PLANET
Networking & Communication

User's Manual

600Mbps Dual Band 802.11n Outdoor Wireless CPE

► **WDAP-8350**

www.PLANET.com.tw

Copyright

Federal Communication Commission Interference Statement

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

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

FCC Caution

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

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

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

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

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

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reasons/remarks
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use; limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

WEEE regulation

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

Revision

User Manual of PLANET 600Mbps Dual Band 802.11n Wireless Outdoor CPE

Model: WDAP-8350

Rev: 1.0 (January, 2016)

Part No. EM-WDAP-8350_v1.0

CONTENTS

FIGURE

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WDAP-8350. Before installing the AP, please verify the contents inside the package box.

WDAP-8350

Quick Guide

Stainless Tight Hoop Strip

x 2

Backplane & Mounting Bracket

Mounting Kit

RJ45 Waterproof Kit

Note

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

1.2 Product Description

Powerful Dual-Band Outdoor WLAN Solution

PLANET WDAP-8350 comes with a high transmission power of **500mW** which can bridge two remote nodes in **5GHz** frequency band and provides clients with **2.4GHz** wireless access over longer distance range. Its fully-protected hardware design makes it capable to ward off direct lightning strikes and unpredictable harsh weathers. Furthermore, the WDAP-8350 adopts the high-class Qualcomm Atheros SoC (System-on-a-Chip) and **Dual-OS Backup** mechanism that provide higher stability to meet the stringent requirements of outdoor solution.

More Flexible for Outdoor Environments

With its dual-RF design and by connecting optional specific types and higher gain antennas to its **N-Type** antenna connectors, the WDAP-8350 can adapt to various applications including connecting IP cameras at multiple locations to the security control center to deploy a surveillance system, or relaying the wireless signal from the urban to the suburban to provide wireless internet service to rural residents simultaneously. With the WDAP-8350, an outdoor wireless infrastructure can be speedily deployed, thus realizing the setting up of an outdoor, long-distance, dual-purpose unit.

All-Weather Rugged Protection

With the **IP66** rated aluminum housing, **Surge Arrester**, **Heater** design and wide-ranging operating temperature from **-40 to 70** degrees C, PLANET WDAP-8350 can perform normally under rigorous weather conditions, including thunderstorms, and hot and cold climates, thus maintaining the connection as stable as that in the general environments.

Seamless Failover and Roaming

In the actual user experience, a redundant setup is important in that the WDAP-8350 enables the auto failover mechanism to activate by using dual images (Dual-OS) while if the active OS fails, it can immediately switch to the standby OS. That can eliminate the difficulty of real-time support in long distance and make failover as simple as possible. Furthermore, it enhances handover of clients between APs by improving the handshaking process to promote better performance, thus reducing the handoff times between APs and associated clients, which means it can quickly hand over to the nearby AP without any disconnection. Benefiting from the auto-backup and fast-roaming, the WDAP-8350 is able to achieve a non-disruptive path failover and seamless roaming.

High-efficiency and Practical Solution to Separating Various Applications

PLANET WDAP-8350 supports multiple SSIDs (16 sets of SSIDs for each band) to allow each virtual wireless network to have a different set of security and also capable to map each VAP to specific virtual network through the use of VLAN tagging which enables isolation of guest and corporate networks. In addition, its dynamic rate adaptation mechanism for multicast guarantees the wireless bandwidth and service quality or the fixed rate of video streaming, which prevents from capacity wasting of multicast packets, thus utilizing the available bandwidth with more efficiency.

Advanced Value-added Characteristics

Featuring an **IPv4/IPv6** dual-stack network, the WDAP-8350 can work with the original IPv4 network structure and also support the cutting-edge IPv6 network, which provides migration from the IPv4 to IPv6 network with ease. With the dynamic power saving mode implementation, it is capable to detect the traffic loading, which consumes low standby power automatically, thus reducing power consumption by less than 30%.

Easy Deployment and Management

Compliant with **IEEE 802.3at PoE+** (**P**ower **o**ver **E**thernet) standard, the WDAP-8350 can be powered by a single UTP cable besides providing data transmission. It thus reduces the needs of extra cables and dedicated electrical outlets which are difficult to reach in outdoor environment. It enables the wireless LAN deployment to become more flexible and worry-free from the power outlet locations. Moreover, with the Planet Smart Discovery Utility, the WDAP-8350 is convenient to be configured remotely and with the Wireless Location Management, it is easy to locate online clients' information.

1.3 Product Features

- **Industrial-grade Wireless LAN**
  - Compliant with IEEE 802.11n 2T2R MIMO with backward compatible with 802.11a/b/g standard
  - Simultaneous 2.4GHz and 5GHz wireless connectivity
  - Equipped with Gigabit LAN and 600Mbps wireless connectivity (Dual-N Band)
  - IPv4 and IPv6 dual-stack management networks

- **Radio and Outdoor Characteristics**
  - Built-in 4 N-Type (Female) antenna connectors
  - High output power up to 500mW with multiple adjustable transmit power control
  - Built-in surge arrester and ground terminal for protection against lightning strikes
  - IP66 aluminum case protection
  - IEEE 802.3at PoE design
  - Wide operating temperature of -40 ~ 70 degrees C
  - Built-in Heater (will auto-launch at -30 degrees C) prevents freeze in harsh environment

- **Wireless Feature Characteristics**
  - Dual-N band performs backhaul WDS link at 5GHz and relay wireless signal at 2.4GHz
  - Multiple wireless modes: AP, WDS PtP and WDS PtMP
  - Supports up to 16 multiple-SSIDs at each frequency band
  - Multicast rate adaptation guarantees wireless bandwidth and service quality
  - Automatic ACK timeout detection smart for long-range connection

- **Secure and Highly-reliable Network Management**
  - Advanced 128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK(TKIP/AES) security, and 802.1x authentication
  - Supports IEEE 802.1Q tagged VLAN over WDS or mapping up to 32 SSIDs
  - Dual-image (dual-OS) backup mechanism
  - Easy Web-based UI and PLANET Smart Discovery supported
  - Telnet command line interface
  - Auto power saving mode reduces power consumption by 30%
  - Easily locate online clients information through the Wireless Location Management
  - System status monitoring includes statistics and associated client list

1.4 Product Specifications

Product	**WDAP-8350** **600Mbps 802.11n Dual Band Outdoor Wireless CPE**	
Hardware		
Interface	Wireless: IEEE 802.11n concurrent 2.4GHz and 5GHz, 2T2R MIMO LAN: 10/100/1000BASE-T, auto-MDI/MDIX, IEEE 802.3at PoE PD	
Antenna	Built-in 4 N-Type (female) antenna connectors with surge arrestor ※ The outdoor antennas need to be purchased separately	
Button/Connector	Reset button, ground terminal, ground lug	
LED	PWR, LAN, 2.4G, 5G	
Material	Aluminum	
Dimensions (W x D x H)	220 x 95 x 220mm	
Weight	2.34kg	
Power Requirement	IEEE 802.3at PoE+	
Power Consumption (max.)	< 24W (high-loading and heater) < 7W (power saving mode)	
Mounting Type	Mast, wall mount	
Wireless Interface Specifications		
Wireless Standard	IEEE 802.11a/n 5GHz IEEE 802.11b/g/n 2.4GHz	
Antenna Structure	802.11n: 2T2R MIMO at each frequency band	
Data Rate	IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54Mbps IEEE 802.11n (20MHz): up to 150Mbps IEEE 802.11n (40MHz): up to 300Mbp at each frequency band	
Media Access Control	CSMA/CA	
Modulation Type	802.11a/g/n: OFDM (BPSK/QPSK/16QAM/64QAM) 802.11b: DSSS (DBPSK/DQPSK/CCK)	
Band Mode	2.4G and 5G concurrent mode	
Frequency Range	2.4GHz: 2.400 ~ 2.484GHz 5GHz: 5.150 ~ 5.850GHz	
Operating Channel	2.4GHz	America -- FCC: 1~11 Europe -- ETSI: 1~13
	5GHz	America -- FCC: 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165 (total 24 channels) Europe -- ETSI:

		36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140 (total 16 channels) ※ 5GHz channel list may be vary in different countries and may be restricted to abide by regional regulatory compliance.
Channel Width	20MHz/40MHz	
Max. RF Power	27dBm for all rate levels and modulation modes	
Output Power Control	1 ~ 100%	
Software Features		
Wireless Mode	■ AP ■ WDS PTP ■ WDS PTMP	
Wireless Encryption	■ WEP (64/128-bit) encryption security ■ WPA / WPA2 (TKIP/AES) ■ WPA-PSK/WPA2-PSK (TKIP/AES) ■ 802.1x authentication	
Wireless Advanced	Enable/Disable SSID broadcast	
	Max. associated station number restriction	
	Multiple SSIDs: up to 16 at 2.4GHz and 16 at 5GHz	
	Supports multiple VLANs mapping to multiple SSIDs	
	Supports fast roaming across APs	
	Provides wireless statistics	
Max. Wired Client	Unlimited	
Max. Wireless Client	Theoretical value: 127 at each band Recommended value: 50 at each band	
Max. WDS Peers	Up to 16 at 2.4GHz and 16 at 5GHz	
QoS	Supports multicast rate adaptation mechanism to guarantee the wireless bandwidth and service quality	
LAN	Static IP, DHCP	
	IPv4 and IPv6 dual-stack management network	
	Supports 802.1Q tagged VLAN	
System Management	Web-based (HTTP) and Telnet command line Interface Supports NTP synchronization Easy firmware upgrade via HTTP/TFTP Easy system backup/restore via HTTP/TFTP Easily locate online clients information through the Wireless Location Management Supports Dual-OS auto-backup mechanism Supports Auto Power Saving Mode mechanism Supports PLANET Smart Discovery Utility	

Standards Conformance	
Standard Compliance	IEEE 802.11n (2T2R, dual-N band up to 600Mbps) IEEE 802.11a IEEE 802.11g IEEE 802.11b IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T
Other Protocols and Standards	CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, SNTP
Environment & Certification	
Temperature	Operating: -40 ~ 70 degrees C Storage: -40 ~ 75 degrees C ※ Built-in Heater (will auto-launch at -30 degrees C)
Humidity	Operating: 10 ~ 95% (non-condensing) Storage: 5 ~ 95% (non-condensing)
IP Level	IP66
ESD Protection	±15kV air-gap discharge ±8kV contact discharge
Surge Protection	±6kV line to ground ±2kV line to line
MTBF	1553658 hrs at 25 degrees C 335788 hrs at 60 degrees C
EMC Emissions Class	B
Regulatory Compliance	CE, FCC, RoHS

Chapter 2. Hardware Installation

Please follow the instructions below to connect WDAP-8350 to the existing network devices and your computers.

2.1 Hardware Description

Physical Specifications	
Dimensions (W x D x H)	220 x 95 x 220mm
Weight	2.34 ± 5g (gross weight)

Appearance

Figure 2-1 Three-way View

2.1.1 The Rear Panel - LED

The rear panel shows the signal indicators of power, Ethernet, 2.4GHz and 5GHz radio status. **Figure 2-2** shows the rear panel of the WDAP-8350.

Rear Panel – LED

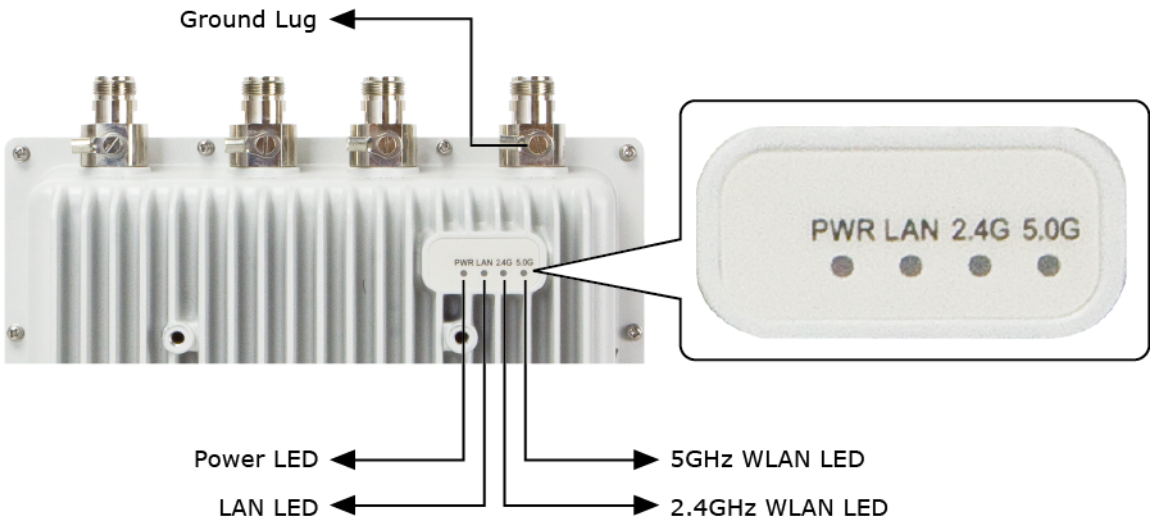


Figure 2-2 LED

LED definition

LED	Color	State	Meaning
Power	**Green**	On	The AP is powered on.
		Off	The AP is powered off.
LAN	**Green**	On	Port linked
		Off	No link
2.4G	**Green**	On	2.4G radio is on.
		Blinking	Data is transmitting or receiving on the 2.4GHz.
		Off	2.4G radio is off.
5.0G	**Green**	On	5G radio is on.
		Blinking	Data is transmitting or receiving on the 5GHz.
		Off	5G radio is off.

Table 2-1 LED Indication

2.1.2 The Top/Bottom Panel – Connector and Port

The top/bottom panel provides the physical connectors connected to the antenna, surge protection wiring and any other network device. **Figure 2-3** and **Figure 2-4** show the top and bottom panels of the WDAP-8350.

Antenna Connector

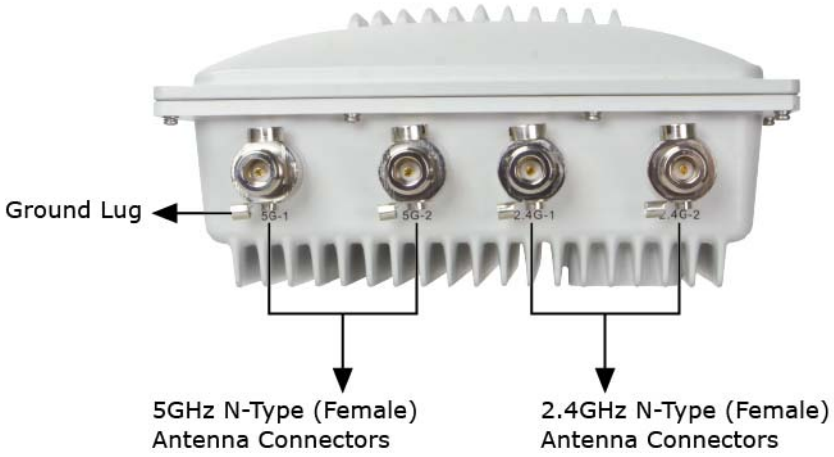


Figure 2-3 Antenna Connectors

Button & Port

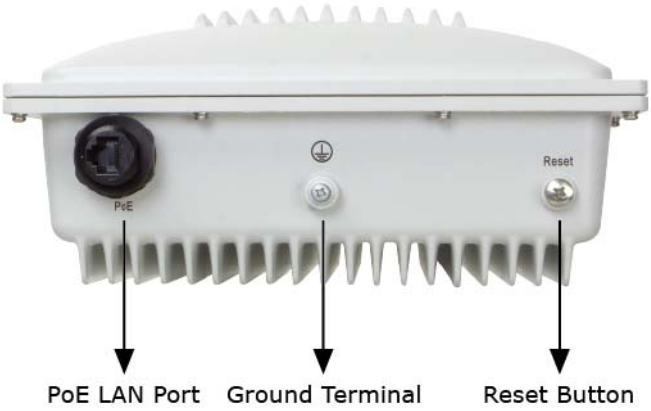


Figure 2-4 Port and Button

H/W Interface definition

Object	Description
Antenna Connector	4 N-type (Female) antenna connectors Built-in surge arrestor on each antenna connector
PoE LAN Port	10/100/1000Mbps RJ-45 port, auto MDI/ MDI-X IEEE 802.3at PoE/PD supported, Class 4
Reset Button	Press the **Reset** button on the device for over 5 seconds to return to the factory default setting.
Ground Lug	The WDAP-8350 has a built-in surge arrestor on each antenna connector. Connecting the grounding wire to the ground lug is required to protect the lightning attack; otherwise, a sudden lightning could cause fatal damage to the WDAP-8350.
Ground Terminal	Attaching the ring grounding terminal to the ground terminal of the WDAP-8350 is required to protect the lightning attack; otherwise, a sudden lightning could cause fatal damage to the WDAP-8350.

After the AP is mounted on a pole/wall and before you provide power to the system, you need to complete the wiring in the position of AP installation. To connect the AP to a reliable earth ground, perform the following steps:

1. Strip one end of the ground wire to the length required for the ground lug or terminal.
2. Crimp the ground wire to the ground lug or ring terminal, using a crimp tool of the appropriate size.
3. Connect the other end of the ground wire to a suitable grounding point at your site.

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 WDAP-8350 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 WDAP-8350, 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, 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** complete grounding wired with the WDAP-8350; otherwise, a sudden lightning could cause fatal damage to the WDAP-8350. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**

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 line made. Antennas, masts, towers, guy wires or cables may lean or fall and con if they are touching or holding any part of equipment when it contacts electri 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 – Pole Mounting

Please install the AP on the pole according to the following Steps.

Step 1. Install the backplane at the rear of WDAP-8350 and screw the 4 short screws with a Phillips screwdriver. Make the long screw rod pass through the holes of the backplane and put the flat pad, spring shim and the screw nut on it in proper order; do not lock it tight.

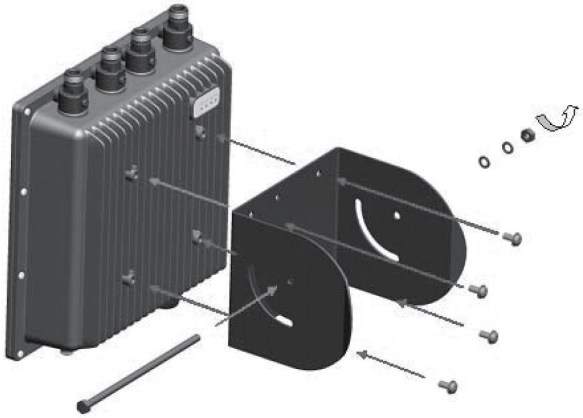


Figure 3-1 Install the backplane

Step 2. Lock the 2 stainless tight hoop strips around the pole by passing through the mounting bracket and lock the fastening screws.

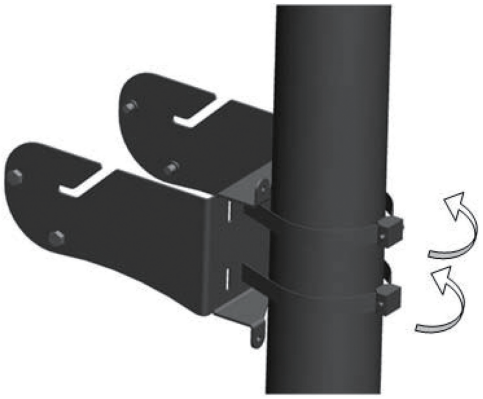


Figure 3-2 Install the stainless tight hoop strips

Step 3. Install the device with the backplane to the mounting bracket on the column and fix the device and mounting bracket together by using 4 hex cap screws.

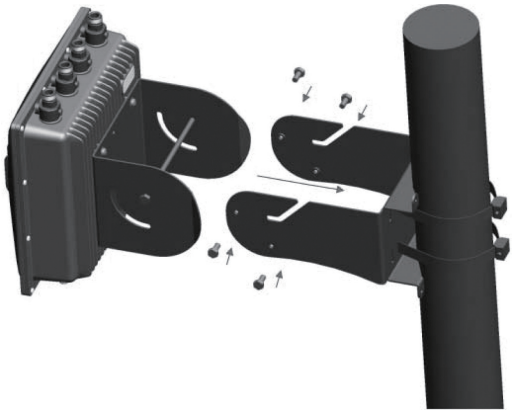


Figure 3-3 Assemble the AP on the pole

3.4 Installing the AP – Wall Mounting

Please install the AP on the wall according to the following steps.

Step 4. As shown in Step 3-1, install the backplane at the rear of the WDAP-8350 first. Then, mark each point in the bracket for the screws. Remove the bracket to drill the points and insert the plastic wall-mounts. Use screws to lock the bracket with a screwdriver.

Step 5. Assemble the device with the mounting bracket on the wall by using 4 short screws and 1 long screw.

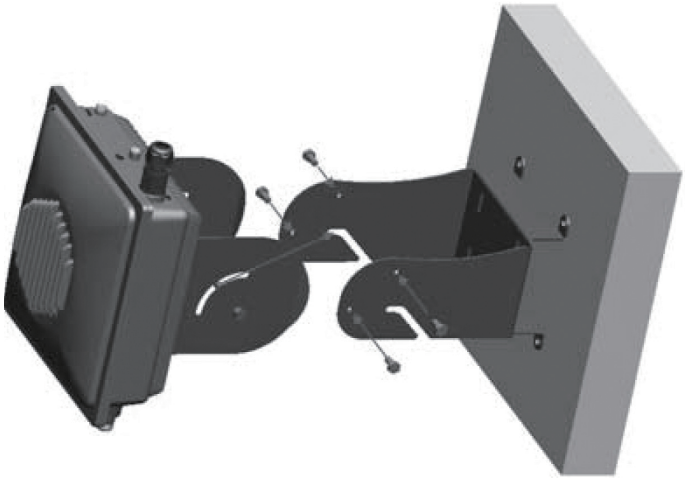


Figure 3-4 Assemble the AP on the wall

3.5 Connecting the Antennas and Powering It Up

Please install the antennas according to the following steps.

Step 1. You can directly connect the antenna to the AP if the antenna's connector is N-Type (M). If not, please connect the N-Type (M) RF cables to N-Type (F) antenna connectors of the WDAP-8350, and connect the other end of the RF cables to the N-Type (F) antennas.

