PLANET
Networking & Communication

User's Manual

2.4GHz 150Mbps 802.11n Outdoor Wireless AP/Router

► WNAP-6315

www.PLANET.com.tw

Copyright

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

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 2.4GHz 802.11n Wireless Outdoor CPE AP/ Router

Model: WNAP-6315

Rev: 1.0 (May, 2015)

Part No. EM-WNAP-6315_v1.0 (2081- E10620-000)

CONTENTS

FIGURE

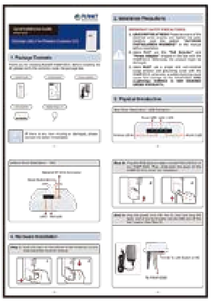
Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WNAP-6315. Before installing the AP, please verify the contents inside the package box.

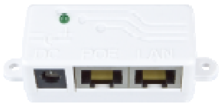
WNAP-6315

Quick Guide



Plastic Strap

PoE Injector



Power Adapter

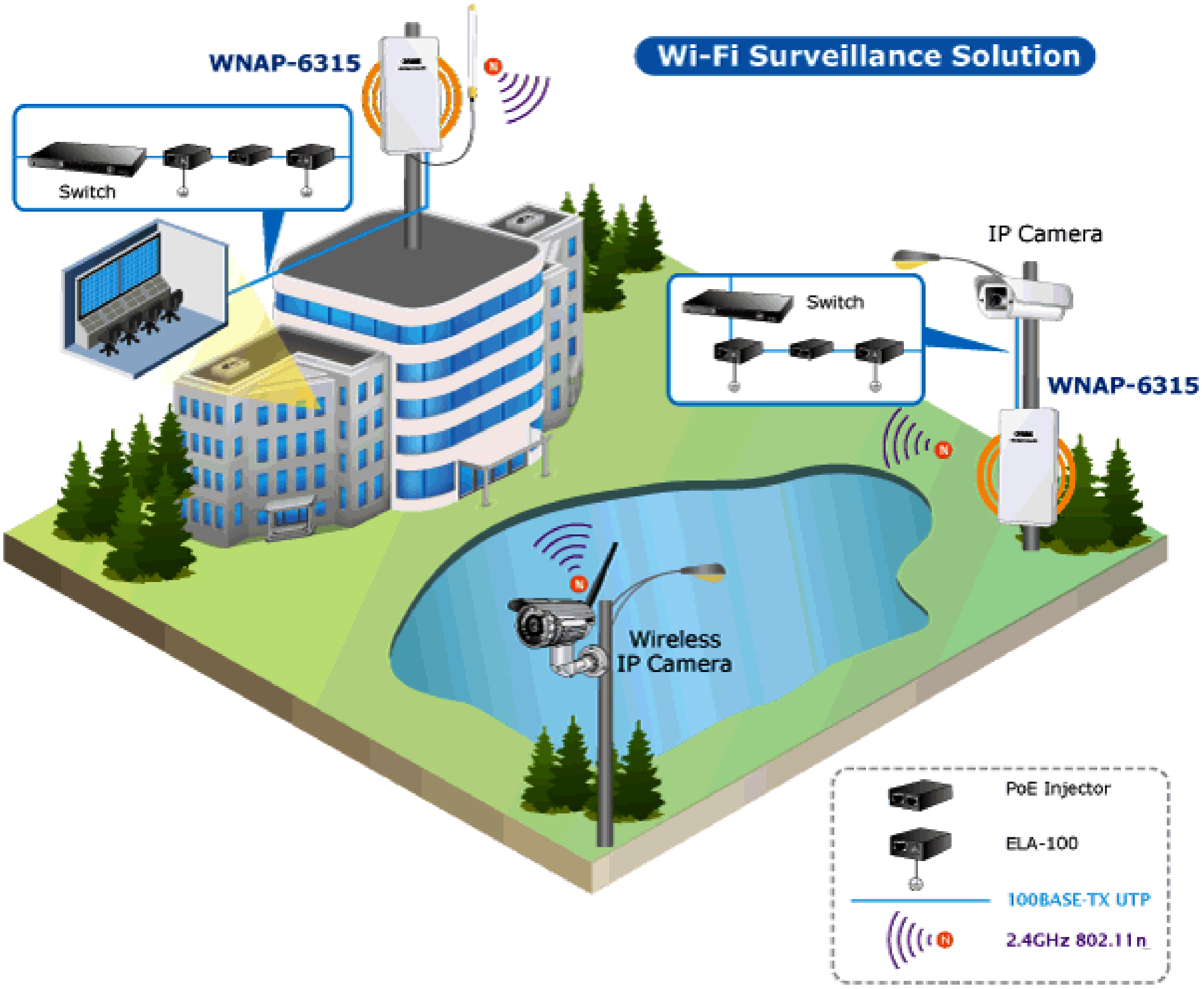
Note

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

1.2 Product Description

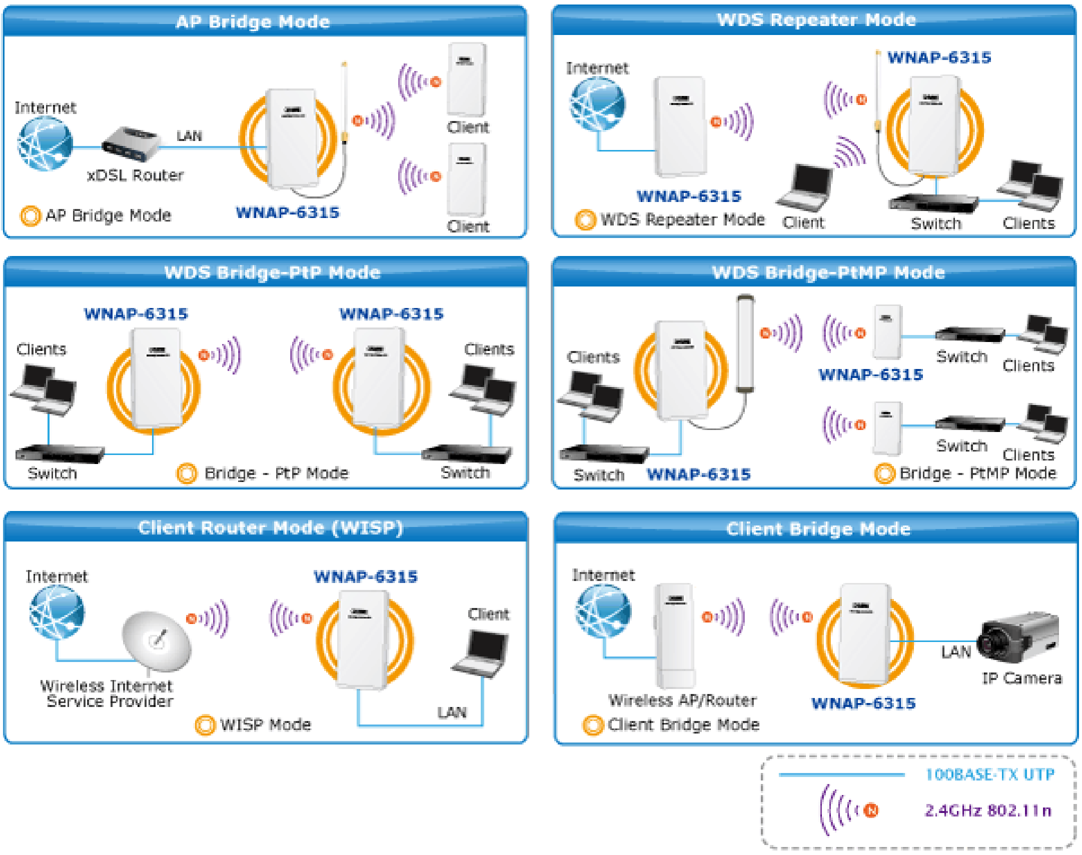
Cost-effective and Flexible Wireless Solution

PLANET WNAP-6315 is compatible with **IEEE 802.11b/g/n standard** and supports a data rate of up to 150Mbps in 802.11n mode. The WNAP-6315 not only has a built-in 12dBi panel antenna but also reserves one **RP-SMA** type antenna connector to allow versatile antenna installations including omnidirectional, yagi, sector, flat-panel and grid antennas. Furthermore, the WNAP-6315 can directly communicate with the wireless IP cameras by using the popular 2.4GHz frequency band, thus turning the surveillance services into a wireless environment.



Multiple Operation Modes Designed for Various Applications

The WNAP-6315 supports as many as 8 wireless operation modes including **AP Bridge, AP Router, Client Bridge, Client Router (WISP), WDS PtP, WDS PtMP, Repeater** and **Universal Repeater**, thus meeting users' various application requirements.



Advanced Security and Rigorous Authentication

The WNAP-6315 supports 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 from unauthorized users or stop an unauthenticated wireless access to bandwidth. Users are granted or denied access to the wireless LAN network based on the ACL (Access Control List) that the administrator pre-established. In addition, with the multiple-SSID feature, you can set up different wireless networks. The WNAP-6315 can therefore serve as a virtual access point for segmented networks tailored to any industrial need.

Rugged Architecture Provides Reliable Outdoor Connection

The WNAP-6315 is equipped with a sturdy and durable housing, meeting the IP55 rating for outdoor usage, which is definitely suitable for harsh environments. Besides, with its UV-resistant feature, the surface of the WNAP-6315's lightweight plastic housing does not yield to brittle fracture easily. Thus, it is as reliable as the metal case but more economical. With the proprietary Power over Ethernet (PoE) design, the WNAP-6315 can be easily installed in the areas where power outlets are not available. Additionally, the reset button on the PoE injector brings convenience to the administrator who can remotely recover the system’s original setting and the self-healing (schedule reboot) capability to keep connection alive all the time.

Easy Deployment and Management

With user-friendly Web UI and step-by-step setup wizard, the WNAP-6315 is easy to install, even for users who never experience in setting up a wireless network. Moreover, with the Planet Smart Discovery Utility and Planet Dynamic DNS service, the WNAP-6315 is convenient to be managed and configured remotely.

1.3 Product Features

- **Industrial Compliant Wireless LAN and LAN**
  - Compliant with IEEE 802.11n wireless technology capable of having a data rate of up to 150Mbps
  - Backward compatible with 802.11b/g standard
  - Equipped with 10/100Mbps RJ45 ports for LAN and WAN with auto MDI/ MDI-X supported
- **Fixed-network Broadband Router**
  - Supports WAN connection types: Dynamic IP, static IP, PPPoE, PPTP and L2TP
  - Supports multiple sessions like IPSec, L2TP and PPTP VPN pass-through
  - Supports virtual server and DMZ for various networking applications
  - Supports DHCP server, UPnP and Planet DDNS
- **RF Interface Characteristics**
  - Built-in 12dBi-directional antenna
  - High Output Power with multiply-adjustable transmit power control
  - Optional RP-SMA connector for flexible wireless deployment
- **Outdoor Environmental Characteristics**
  - IP55-rated outdoor UV-resistant plastic enclosure
  - Passive PoE design
  - Reset button on PoE injector
  - Operating temperature: -20~70 degrees C
- **Multiple Operations and Wireless Modes**
  - Multiple operation modes: Bridge, Gateway and WISP
  - Multiple wireless modes: AP Bridge, AP Router, Client Bridge, WDS PtP, WDS PtMP, Repeater, Universal Repeater and Client Router (WISP)
  - Supports multiple-SSID to allow users to access different networks through a single AP
  - Supports WMM (Wi-Fi Multimedia) for better performance
- **Secure Network Connection**
  - Supports software Wi-Fi Protected Setup (WPS)
  - Advanced security: 64/128-bit WEP, WPA / WPA2, WPA-PSK / WPA2-PSK (TKIP/AES) and 802.1X authentication
  - Supports NAT firewall features with SPI function to protect against DoS attacks
  - Supports IP / Protocol-based access control and MAC filtering
- **Easy Installation and Management**
  - Web-based UI and Quick Setup Wizard for easy configuration
  - Planet Smart Discovery Utility allows administrator to discover and locate each AP
  - System status monitoring includes DHCP Client and System Log

1.4 Product Specifications

Product	**WNAP-6315** **2.4GHz 802.11n Wireless Outdoor CPE AP/ Router**
Hardware	
Standard Support	IEEE 802.11b/g/n IEEE 802.3 IEEE 802.3u IEEE 802.3x
Memory	32 Mbytes DDR SDRAM 4 Mbytes Flash
PoE	Passive PoE
Interface	Wireless IEEE 802.11b/g/n, 1T1R PoE LAN (LAN 1): 1 x 10/100BASE-TX, auto-MDI/MDIX, passive PoE LAN 2/ WAN: 1 x 10/100BASE-TX, auto-MDI/MDIX
Antenna	Internal (Default): 12dBi directional antenna ■ Horizontal: 30 degree ■ Vertical: 20 degree External (Optional): RP-SMA type Connector ■ Switchable by Software ■ For External Antenna Mode, attach antenna before power on
Wireless RF Specifications	
Wireless Technology	IEEE 802.11b/g IEEE 802.11n
Data Rate	IEEE 802.11b: 1, 2, 5.5, 11Mbps IEEE 802.11g: up to 54Mbps IEEE 802.11n (20MHz): up to 72Mbps IEEE 802.11n (40MHz): up to 150Mbps
Media Access Control	CSMA/CA
Modulation	Transmission/Emission type: OFDM Data modulation type: OFDM with BPSK, QPSK, 16-QAM, 64-QAM
Frequency Band	2.412GHz ~ 2.484GHz
Operating Channel	America/ FCC: 2.414~2.462GHz (11 Channels) Europe/ ETSI: 2.412~2.472GHz (13 Channels)
RF Output Power (Max.)	IEEE 802.11b: up to 26 ± 1dBm IEEE 802.11g: up to 21 ± 1dBm IEEE 802.11n: up to 17 ± 1dBm
Receiver Sensitivity (dBm)	IEEE 802.11b: -97dBm IEEE 802.11g: -90dBm IEEE 802.11n: -90dBm
Output Power Control	5-level TX power control
Software Features	
LAN	Built-in DHCP server supporting static IP address distribution

	Supports UPnP
	Supports IGMP Proxy
	Supports 802.1d STP (Spanning Tree)
WAN	■ Static IP ■ DHCP (Dynamic IP) ■ PPPoE ■ PPTP ■ L2TP
VPN Passthrough	■ PPTP ■ L2TP ■ IPSec ■ IPv6
Operation Mode	■ Gateway ■ Bridge ■ WISP
Firewall	NAT firewall with SPI (Stateful Packet Inspection)
	Built-in NAT server supporting virtual server and DMZ
	Built-in firewall with port/ IP address/ MAC/ URL filtering
Wireless Mode	■ AP Bridge ■ AP Router ■ Client Bridge ■ Client Router (WISP) ■ WDS PtP ■ WDS PtMP ■ WDS Repeater ■ Universal Repeater (AP+Client)
Max. SSID	Up to 5
Channel Width	20MHz / 40MHz
Wireless Isolation	Enable to isolate each connected wireless client so that they cannot access mutually
Encryption Type	64/128-bit WEP, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X
Wireless Security	Wireless LAN ACL (Access Control List) filtering
	Wireless MAC address filtering
	Supports WPS (Wi-Fi Protected Setup)
	Enable/Disable SSID Broadcast
Max. Wireless Clients	20
Max. WDS APs	8
Max. Wired Clients	253
WMM	Supports Wi-Fi multimedia
QoS	Supports Quality of Service for bandwidth control
NTP	Network Time Management
Self Healing	Supports Schedule Reboot
B/G Protection Mode	Supports protection mechanism to prevent collisions among 802.11b/g modes
IAPP Roaming	Supports IAPP (Inter Access Point Protocol) roaming

Management	Web UI, DHCP Client, Configuration Backup and Restore, Dynamic DNS
Diagnostic Tool	System Log
Mechanical and Power	
IP Level	IP55
Material	Outdoor UV-resistant enclosure
Dimensions (W x D x H)	127 x 63 x 254 mm
Weight	485g
Installation	Pole mounting or wall mounting
Power Requirements	LAN1 ■ 12V DC, 1A/ passive PoE ■ Pin 4 V DC+ ■ Pin 5 reset ■ Pin 7, 8 V DC-
Power Consumption (Max.)	4W
Environment and Certification	
Operating Temperature	-20~70 degrees C
Operating Humidity	10~95% non-condensing
Regulatory	CE, FCC, RoHS
Accessory	
Standard Accessories	■ WNAP-6315 x 1 ■ 12V Power Adapter x 1 ■ PoE Injector x 1 ■ Plastic Strap x 1 ■ Quick Installation Guide x 1

Chapter 2. Hardware Installation

Please follow the instructions below to connect WNAP-6315 to the existing network devices and your computers.

2.1 Hardware Description

- **Dimensions**: 127 x 63 x 254 mm (W x D x H)

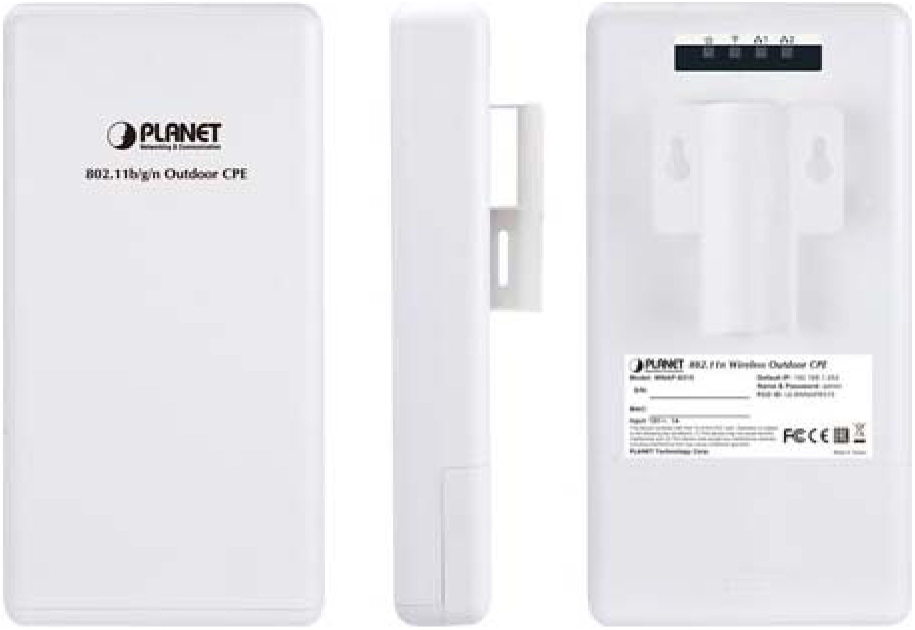


Figure 2-1 Three-way View

Rear Panel – LED

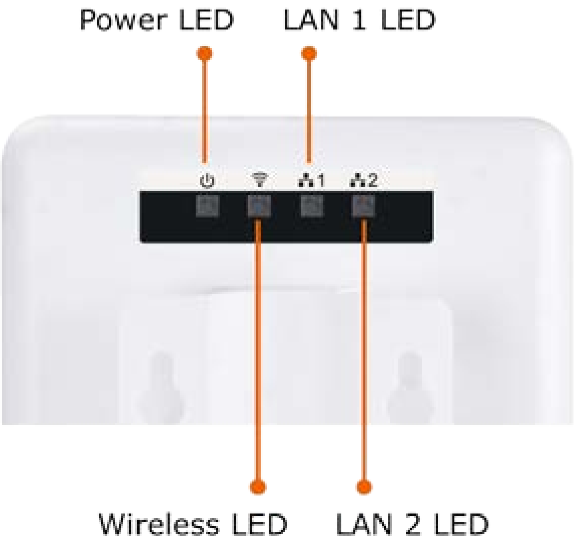


Figure 2-2 LED

LED Definition

LED	Color	State	Meaning
Power	Blue	On	System On
	Blue	Off	System Off
WLAN	Blue	On	Wireless Radio On.
	Blue	Off	Wireless Radio Off.
	Blue	Blinking	Data is transmitting or receiving on the wireless.
LAN1	Blue	On	Port linked.
	Blue	Off	No link.
	Blue	Blinking	Data is transmitting or receiving on the LAN interface.
LAN2 (WAN)	Blue	On	Port linked.
	Blue	Off	No link.
	Blue	Blinking	Data is transmitting or receiving on the WAN interface.

Table 2-1 The LED Indication

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 2-3** shows the bottom panel of the WNAP-6315.

Bottom Panel

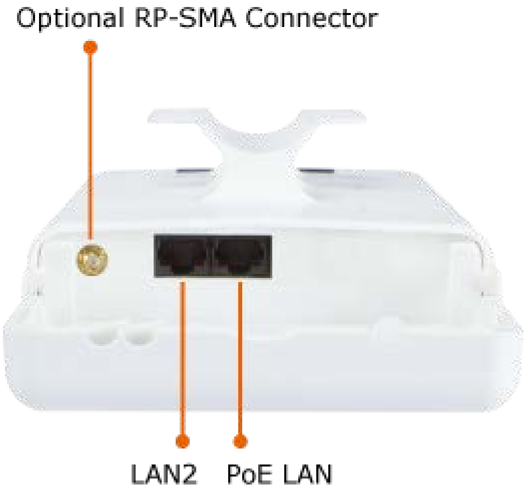
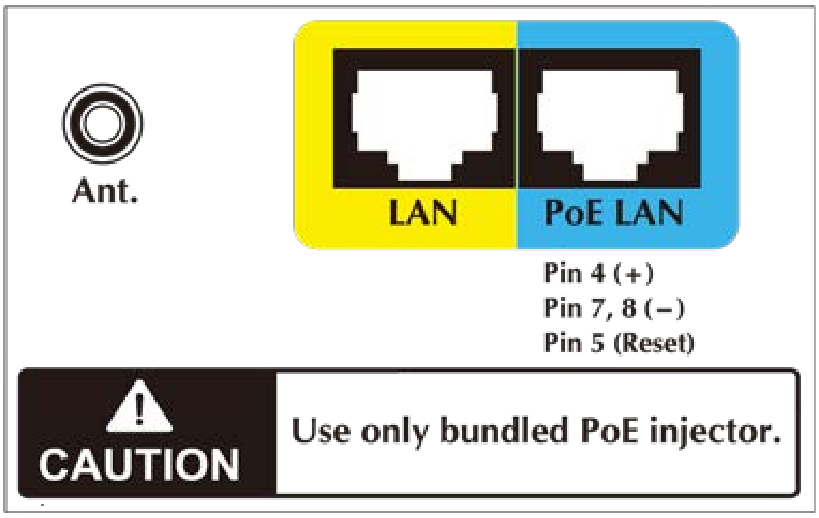


Figure 2-3 Port and Connector of WNAP-6315



Pin 4 (+)
Pin 7, 8 (–)
Pin 5 (Reset)

CAUTION

Use only bundled PoE injector.

Figure 2-4 Port and Connector Description Label

PoE Injector

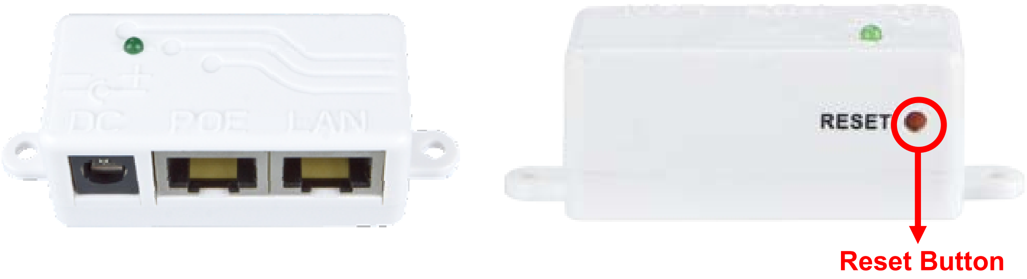
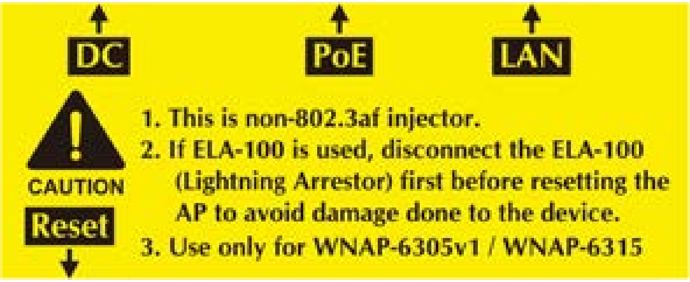


Figure 2-5 PoE Injector of WNAP-6315



DC
PoE
LAN
CAUTION
Reset

1. This is non-802.3af injector.
2. If ELA-100 is used, disconnect the ELA-100 (Lightning Arrestor) first before resetting the AP to avoid damage done to the device.
3. Use only for WNAP-6305v1 / WNAP-6315

Figure 2-6 Label of PoE Injector

H/W Interface Definition

Interface	Function
RP-SMA Connector	You can use the RP-SMA connector to connect with the 2.4GHz outdoor antenna. ※ For External Antenna Mode, you MUST physically attach antenna before powering on. Then, configure the Antenna Switch (Wireless Advanced page) from "**Internal**" to "**External**" via Web UI.
LAN (Passive PoE)	10/100Mbps RJ45 port, auto MDI/ MDI-X & passive PoE supported. Connect LAN port to the PoE injector to power on the device. **PIN assignment:** ■ Pin 4 VDC+ ■ Pin 5 Reset ■ Pin 7, 8 VDC-
WAN	10/100Mbps RJ45 port, auto MDI/ MDI-X. Connect this port to the xDSL modem in gateway mode. Connect this port to the network equipment in bridge mode.
Reset	Push continually the reset button on the PoE injector about 10 seconds to reset the configuration parameters to factory defaults. **※ If you have connected with the thunder protector like PLANET ELA-100, please DO NOT press the reset button on the PoE injector to prevent the ELA-100 from being damaged. Remove the thunder protector before pushing the reset button.**

Table 2-2 The PoE Injector Indication

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 WNAP-6315 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 WNAP-6315, 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** use a proper and well-installed surge arrestor and grounding kit with WNAP-6315; otherwise, a random lightning could easily cause fatal damage to the WNAP-6315. **EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.**

- Users MUST use the “**PoE Injector**” and “**Power Adapter**” shipped in the box with the WNAP-6315. Otherwise, the product might be damaged.

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. Push the latch on the bottom of the WNAP-6315 to remove the sliding cover.

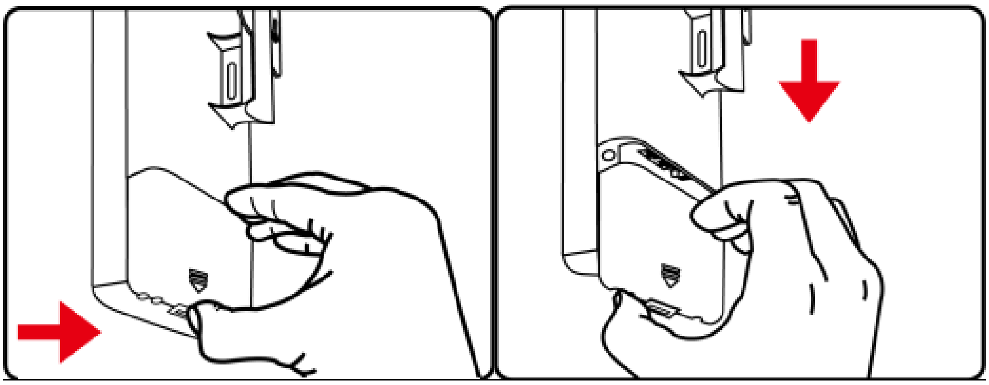


Figure 3-1 Connect the Antenna

Step 2. Plug the RJ45 Ethernet cable into the PoE LAN Port of the WNAP-6315. Then, slide back the cover of the WNAP-6315 to finish the installation.

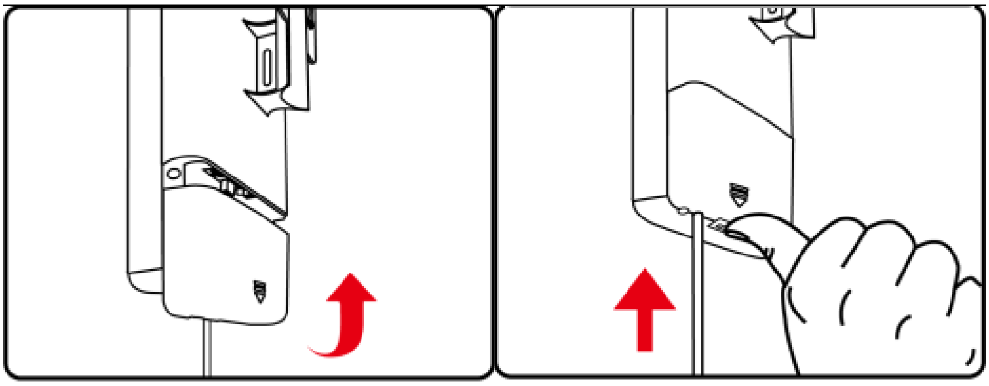


Figure 3-2 Connect the Ethernet cable

Step 3. Plug the power cord into the DC port and plug the other end of the RJ45 cable into the POE port of the PoE injector (See Step 2).

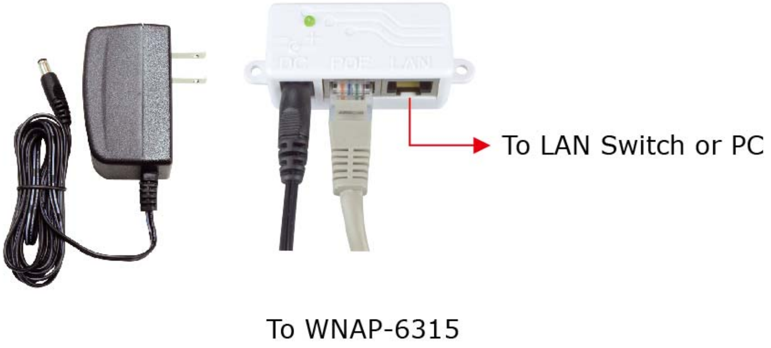


Figure 3-3 Connect the PoE injector

Step 4. Successful installation.

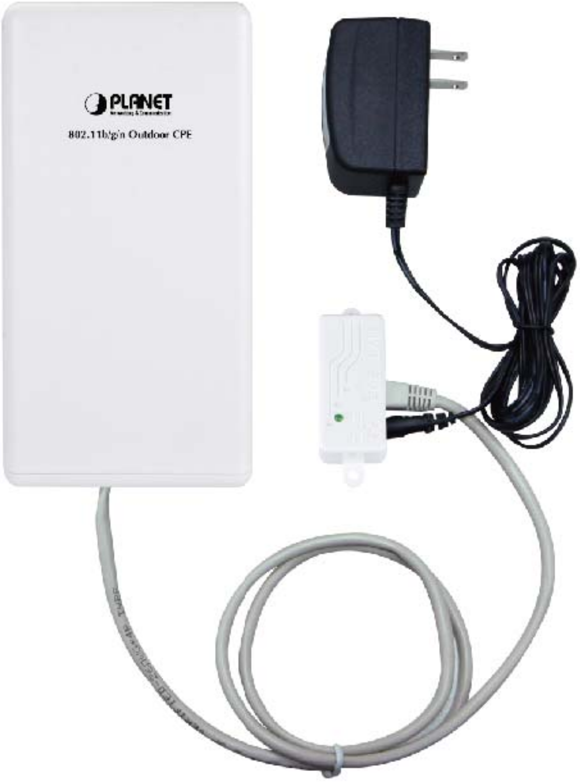


Figure 3-4 Connect the PoE injector

Step 5. Pole Mounting:

Place the strap through the slot on the back of the WNAP-6315 and then around the pole. Tighten the strap to secure the WNAP-6315.

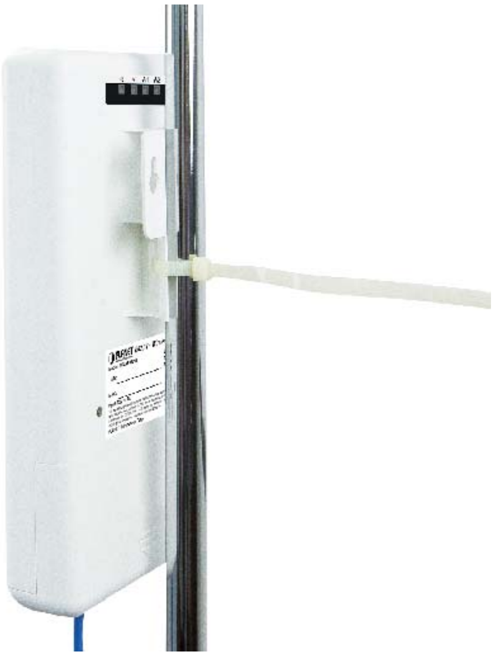


Figure 3-5 Pole Mounting

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 WNAP-6315 is **192.168.1.253**. 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 WNAP-6315 with your PC by an Ethernet cable plugging in LAN port on one side and in LAN port of PC on the other side. Please power on the WNAP-6315 by PoE injector 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.

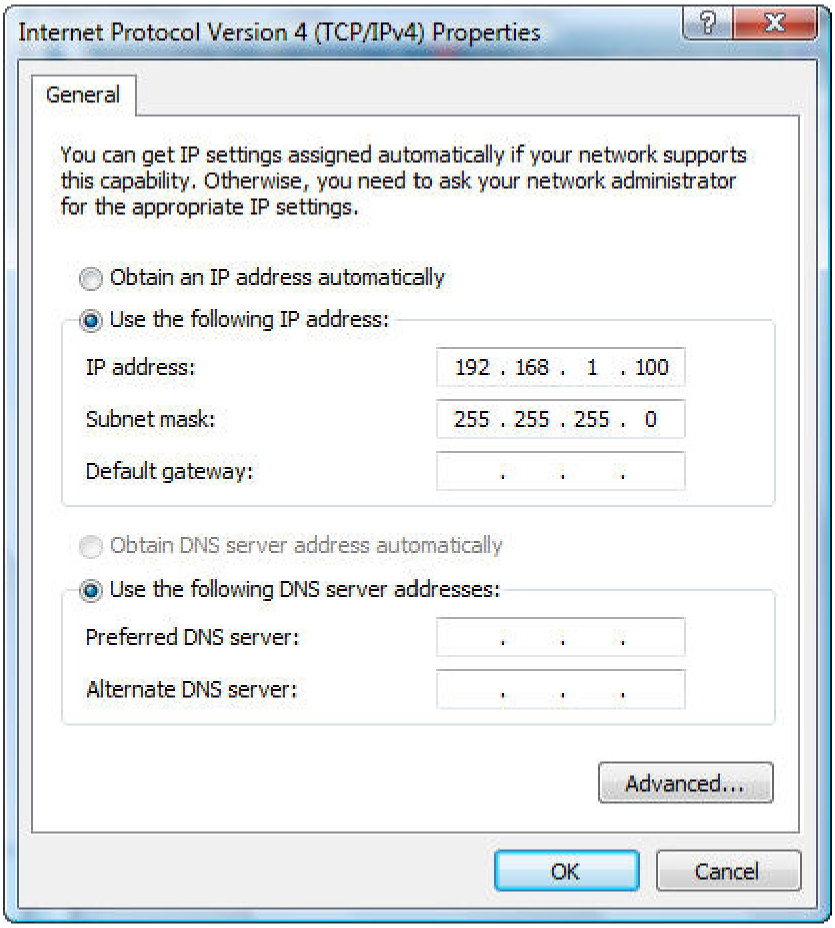
4.1.1 Configuring the IP Address Manually

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 WNAP-6315 is 192.168.1.253, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 252), Subnet Mask is 255.255.255.0.

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 WNAP-6315 is 192.168.1.253 and the DSL router is 192.168.1.254, you may choose from 192.168.1.1 to 192.168.1.252.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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.

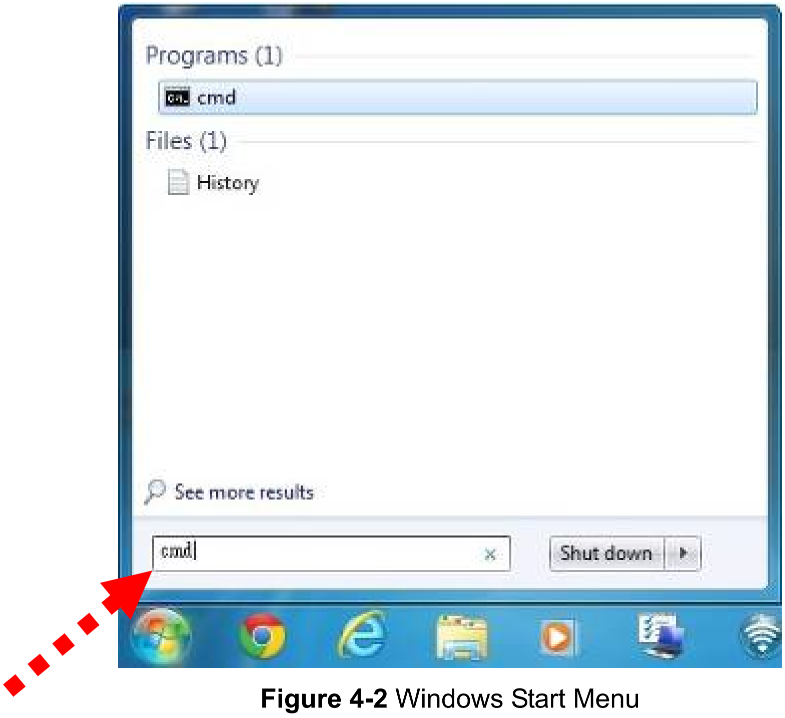
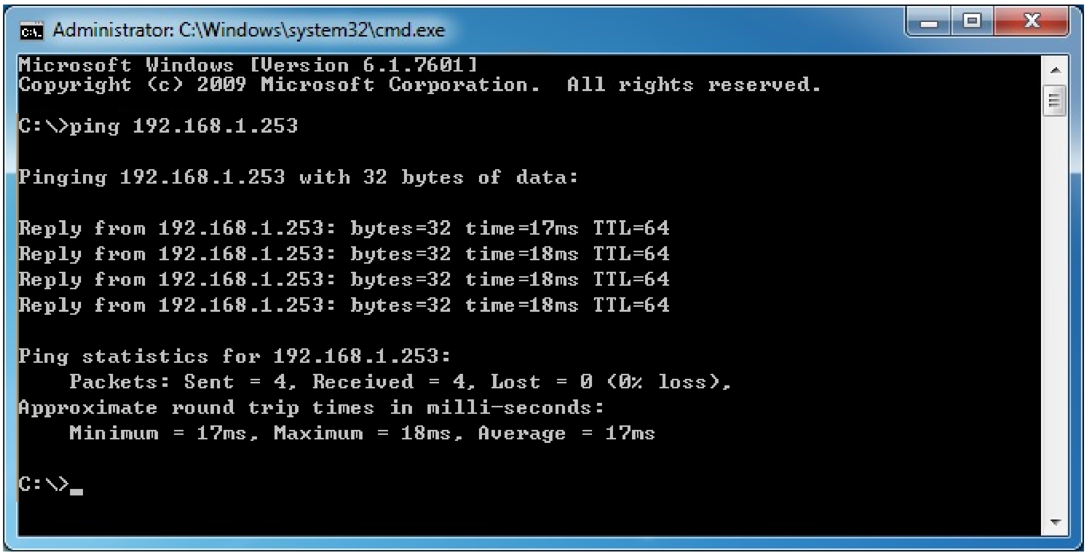


Figure 4-2 Windows Start Menu

3. Open a command prompt, type ping **192.168.1.253** and then press **Enter**.

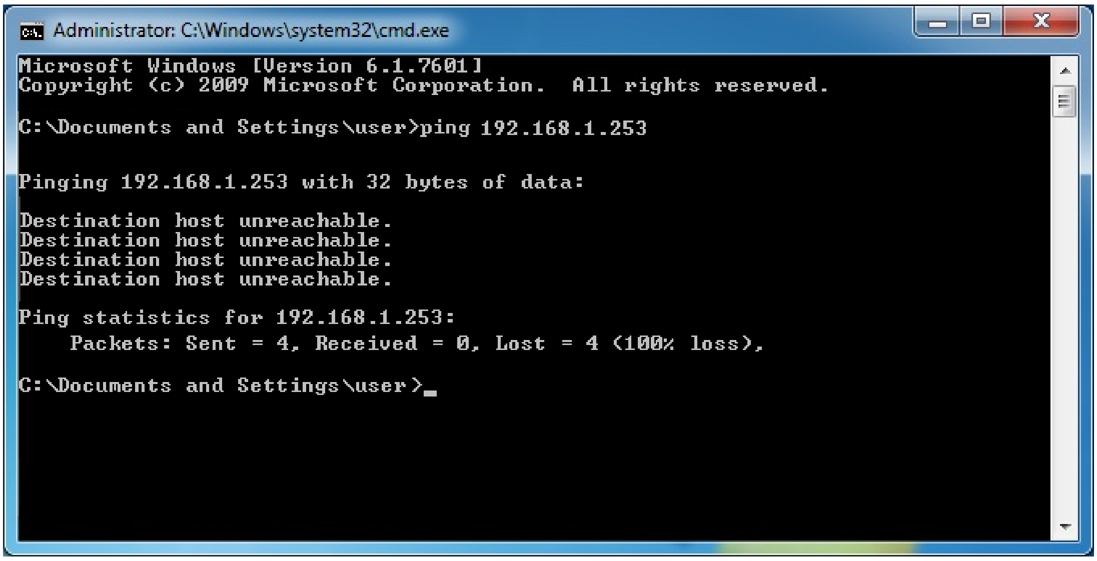
- If the result displayed is similar to **Figure 4-3**, it means the connection between your PC and the AP has been established well.


Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time=17ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms

C:\>_
```

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.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Documents and Settings\user>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\user>_
```

Figure 4-4 Failed Result of Ping Command

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

4.2 Starting Setup in the Web UI

It is easy to configure and manage the AP with the web browser.

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

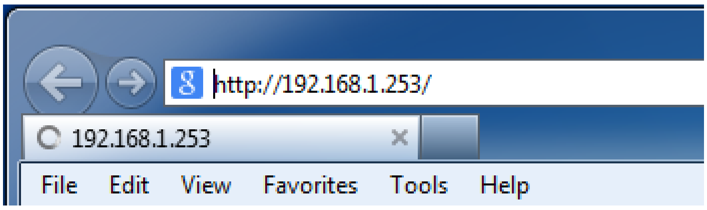
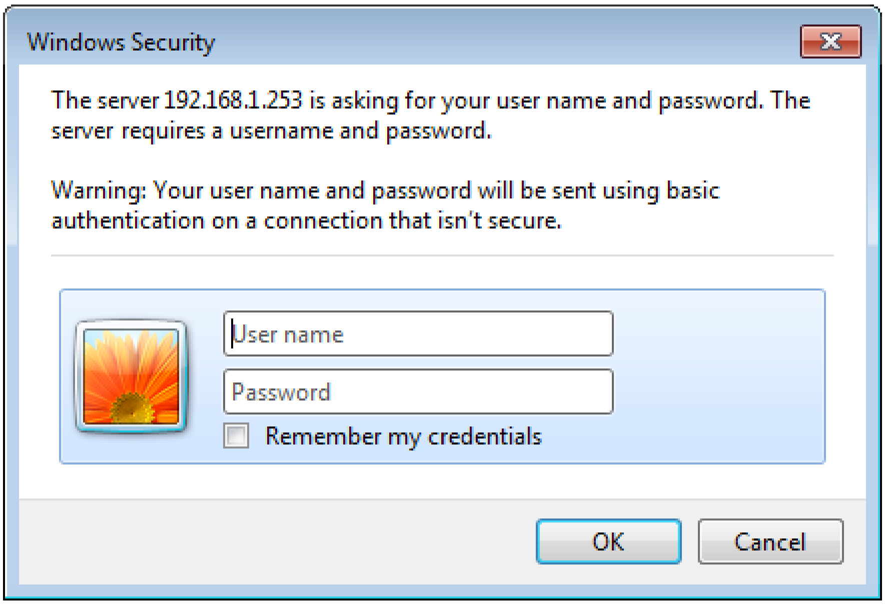


Figure 4-5 Login by default IP address

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


Windows Security

The server 192.168.1.253 is asking for your user name and password. The server requires a username and password.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

Figure 4-6 Login Window

Default IP Address: **192.168.1.253**

Default User name: **admin**

Default Password: **admin**

Note

If the above screen does not pop up, it may mean that your web-browser has been set to a proxy. Go to **Tools menu>Internet Options>Connections>LAN Settings** 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.

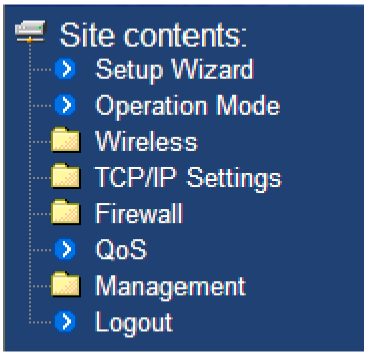
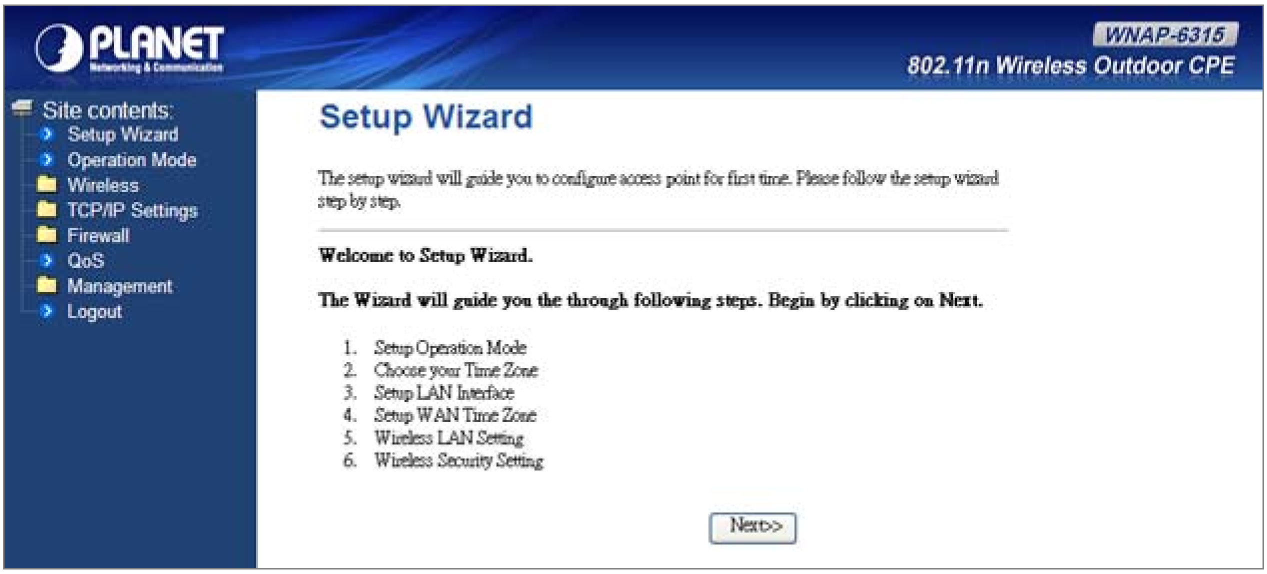


Figure 5-1 Main Menu

5.1 Setup Wizard

The Setup Wizard will guide the user to configure the WNAP-6315 easily and quickly. Select the Setup Wizard on the left side of the screen and by clicking on Next on the Setup Wizard screen shown below, you will then name your WNAP-6315 and set up its security.



Setup Wizard

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step.

Welcome to Setup Wizard.

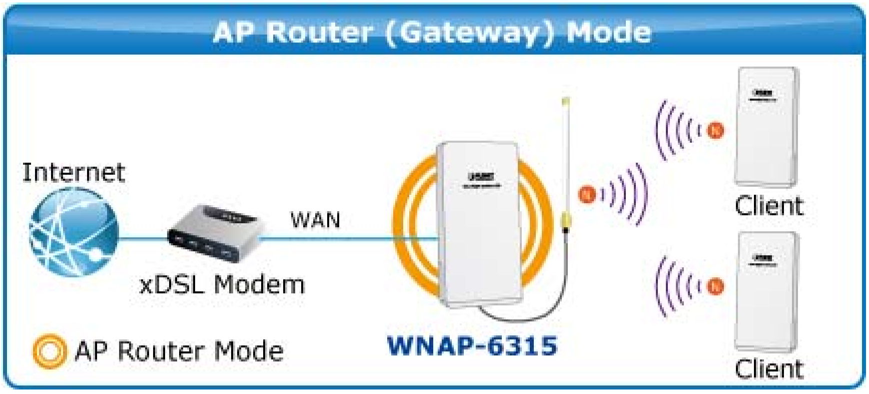
The Wizard will guide you the through following steps. Begin by clicking on Next.

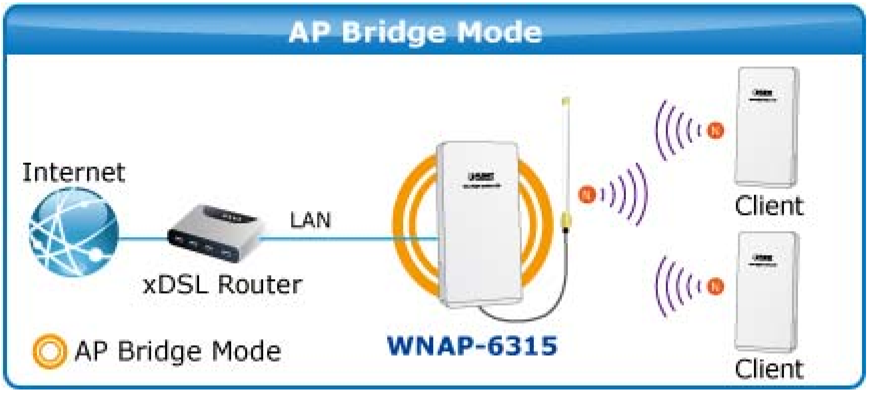
1. Setup Operation Mode
2. Choose your Time Zone
3. Setup LAN Interface
4. Setup WAN Time Zone
5. Wireless LAN Setting
6. Wireless Security Setting

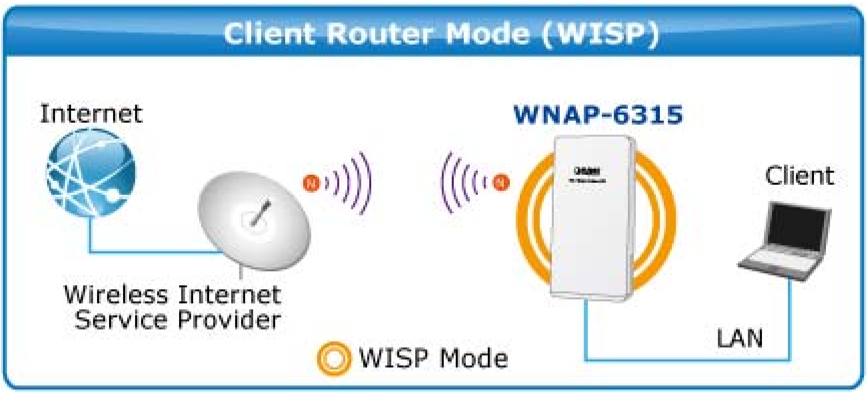
Figure 5-2 Setup Wizard

Step 1: Setup Operation Mode

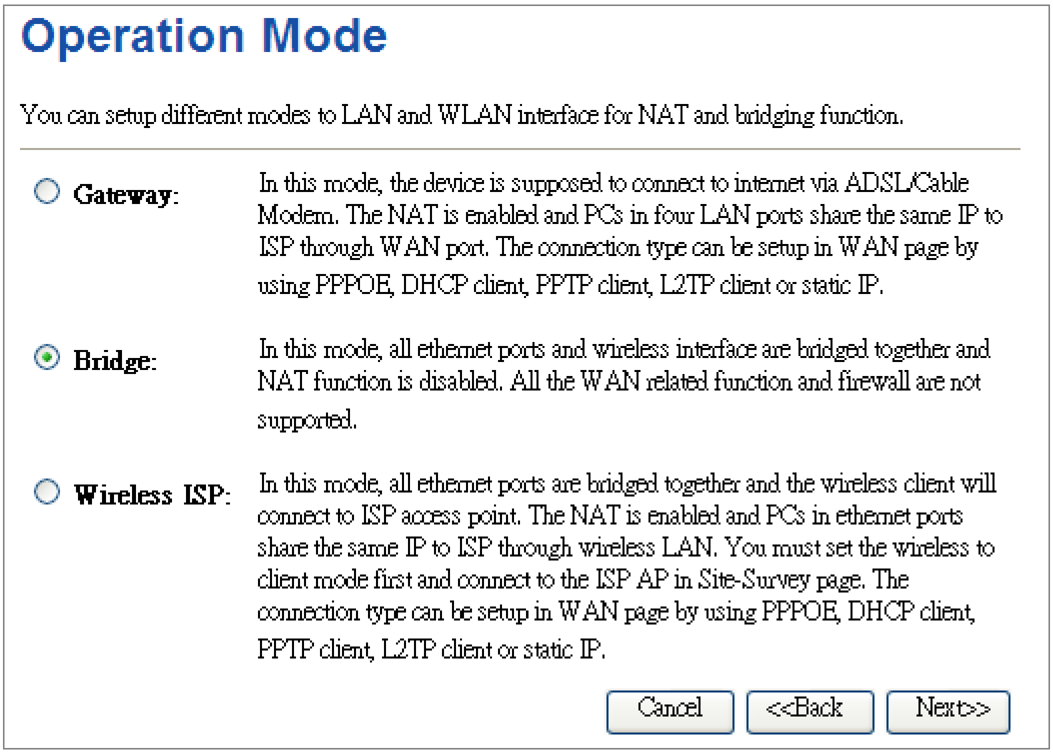
The AP supports three operation modes**, Gateway**, **Bridge** and **Wireless ISP**.







