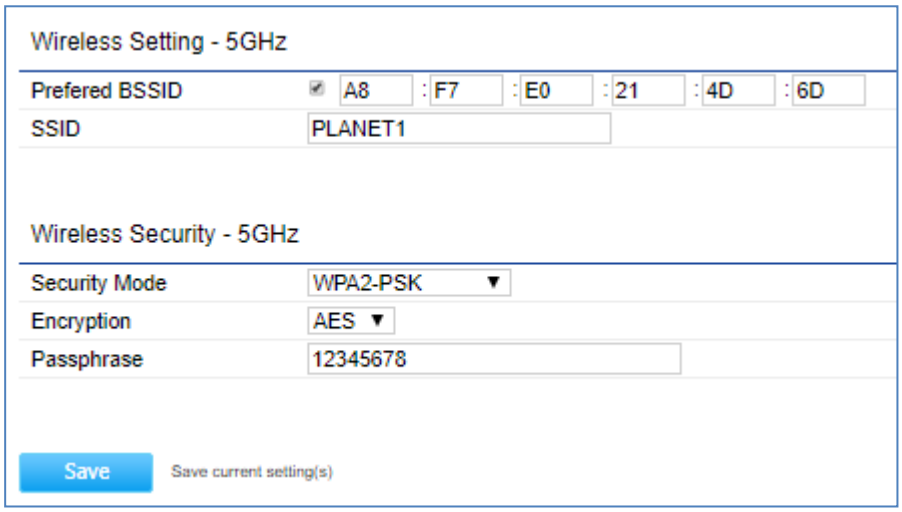

9. In the AP-2, go to "**Network-> Wireless**" page to configure the Operation Mode to "**Client Bridge**" mode. Then, click "**Scan**" button to site survey the AP-1.