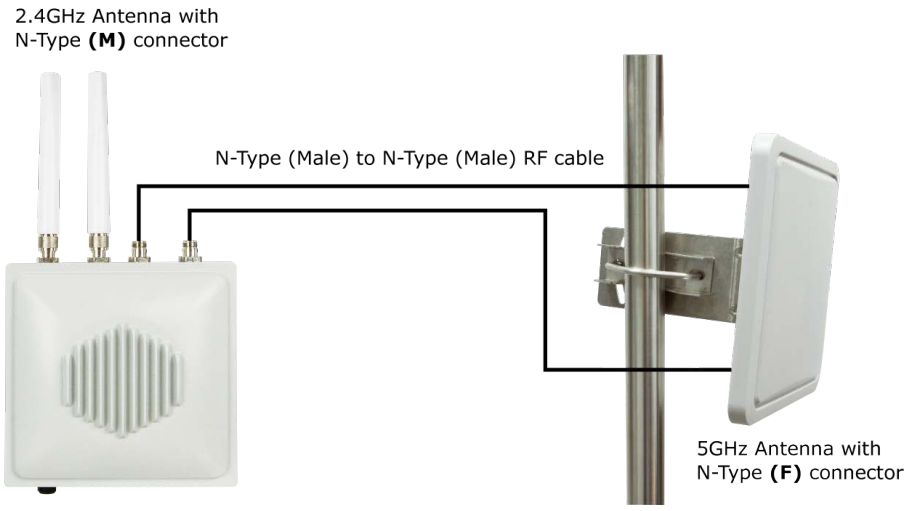


Figure 3-5 Connect to the antennas

(※ The actual antenna connection depends on the antenna type you choose. The antennas are required and must be purchased separately.)

Step 2. Plug the RJ45 Ethernet cable into the PoE port of the WDAP-8350 through the waterproof kit, and plug the other side of the RJ45 cable into the PoE port of the PoE switch to finish the installation.

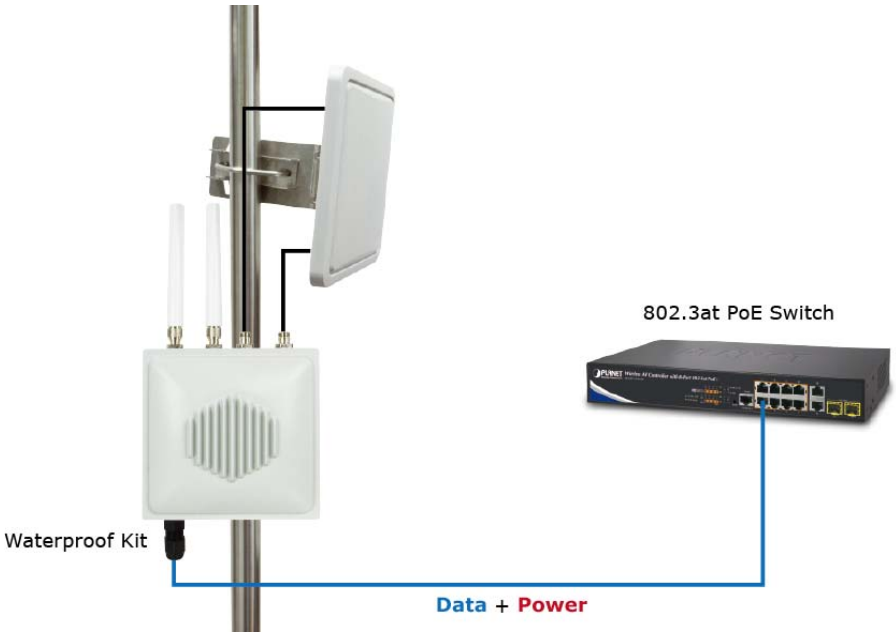


Figure 3-6 Connect the AP to the PoE Switch

(※ Please remember to install the ground cables onto the ground terminal and ground lugs)

Step 3. Successful installation.

Chapter 4. Quick Installation Guide

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

Note

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 WDAP-8350 is **192.168.1.10**. And the default Subnet Mask is 255.255.255.0. These values can be changed as you want. In this guide, we use all the default values for description.

Connect the WDAP-8350 with your PC by an Ethernet cable plugging in PoE LAN port on one side and in LAN port of PC on the other side. Please power on the WDAP-8350 by PoE switch through the PoE port.

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 manual if needed.

4.1.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx (If the default IP address of the WDAP-8350 is 192.168.1.10, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 253, except 192.168.1.10). Subnet Mask is 255.255.255.0.
- If the DHCP server is enabled in the PoE switch, please disable it before finishing configuring the AP.

1 Select **Use the following IP address** radio button, and then configure the IP address of the PC.

2 For example, as the default IP address of the WDAP-8350 is 192.168.1.10 and the DSL router is 192.168.1.254, you may choose from 192.168.1.1 to 192.168.1.253, except 192.168.1.10.

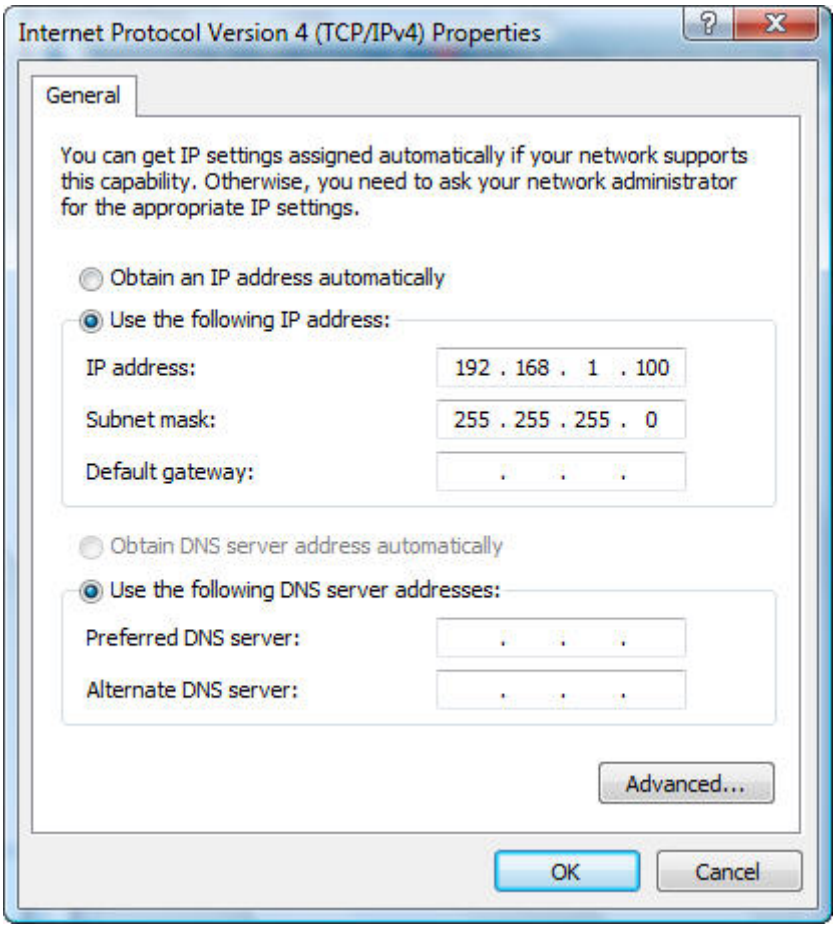


Figure 4-1 TCP/IP Setting

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.

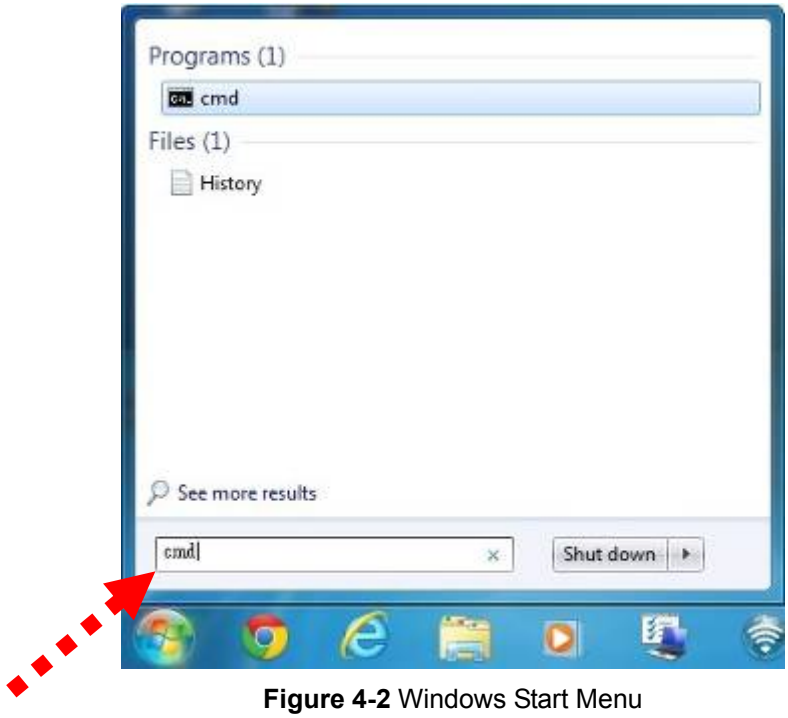


Figure 4-2 Windows Start Menu

3. Open a command prompt, type ping **192.168.1.10** 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.

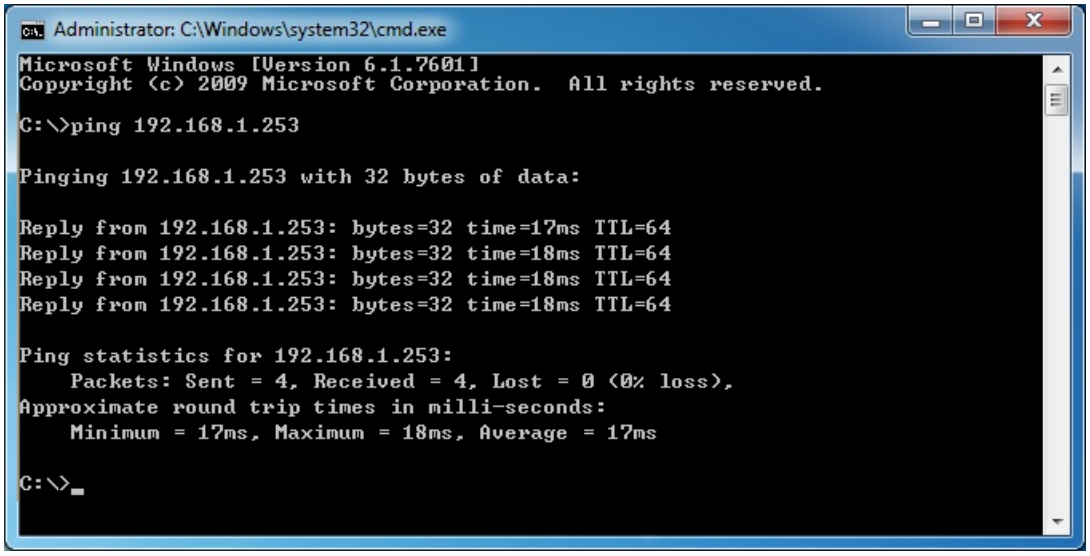


Figure 4-3 Successful Result of Ping command

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

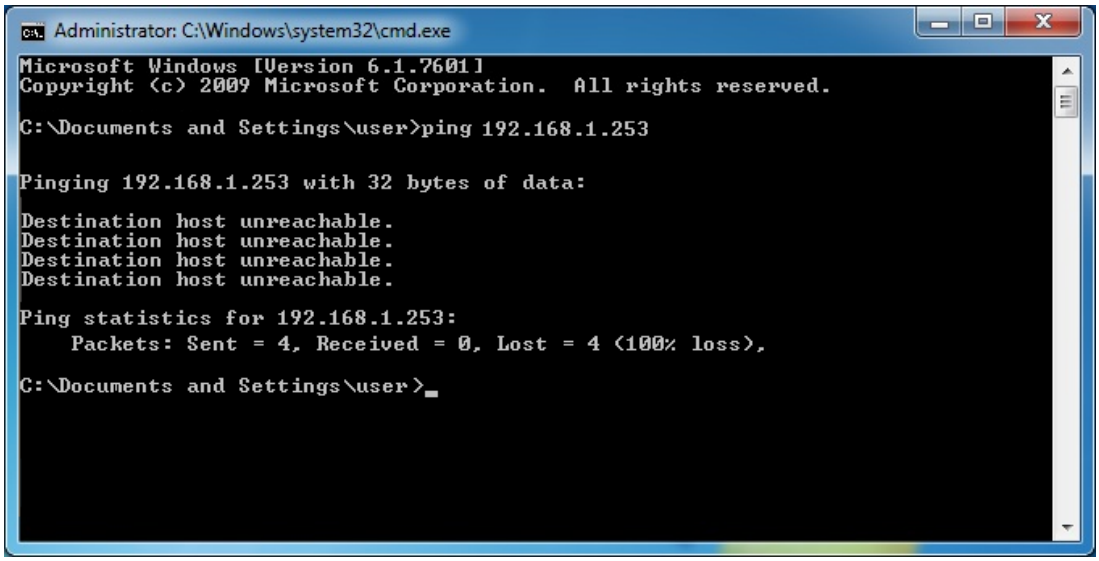


Figure 4-4 Failed Result of Ping Command

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 AP with the web browser.

Step 1. To access the configuration utility, open a web-browser and enter the default IP address http://192.168.1.10 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: **192.168.1.10**

Default User name: **admin**

Default Password: **admin**

Note

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

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and features under the main menu below, allowing you to manage the AP with ease.

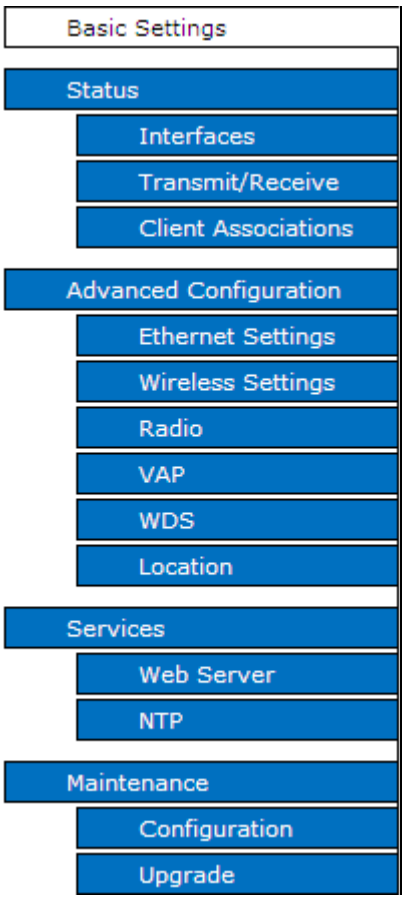


Figure 5-1 Main Menu

5.1 Basic Settings

On the Basic Settings page, you can view various information about the AP, including IP and MAC address information, and configure the administrator password for the AP.

Choose menu "**Basic Settings**" to view the basic information of the AP.

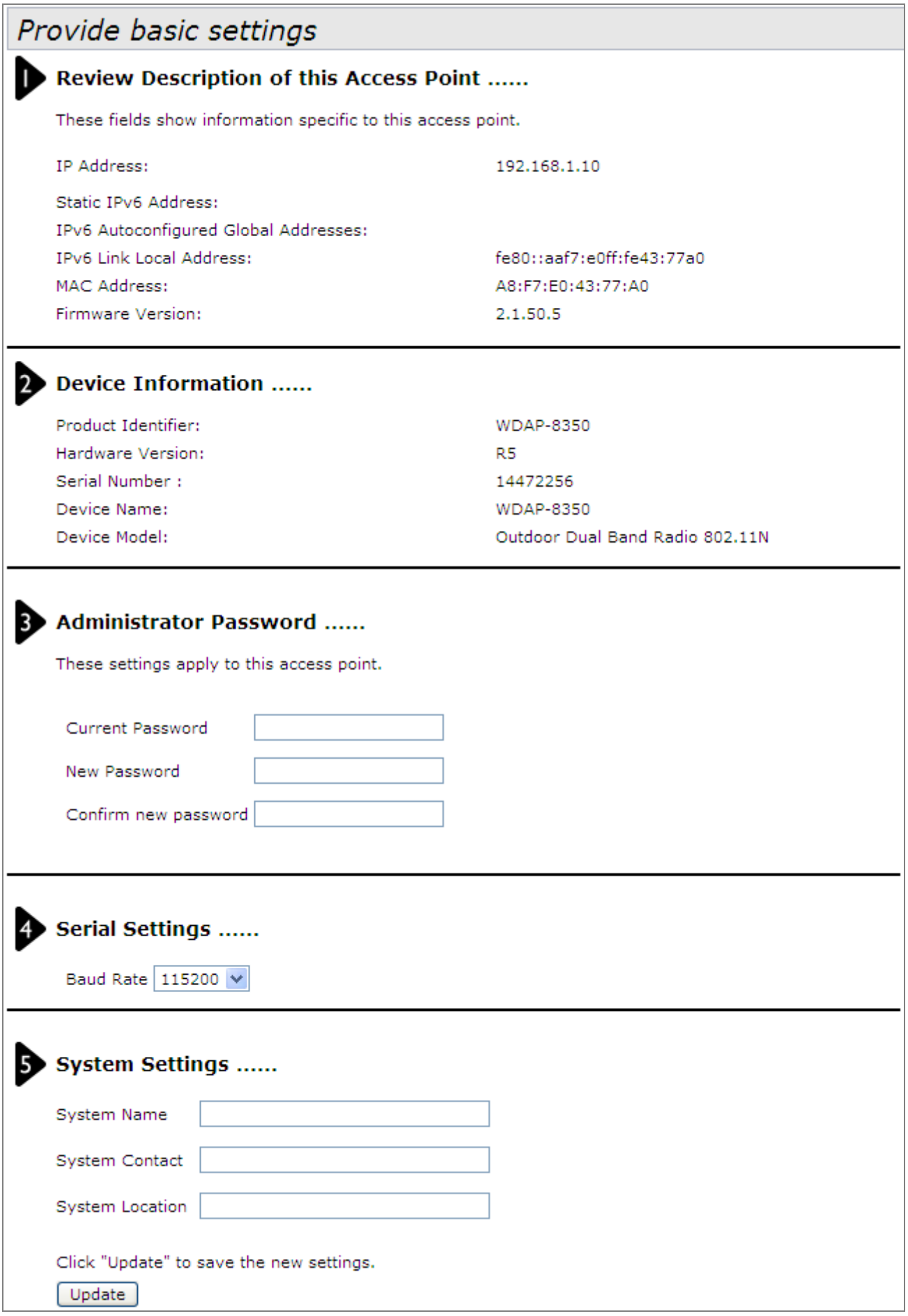


Figure 5-2 Basic Settings

The page includes the following fields:

Object	Description
IP Address	Shows the IP address assigned to the AP. This field is not editable on this page because the IP address is already assigned (either by DHCP, or statically through the Ethernet Settings page).
Static IPv6 Address	Shows the IPv6 address assigned to the AP. This field is not editable on this page because the IP address is already assigned (statically through the Ethernet Settings page).
IPv6 Autoconfigured Global Addresses	If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed.
IPv6 Link Local Address	Shows the IPv6 Link Local address, which is the IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
MAC Address	Shows the MAC address of the AP. The address shown here is the MAC address associated with the management interface. This is the address by which the AP is known externally to other networks.
Firmware Version	Shows version information about the firmware currently installed on the AP. As new versions of the WLAN AP firmware become available, you can upgrade the firmware on your APs.
Product Identifier	Identifies the AP hardware model.
Hardware Version	Identifies the AP hardware version.
Serial Number	Shows the AP serial number.
Device Name	Generic name to identify the type of hardware.
Device Description	Provides information about the product hardware.
Current Password	Enter the current administrator password. You must correctly enter the current password before you are able to change it.
New Password	Enter a new administrator password. The characters you enter are displayed as bullet characters to prevent others from seeing your password as you type. The administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces. Note: As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.
Confirm New Password	Re-enter the new administrator password to confirm that you typed it as intended.
Baud Rate	Select a baud rate for the serial port connection. The baud rate on the AP must match the baud rate on the terminal or terminal emulator to connect to the AP command-line interface (CLI) by using a serial (console) connection.

	The following baud rates are available: 9600, 19200, 38400, 57600, 115200.
System Name	Enter a name for the AP. This name appears only on the Basic Settings page and is a name to identify the AP to the administrator. Use up to 64 alphanumeric characters, for example My AP.
System Contact	Enter the name, e-mail address, or phone number of the person to contact regarding issues related to the AP.
System Location	Enter the physical location of the AP, for example Conference Room A.

How to connect to the AP by Using the IPv6 Address:

Connect to the AP by typing the IPv6 global or link local address into your browser as described below.

Note: The following instructions and examples work with Microsoft Internet Explorer 10(IE10) and might not work well with other browsers.

To connect to an IPv6 global address, add square brackets around the IPv6 address.

For example, if the AP global IPv6 address is 2520::230:abff:fe00:2420, type the following address into the address field: http://[2520::230:abff:fe00:2420].

To connect to the iPv6 link local address, replace the colons (:) with hyphens (-), add the interface number preceded with an "s," then add ".ipv6-literal.net."

For example, if the AP link local address is fe80::230:abff:fe00:2420, and the Windows interface is defined as "%6," type the following address into the address field: http://fe80--230-abff-fe00-2420s6.ipv6-literal.net.

5.2 Status

5.2.1 Interfaces

This page displays the current settings of the AP. It displays the Wired Settings and the Wireless Settings.

Choose menu "**Status -> Interfaces**" to view and edit the wired or wireless interface setting of the AP.