Each mode is suitable for different uses. Please choose the correct mode.



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

○ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

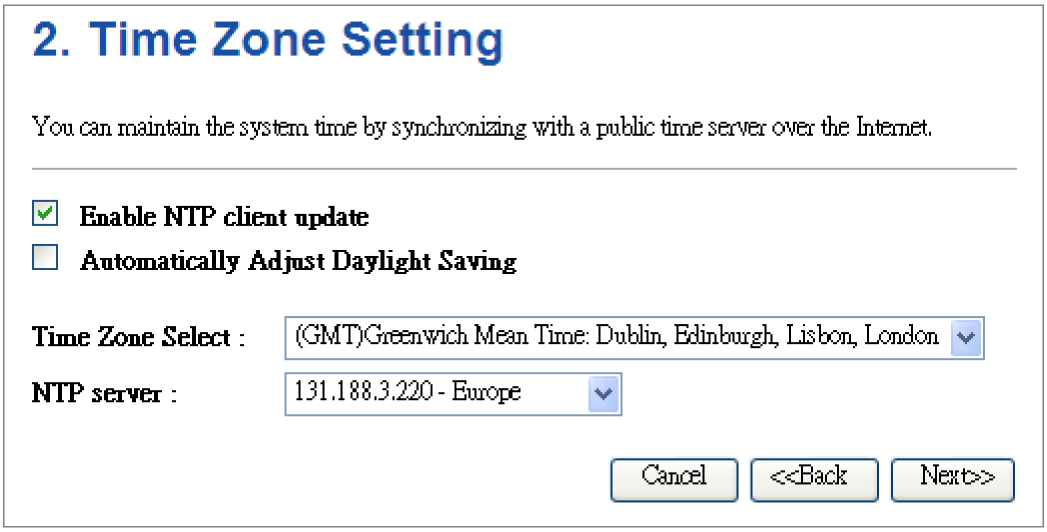
● **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Figure 5-3 Wizard –Setup Operation Mode

Step 2: Time Zone Setting

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. Daylight Saving can also be configured to automatically adjust the time when needed.



2. Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

☑ **Enable NTP client update**

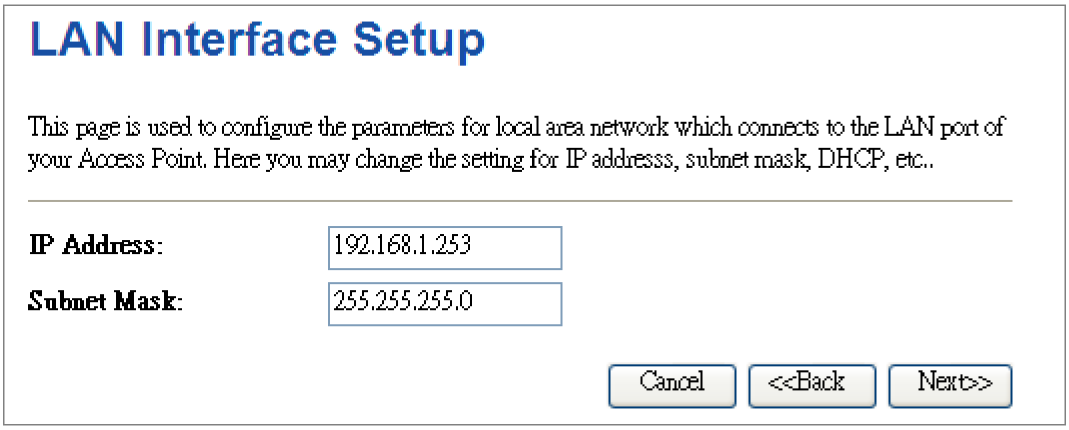
☐ **Automatically Adjust Daylight Saving**

Time Zone Select : (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

NTP server : 131.188.3.220 - Europe

Figure 5-4 Wizard – Time Zone Setup

Step 3: Setup LAN Interface



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

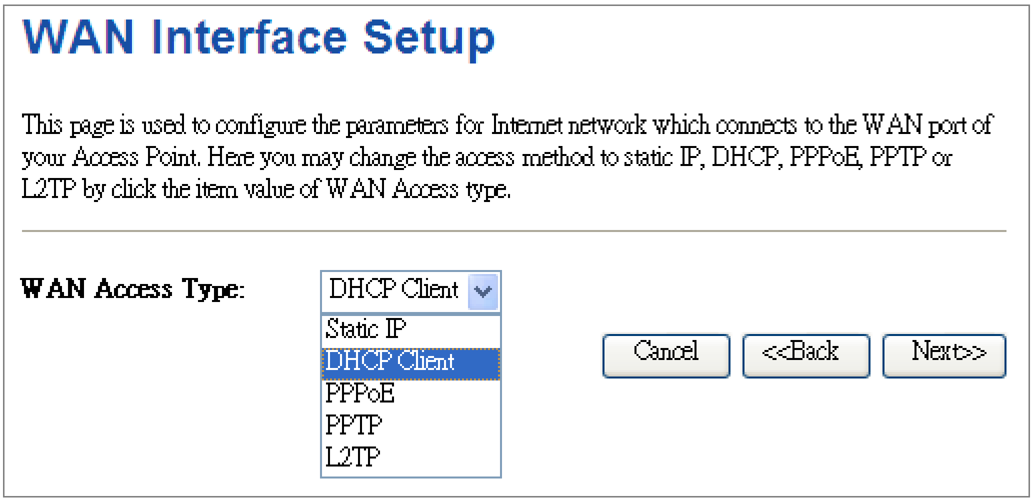
IP Address: 192.168.1.253

Subnet Mask: 255.255.255.0

Figure 5-5 Wizard – Setup LAN Interface

Step 4: Setup WAN Interface

The Wireless AP supports five access modes in the WAN side. Please choose the correct mode according to your ISP Service.



WAN Interface Setup

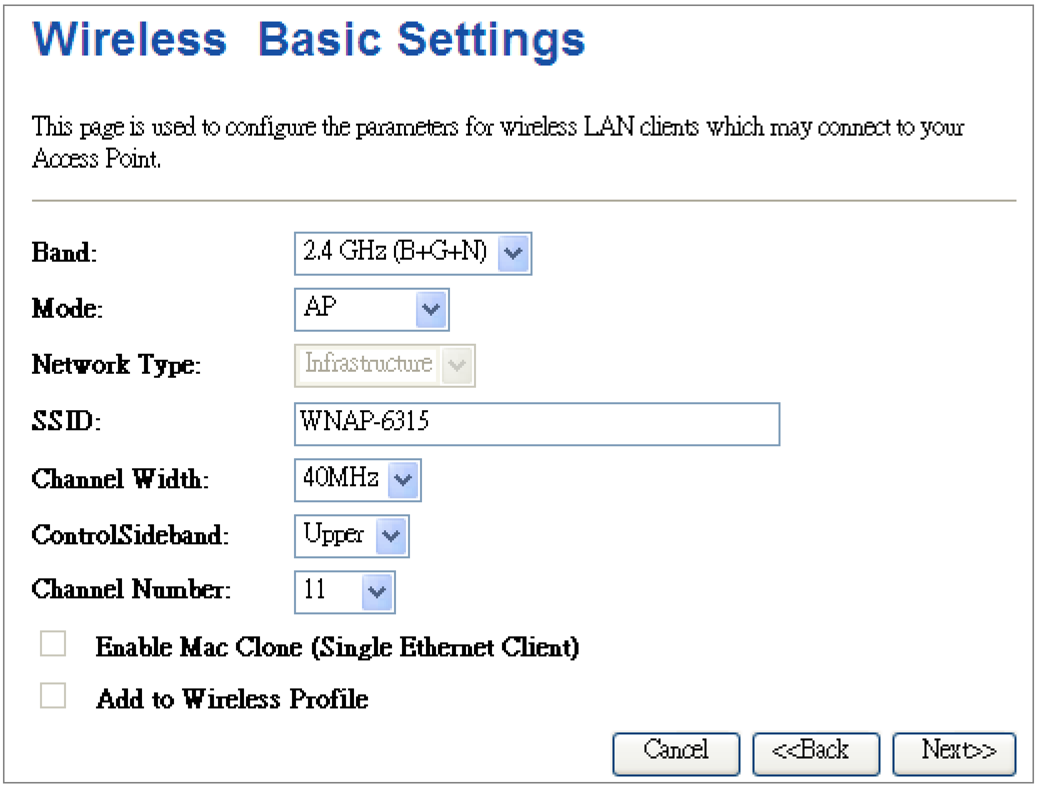
This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Figure 5-6 Wizard – WAN Interface Setup

Step 5: Wireless LAN Setting

Configure the wireless parameters according to your application. For this section you can set **AP**, **Client**, **WDS** and **AP+WDS (Repeater)** mode.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point.

Band: 2.4 GHz (B+G+N)

Mode: AP

Network Type: Infrastructure

SSID: WNAP-6315

Channel Width: 40MHz

ControlSideband: Upper

Channel Number: 11

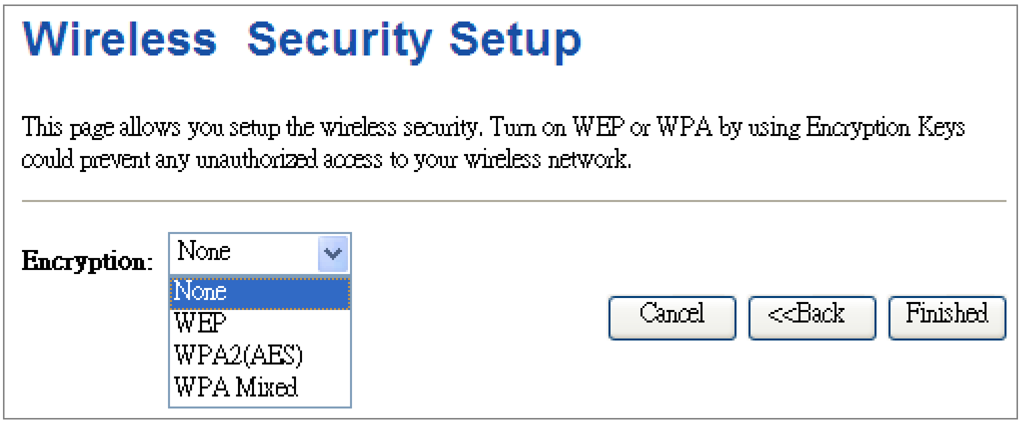
□ Enable Mac Clone (Single Ethernet Client)

□ Add to Wireless Profile

Figure 5-7 Wizard - Wireless LAN Setting

Step 6: Wireless Security Setting

Secure your wireless network by turning on the WPA or WEP security feature on the AP. For this section you can set **WEP** and **WPA-PSK** security mode.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

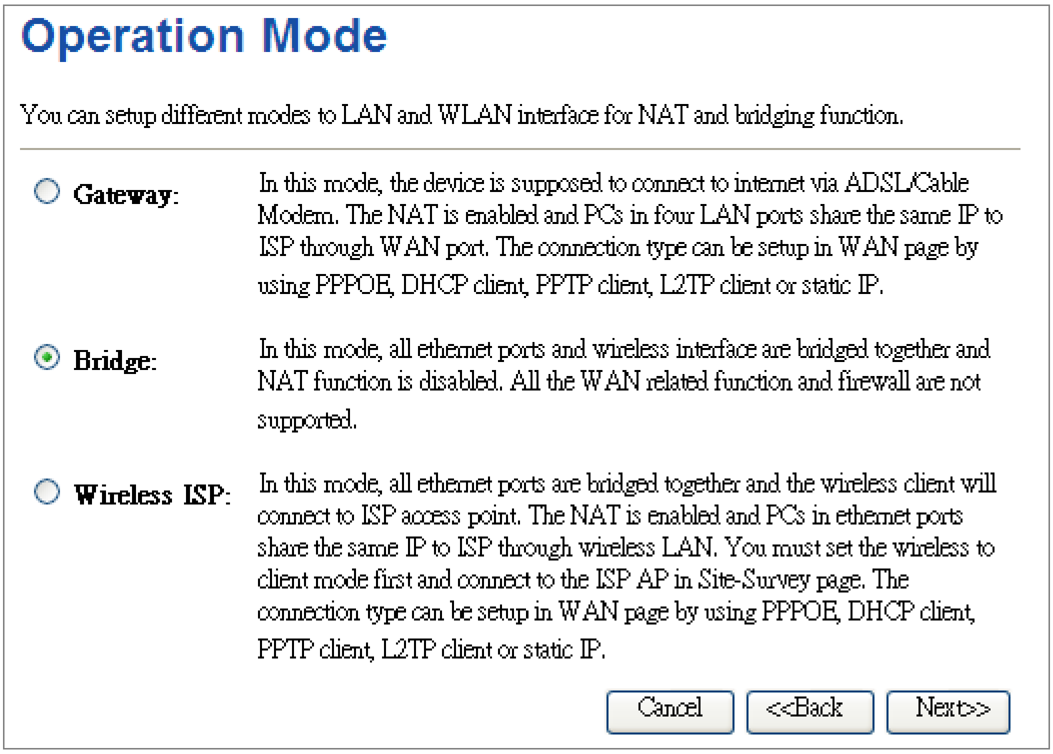
Encryption: None

Figure 5-8 Wizard - Wireless Security Setting

Click the Finished button to make your wireless configuration to take effect.

5.2 Operation Mode

This page shows the current operation mode, and users can set different modes to LAN and WLAN interface for NAT and bridging function on the WNAP-6315.



Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

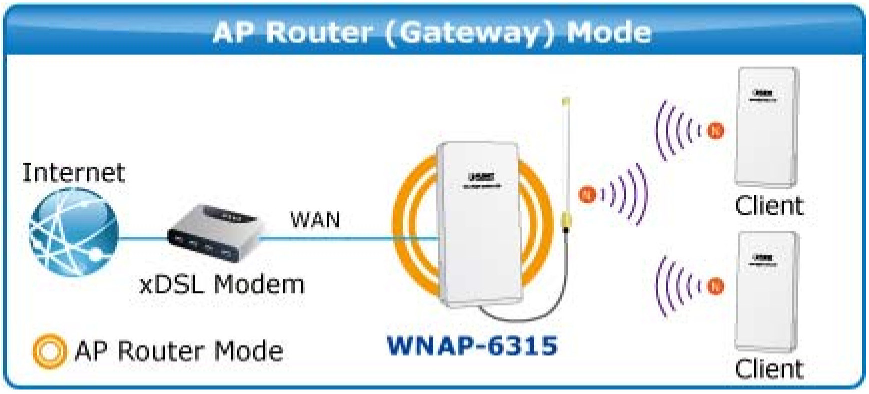
○ **Gateway:** In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in four LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

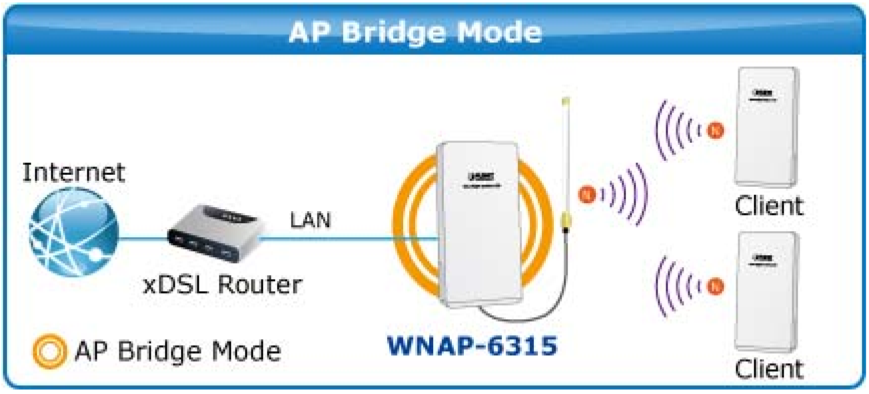
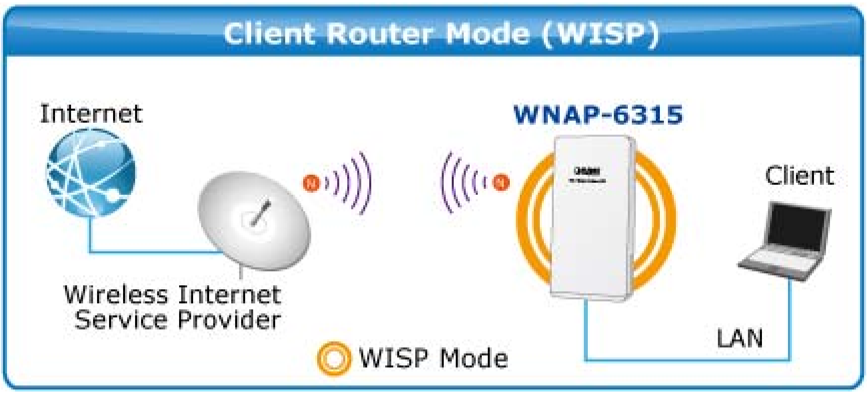
● **Bridge:** In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.

○ **Wireless ISP:** In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

Figure 5-9 Operation Mode

The page includes the following fields:

Object	Description
Gateway	In this mode, the device enables multi-user to share Internet via ADSL/Cable Modem. The wireless port shares the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.  AP Router (Gateway) Mode Internet WAN xDSL Modem AP Router Mode WNAP-6315 Client Client
Bridge	In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can't be connected easily together

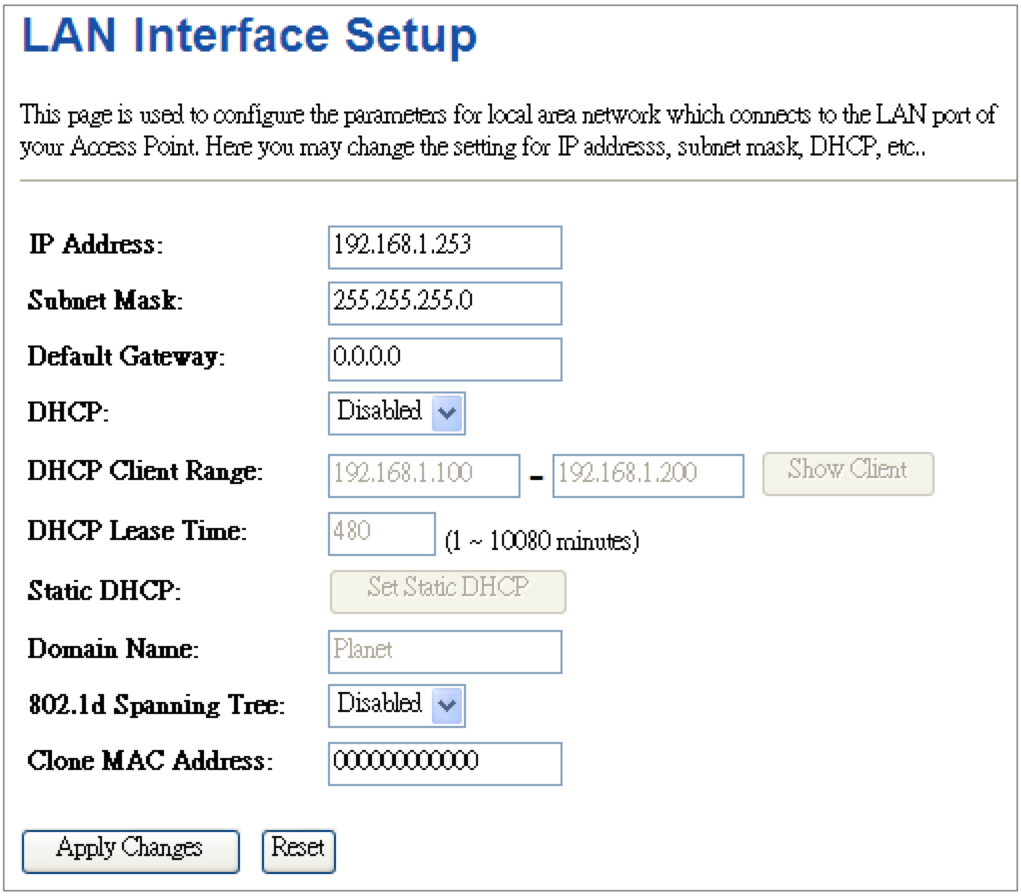
	with a cable.  AP Bridge Mode Internet LAN xDSL Router AP Bridge Mode WNAP-6315 Client Client
Wireless ISP	In this mode, the device enables multi-user to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the **Wireless port works as a WAN port** at **Client Router** mode. The Ethernet port acts as a LAN port.  Client Router Mode (WISP) Internet WNAP-6315 Client Wireless Internet Service Provider LAN WISP Mode

5.3 TCP/IP Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your AP. Here you may change the setting for IP address, subnet mask, DHCP, etc.

5.3.1 LAN Interface

On the LAN Settings page, you can configure the IP parameters of the LAN on the screen as shown below.



LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address: 192.168.1.253

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Disabled

DHCP Client Range: 192.168.1.100 - 192.168.1.200

DHCP Lease Time: 480 (1 ~ 10080 minutes)

Domain Name: Planet

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

Figure 5-10 LAN Setting

The page includes the following fields:

Object	Description
IP Address	The default LAN IP address of the WNAP-6315 is **192.168.1.253**. You can change it according to your request.
Subnet Mask	Default is **255.255.255.0**. You can change it according to your request.
Default Gateway	Default is **192.168.1.253**. You can change it according to your request.
DHCP	You can select a **Disabled**, **Client**, **and Server**. Default is **Disabled**, meaning the WNAP-6315 must connect to a router to assign IP addresses to clients.
DHCP Client Range	For the **Server** mode, you must enter the DHCP client IP address range in the field. And you can click the “**Show Client**” button to show

	the Active DHCP Client Table.
Static DHCP	Click the "**Set Static DHCP**" button and you can reserve some IP addresses for those network devices with the specified MAC addresses anytime when they request IP addresses.
Domain Name	Default is **Planet**.
802.1d Spanning Tree	You can enable or disable the Spanning Tree function.
Clone MAC Address	You can input an MAC address here for using clone function.
UPnP Enable	You can enable or disable the UPnP function. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Note

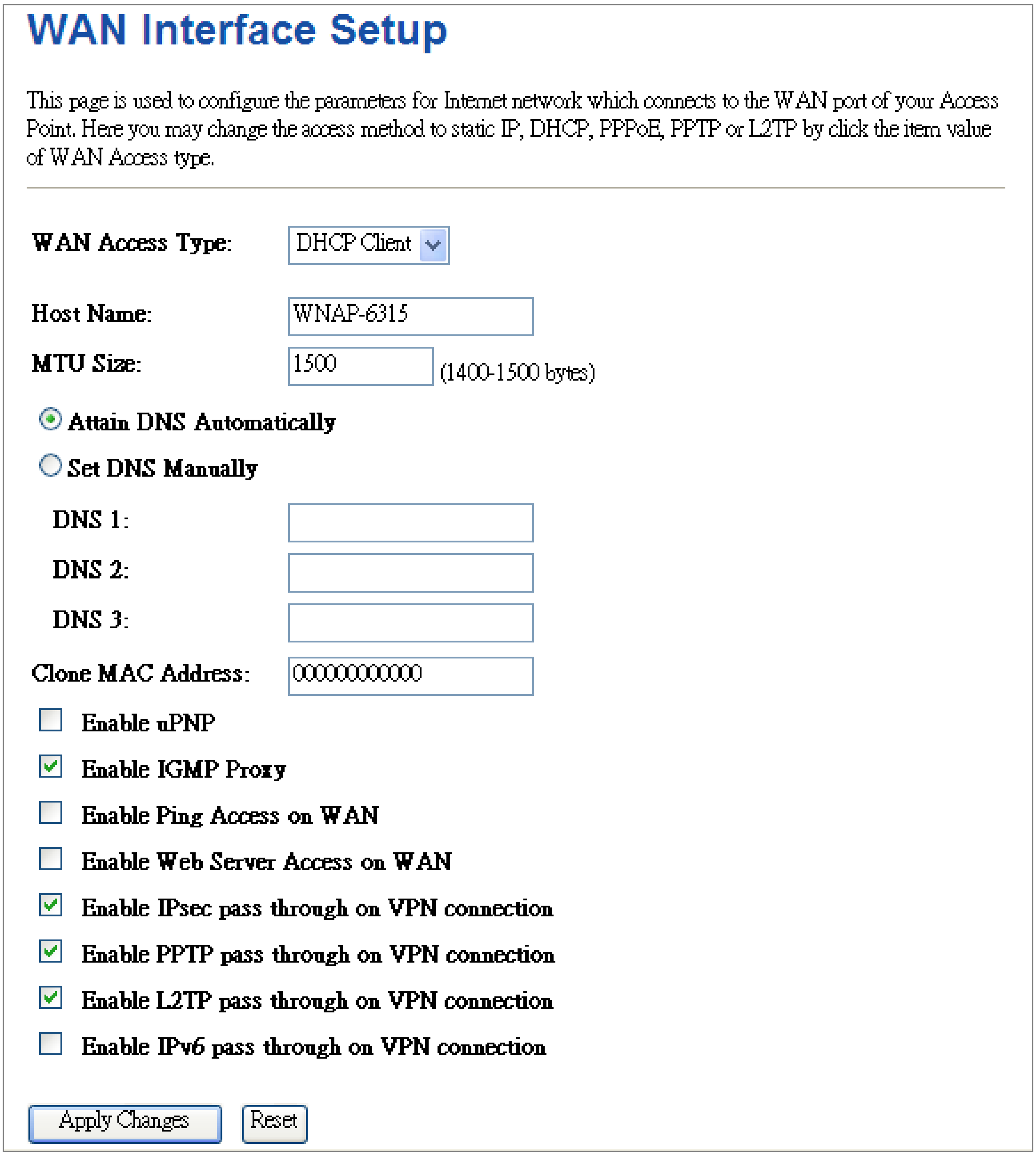
If you change the IP address of LAN, you must use the new IP address to login the AP.

Note

When the IP address of the WNAP-6315 is changed, the clients on the network often need to wait for a while or even reboot before they can access the new IP address. For an immediate access to the AP, please flush the netbios cache on the client computer by running the "**nbtstat –r**" command before using the device name of the WNAP-6315 to access its Web Management page.

5.3.2 WAN Interface

On the WAN Settings page, you can configure the IP parameters of the WAN on the screen as shown below.



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Host Name: WNAP-6315

MTU Size: 1500 (1400-1500 bytes)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable uPNP

☑ Enable IGMP Proxy

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

☑ Enable L2TP pass through on VPN connection

□ Enable IPv6 pass through on VPN connection

Figure 5-11 WAN Setting

The page includes the following fields:

Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill the correct parameters from your local ISP in the fields which appear below.	
	DHCP Client	Select DHCP Client to obtain IP Address information automatically from your ISP.
	Static IP	Select Static IP Address if all the Internet port's IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, subnet mask, gateway address, and DNS

		address provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format. **IP Address** Enter the IP address assigned by your ISP. **Subnet Mask** Enter the Subnet Mask assigned by your ISP. **Default Gateway** Enter the Gateway assigned by your ISP. **DNS** The DNS server information will be supplied by your ISP.
	PPPoE	Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. **User Name** Enter your PPPoE user name. **Password** Enter your PPPoE password.
	PPTP	Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with IP information and PPTP Server IP Address; of course, it also includes a username and password. This mode is typically used for DSL services. **IP Address** Enter the IP address. **Subnet Mask** Enter the Subnet Mask. **Server IP Address** Enter the PPTP Server IP address provided by your ISP. **User Name** Enter your PPTP user name. **Password** Enter your PPTP password.
	L2TP	Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. **IP Address** Enter the IP address. **Subnet Mask**

<table>
<tr><td></td><td></td><td>Enter the Subnet Mask.
<b>Server IP Address</b>
Enter the L2TP Server IP address provided by your ISP.
<b>User Name</b>
Enter your L2TP user name.
<b>Password</b>
Enter your L2TP password.</td></tr>
<tr><td><b>Host Name</b></td><td colspan="2">This option specifies the Host Name of the Wireless AP.</td></tr>
<tr><td><b>MTU Size</b></td><td colspan="2">The normal <b>MTU</b> (Maximum Transmission Unit) value for most Ethernet networks is 1492 Bytes. It is not recommended that you change the default <b>MTU Size</b> unless required by your ISP.</td></tr>
<tr><td><b>Attain DNS Automatically</b></td><td colspan="2">Select “<b>Attain DNS Automatically</b>”, the DNS servers will be assigned dynamically from your ISP.</td></tr>
<tr><td><b>Set DNS Manually</b></td><td colspan="2">If your ISP gives you one or two DNS addresses, select <b>Set DNS Manually</b> and enter the primary and secondary addresses into the correct fields.</td></tr>
<tr><td><b>Clone MAC Address</b></td><td colspan="2">You can input a MAC address here for using clone function.</td></tr>
<tr><td><b>Enable uPNP</b></td><td colspan="2">Check to disable/enable uPNP function (default = disabled)</td></tr>
<tr><td><b>Enable IGMP Proxy</b></td><td colspan="2">Check to disable/enable IGMP function (default = enabled)</td></tr>
<tr><td><b>Enable Ping Access on WAN</b></td><td colspan="2">Check to enable the Ping Access on WAN function (default = disabled)</td></tr>
<tr><td><b>Enable Web Server Access on WAN</b></td><td colspan="2">Check to enable the Web Server Access on WAN function (default = disabled)</td></tr>
<tr><td><b>Enable IPsec pass through on VPN connection</b></td><td colspan="2">Check to enable the IPsec pass through on VPN connection function (default = enabled)</td></tr>
<tr><td><b>Enable PPTP pass through on VPN connection</b></td><td colspan="2">Check to enable the PPTP pass through on VPN connection function (default = enabled)</td></tr>
<tr><td><b>Enable L2TP pass through on VPN connection</b></td><td colspan="2">Check to enable the L2TP pass through on VPN connection function (default = enabled)</td></tr>
<tr><td><b>Enable IPv6 pass through on VPN connection</b></td><td colspan="2">Check to enable the IPv6 pass through on VPN connection function (default = disabled)</td></tr>
</table>

Note

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Note

WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the router will not work properly. In case of emergency, press the hardware "Reset" button.

5.4 Wireless

The wireless menu contains submenus of the settings about wireless network. Please refer to the following sections for the details.

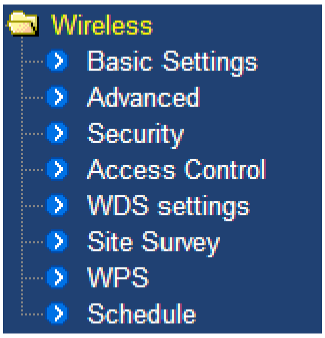


Figure 5-12 Wireless – Main Menu

5.4.1 Basic Settings

Choose menu “**Wireless → Basic Settings**” and you can configure the wireless basic settings for the wireless network on this page. After the configuration is done, please click the “**Apply Changes**” button to save the settings.

First of all, the wireless AP supports multiple wireless modes for different network applications, which include:

- **AP**
- **Multiple SSIDs**
- **Universal Repeater**
- **Client**
- **WDS**
- **AP+WDS**

It is so easy to combine the WNAP-6315 with the existing wired network. The WNAP-6315 definitely provides a total network solution for the home and the SOHO users.

- **AP**

  Standard **Access Point**

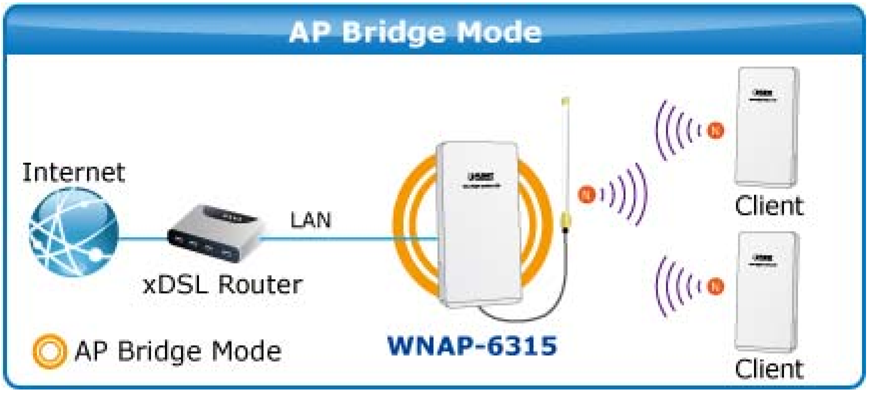
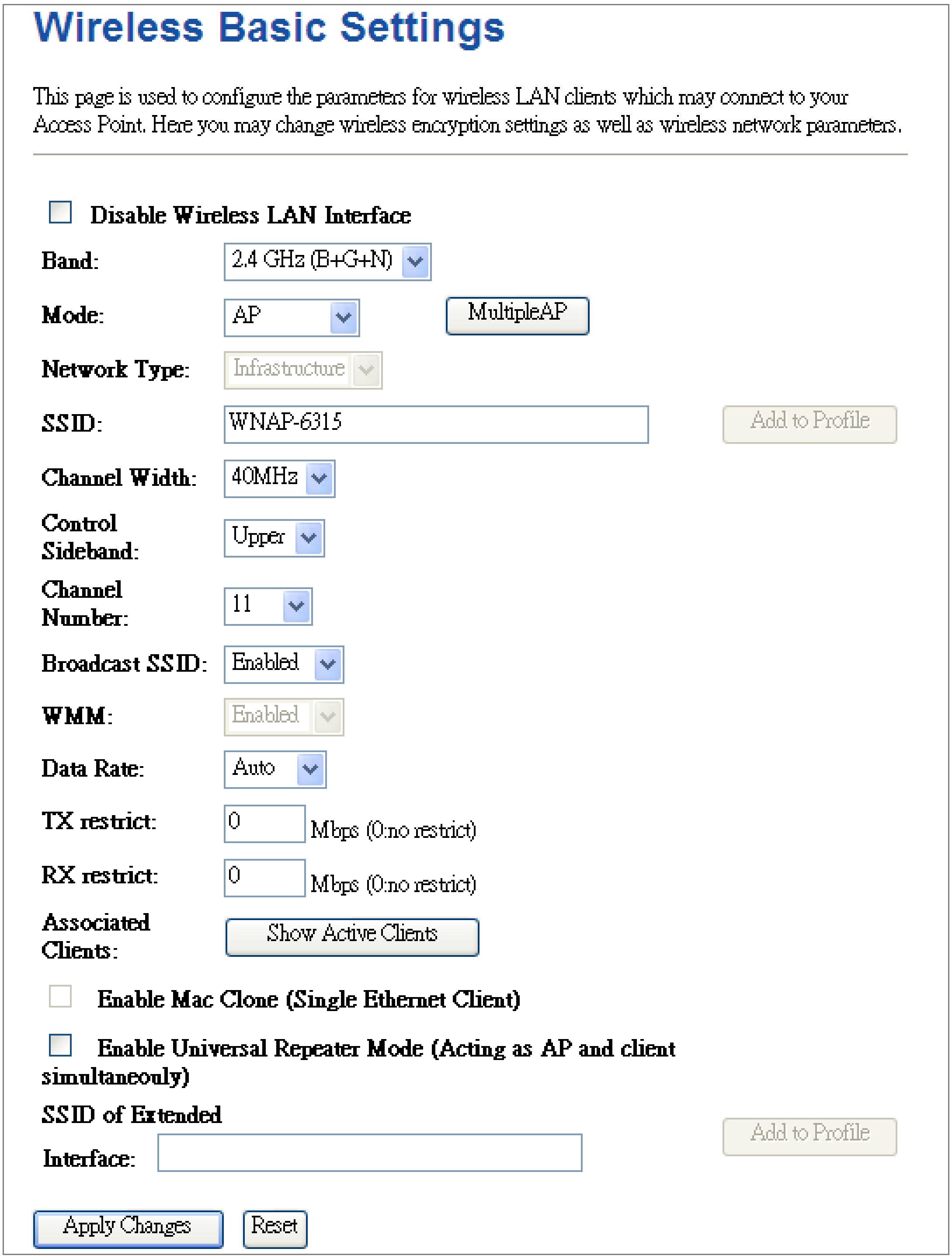


Figure 5-13 Topology – AP Bridge Mode



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP MultipleAP

Network Type: Infrastructure

SSID: WNAP-6315 Add to Profile

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

TX restrict: 0 Mbps (0:no restrict)

RX restrict: 0 Mbps (0:no restrict)

Associated Clients: Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface: Add to Profile

Apply Changes Reset

Figure 5-14 Wireless Basic Settings of AP

The page includes the following fields:

Object	Description
Disable Wireless LAN Interface	Check the box to disable the wireless function.
Band	Select the desired mode. Default is “**2.4GHz (B+G+N)**”. It is strongly recommended that you set the Band to “2.4GHz (B+G+N)”, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the WNAP-6315.

	■ **2.4 GHz (B)**: 802.11b mode, rate is up to 11Mbps ■ **2.4 GHz (G)**: 802.11g mode, rate is up to 54Mbps ■ **2.4 GHz (N)**: 802.11n mode, rate is up to 150Mbps(1T1R) ■ **2.4 GHz (B+G)**: 802.11b/g mode, rate is up to 11Mbps or 54Mbps ■ **2.4 GHz (G+N)**: 802.11g/n mode, rate is up to 54Mbps or 150Mbps ■ **2.4 GHz (B+G+N)**: 802.11b/g/n mode, rate is up to 11Mbps, 54Mbps, or 150Mbps
Mode	There are four kinds of wireless mode selections: ■ **AP** ■ **Client** ■ **WDS** ■ **AP+WDS** If you select WDS or AP+WDS, please click "**WDS Settings**" submenu for the related configuration. Furthermore, click the "**Multiple AP"** button to enable multiple SSID function.
SSID	The ID of the wireless network. User can access the wireless network via the ID only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with. Default: **WNAP-6315**
Channel Width	You can select **20MHz**, or **40MHz**.
Channel Number	You can select the operating frequency of wireless network. Default: **11**
Broadcast SSID	If you enable "Broadcast SSID", every wireless station located within the coverage of the AP can discover its signal easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling "Broadcast SSID" can provide better wireless network security. Default is "**Enabled**".
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.** Default is "**Auto"**.
Associated Clients	Click the "**Show Active Clients**" button to show the status table of active wireless clients.
Enable Universal Repeater Mode **(Acting as AP and client simultaneously)**	Universal Repeater is a technology used to extend wireless coverage. To enable Universal Repeater mode, check the box and enter the SSID you want to broadcast in the field below. Then please click "Security" submenu for the related settings of the AP you want to connect with.

Multiple-SSID

Enable multiple-SSID can broadcast multiple WLAN SSID's using virtual interfaces. You can have different encryption settings for each WLAN and you can restrict what they have access to.

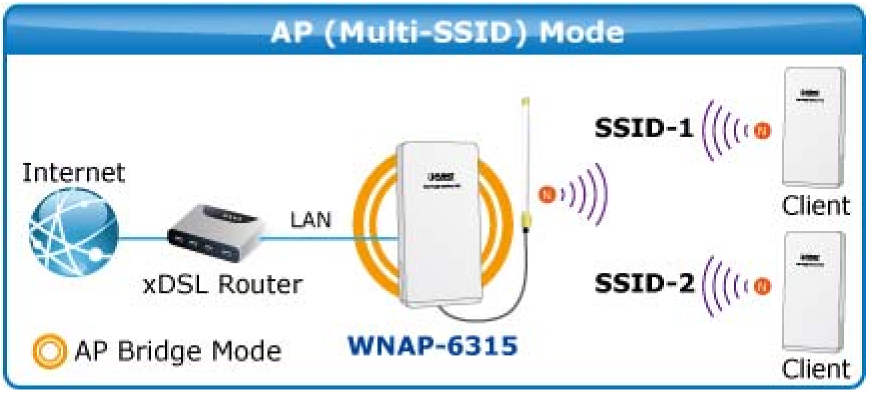
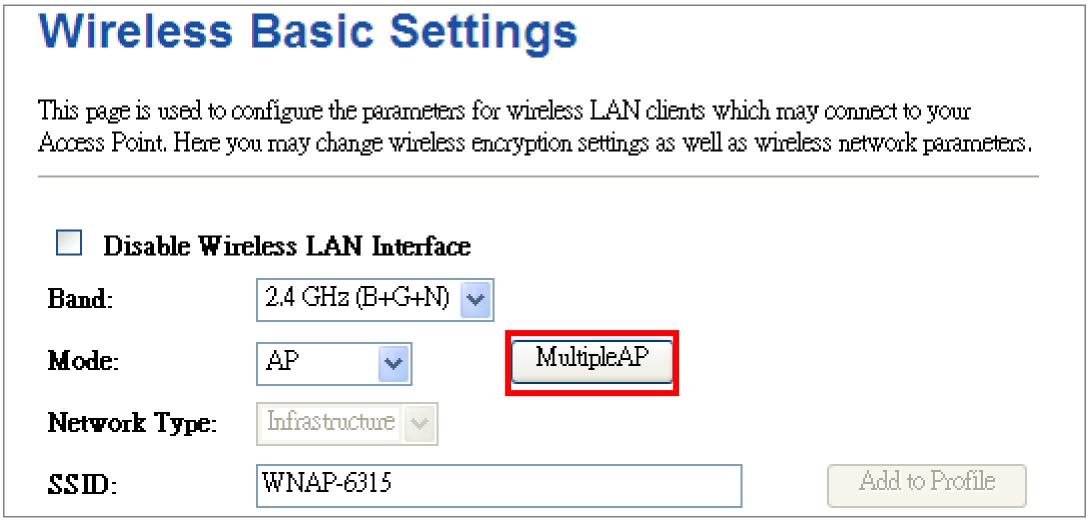


Figure 5-15 Topology – Multiple-SSID Mode

Choose menu "**Wireless** → **Basic Settings** → **Multiple AP**" to configure the device as a general wireless access point with multiple SSIDs.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

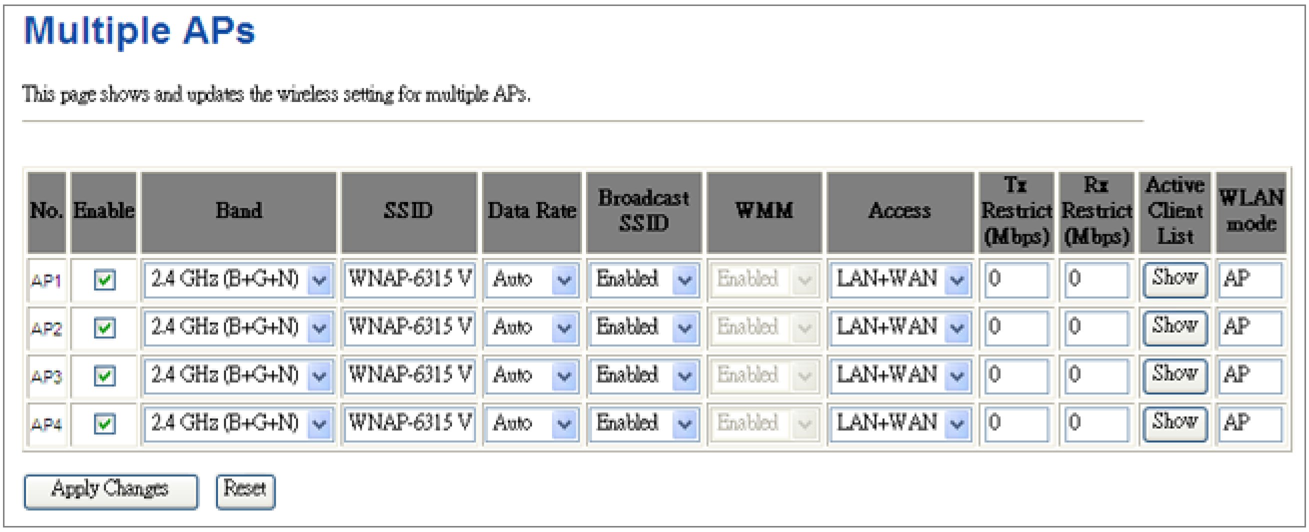
Mode: AP

Network Type: Infrastructure

SSID: WNAP-6315

Figure 5-16 Wireless Basic Settings – Multiple AP

The device supports up to four multiple Service Set Identifiers. You can back to the **Basic Settings** page to set the Primary SSID. The SSID's factory default setting is **WNAP-6315 VAP1~4 (Multiple-SSID 1~4)**. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. When the information for the new SSID is finished, click the **Apply Changes** button to let your changes take effect.



Multiple APs

This page shows and updates the wireless setting for multiple APs.

No.	Enable	Band	SSID	Data Rate	Broadcast SSID	WMM	Access	Tx Restrict (Mbps)	Rx Restrict (Mbps)	Active Client List	WLAN mode
AP1	☑	2.4 GHz (B+G+N)	WNAP-6315 V	Auto	Enabled	Enabled	LAN+WAN	0	0	Show	AP
AP2	☑	2.4 GHz (B+G+N)	WNAP-6315 V	Auto	Enabled	Enabled	LAN+WAN	0	0	Show	AP
AP3	☑	2.4 GHz (B+G+N)	WNAP-6315 V	Auto	Enabled	Enabled	LAN+WAN	0	0	Show	AP
AP4	☑	2.4 GHz (B+G+N)	WNAP-6315 V	Auto	Enabled	Enabled	LAN+WAN	0	0	Show	AP

Figure 5-17 Multiple-SSID

Once you have applied and saved those settings, you can then go to the "**Wireless** → **Security**" page on the AP to set up security settings for each of the SSIDs.

- **Universal Repeater**

This mode allows the AP with its own BSS to relay data to a root AP to which it is associated with WDS disabled. The wireless repeater relays signal between its stations and the root AP for greater wireless range.

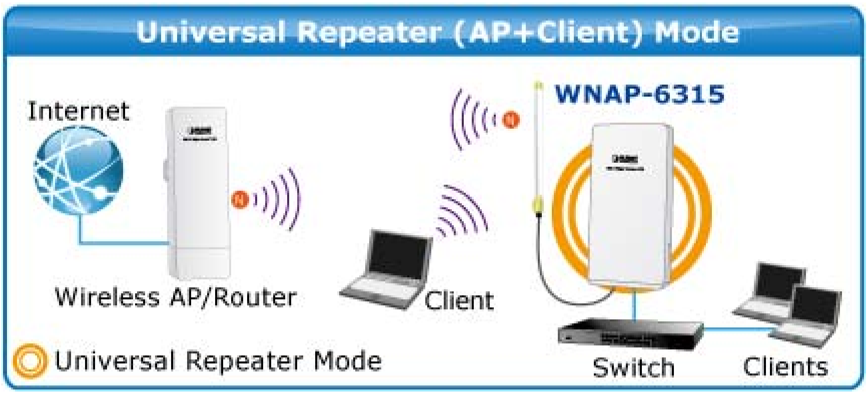
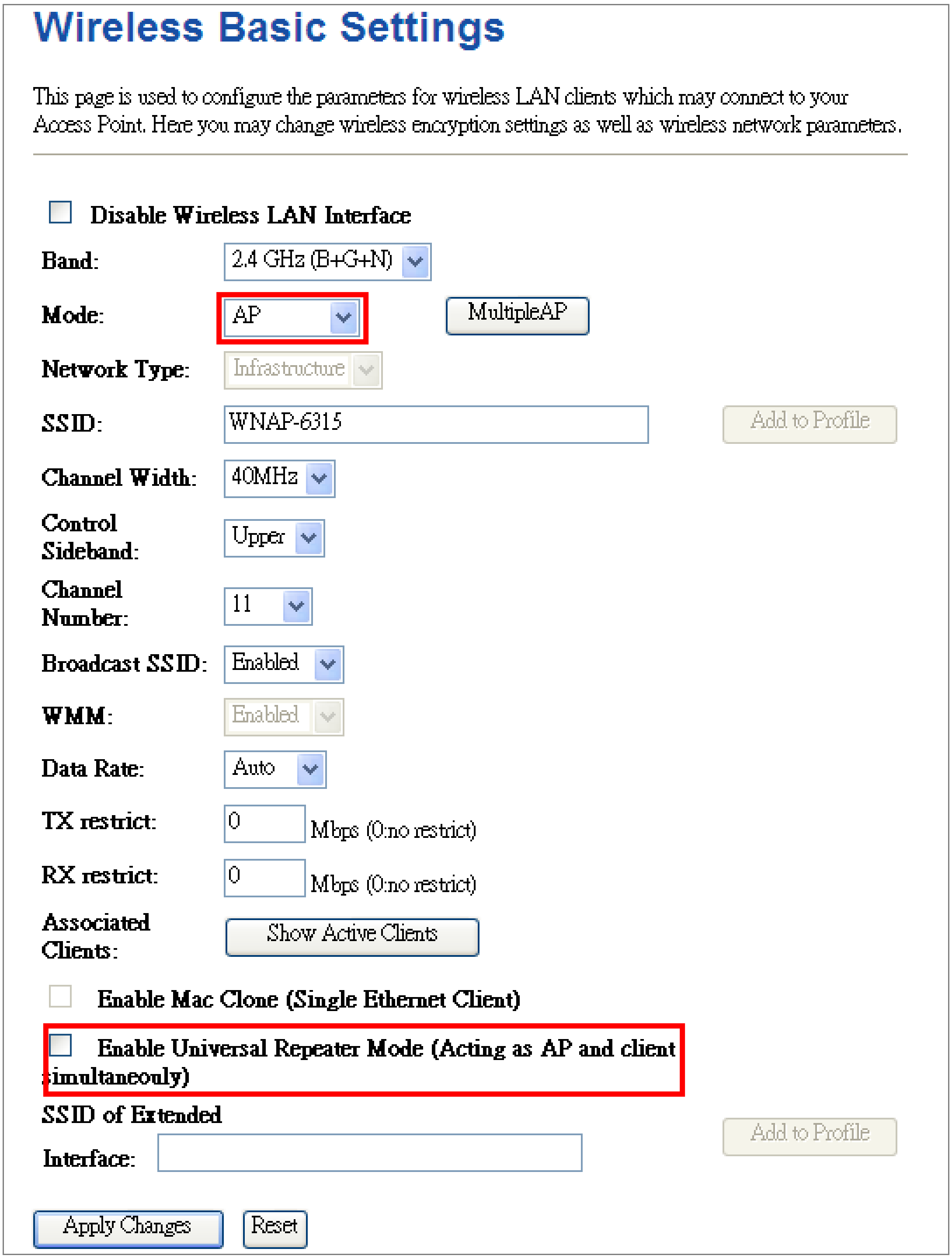


Figure 5-18 Topology – Universal Repeater Mode

1. Example of how to configure **Universal Repeater Mode**. Please take the following steps:

To configure each wireless parameter, please go to the "**Wireless→ Basic Settings**" page.