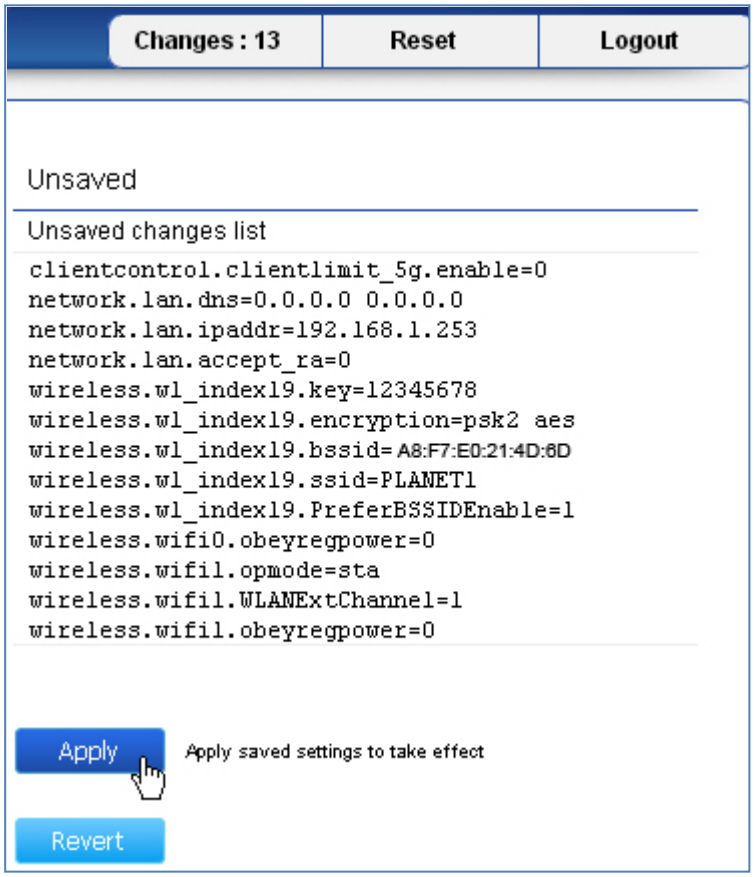

10. Click the AP-1.



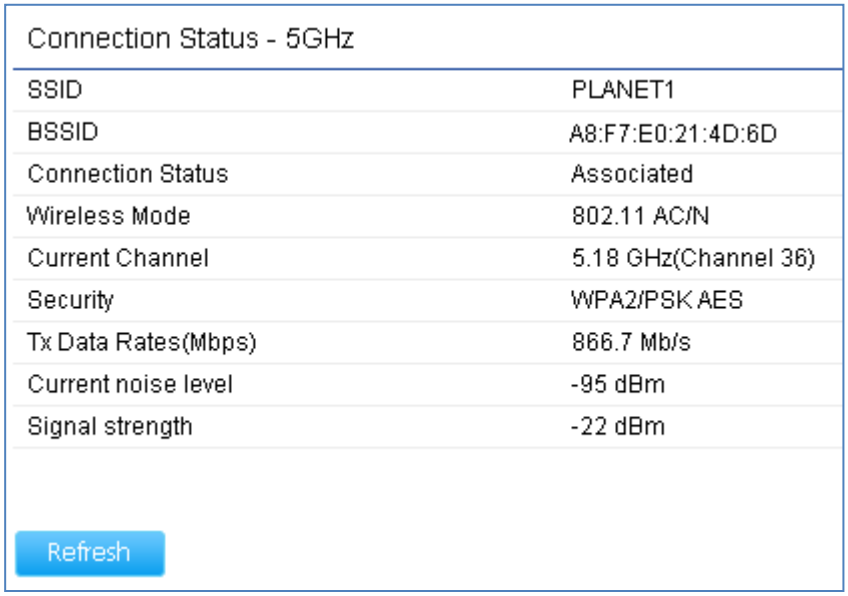

11. Click the check box of the preferred BSSID and configure the same encryption as the AP-1. Then, click "**Save**" to save the configurations.



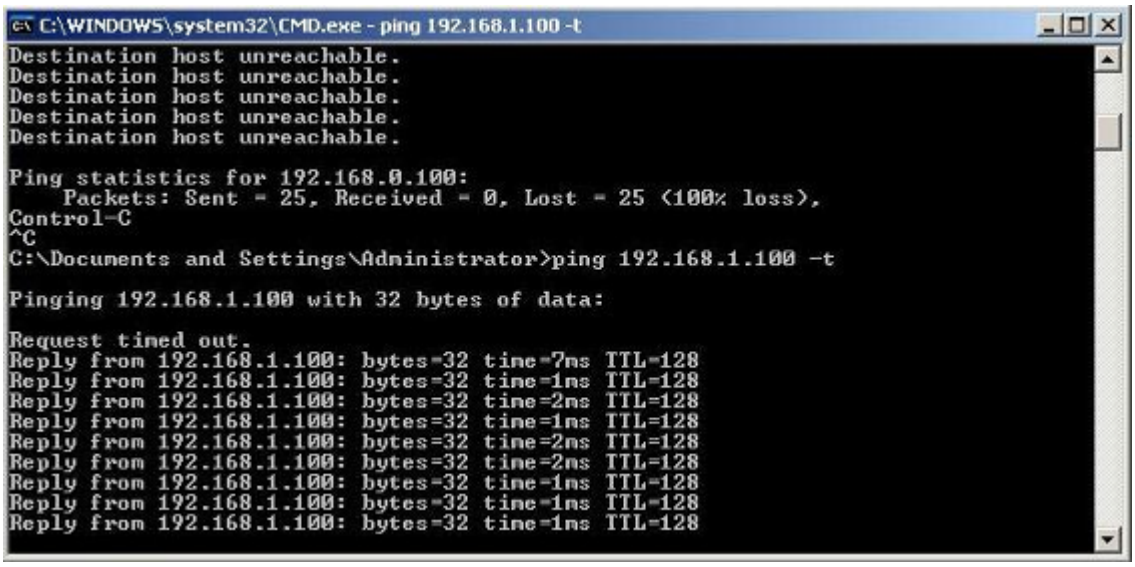
12. In the wireless main page, click "**Save**" to save the configurations.
13. Go to the "**Changes**" page to click "**Apply**" to apply the saved settings to take effect.




14. In the AP-2, go to the "**Overview-> Connections**" page to check whether the AP-2 is associated with the AP-1 successfully.




15. Use command line tool to ping each other to ensure the link is successfully established.
    E.g. from Site-1, ping 192.168.1.200; and at Site-2, ping 192.168.1.100.



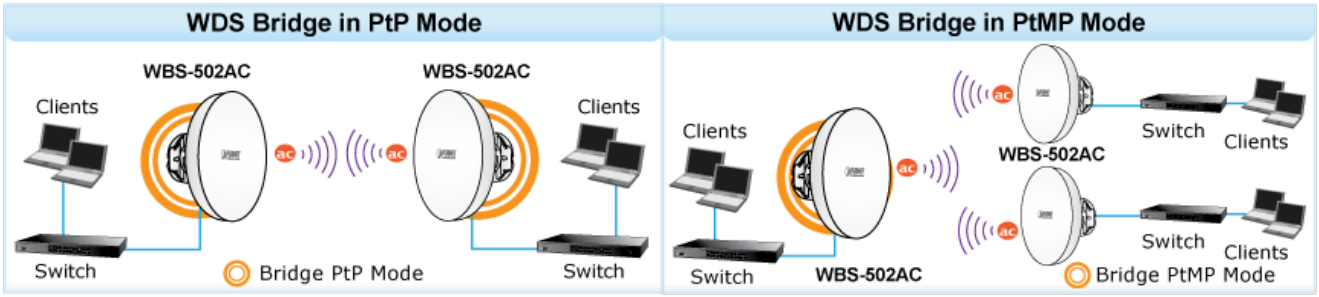

Note

The following should be noted:

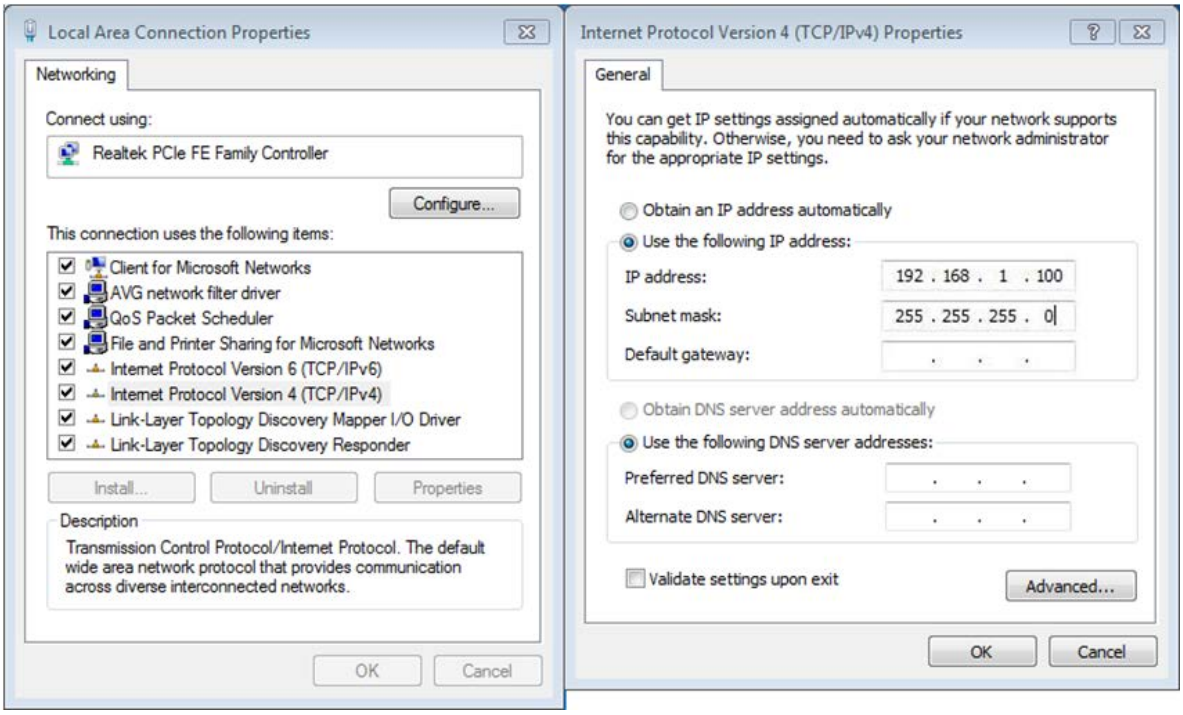
- The encryption method must be the same at both sites if configured.
- Both sites must be Line-of-Sight.
- For backhaul link, please configure the channel to a fixed one.
- For PtP connection over 1km, please adjust "**Distance**" setting to the actual distance between both sites in the both sites' wireless setting page.