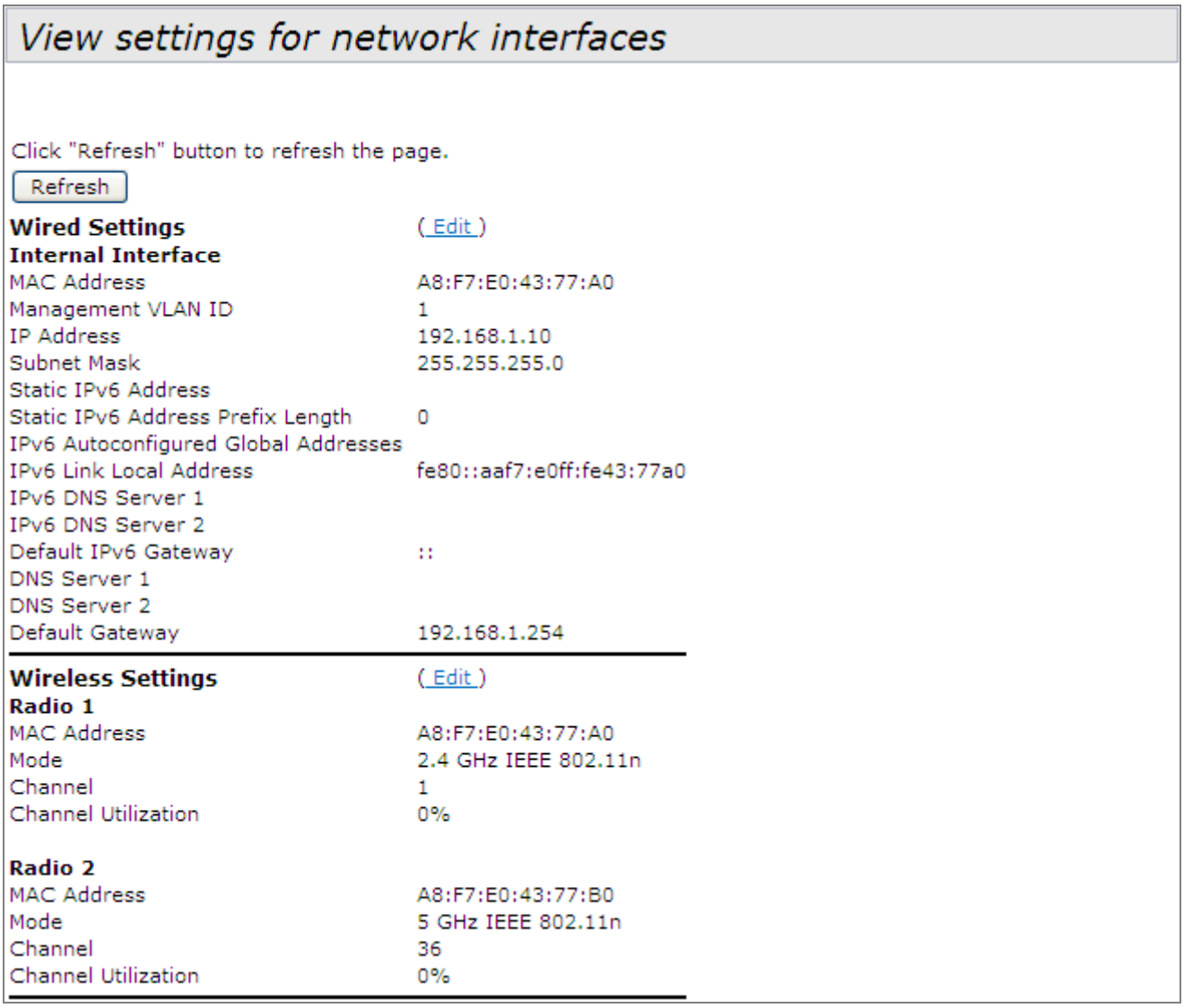


Figure 5-3 Basic Settings

- **Wired Settings (Internal Interface)**

The Internal interface includes the Ethernet MAC Address, Management VLAN ID, IP Address (IPv4 and IPv6), Subnet Mask, and DNS information (IPv4 and IPv6). If you want to change any of these settings, click the Edit link. After you click **Edit**, you are redirected to the **Ethernet Settings** page.

- **Wireless Settings**

The Radio Interface includes the Radio Mode, Channel and Channel Utilization. The Wireless Settings section also shows the MAC address (read-only) associated with each radio interface.

If you want to change the Radio Mode or Channel settings, click the Edit link. After you click Edit, you are redirected to the Wireless Settings page.

5.2.2 Transmit/Receive

The Transmit/Receive page provides basic information for the current AP. It also includes a real-time display of the transmit and receive statistics for the AP and VAP Ethernet interfaces for both radios. All transmit and receive statistics shown are totals since the AP was rebooted. If you reboot the AP, the transmit and receive totals will reset.

Choose menu "**Status -> Transmit/Receive**" to view the transmit and receive statistics of the AP.

Note: The statistics of the Ethernet interface and the VAPs on both radio interfaces are counted separately. There are no connections between them.

View transmit and receive statistics for this access point

Click "Refresh" button to refresh the page.

Refresh

Interface	Status	MAC Address	Name (SSID)
LAN	up	A8:F7:E0:43:77:A0	-
wlan0:wds0	unlinked	A8:F7:E0:43:77:A0	8350_WDS_2G
wlan0:vap1	up	A8:F7:E0:43:77:A1	PLANET_AP_2G vap1
wlan0:vap2	down	A8:F7:E0:43:77:A2	Virtual Access Point 2
wlan0:vap3	down	A8:F7:E0:43:77:A3	Virtual Access Point 3
wlan0:vap4	down	A8:F7:E0:43:77:A4	Virtual Access Point 4
wlan0:vap5	down	A8:F7:E0:43:77:A5	Virtual Access Point 5
wlan0:vap6	down	A8:F7:E0:43:77:A6	Virtual Access Point 6
wlan0:vap7	down	A8:F7:E0:43:77:A7	Virtual Access Point 7
wlan0:vap8	down	A8:F7:E0:43:77:A8	Virtual Access Point 8
wlan0:vap9	down	A8:F7:E0:43:77:A9	Virtual Access Point 9
wlan0:vap10	down	A8:F7:E0:43:77:AA	Virtual Access Point 10
wlan0:vap11	down	A8:F7:E0:43:77:AB	Virtual Access Point 11
wlan0:vap12	down	A8:F7:E0:43:77:AC	Virtual Access Point 12
wlan0:vap13	down	A8:F7:E0:43:77:AD	Virtual Access Point 13
wlan0:vap14	down	A8:F7:E0:43:77:AE	Virtual Access Point 14
wlan0:vap15	down	A8:F7:E0:43:77:AF	Virtual Access Point 15
wlan1:wds0	unlinked	A8:F7:E0:43:77:B0	8350_WDS_5G
wlan1:vap1	down	A8:F7:E0:43:77:B1	Virtual Access Point 1
wlan1:vap2	down	A8:F7:E0:43:77:B2	Virtual Access Point 2
wlan1:vap3	down	A8:F7:E0:43:77:B3	Virtual Access Point 3
wlan1:vap4	down	A8:F7:E0:43:77:B4	Virtual Access Point 4
wlan1:vap5	down	A8:F7:E0:43:77:B5	Virtual Access Point 5
wlan1:vap6	down	A8:F7:E0:43:77:B6	Virtual Access Point 6
wlan1:vap7	down	A8:F7:E0:43:77:B7	Virtual Access Point 7
wlan1:vap8	down	A8:F7:E0:43:77:B8	Virtual Access Point 8
wlan1:vap9	down	A8:F7:E0:43:77:B9	Virtual Access Point 9
wlan1:vap10	down	A8:F7:E0:43:77:BA	Virtual Access Point 10
wlan1:vap11	down	A8:F7:E0:43:77:BB	Virtual Access Point 11
wlan1:vap12	down	A8:F7:E0:43:77:BC	Virtual Access Point 12
wlan1:vap13	down	A8:F7:E0:43:77:BD	Virtual Access Point 13
wlan1:vap14	down	A8:F7:E0:43:77:BE	Virtual Access Point 14
wlan1:vap15	down	A8:F7:E0:43:77:BF	Virtual Access Point 15

Figure 5-4 Transmit/Receive Statistics – 1

Transmit

Interface	Total packets	Total bytes	Total dropped packets	Total dropped bytes	Errors
LAN	161	77998	0	0	0
wlan0:wds0	0	0	20	13312	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:wds0	0	0	33	23400	0
wlan1:vap1	0	0	0	0	0
wlan1:vap2	0	0	0	0	0
wlan1:vap3	0	0	0	0	0
wlan1:vap4	0	0	0	0	0
wlan1:vap5	0	0	0	0	0
wlan1:vap6	0	0	0	0	0
wlan1:vap7	0	0	0	0	0
wlan1:vap8	0	0	0	0	0
wlan1:vap9	0	0	0	0	0
wlan1:vap10	0	0	0	0	0
wlan1:vap11	0	0	0	0	0
wlan1:vap12	0	0	0	0	0
wlan1:vap13	0	0	0	0	0
wlan1:vap14	0	0	0	0	0
wlan1:vap15	0	0	0	0	0

Figure 5-5 Transmit/Receive Statistics – 2

Receive

Interface	Total packets	Total bytes	Total dropped packets	Total dropped bytes	Errors
LAN	131	19155	0	0	0
wlan0:wds0	1160	315806	0	0	0
wlan0:vap1	684	114277	0	0	0
wlan0:vap2	0	0	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:wds0	0	0	0	0	0
wlan1:vap1	0	0	0	0	0
wlan1:vap2	0	0	0	0	0
wlan1:vap3	0	0	0	0	0
wlan1:vap4	0	0	0	0	0
wlan1:vap5	0	0	0	0	0
wlan1:vap6	0	0	0	0	0
wlan1:vap7	0	0	0	0	0
wlan1:vap8	0	0	0	0	0
wlan1:vap9	0	0	0	0	0
wlan1:vap10	0	0	0	0	0
wlan1:vap11	0	0	0	0	0
wlan1:vap12	0	0	0	0	0
wlan1:vap13	0	0	0	0	0
wlan1:vap14	0	0	0	0	0
wlan1:vap15	0	0	0	0	0

Figure 5-6 Transmit/Receive Statistics – 3

The page includes the following fields:

Object	Description
Interface	The name of the Ethernet, VAP or WDS interface.
Status	Shows whether the interface is up or down.
MAC Address	MAC address for the specified interface. The AP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.
Name (SSID)	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP or WDS tab.
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this AP.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this AP.
Total Dropped Packets	Indicates total number of packets sent (in Transmit table) or received (in Received table) by this AP that were dropped.
Total Dropped Bytes	Indicates total number of bytes sent (in Transmit table) or received (in Received table) by this AP that were dropped.
Errors	Indicates total errors related to sending and receiving data on this AP.

5.2.3 Client Associations

This page provides the list of the associated clients on the AP according to each enabled SSID. In the list, the system administrator can view the connection status and received packets from each client thus able to troubleshoot the abnormal connection.

Choose menu "**Status -> Client Associations**" to view the current associated clients of the AP.

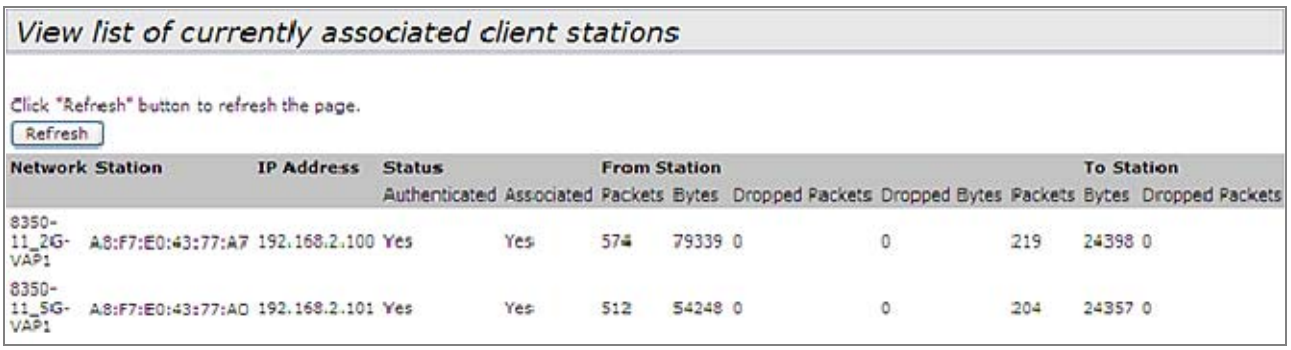


Figure 5-7 Client Associations

The page includes the following fields:

Object		Description
Network		The SSID of the client associated network.
Station		The MAC address of the associated client.
IP Address		The IP address of the associated client.
Status	**Authenticated**	This field indicates the status of client's IEEE 802.11 authentication.
	Associated	This field indicates the status of client's association.
From Station	**Packets**	Indicates total number of packets received from the client.
	Bytes	Indicates total number of bytes received from the client.
	Dropped packets	Indicates total number of dropped packets after receiving from the client.
	Dropped Bytes	Indicates total number of dropped bytes after receiving from the client.
To Station	**Packets**	Indicates total number of packets transmitted to the client.
	Bytes	Indicates total number of bytes transmitted to the client.
	Dropped packets	Indicates total number of dropped packets after transmitting to the client.
	Dropped Bytes	Indicates total number of dropped bytes after transmitting to the client.

5.3 Advanced Configuration

5.3.1 Ethernet Settings

This page allows the administrator to configure the Ethernet related settings including the LAN IP address of IPv4/IPv6, LAN connection type, and management VLAN ID settings of the AP.

Choose menu "**Advanced Configuration -> Ethernet Settings**" to configure the Ethernet setting of the AP.

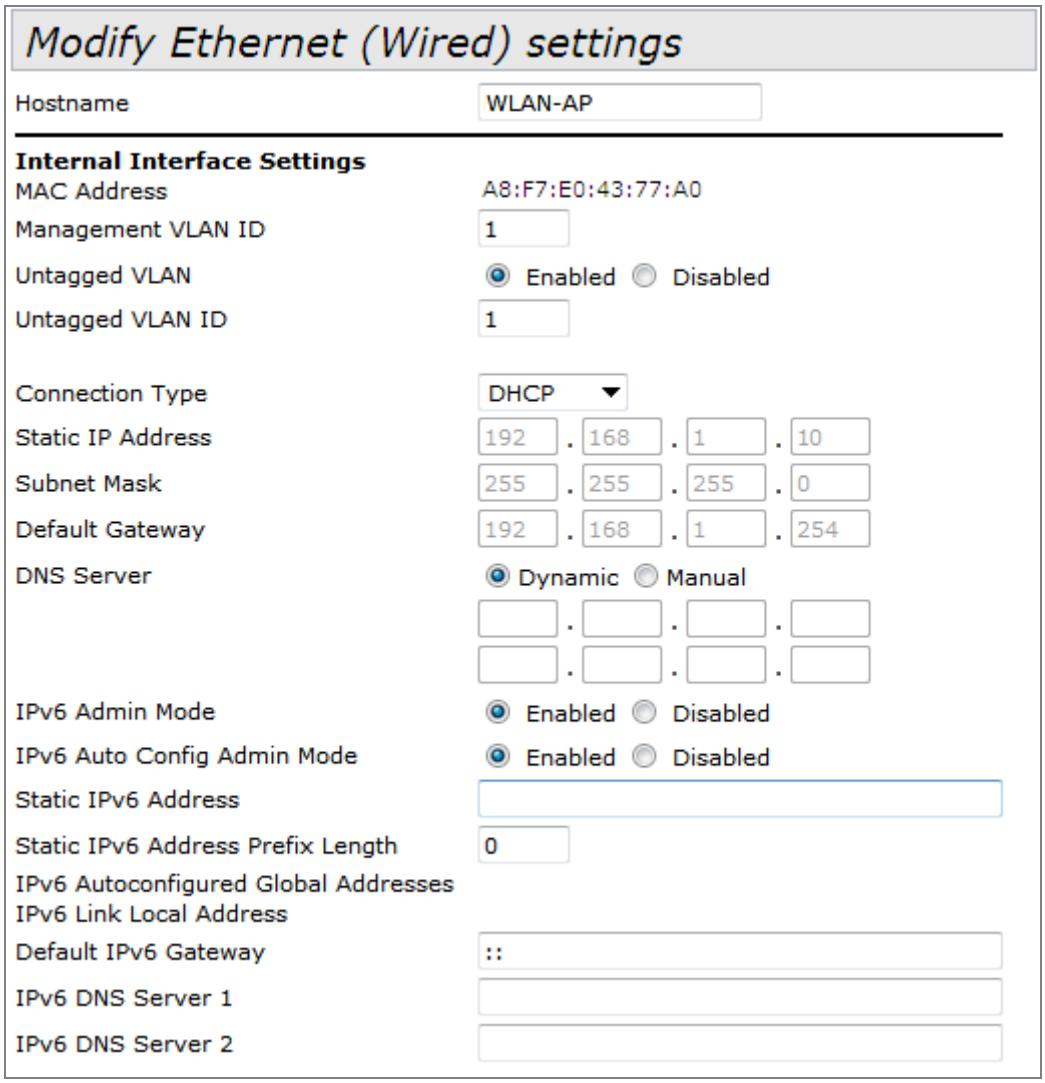


Figure 5-8 Ethernet Settings

The page includes the following fields:

Object	Description
Hostname	The host name of the AP.
MAC Address	MAC address of the LAN interface of the AP.
Management VLAN ID	The management VLAN is used to access the VLAN which is associated with the IP address of AP.
Untagged VLAN	If the untagged VLAN is disabled, all the packets will be marked with the same VLAN number.
Untagged VLAN ID	The packet transmitted in this VLAN has no tagged VLAN number.
Connection Type	Select **DHCP (Dynamic IP)** to get IP address from DHCP server or select **Static IP** to configure IP address manually.
Static IP Address	Configure the static IP address. If the IP obtained is DHCP, this property cannot be used.

Subnet Mask	Configure the subnet mask. If the IP obtained is DHCP, this property cannot be used.
Default Gateway	Configure the default gateway. If the IP obtained is DHCP, this property cannot be used.
DNS Server	Configure the DNS mode. In the manual appointed mode, the DNS address can be configured to analyze the domain name.
IPv6 Admin Mode	IPv6 management on-off. If it is enabled, AP and AC can be managed through the IPv6 address; if the IPv4 and IPv6 are both enabled, IPv4 is preferential.
IPv6 Auto Config Admin Mode	IPv6 automatic address. If it is enabled, AP will get the address automatically.
Static IPv6 Address	Show the static IPv6 address of AP.
Static IPv6 Address Prefix Length	Show the prefix length of static IPv6 address.
IPv6 Autoconfigured Global Addresses	Show the IPv6 address that the AP gets dynamically. If there are multiple addresses, they can be shown in the list.
IPv6 Link Local Address	Show the IPv6 link local address of AP.
Default IPv6 Gateway	Show the default IPv6 gateway of AP.
IPv6 DNS Server 1	Show the IPv6 DNS server 1 of AP.
IPv6 DNS Server 2	Show the IPv6 DNS server 2 of AP.

5.3.2 Wireless Settings

This page allows the administrator to enable or disable radio interface and configure the basic settings including the radio mode, channel for each radio interface.

Choose menu “**Advanced Configuration -> Wireless Settings**” to configure the wireless setting of the AP.

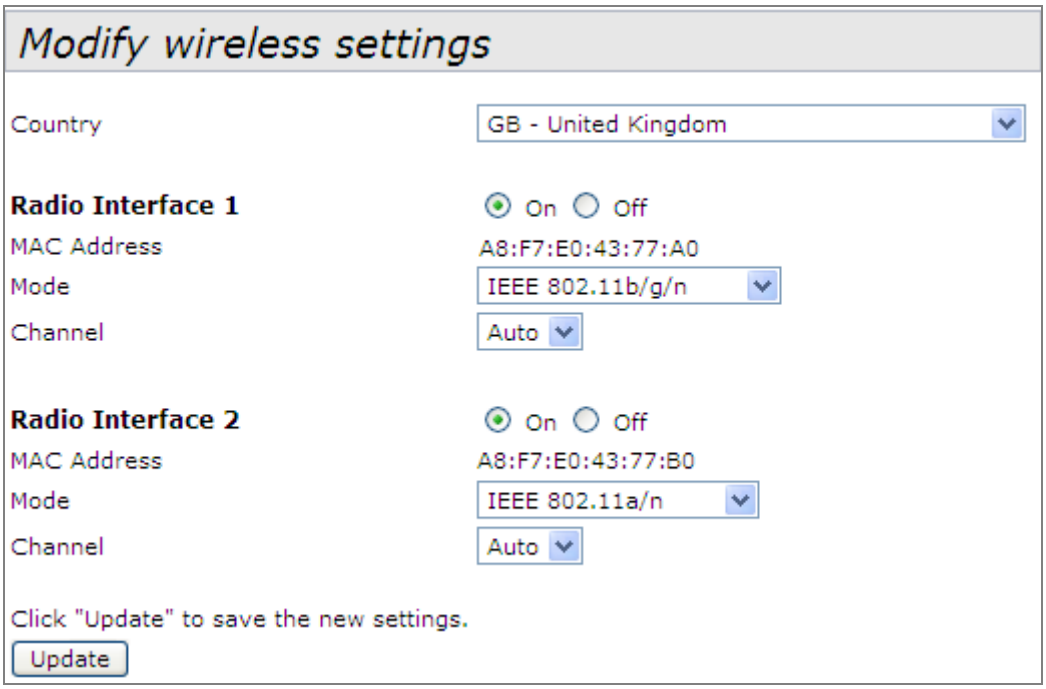


Figure 5-9 Wireless Settings

The page includes the following fields:

Object	Description
Country	Select your country from the list. The supported channels will vary based on the regulation in different countries/regions. If your country is not in the drop-down list, you can select any other country which supports channels conforming to your country.
Radio Interface 1	Select **On** or **Off** to enable or disable the Radio Interface 1 which utilizes 2.4GHz frequency band.
MAC Address	MAC address for the Radio Interface 1. This MAC address must be configured on the WDS setting page when establishing the WDS connection which utilizes 2.4GHz frequency band. The AP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.
Mode	Choose the IEEE wireless network mode for the Radio Interface 1 according to your wireless clients. Default: IEEE 802.11b/g/n
Channel	You can select the operating channel of the Radio Interface 1 for the wireless network. Default: Auto
Radio Interface 2	Select **On** or **Off** to enable or disable the Radio Interface 2 which utilizes 5GHz frequency band.
MAC Address	MAC address for the Radio Interface 2. This MAC address must be configured on the WDS setting page when establishing the WDS connection which utilizes 5GHz frequency band.

	The AP has a unique MAC address for each interface. Each radio has a different MAC address for each interface on each of its two radios.
Mode	Choose the IEEE wireless network mode for the Radio Interface 2 according to your wireless clients. Default: IEEE 802.11a/n
Channel	You can select the operating channel of the Radio Interface 2 for the wireless network. Default: Auto

1. When configured to "Auto", you may not able to discover the AP through the wireless clients without supporting the same channel list. For example, if your country does not conform to FCC regulation, and if you set the country to "United States" and channel to "Auto", the AP will automatically switch to the less occupied channel from the channel list of the country allowed. In other words, if there is any channel that your wireless client does not support, you may not discover the AP until the AP automatically switches to the channel that the client supports.

2. When establishing WDS point to point connection, the channel must be configured to the same fixed channel.

5.3.3 Radio

The page includes the general wireless advanced settings of each radio interface.
Choose menu “**Advanced Configuration -> Radio**” to configure the wireless radio setting of the AP.