Step 1. Configure wireless mode to "**AP**" and then check "**Enable Universal Repeater Mode (Acting as AP and client simultaneously)**". Click "**Apply Changes**" to take effect.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ **Disable Wireless LAN Interface**

Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	WNAP-6315
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
TX restrict:	0 Mbps (0:no restrict)
RX restrict:	0 Mbps (0:no restrict)

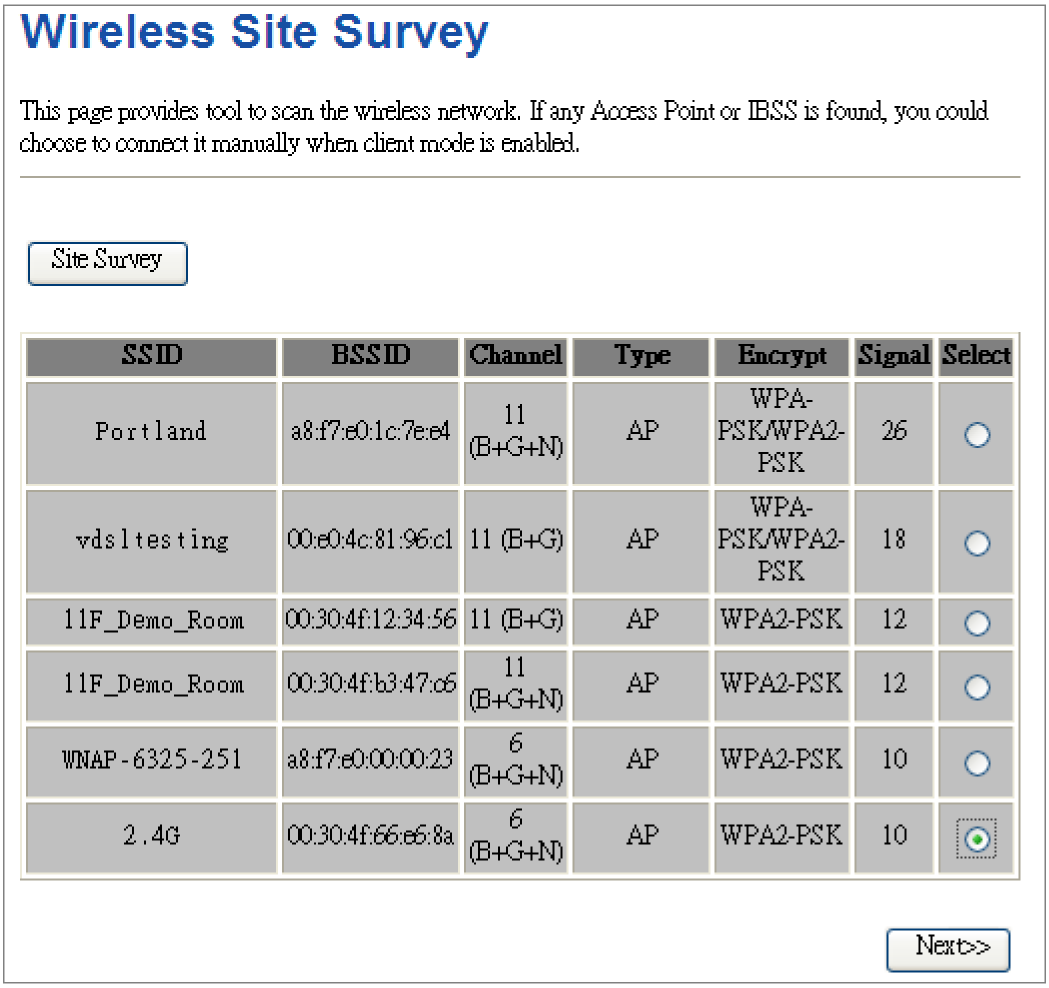
□ **Enable Mac Clone (Single Ethernet Client)**

□ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

SSID of Extended Interface:

Figure 5-19 Universal Repeater-1

Step 2. Go to **Site Survey** page to find the root AP. Select the root AP that you want to repeat the signal and then click "**Next**".



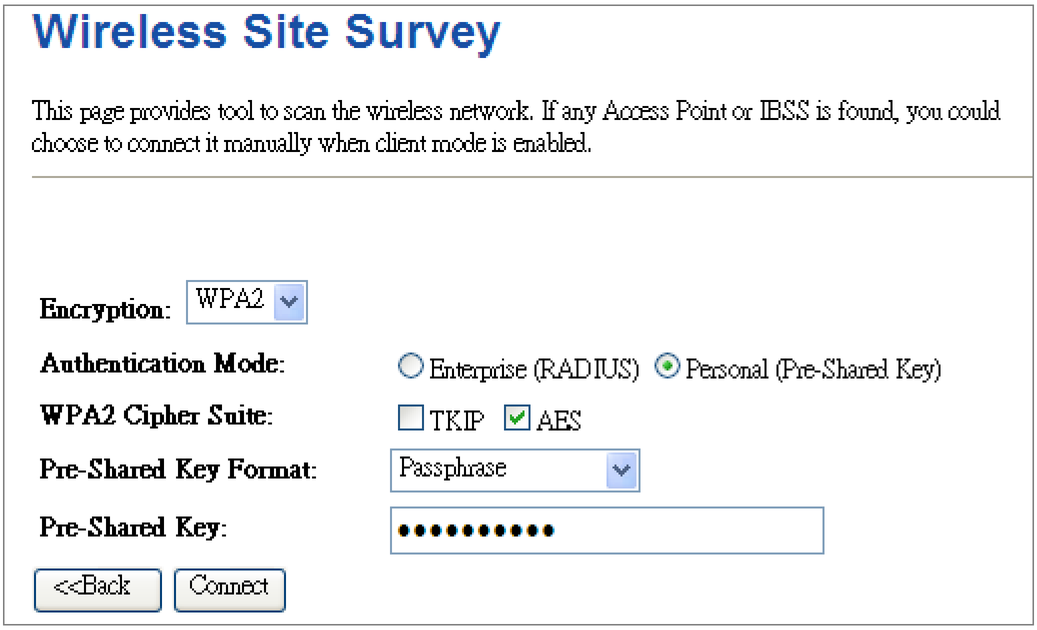
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Portland	a8:f7:e0:1c:7e:e4	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	26	○
vdsltesting	00:e0:4c:81:96:c1	11 (B+G)	AP	WPA-PSK/WPA2-PSK	18	○
11F_Demo_Room	00:30:4f:12:34:56	11 (B+G)	AP	WPA2-PSK	12	○
11F_Demo_Room	00:30:4f:b3:47:c6	11 (B+G+N)	AP	WPA2-PSK	12	○
WNAP-6325-251	a8:f7:e0:00:00:23	6 (B+G+N)	AP	WPA2-PSK	10	○
2.4G	00:30:4f:66:e6:8a	6 (B+G+N)	AP	WPA2-PSK	10	●

Figure 5-20 Universal Repeater-2

Step 3. Select the correct encryption method and enter the security key. Then, click "**Connect**".



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Encryption: WPA2

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

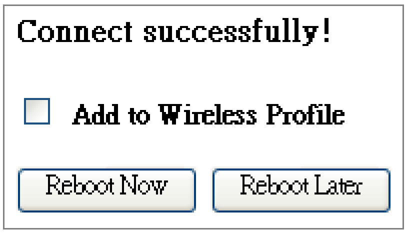
WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ●●●●●●●●●●●

Figure 5-21 Universal Repeater-3

Step 4. Check "**Add to Wireless Profile**" and click "**Reboot Now**".

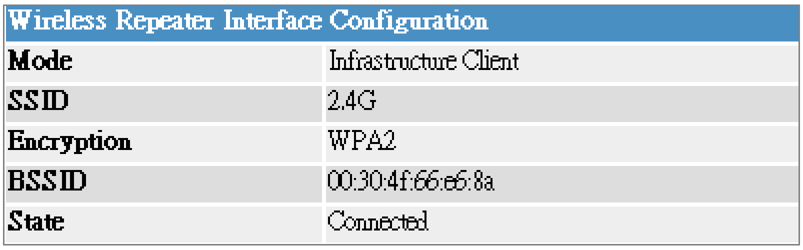


Connect successfully!

□ Add to Wireless Profile

Figure 5-22 Universal Repeater-4

Step 5. Go to "**Management-> Status**" page to check whether the state of Repeater interface should be "**Connected**".



Wireless Repeater Interface Configuration	
Mode	Infrastructure Client
SSID	2.4G
Encryption	WPA2
BSSID	00:30:4f:66:e6:8a
State	Connected

Figure 5-23 Universal Repeater-5

■ Client (Infrastructure)

Combine the Wireless AP to the Ethernet devices such as IP camera to make it be wireless station.

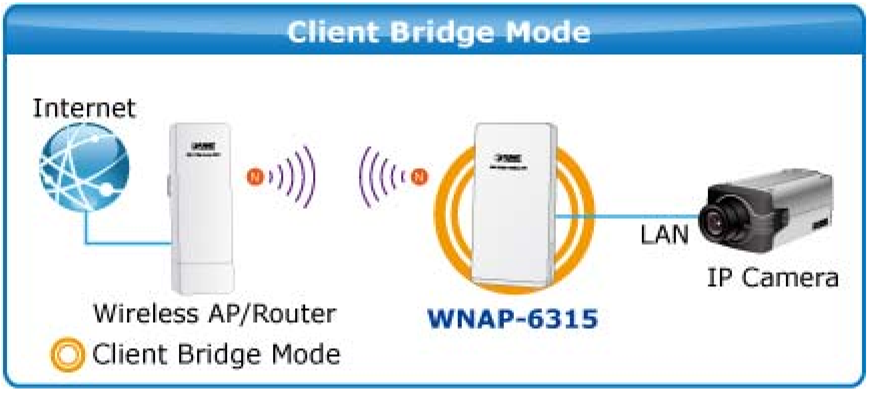
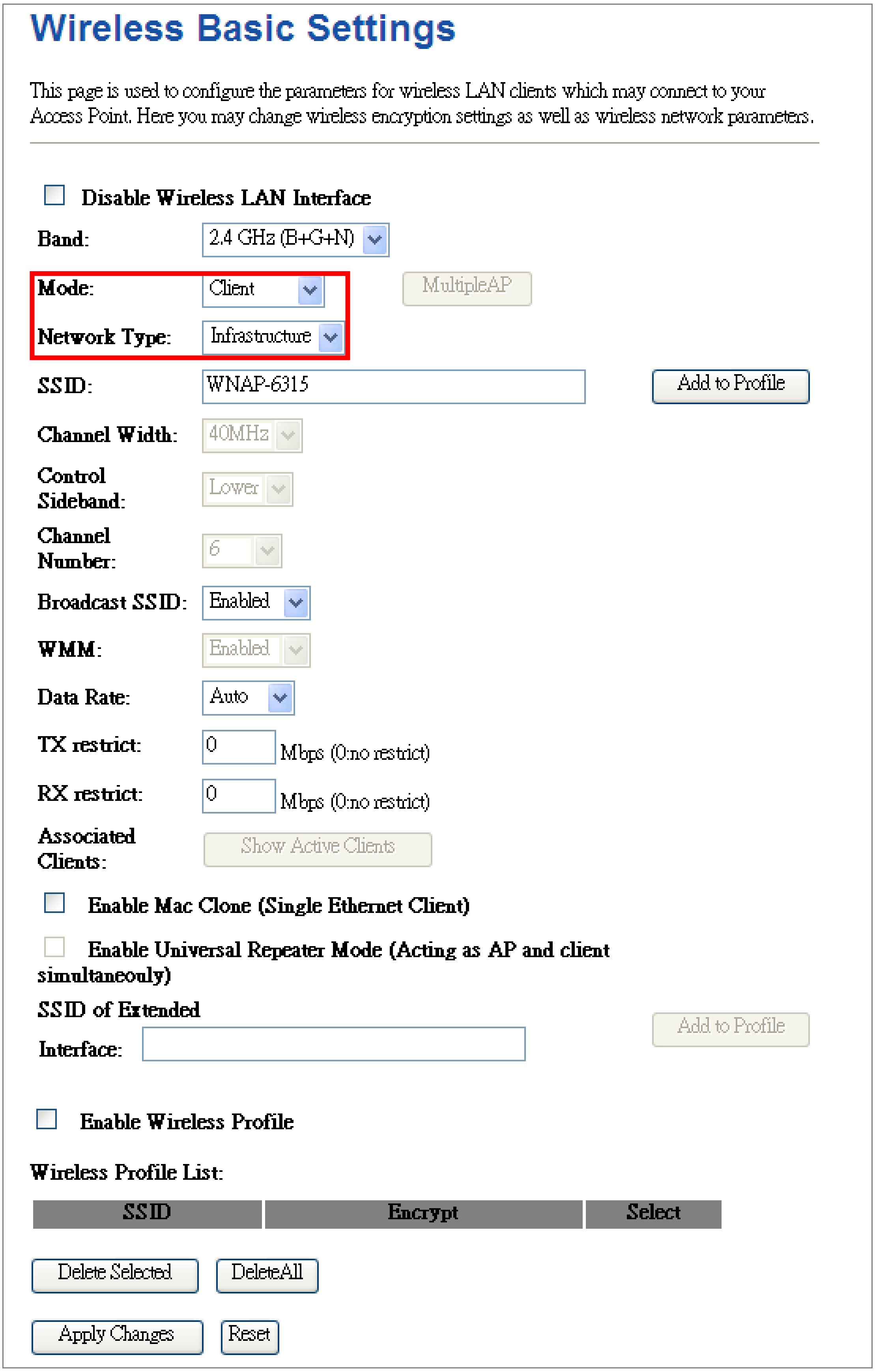


Figure 5-24 Topology – Client Mode



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: Client

Network Type: Infrastructure

SSID: WNAP-6315

Channel Width: 40MHz

Control Sideband: Lower

Channel Number: 6

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

TX restrict: 0 Mbps (0:no restrict)

RX restrict: 0 Mbps (0:no restrict)

Associated Clients:

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

□ Enable Wireless Profile

Wireless Profile List:

SSID	Encrypt	Select

Figure 5-25 Wireless Basic Settings – Client

The page includes the following fields:

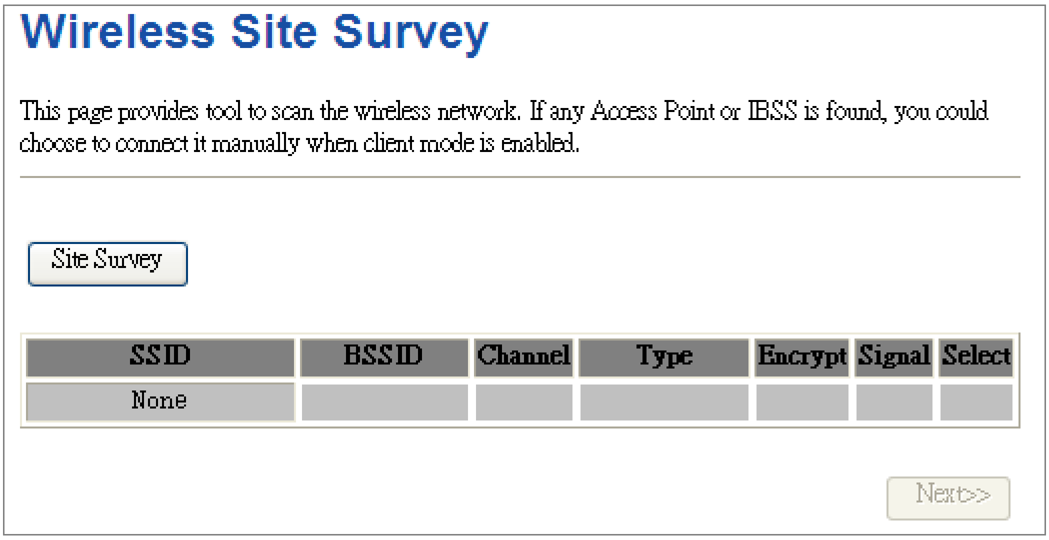
Object	Description
Disable Wireless LAN Interface	Check the box to disable the wireless function.
Band	Select the desired mode. Default is "**2.4GHz (B+G+N)**". It is strongly recommended that you set the Band to "2.4GHz (B+G+N)", and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the WNAP-6315. ■ **2.4 GHz (B)**: 802.11b mode, rate is up to 11Mbps ■ **2.4 GHz (G)**: 802.11g mode, rate is up to 54Mbps ■ **2.4 GHz (N)**: 802.11n mode, rate is up to 150Mbps(1T1R) ■ **2.4 GHz (B+G)**: 802.11b/g mode, rate is up to 11Mbps or 54Mbps ■ **2.4 GHz (G+N)**: 802.11g/n mode, rate is up to 54Mbps or 150Mbps ■ **2.4 GHz (B+G+N)**: 802.11b/g/n mode, rate is up to 11Mbps, 54Mbps, or 150Mbps
Mode	There are four kinds of wireless mode selections: ■ **AP** ■ **Client** ■ **WDS** ■ **AP+WDS** If you select WDS or AP+WDS, please click "**WDS Settings**" submenu for the related configuration. Furthermore, click the "**Multiple AP"** button to enable multiple SSID function.
Network Type	In **Infrastructure**, the wireless LAN serves as a wireless station. And the user can use the PC equipped with the WNAP-6315 to access the wireless network via other access points. In **Ad hoc**, the wireless LAN will use the Ad-hoc mode to operate. Default is "**Infrastructure**". Note: only while the wireless mode is set to "**Client**", then the **Network Type** can be configured.
SSID	The ID of the wireless network. User can access the wireless network via the ID only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with. Default: **WNAP-6315**
Broadcast SSID	If you enable "Broadcast SSID", every wireless station located within the coverage of the WNAP-6315 can discover its signal easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling "Broadcast SSID" can provide better wireless network security.

	Default is “**Enabled**”.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it’s not necessary to change this value unless you know what will happen after modification.** Default is “**Auto”**.
Enable Mac Clone (Single Ethernet Client)	Enable Mac Clone.

- Example of how to configure **Client Mode**. Please take the following steps:

To configure each wireless parameter, please go to the “**Wireless** → **Basic Settings**” page.

Step 1. Go to “**Wireless** → **Site Survey**” page and click “**Site Survey**” button.



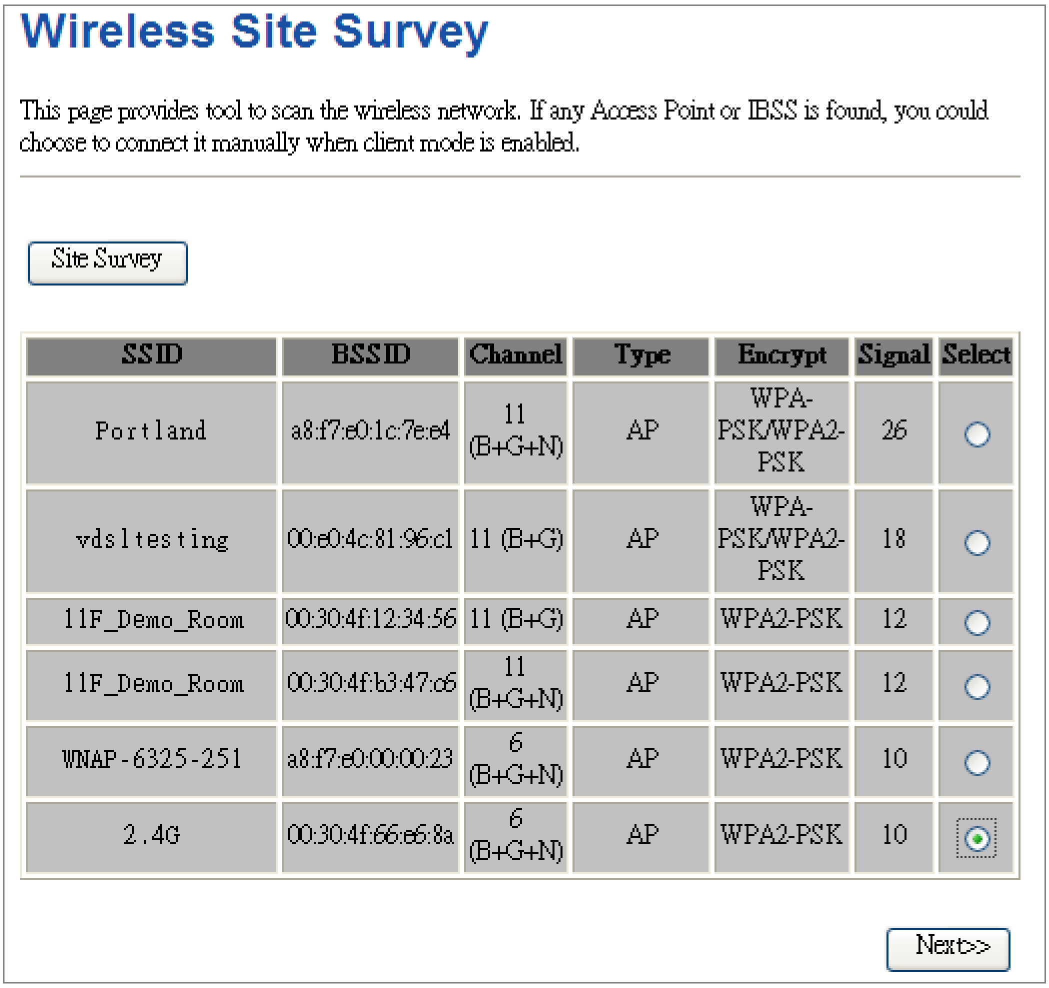
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
None						

Figure 5-26 Client – Survey

Step 2. Choose the root AP from the list. If the root AP is not listed in the table, re-click "**Site Survey**" to update the list.



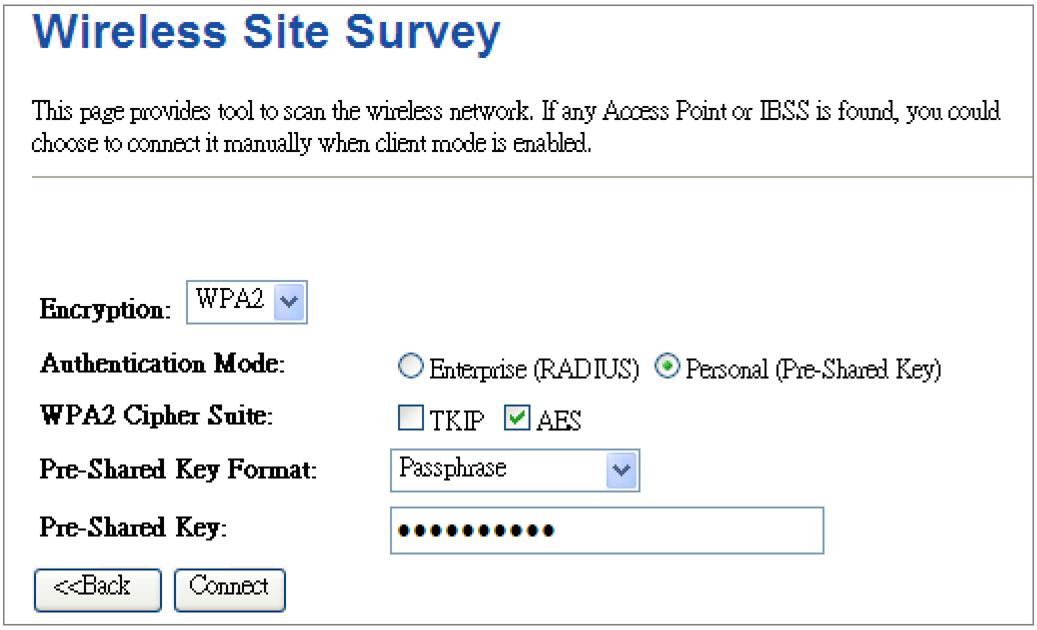
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Portland	a8:f7:e0:1c:7e:e4	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	26	○
vdsltesting	00:e0:4c:81:96:c1	11 (B+G)	AP	WPA-PSK/WPA2-PSK	18	○
11F_Demo_Room	00:30:4f:12:34:56	11 (B+G)	AP	WPA2-PSK	12	○
11F_Demo_Room	00:30:4f:b3:47:c6	11 (B+G+N)	AP	WPA2-PSK	12	○
WNAP-6325-251	a8:f7:e0:00:00:23	6 (B+G+N)	AP	WPA2-PSK	10	○
2.4G	00:30:4f:66:e6:8a	6 (B+G+N)	AP	WPA2-PSK	10	●

Figure 5-27 Client – AP List

Step 3. Enter the Security Key of the root AP and then click "**Connect**".



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Encryption: WPA2

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

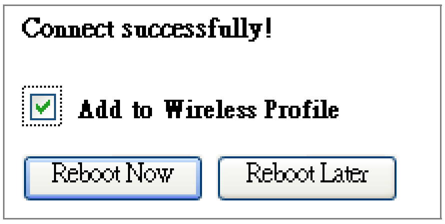
WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ●●●●●●●●●●●

Figure 5-28 Client – Security

Step 4. Wait until the connection established. Check the "**Add to Wireless Profile**" option and then reboot it.



Connect successfully!

☑ **Add to Wireless Profile**

Figure 5-29 Client – Status

- **WDS**

Connect this Wireless AP with up to 8 WDS-capable wireless APs to expand the scope of network.

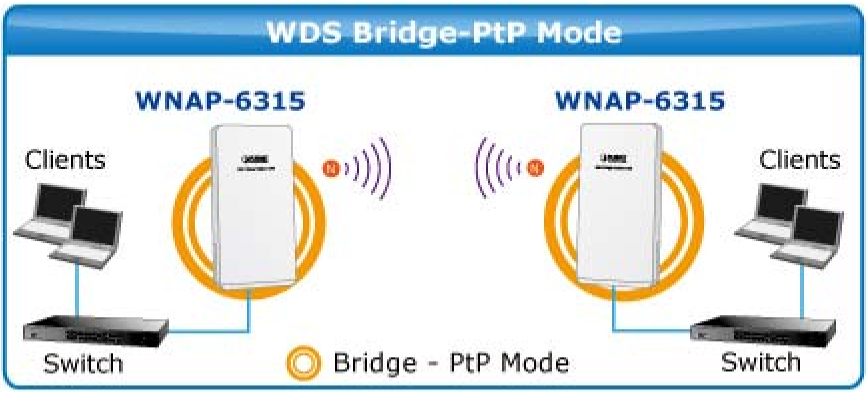


Figure 5-30 Topology – WDS PtP Mode

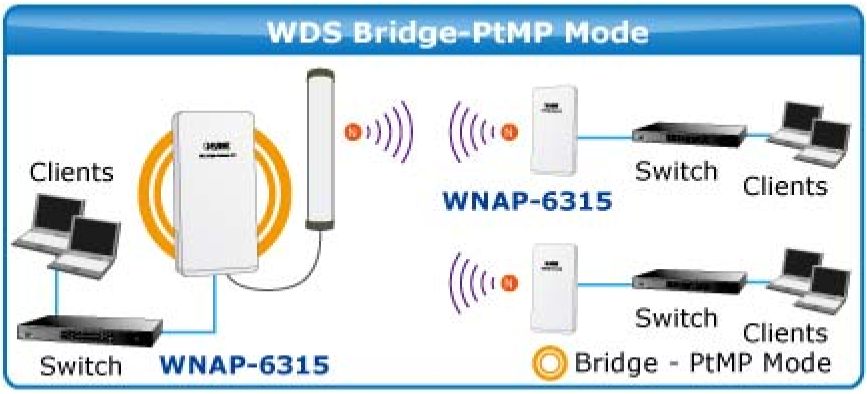
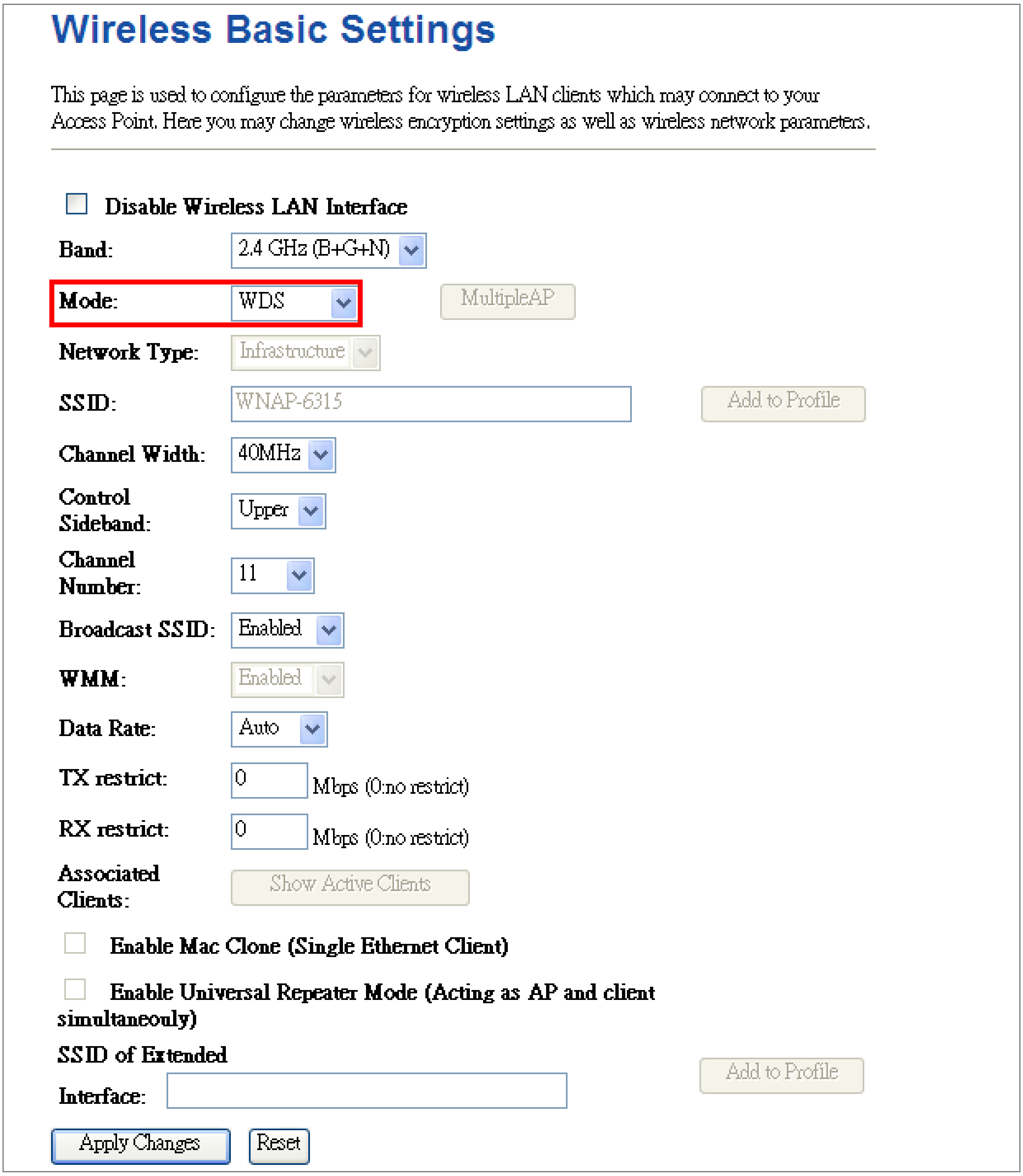


Figure 5-31 Topology – WDS PtMP Mode



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: WDS

Network Type: Infrastructure

SSID: WNAP-6315

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

TX restrict: 0 Mbps (0:no restrict)

RX restrict: 0 Mbps (0:no restrict)

Associated Clients:

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Figure 5-32 Wireless Basic Settings – WDS

The page includes the following fields:

Object	Description
Disable Wireless LAN Interface	Check the box to disable the wireless function.
Band	Select the desired mode. Default is “**2.4GHz (B+G+N)**”. It is strongly recommended that you set the Band to “2.4GHz (B+G+N)”, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the

	WNAP-6315. ■ **2.4 GHz (B)**: 802.11b mode, rate is up to 11Mbps ■ **2.4 GHz (G)**: 802.11g mode, rate is up to 54Mbps ■ **2.4 GHz (N)**: 802.11n mode, rate is up to 150Mbps(1T1R) ■ **2.4 GHz (B+G)**: 802.11b/g mode, rate is up to 11Mbps or 54Mbps ■ **2.4 GHz (G+N)**: 802.11g/n mode, rate is up to 54Mbps or 150Mbps ■ **2.4 GHz (B+G+N)**: 802.11b/g/n mode, rate is up to 11Mbps, 54Mbps, or 150Mbps
Mode	There are four kinds of wireless mode selections: ■ **AP** ■ **Client** ■ **WDS** ■ **AP+WDS** If you select WDS or AP+WDS, please click "**WDS Settings**" submenu for the related configuration. Furthermore, click the "**Multiple AP"** button to enable multiple SSID function.
Channel Width	You can select **20MHz**, or **40MHz**
Control Sideband	You can select **Upper** or **Lower**.
Channel Number	You can select the operating frequency of wireless network.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.** Default is "**Auto"**.

- **AP+ WDS**

Connect this Wireless AP with up to 8 WDS-capable wireless APs, and connect another AP to provide service for all wireless stations within its coverage.

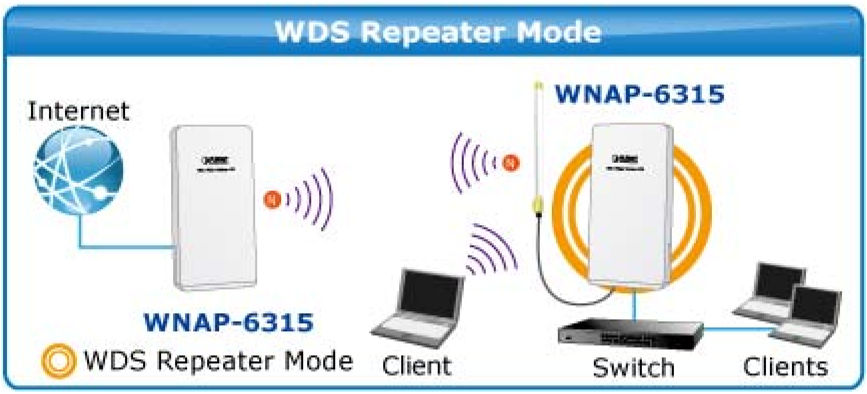
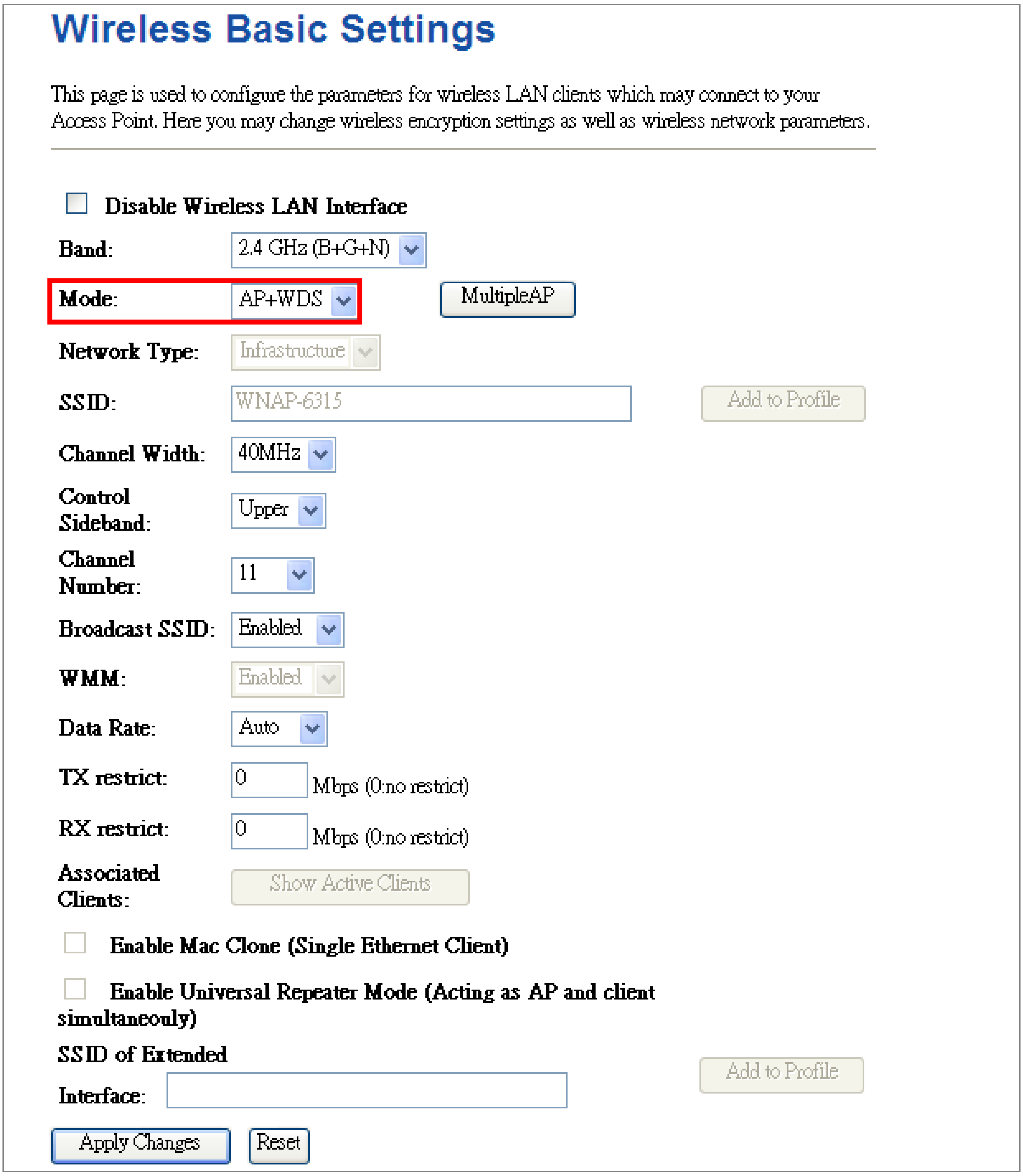


Figure 5-33 Topology – WDS+AP Mode



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)	
Mode:	AP+WDS	MultipleAP
Network Type:	Infrastructure	
SSID:	WNAP-6315	Add to Profile
Channel Width:	40MHz	
Control Sideband:	Upper	
Channel Number:	11	
Broadcast SSID:	Enabled	
WMM:	Enabled	
Data Rate:	Auto	
TX restrict:	0 Mbps (0:no restrict)	
RX restrict:	0 Mbps (0:no restrict)	
Associated Clients:	Show Active Clients	

☐ Enable Mac Clone (Single Ethernet Client)

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface: [ ] Add to Profile

Apply Changes | Reset

Figure 5-34 Wireless Basic Settings – WDS+AP

The page includes the following fields:

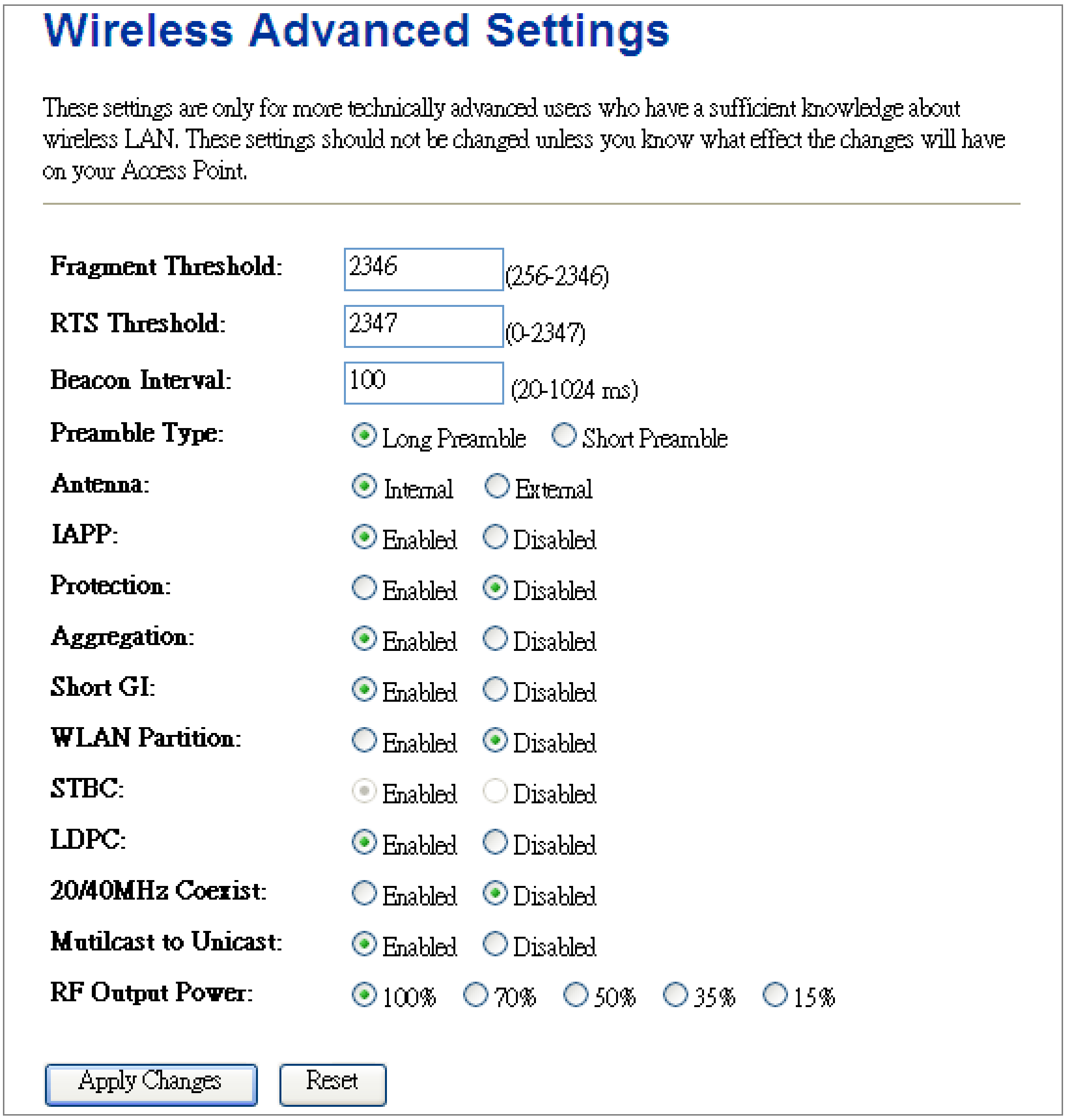
Object	Description
Disable Wireless LAN Interface	Check the box to disable the wireless function.
Country	Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router

	in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.
Band	Select the desired mode. Default is "**2.4GHz (B+G+N)**". It is strongly recommended that you set the Band to "2.4GHz (B+G+N)", and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the WNAP-6315. ■ **2.4 GHz (B)**: 802.11b mode, rate is up to 11Mbps ■ **2.4 GHz (G)**: 802.11g mode, rate is up to 54Mbps ■ **2.4 GHz (N)**: 802.11n mode, rate is up to 150Mbps(1T1R) ■ **2.4 GHz (B+G)**: 802.11b/g mode, rate is up to 11Mbps or 54Mbps ■ **2.4 GHz (G+N)**: 802.11g/n mode, rate is up to 54Mbps or 150Mbps ■ **2.4 GHz (B+G+N)**: 802.11b/g/n mode, rate is up to 11Mbps, 54Mbps, or 150Mbps
Mode	There are four kinds of wireless mode selections: ■ **AP** ■ **Client** ■ **WDS** ■ **AP+WDS** If you select WDS or AP+WDS, please click "**WDS Settings**" submenu for the related configuration. Furthermore, click the "**Multiple AP"** button to enable multiple SSID function.
SSID	The ID of the wireless network. User can access the wireless network via the ID only. However, if you switch to Client Mode, this field becomes the SSID of the AP you want to connect with. Default: **WNAP-6315**
Channel Width	You can select **20MHz**, or **40MHz**
Control Sideband	You can select **Upper** or **Lower**.
Channel Number	You can select the operating frequency of wireless network.
Broadcast SSID	If you enable "Broadcast SSID", every wireless station located within the coverage of the WNAP-6315 can discover its signal easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling "Broadcast SSID" can provide better wireless network security. Default is "**Enabled**".
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.** Default is "**Auto"**.

Associated Clients	Click the "**Show Active Clients**" button to show the status table of active wireless clients.
Enable Universal Repeater Mode (Acting as AP and client simultaneously)	Universal Repeater is a technology used to extend wireless coverage. To enable Universal Repeater Mode, check the box and enter the SSID you want to broadcast in the field below. Then please click "Security" submenu for the related settings of the AP you want to connect with.

5.4.2 Advanced Settings

Choose menu "**Wireless→ Advanced Settings**" to configure the wireless advanced settings for the wireless network on this page. After the configuration, please click the "Apply Changes" button to save the settings.



Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Preamble Type: ● Long Preamble ○ Short Preamble

Antenna: ● Internal ○ External

IAPP: ● Enabled ○ Disabled

Protection: ○ Enabled ● Disabled

Aggregation: ● Enabled ○ Disabled

Short GI: ● Enabled ○ Disabled

WLAN Partition: ○ Enabled ● Disabled

STBC: ● Enabled ○ Disabled

LDPC: ● Enabled ○ Disabled

20/40MHz Coexist: ○ Enabled ● Disabled

Mutilcast to Unicast: ● Enabled ○ Disabled

RF Output Power: ● 100% ○ 70% ○ 50% ○ 35% ○ 15%

Figure 5-35 Wireless Advanced Settings

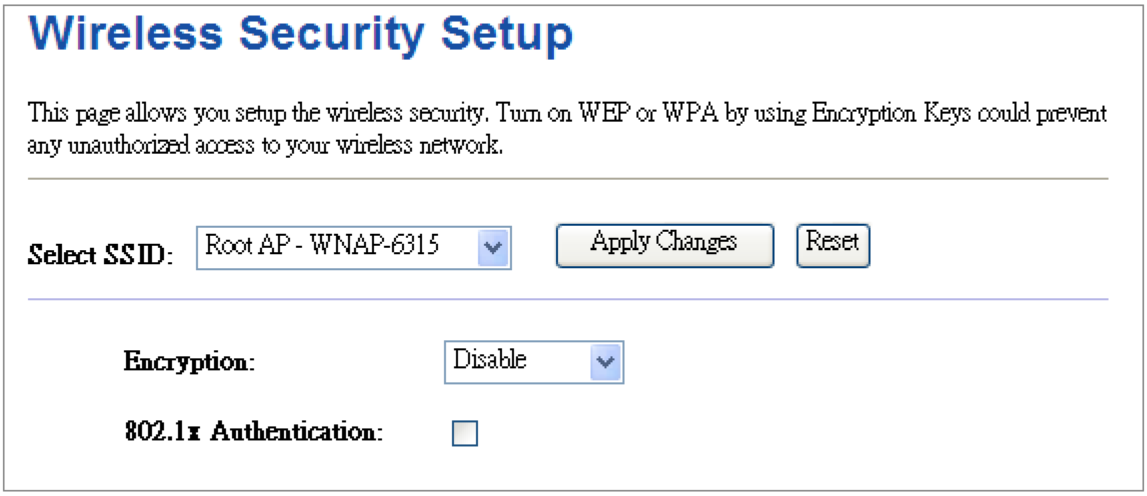
The page includes the following fields:

Object	Description
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 “2347”.
Beacon Interval	The interval of time that this access point broadcasts a beacon. Beacon is used to synchronize the wireless network. Default is “100”.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “**Short Preamble**” is suitable for high traffic wireless network. “**Long Preamble**” can provide more reliable communication. Default is “Long Preamble”.
Antenna	Choose **“External”** to switch the antenna to external antenna. ※ For External Antenna Mode, user MUST physically attach antenna before powering on. Then, configure the Antenna Switch (Wireless Advanced page) from “**Internal**” to “**External**”. Default is “Internal”.
IAPP	**IAPP (Inter-Access Point Protocol)** enabled is recommended as it describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems. Default is “Enabled”.
Protection	Enables a backward compatible protection mechanism for 802.11b clients. When the protection mode is enabled can slow the throughput of the 802.11g/n clients by as much as 50%. Default is “Disabled”.
Aggregation	It is a function where the values of multiple rows are grouped together. Default is “Enabled”
Short GI	It is used to set the time that the receiver waits for RF reflections to settle out before sampling data. Default is “Enabled”
WLAN Partition	This feature also called “**WLAN isolation**” or “**Block Relay**”. If this is enabled, wireless clients cannot exchange data through the WNAP-6315. Default is “Disabled”.
STBC	Activate **Space Time Blocking Code (STBC)** which does not need channel statement information (CSI). Default Setting: "Enabled"
LDPC	Low-density Parity-check Code is wireless data transmit algorithm. Default Setting: "Enabled"
20/40MHz Coexist	Configure 20/40MHz coexisting scheme. If you set up as "Enabled", "20MHz" and "40MHz" will coexist.

	Default Setting: "Disabled"
Multicast to Unicast:	Enables multicast traffic streams to be converted to unicast traffic before delivery to wireless clients. Converting multicast traffic to unicast before sending to wireless clients allows a longer DTIM (Data Beacon Rate) interval to be set. A longer DTIM interval prevents clients in power-save mode having to activate their radios to receive the multicast data, which reduce power consumption. Default Setting: “Enabled”
RF Output Power	Users can adjust the wireless output power to different levels. For short distance of PtP connection within 1Km, it is suggested to reduce the output power to 50% or lower to prevent interference with each other. Default is “100%”.

5.4.3 Security

Choose menu “**Wireless → Security**” to configure the settings of wireless security for the wireless network on this page. After the configuration, please click the “Apply Changes” button to save the settings.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: Disable

802.1x Authentication: □

Figure 5-36 Wireless Security Settings

The page includes the following fields:

Object	Description
Select SSID	Select the SSID you want to configure the wireless security function, which includes the root one and the client one.
Encryption	■ **Disable:** No security setup for wireless connection.