# Q2: How to set up the WDS Connection

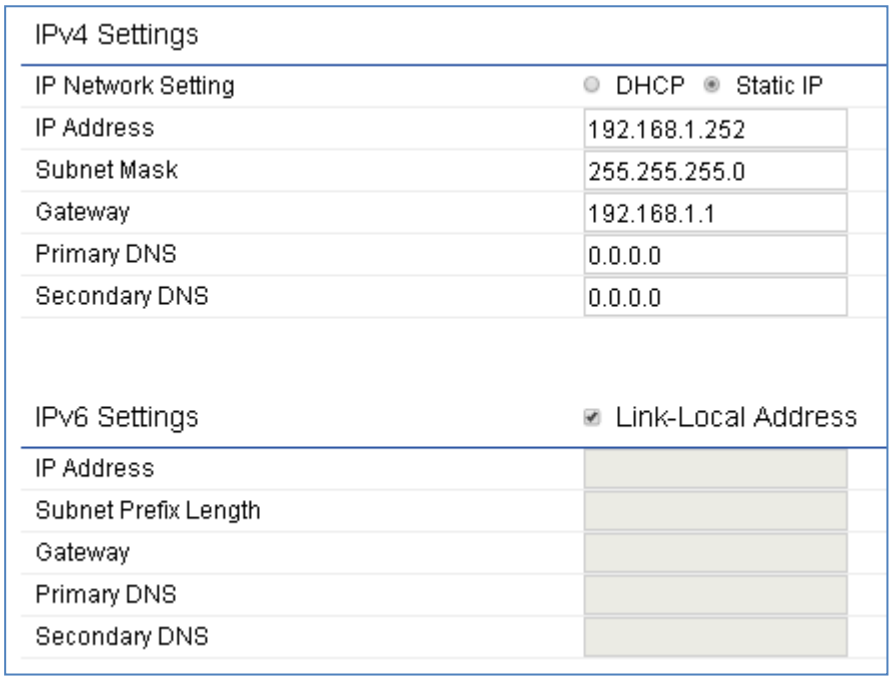
**Topology:**



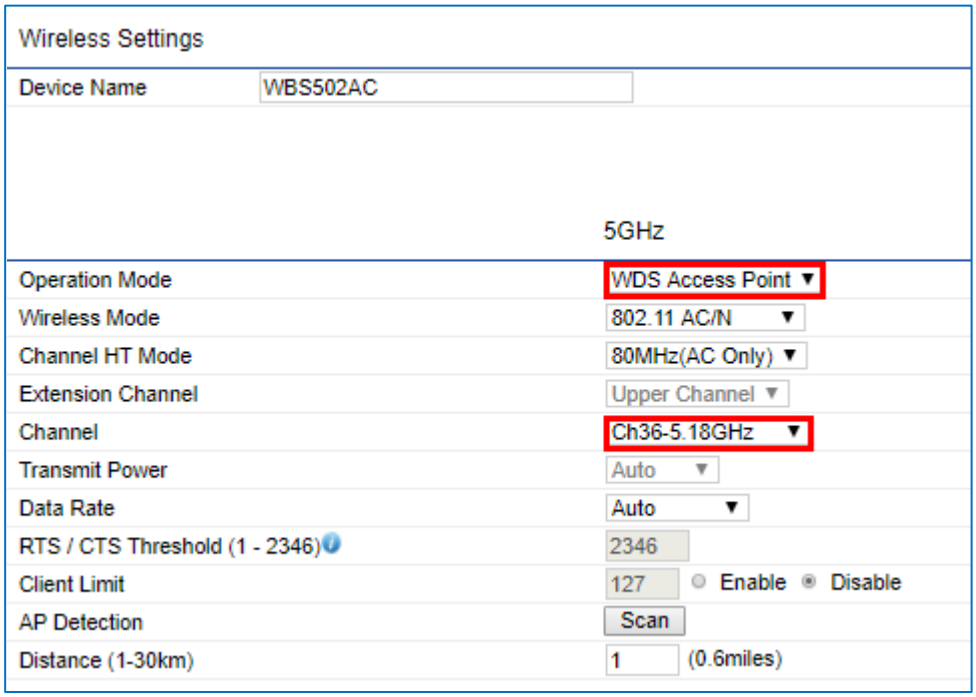

1. Use static IP in the PCs that are connected with AP-1 (Site-1) and AP-2 (Site-2). In this case, Site-1 is "192.168.1.100", and Site-2 is "192.168.1.200".