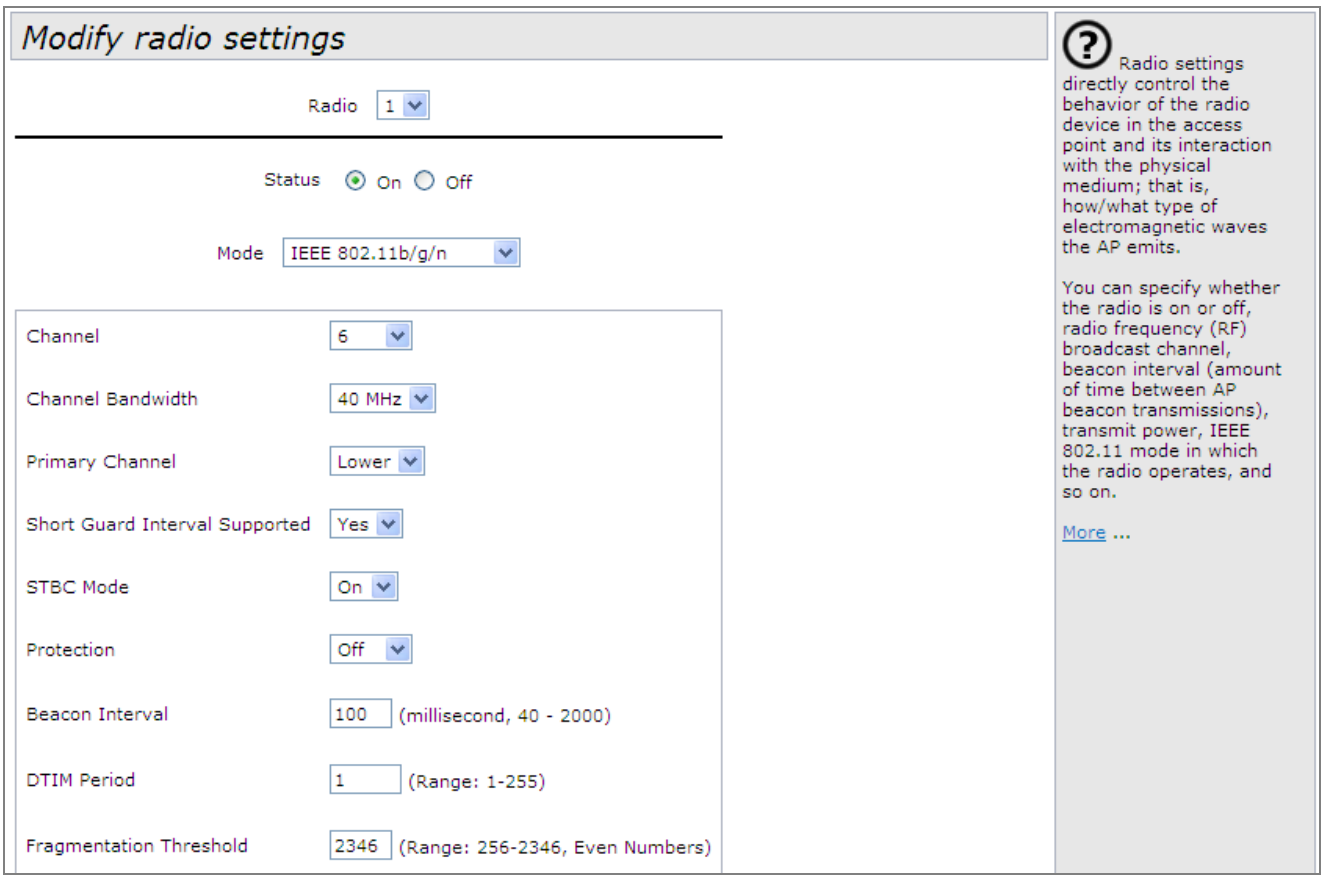


Figure 5-10 Radio Settings – 1/2

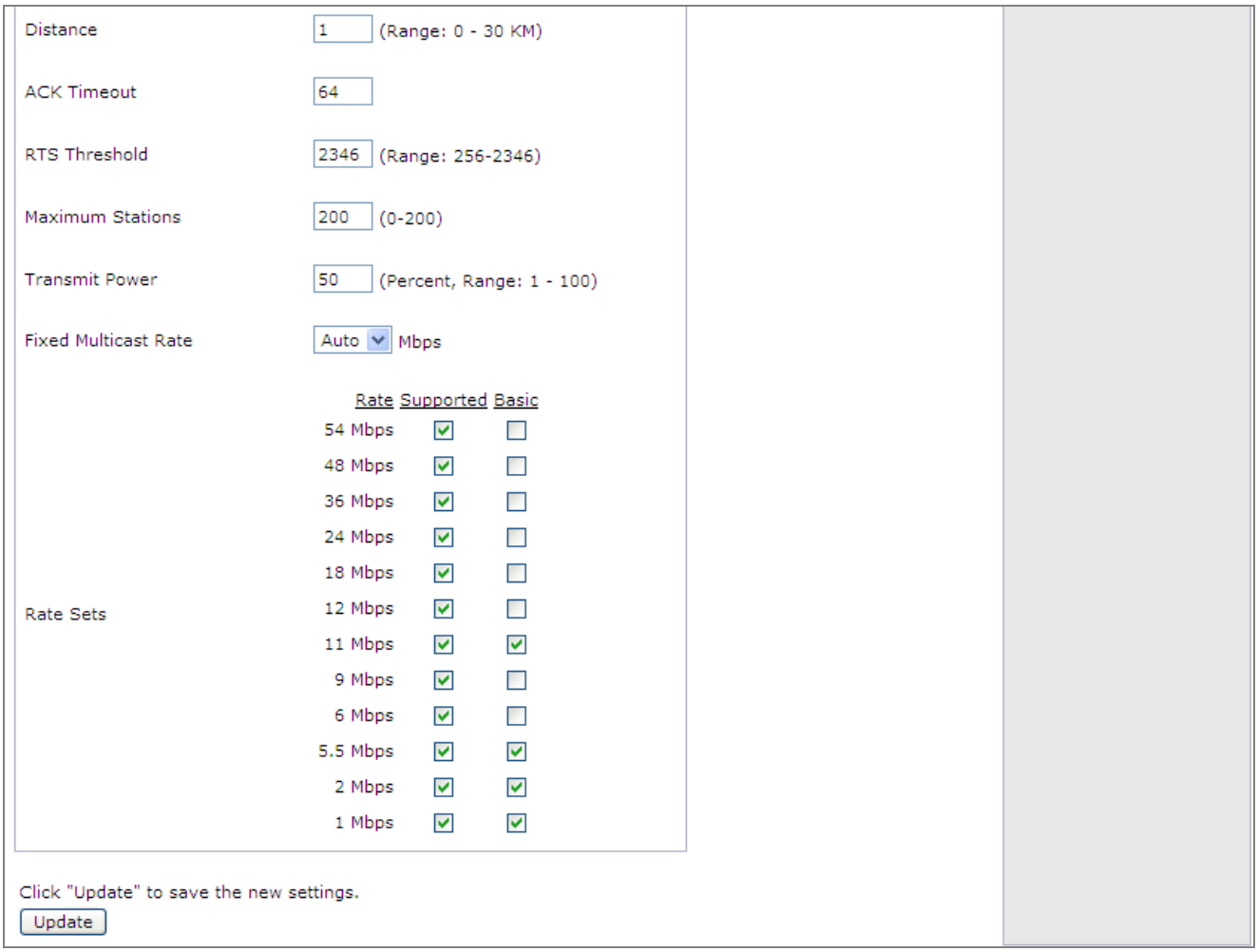


Figure 5-11 Radio Settings – 2/2

The page includes the following fields:

Object	Description
Radio	As for the wireless interface, choose radio 1 to configure the wireless advanced parameters of 2.4GHz or choose radio 2 to configure the wireless advanced parameters of 5GHz.
Status	When On, enable the radio interface you choose. When Off, disable the radio interface you choose.
Mode	The wireless standard used by the selected radio interface.
Channel	You can select the operating channel of the Radio Interface 1 for the wireless network.
Channel Bandwidth	The channel bandwidth in 802.11n mode.
Primary Channel	The mode of the primary channel (only the 802.11n mode is supported)
Short Guard Interval Supported	It is used to set the time that the receiver waits for RF reflections to settle out before sampling data. Default is enabled. Only the 802.11n mode is supported.
STBC Mode	Space-time block codes are used for MIMO systems to enable the transmission of multiple copies of a data stream across a number of antennas and to exploit

	the various received versions of the data to improve the reliability of data-transfer.
Protection	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to the transmission of heavy frame traffic. Default is disabled.
Beacon Interval	The interval of time that this access point broadcasts a beacon. Beacon is used to synchronize the wireless network. Default is “100”.
DTIM Interval	DTIM stands for delivery traffic indication map or message. It is basically an additional message added after the normal beacon broadcast by your router or access point. A DTIM interval can be set anywhere from 1 to 255. If you want to optimize the power saving features on your mobile devices, you should select a high DTIM setting. Alternatively, if you set your DTIM interval too high, you may lose connectivity in some environments. Default is “1” (Range: 1~255)
Fragment Threshold	You can specify the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance. Default is “2346”.
RTS Threshold	When the packet size is smaller than the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet. Default is “2346”.
Maximum Stations	Configure the maximum number of associated stations. Each radio interface is suggested not to configure over 50 stations to ensure the wireless bandwidth and stability.
Transmit Power	Configure the percentage of the output transmission power of the selected radio interface (Range: 1~100). In the short distance of point to point connection within 1km, suggest reducing the transmit power at least by half to prevent near-field interference from each other.
Fixed Multicast Rate	The multicast rate is the baseline level that a Wi-Fi device must be able to deliver in order to connect to the router. Lower multicast rates mean weaker, farther signals are allowed to connect. Higher multicast rates mean that only close, strong signals are allowed. Turning up your multicast rate will decrease the effective range of your Wi-Fi network.
Rate Sets	Configure the transmission rate set and the basic broadcast rate set that are supported by RF.

5.3.4 VAP

This page displays the VAP settings including SSID, Security and VLAN ID of each radio interface. You can edit the SSID, Security and VLAN ID or enable multiple SSIDs on this page.

Choose menu "**Advanced Configuration -> VAP**" to configure the wireless SSID/VAP setting of the AP.

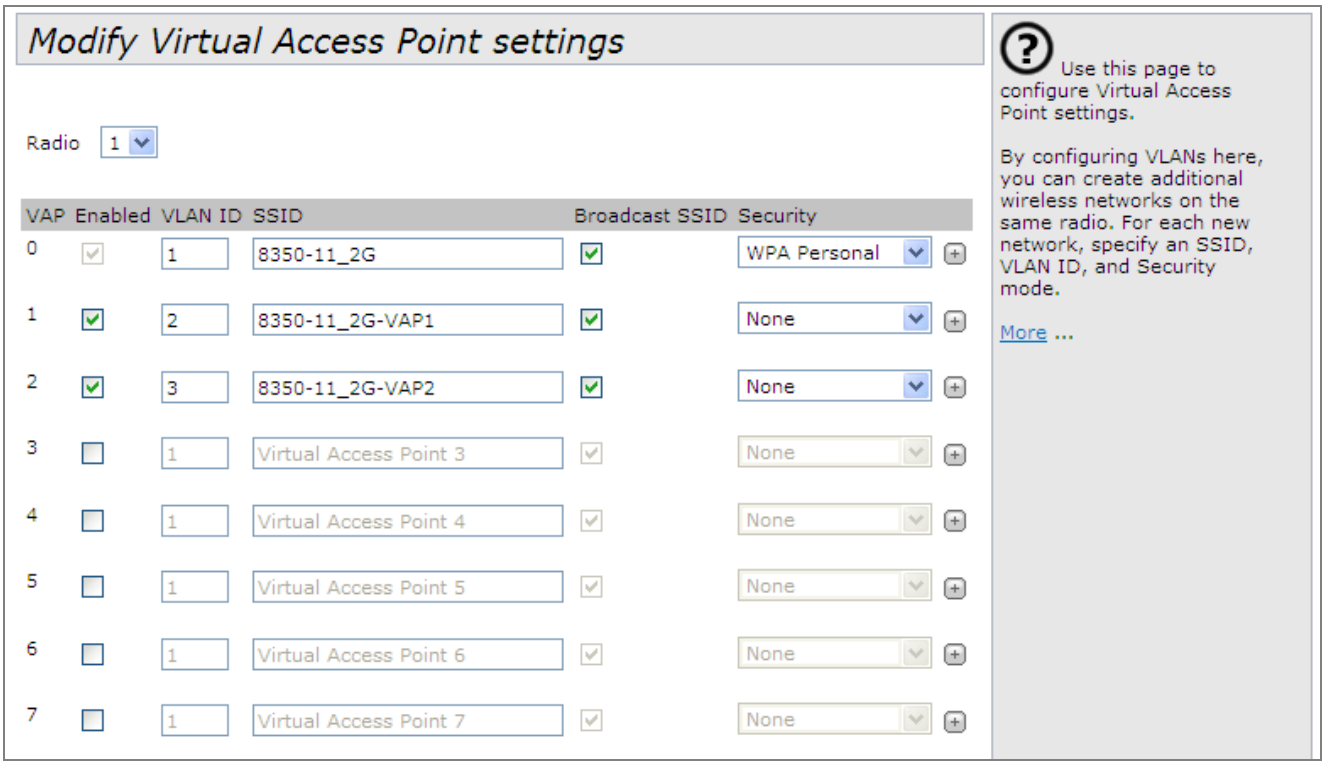


Figure 5-12 VAP Settings

The page includes the following fields:

Object	Description
Radio	Choose the configured radio interface. Each radio interface supports maximum 16 Virtual APs (VAP 0~15).
VAP	Show the ID number of the virtual AP.
Enabled	Check it to enable the selected VAP of this radio interface.
VLAN ID	Configure the VLAN that the client associated with the virtual AP belongs to.
SSID	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network.
Broadcast SSID	Configure if the SSID is broadcast
Security	**None Security** No security setup for wireless connection.
	Static WEP Security Select **Key Length** and **Key Type** for the format of the WEP Keys. Hex (64/128 bits): enter 10/26 **Hexadecimal** digits (any combination of 0-9, a-f, A-F, zero key is not promoted) in the **WEP Keys** field.

	ASCII (64/128 bits): enter 5/13 **ASCII** characters in the **WEP Keys** field.
	WPA Personal Please enter at least 8 ASCII characters (Passphrase) or 64 Hexadecimal characters. All of the Cipher Suites support **TKIP** and **AES**. WPA with TKIP is a medium level encryption and is supported by most wireless devices and operating systems. WPA2 with CCMP (AES) is a high-level encryption and is supported by most wireless devices and operating systems.
	WPA Enterprise Select the WPA Enterprise to enable 802.1x RADIUS authentication by external RADIUS server. Enter the **IP Address**, **Port**, and **Password** of the Radius Server for clients' authentication.

5.3.4.1. None Security

When choosing the security configuration as none, the security configuration will not be needed in clients association. It can be associated with the virtual AP directly.

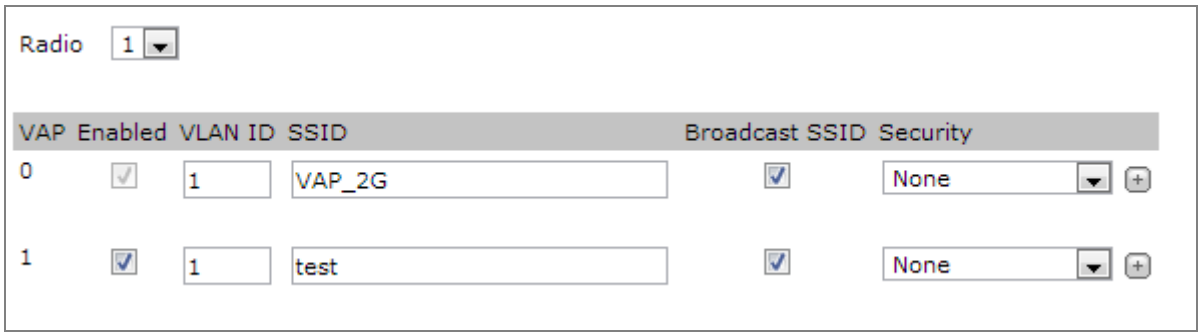


Figure 5-13 Security Setting – None

5.3.4.2. Static WEP Security

Choose the security configuration as static WEP to show the detailed configuration information of static WEP security configuration. The direct key should be input in client to pass the authentication or the decryption packet.

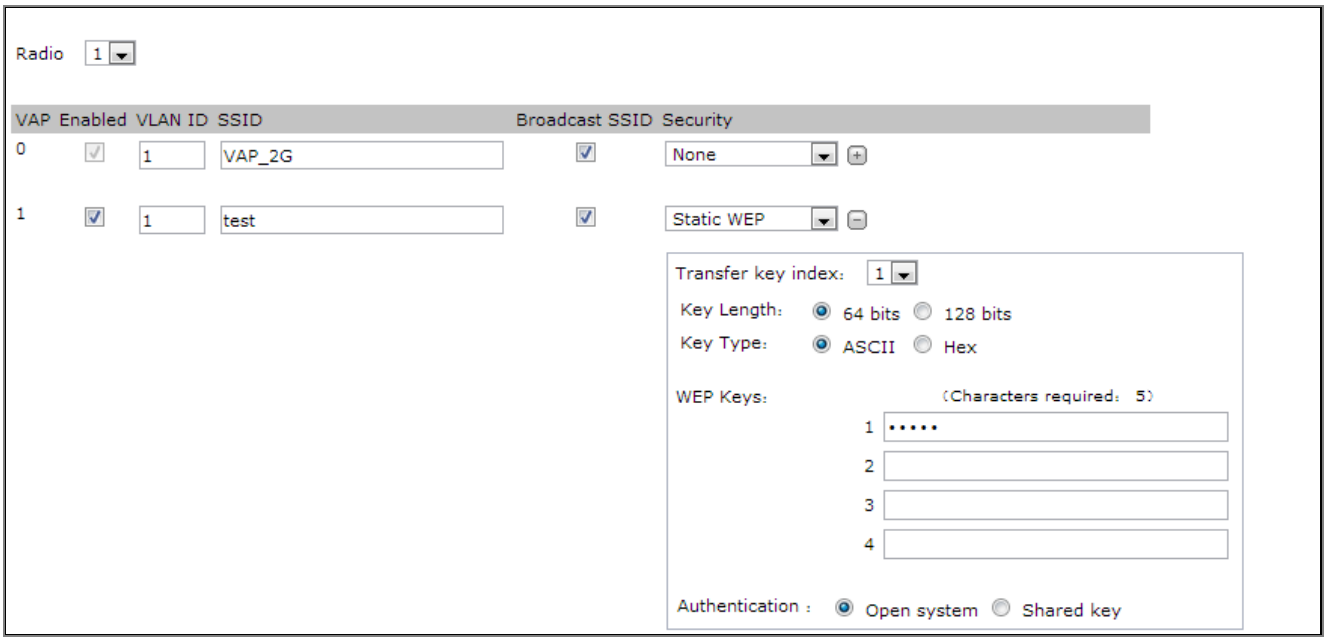


Figure 5-14 Security Setting – WEP

The page includes the following fields:

Object	Description
Transfer Key Index	Configure the key index.
Key Length	Configure the length of key.
Key Type	Configure the type of key.
WEP Keys	Configure the key of 1-4. Hex (64/128 bits): enter 10/26 **Hexadecimal** digits (any combination of 0-9, a-f, A-F, zero key is not promoted) in the **WEP Keys** field. ASCII (64/128 bits): enter 5/13 **ASCII** characters in the **WEP Keys** field.
Authentication	Configure the authentication mode.

5.3.4.3. WPA Personal Security

Choose the security configuration as WPA Personal to show the detailed configuration information of WPA Personal security configuration. The direct key should be input in client to pass the authentication.

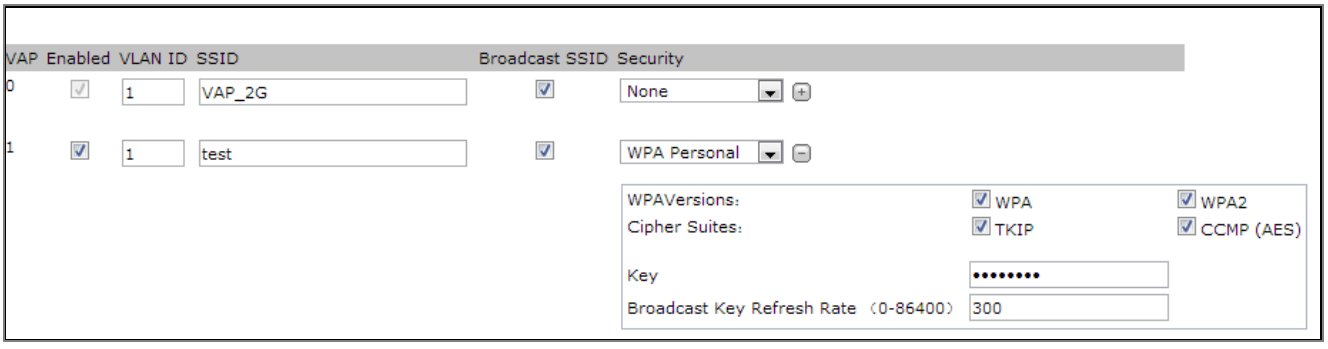


Figure 5-15 Security Setting – WPA Personal

The page includes the following fields:

Object	Description
WPA Versions	Configure the WPA version.
Cipher Suites	Configure the cipher suites.
Key	Configure the key.
Broadcast Key Refresh Rate (0-86400)	Configure the interval of broadcast key update (Range: 0~86400 second). The default value is 300.

5.3.4.4. WPA Enterprise Security

Choose the security configuration as WPA Enterprise to show the detailed configuration information of WPA Enterprise security configuration. The direct user name and password existed in radius server should be input in client to pass the authentication.