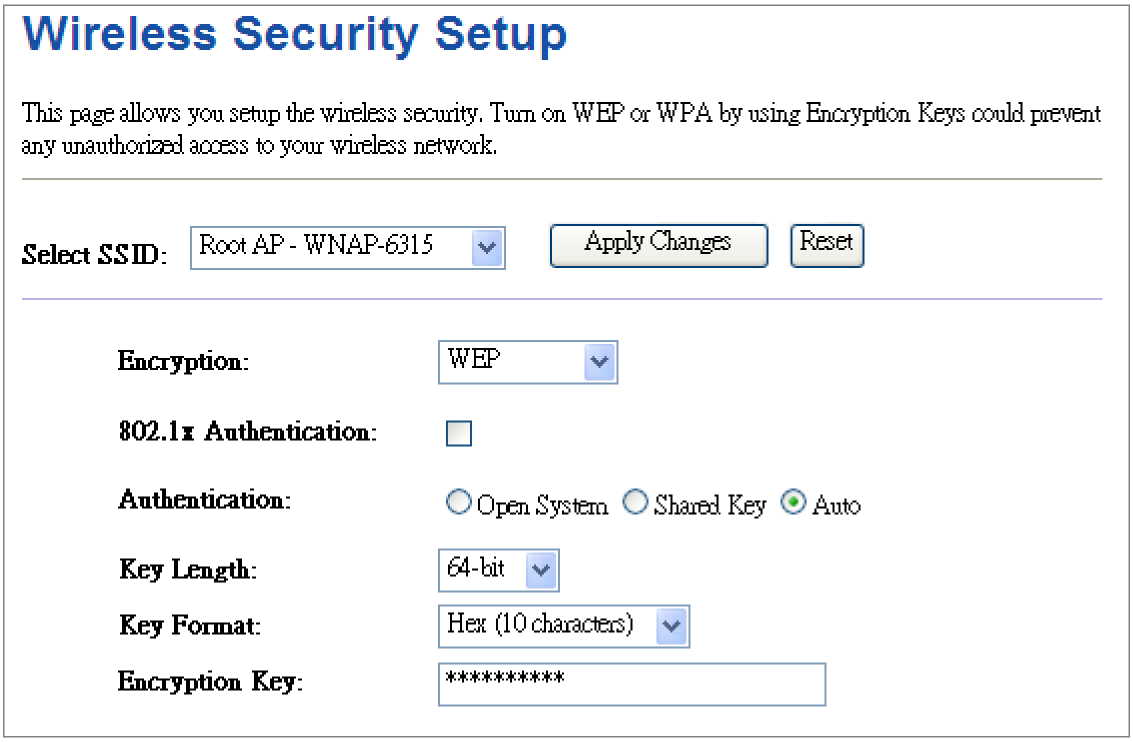
	■ **WEP:** It is based on the IEEE 802.11 standard. And the default setting of authentication is **Automatic**, which can select **Open System** or **Shared Key** authentication type automatically based on the wireless station's capability and request. Furthermore, you can select **Key Length** and enter 10 and 26 **Hexadecimal** digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 and 13 **ASCII** characters in the **Encryption Key** field.
	■ **WPA2:** WPA2 is a high level encryption and is supported by most wireless devices and operating systems.
	■ **WPA-Mixed:** WPA Mixed Mode allows the use of both WPA and WPA2 at the same time.
Authentication Mode	■ **Enterprise (RADIUS)** When you select the authentication mode based on Enterprise (Radius Server), please enter the **IP Address**, **Port**, and **Password** of the Radius Server.
	■ **Personal (Pre-Shared Key)** When you select the other authentication mode based on Personal (Pre-Shared Key), please enter at least 8 ASCII characters (Passphrase) or 64 Hexadecimal characters. All of the Cipher Suites support **TKIP** and **AES**.
802.1x Authentication	Enable 802.1x authentication function and then enter the **IP Address**, **Port**, and **Password** of the Radius Server.

- **Disable:**

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

- **WEP:**

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



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: WEP

802.1x Authentication: □

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bit

Key Format: Hex (10 characters)

Encryption Key: **********

Figure 5-37 Security Settings – WEP

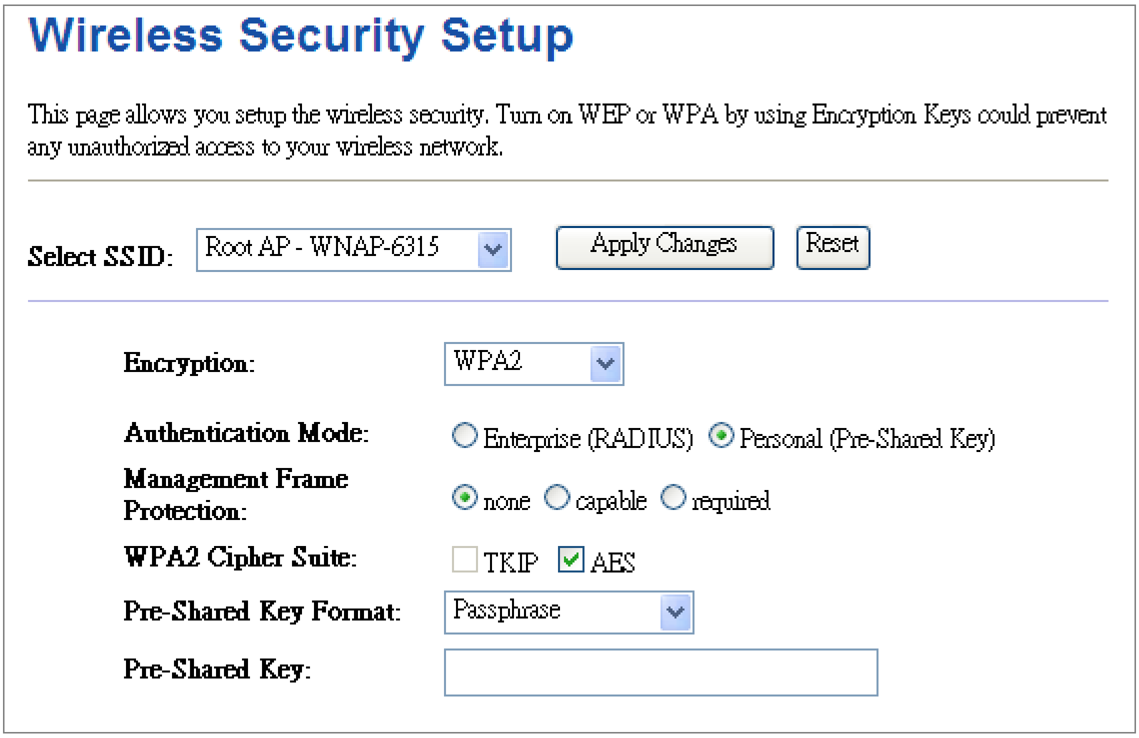
The page includes the following fields:

Object	Description
Encryption	You can disable the encryption or select WEP, WPA2, and WPA-Mixed as the encryption method to your wireless network.
802.1x Authentication	Enable 802.1x authentication function and then enter the IP Address, Port, and Password of the Radius Server.
Authentication	Configures the WEP security mode used by clients. When using WEP, be sure to define at least one static WEP key for the Wireless AP and all its clients. There are three options provided: **Open System** — this authentication accepts any client attempting to connect the Wireless AP without verifying its identity. **Shared Key** — the shared-key security uses a WEP key to authenticate clients connecting to the network and for data encryption. **Auto** — allows wireless clients to connect to the network using Open-WEP (uses WEP for encryption only) or Shared-WEP (uses WEP for authentication and encryption).
Key Length	Choose the WEP key length. You can choose **64-bit** or **128-bit**.
Key Format	You can choose **ASCII** or **Hex** format.
Encryption Key	Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for

	128-bit keys.

- **WPA2:**

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an enterprise and personal mode of operation.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: WPA2

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

Management Frame Protection: ● none ○ capable ○ required

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

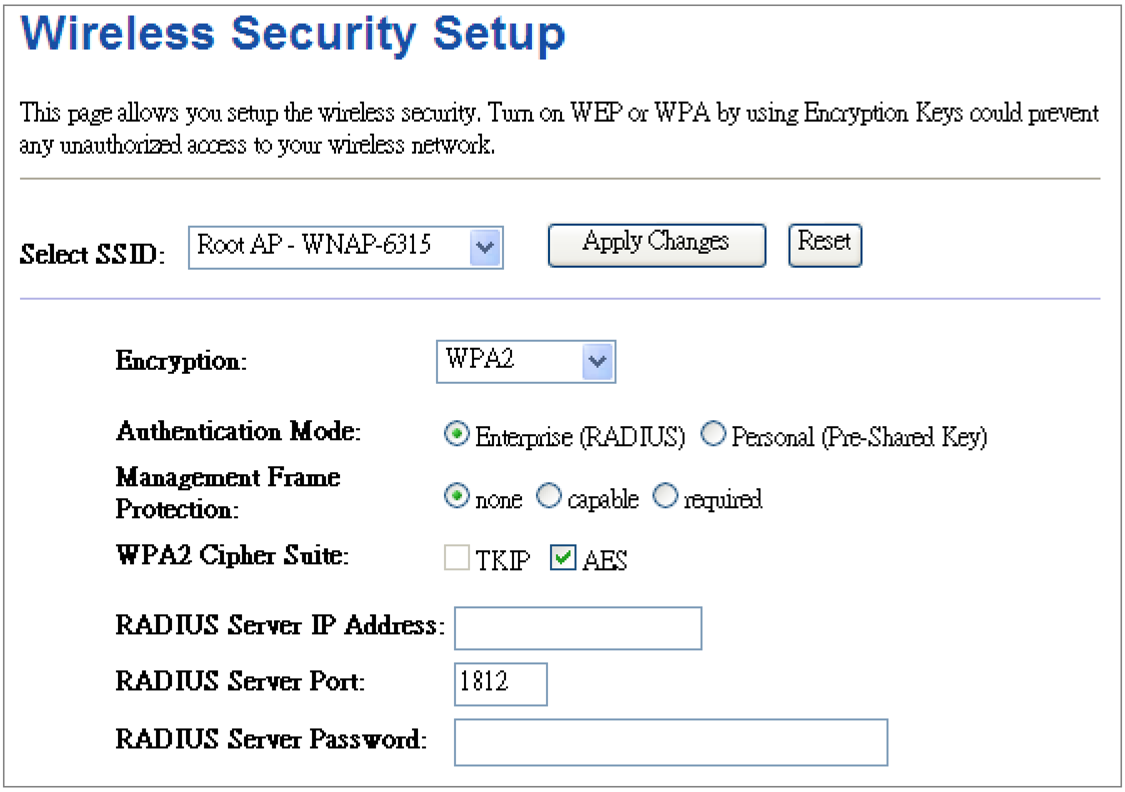
Pre-Shared Key:

Figure 5-38 Security Settings – WPA2 Personal

The page includes the following fields:

Object	Description
Encryption	You can disable the encryption or select WEP, WPA2, and WPA-Mixed as the encryption method to your wireless network.
Authentication Mode	Select “Enterprise (RADIUS)” for user authentication and you will require a RADIUS authentication server to be configured on the wired network. Select “Personal (Pre-Shared Key)” and you will require a pre-shared key to be configured for client authentication.
Management Frame Protection	Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support. If you choose this to “Required”, then clients are allowed to associate only if MFP is negotiated. If you choose “Capable”, then the non-supporting clients are allows to associate (without using MFP).

WPA2 Cipher Suite	Selects the data encryption type to use. (Default is determined by the Encryption Mode selected.) **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.
Pre-Shared Key Format	Specify the format of the key, pass phrase or hex. The WPA Pre-shared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)
Pre-Shared Key	Enter the key whose format is limited by the key format.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: WPA2

Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

Management Frame Protection: ● none ○ capable ○ required

WPA2 Cipher Suite: □ TKIP ☑ AES

RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

Figure 5-39 Security Settings – WPA2 Enterprise

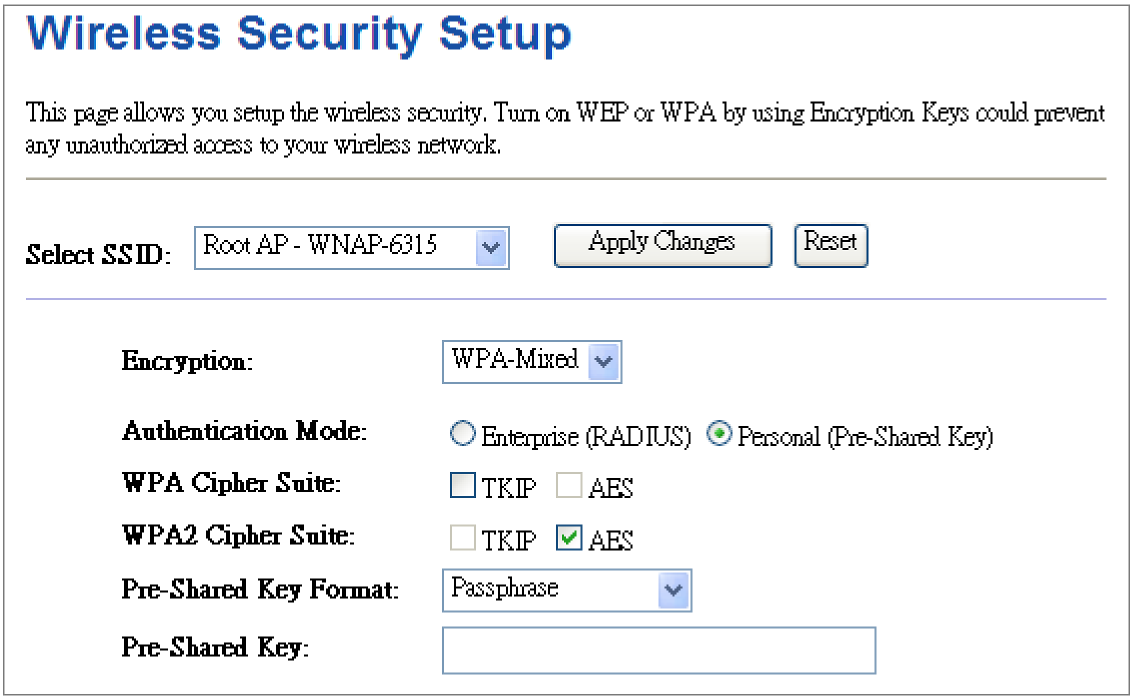
The page includes the following fields:

Object	Description
Encryption	You can disable the encryption or select WEP, WPA2, and WPA-Mixed as the encryption method to your wireless network.
Authentication Mode	Select "Enterprise (RADIUS)" for user authentication and you will require a RADIUS authentication server to be configured on the wired network. Select "Personal (Pre-Shared Key)" and you will require a pre-shared key to be configured for client authentication.
Management Frame Protection	Management frame protection (MFP) provides security for the otherwise unprotected and unencrypted 802.11 management messages passed between access points and clients. MFP provides both infrastructure and client support. If you choose this to "Required", then clients are allowed to associate only if MFP is negotiated. If you choose "Capable", then the non-supporting clients are allows to associate (without using MFP).
WPA2 Cipher Suite	Selects the data encryption type to use. (Default is determined by the Encryption Mode selected.) **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

	AES — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.
RADIU Server IP Address	Enter the RADIUS server host IP address.
RADIU Server Port	Set the UDP port used in the authentication protocol of the RADIUS server. (Range: 1024-65535; Default: 1812)
RADIU Server Password	A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. Enter a shared secret/password between 1 and 99 characters in length.

- **WPA-Mixed:**

Please refer to the WPA2 section for the definition of each field.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: WPA-Mixed

Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

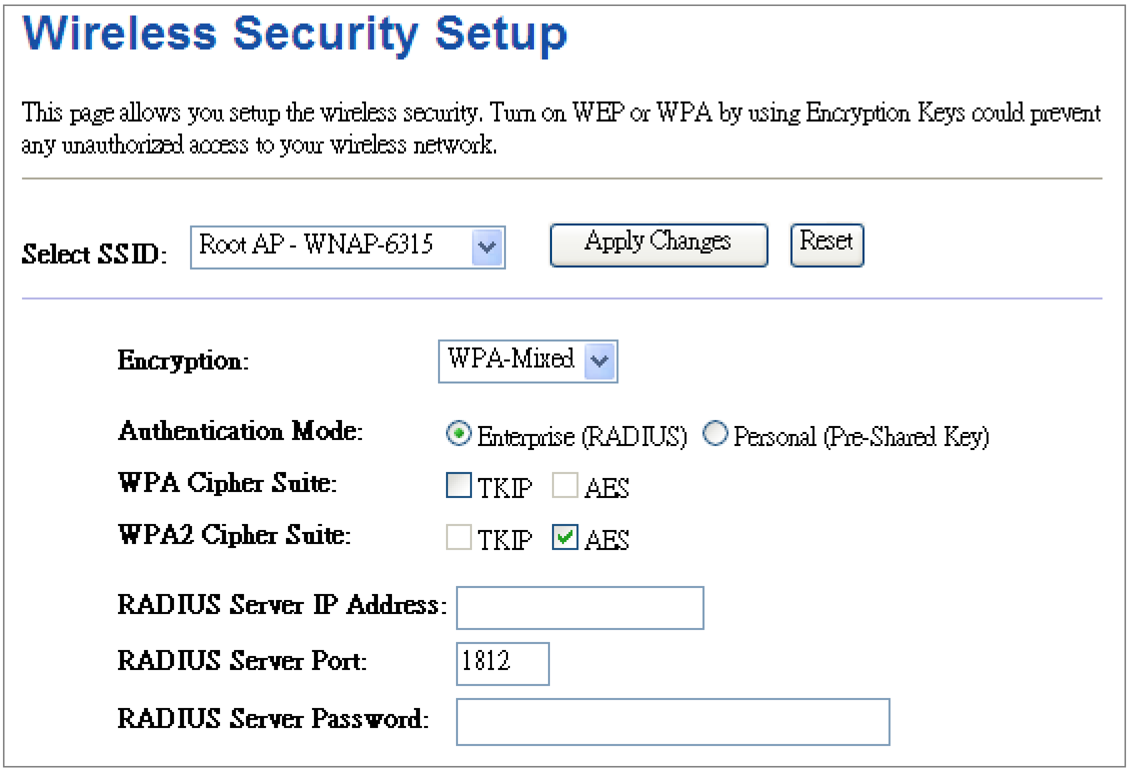
WPA Cipher Suite: □ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Figure 5-40 Security Settings – WPA-Mixed Personal



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: WPA-Mixed

Authentication Mode: ● Enterprise (RADIUS) ○ Personal (Pre-Shared Key)

WPA Cipher Suite: □ TKIP □ AES

WPA2 Cipher Suite: □ TKIP ☑ AES

RADIUS Server IP Address:

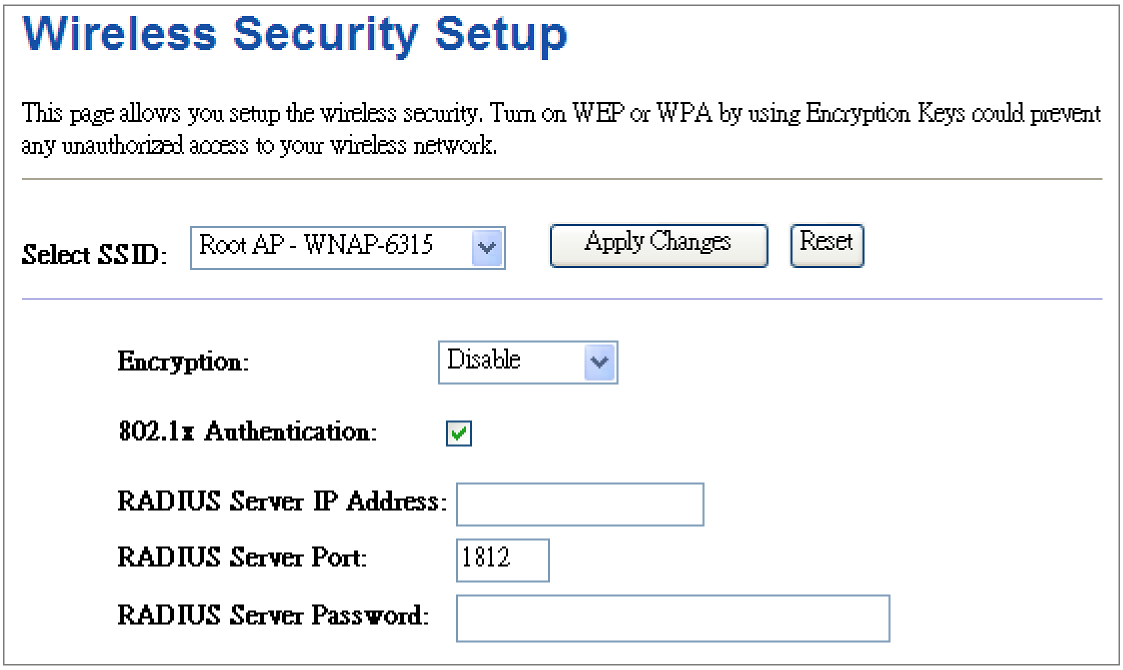
RADIUS Server Port: 1812

RADIUS Server Password:

Figure 5-41 Security Settings – WPA-Mixed Enterprise

- **802.1x Authentication:**

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID: Root AP - WNAP-6315

Encryption: Disable

802.1x Authentication: ☑

RADIUS Server IP Address:

RADIUS Server Port: 1812

RADIUS Server Password:

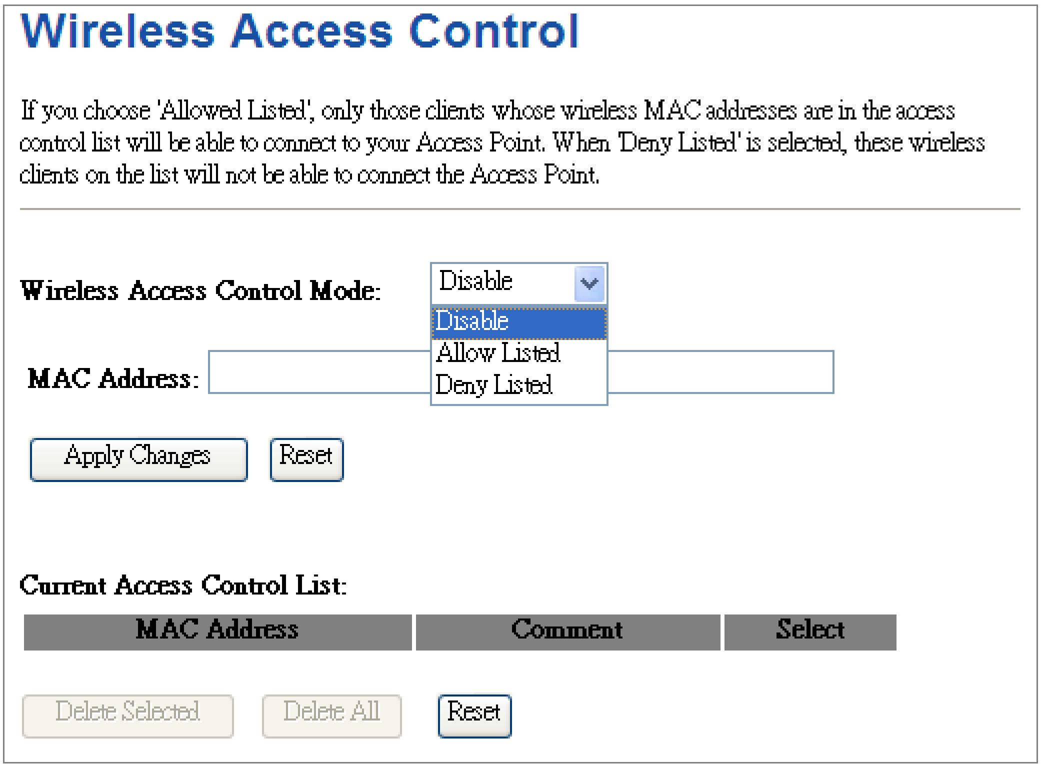
Figure 5-42 Security Settings – 802.1x Authentication

The page includes the following fields:

Object	Description
Encryption	You can disable the encryption or select WEP, WPA2, and WPA-Mixed as the encryption method to your wireless network.
802.1x Authentication	Enable 802.1x authentication function and then enter the IP Address, Port, and Password of the Radius Server.
RADIU Server IP Address	Enter the RADIUS server host IP address.
RADIU Server Port	Set the UDP port used in the authentication protocol of the RADIUS server. (Range: 1024-65535; Default: 1812)
RADIU Server Password	A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. Enter a shared secret/password between 1 and 99 characters in length.

5.4.4 Access Control

Choose menu "**Wireless → Access Control**" to allow or deny the computer of specified MAC address to connect with the WNAP-6315 on this page. After the configuration, please click the "Apply Changes" button to save the settings.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable

Current Access Control List:

MAC Address	Comment	Select

Figure 5-43 Wireless Access Control

The page includes the following fields:

Object	Description
Wireless Access Control Mode	You can choose to set the Allowed-List, Denied-List, or disable this function.
MAC Address	Enter the MAC address you want to allow or deny connection to the WNAP-6315 in the field.
Comment	You can make some comment on each MAC address on the list.
Current Access Control List	You can select some MAC addresses and click the "Delete Selected" button to delete it.

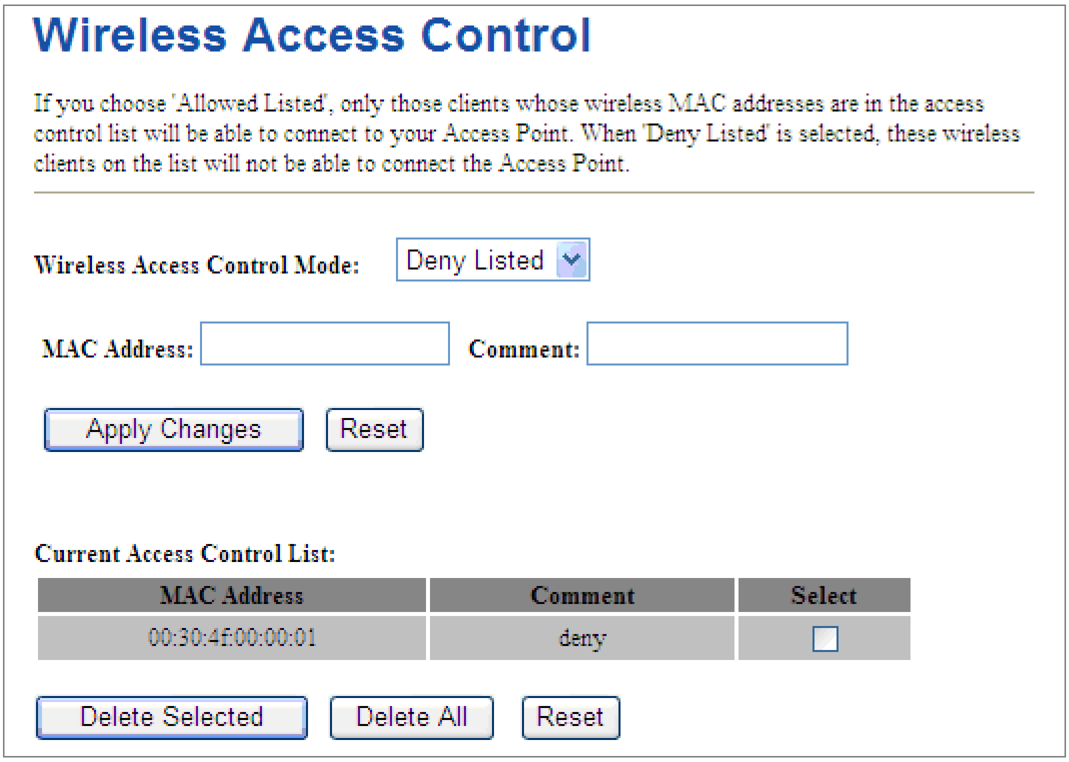
- **Wireless Access Control example:**

To deny a PC at the MAC address of 00:30:4F:00:00:01 to connect to your wireless network, do as follows:

Step 1. Select "**Deny**" from MAC Address Filter drop-down menu.

Step 2. Enter 00:30:4F:00:00:01 in the MAC address box and click "**Add**".

Step 3. Click the "**OK**" button to save your settings and you can add more MAC addresses, if you like, simply repeat the above steps.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Deny Listed

MAC Address: Comment:

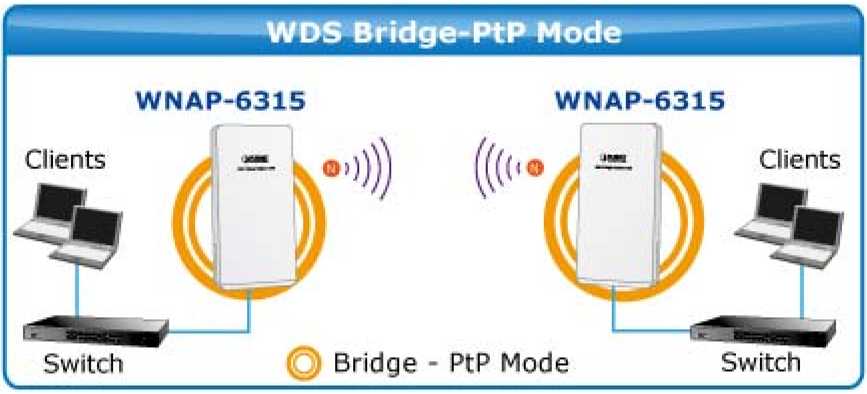
Current Access Control List:

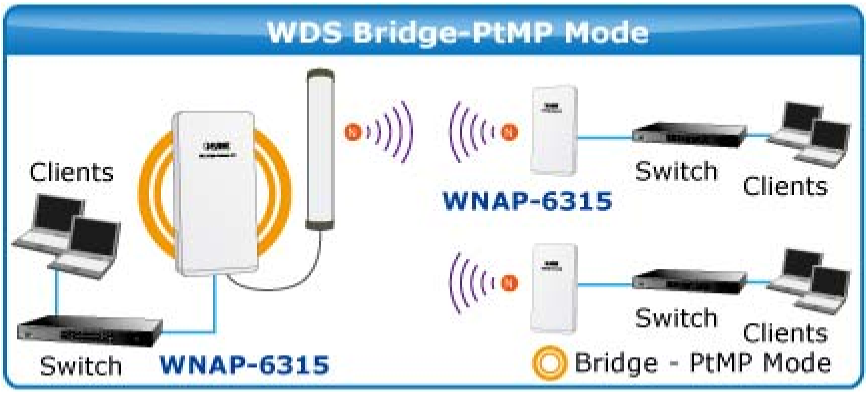
MAC Address	Comment	Select
00:30:4f:00:00:01	deny	□

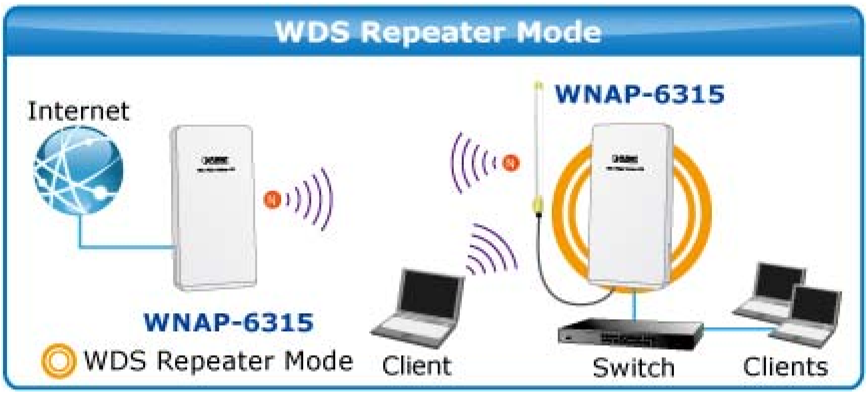
Figure 5-44 Wireless Access Control – Deny

5.4.5 WDS

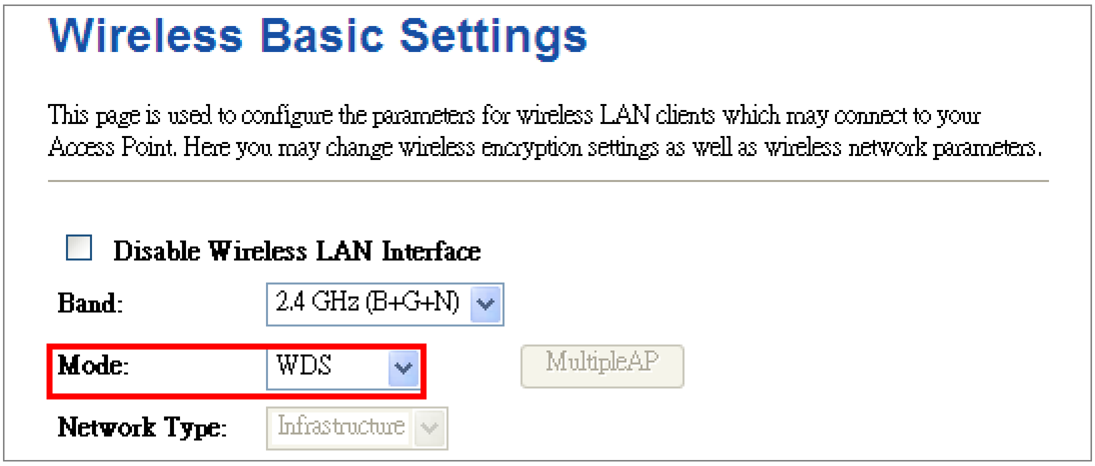
WDS (Wireless Distribution System) feature can be used to extend your existing wireless network coverage.







Before configuring the WDS Setting page, you have to select the wireless mode to “**WDS**” on the **Wireless** -> **Basic Settings** web page.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ **Disable Wireless LAN Interface**

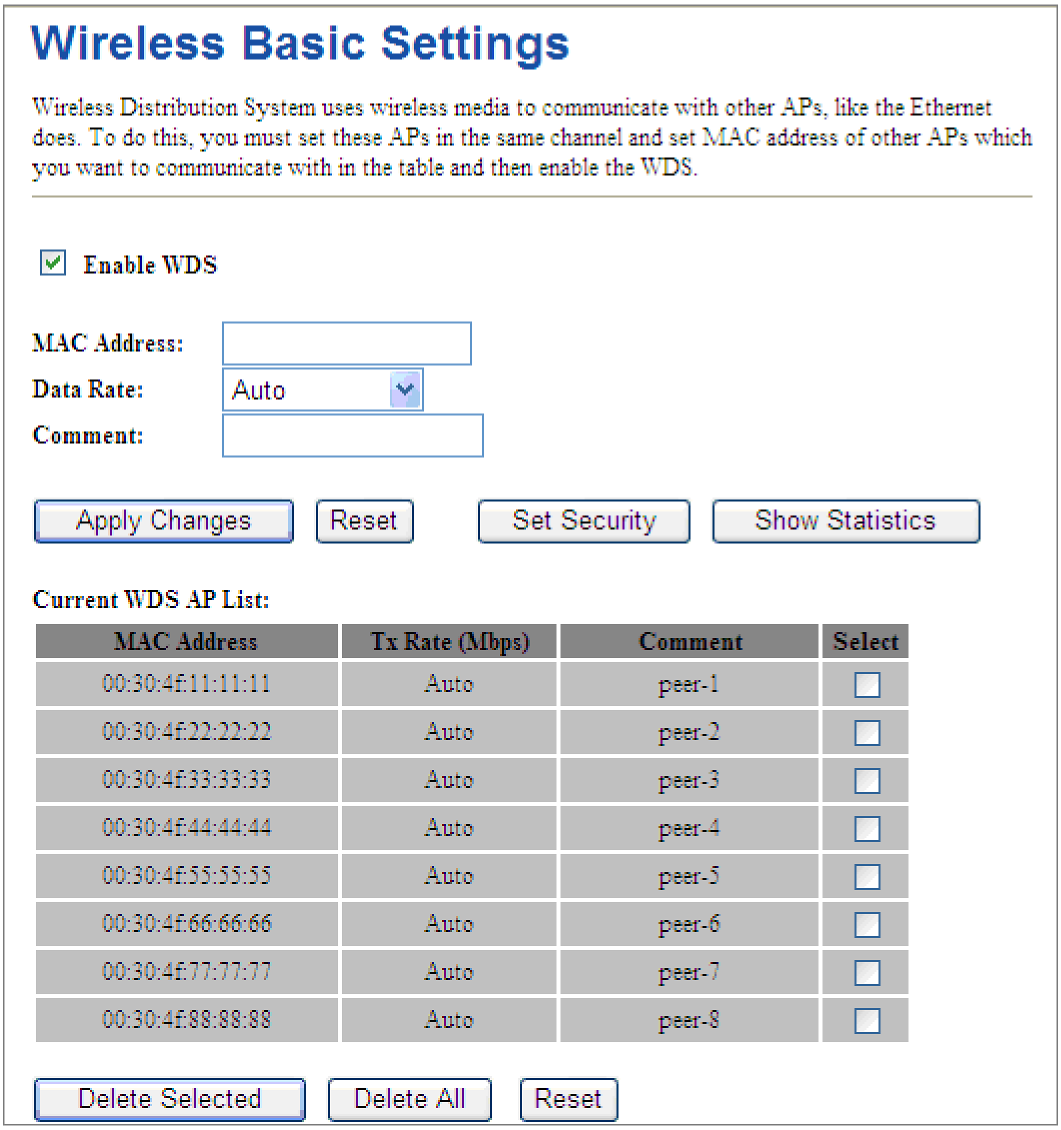
Band: 2.4 GHz (B+G+N)

Mode: WDS

Network Type: Infrastructure

Figure 5-45 WDS Mode

Choose menu "**Wireless → WDS Settings**" to configure WDS to connect the WNAP-6315 with another AP on this page. After the configuration, please click the "**Apply Changes**" button to save the settings.



Wireless Basic Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☑ **Enable WDS**

MAC Address:

Data Rate: Auto

Comment:

Current WDS AP List:

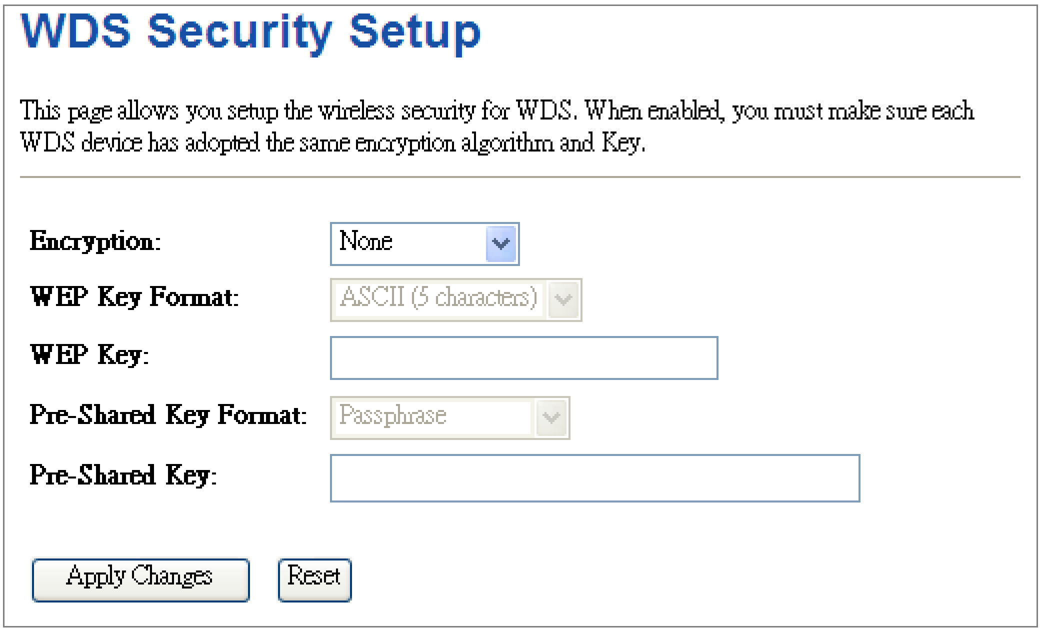
MAC Address	Tx Rate (Mbps)	Comment	Select
00:30:4f:11:11:11	Auto	peer-1	☐
00:30:4f:22:22:22	Auto	peer-2	☐
00:30:4f:33:33:33	Auto	peer-3	☐
00:30:4f:44:44:44	Auto	peer-4	☐
00:30:4f:55:55:55	Auto	peer-5	☐
00:30:4f:66:66:66	Auto	peer-6	☐
00:30:4f:77:77:77	Auto	peer-7	☐
00:30:4f:88:88:88	Auto	peer-8	☐

Figure 5-46 WDS Settings

The page includes the following fields:

Object	Description
Enable WDS	Check the box to enable the WDS function. Please select **WDS** or **AP+WDS** in the Mode of **Wireless Basic Settings** before you enable WDS on this page.
MAC Address	You can enter the MAC address of the AP you want to connect with.
Data Rate	Default is “**Auto”**.
Comment	You can make some comment for each MAC address on the list.
Set Security	Click the “**Set Security**” button to configure the wireless security parameters of the AP you want to connect via WDS.
Show Statics	Click the “Show Statics” button to show the WDS AP.
Current WDS AP List	You can select some MAC addresses of the AP and click the “Delete Selected” button to delete it.

Once clicked “Set Security” to enter the following page to configure the encryption method and pre-shared key for the WDS connection.



WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption: None

WEP Key Format: ASCII (5 characters)

WEP Key:

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

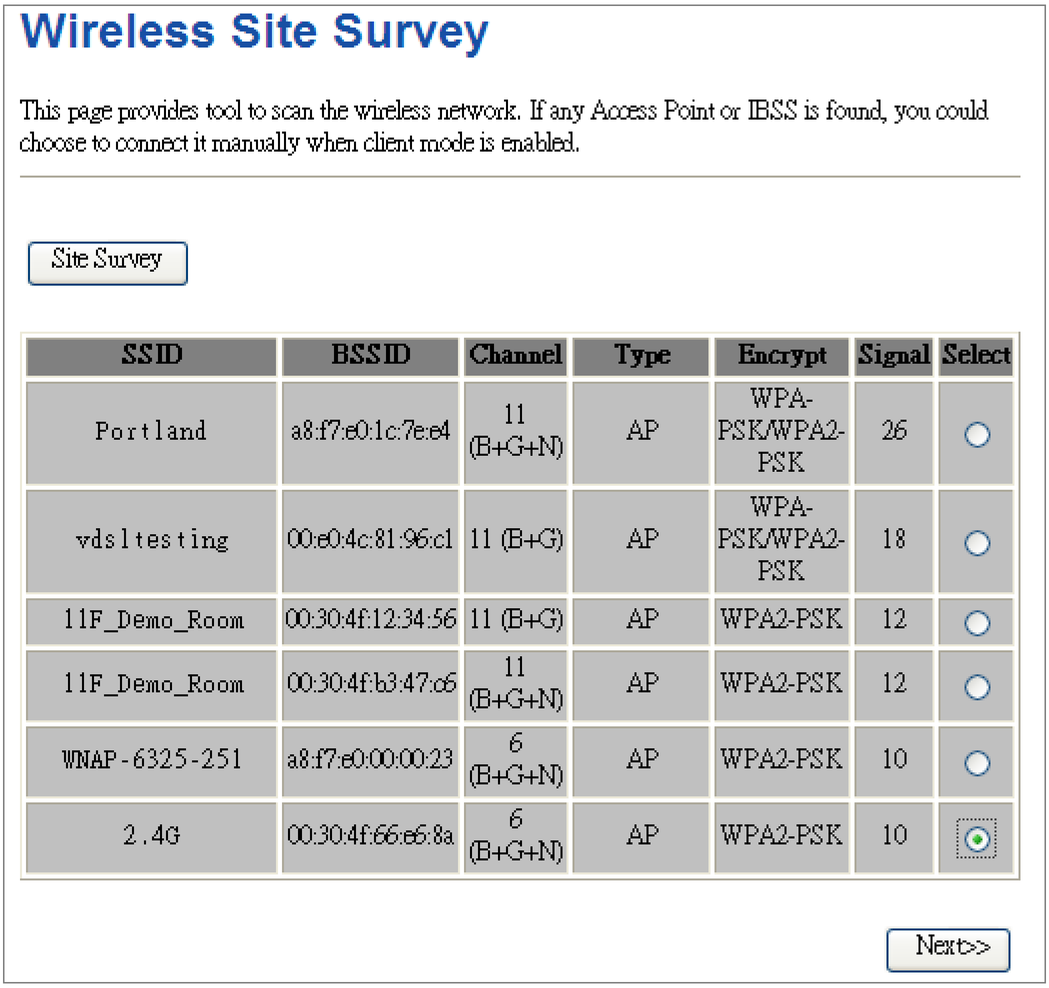
Figure 5-47 WDS – Set Security

WDS feature can only be implemented between 2 wireless devices that both support the WDS feature. Plus, **channel**, **security settings** and **security key** must be **the same** on both such devices.

To encrypt your wireless network, click "**Set Security**". For the detail of wireless security, see **section 5.5.4**. Do remember to reboot the device after you save your wireless security settings; otherwise, the WDS feature may not function.

5.4.6 Site Survey

Choose menu "**Wireless → Site Survey**" to scan the available local AP. If any Access Point is found, you could choose any one to connect with manually when the **Client Mode** is enabled.



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Portland	a8:f7:e0:1c:7e:e4	11 (B+G+N)	AP	WPA-PSK/WPA2-PSK	26	○
vdsltesting	00:e0:4c:81:96:c1	11 (B+G)	AP	WPA-PSK/WPA2-PSK	18	○
11F_Demo_Room	00:30:4f:12:34:56	11 (B+G)	AP	WPA2-PSK	12	○
11F_Demo_Room	00:30:4f:b3:47:c6	11 (B+G+N)	AP	WPA2-PSK	12	○
WNAP-6325-251	a8:f7:e0:00:00:23	6 (B+G+N)	AP	WPA2-PSK	10	○
2.4G	00:30:4f:66:e6:8a	6 (B+G+N)	AP	WPA2-PSK	10	●

Next>>

Figure 5-48 Site Survey

5.4.7 WPS

WPS (**Wi-Fi Protected Setup**) is designed to ease setup of security Wi-Fi networks and subsequently network management. This Wireless Router supports WPS features for **AP mode**, **AP+WDS mode**, **Infrastructure-Client mode**, and the wireless root interface of **Universal Repeater mode**.

Simply enter a PIN code or press the software PBC button or hardware WPS button (if any) and a secure wireless connection is established.

- **PBC**: If you find the WPS LED blinking for 2 minutes after you press the hardware WPS button on the device, it means that PBC encryption method is successfully enabled. And an authentication will be performed between your router and the WPS/PBC-enabled wireless client device during this time; if it succeeds, the wireless client device connects to your device, and the WPS LED turns off. Repeat steps mentioned above if you want to connect more wireless client devices to the device.
- **PIN** : To use this option, you must know the PIN code from the wireless client and enter it in corresponding field on your device while using the same PIN code on client side for such connection.

The page includes the following fields:

Object	Description
Disable WPS	You can check the box to disable the WPS function.
WPS Status	Here you can check if the connection via WPS is established or not.
Self-PIN Number	It is the PIN number of the WNAP-6315 here.
Push Button Configuration	Click the “Start PBC” to activate WPS as well in the client device within 2 minutes.
Client PIN Number	In addition to the PBC method, you can also use the PIN method to activate the WPS. Just enter the PIN number of the client device in the field and click the “Start PIN” button.

Note

The WPS encryption can be implemented only between your Router and another WPS-capable device.

➢ Example of how to establish wireless connection using **WPS**. Please take the following steps:

Step 1. Choose menu “**Wireless → WPS**” to configure the setting for WPS. After the configuration, please click the “Apply Changes” button to save the settings.

Step 2. Add a new device.

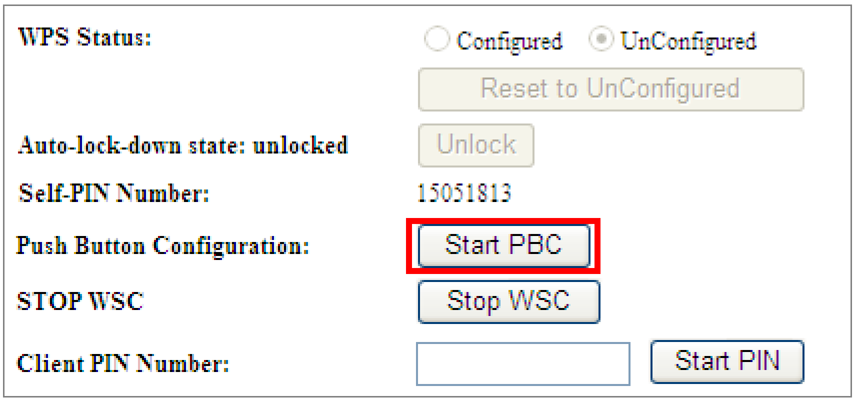
If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and AP using either Push Button Configuration (PBC) method or PIN method.

Note

To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function.

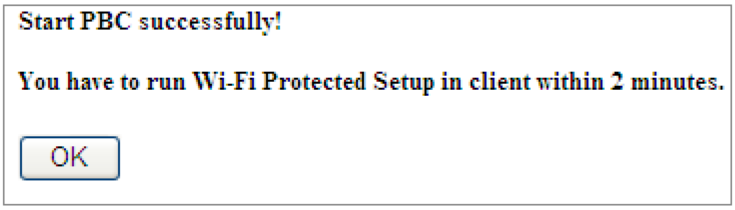
A. By Push Button Configuration (PBC)

i. Click the “Start PBC” Button on the WPS page of the AP.



WPS Status:	○ Configured ● UnConfigured
	Reset to UnConfigured
Auto-lock-down state: unlocked	Unlock
Self-PIN Number:	15051813
Push Button Configuration:	Start PBC
STOP WSC	Stop WSC
Client PIN Number:	Start PIN

Figure 5-49 WPS-PBC



Start PBC successfully!

You have to run Wi-Fi Protected Setup in client within 2 minutes.

Figure 5-50 WPS-PBC

ii. Press and hold the WPS Button equipped on the adapter directly for 2 or 3 seconds. Or you can click the WPS button with the same function in the configuration utility of the adapter. The process must be finished within 2 minutes.

iii. Wait for a while until the next screen appears. Click **OK** to complete the WPS configuration.

B. By PIN

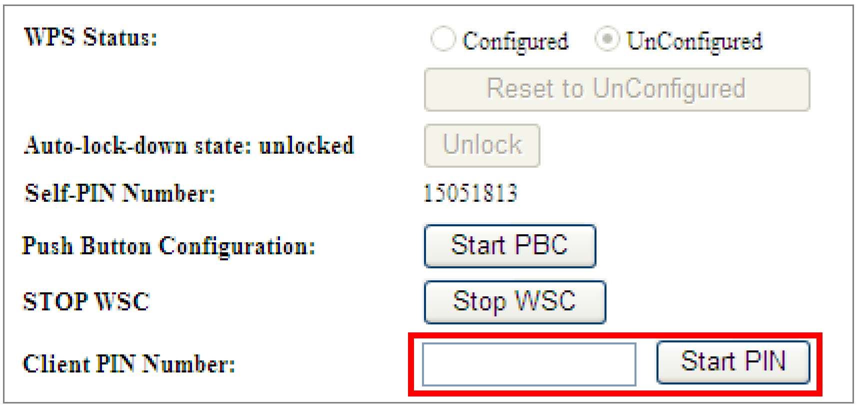
If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN of your Wireless adapter into the configuration utility of the AP

i. Enter the PIN code of the wireless adapter in the field behind **Client PIN Number** in the following figure and then click **Start PIN**.

Note

The PIN code of the adapter is always displayed on the WPS configuration screen.



WPS Status: ○ Configured ● UnConfigured

Auto-lock-down state: unlocked

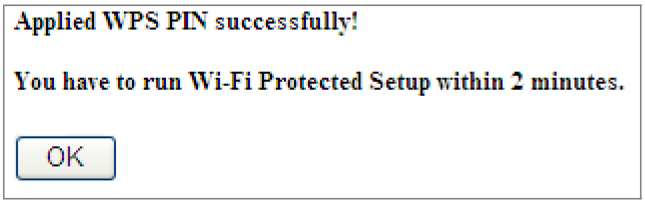
Self-PIN Number: 15051813

Push Button Configuration:

STOP WSC

Client PIN Number:

Figure 5-51 WPS-PIN



Applied WPS PIN successfully!