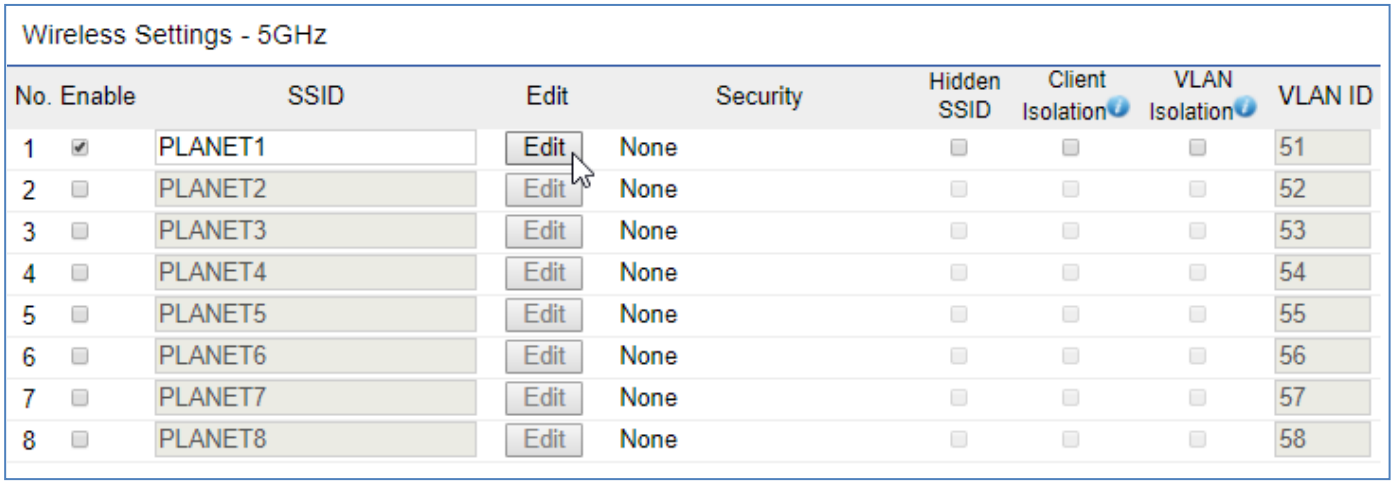

2. In the AP-1, go to "**Network-> Basic**" to configure the IP address to static and must different from the AP-2.



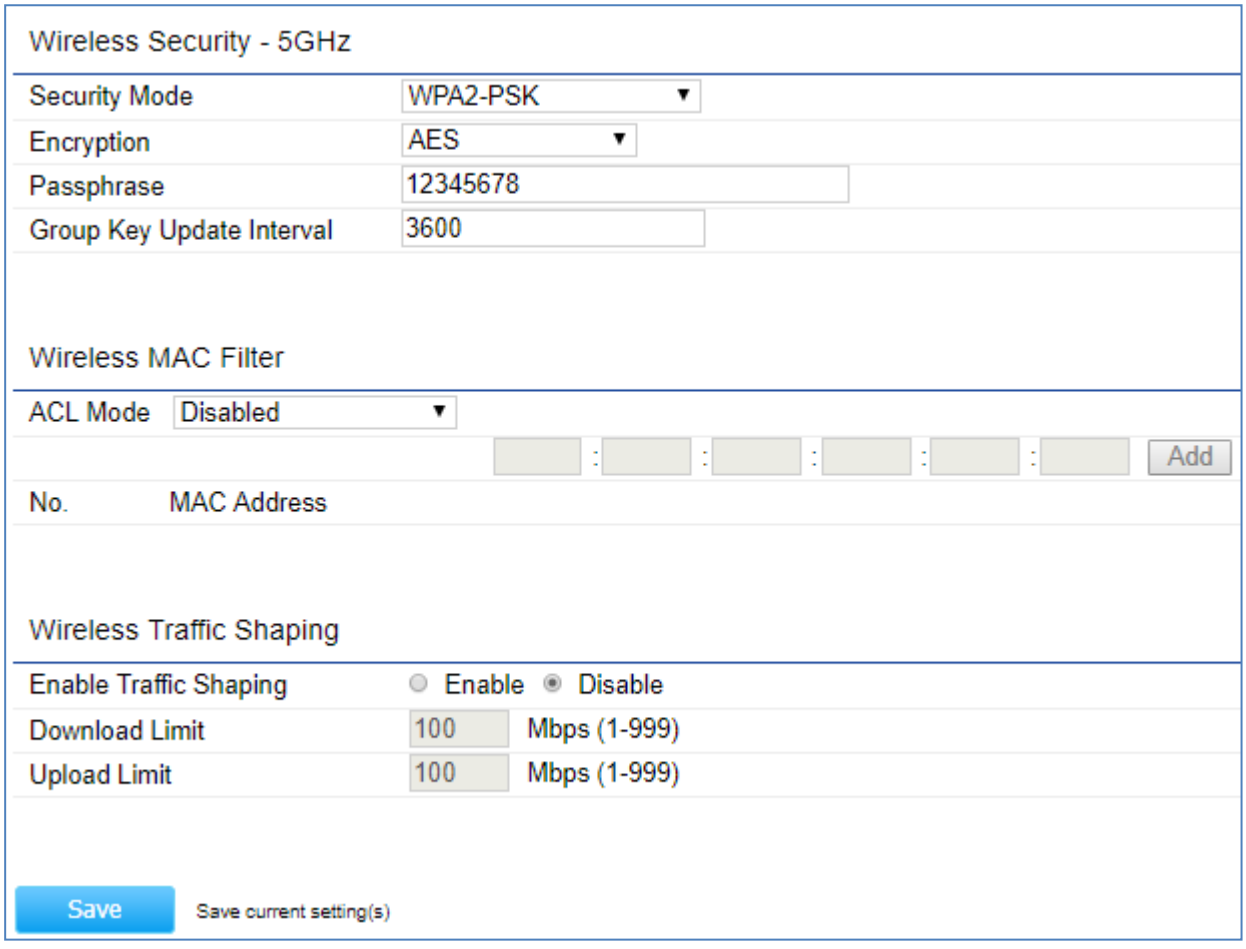

3. In the AP-1, go to "**Network-> Wireless**" page and configure the following wireless parameters:
   (1) Operation Mode: set to "**WDS Access Point**" mode.
   (2) Channel: set to a fixed channel (e.g. channel 36)