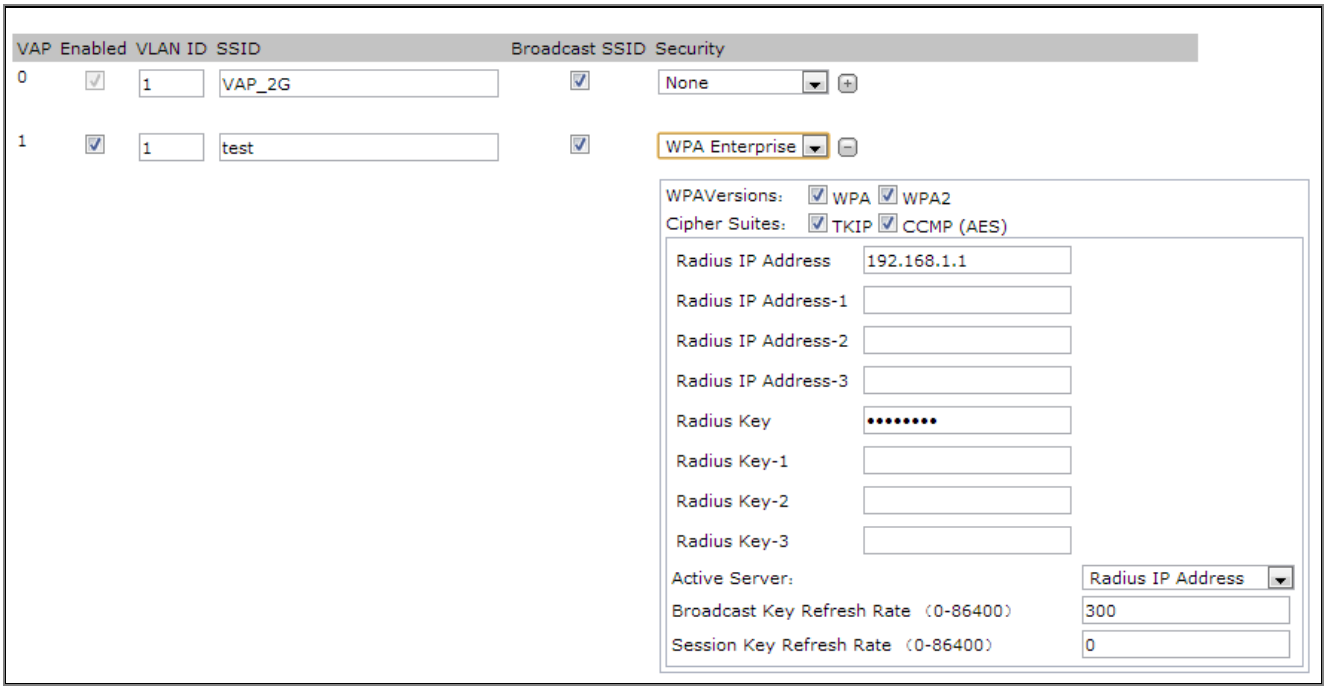


Figure 5-16 Security Setting – WPA Enterprise

The page includes the following fields:

Object	Description
WPA Versions	Configure the WPA version.
Cipher Suites	Configure the cipher suites.
RADIUS IP Address	Configure the IP address of RADIUS server.
RADIUS IP Address of 1-3	Configure the IP address of the backup RADIUS server.
RADIUS Key	Configure the RADIUS server key.
RADIUS Key of 1-3	Configure the key of the backup radius server.
Active Server	Choose the RADIUS server.
Broadcast Key Refresh Rate (0-86400)	Configure the interval of broadcast key update (Range: 0~86400 second). The default value is 300.
Session Key Refresh Rate (0-86400)	Configure the interval of unicast key update (Range: 0~86400 second). The default value is 0.

5.3.5 WDS

This page displays the WDS bridge settings of each radio interface. To establish the WDS connection, besides the channel and security which must be the same, both sites should enter the MAC address with each other. The WDS AP mode should be configured in the master AP; others should be configured to the WDS Client.
Choose menu "**Advanced Configuration -> WDS**" to configure the WDS setting of the AP.

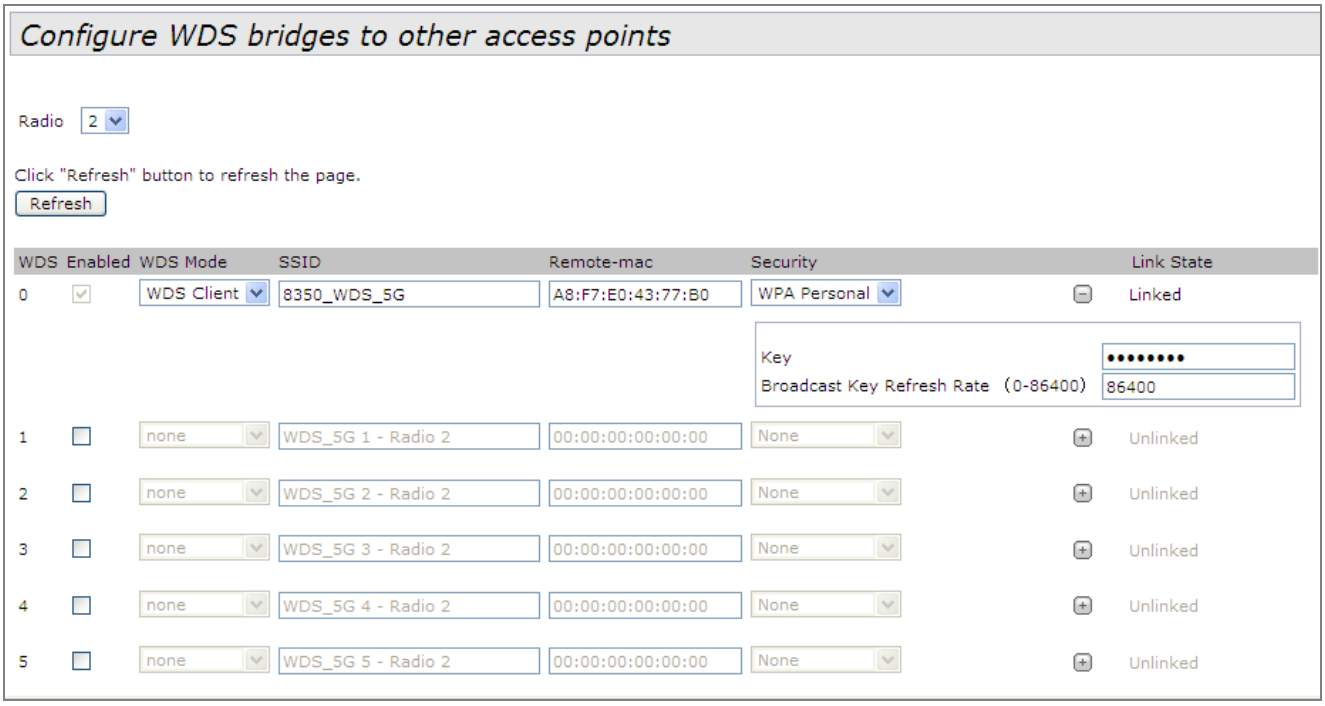


Figure 5-17 WDS Settings

The page includes the following fields:

Object	Description
Radio	Choose the configured radio interface. Each radio interface supports maximum 16 Virtual APs (VAP 0~15).
WDS	Show the ID number of the WDS connection.
Enabled	Check it to enable the selected VAP of this radio interface.
WDS Mode	WDS AP: This mode acts as the master AP in the WDS connection. WDS Client: This mode acts as the slave AP in the WDS connection.
SSID	Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network.
Remote-mac	Configure the remote MAC address to establish the connection. The MAC address must be wireless MAC address and use the same radio interface.
Security	Configure the security mode. Configure the security mode. Different radio interface can be configured to different security, but each WDS entry by using the same radio interface must be configured to the same security.
Link State	The field displays the WDS connection status. Once the connection is established, the status will indicate “Linked”.

5.3.6 Location

This page displays the wireless location settings of the AP. The AP scans and collects the wireless clients' location information which will be reported to the location server.

Choose menu "**Advanced Configuration -> Location**" to configure the wireless location setting for the clients.

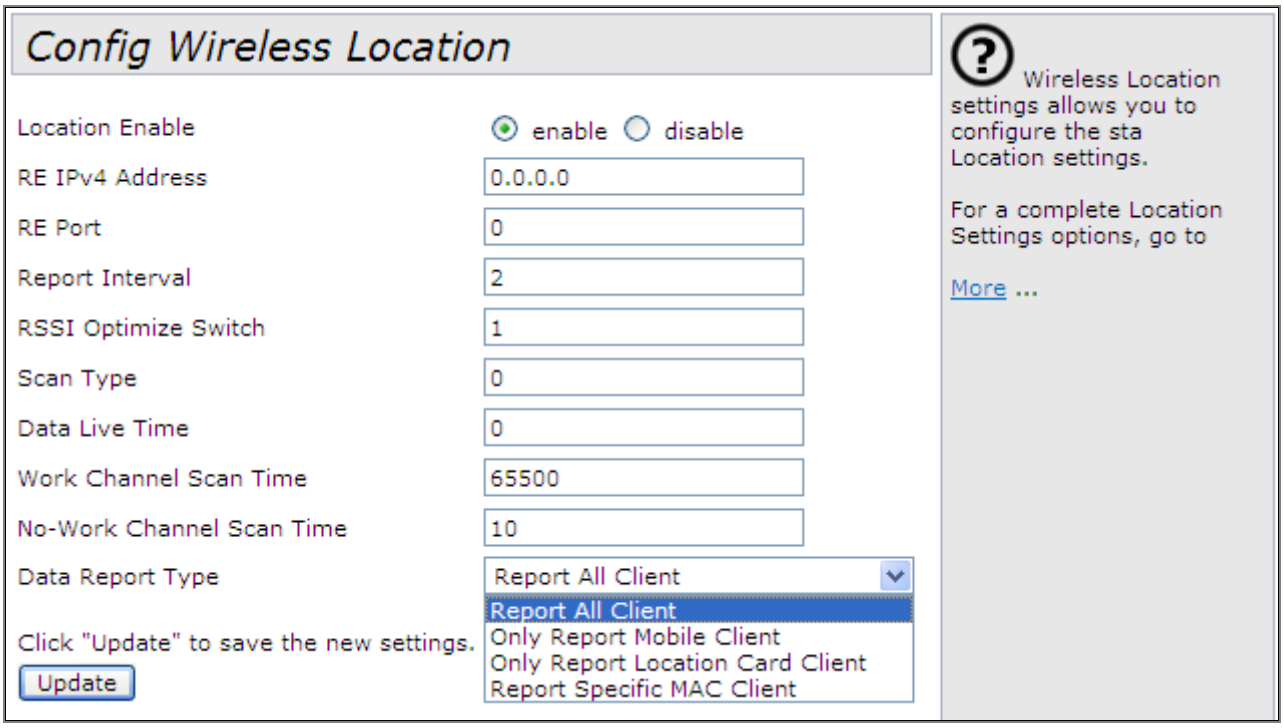


Figure 5-18 Location Settings

The page includes the following fields:

Object	Description
Location Enable	Select "enable" or "disable" to open or close the wireless location.
RE IPv4 Address	Location Server IPv4 Address (Format: 192.168.1.100).
RE Port	Location Server Port (Range: 1-65535).
Report Interval	The interval of AP report clients' information to Location Server. Unit: second.
RSSI Optimize Switch	AP Optimization feature: 0: Close Optimization 1: Open Optimization
Scan Type	The method of AP scan (Only for 2.4G): 0: scan all channels. 1: only scan 1, 6, 11 non-overlapping channels.
Data Live Time	Test field, set to 1
Work Channel Scan Time	Work channel scan time. Unit: millisecond. Attention: add "Work channel scan time" & "No-work channel scan time" to

	multiples of 1000.
No-Work Channel Scan Time	No-work channel scan time. Unit: millisecond. Attention: add “Work channel scan time” & “No-work channel scan time” to multiples of 1000.
Data Report Type	Select which clients’ data that the AP should report to location server.

5.4 Services

This section includes Web Server and NTP settings of the AP.

5.4.1 Web Server

This page allows you to configure the HTTP server settings of the AP. The AP can be managed through HTTP sessions. By default HTTP access is enabled. Choose menu “**Services -> Web Server**” to configure the web server setting of the AP.

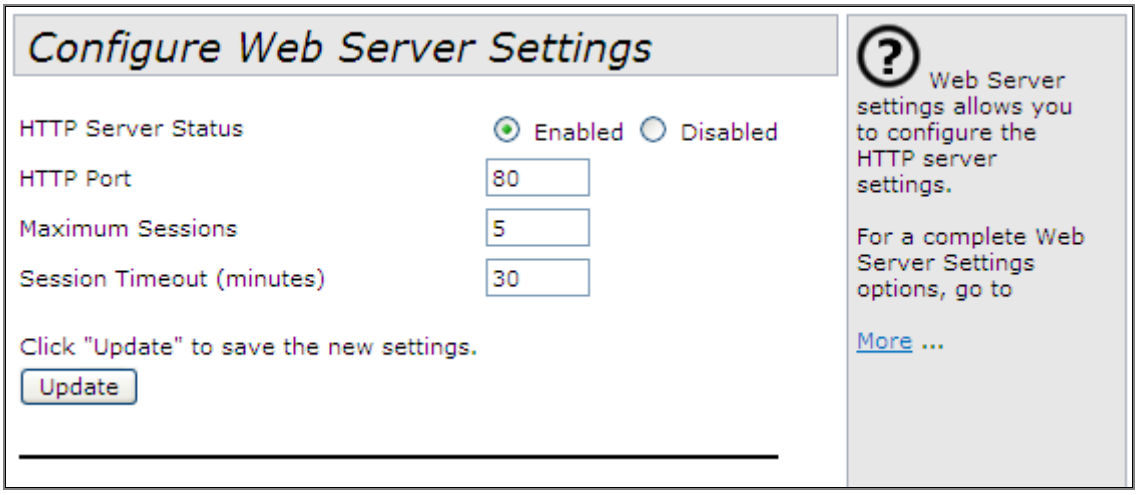


Figure 5-19 Web Server Settings

The page includes the following fields:

Object	Description
HTTP Server Status	Select “Enabled” or “Disabled” to allow access the AP through HTTP.
HTTP Port	Specify the port number for HTTP traffic (the range is 0-65535 and default is 80).
Maximum Sessions	Set the maximum session that allows accessing the http server of the AP. When a user logs on to the AP web interface, a session is created. This session is maintained until the user logs off or the session inactivity timer expires. Enter the number of web sessions. The range is 1-10 sessions. If the maximum number of sessions is reached, the next user who attempts to log on to the AP web interface receives an error message about the session limit.
Session Timeout (minutes)	Set the session timeout in minutes of the http server. Enter the maximum amount of time, in minutes; an inactive user remains logged

	on to the AP web interface. When the configured timeout is reached, the user is automatically logged off the AP. The range is 1-1440 minutes (1440 minutes = 1 day).
Update	Click the “Update” button to apply the changes and to save the settings.

If you disable the protocol you are currently using to access the AP management interface, the current connection will end and you will not be able to access the AP by using that protocol until it is enabled.

5.4.2 NTP

NTP (Network Time Protocol) is used to synchronize time keeping among a set of distributed time servers and clients. To synchronize the system time with the specified NTP server, the internet connection must be reachable. Choose menu "**Services -> NTP**" to configure the NTP setting of the AP.

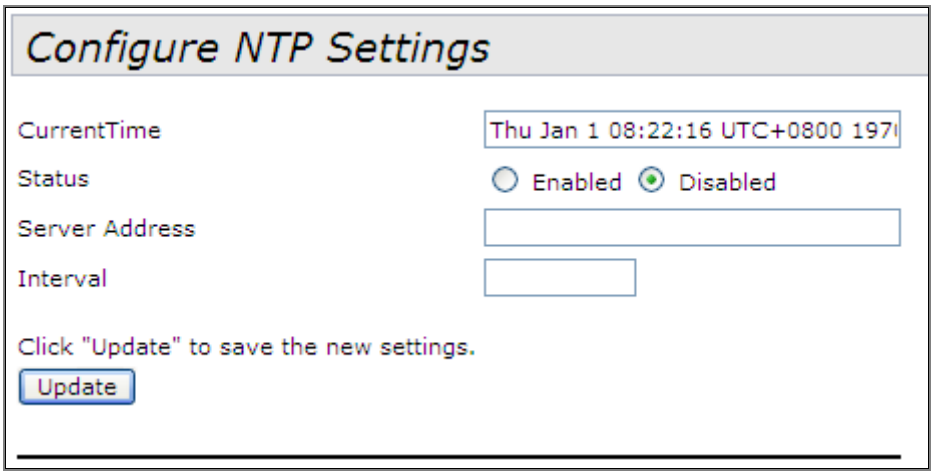


Figure 5-20 NTP Settings

The page includes the following fields:

Object	Description
Current Time	Displays the current time of the AP.
Status	Enable or disable the NTP function.
Server Address	Specify the IPv4 or IPv6 address for NTP Server.
Interval	Specify the interval for NTP client to adjust time. The range is 1~2147483647 (unit: second).
Errors	Indicates total errors related to sending and receiving data on this AP.

5.5 Maintenance

5.5.1 Configuration

This page allows you to backup/restore the settings of the AP through the http or tftp method.

Choose menu "**Maintenance -> Configuration**" to back up or restore the settings of the AP.

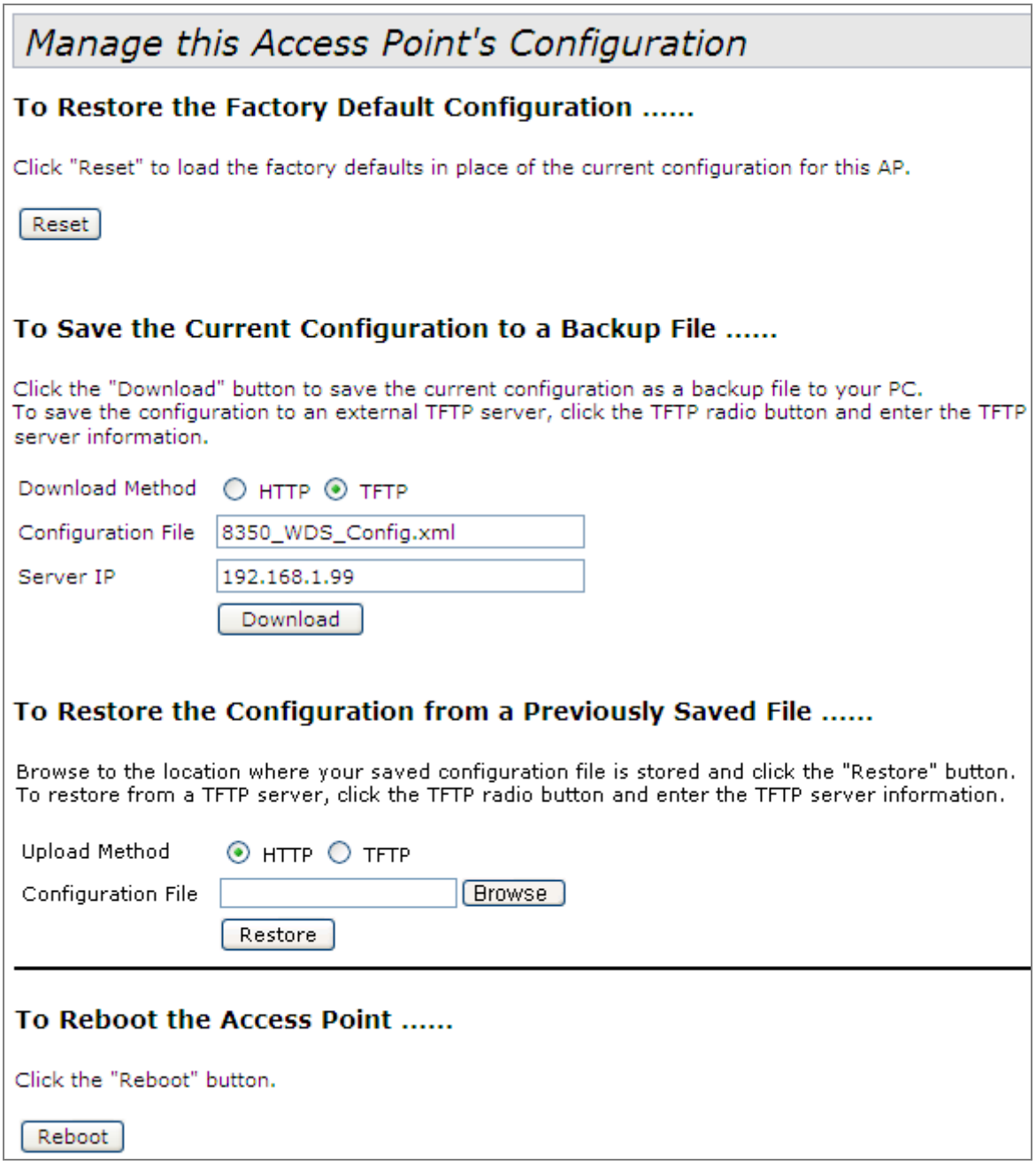


Figure 5-21 Configuration Backup/Restore

The page includes the following fields:

Object	Description
To Restore the Factory Default Configuration…	
Reset	Click “Reset” to load the factory defaults in place of the current configuration for this AP.
To Save the Current Configuration to a Backup File…	
Download Method	Select download method by using HTTP or TFTP. Choose the download method as HTTP mode, click the “download” button and confirm it, then the current configuration files of AP will be downloaded through HTTP directly. Choose the download method as TFTP mode, input the file name of the configuration file (the format is *.xml) and the IP address of TFTP server. Then click the “download” button and confirm it. The configuration file will be downloaded to the appointed TFTP server and the file name is the input name.
Configuration File	Specify the configuration filename (the format is *.xml)
Server IP	Specify the TFTP server IP address.
Download	Click the “download” button to download the configuration file.
To Restore the Configuration from a Previously Saved File…	
Upload Method	Select upload method by using HTTP or TFTP.
Configuration File	Click “Browse” to select the previously saved configuration file.
Restore	Click “Restore” to restore the selected configuration file to the AP.
To Reboot the Access Point…	
Reboot	Click the “Reboot” button to reboot the AP.

5.5.2 Upgrade

This page displays the current settings of the AP. It displays the Wired Settings and the Wireless Settings.