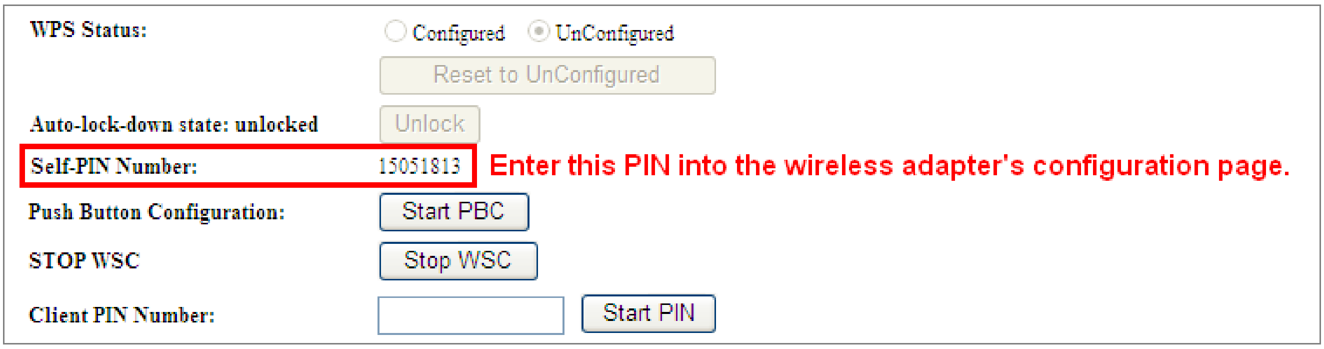
You have to run Wi-Fi Protected Setup within 2 minutes.

Figure 5-52 WPS-PIN

ii. For the configuration of the wireless adapter, please choose the option that you want to **enter PIN into the AP (Enrollee)** in the configuration utility of the WPS and click **Next** until the process finishes.

Method Two: Enter the PIN of the AP into the configuration utility of your Wireless adapter

i. Click the "Start PBC" Button on the WPS page of the AP. Get the Current PIN code of the AP in WPS page (each AP has its unique PIN code).



WPS Status: ○ Configured ● UnConfigured

Auto-lock-down state: unlocked

Self-PIN Number: 15051813

Enter this PIN into the wireless adapter's configuration page.

Push Button Configuration:

STOP WSC

Client PIN Number:

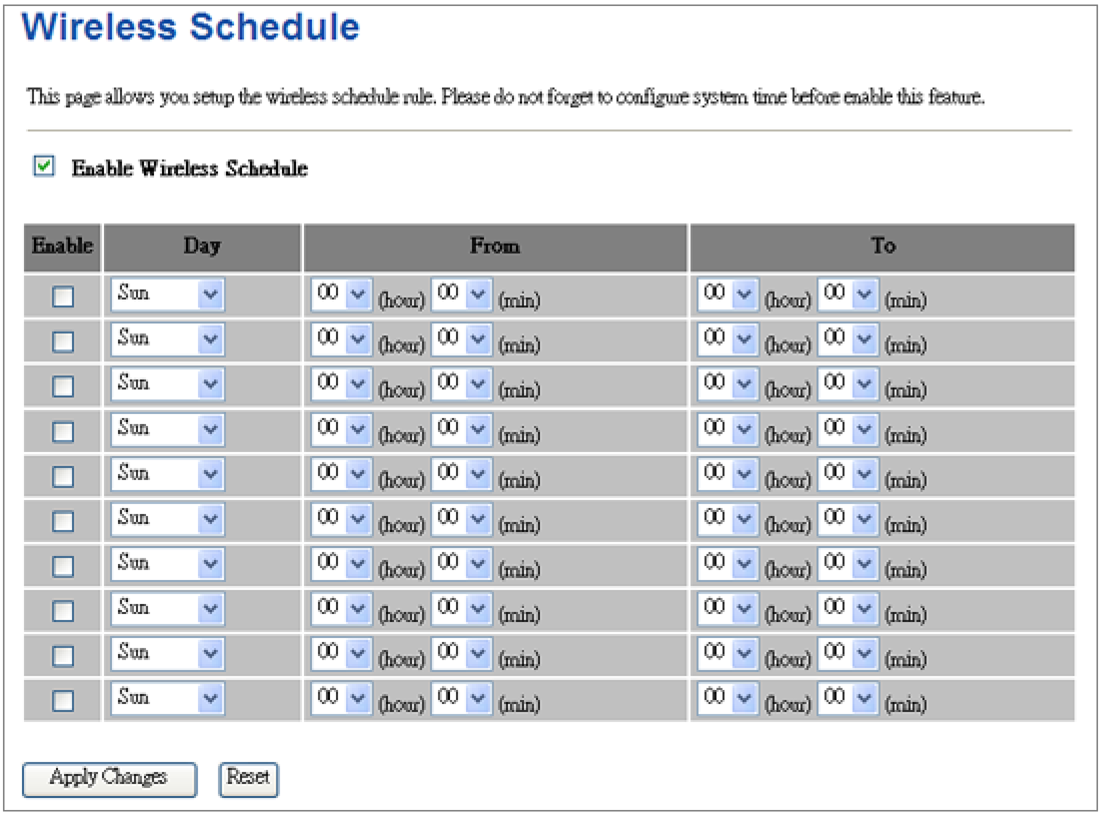
Figure 5-53 WPS-PIN

ii. For the configuration of the wireless adapter, please choose the option that you want to **enter the PIN of the AP (Registrar)** in the configuration utility of the Wireless adapter and enter it into the field. Then click **Next** until the process finishes.

5.4.8 Schedule

Wireless Schedules will enable or disable your wireless access at a set time based on your predefined schedule. This feature is often used for restricting access to all users (such as children, employees and guests) during specific times of the day for parental control or security reasons.

Choose menu “**Wireless → Schedule**” to configure the schedule rule of enabling wireless function. After the configuration, please click the “**Apply Changes**” button to save the settings.



Wireless Schedule

This page allows you setup the wireless schedule rule. Please do not forget to configure system time before enable this feature.

☑ Enable Wireless Schedule

Enable	Day	From	To
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)
□	Sun	00 (hour) 00 (min)	00 (hour) 00 (min)

Figure 5-54 Schedule

Note

When setting the Wireless Schedule, it is important to ensure that your **System Clock** settings have been configured. If not, your Wireless Schedule will not function correctly.

5.5 Firewall

This section contains firewall settings include Port/IP/MAC/URL Filtering/Forwarding and DMZ which are only functioning when the AP configured to "Gateway" mode. Please refer to the following sections for the details.

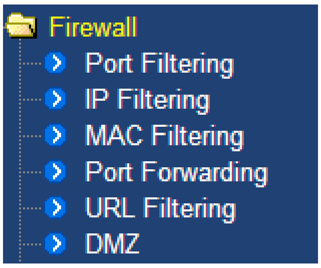
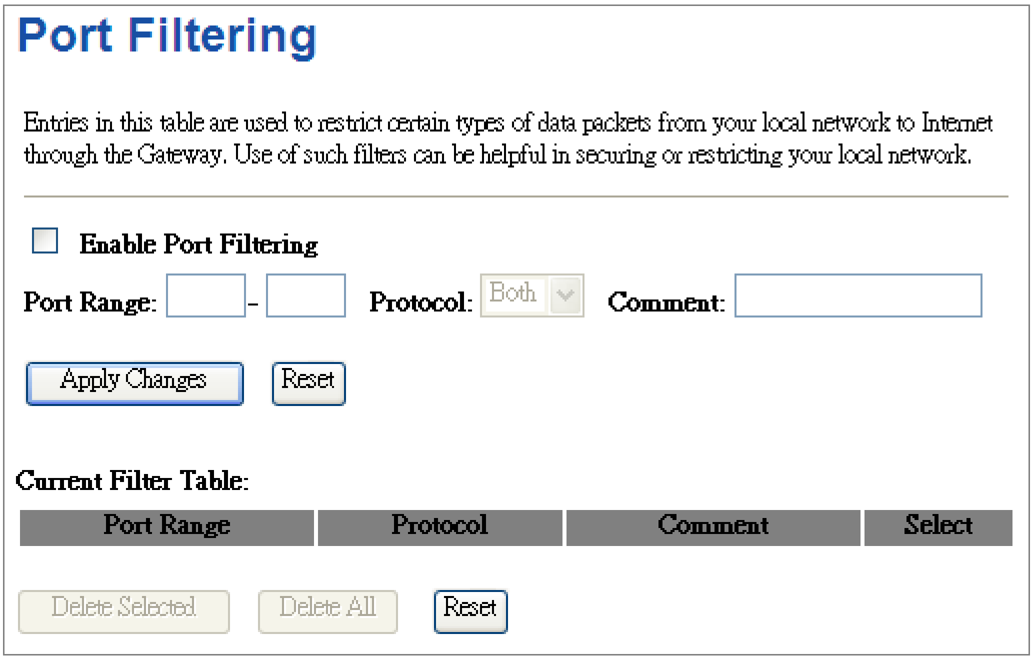


Figure 5-55 Firewall – Main Menu

5.5.1 Port Filtering

Choose menu "**Firewall → Port Filtering**", and you can configure to re-direct a particular range of service port numbers from the Internet network to a particular LAN IP address. It helps users to host some servers behind the firewall. After the configuration, please click the "**Apply Changes**" button to save the settings.



Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable Port Filtering

Port Range: ___ - ___ Protocol: Both Comment: ___

Current Filter Table:

Port Range	Protocol	Comment	Select

Figure 5-6-1 Port Filtering

The page includes the following fields:

Object	Description
Enable Port Filtering	Enable Port Filtering function
Port Range	Add ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Protocol	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocol

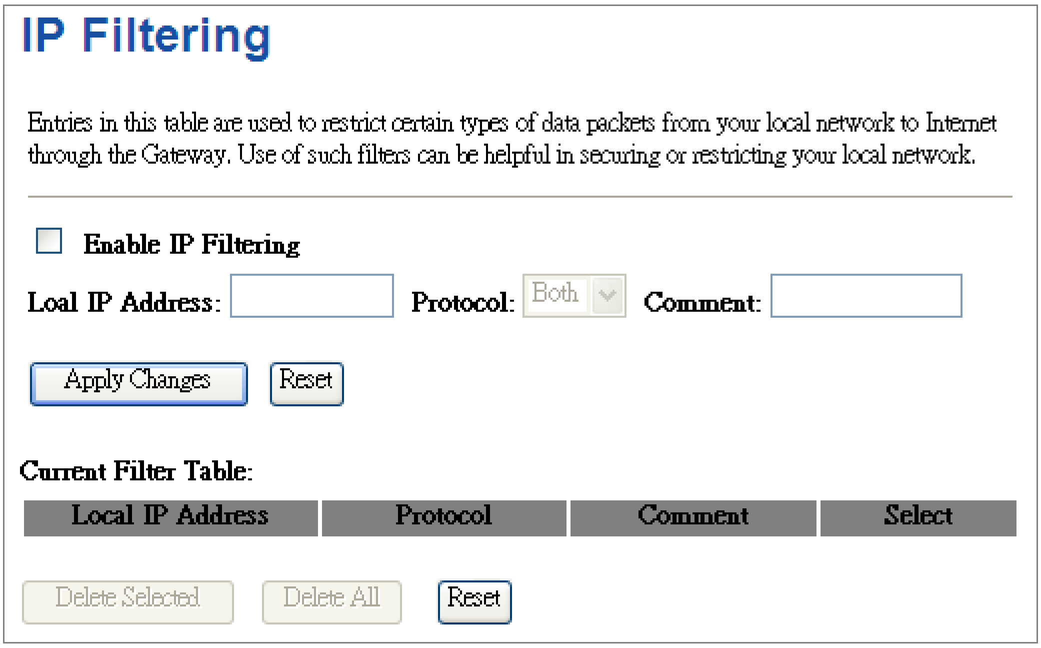
Comment	The description of this setting

Check the "**Select**" box of which rule you want to delete, and then click the "**Delete Selected**" button to delete it.

5.5.2 IP Filtering

IP Filtering is used to block internet or network access to **specific IP addresses** on your local network. The restricted user may still be able to login to the network but will not be able to access the internet. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the user you wish to block.

Choose menu "**Firewall → IP Filtering**", and you can configure which IP address and protocol to be restricted. After the configuration, please click the "**Apply Changes**" button to save the settings.



IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

□ Enable IP Filtering

Loal IP Address: [ ] Protocol: Both Comment: [ ]

Current Filter Table:

Local IP Address	Protocol	Comment	Select

Figure 5-6-1 IP Filtering

The page includes the following fields:

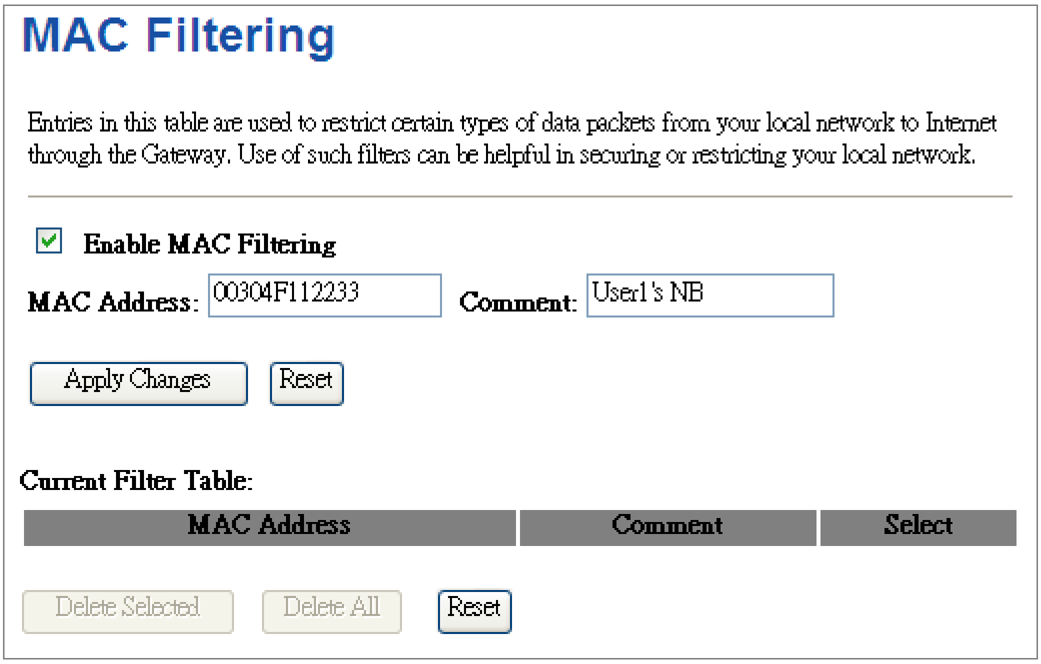
Object	Description
Enable IP Filtering	Check this box to enable IP Filter function
Local IP Address	Add LAN IP address you want to control
Protocol	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocol
Comment	The description of this setting

Check the "**Select**" box of which rule you want to delete, and then click the "**Delete Selected**" button to delete it.

5.5.3 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Wireless Router. Use of such filters can be helpful in securing or restricting your local network.

Choose menu “**Security Setup→ MAC Filter**”, and you can configure which computer of the specified MAC address to be restricted. After the configuration, please click the “**Apply Changes**” button to save the settings.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☑ Enable MAC Filtering

MAC Address: 00304F112233 Comment: User1's NB

Current Filter Table:

MAC Address	Comment	Select

Figure 5-7-4 MAC Filtering

The page includes the following fields:

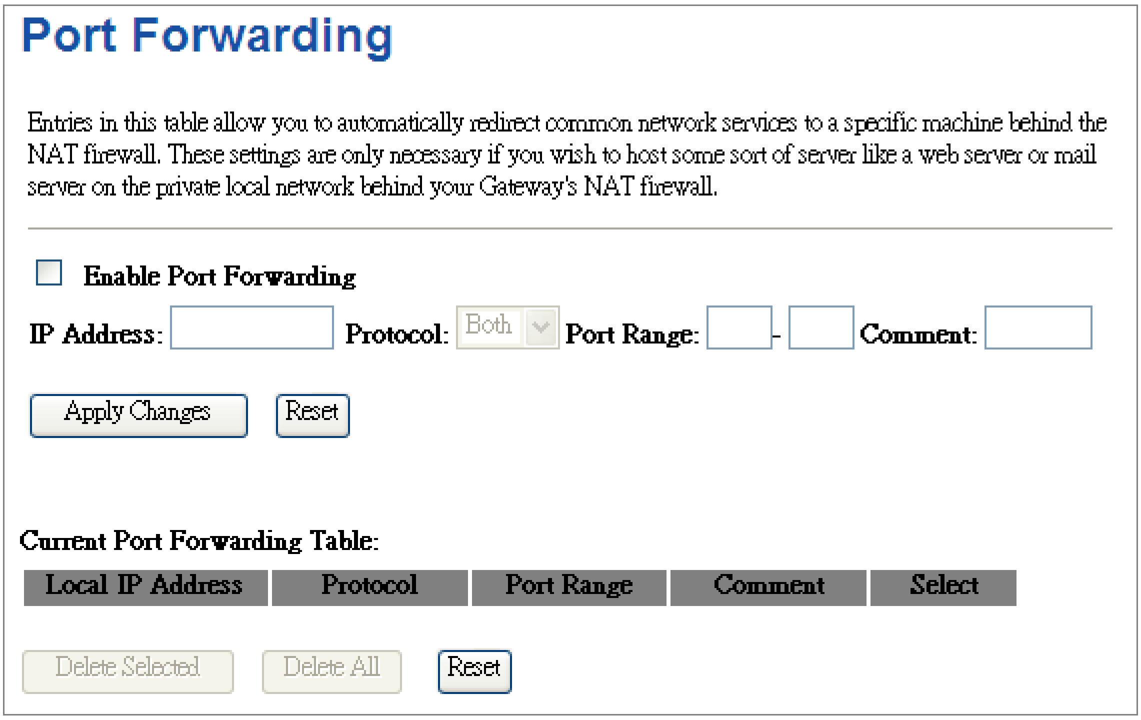
Object	Description
Enable MAC Filtering	Enable MAC filtering
MAC Address	Add MAC address you want to control. You can add maximum 20 MAC Addresses in the table.
Comment	The description of this setting

Check the “**Select**” box of which rule you want to delete, and then click the “**Delete Selected**” button to delete it.

5.5.4 Port Forwarding

Choose menu "**Firewall → Port Forwarding**", and you can configure to re-direct a particular range of service port numbers from the Internet network to a particular LAN IP address. It helps users to host some servers behind the firewall.

After the configuration, please click the "**Apply Changes**" button to save the settings.



Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

□ Enable Port Forwarding

IP Address: ____ Protocol: Both Port Range: ____ - ____ Comment: ____

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select

Figure 5-6-1 Port Forwarding

The page includes the following fields:

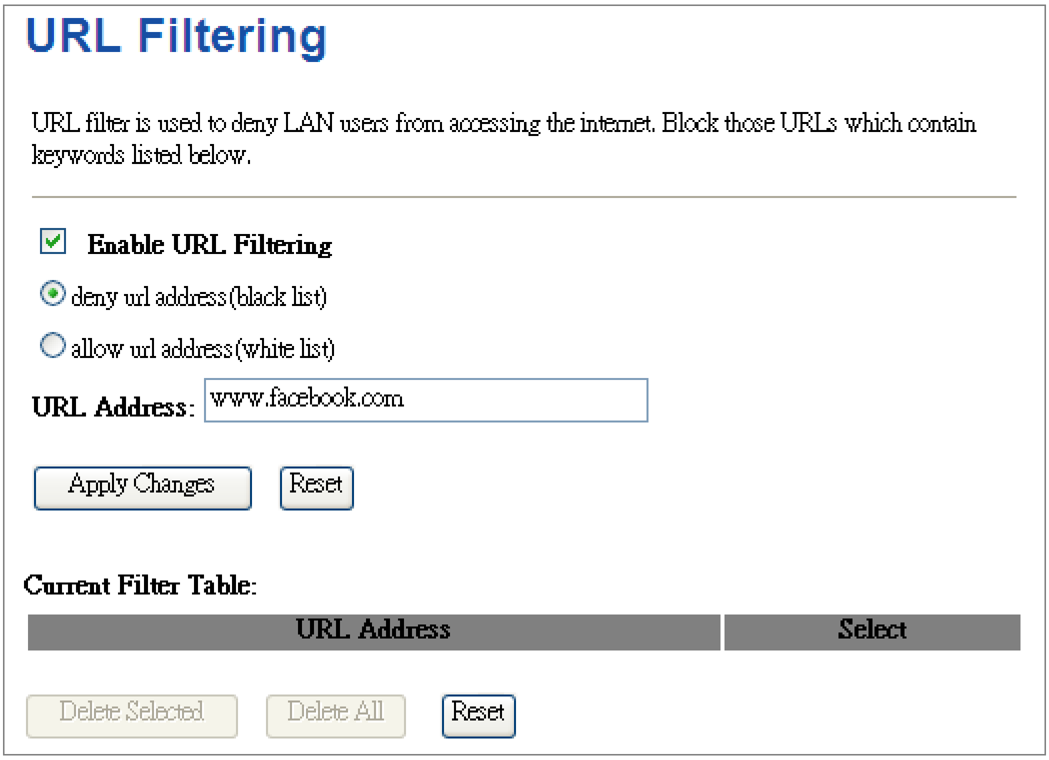
Object	Description
Enable Port Forwarding	Enable Port Forwarding function
IP Address	Add **LAN IP address** of specified host or server on the private local network
Protocol	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocol
Port Range	Add ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.
Comment	The description of this setting

Check the "**Select**" box of which rule you want to delete, and then click the "**Delete Selected**" button to delete it.

5.5.5 URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Choose menu “**Firewall → URL Filtering**”, and you can configure which URL addresses to be blocked. After the configuration, please click the “**Apply Changes**” button to save the settings.



URL Filtering

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

☑ **Enable URL Filtering**

● deny url address(black list)

○ allow url address(white list)

URL Address: www.facebook.com

Current Filter Table:

URL Address	Select

Figure 5-7-3 URL Filtering

The page includes the following fields:

Object	Description
Enable URL Filtering:	Check this box to enable URL Filter function.
IP Address:	The IP Address that you want to filter.
URL Address:	The URL Address that you want to filter.

Check the “**Select**” box of which rule you want to delete, and then click the “**Delete Selected**” button to delete it.

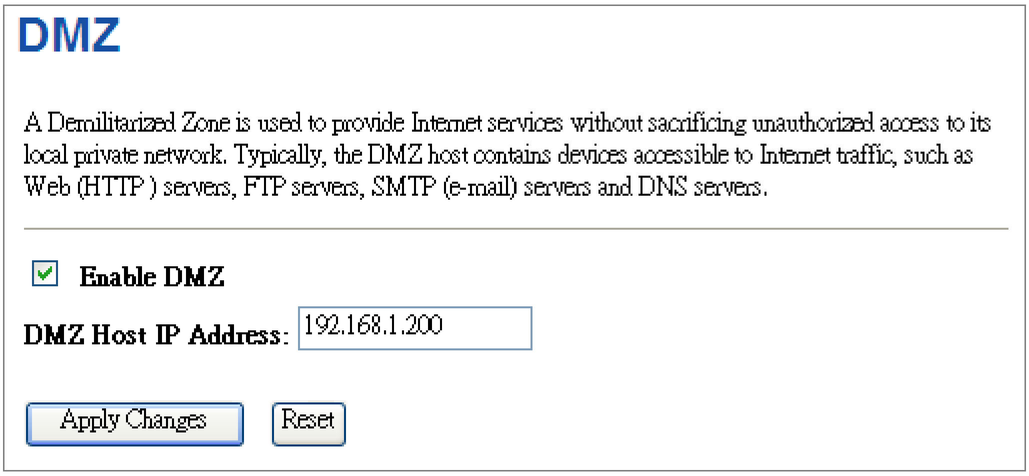
Note

If you wish to block www.facebook.com, simply type in "facebook" and the Wireless AP/Router will block all websites with the text "facebook" in the URL.

5.5.6 DMZ

This page allows you to set a **De-militarized Zone (DMZ)** to separate internal network and Internet.

Choose menu “**Firewall → DMZ**”, and you can configure the private IP address of DMZ. The DMZ feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video conferencing. After the configuration, please click the “**Apply Changes**” button to save the settings.



DMZ

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

☑ Enable DMZ

DMZ Host IP Address: 192.168.1.200

Figure 5-6-2 DMZ

The page includes the following fields:

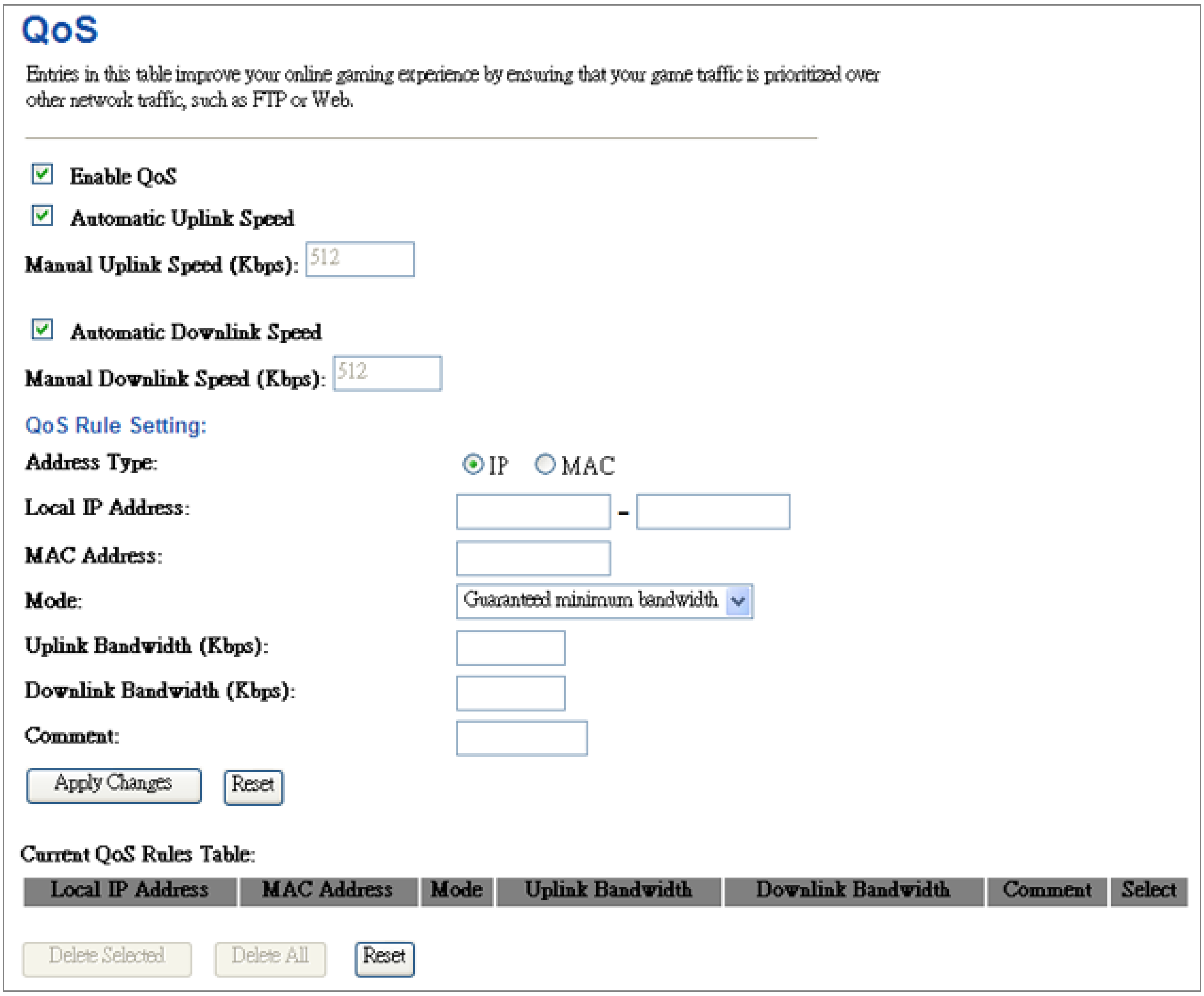
Object	Description
Enable DMZ	Check the box to enable DMZ function. If the DMZ Host Function is enabled, it means that you set up DMZ host at a particular computer to be exposed to the Internet so that some applications/software, especially Internet / online game can have two way connections.
DMZ Host IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port / Public IP address above.

5.6 QoS

The **QoS (Quality of Service)** helps improve your network gaming performance by prioritizing applications. By default the bandwidth control are disabled and application priority is not classified automatically. In order to complete this settings, please follow the steps below.

1. Enable this function.
2. Enter the total speed or choose automatic mode.
3. Enter the IP address or MAC address user want to control.
4. Specify how to control this PC with this IP address or MAC address, including maximum or minimum bandwidth, priority and its up/down speed.

After the configuration, please click the "**Apply Changes**" button to save the settings.



QoS

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

☑ Enable QoS

☑ Automatic Uplink Speed

Manual Uplink Speed (Kbps): 512

☑ Automatic Downlink Speed

Manual Downlink Speed (Kbps): 512

QoS Rule Setting:

Address Type: ● IP ○ MAC

Local IP Address: -

MAC Address:

Mode: Guaranteed minimum bandwidth

Uplink Bandwidth (Kbps):

Downlink Bandwidth (Kbps):

Comment:

Current QoS Rules Table:

Local IP Address	MAC Address	Mode	Uplink Bandwidth	Downlink Bandwidth	Comment	Select

Figure 5-9-1 QoS

The page includes the following fields:

Object	Description
Enable QoS	Check the box to enable the QoS function.
Automatic Uplink Speed	Check the box to adjust the uplink speed automatically by the WNAP-6315. Or enter the uplink data rate manually in the field below.
Automatic Downlink Speed	Check the box to adjust the downlink speed automatically by the WNAP-6315. Or enter the downlink data rate manually in the field below.
QoS Rule Setting	To set the priority rule, you can appoint the computer by **IP** address or **MAC** address, and enter it in the correct field. Select **minimum** or **maximum** bandwidth, and then fill the **uplink** and **downlink** data rate into the field.

5.7 Management

This section focuses on how to maintain AP, including Restore to Factory Default Setting, Backup/Restore, Firmware Upgrade, Reboot, Password Change and Syslog.

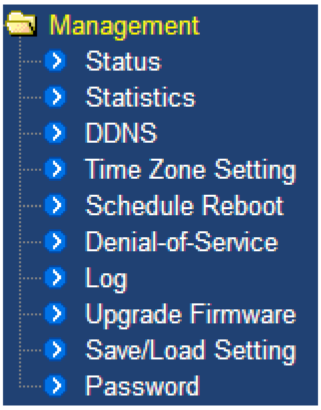
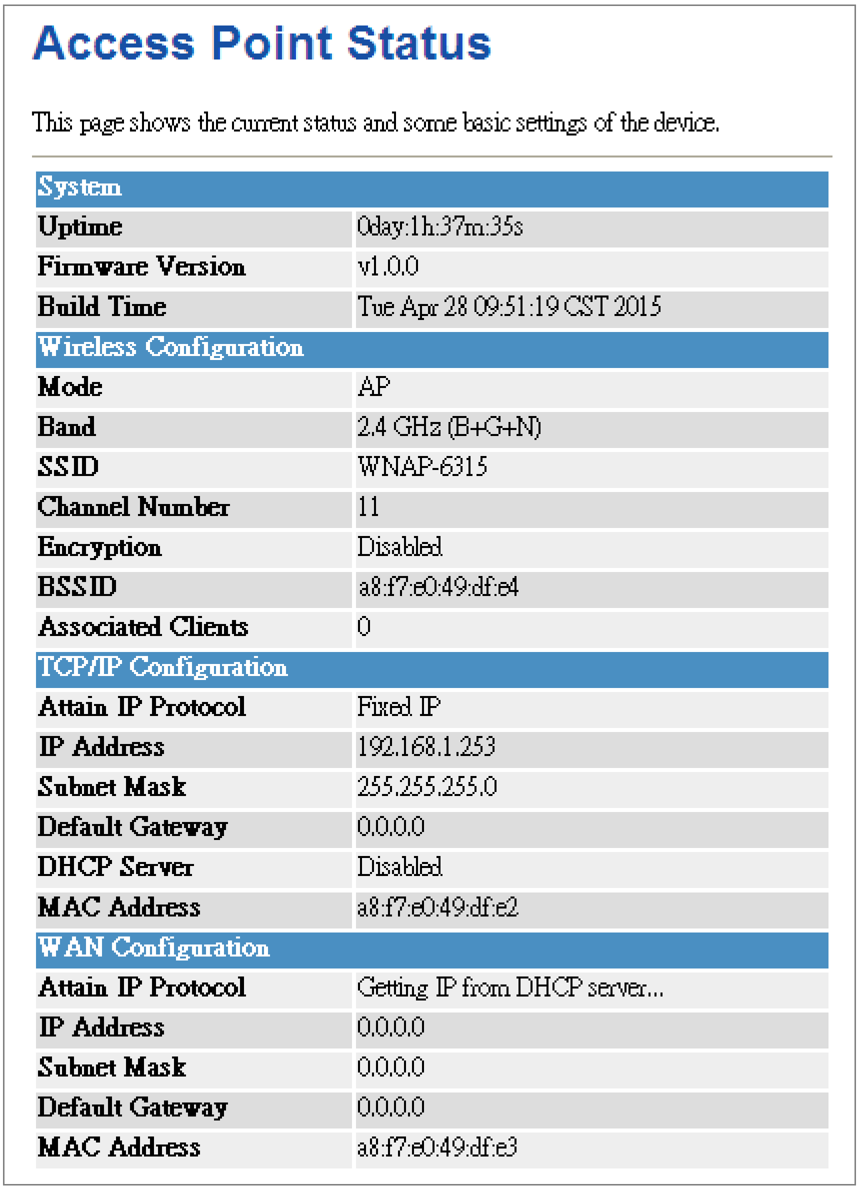


Figure 5-56 Management – Main Menu

5.7.1 Status

You can use this function to realize the instantaneous information of the Wireless AP. The Information displayed here may vary on different configurations.

Choose menu “**Management → Status**” to show the current status and some basic settings of the WNAP-6315.



Access Point Status

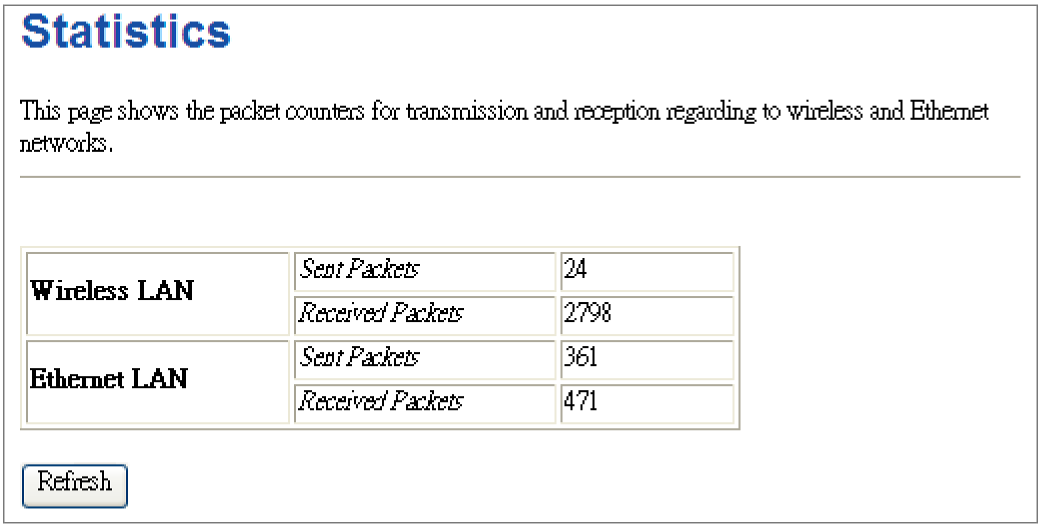
This page shows the current status and some basic settings of the device.

System	
Uptime	0day:1h:37m:35s
Firmware Version	v1.0.0
Build Time	Tue Apr 28 09:51:19 CST 2015
Wireless Configuration	
Mode	AP
Band	2.4 GHz (B+G+N)
SSID	WNAP-6315
Channel Number	11
Encryption	Disabled
BSSID	a8:f7:e0:49:df:e4
Associated Clients	0
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.253
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	a8:f7:e0:49:df:e2
WAN Configuration	
Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	a8:f7:e0:49:df:e3

Figure 5-57 Status

5.7.2 Statistics

Choose menu “**Management → Statistics**” to show the packet counters for transmission and reception regarding wireless and Ethernet network.



Statistics

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	*Sent Packets*	24
	Received Packets	2798
Ethernet LAN	*Sent Packets*	361
	Received Packets	471

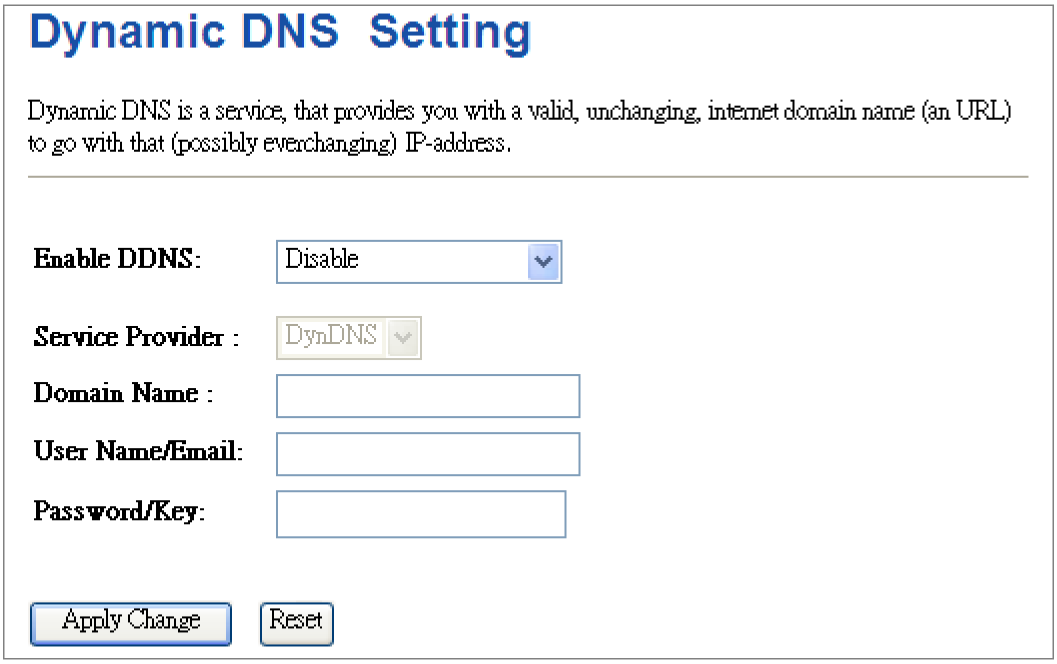
Figure 5-58 Statistics

The page includes the following fields:

Object	Description
Wireless LAN ***Sent Packets***	It shows the statistic count of sent packets on the wireless LAN interface.
Wireless LAN ***Received Packets***	It shows the statistic count of received packets on the wireless LAN interface.
Ethernet LAN ***Sent Packets***	It shows the statistic count of sent packets on the Ethernet LAN interface.
Ethernet LAN ***Received Packets***	It shows the statistic count of received packets on the Ethernet LAN interface.
Refresh	Click the refresh the statistic counters on the screen.

5.7.3 DDNS (Dynamic DNS Settings)

Enable “**Operation Mode**” → “**Gateway**” or “**Wireless ISP**” mode and then enter the “**DDNS**” page by choosing menu “**Management → DDNS**”. This section allows you to configure the DDNS settings.



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS:	Disable
Service Provider :	DynDNS
Domain Name :	
User Name/Email:	
Password/Key:	

Figure 5-59 Dynamic DNS Settings

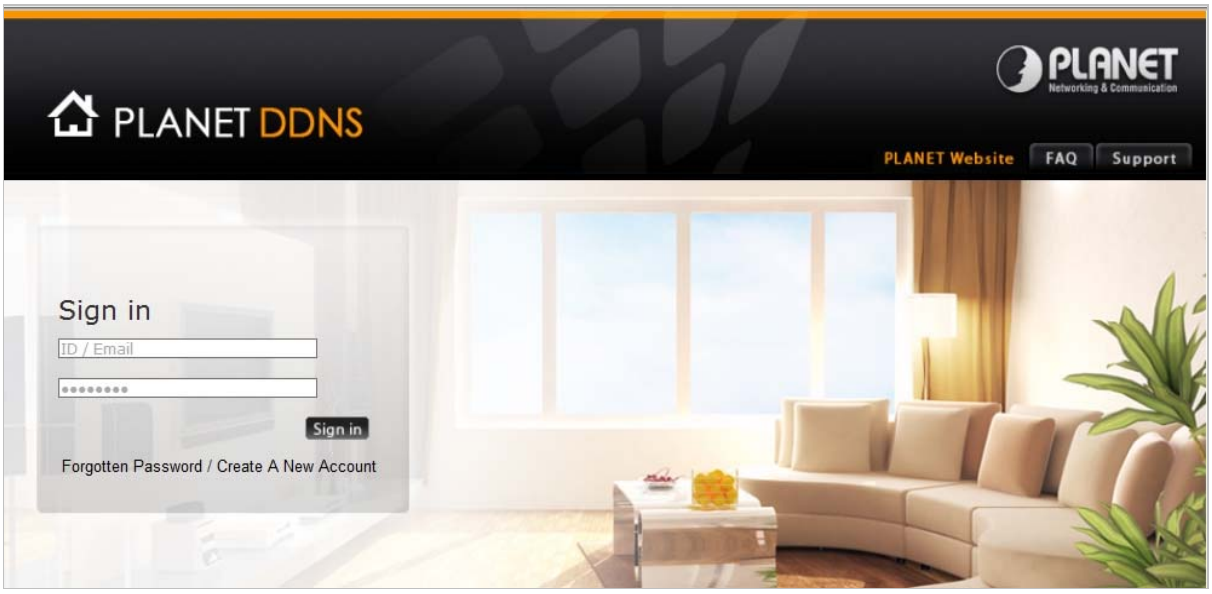
Object	Description
• **Enable DDNS**	**Disable:** Disable DDNS function **Enable Easy DDNS:** Enable PLANET Easy DDNS **Enable Dynamic DDNS:** You are allowed to modify the DDNS settings.
• **Service Provider**	Select a server provider or disable the existing server.
• **Domain Name**	Enter the host name or domain name provided by DDNS provider.
• **Account**	Enter the DDNS user name of the DDNS account.
• **Password**	Enter the DDNS password of the DDNS account.

Example of Planet DDNS Settings:

Note

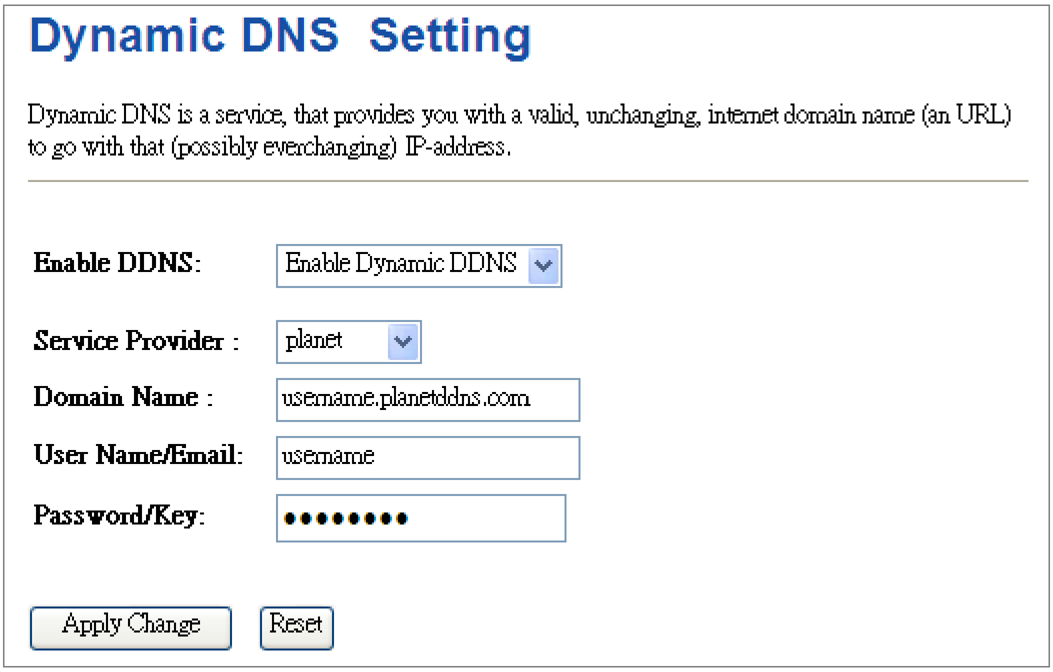
Please go to http://www.planetddns.com/ to register a Planet DDNS account.

Please refer to the FAQ (http://www.planetddns.com/index.php/faq) for how to register a free account.


PLANET DDNS
PLANET Networking & Communication
PLANET Website
FAQ
Support
Sign in
ID / Email
••••••••
Sign in
Forgotten Password / Create A New Account

Enable “**Operation Mode**” → “**Gateway**” or “**Wireless ISP**” mode and then enter the “**DDNS**” page by choosing menu “**Management → DDNS**”.

Step 1. Select “**Enable Dynamic DDNS**” and “**PlanetDDNS.com**” from the list of Dynamic DNS Provider to use the Planet DDNS service.



Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS:	Enable Dynamic DDNS
Service Provider :	planet
Domain Name :	username.planetddns.com
User Name/Email:	username
Password/Key:	•••••••••

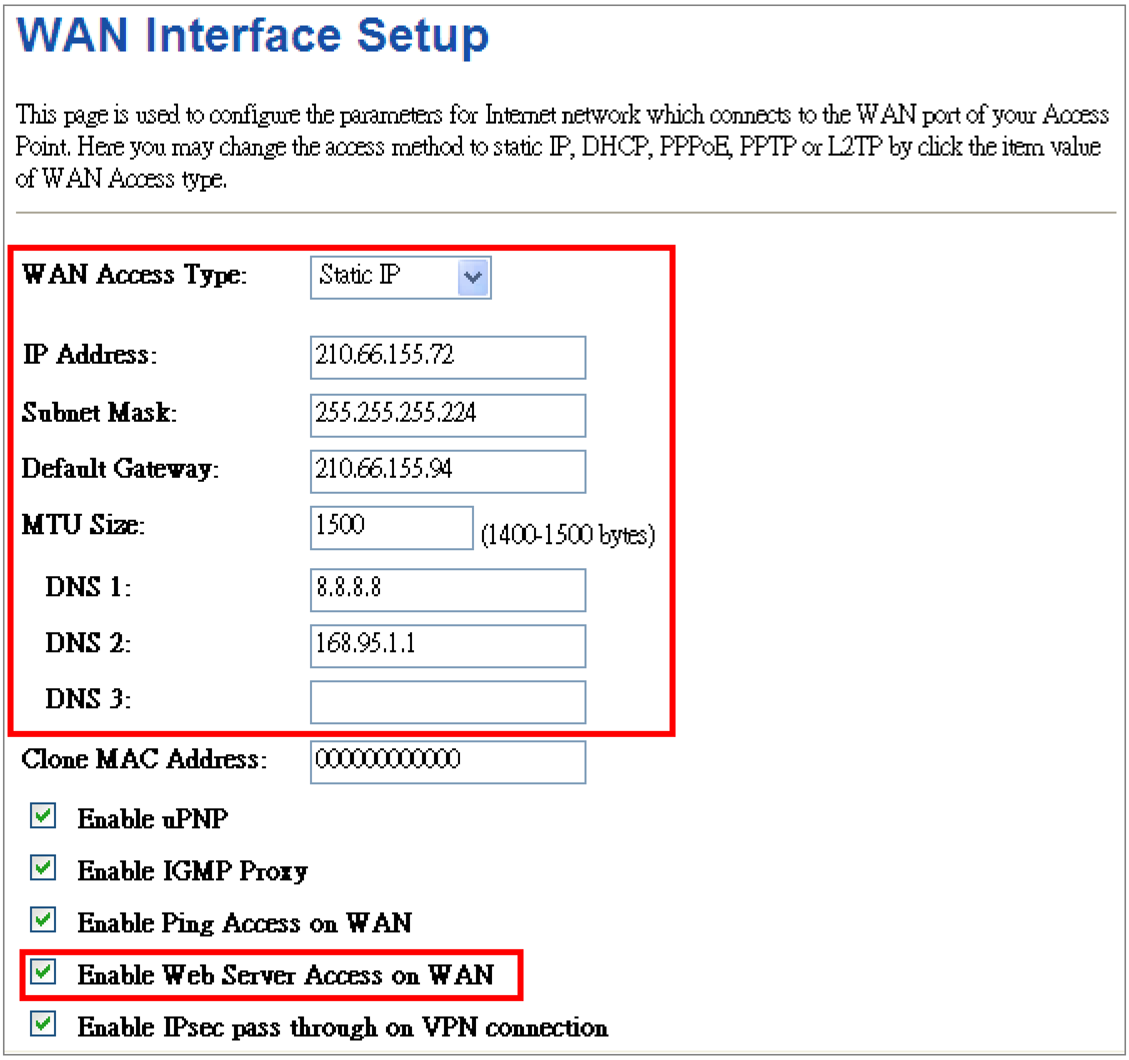
Step 2. Configure the DDNS account that has been registered in Planet DDNS website.

Domain Name: Enter your DDNS host (format: xxx.planetddns.com, xxx is the registered domain name)

User Name/Email: Enter your registered DDNS user name.

Password: Enter the password of your account.

Step 3. Go to “**TCP/IP Settings → WAN Interface Setup**” to enable Web Server Access on WAN port and configure WAN connection to Static IP (fixed IP).



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 210.66.155.72

Subnet Mask: 255.255.255.224

Default Gateway: 210.66.155.94

MTU Size: 1500 (1400-1500 bytes)

DNS 1: 8.8.8.8

DNS 2: 168.95.1.1

DNS 3:

Clone MAC Address: 000000000000

☑ **Enable uPNP**

☑ **Enable IGMP Proxy**

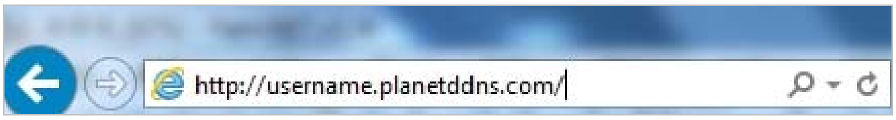
☑ **Enable Ping Access on WAN**

☑ **Enable Web Server Access on WAN**

☑ **Enable IPsec pass through on VPN connection**

Step 4. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable.