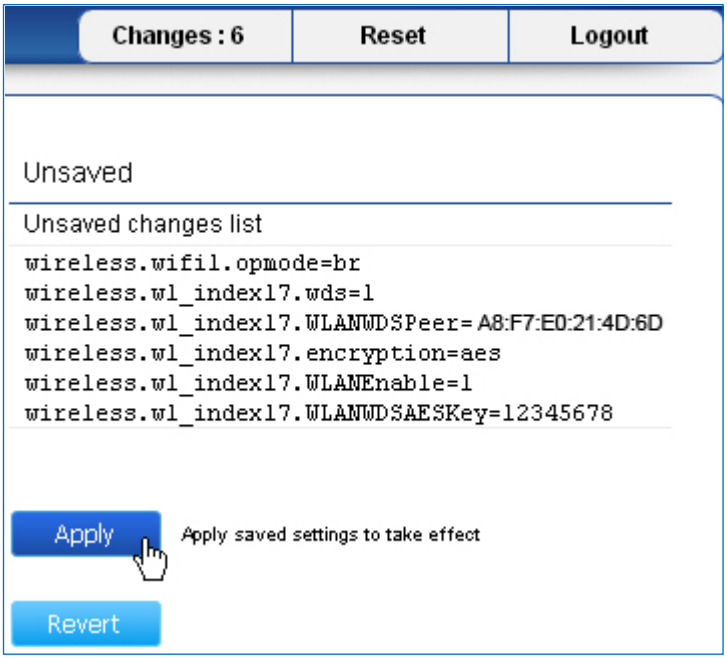

4. Click "**Edit**" in the wireless settings section.



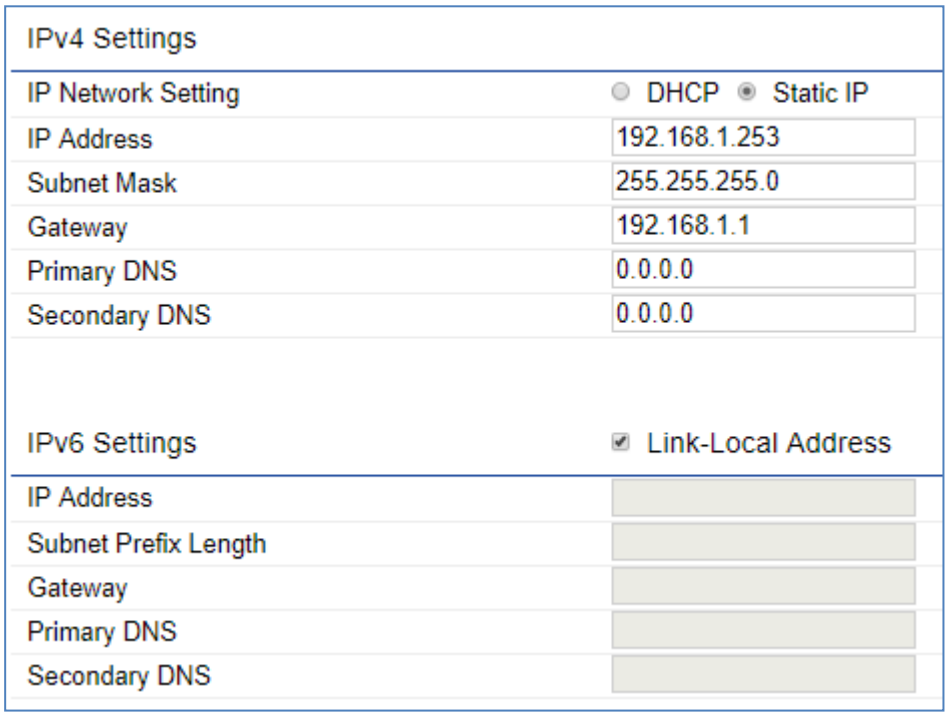

5. In the wireless security section, configure the encryption and passphrase (WPA2-PSK/AES is suggested). Then, click "**Save**" to go back to the main page.



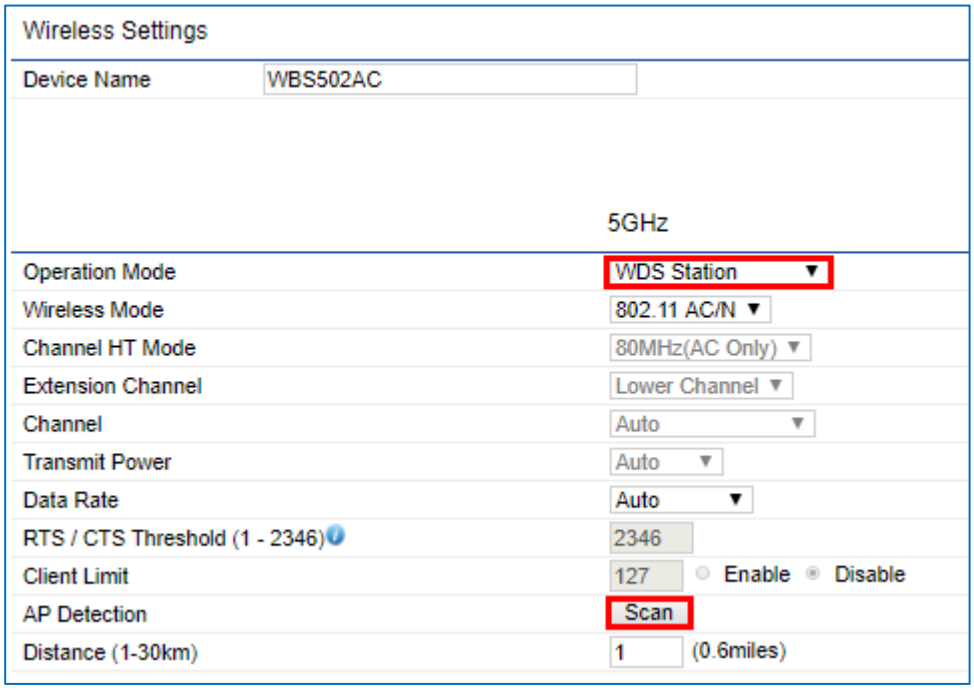

6. In the wireless main page, click "**Save**" to save the configurations.
7. Go to the "**Changes**" page to click "**Apply**" to apply the saved settings to take effect.