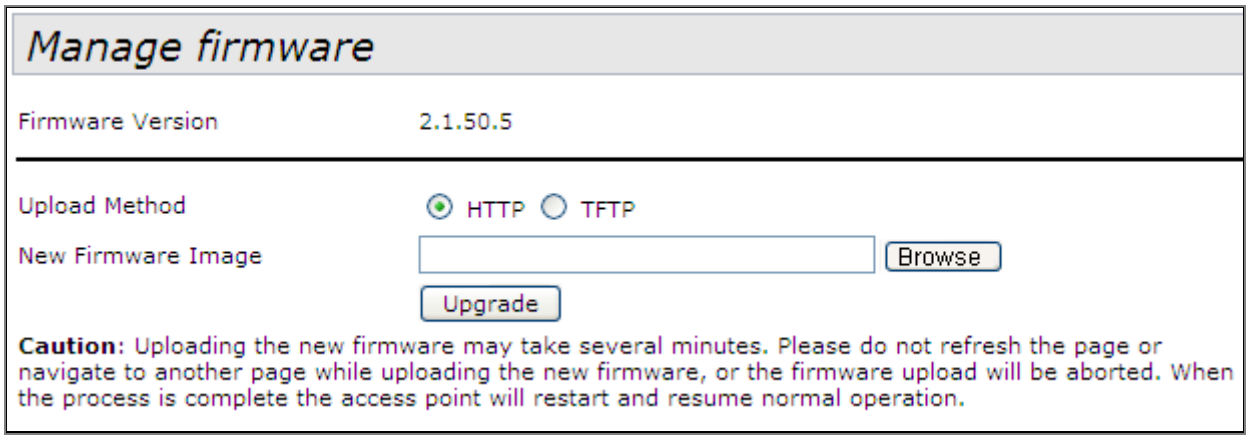


Figure 5-22 Firmware Upgrade

The page includes the following fields:

Object	Description
Firmware Version	This field indicates the current firmware version.
Upload Method	Select upload method by using HTTP or TFTP. If you choose the upload method as HTTP mode, after specifying the new firmware image, you can click the “Upgrade” button to upgrade the firmware to the AP directly. If you choose the download method as TFTP mode, please ensure you have TFTP utility and have already put the image in the TFTP folder for upgrade.
New Firmware Image	Click “Browse” to select the previously saved configuration file.
Upgrade	Click the “Upgrade” button to upgrade the firmware to the AP.

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WDAP-8350 is configured to "**default**".

6.1 Windows XP (Wireless Zero Configuration)

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

Figure 6-1 System Tray – Wireless Network Icon

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

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

(1) Select SSID [default]

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

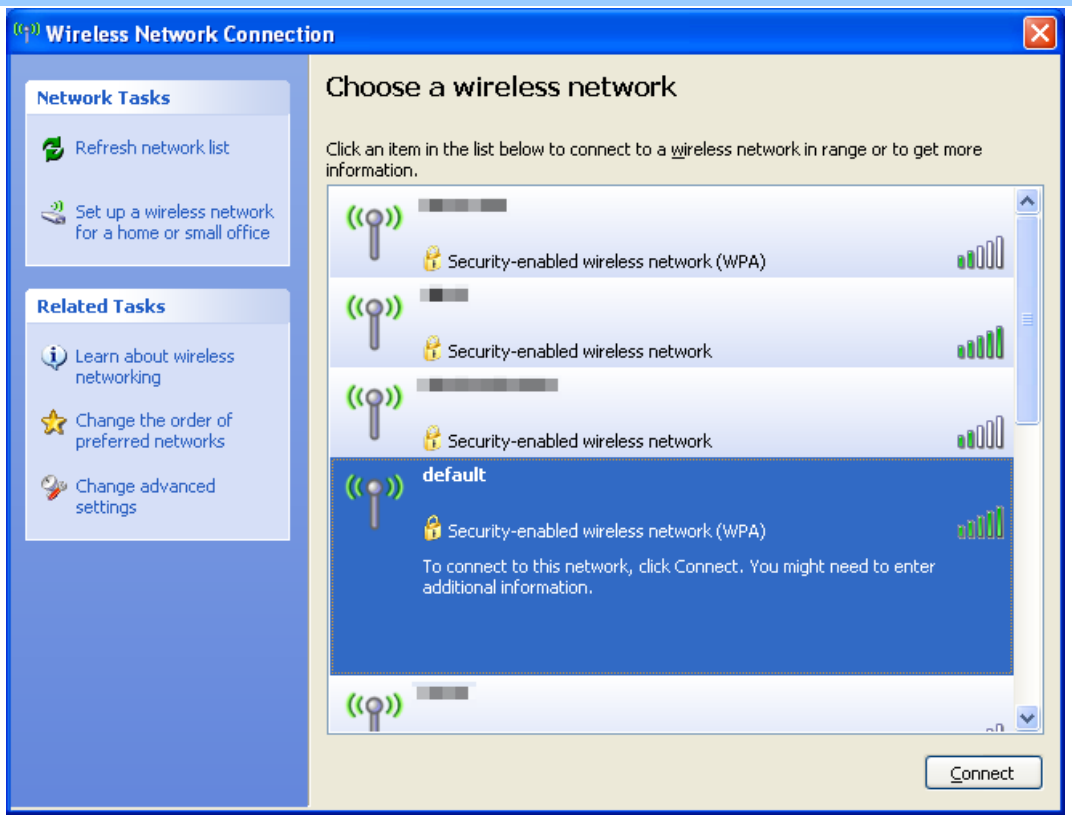


Figure 6-2 Choose a Wireless Network

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

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key

(3) Click the [Connect] button

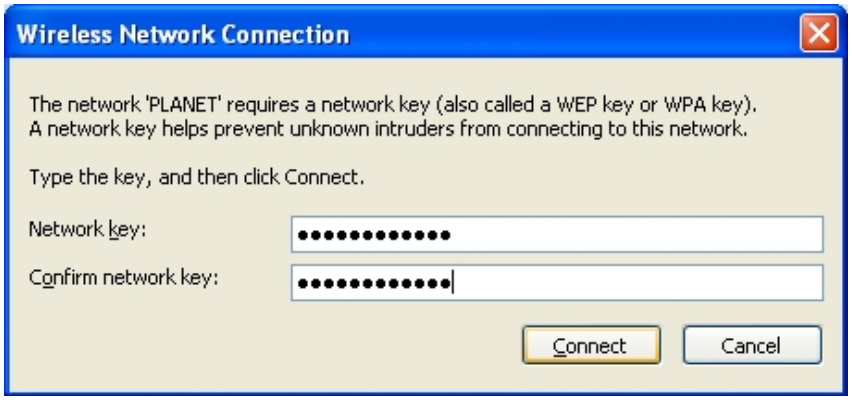


Figure 6-3 Enter the Network Key

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

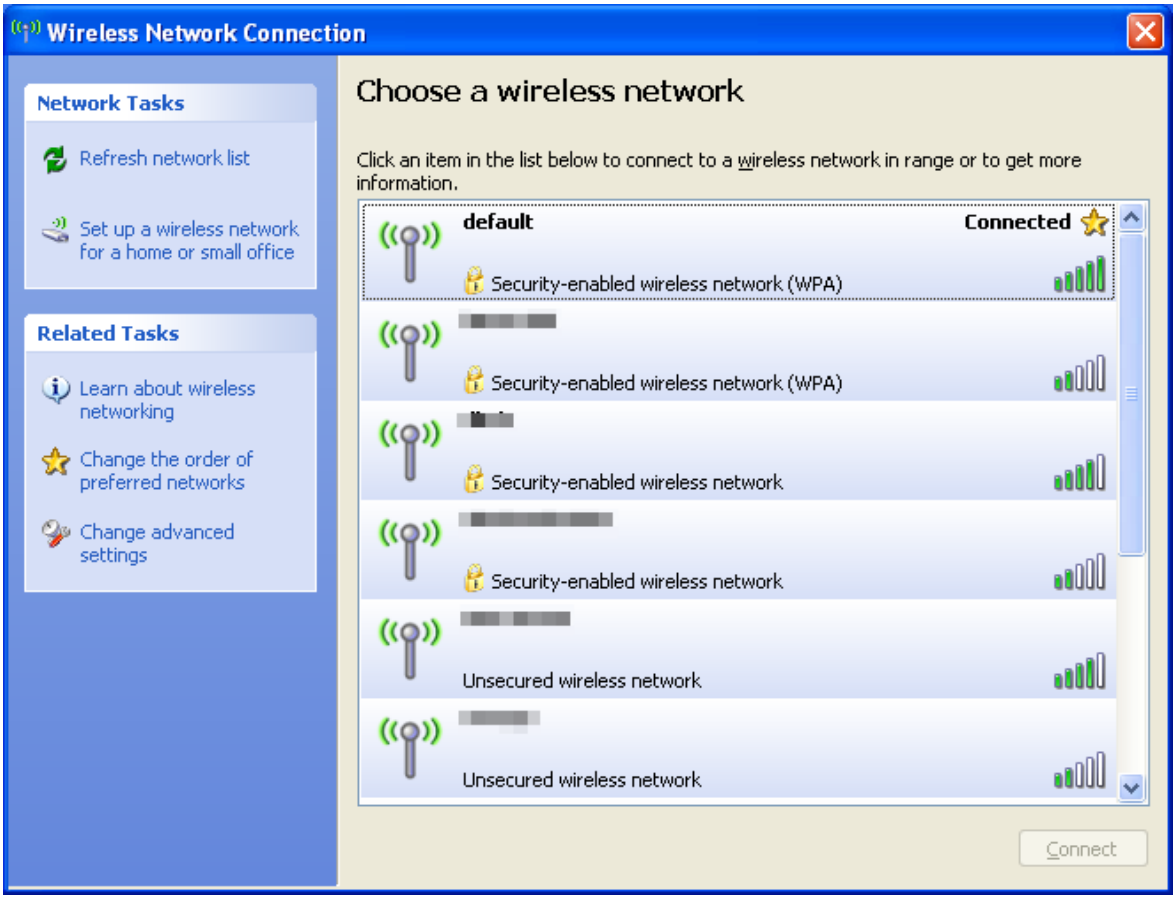


Figure 6-4 Choose a Wireless Network -- Connected

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

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

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

Figure 6-5 Network Icon

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

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

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

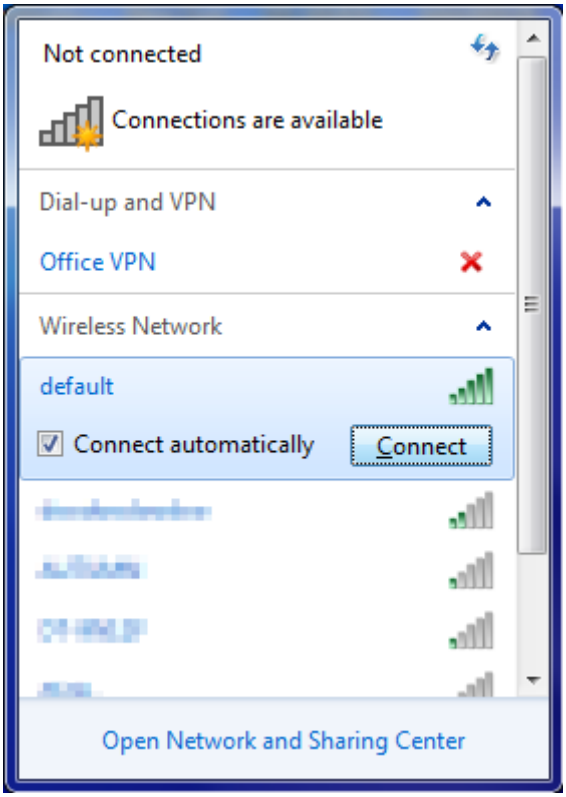


Figure 6-6 WLAN AutoConfig

Note

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

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

(1) The Connect to a Network box will appear
(2) Enter the encryption key
(3) Click the [OK] button

Figure 6-7 Type the Network Key

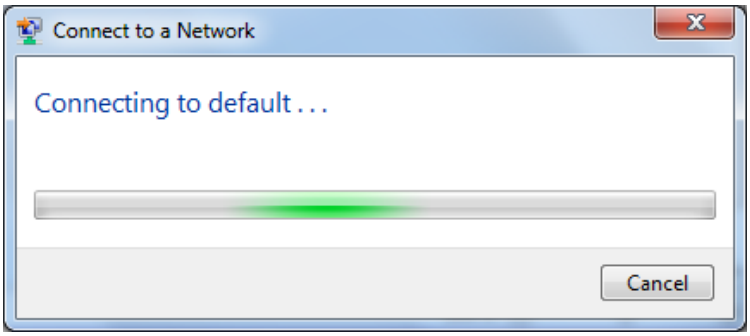


Figure 6-8 Connect to a Network

Step 4: Check if "**Connected**" is displayed

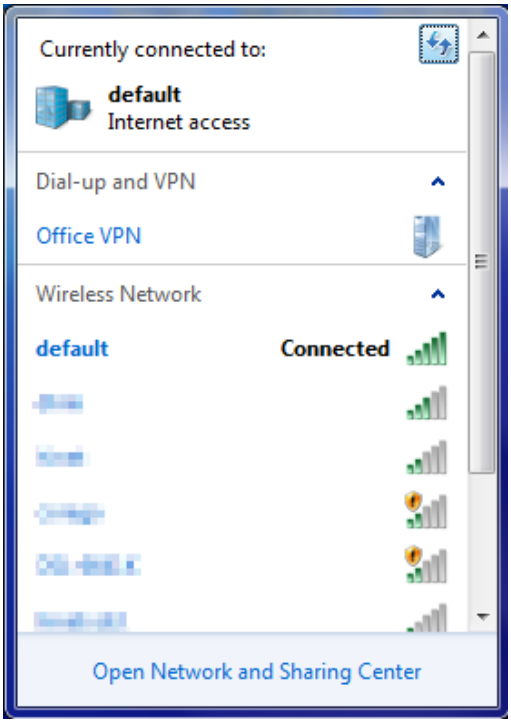


Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the WDAP-8350 is configured to “default”.

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

The AirPort Network Connection menu will appear

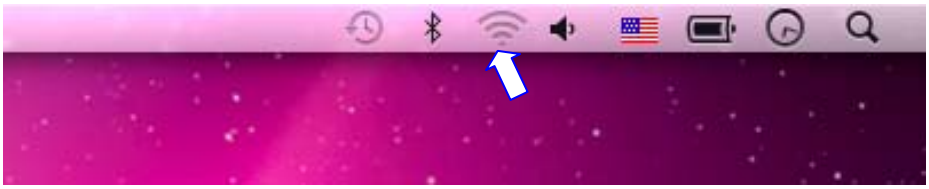


Figure 6-10 Mac OS – Network Icon

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

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

(2) Double-click on the selected SSID

Figure 6-11 Highlight and Select the Wireless Network

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

(1) Enter the encryption key

(2) Click the [OK] button

Figure 6-12 Enter the Password

Note

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

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

If "Yes", then there will be a "check" symbol before SSID.

Figure 6-13 Connected to the Network

There is another way to configure the MAC OS X Wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

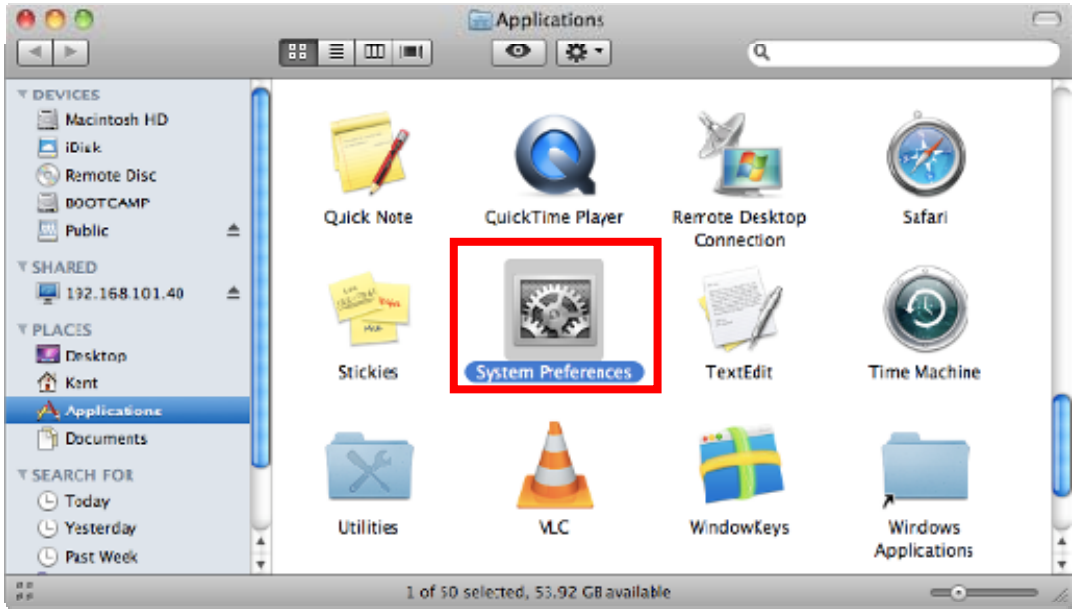


Figure 6-14 System Preferences

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

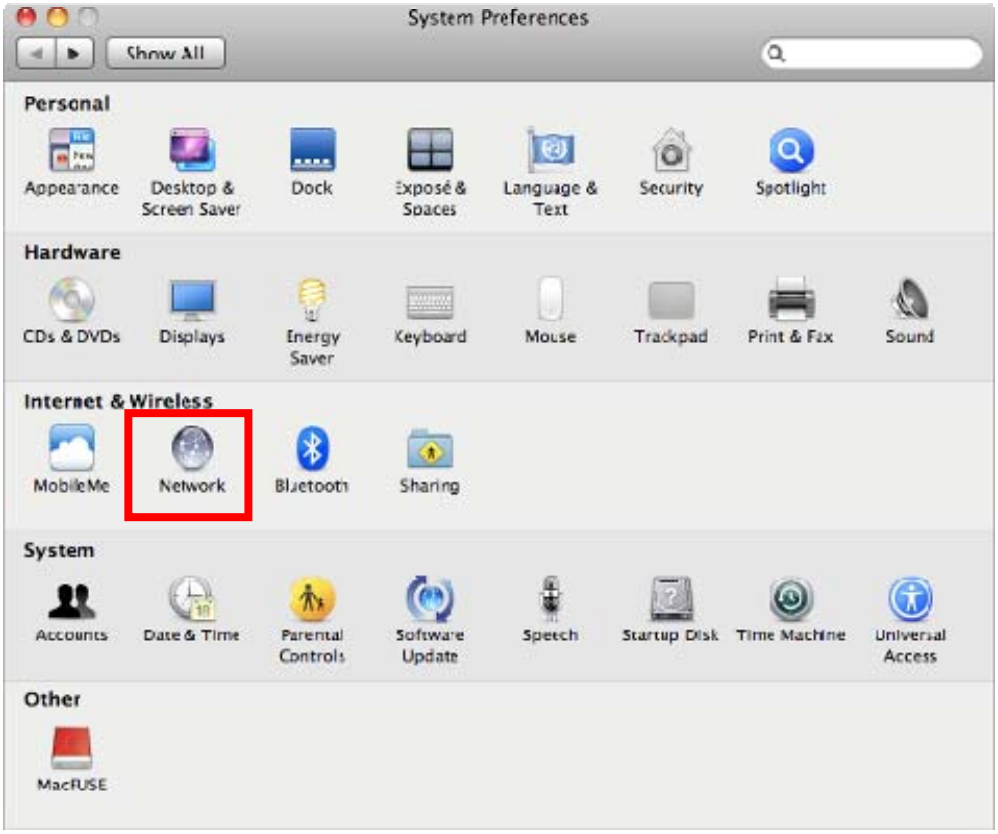


Figure 6-15 System Preferences -- Network

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

(1) Choose the **AirPort** on the left-menu (make sure it is ON)

(2) Select Network Name [**default**] here

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

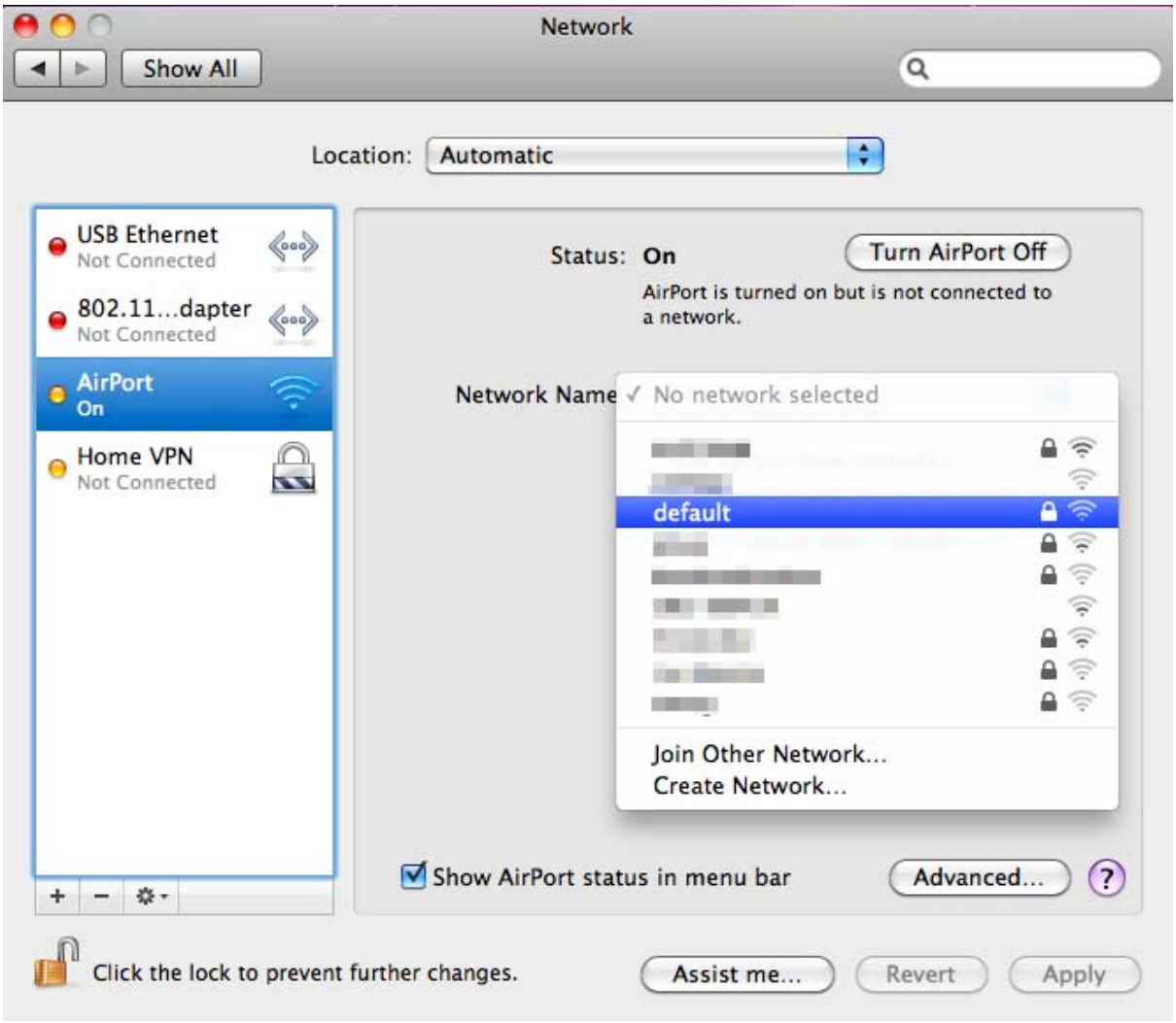


Figure 6-16 Select the Wireless Network

6.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the WDAP-8350 is configured to "**default**".