In a remote computer, enter the DDNS host name as the figure shown below. Then, you should be able to login the WNAP-6315 remotely.



http://username.planetddns.com/

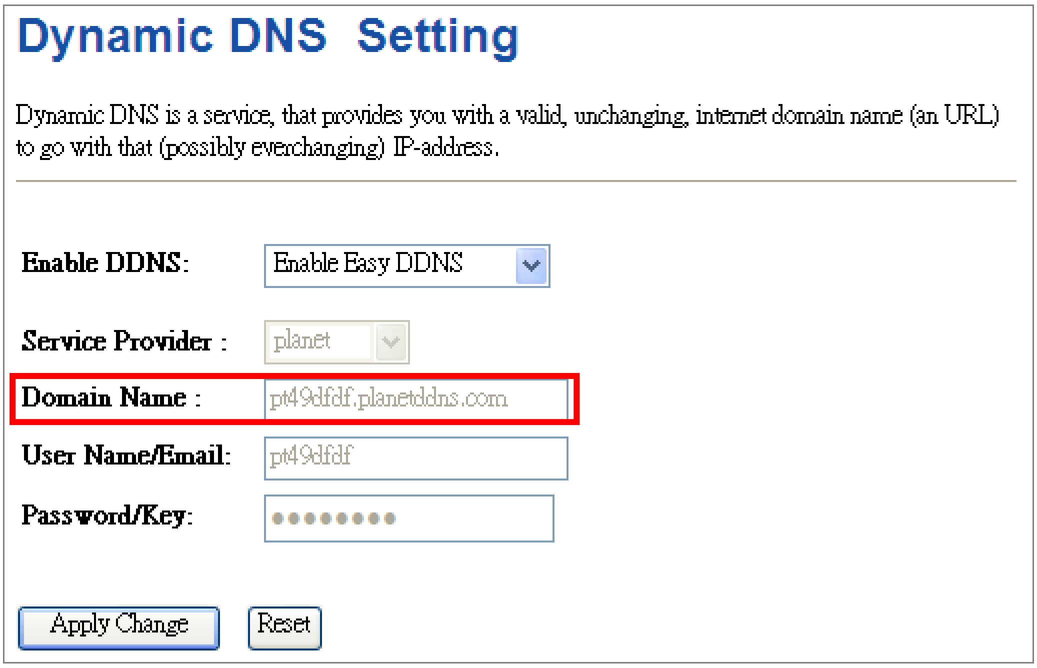
Example of Easy DDNS Settings:

> Note
>
> This service is not required to register any DDNS account.

Please refer to the procedure listed as follows to configure using Planet Easy DDNS service.

Step 1. Select “**Enable Easy DDNS**” to use the Planet Easy DDNS service.

Domain Name: Display the specified domain name for this device. (Format: ptxxxxxx.planetddns.com, xxxxxx is the last six-digit of the WAN Port MAC address)

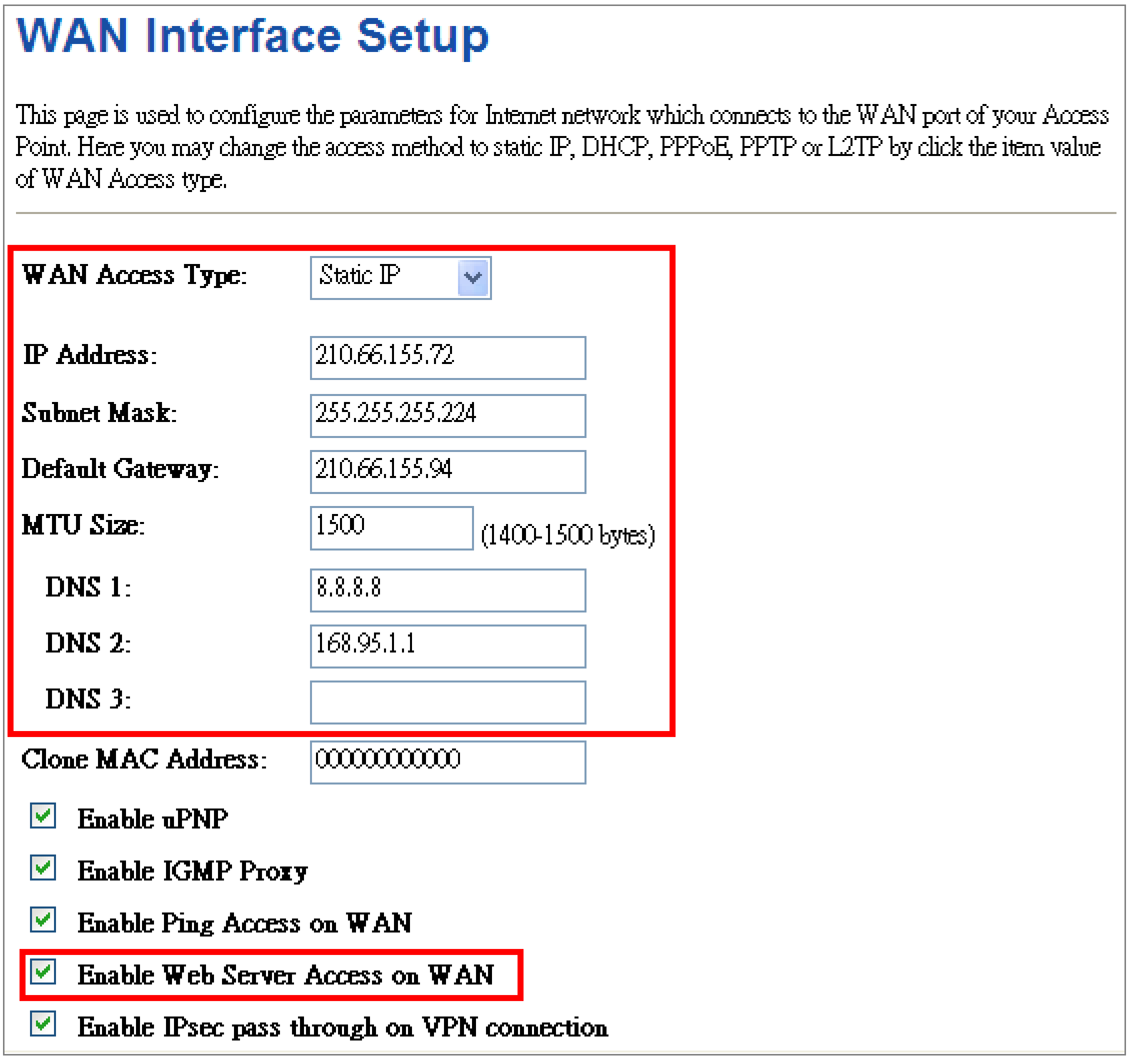


Dynamic DNS Setting

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

Enable DDNS:	Enable Easy DDNS
Service Provider :	planet
Domain Name :	pt49dfdf.planetddns.com
User Name/Email:	pt49dfdf
Password/Key:	••••••••

Step 2. Go to “**TCP/IP Settings → WAN Interface Setup**” to enable Web Server Access on WAN port and configure WAN connection to Static IP (fixed IP).



WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE, PPTP or L2TP by click the item value of WAN Access type.

WAN Access Type:	Static IP
IP Address:	210.66.155.72
Subnet Mask:	255.255.255.224
Default Gateway:	210.66.155.94
MTU Size:	1500 (1400-1500 bytes)
DNS 1:	8.8.8.8
DNS 2:	168.95.1.1
DNS 3:	
Clone MAC Address:	000000000000

☑ Enable uPNP

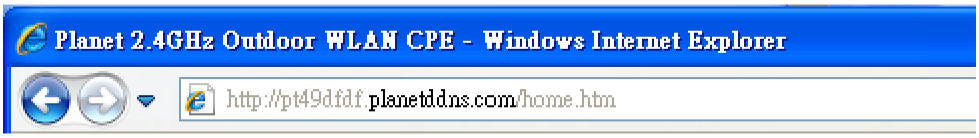
☑ Enable IGMP Proxy

☑ Enable Ping Access on WAN

☑ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

Step 3. Save the setting and connect your WAN port of the Wireless AP to the internet via Ethernet cable. In a remote computer, enter the Easy Domain Name displayed in **Step 1**. Then, you should be able to login the WNAP-6315 remotely.



Planet 2.4GHz Outdoor WLAN CPE - Windows Internet Explorer

http://pt49dfdf.planetddns.com/home.htm

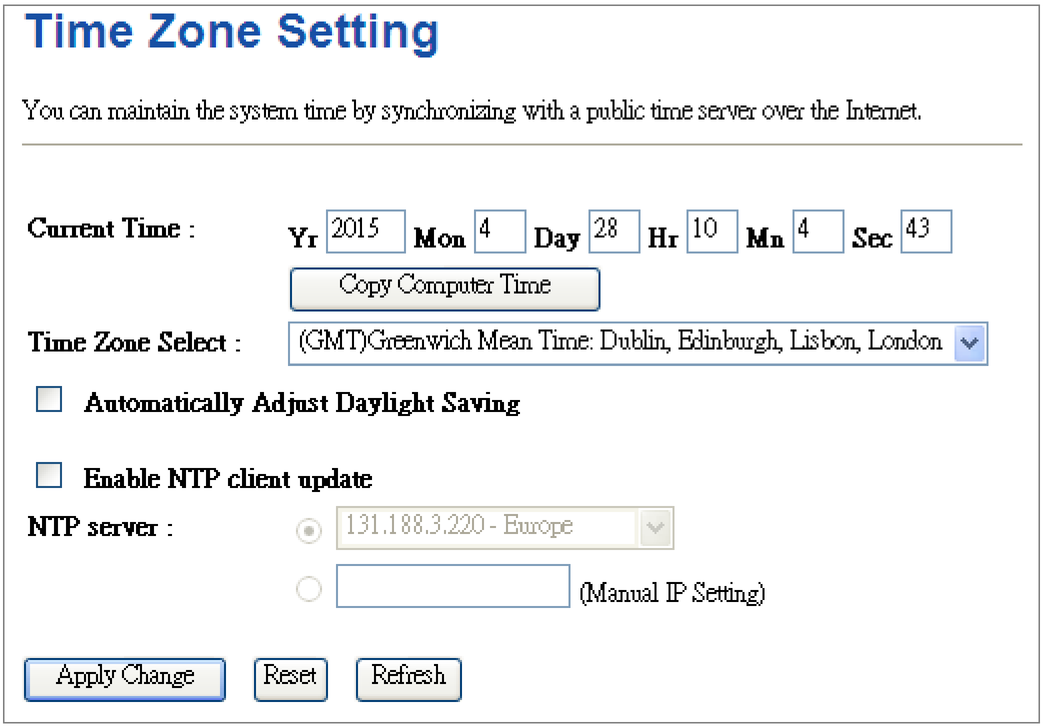
5.7.4 Time Zone Setting

This section assists you in setting the Wireless AP's system time. You can either select to set the time and date manually or automatically obtain the GMT time from Internet.

Choose menu "**Management → Time Zone Setting**" to configure the system time. You can also maintain the system time by synchronizing with a public time server over the Internet. After the configuration, please click the "**OK**" button to save the settings.

Note

The configured time and date settings are lost when the Wireless AP is powered off.



Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

Current Time : Yr 2015 Mon 4 Day 28 Hr 10 Mn 4 Sec 43

Time Zone Select : (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

□ Automatically Adjust Daylight Saving

□ Enable NTP client update

NTP server : ● 131.188.3.220 - Europe

○ (Manual IP Setting)

Figure 5-60 Time Zone Settings

The page includes the following fields:

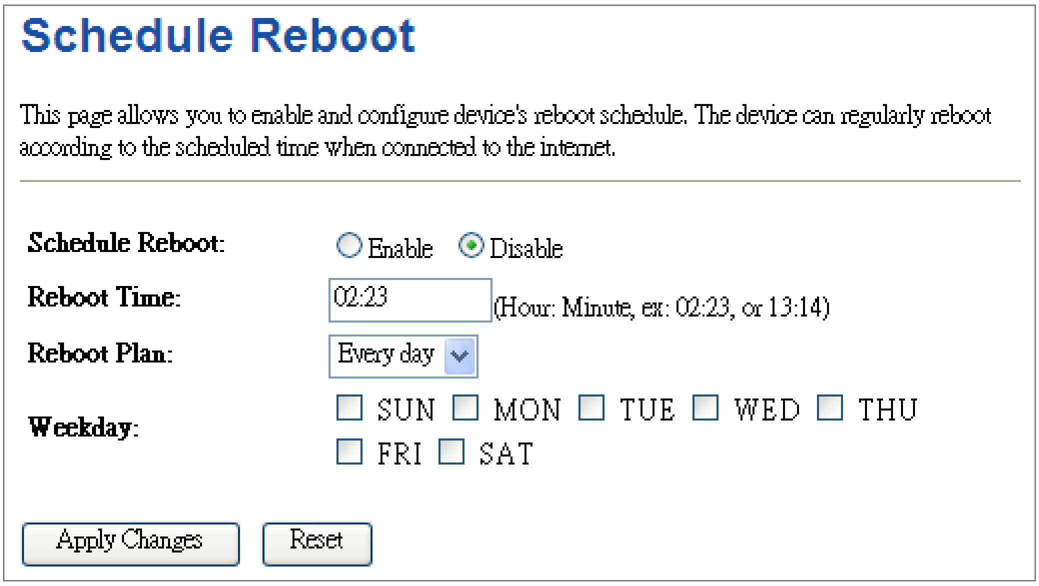
Object	Description
Current Time	Input current time manually. You can click "**Copy Computer Time**" button to copy the PC's current time to the AP.
Time Zone Select	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Automatically Adjust Daylight Saving	Select the time offset, if your location observes daylight saving time.
Enable NTP client update	Check to enable NTP update. Once this function is enabled, AP will automatically update current time from NTP server.
NTP Server	User may select prefer NTP sever or input address of NTP server manually.

Note

If the AP loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the AP, or you must enable the NTP Server option.

5.7.5 Schedule Reboot

This page allows you to enable and configure system reboot schedule. The device can regularly reboot according to the reserved time when connecting to the Internet.



Schedule Reboot

This page allows you to enable and configure device's reboot schedule. The device can regularly reboot according to the scheduled time when connected to the internet.

Schedule Reboot: ○ Enable ● Disable

Reboot Time: 02:23 (Hour: Minute, ex: 02:23, or 13:14)

Reboot Plan: Every day

Weekday: □ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT

Figure 5-61 Schedule Reboot

The page includes the following fields:

Object	Description
Schedule Reboot Setting	Enable or disable the Schedule Reboot function.
Reboot Time	Enter the Reboot Time (24-hour format) to enable this function to take effect.
Reboot Plan	There are two Reboot Plans supported in the AP: **Weekday:** select this option to let the device reboot automatically according to the reserved time in one or more days of a week. **Every day:** select this option to let the device reboot automatically according to the reserved time every day.
Weekday	Check one or more days to let the device auto reboot on schedule. When choosing "Every day" as your reboot plan, the "Weekday" will be grayed out (disabled), which means Every day will auto reboot at the time that you scheduled.

Note

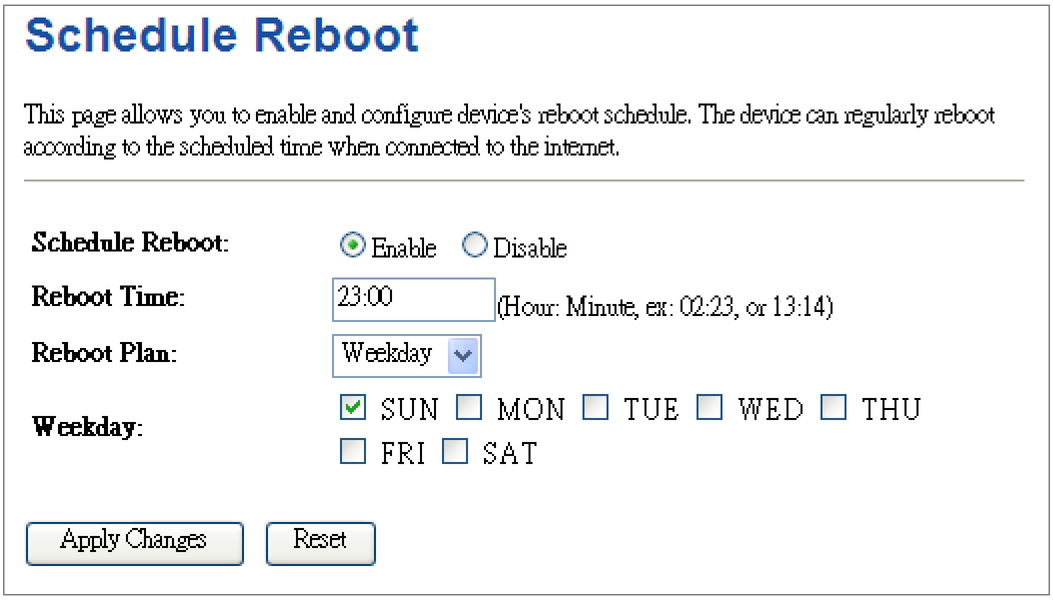
1. This setting will only take effect when the Internet connection is accessible and the GMT time is configured correctly.
2. You must select at least one day when choosing "**Weekday**" as your reboot plan.
3. When choosing "**Every day**" as your reboot plan, the "**Weekday**" will be grayed out (disabled), which means **Every day** will auto reboot at the time that you schedule.

- Example of how to configure **Schedule Reboot**. Please take the following steps:

Before configured schedule reboots, please ensure the Internet connection is accessible and the GMT time is configured correctly according to **NTP Settings** page.

Step 1. Select the Schedule Reboot Setting checkbox.

Step 2. Enter the Reboot Time (24-hour format) to enable this function to take effect. For example, if you want this function to work at 23:00 every Sunday, choose "Weekday" in the Reboot Plan field.



Schedule Reboot

This page allows you to enable and configure device's reboot schedule. The device can regularly reboot according to the scheduled time when connected to the internet.

Schedule Reboot: ● Enable ○ Disable

Reboot Time: 23:00 (Hour: Minute, ex: 02:23, or 13:14)

Reboot Plan: Weekday

Weekday: ☑ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT

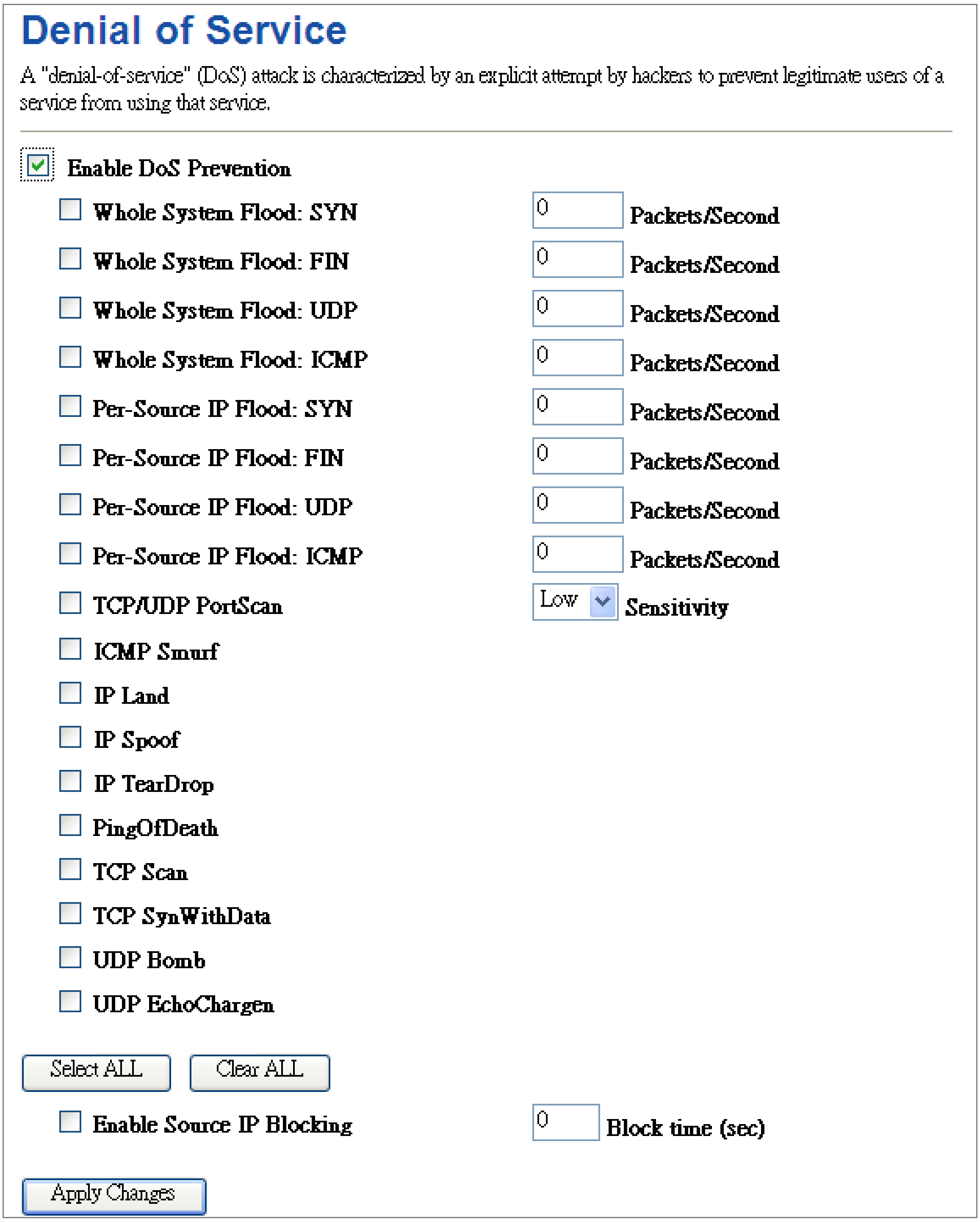
Figure 5-62 Schedule Reboot - Example

Step 3. Click the “Apply Changes” button to take this function effect.

5.7.6 Denial of Service (DoS)

The Wireless Router can prevent specific DoS attacks from entering your network. A "**Denial-of-Service**" (**DoS**) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Choose menu “**Management → Denial-of-Service**” to configure the settings of DoS attack prevention. After the configuration, please click the “**Apply Changes**” button to save the settings.



Denial of Service

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☑ Enable DoS Prevention

□ Whole System Flood: SYN	0	Packets/Second
□ Whole System Flood: FIN	0	Packets/Second
□ Whole System Flood: UDP	0	Packets/Second
□ Whole System Flood: ICMP	0	Packets/Second
□ Per-Source IP Flood: SYN	0	Packets/Second
□ Per-Source IP Flood: FIN	0	Packets/Second
□ Per-Source IP Flood: UDP	0	Packets/Second
□ Per-Source IP Flood: ICMP	0	Packets/Second
□ TCP/UDP PortScan	Low	Sensitivity
□ ICMP Smurf		
□ IP Land		
□ IP Spoof		
□ IP TearDrop		
□ PingOfDeath		
□ TCP Scan		
□ TCP SynWithData		
□ UDP Bomb		
□ UDP EchoChargen		

□ Enable Source IP Blocking 0 Block time (sec)

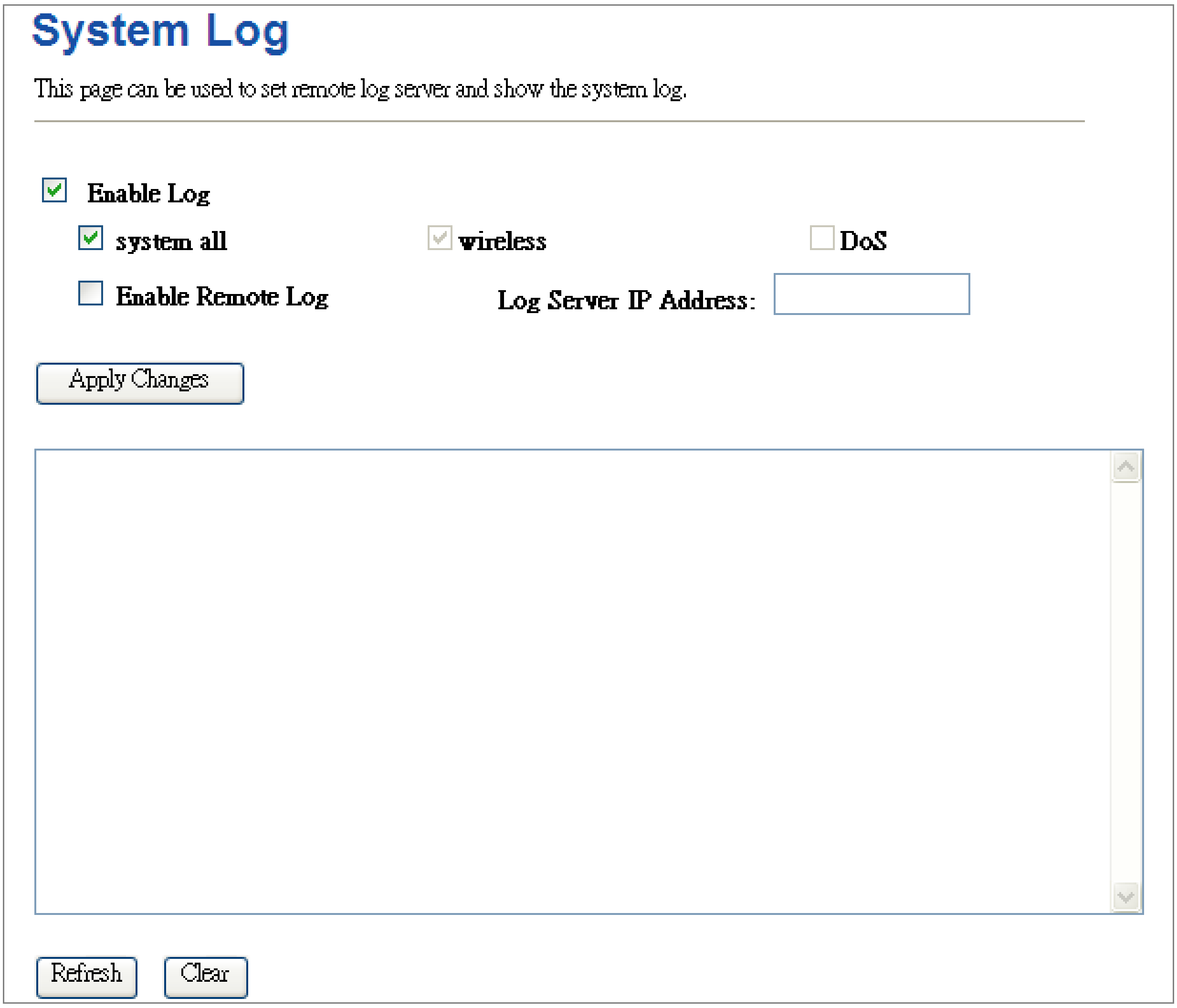
Figure 5-7-6 Denial of Service

The page includes the following fields:

Object	Description
Enable DoS Prevention	Check to enable DoS function. User may set other related configurations about DoS below

5.7.7 LOG

Choose menu "**Management → Log**" to configure the settings of system log. You can check the box of the items you want to record it in the log. After the configuration, please click the "Apply" button to save the settings.



System Log

This page can be used to set remote log server and show the system log.

☑ Enable Log

☑ system all ☑ wireless □ DoS

□ Enable Remote Log Log Server IP Address:

Figure 5-63 System Log

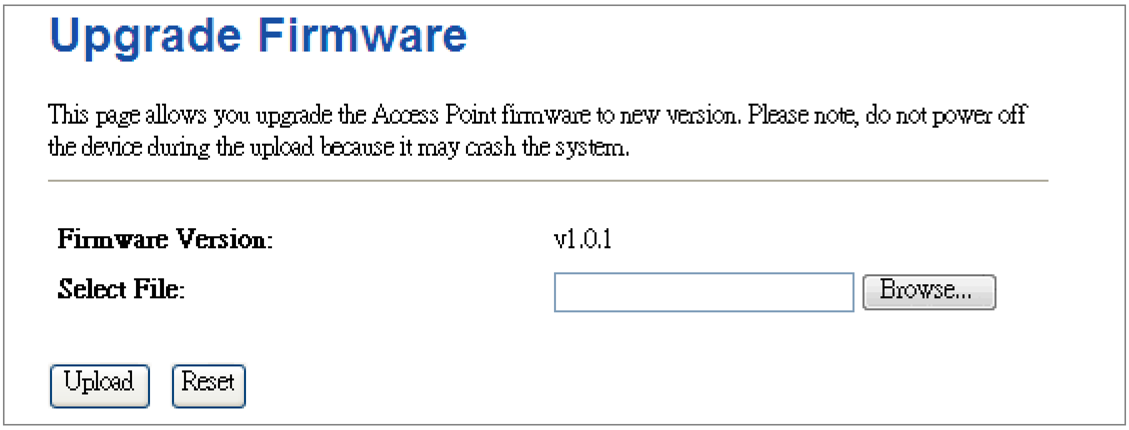
The page includes the following fields:

Object	Description
Enable Log	Check to enable log function.
System all	Check this option to display all the system logs.
Wireless	Check this option to display only the logs related to wireless module.
Enable Remote Log	Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it.
Log Server IP Address	Enter the LAN IP address of the Syslog Server.
Refresh	Click this button to update the log.
Clear	Click this button to clear the current log.

5.7.8 Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Choose menu "**Management → Upgrade Firmware**" to upgrade the firmware of the WNAP-6315. Select the new firmware file downloaded from the PLANET website and then click "**Upload**" button to upgrade it.



Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Firmware Version: v1.0.1

Select File:

Figure 5-64 Upgrade Firmware

The page includes the following fields:

Object	Description
Firmware Version	Display the current firmware version of the AP.
Select File	Browse and select file you want to upgrade and press Upload to perform upgrade. **Please wait till the related information is shown on the screen after upgrade is finished.**

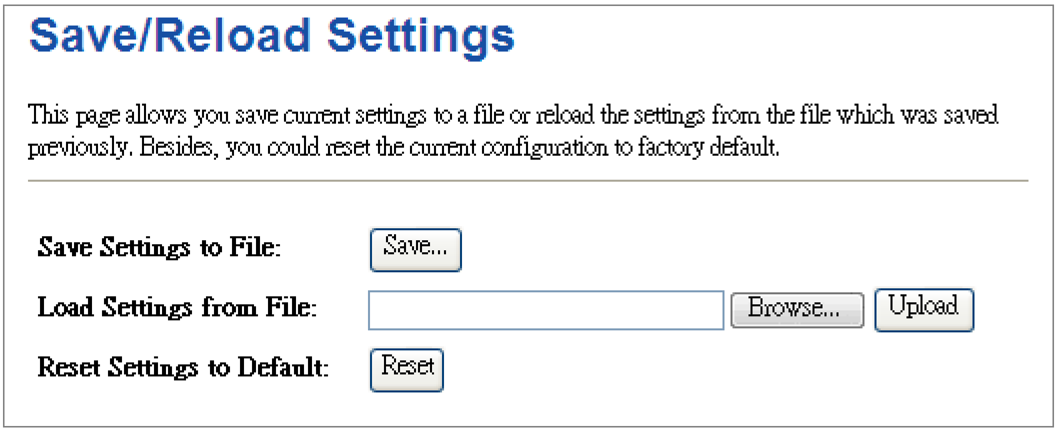
Note

Do not disconnect the Wireless AP from your management PC (the PC you use to configure the device) or power off it during the upgrade process; otherwise, it may be permanently damaged. The Wireless AP will restart automatically when the upgrade process, which takes several minutes, to complete.

5.7.9 Save/Load Setting

Choose menu "**Management → Save/Load Setting**" to back up or reset the configuration of the WNAP-6315.

Once you have configured the Wireless AP the way you want it, you can save these settings to a configuration file on your local hard drive that can later be imported to your Wireless AP in case the device is restored to factory default settings.



Save/Reload Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Figure 5-65 Save/Reload Settings

The page includes the following fields:

Object	Description
Save Settings to File	Click the "**Save…**" button to back up the configuration of the WNAP-6315 and then save the "config.dat" in your computer.
Load Settings from File	Select the configuration file of the WNAP-6315 and then click the "**Upload**" button to reload the configuration back into the WNAP-6315.
Reset Settings to Default	Click the "**Reset**" button to reset all settings of the WNAP-6315 to factory default. **Factory Default Settings:** User Name: **admin** Password: **admin** IP Address: **192.168.1.253** Subnet Mask: **255.255.255.0** Default Gateway: **192.168.1.253** DHCP: **Disabled** SSID: **WNAP-6315** Wireless Security: **None**

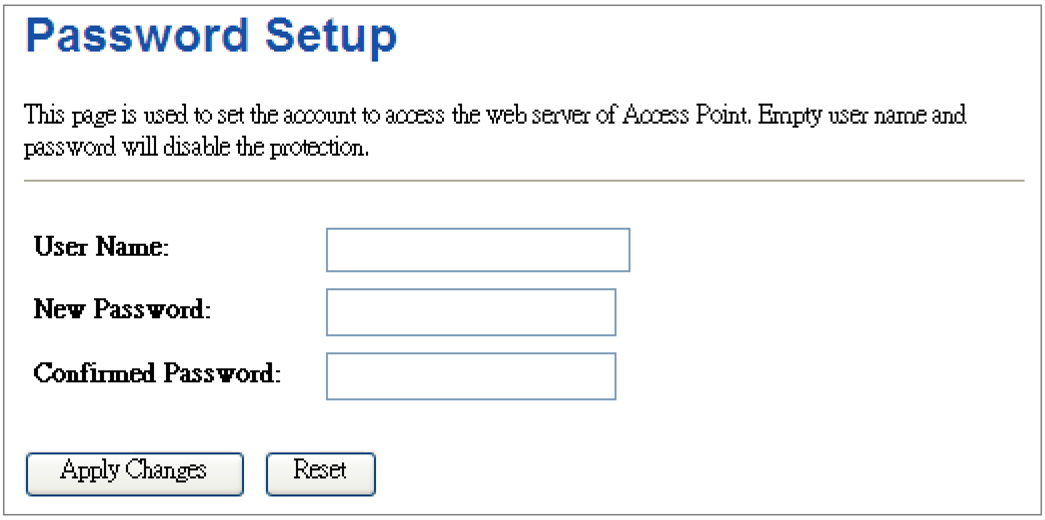
Note

To activate your settings, you need to reboot the Wireless AP after you reset it.

5.7.10 Password

To ensure the Wireless AP's security, you will be asked for your password when you access the Wireless AP's Web-based Utility. The default user name and password are "admin". This page will allow you to add or modify the user name and password.

Choose menu "**Management → Password**" to change the user name and password which is inputted to access the web UI of the WNAP-6315.



Password Setup

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

User Name:

New Password:

Confirmed Password:

Figure 5-66 Password Setup

The page includes the following fields:

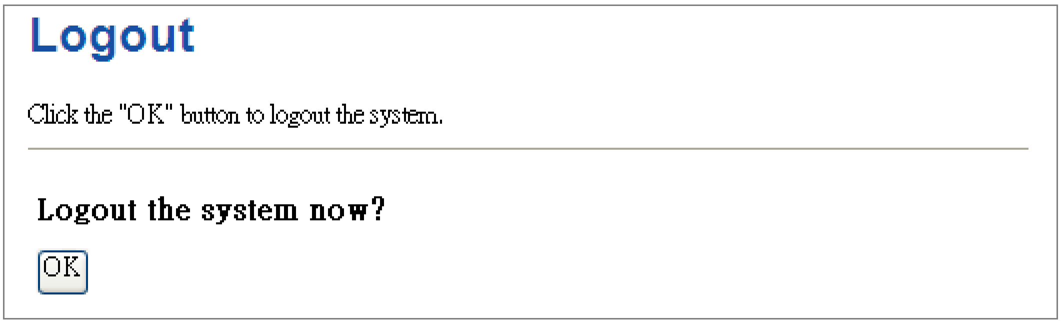
Object	Description
User Name	Enter user name.
New Password	Input password for this user.
Confirmed Password	Confirm password again.

Note

For the sake of security, it is highly recommended that you change default login password and user name.

5.7.11 Logout

To logout the WNAP-6315, please select “**Logout**” from the left-side menu. Then, click “**OK**” to logout.



Logout

Click the "OK" button to logout the system.

Logout the system now?

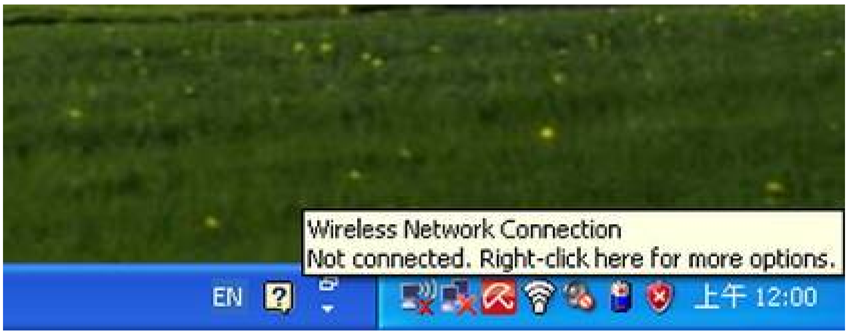
Figure 5-67 Logout

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WNAP-6315 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



Wireless Network Connection
Not connected. Right-click here for more options.

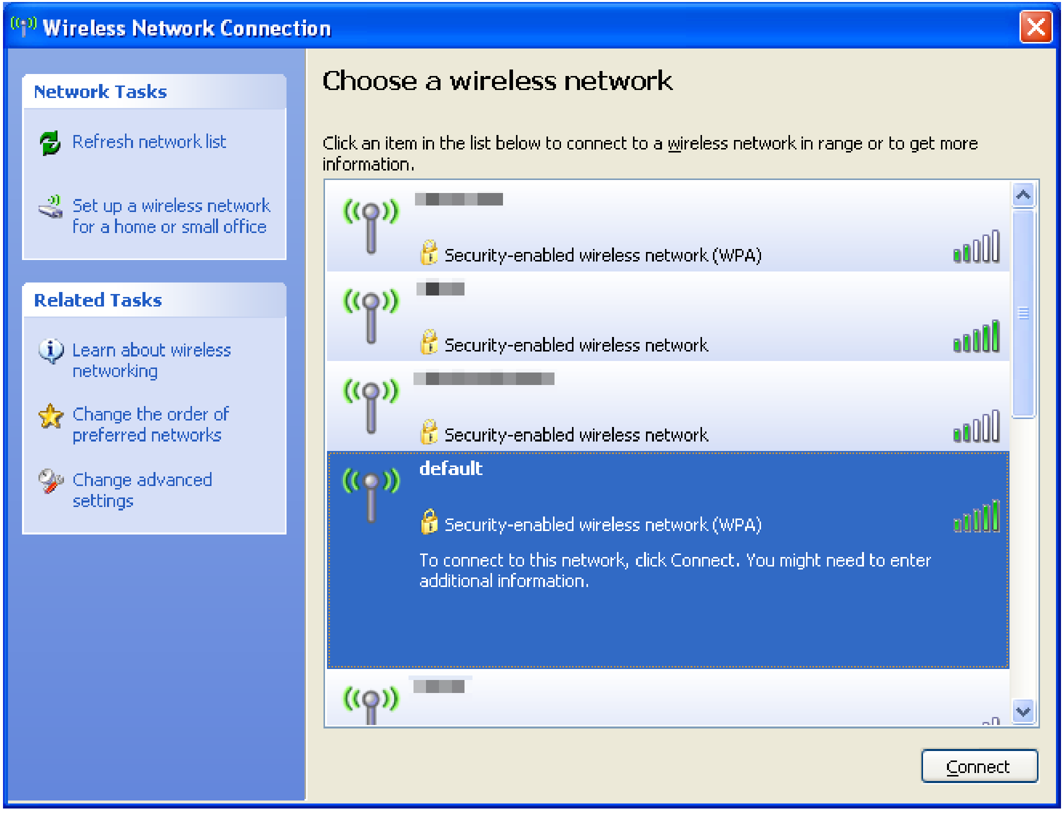
Figure 6-1 System Tray – Wireless Network Icon

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



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Security-enabled wireless network (WPA)

Security-enabled wireless network

Security-enabled wireless network

default

Security-enabled wireless network (WPA)

To connect to this network, click Connect. You might need to enter additional information.

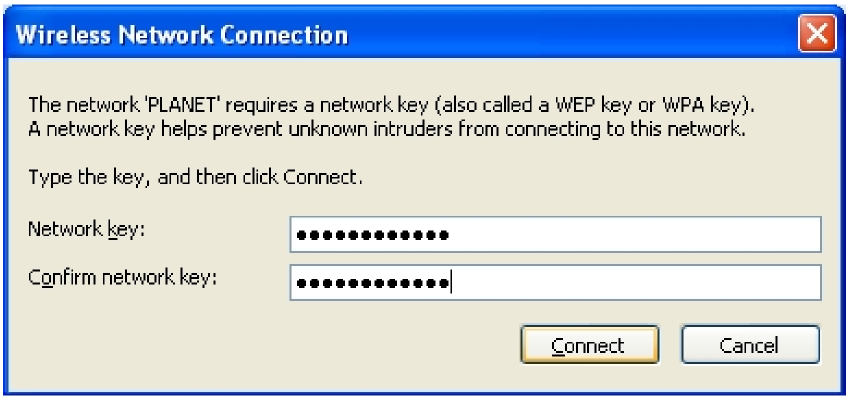
Figure 6-2 Choose a wireless network

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

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that is configured in section 5.4.3

(3) Click the [Connect] button



Wireless Network Connection

The network 'PLANET' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

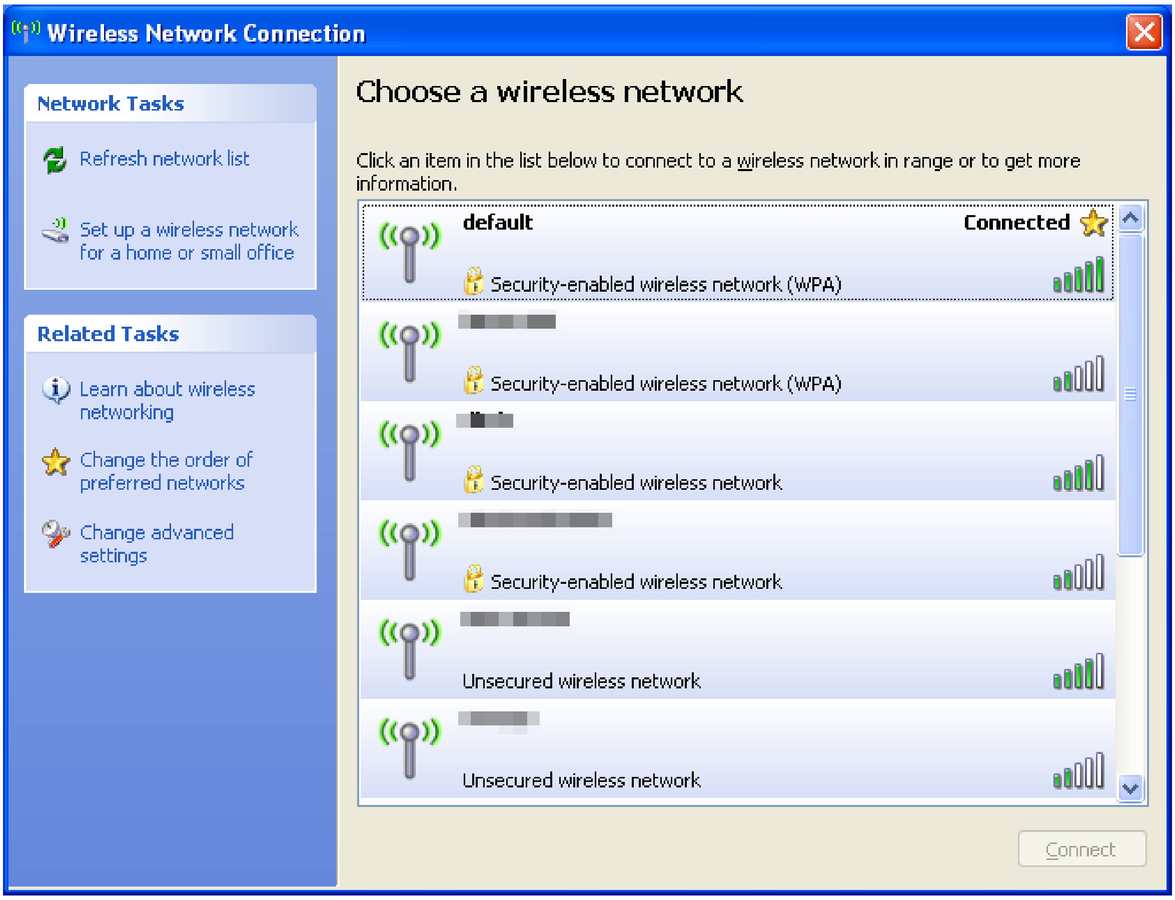
Type the key, and then click Connect.

Network key: ●●●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●●●

Figure 6-3 Enter the network key

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



Wireless Network Connection

Network Tasks

- Refresh network list
- Set up a wireless network for a home or small office

Related Tasks

- Learn about wireless networking
- Change the order of preferred networks
- Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

default — **Connected**
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network

[redacted]
Security-enabled wireless network

[redacted]
Unsecured wireless network

[redacted]
Unsecured wireless network

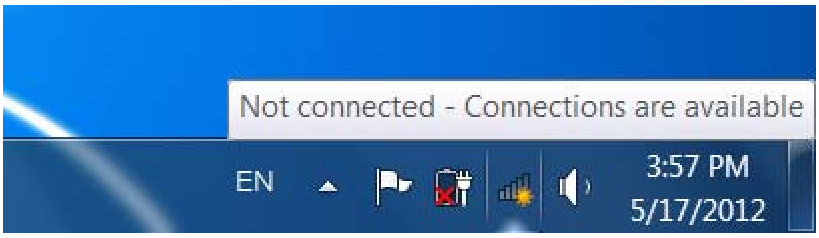
Figure 6-4 Choose a wireless network -- Connected

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



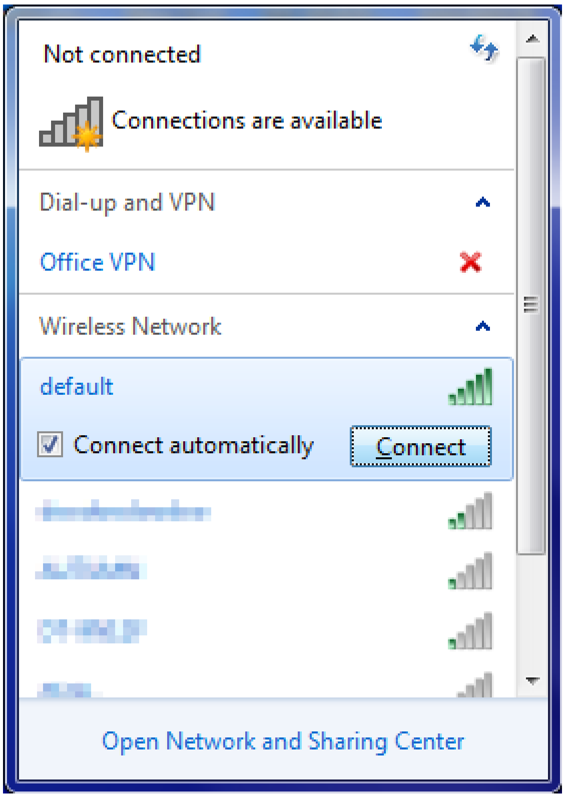
Not connected - Connections are available

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



Not connected

Connections are available

Dial-up and VPN

Office VPN

Wireless Network

default

☑ Connect automatically

Figure 6-6 WLAN AutoConfig

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

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

(1) The Connect to a Network box will appear

(2) Enter the encryption key that is configured in section 5.4.3

(3) Click the [OK] button

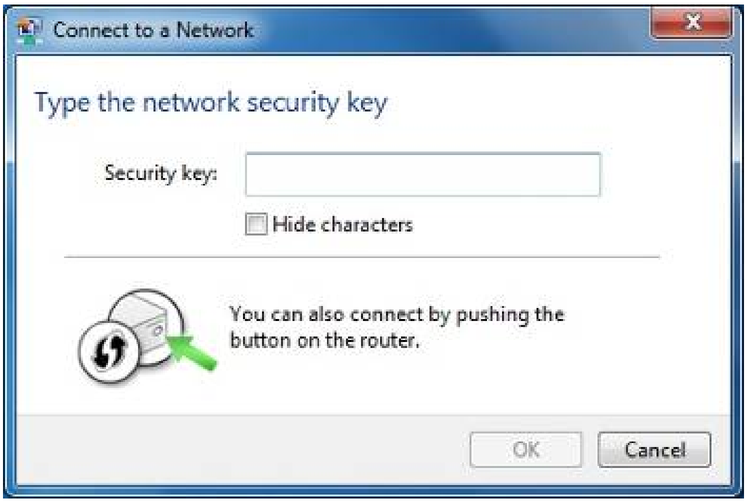

Connect to a Network
Type the network security key
Security key:
□ Hide characters
You can also connect by pushing the button on the router.
OK
Cancel

Figure 6-7 Type the network key

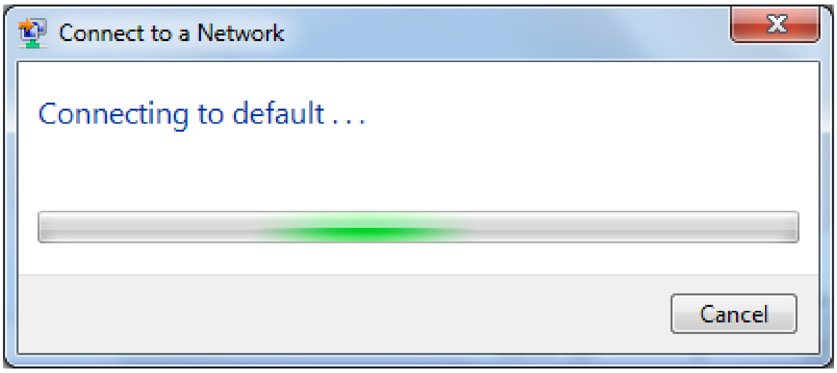
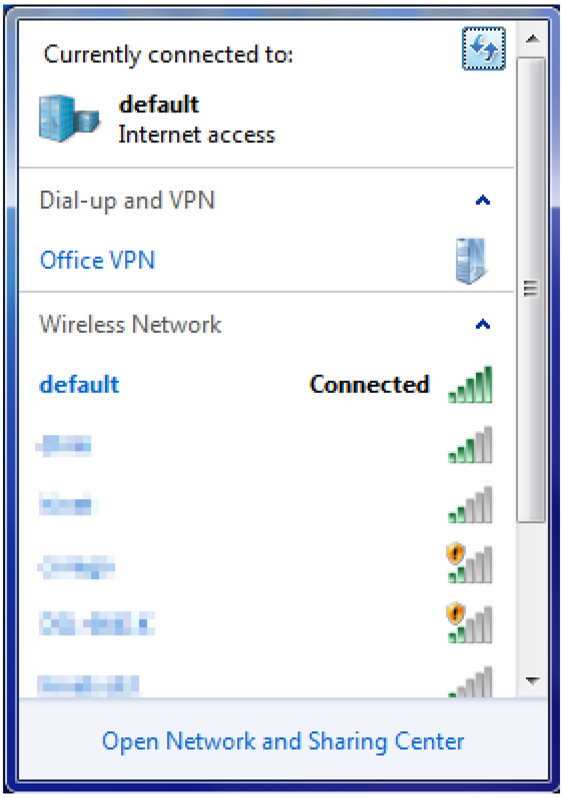


Figure 6-8 Connecting to a Network

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



Currently connected to:

default
Internet access

Dial-up and VPN

Office VPN

Wireless Network

default **Connected**

Open Network and Sharing Center

Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the WNAP-6315 is configured to “default”.