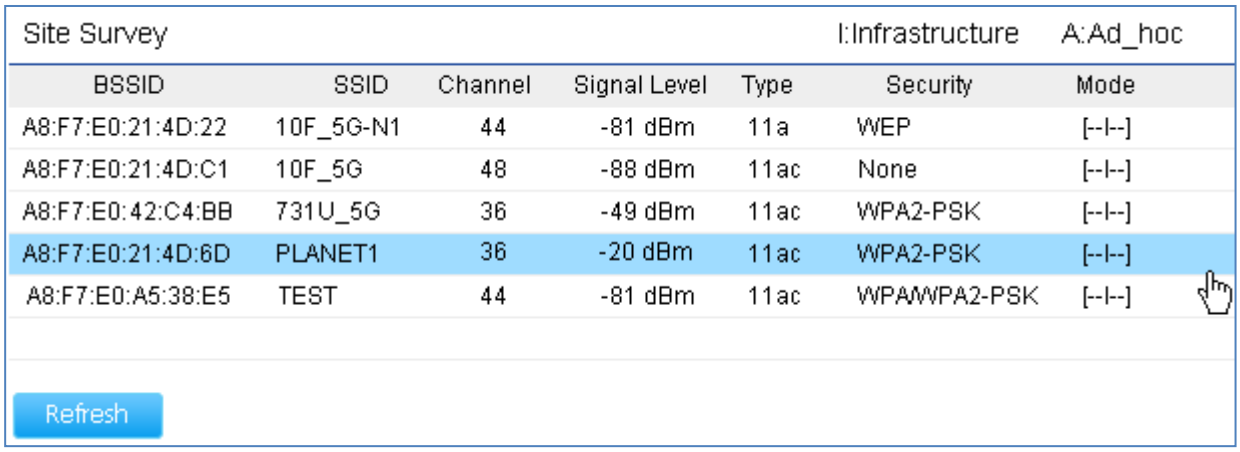

8. In the AP-2, go to "**Network-> Basic**" to ensure the IP address is static and different from the AP-1.



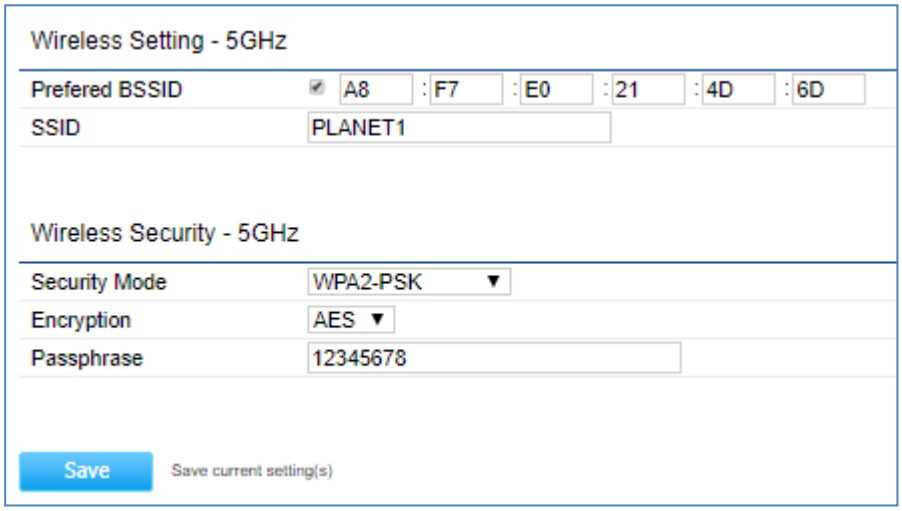

9. In the AP-2, go to "**Network-> Wireless**" page to configure the Operation Mode to "**WDS Station**" mode. Then, click "**Scan**" button to site survey the AP-1.