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

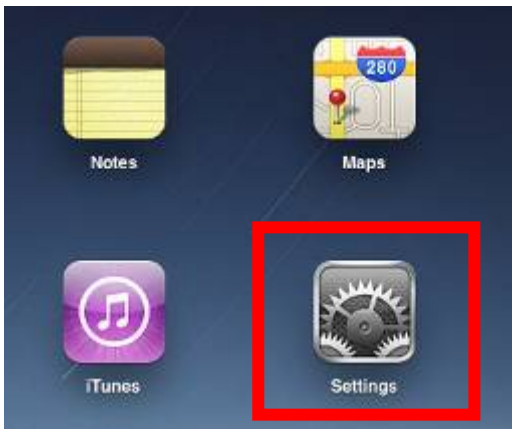


Figure 6-17 iPhone – Settings Icon

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

(3) Tap [**General**] \ [**Network**]

(4) Tap [**Wi-Fi**]

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

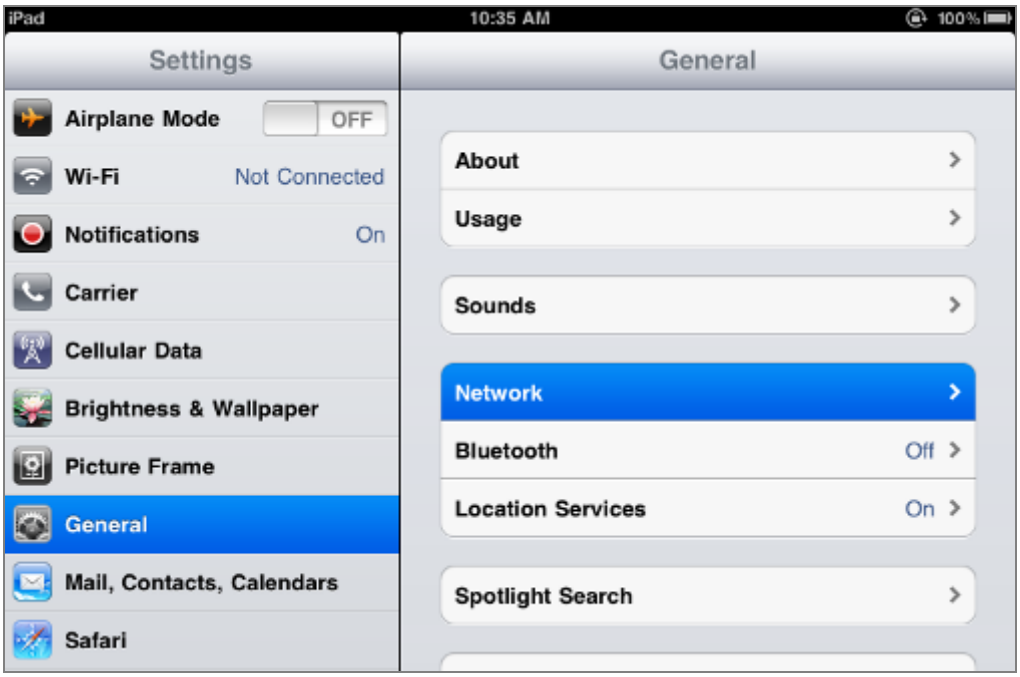


Figure 6-18 Wi-Fi Setting

Figure 6-19 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

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

Figure 6-20 Turn on Wi-Fi

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

(1) The password input screen will be displayed

(2) Enter the encryption key

(3) Tap the [**Join**] button

Figure 6-21 iPhone -- Enter the Password

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

If “Yes”, then there will be a “check” symbol before the SSID.

Figure 6-22 iPhone -- Connected to the Network

Appendix A: Planet Smart Discovery Utility

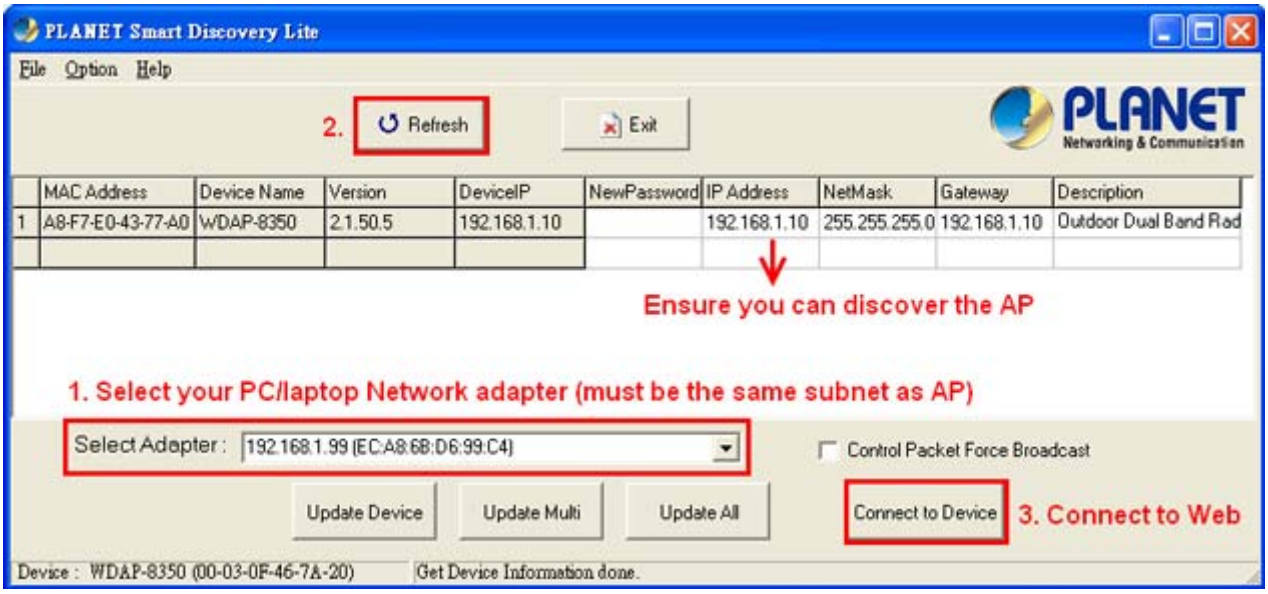
To easily list the WDAP-8350 in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution. The utility is available at: http://www.planet.com.tw/en/product/images/48590/Planet_Utility.zip

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

Step 1: **Planet Smart Discovery Utility** is in administrator PC.

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

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



Step 4: Press the **"Connect to Device"** button and then the Web login screen appears.

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

Appendix B: Troubleshooting

If you find the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the dealer for help. Some problems can be solved by yourself within a very short time.

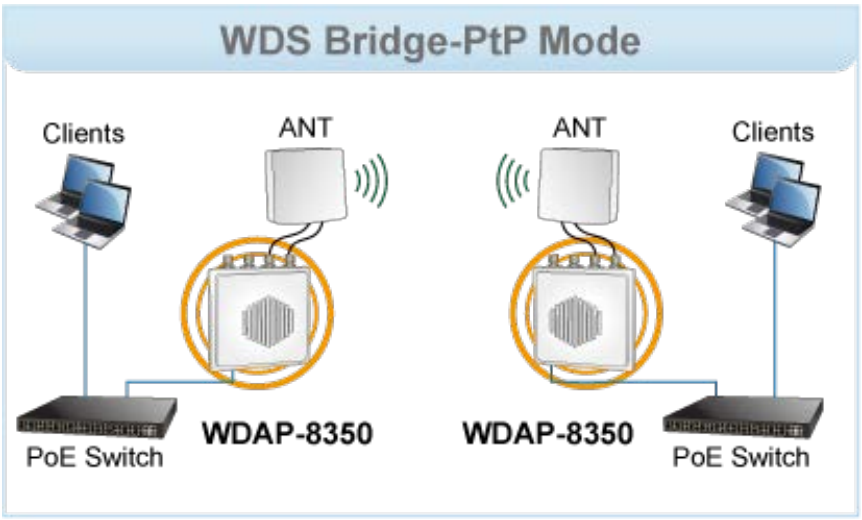
Scenario	Solution
The AP is not responding to me when I want to access it by Web browser.	a. Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be correctly and firmly inserted to the AP. b. If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered. c. You must use the same IP address section which AP uses. d. Are you using MAC or IP address filter? Try to connect the AP by another computer and see if it works; if not, please reset the AP to the factory default settings (pressing the 'reset' button for over 7 seconds). e. Use the Smart Discovery Tool to see if you can find the AP or not. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all the solutions above don't work, contact the dealer for help.
I can't get connected to the Internet.	a. Go to 'Status' -> 'Internet Connection' menu on the router connected to the AP, and check Internet connection status. b. Please be patient, sometimes Internet is just that slow. c. If you've connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password entered in the router's settings again. e. Call your Internet service provider and check if there's something wrong with their service. f. If you just can't connect to one or more websites, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the AP and try again later. h. Reset the device provided by your Internet service

	provider too. i. Try to use IP address instead of host name. If you can use IP address to communicate with a remote server, but can't use host name, please check DNS setting.
I can't locate my AP by my wireless device.	a. 'Broadcast ESSID' set to off? b. Both two antennas are properly secured. c. Are you too far from your AP? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	a. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes. Please be patient. c. Try to reset the AP and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. e. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; the password is wrong.	a. Make sure you're connecting to the correct IP address of the AP! b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The AP becomes hot	a. This is not a malfunction, if you can keep your hand on the AP's case. b. If you smell something wrong or see the smoke coming out from AP or A/C power adapter, please disconnect the AP and power source from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

Appendix C: Frequently Asked Questions

Q1: How to set up the WDS PtP Connection

Topology:

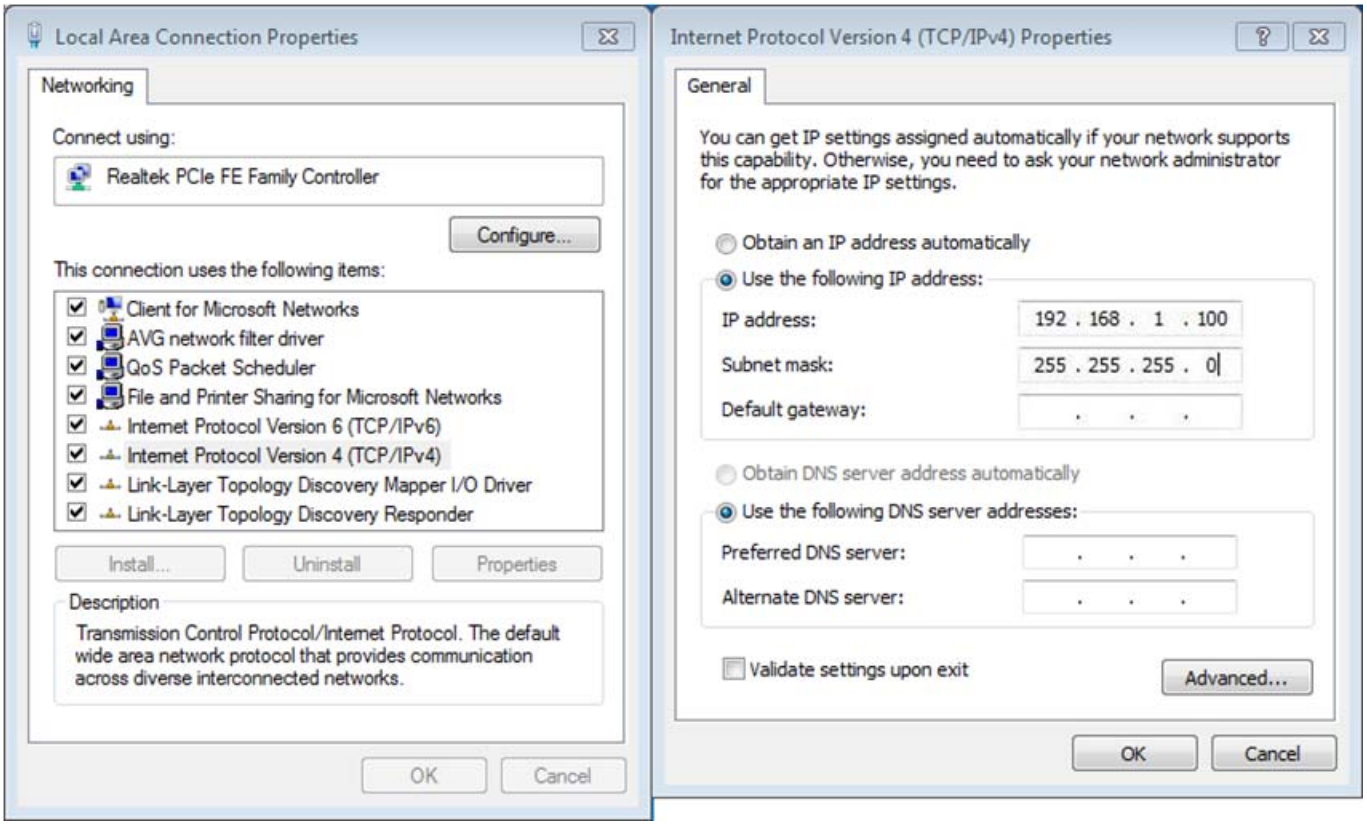


NOTE:

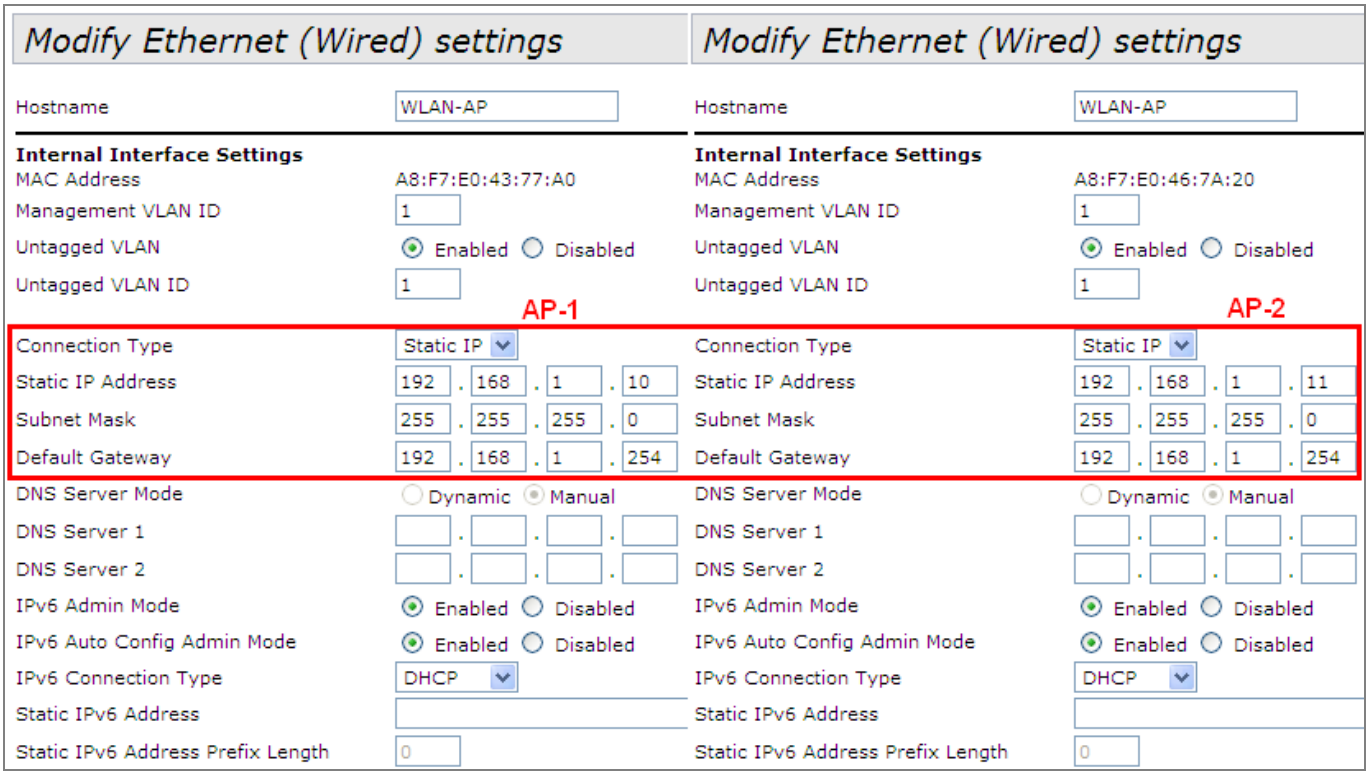
1. The default LAN IP is "**DHCP Client**", please disable any device with DHCP Server enabled.
2. Please configure your PC/laptop to use static IP (192.168.1.x, x can be 1~254 except 10) to access the AP.
3. The default IP of the AP is "**192.168.1.10**" and the default login username and password are both "admin".
4. In this case, we use **5GHz** (Radio2) to establish the WDS connection.

Procedure:

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**".



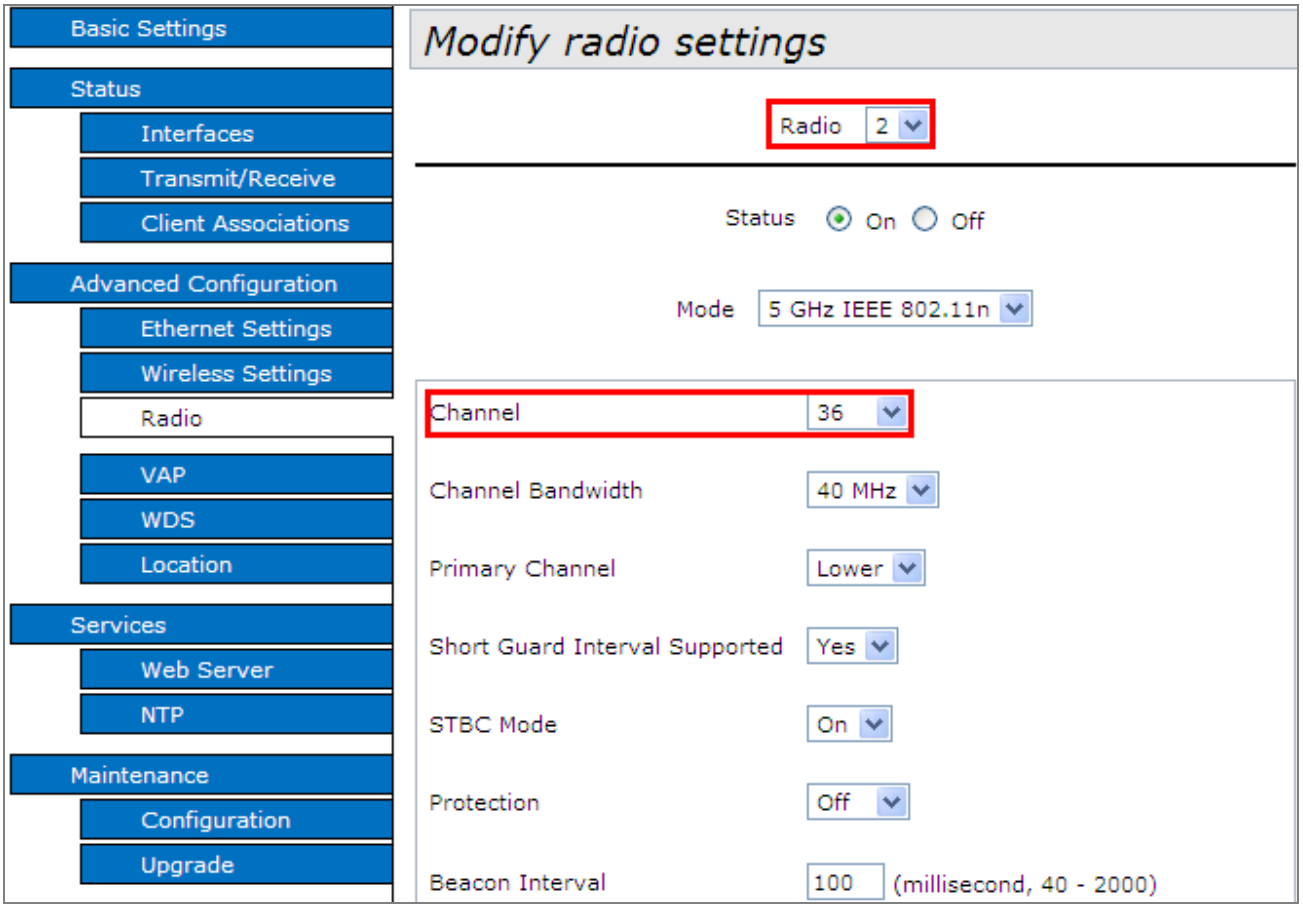
2. In AP-1 and AP-2, go to "**Advanced Configuration-> Ethernet Settings**" to configure the connection type to "**Static IP**" and configure them to use a different IP address.

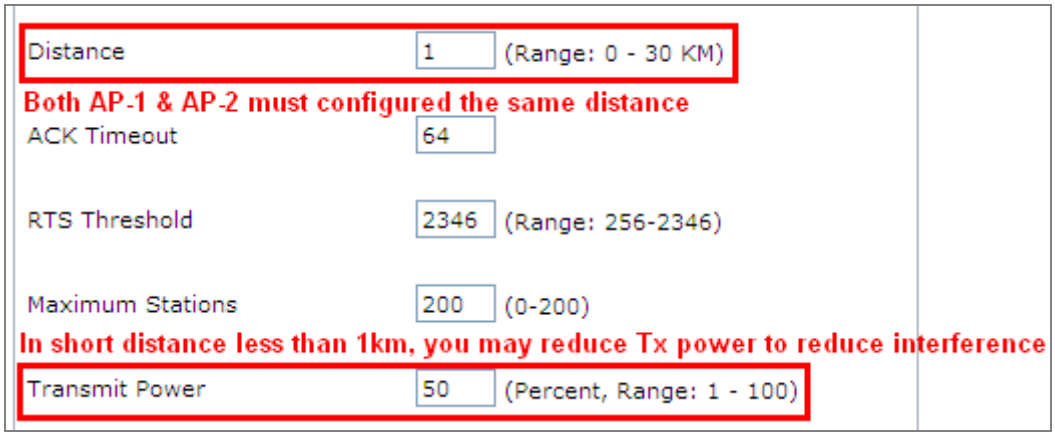


3. In AP-1 and AP2, go to "**Advanced Configuration-> Radio**" to configure the radio setting and channel.

1) **Radio**: Select the frequency that you want to use. (In this case, use 5GHz/Radio 2.)