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

The AirPort Network Connection menu will appear

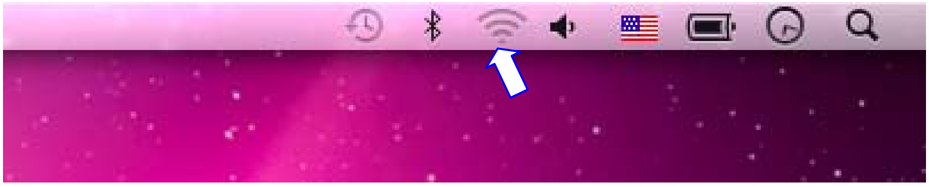


Figure 6-10 Mac OS – Network icon

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

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

(2) Double-click on the selected SSID

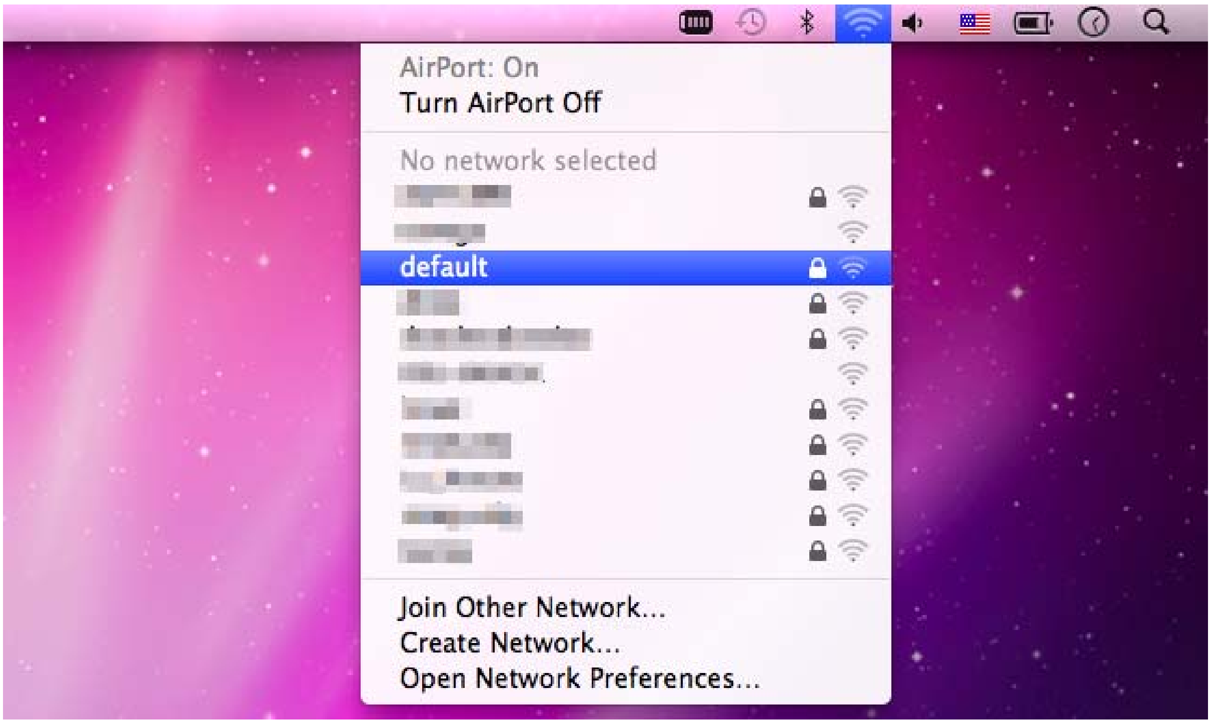
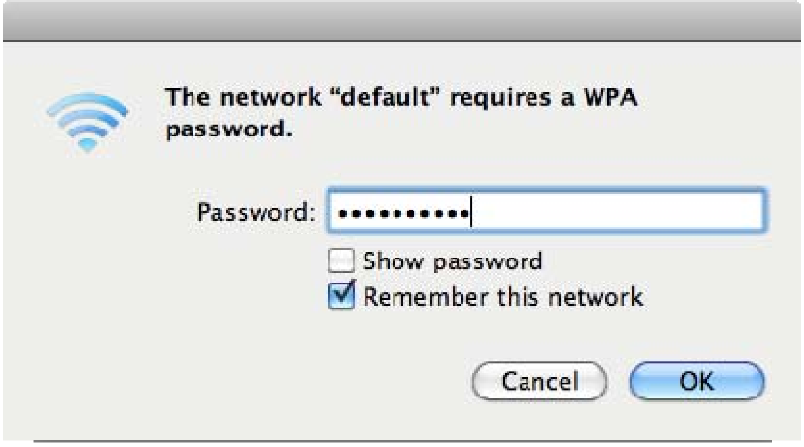


Figure 6-11 Highlight and select the wireless network

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

(1) Enter the encryption key that is configured in section 5.4.3

(2) Click the [OK] button



The network "default" requires a WPA password.

Password: ••••••••••

Figure 6-12 Enter the Password

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

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

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

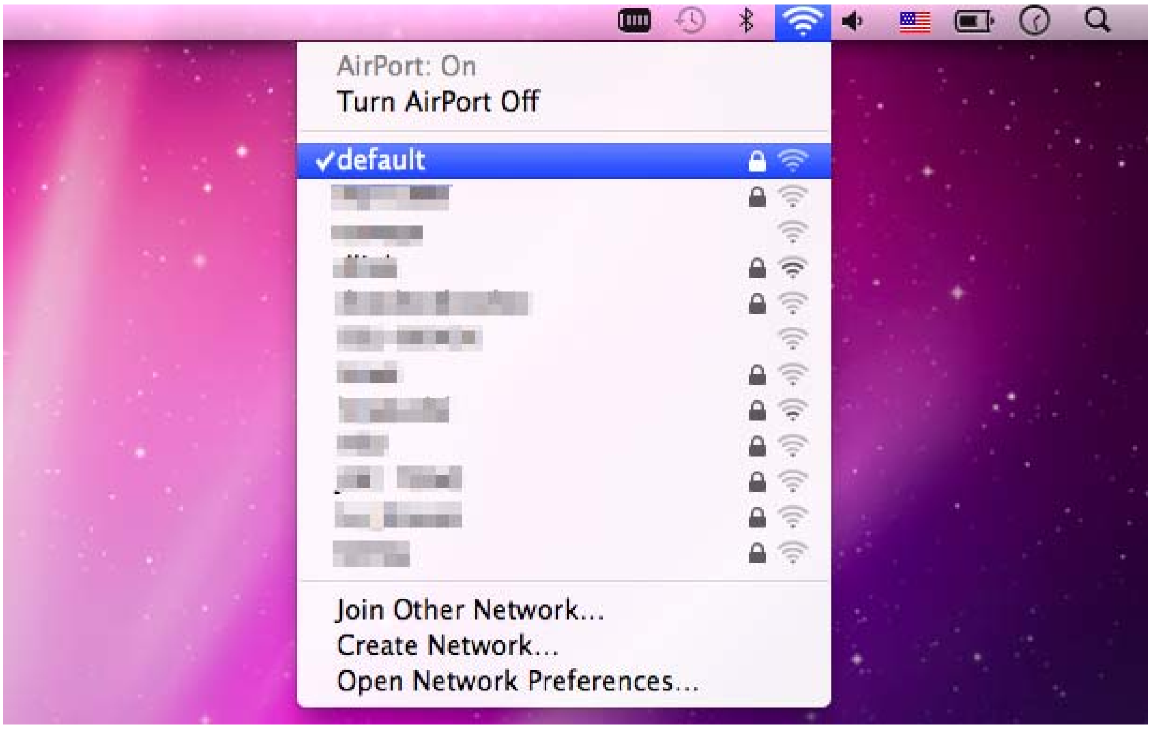


Figure 6-13 Connected to the Network

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

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

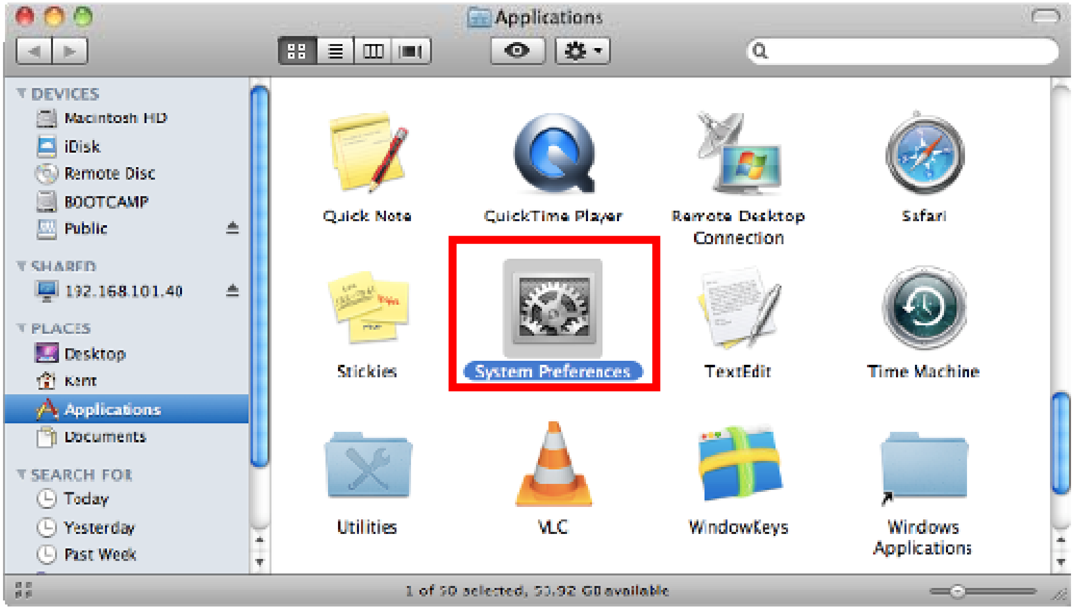


Figure 6-14 System Preferences

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

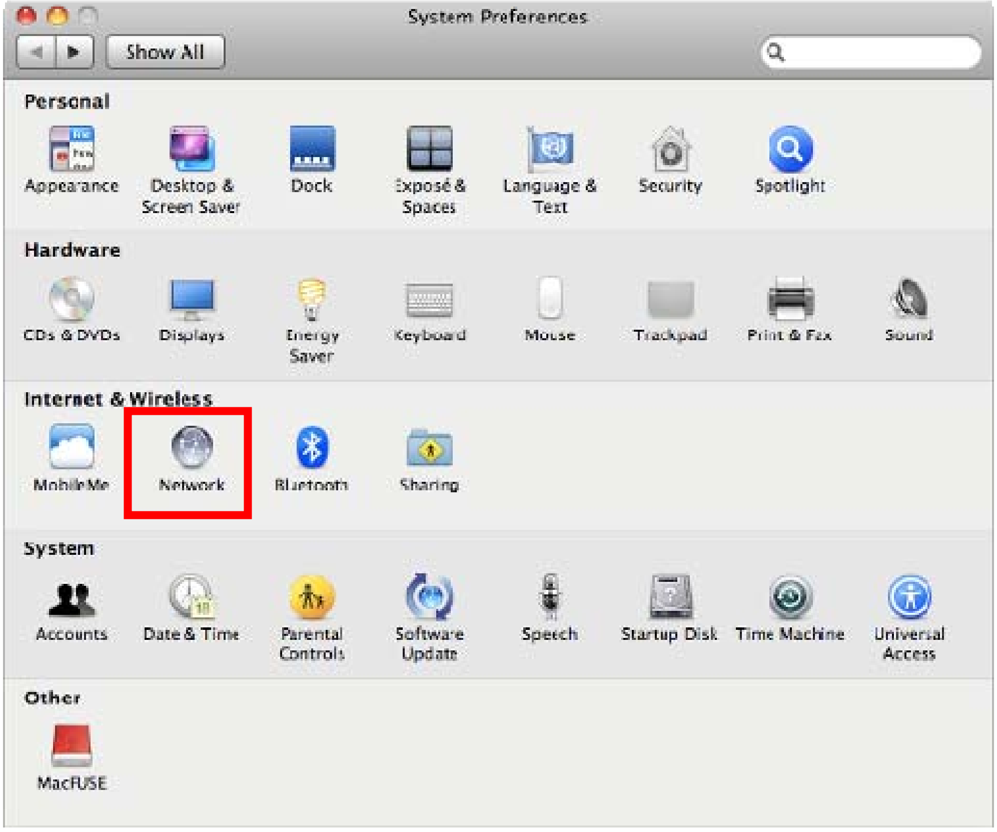


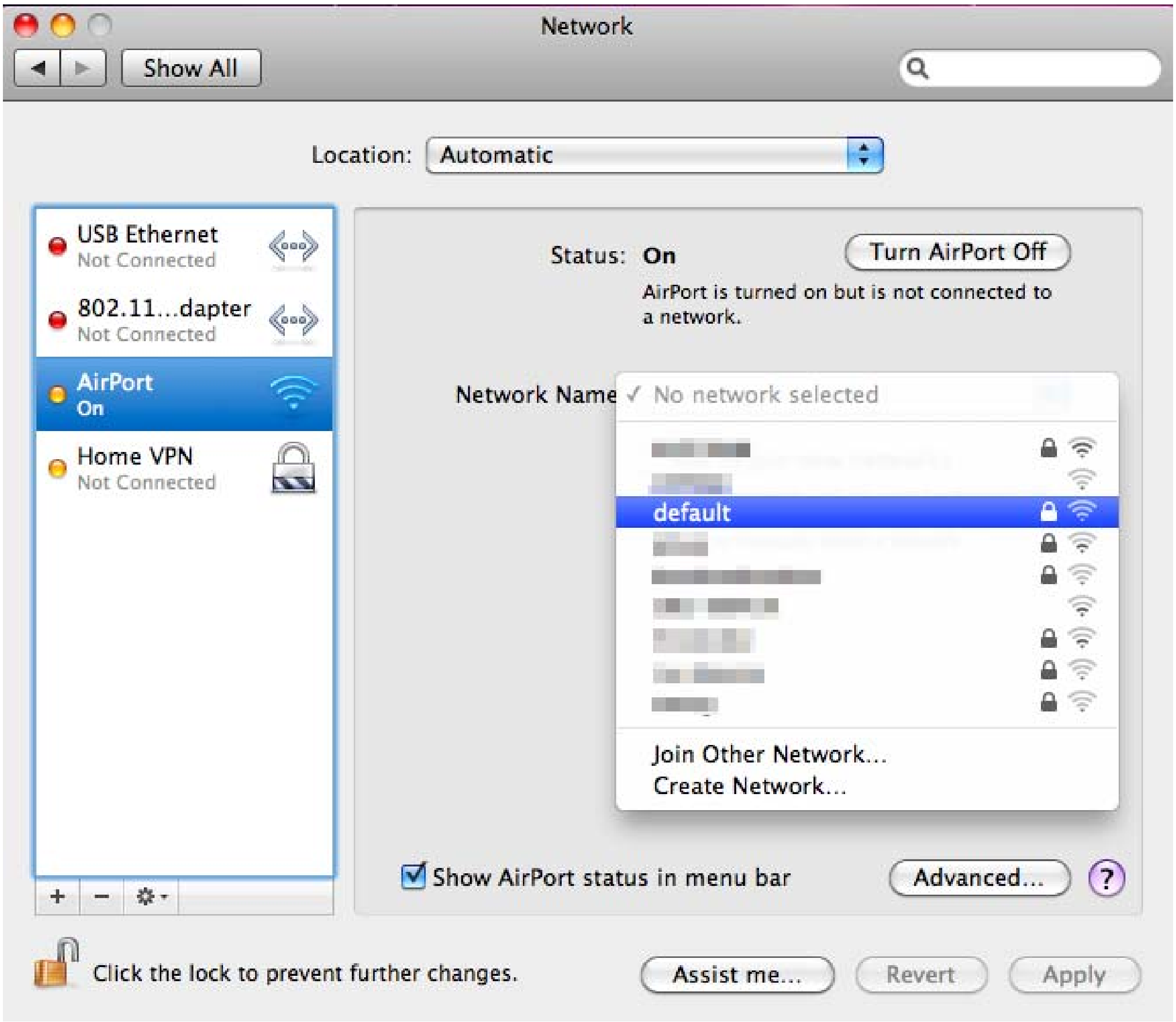
Figure 6-15 System Preferences -- Network

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

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

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

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



Location: Automatic

USB Ethernet — Not Connected

802.11...dapter — Not Connected

AirPort — On

Home VPN — Not Connected

Status: **On**

AirPort is turned on but is not connected to a network.

Network Name ✓ No network selected

default

Join Other Network...

Create Network...

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

Figure 6-16 Select the Wireless Network

6.4 iPhone / iPod Touch / iPad

In the following sections, the **default SSID** of the WNAP-6315 is configured to “**default**”.

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

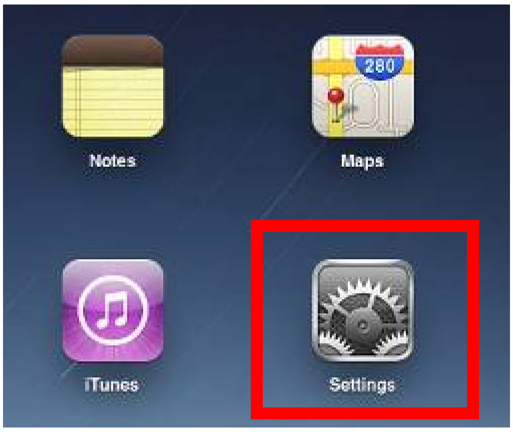


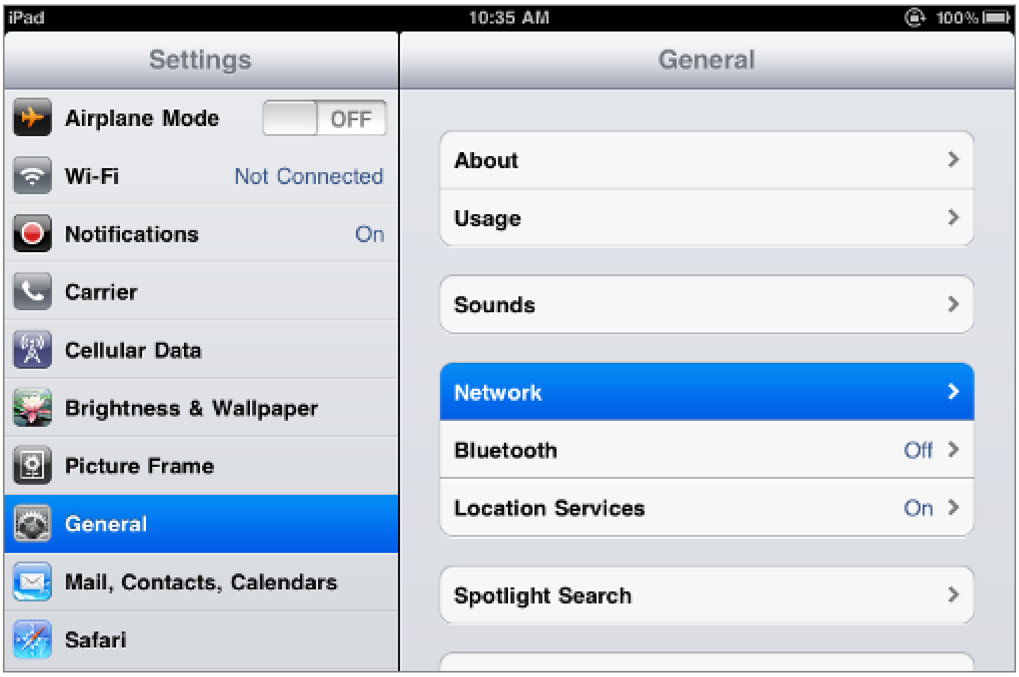
Figure 6-17 iPhone – Settings icon

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

(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”.



Airplane Mode OFF
Wi-Fi Not Connected
Notifications On
Carrier
Cellular Data
Brightness & Wallpaper
Picture Frame
General
Mail, Contacts, Calendars
Safari

About
Usage
Sounds
Network
Bluetooth Off
Location Services On
Spotlight Search

Figure 6-18 Wi-Fi Setting

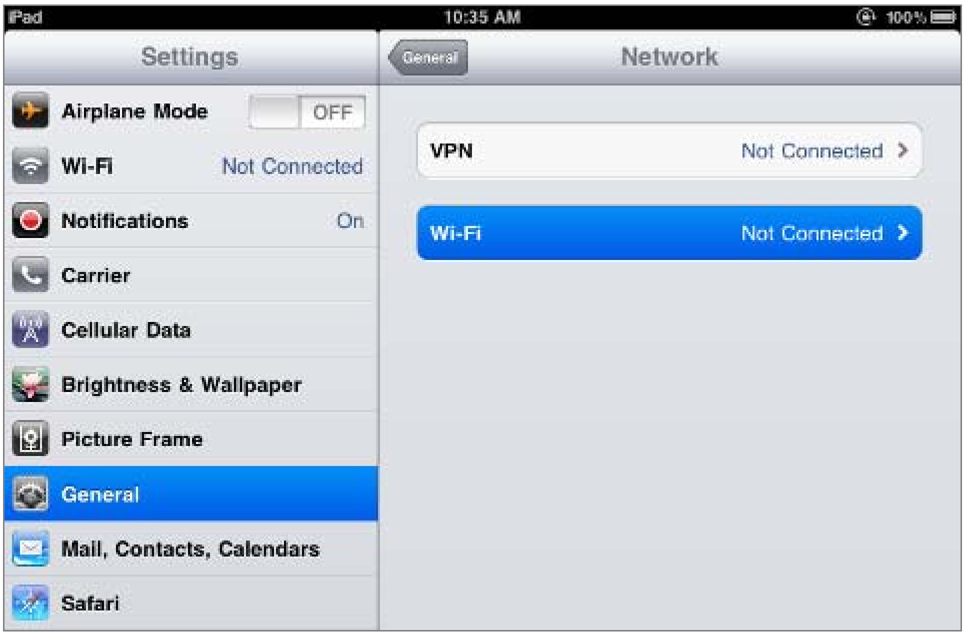


Figure 6-19 Wi-Fi Setting – Not Connected

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]**

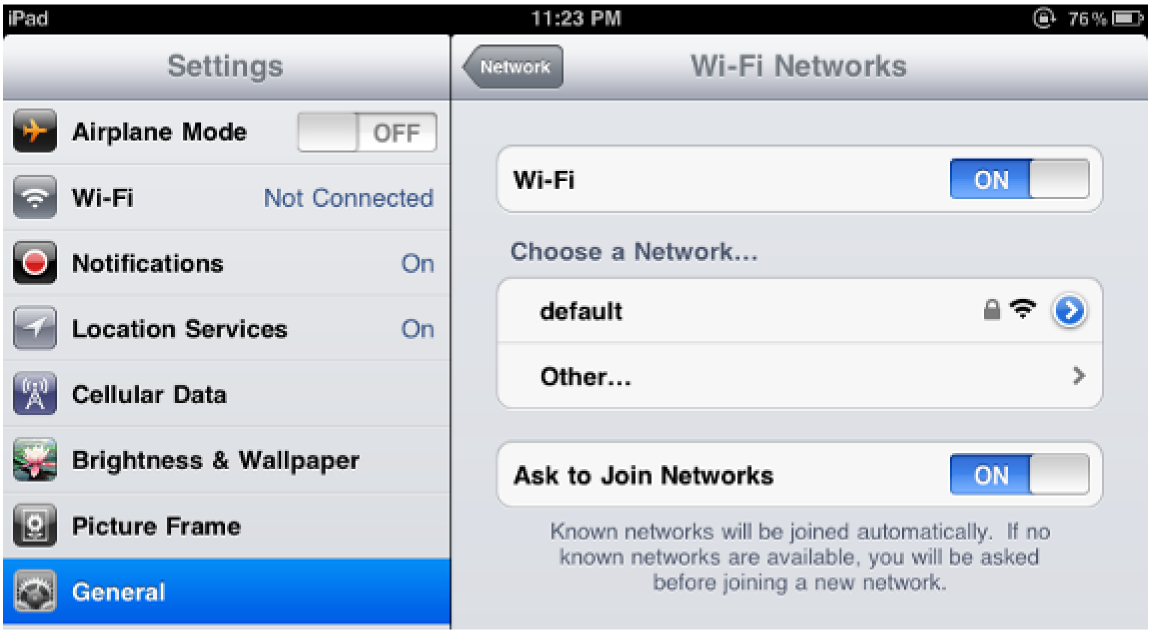


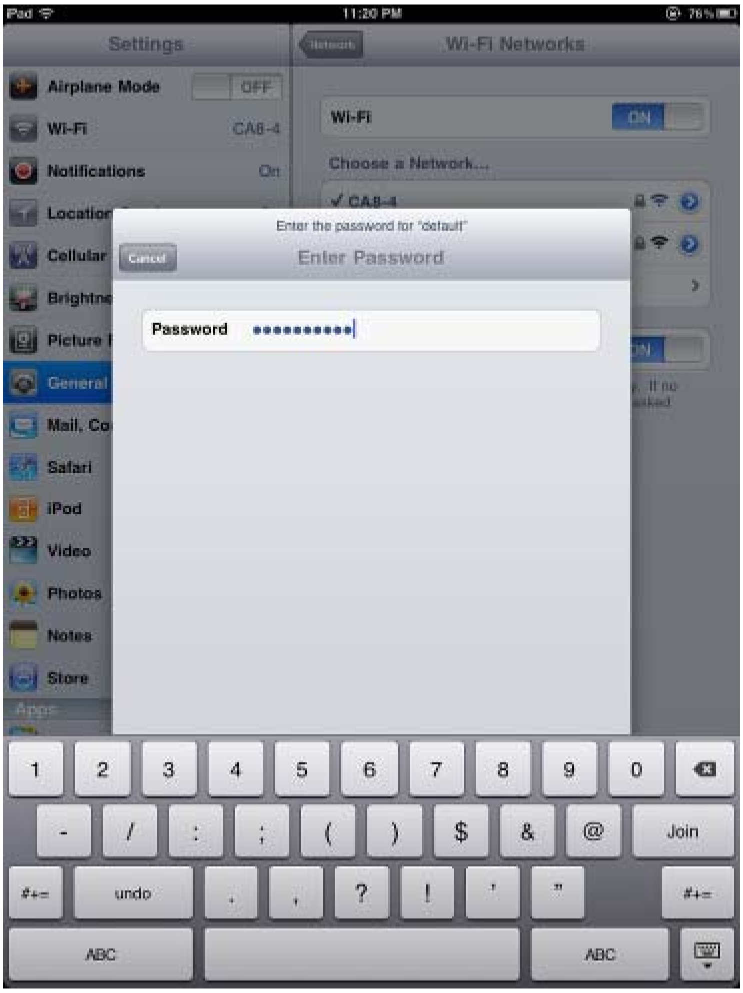
Figure 6-20 Turn on Wi-Fi

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

(1) The password input screen will be displayed

(2) Enter the encryption key that is configured in section 5.4.3

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



Enter the password for "default"

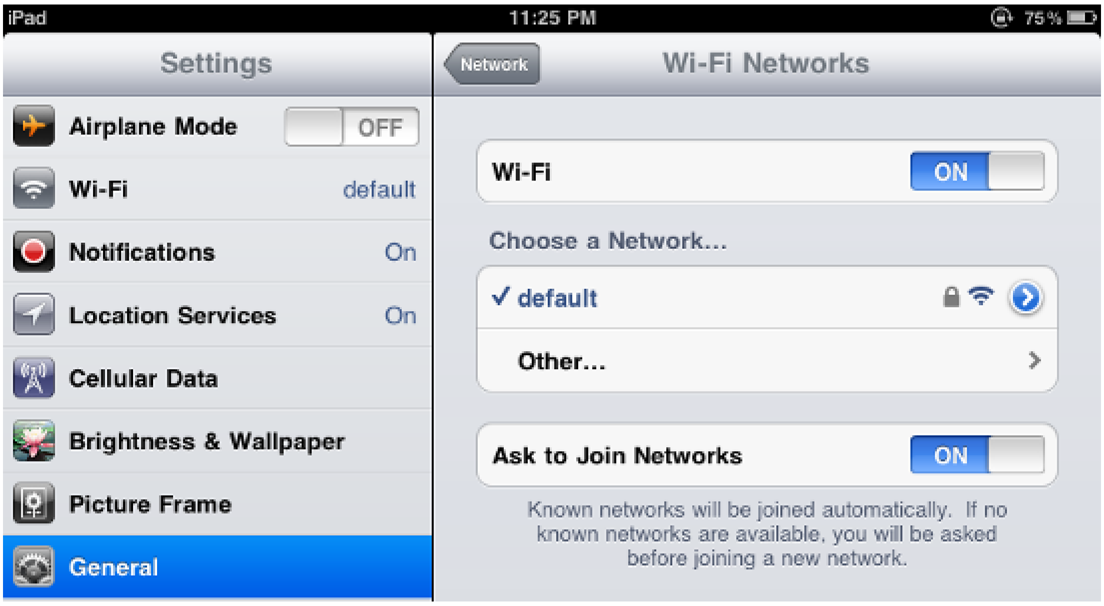
Enter Password

Password ●●●●●●●●●●●

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 in the front of the SSID.



Airplane Mode OFF

Wi-Fi default

Notifications On

Location Services On

Wi-Fi ON

Choose a Network...

✓ default

Other...

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Figure 6-22 iPhone -- Connected to the Network

Appendix A: Planet Smart Discovery Utility

To easily list the WNAP-6315 in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution. To get the Planet Smart Discovery Utility, please contact support@planet.com.tw.

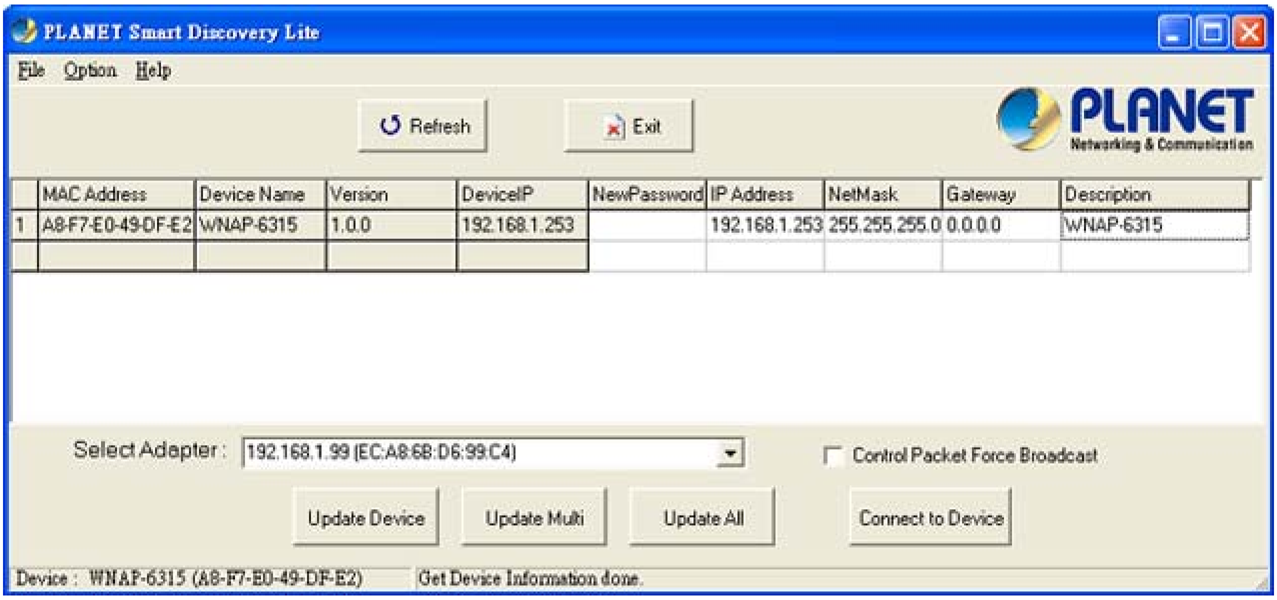
The following installation instructions guide you to running the Planet Smart Discovery Utility.

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

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

Planet_Utility.exe
PLANET Corp.

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



	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description
1	A8-F7-E0-49-DF-E2	WNAP-6315	1.0.0	192.168.1.253		192.168.1.253	255.255.255.0	0.0.0.0	WNAP-6315

Select Adapter : 192.168.1.99 (EC:A8:6B:D6:99:C4)

☐ Control Packet Force Broadcast

Device : WNAP-6315 (A8-F7-E0-49-DF-E2) Get Device Information done.

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

Note

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.

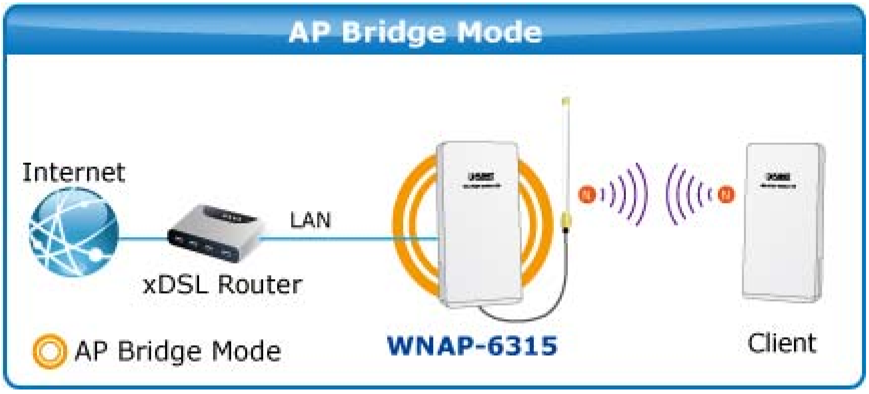
Scenario	Solution
The AP is not responding to me when I want to access it by Web browser.	a. Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be correctly and firmly inserted to the AP. b. If all LED on this AP is off, please check the status 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 '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 website, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the AP and try again later. h. Reset the device provided by your Internet service provider too.

	i. Try to use IP address instead of host name. If you can use IP address to communicate with a remote server, 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.

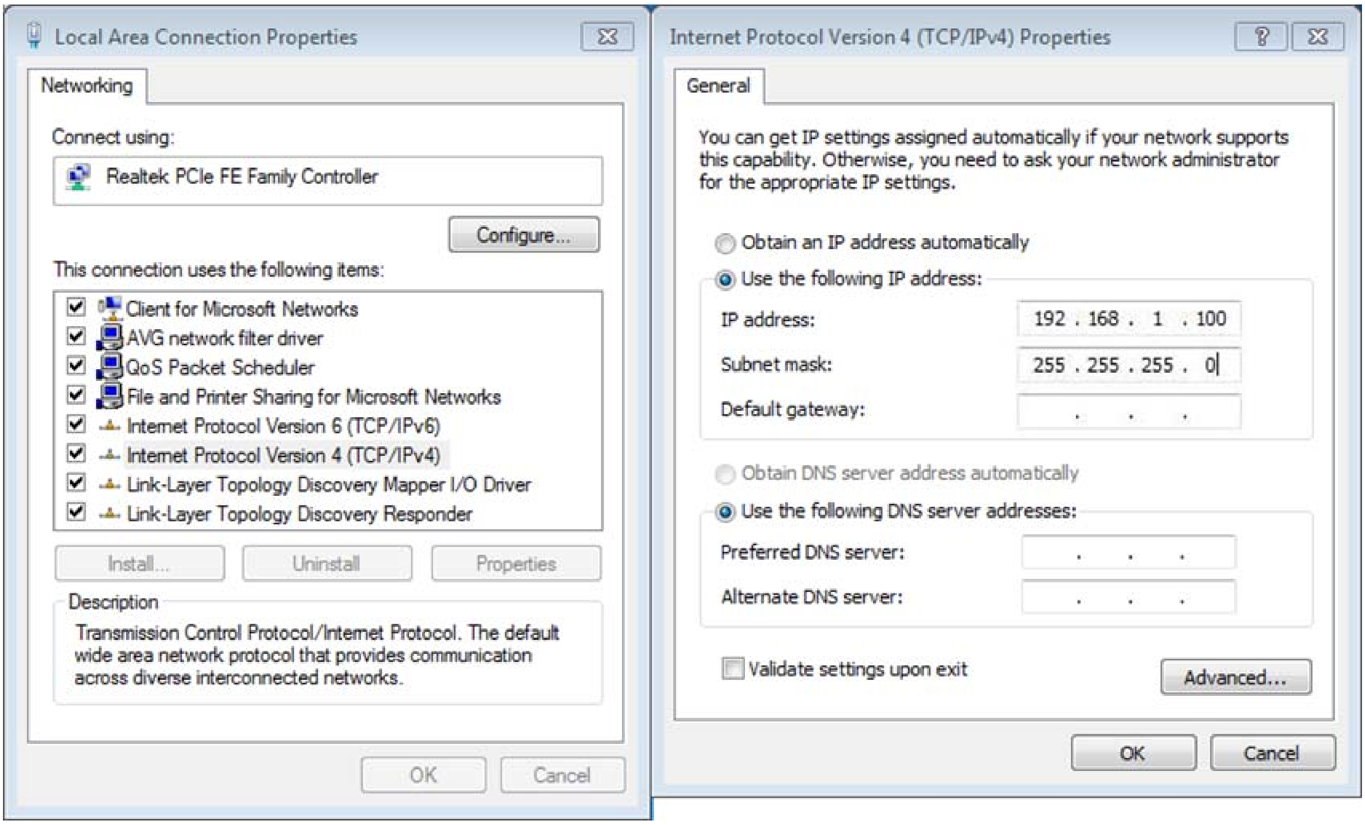
Appendix C: Frequently Asked Questions

Q1: How to set up the AP Client Connection

Topology:



Step 1. Use static IP in the PCs that are connected with AP-1(WNAP-6315, Site-1) and AP-2 (Client, Site-2). In this case, Site-1 is "**192.168.1.100**", and Site-2 is "**192.168.1.200**".



Local Area Connection Properties

Networking

Connect using:

Realtek PCIe FE Family Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ AVG network filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

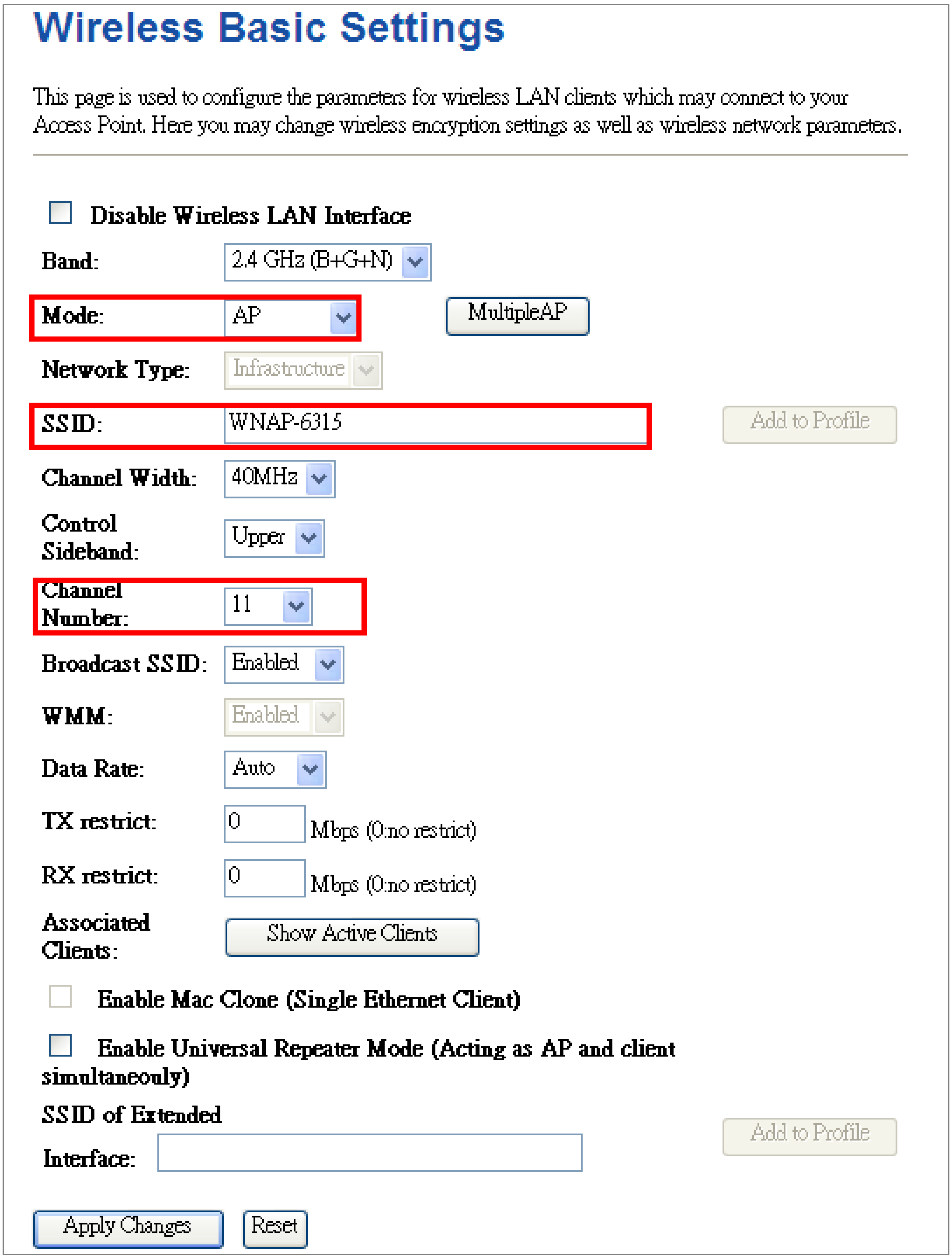
Advanced...

OK Cancel

Step 2. In AP-1, go to "**Wireless→ Basic Settings**" to configure it to **AP** Mode. Then, configure the following wireless parameters for your wireless network.

1) **Network ID (SSID)**: set to a unique value

2) **Channel**: set to a fixed one or auto (suggested set to fixed channel).



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

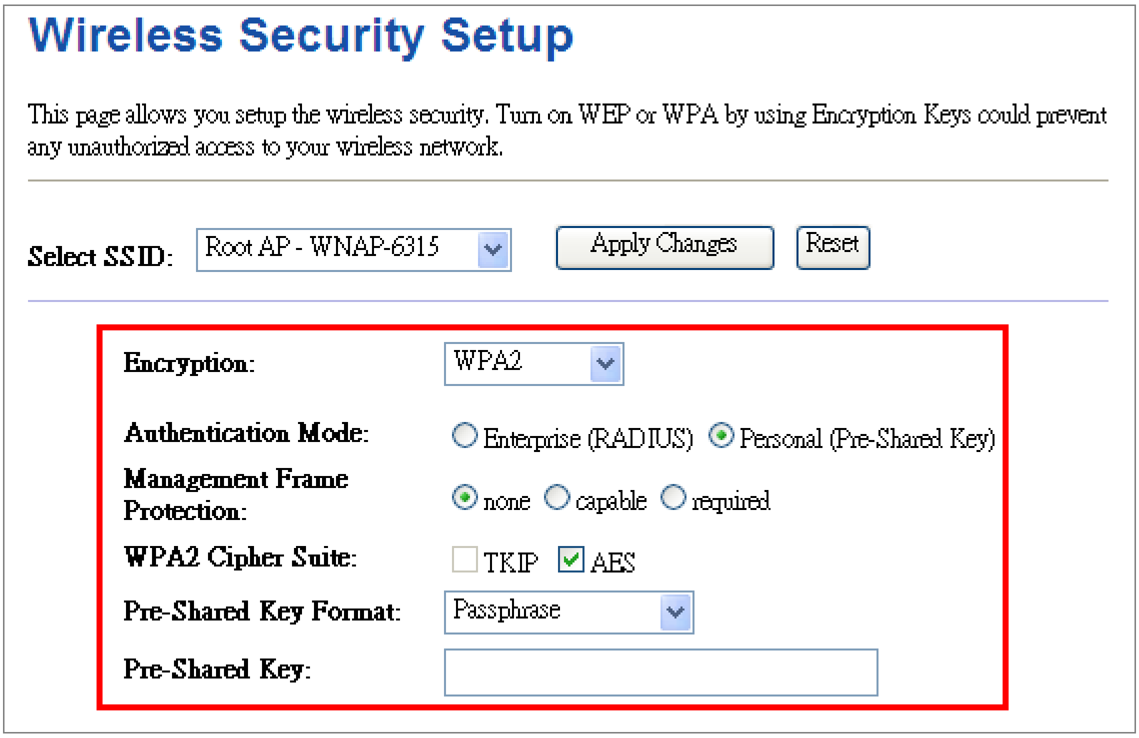
Band:	2.4 GHz (B+G+N)
Mode:	AP
Network Type:	Infrastructure
SSID:	WNAP-6315
Channel Width:	40MHz
Control Sideband:	Upper
Channel Number:	11
Broadcast SSID:	Enabled
WMM:	Enabled
Data Rate:	Auto
TX restrict:	0 Mbps (0:no restrict)
RX restrict:	0 Mbps (0:no restrict)
Associated Clients:	Show Active Clients

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Step 3. Go to "**Wireless→ Security**" to configure the security setting.



Wireless Security Setup

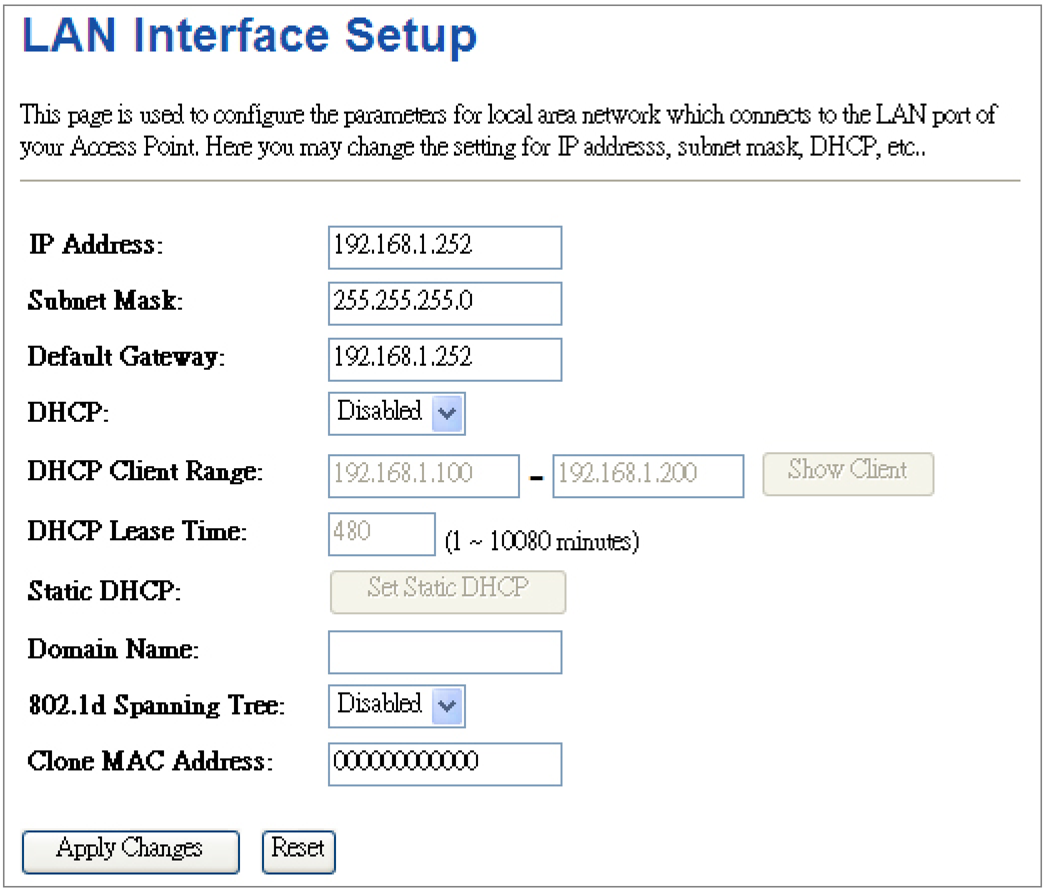
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Select SSID:	Root AP - WNAP-6315

Encryption:	WPA2
Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
Management Frame Protection:	● none ○ capable ○ required
WPA2 Cipher Suite:	□ TKIP ☑ AES
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	

Step 4. In AP-2, modify the default IP to the same IP range but different from AP-1.

In this case, the IP is changed to **192.168.1.252**.