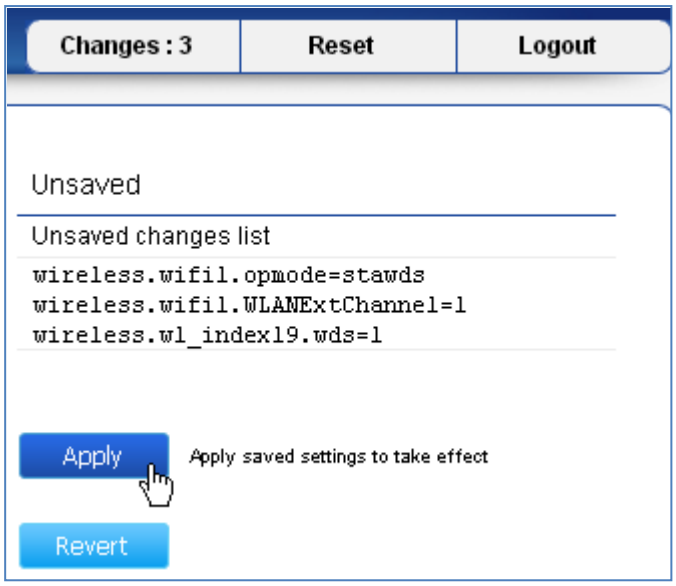

10. Click the AP-1.



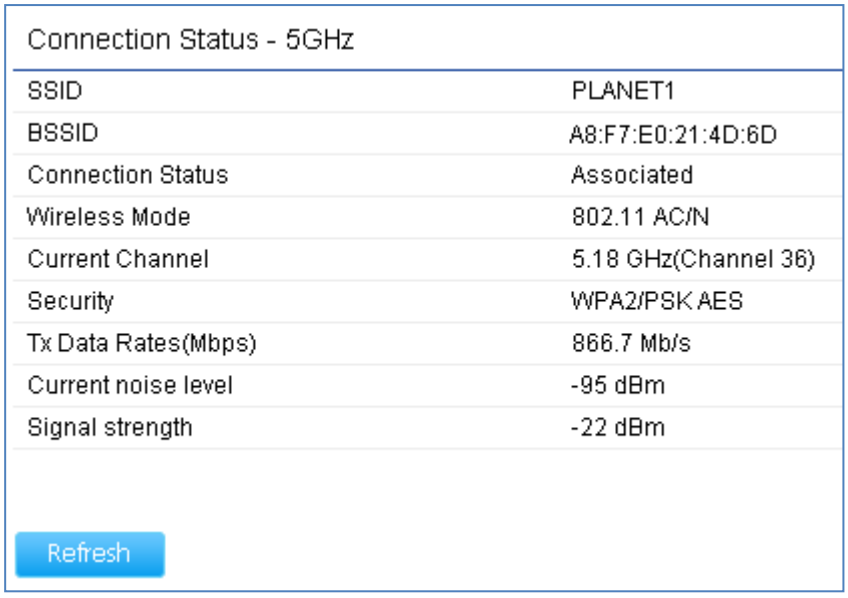

11. Click the check box of the preferred BSSID and configure the same encryption as the AP-1. Then, click "**Save**" to save the configurations.



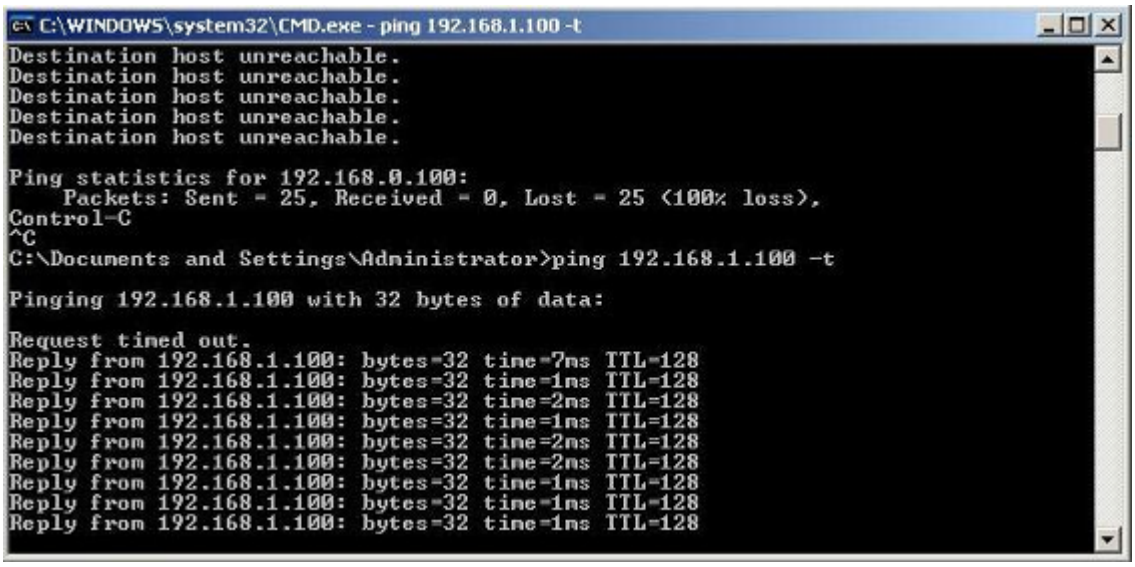
12. In the wireless main page, click “**Save**” to save the configurations.
13. Go to the “**Changes**” page to click “**Apply**” to apply the saved settings to take effect.




14. In the AP-2, go to the “**Overview-> Connections**” page to check whether the AP-2 is associated with the AP-1 successfully.




15. Use command line tool to ping each other to ensure the link is successfully established.
    E.g. from Site-1, ping 192.168.1.200; and at Site-2, ping 192.168.1.100.




Note

The following should be noted:

- The encryption method must be the same at both sites if configured.
- Both sites must be Line-of-Sight.
- For backhaul link, please configure the channel to a fixed one.
- For PtP connection over 1km, please adjust "**Distance**" setting to the actual distance between both sites in the both sites' wireless setting page.

# 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-ħtiġijiet 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<br>Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) | **Nederlands** | Hierbij verklaart , **PLANET Technology orporation,** 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** | *ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **900Mbps 802.11ac Wireless Outdoor CPE***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ*<br>*ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ* | **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<br>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<br>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,** apliecina, 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. |