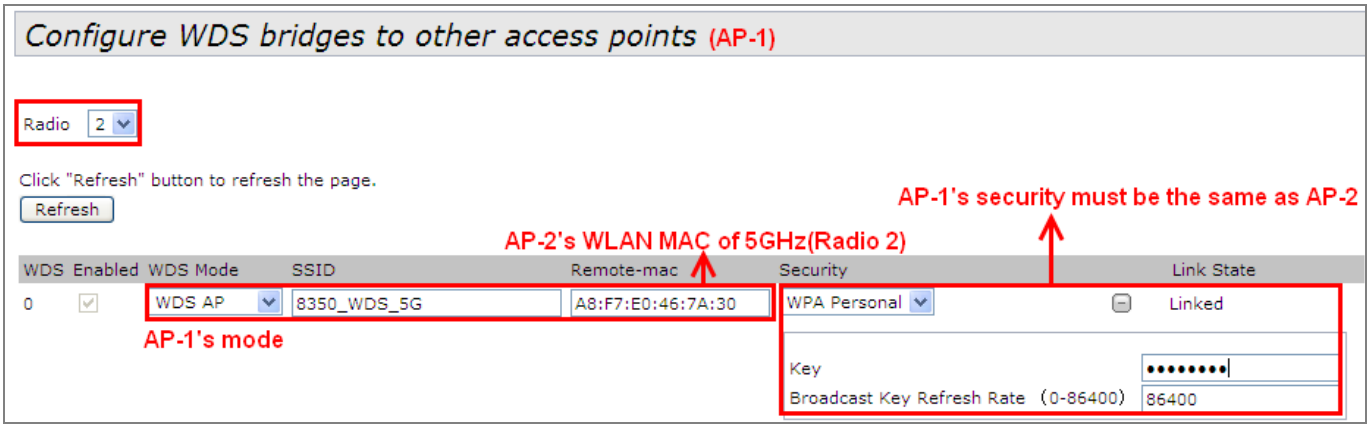
2) **Channel**: Set to a fixed one (Both AP-1 and AP-2 must use the same fixed channel.)



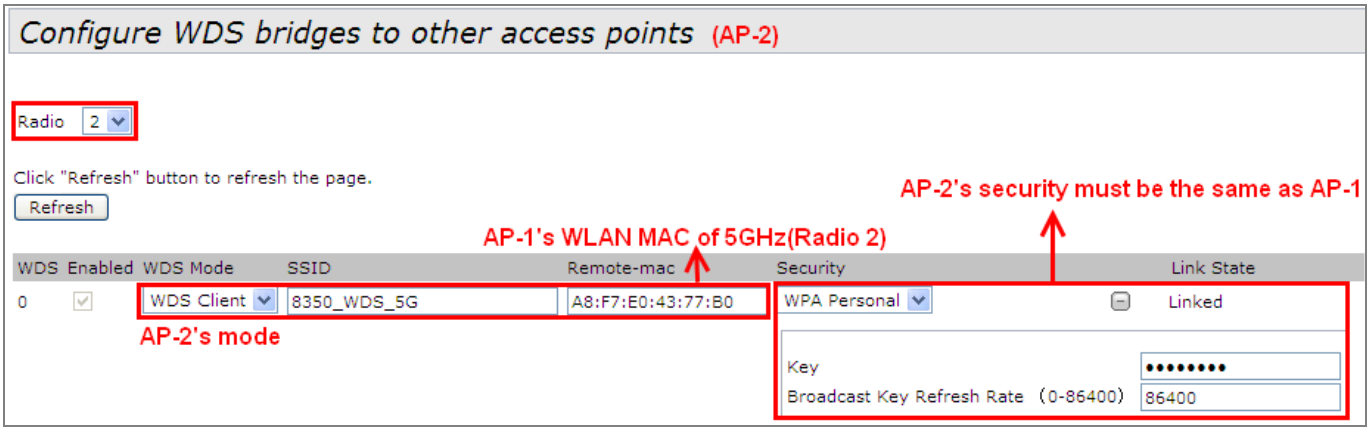


4. In AP-1 and AP-2, go to "**Advanced Configuration-> WDS**" to configure the WDS setting. The SSID and Security must be the same.

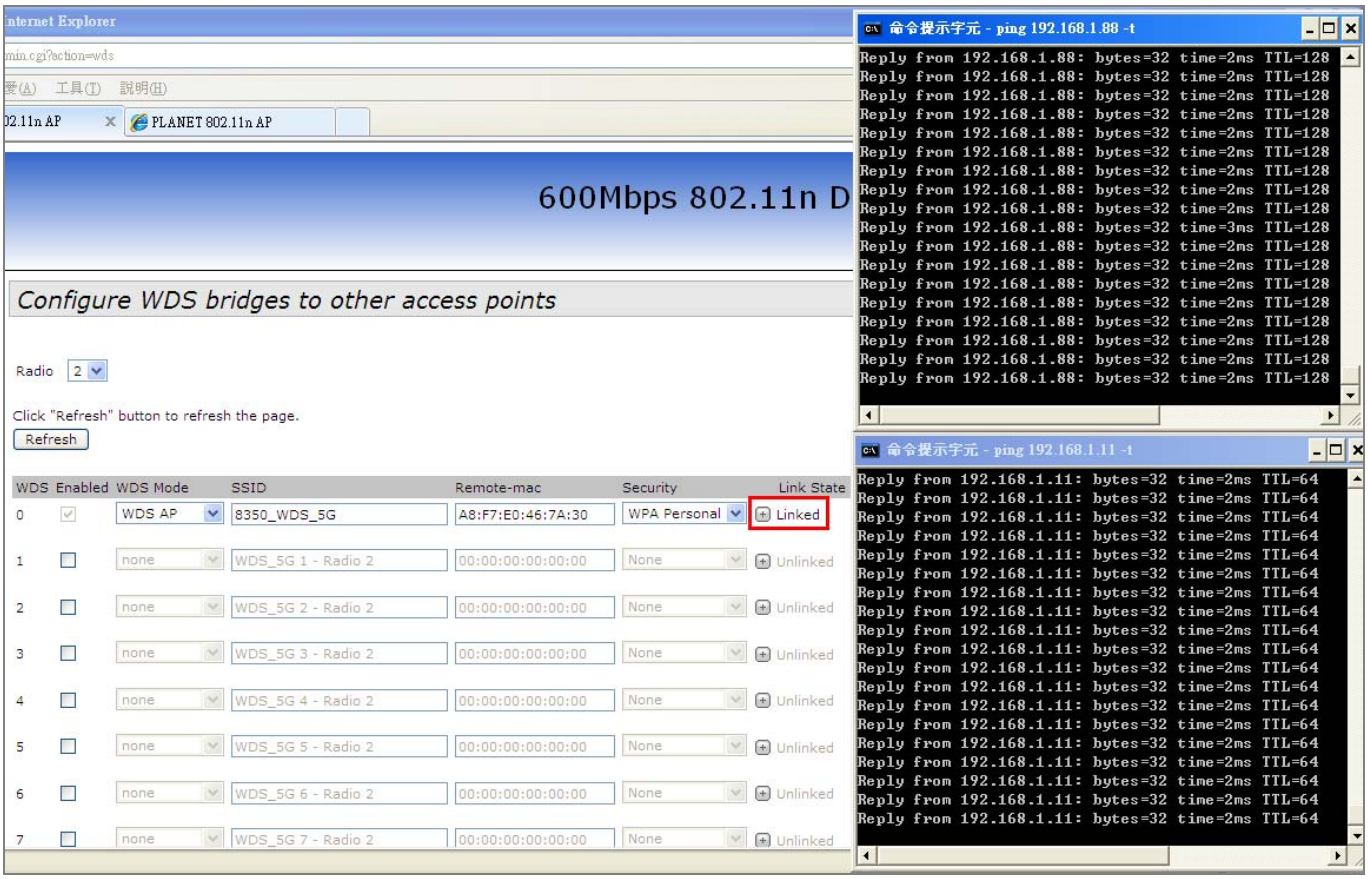
[AP-1's setting]

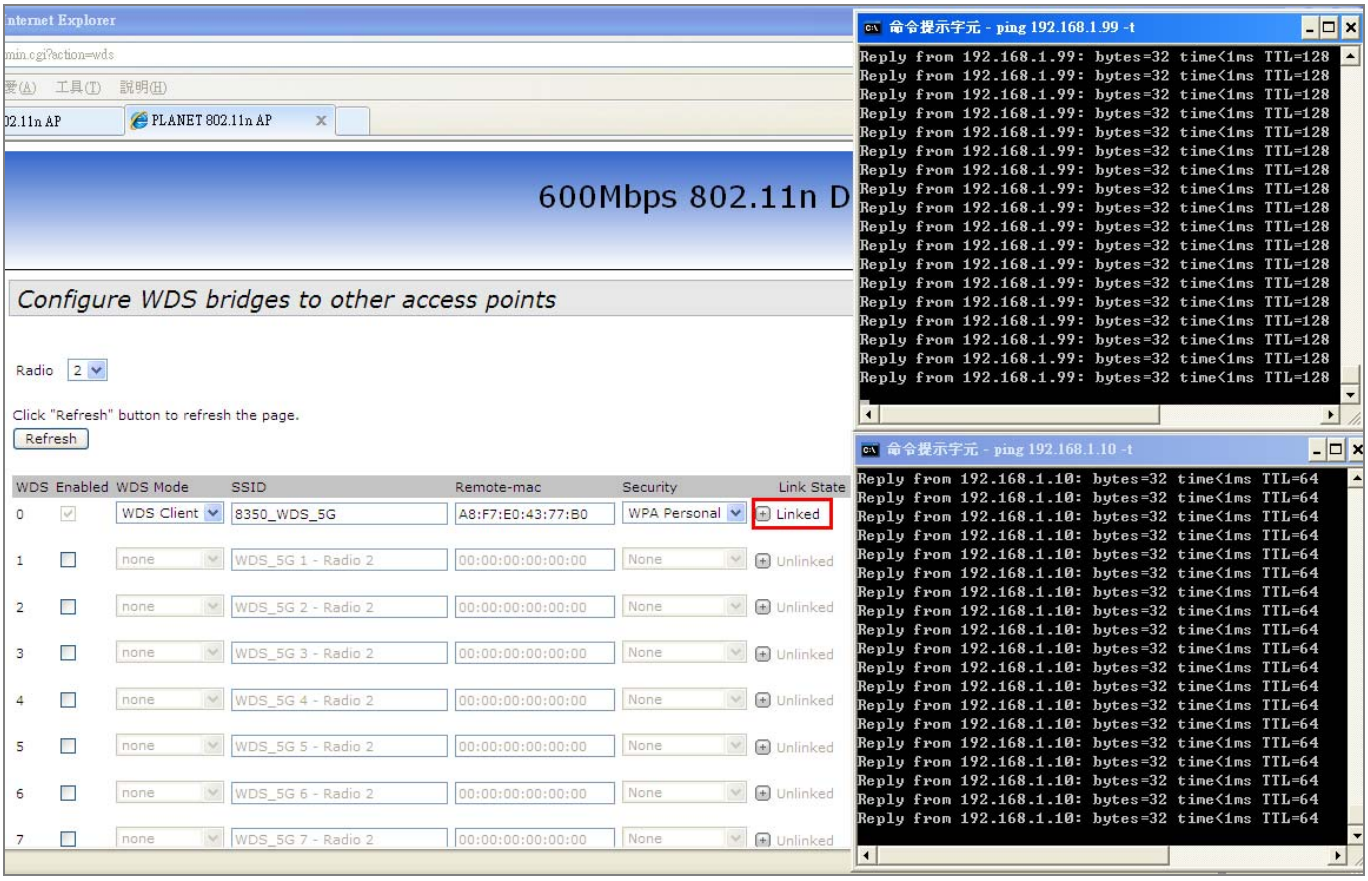


[AP-2's setting]



5. In AP-1 and AP-2, ping each other to ensure the connection has been established. Once the connection is established, the "**Link State**" will be "**Linked**".



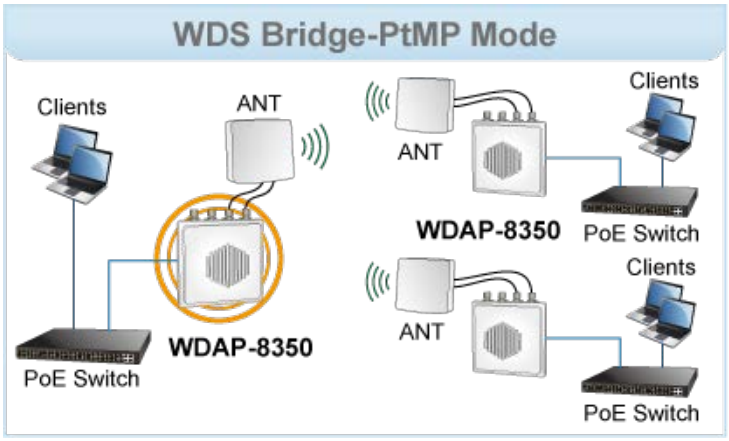


The following hints should be paid attention to:

1) The SSID, channel and security must be the same in both sites.
2) Both sites must be Line-Of-Sight.
3) For the short distance less than 1km, please reduce the "Transmit power" of both sites.
4) For the long distance over 1km, please adjust the "Transmit Distance" to the actual distance.

Q2: How to set up the WDS PtMP Connection

Topology:



NOTE:

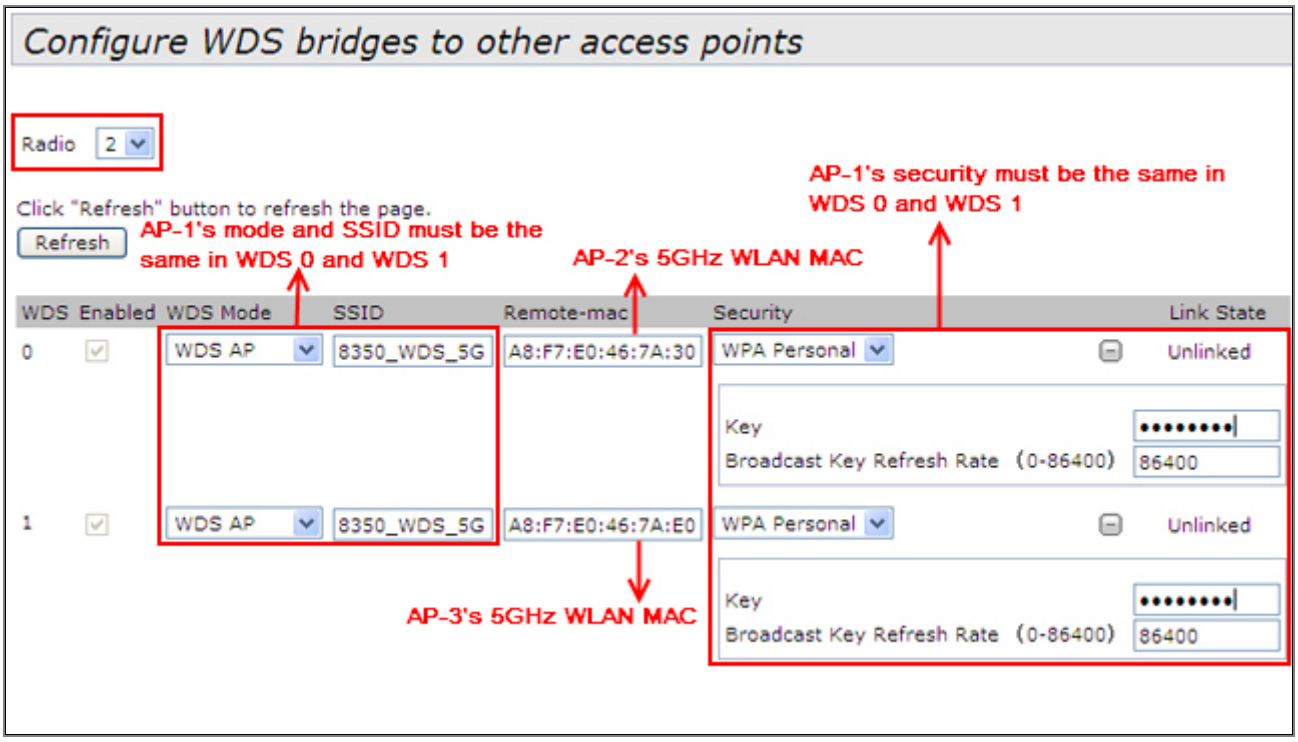
1. The default LAN IP is "**DHCP Client**"; please disable any device with DHCP Server enabled.
2. Please configure your PC/laptop to use static IP (192.168.1.x, x can be 1~254 except 10) to access the AP.
3. The default IP of the AP is "**192.168.1.10**" and the default login username and password are both "admin".
4. In this case, we use **5GHz** (Radio2) to establish the WDS connection.

Procedure:

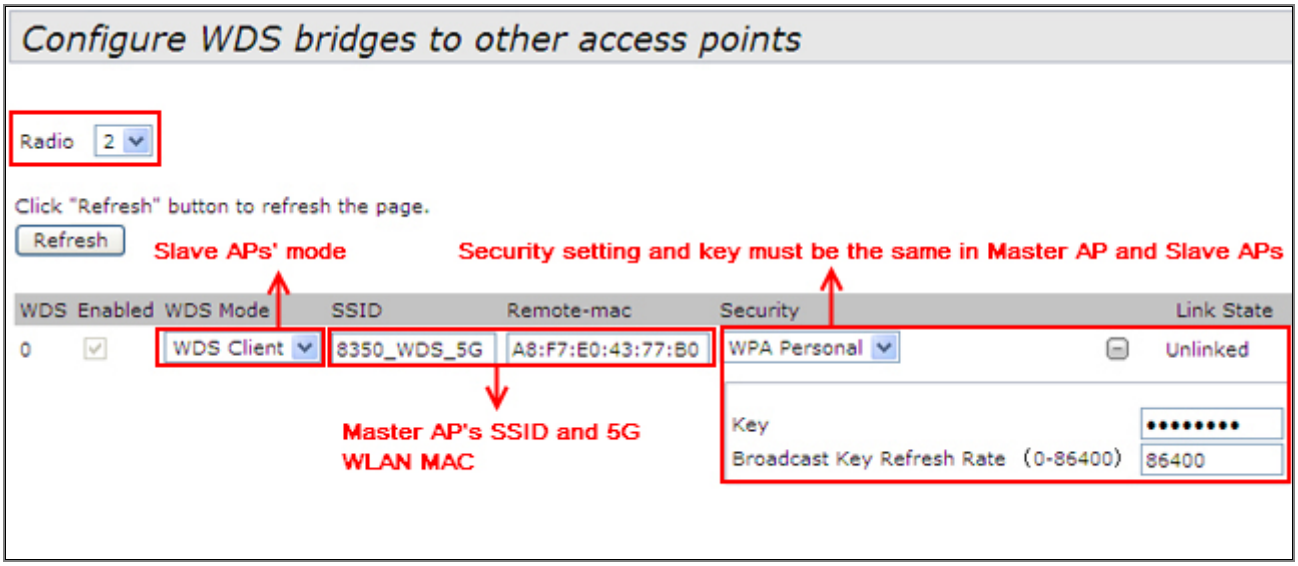
1. Refer to **WDS PtP step 1~3** to configure the master AP and the slave APs.
2. Then, go to "**Advanced Configuration-> WDS**" page of each AP to configure the WDS setting. The SSID and Security must be the same.

[Master AP's setting]

Each entry is for one slave AP. For example, if you have 3 slave APs, you have to configure 3 WDS entries in the master AP.



[Each Slave AP's setting]



3. Once the connection is established, the Link State will be "Linked".

The following hints should be paid attention to:

1) The SSID, channel and security must be the same in all sites.
2) All sites must be Line-Of-Sight.
3) For the short distance less than 1km, please reduce the "Transmit power" of all sites.
4) For the long distance over 1km, please adjust the "Transmit Distance" to the actual distance.

EC Declaration of Conformity

For the following equipment:

*Type of Product: 600Mbps Dual Band 802.11n Outdoor Wireless CPE
*Model Number: WDAP-8350

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is here with confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 2014/53/EU R&TTE, Low Voltage Directive 2014/35/EU; EMC Directive 2014/30/EU.

For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.9.1	(2012-06)
EN 301 489-17 V2.2.1	(2012-09)
EN 301 489-1 V1.9.2	(2011-09)
EN 301 893-1 V1.7.1	(2012-06)
EN 62311	(2008)
EN 60950-1	(2006+A11:2009+A1:2010+A12:2011+A2: 2013)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Director**

Taiwan	**29 Jan., 2016**	
Place	*Date*	*Legal Signature*

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation,** declares that this **Outdoor Wireless AP** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **Outdoor Wireless AP** tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation,** tímto prohlašuje, že tato **Outdoor Wireless AP** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **Outdoor Wireless AP** megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation,** erklærer herved, at følgende udstyr **Outdoor Wireless AP** overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **Outdoor Wireless AP** 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 **Outdoor Wireless AP** in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)	**Nederlands**	Hierbij verklaart , **PLANET Technology orporation,** dat **Outdoor Wireless AP** 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 **Outdoor Wireless AP** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation,** oświadcza, że **Outdoor Wireless AP** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC”.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **Outdoor Wireless AP***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*	**Português**	**PLANET Technology Corporation**, declara que este **Outdoor Wireless AP** 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 **Outdoor Wireless AP** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	**Slovensky**	Výrobca **PLANET Technology Corporation,** týmto deklaruje, že táto **Outdoor Wireless AP** 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 **Outdoor Wireless AP** 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 **Outdoor Wireless AP** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , **PLANET Technology Corporation,** dichiara che questo **Outdoor Wireless AP** è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **Outdoor Wireless AP** 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 **Outdoor Wireless AP** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation,** att denna **Outdoor Wireless AP** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.