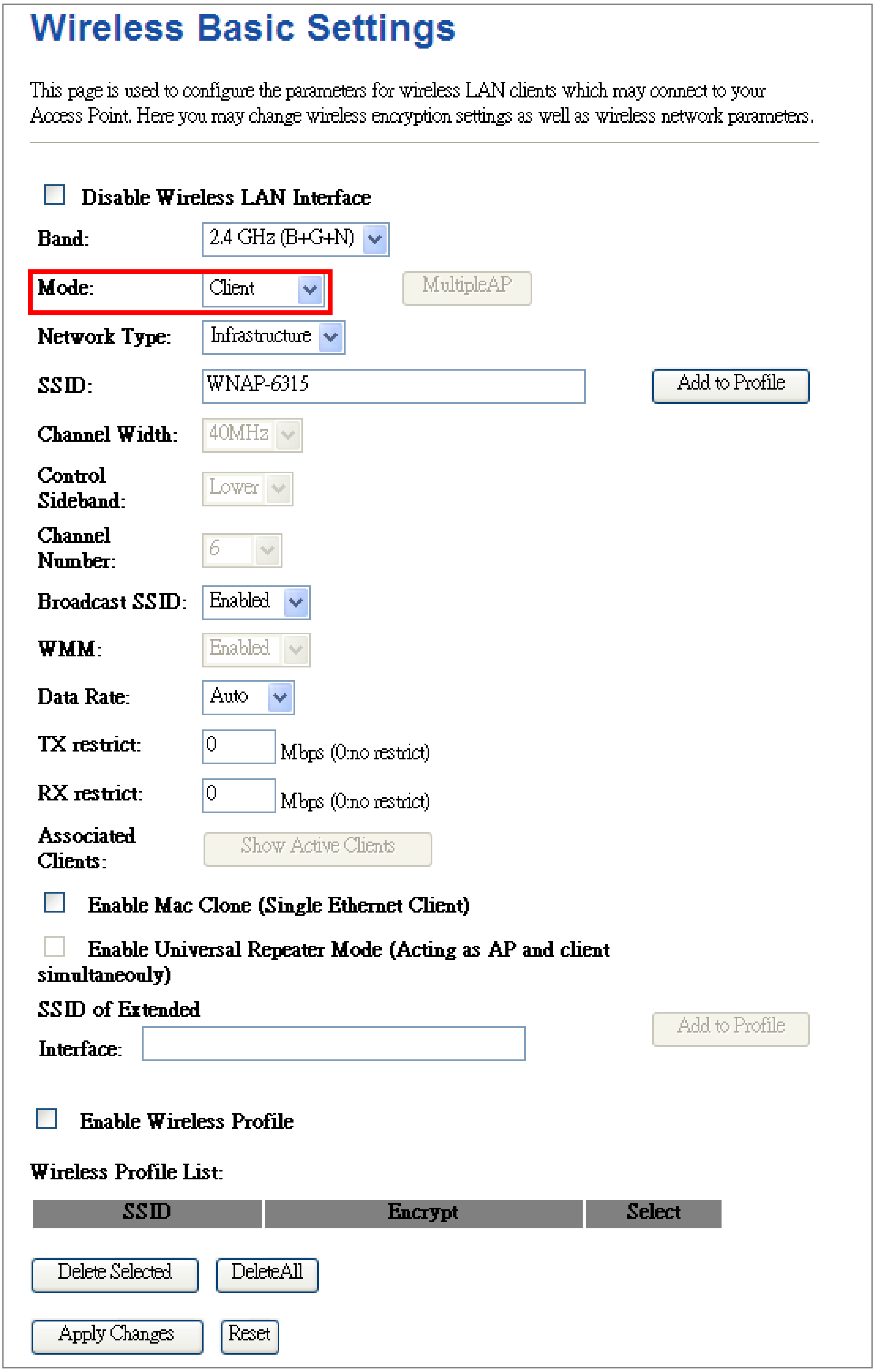


LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.252
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.252
DHCP:	Disabled
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DHCP Lease Time:	480 (1 ~ 10080 minutes)
Static DHCP:	Set Static DHCP
Domain Name:	
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Step 5. In AP-2, configure it in "**Client**" mode.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G+N)

Mode: Client

Network Type: Infrastructure

SSID: WNAP-6315

Channel Width: 40MHz

Control Sideband: Lower

Channel Number: 6

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

TX restrict: 0 Mbps (0:no restrict)

RX restrict: 0 Mbps (0:no restrict)

Associated Clients:

□ **Enable Mac Clone (Single Ethernet Client)**

□ **Enable Universal Repeater Mode (Acting as AP and client simultaneouly)**

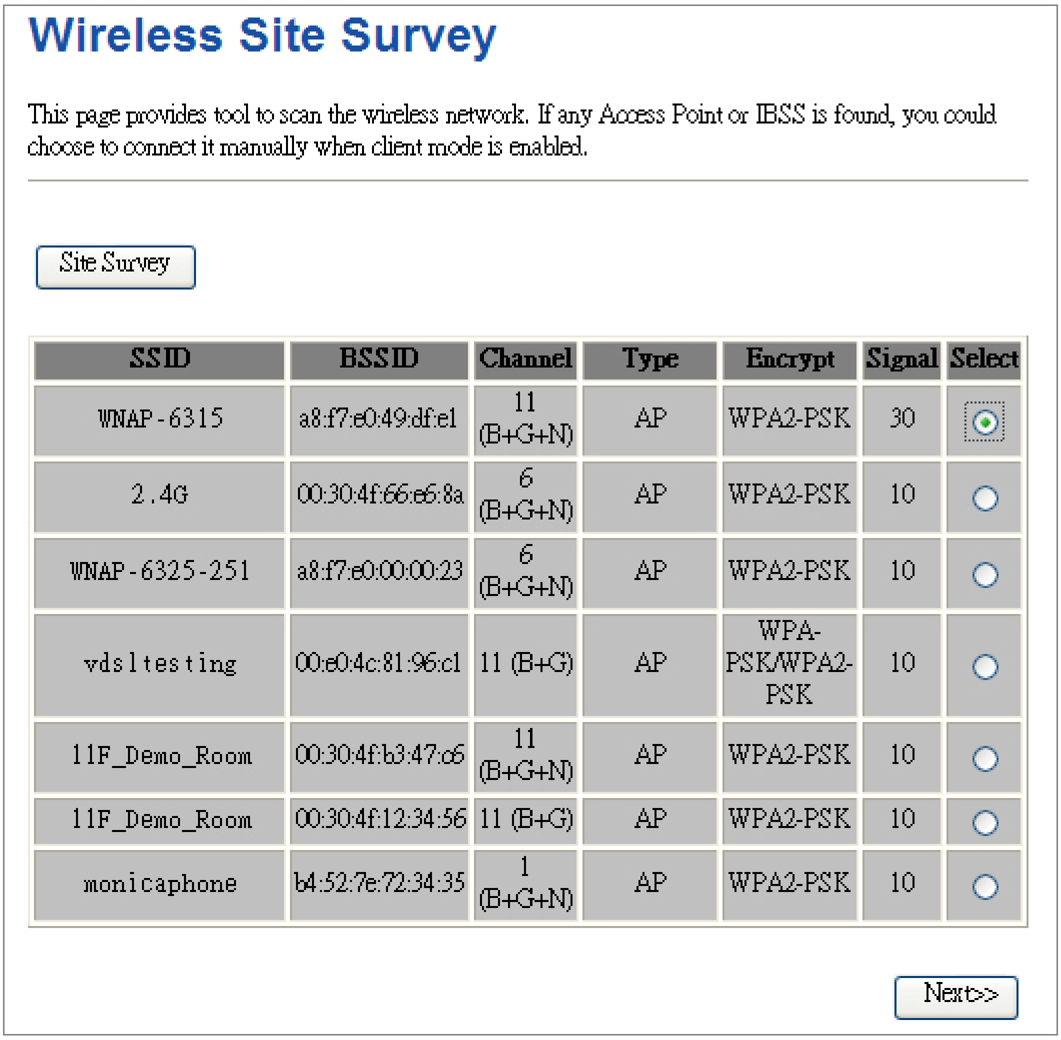
SSID of Extended Interface:

□ **Enable Wireless Profile**

Wireless Profile List:

SSID	Encrypt	Select

Step 6. Go to "**Wireless→ Site Survey**" to find the AP-1. Then, select it and click "**Next**".

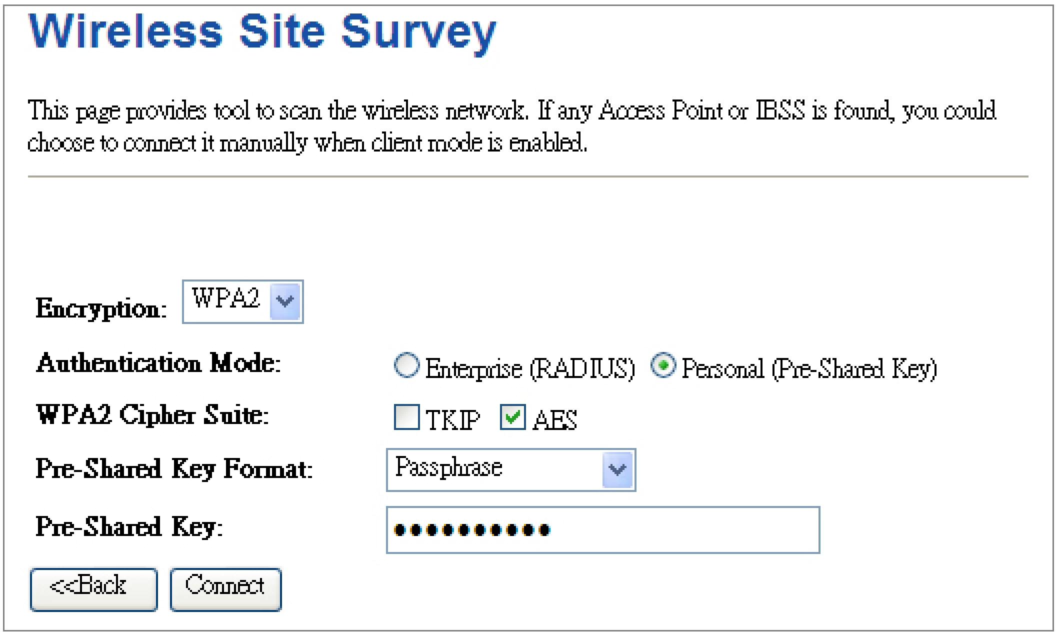


Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
WNAP-6315	a8:f7:e0:49:df:e1	11 (B+G+N)	AP	WPA2-PSK	30	●
2.4G	00:30:4f:66:e6:8a	6 (B+G+N)	AP	WPA2-PSK	10	○
WNAP-6325-251	a8:f7:e0:00:00:23	6 (B+G+N)	AP	WPA2-PSK	10	○
vdsltesting	00:e0:4c:81:96:c1	11 (B+G)	AP	WPA-PSK/WPA2-PSK	10	○
11F_Demo_Room	00:30:4f:b3:47:c6	11 (B+G+N)	AP	WPA2-PSK	10	○
11F_Demo_Room	00:30:4f:12:34:56	11 (B+G)	AP	WPA2-PSK	10	○
monicaphone	b4:52:7e:72:34:35	1 (B+G+N)	AP	WPA2-PSK	10	○

Step 7. Configure the Encryption and Pre-Shared Key which must be the same as AP-1. Then click "**Connect**".



Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Encryption: WPA2

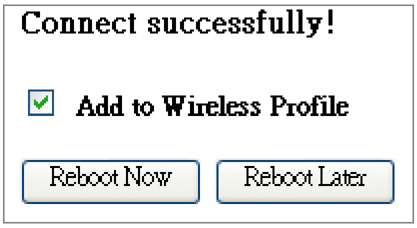
Authentication Mode: ○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)

WPA2 Cipher Suite: □ TKIP ☑ AES

Pre-Shared Key Format: Passphrase

Pre-Shared Key: ●●●●●●●●●●●

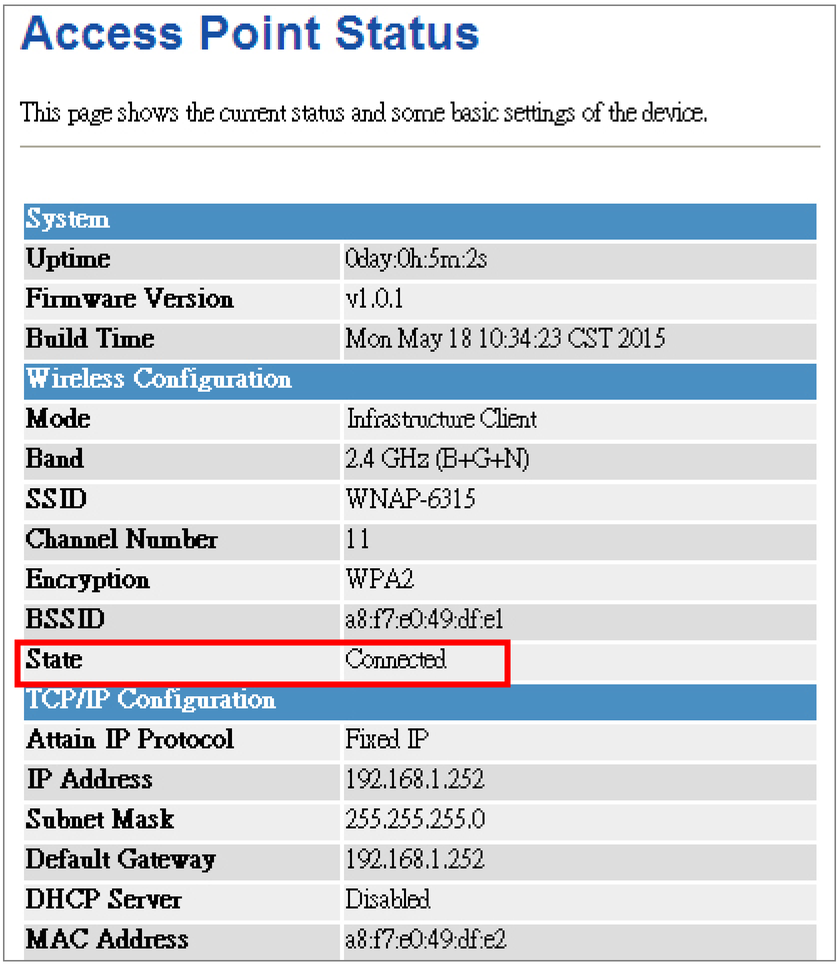
Step 8. Check "**Add to Wireless Profile**" and click "**Reboot Now**" to apply the setting.



Connect successfully!

☑ Add to Wireless Profile

Step 9. Go to "**Management→ Status**" to check the connection state should be "**Connected**".



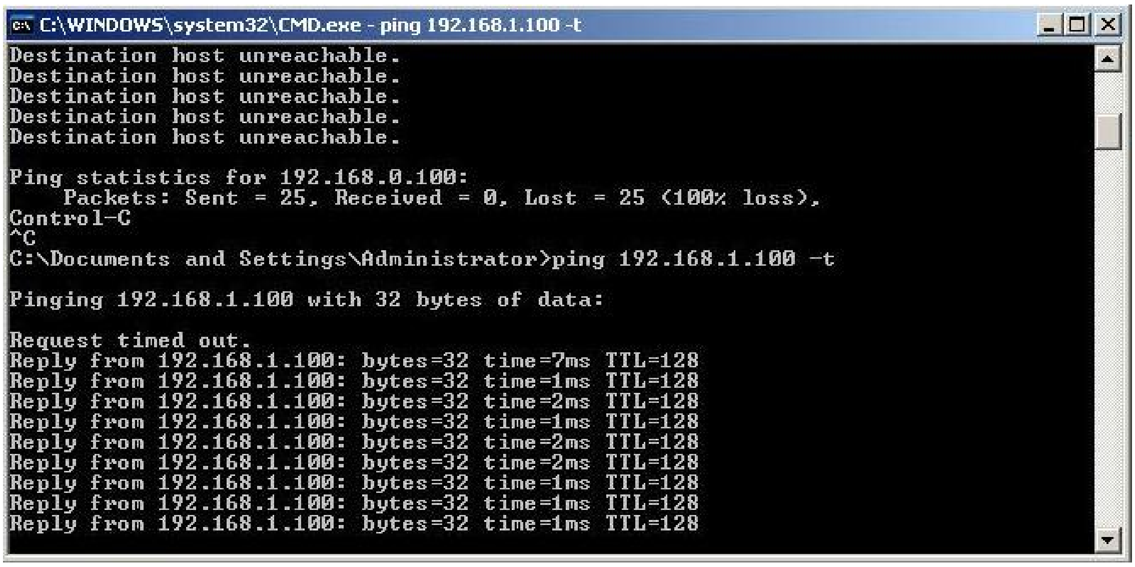
Access Point Status

This page shows the current status and some basic settings of the device.

System	
Uptime	0day:0h:5m:2s
Firmware Version	v1.0.1
Build Time	Mon May 18 10:34:23 CST 2015
Wireless Configuration	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	WNAP-6315
Channel Number	11
Encryption	WPA2
BSSID	a8:f7:e0:49:df:e1
State	Connected
TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.1.252
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.252
DHCP Server	Disabled
MAC Address	a8:f7:e0:49:df:e2

Step 10. Use command line tool to ping each other to ensure the link is successfully established.

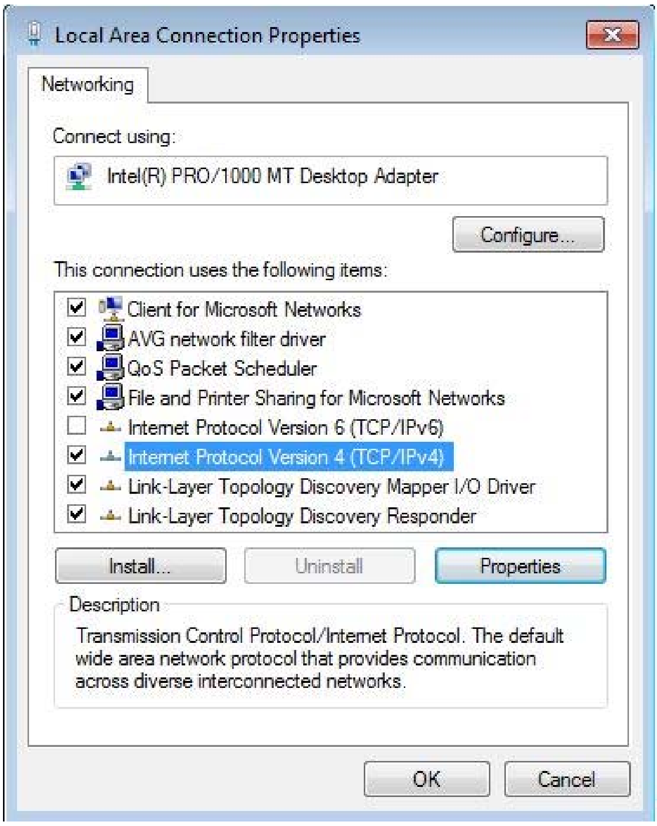
From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.100.



C:\WINDOWS\system32\CMD.exe - ping 192.168.1.100 -t

```
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

Step 11. Configure the TCP/IP settings of Site-2 to "**Obtain an IP address automatically**".



Local Area Connection Properties

Networking

Connect using:

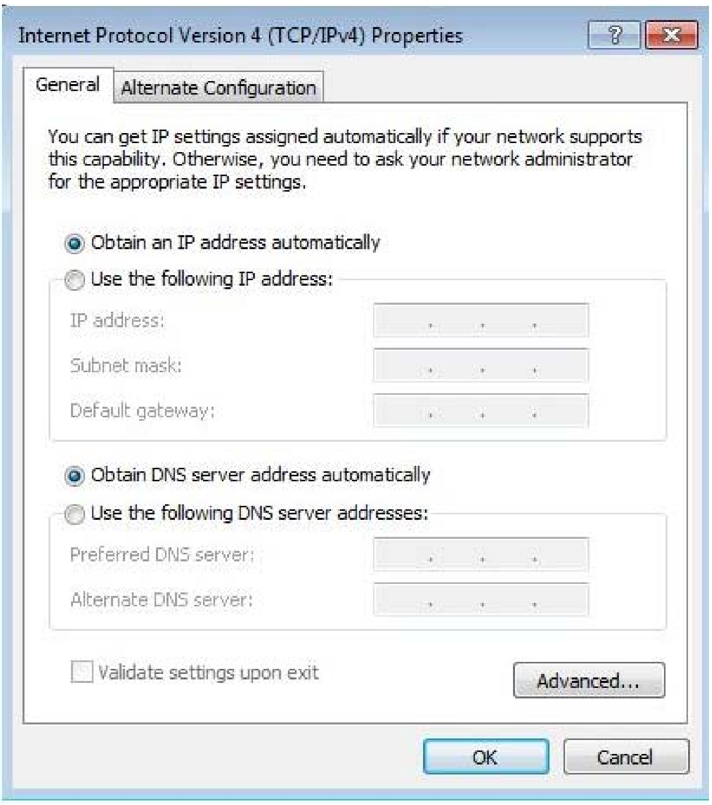
Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ AVG network filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

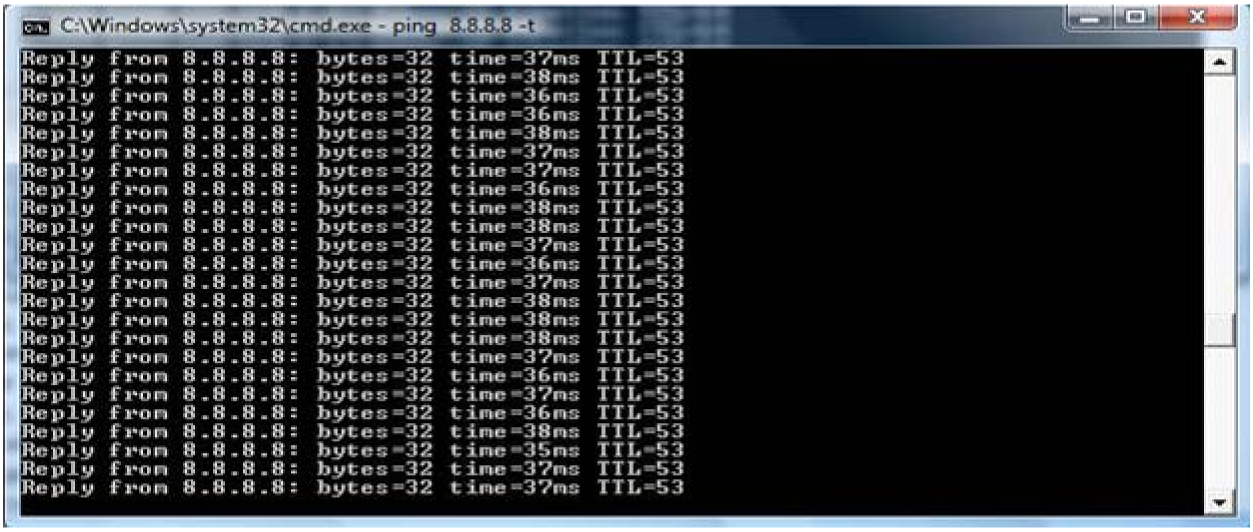
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Step 12. Use command line tool to ping the DNS (e.g. Google) to ensure the Site-2 can access internet through the wireless connection.



C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t

```
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=35ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
```

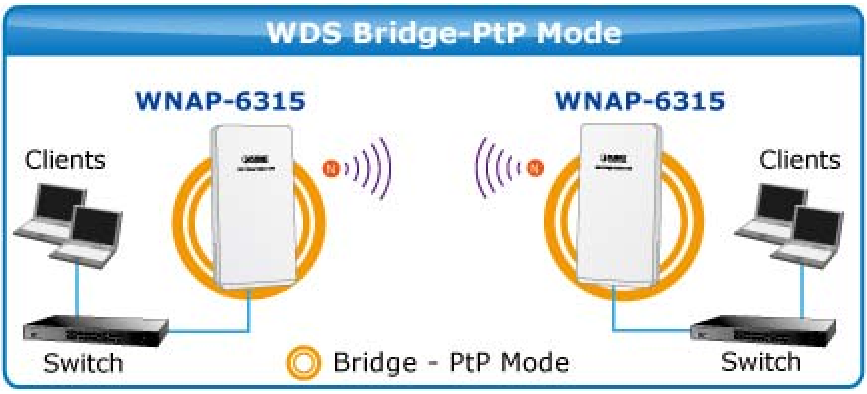
Note

The attention of the following hints should be paid:

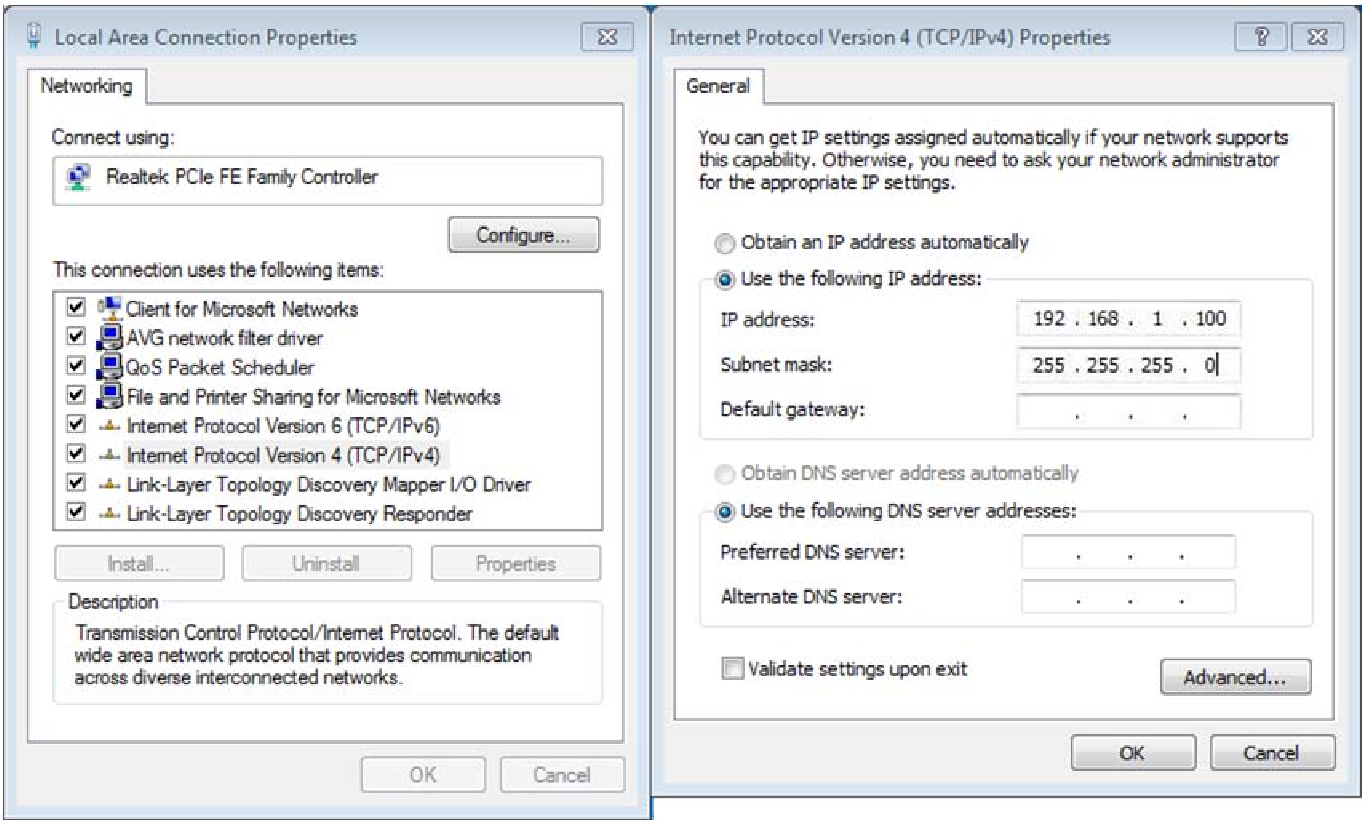
1) The encryption method must be the same as that of both sites if configured.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "**RF Output Power**" of both sites to half or lower.

Q2: How to setup the WDS Connection

Topology:



Step 1. Use static IP in the PCs that are connected with WNAP-6315-1(Site-1) and WNAP-6315-2(Site-2), in this case, Site-1 is "**192.168.1.100**", and Site-2 is "**192.168.1.200**".


Local Area Connection Properties

Networking

Connect using:

Realtek PCIe FE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ AVG network filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

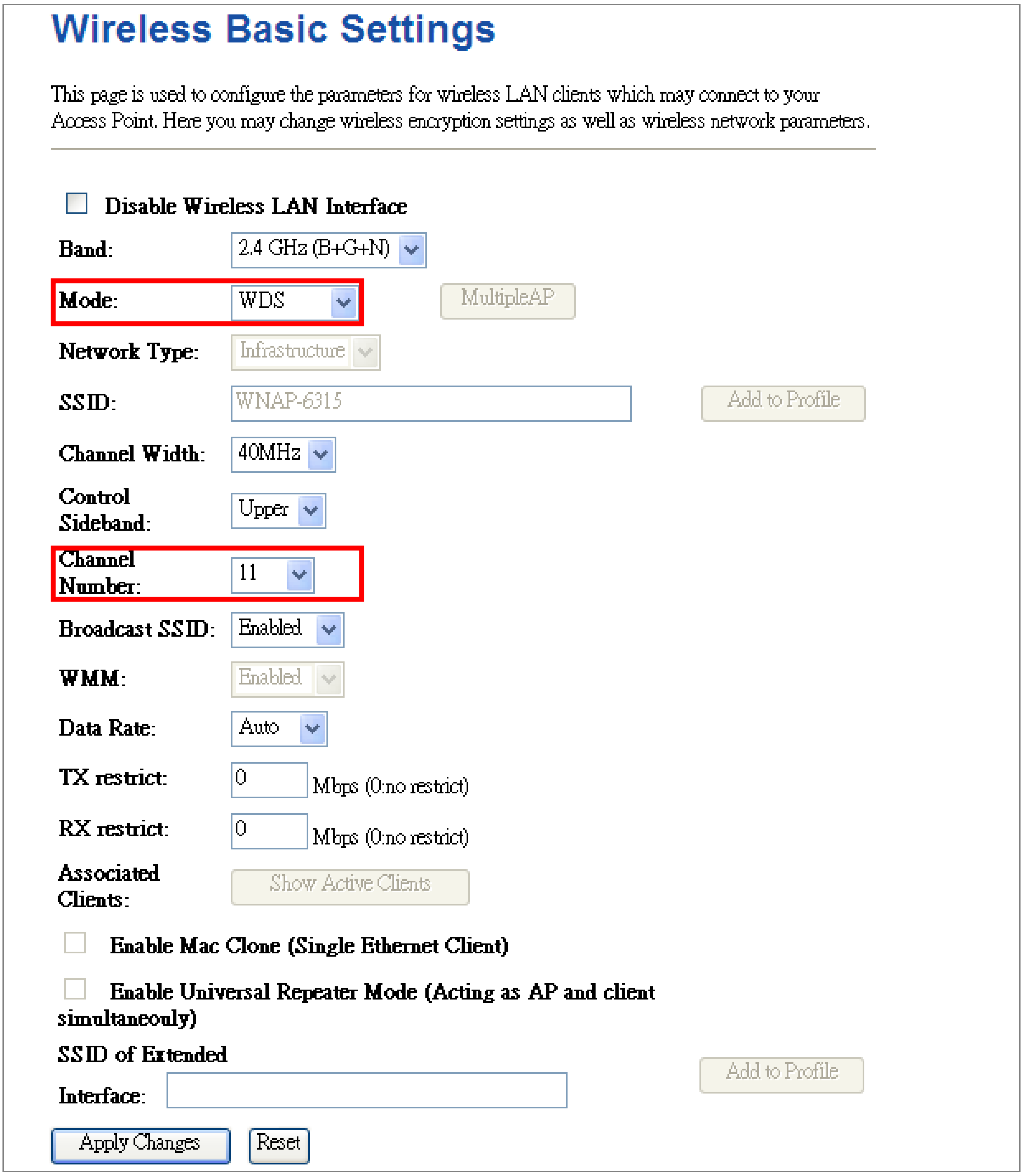
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Step 2. In AP-1, go to “**Wireless→ Basic Settings**” to configure it to “**WDS**” Mode. Then, set the channel number to a fixed one.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band:	2.4 GHz (B+G+N)	
Mode:	WDS	MultipleAP
Network Type:	Infrastructure	
SSID:	WNAP-6315	Add to Profile
Channel Width:	40MHz	
Control Sideband:	Upper	
Channel Number:	11	
Broadcast SSID:	Enabled	
WMM:	Enabled	
Data Rate:	Auto	
TX restrict:	0 Mbps (0:no restrict)	
RX restrict:	0 Mbps (0:no restrict)	
Associated Clients:	Show Active Clients	

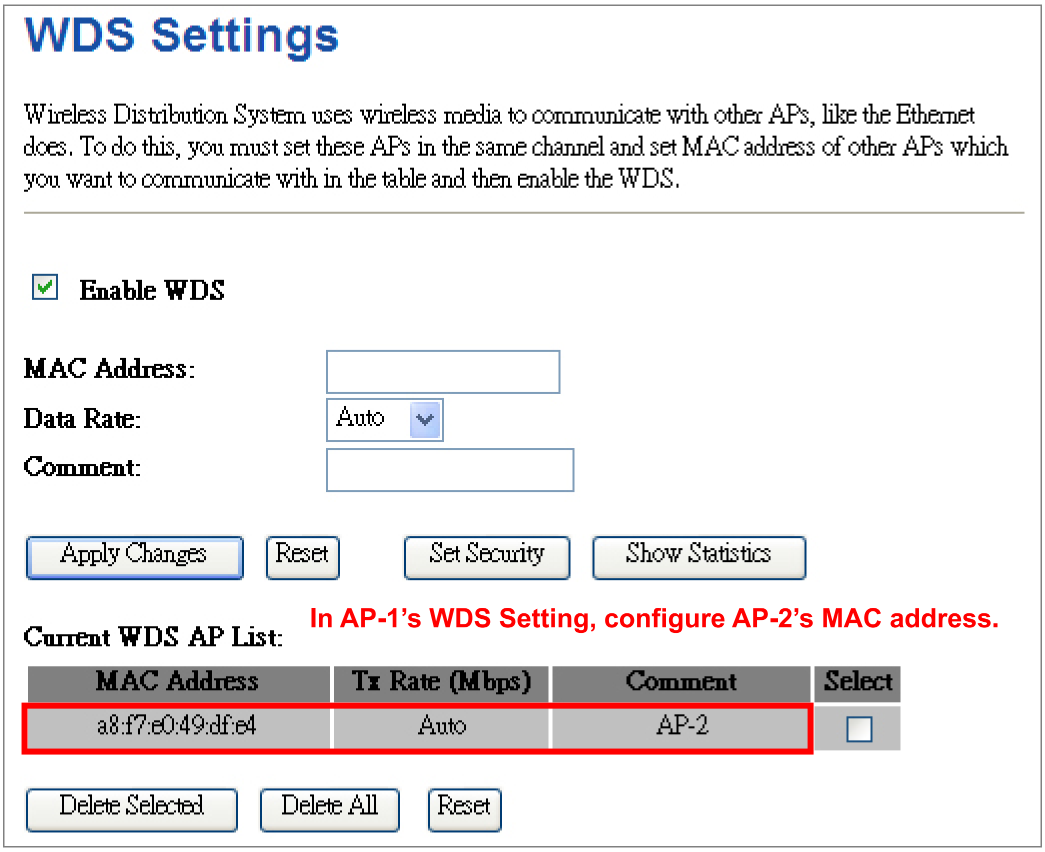
□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface: Add to Profile

Apply Changes Reset

Step 3. Go to “**Wireless→ WDS Settings**” to configure the AP-2’s MAC address.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

☑ **Enable WDS**

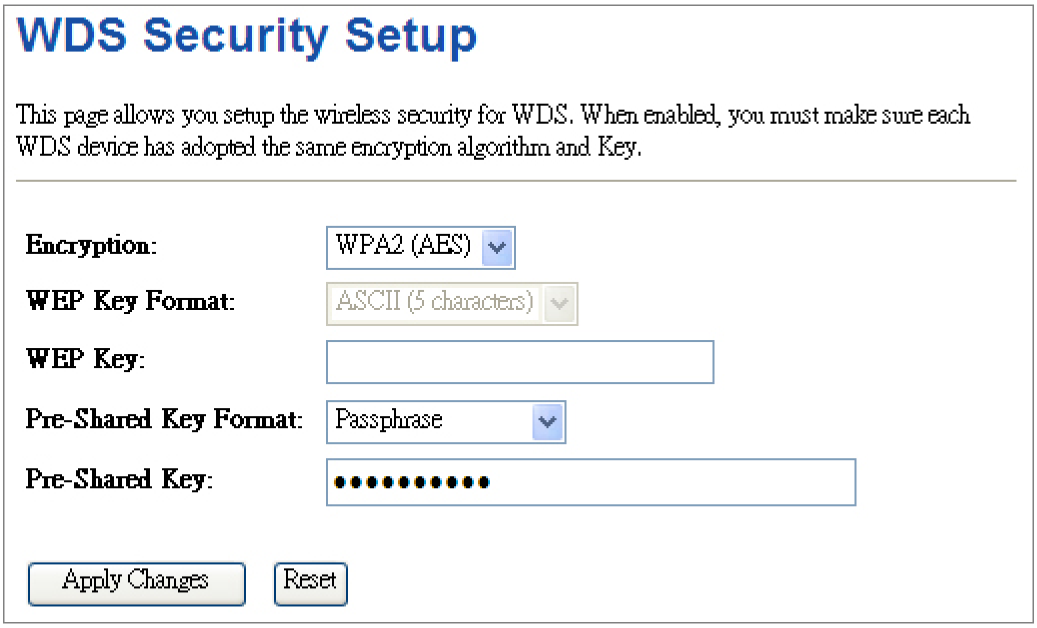
MAC Address:	
Data Rate:	Auto
Comment:	

In AP-1’s WDS Setting, configure AP-2’s MAC address.

Current WDS AP List:

MAC Address	Tx Rate (Mbps)	Comment	Select
a8:f7:e0:49:df:e4	Auto	AP-2	□

Step 4. If you select “**Reboot Later**”, you can click “**Set Security**” to continue to configure the encryption and security key of the WDS connection. Then, click “**Apply Changes**” to apply the setting.



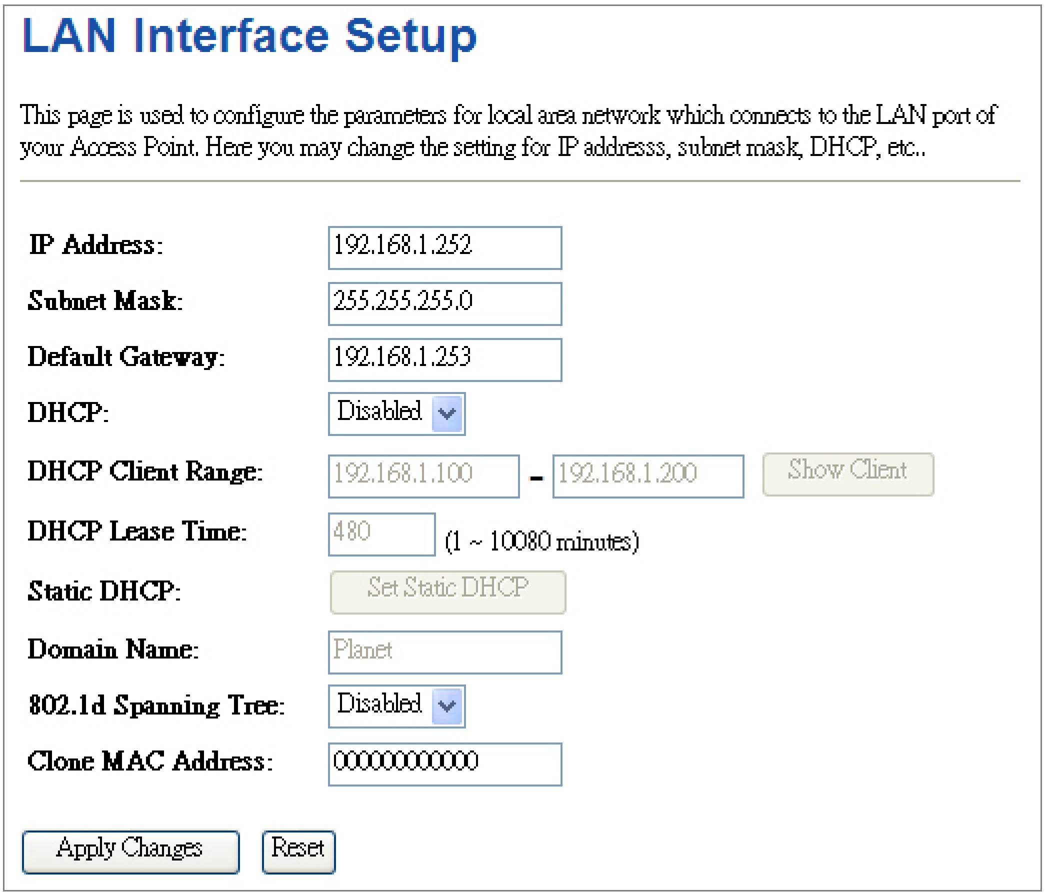
WDS Security Setup

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	WPA2 (AES)
WEP Key Format:	ASCII (5 characters)
WEP Key:	
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	●●●●●●●●●●

Step 5. In AP-2, modify the default IP to the same IP range but different from AP-1.

In this case, the IP is changed to **192.168.1.252**.

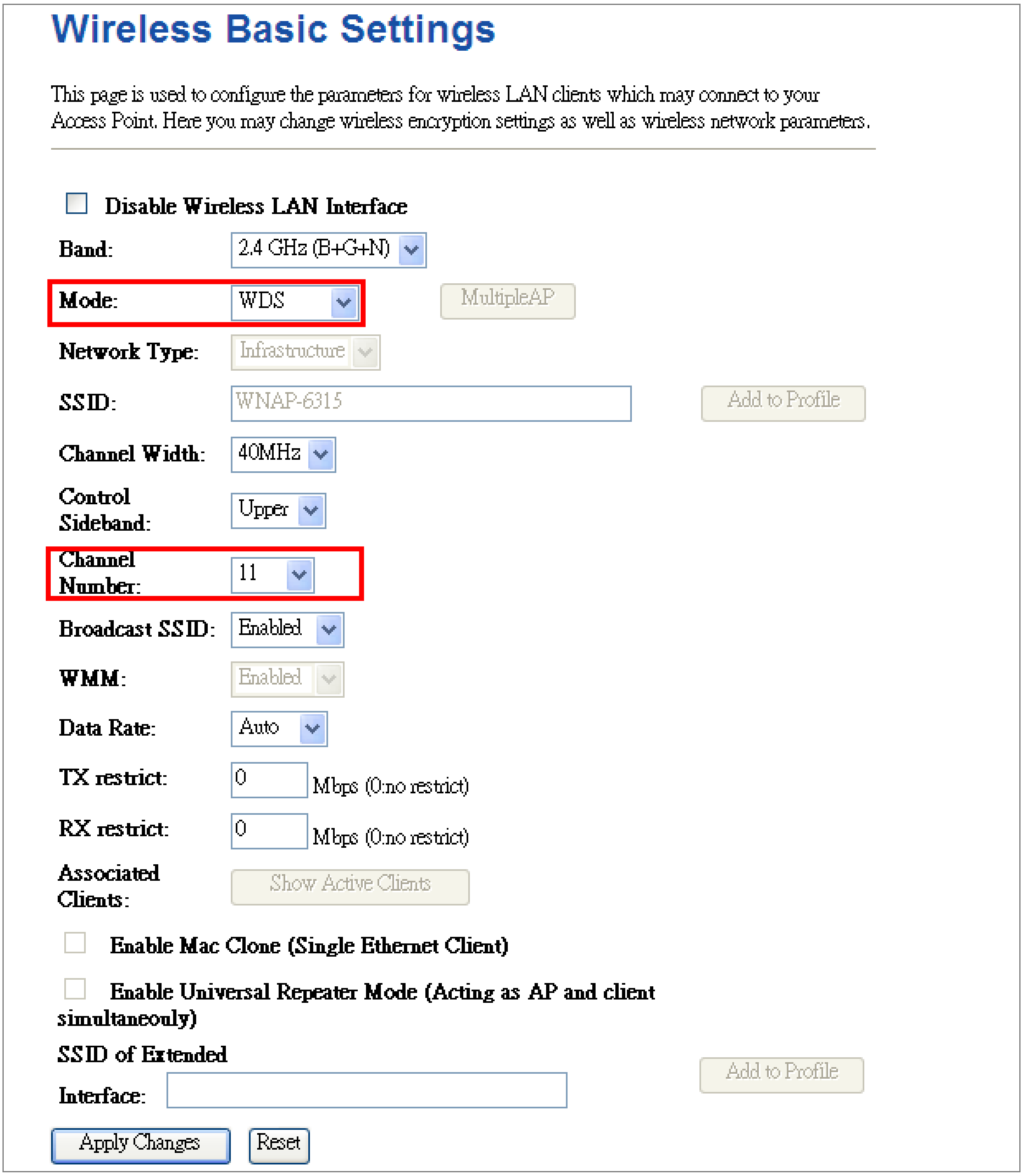


LAN Interface Setup

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..

IP Address:	192.168.1.252
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.253
DHCP:	Disabled
DHCP Client Range:	192.168.1.100 - 192.168.1.200 Show Client
DHCP Lease Time:	480 (1 ~ 10080 minutes)
Static DHCP:	Set Static DHCP
Domain Name:	Planet
802.1d Spanning Tree:	Disabled
Clone MAC Address:	000000000000

Step 6. In AP-2, configure it to "**WDS**" mode and set the channel to the fixed one which is the same as AP-1.



Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G+N)

Mode: WDS

Network Type: Infrastructure

SSID: WNAP-6315

Channel Width: 40MHz

Control Sideband: Upper

Channel Number: 11

Broadcast SSID: Enabled

WMM: Enabled

Data Rate: Auto

TX restrict: 0 Mbps (0:no restrict)

RX restrict: 0 Mbps (0:no restrict)

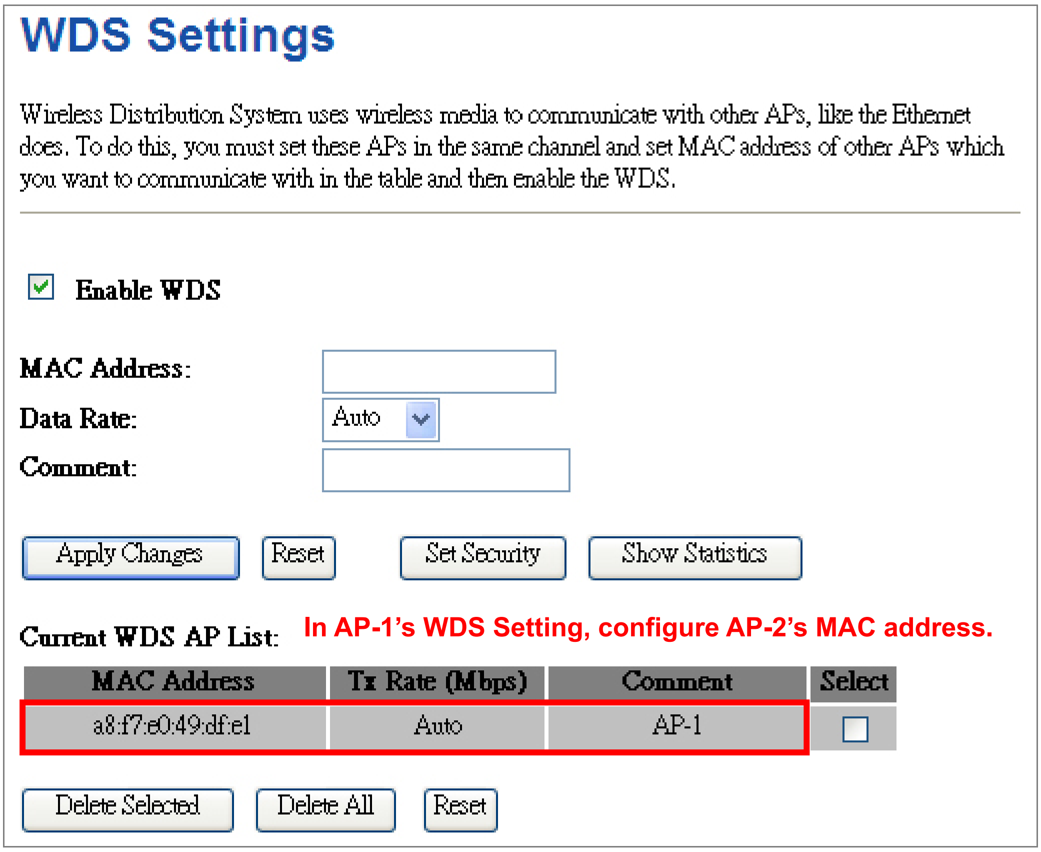
Associated Clients:

□ Enable Mac Clone (Single Ethernet Client)

□ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

Step 7. Go to “**Wireless→ WDS Settings**” to configure the AP-1’s MAC address.



WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

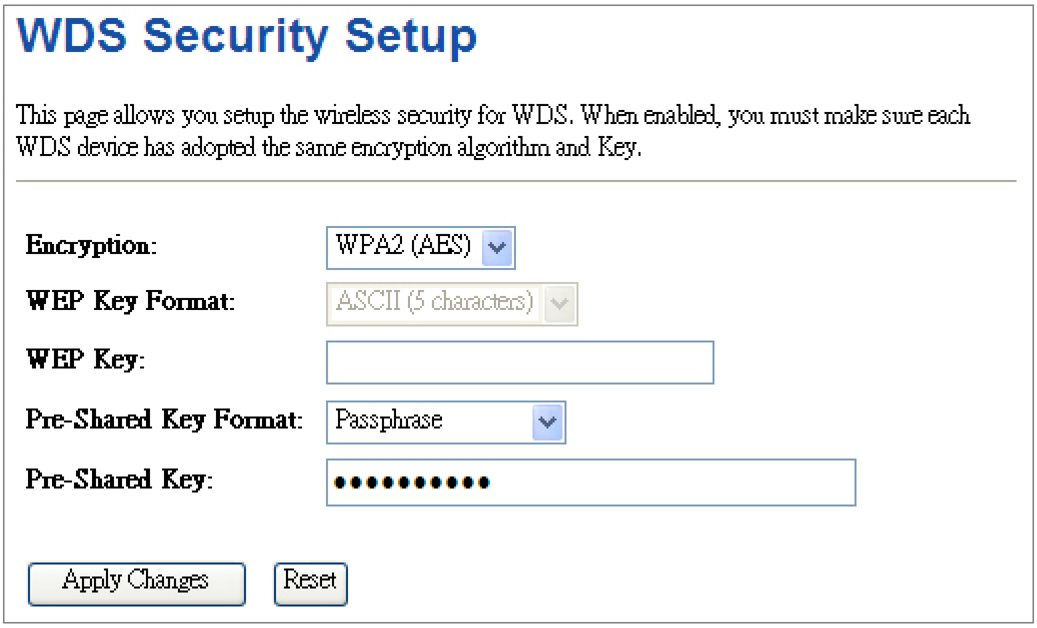
☑ **Enable WDS**

MAC Address:	
Data Rate:	Auto
Comment:	

Current WDS AP List: In AP-1’s WDS Setting, configure AP-2’s MAC address.

MAC Address	Tx Rate (Mbps)	Comment	Select
a8:f7:e0:49:df:e1	Auto	AP-1	□

Step 8. If you select “**Reboot Later**”, you can click “**Set Security**” to continue to configure the encryption and security key of the WDS connection.



WDS Security Setup

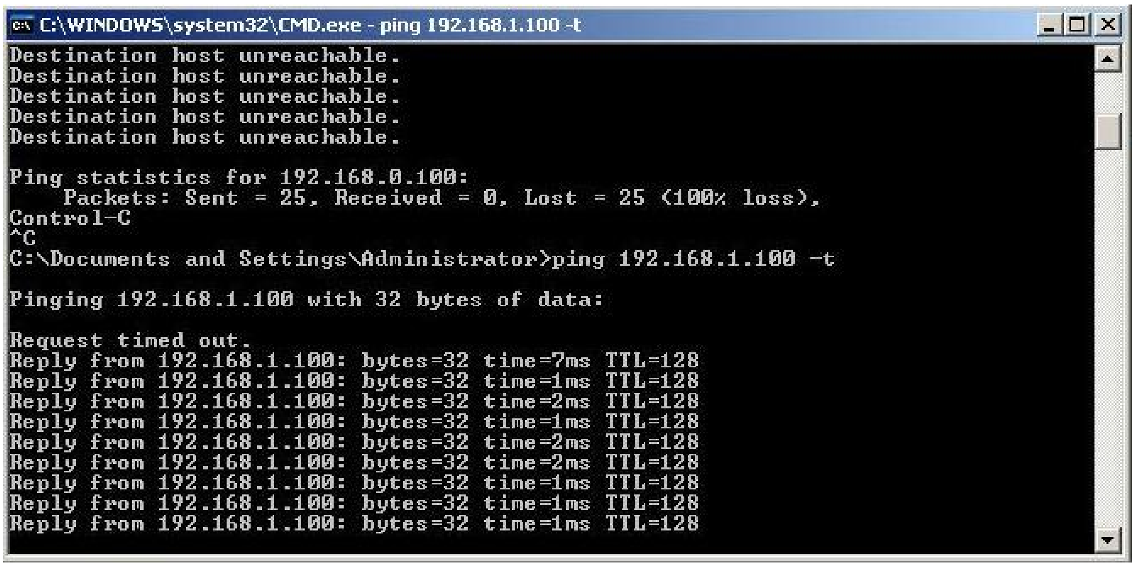
This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

Encryption:	WPA2 (AES)
WEP Key Format:	ASCII (5 characters)
WEP Key:	
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	••••••••••

Step 9. Click "**Apply Changes**" to apply the settings.

Step 10. Use command line tool to ping each other to ensure the link is successfully established.

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



```
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

Note

The attention of the following hints should be paid:

1) The encryption method and channel must be the same for both sites.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "**RF Output Power**" of both sites to half or lower.

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product : 2.4GHz 802.11n 150Mbps Wireless LAN Outdoor CPE AP/Router

*Model Number : WNAP-6315

* 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 herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE, Low Voltage Directive 2006/95/EC.
For the evaluation regarding the R&TTE the following standards were applied:

EN 55022 CLASS B	(2010/AC:2011)
EN 61000-3-2	(2006+A1:2009+A2:2009)
EN 61000-3-3	(2013)
EN 55024	(2010)
IEC61000-4-2	(2008)
IEC61000-4-3	(2006+A1:2007+A2:2010)
IEC61000-4-4	(2012)
IEC61000-4-5	(2014)
IEC61000-4-6	(2013)
IEC61000-4-8	(2009)
IEC61000-4-11	(2004)
EN 300 328 V1.8.1	(2012)
EN301 489-1 V1.9.2	(2011)
EN 301 489-17 V2.2.1	(2012)
EN 62311	(2008)
EN 60950-1	(2006 + A11: 2009 + A1:2010 + A12:2011)

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
Place

24th July, 2015
Date

Kent Kang
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.