11n Wireless Access Point

WNAP-1120

WNAP-1120PE

User's Manual

Copyright

Federal Communication Commission Interference Statement

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

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

FCC Caution

To assure continued compliance. (Example-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, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

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.

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, and France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Potential restrictive use

France: Only channels 10, 11, 12 and 13

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's Manual for PLANET 802.11N Wireless Access Point

Model: EM-WNAP1120v2 / WNAP-1120PE

Rev: 2.3 (March, 2009)

Part No. EM-WNAP1120v2

TABLE OF CONTENTS

Chapter 1 Introduction

Thank you for purchasing WNAP-1120PE / WNAP-1120. This manual guides you on how to install and properly use the WNAP-1120PE/WNAP-1120 in order to take full advantage of its features.

The WNAP-1120PE / WNAP-1120 is the 802.11n Wireless Access Point with high speed 300Mbps IEEE802.11n Draft 2.0 MIMO Technology. Fully compliant with IEEE802.11b/g standard, it provides powerful features such as the Web Configuration, Multiple SSID / VLAN tag, Built-in Radius server, MAC filter, WPA2-PSK, WPA and WPA2. With the six wireless operating modes, establish their wireless easily. Without utility install, user doesn't need to find the utility for this product in lots of program list. It can be configured in different OS that provides web browser. There are two models in this 802.11n Wireless Access Point, WNAP-1120, standard model and WNAP-1120PE, PoE (Power over Ethernet) model.
In the following sections throughout this guide, unless specified, terms "**11N AP**" will means your WNAP-1120 or WNAP-1120PE.

1.1 Package Contents

Make sure that you have the following items:

- 1 x **11N AP**
- 1 x 5V 1A Power Adapter
- 1 x User's Manual CD
- 2 x 3dBi External Antenna
- 1 x Ethernet Cable
- 1 x Quick Installation Guide

Note:	If any of the above items are missing, contact your supplier as soon as possible.

1.2 Features

- Compliant with IEEE 802.11n (Draft 2.0) wireless technology capable of up to 300Mbps data rate
- Support PoE port (IEEE802.3af compliant for WNAP-1120PE)
- Supports Wi-Fi Protected Setup (WPS)
- Compliant with 802.11g / 802.11b standard
- Farther coverage, less dead spaces and higher throughput with 802.11n technology
- Supports 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 (AES with IEEE 802.1x)
- AP / Station-Infrastructure / Bridge Point to Point / Bridge Point to Multipoint / WDS / Repeater modes supported
- Supports DHCP Server
- System monitoring includes Active wireless client Table.

- Easy to use Web-based GUI for configuration and management purposes
- Multiple SSID / 802.11Q tagging function
- MAC filter access control and Built-in Radius Server function

1.3 LED Indicators

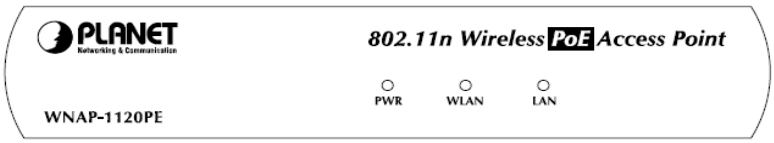


Figure: Front panel of 11N AP (example on WNAP-1120PE)

LED	Color	STATE	MEANING
PWR	Green	On	Device power on
		Off	Device power off
		Blinking	During boot up procedure
WLAN	Orange	Blinking	Transmitting or receiving data through the Wireless LAN
		Off	Wireless LAN is no function
LAN	Green	On	Link is established
		Blinking	Packets are transmitting or receiving
		Off	LAN port is not connected

1.4 Wireless Performance

The following information will help you utilizing the wireless performance and operating coverage of **11N AP**.

1. **Site selection**

   To avoid interferences, please locate the **11N AP** and wireless client away from transformers, microwave ovens, heavy-duty motors, fluorescent lights and other industrial equipments. Keep the number of walls or ceilings between AP and clients as few as possible. Otherwise the signal strength may be seriously reduced. Place the **11N AP** in an open space or add additional Access Point as needed to improve the coverage.

2. **Environmental factors**

   The wireless network is easily affected by many environment factors. Every environment is unique with different obstacles, construction materials, weather, etc. It is hard to determine the exact operation rage of **11N AP** in a specific location without testing.

3. **Antenna adjustment**

   The **11N AP** is designed base on 2T2R 11n MIMO technology. The two antennas (circled) are designed for TX/RX (Transmitting / Receiving) at the same time.

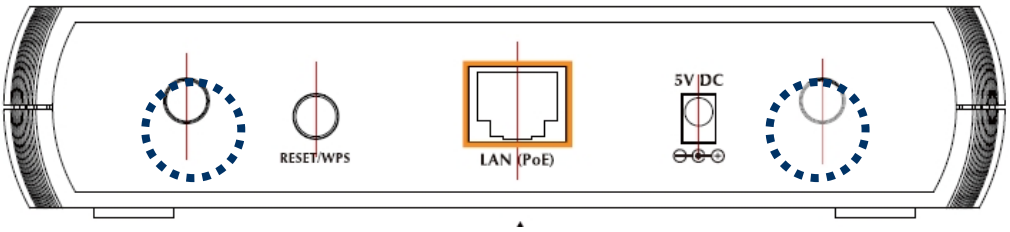


Figure: Rear Panel of 11N AP (example on WNAP-1120PE)

The bundle antennas of **11N AP** are adjustable. Firstly install the antennas pointing straight up, and then smoothly adjust it if the radio signal strength is poor. But the signal reception is definitely weak in some certain areas, such as location right down the antenna.

Moreover, with RP-SMA connector, the original antennas of the **11N AP** can be replaced with other external antennas to extend the coverage. Please check the specification of the antenna you want to use, and make sure it can be used on **11N AP**.

4. WLAN Type

If your **11N AP** is installed in an 802.11n and 802.11b/g mixed WLAN, its performance will be reduced significantly. Because every 802.11n OFDM packet needs to be preceded by an RTS-CTS or CTS packet exchange that can be recognized by legacy 802.11b/g devices. This additional overhead lowers the speed. If there are no 802.11b devices connected, or if connections to all 802.11b/g devices are denied so that your **11N AP** can operate in 11n-only mode, then its data rate shall increased up to 300Mbps.

1.5 Reset/WPS Button

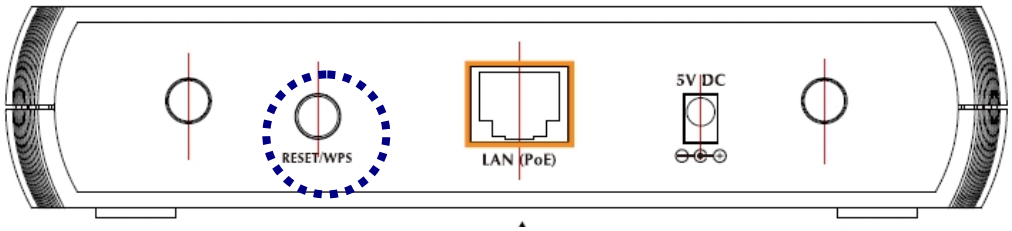


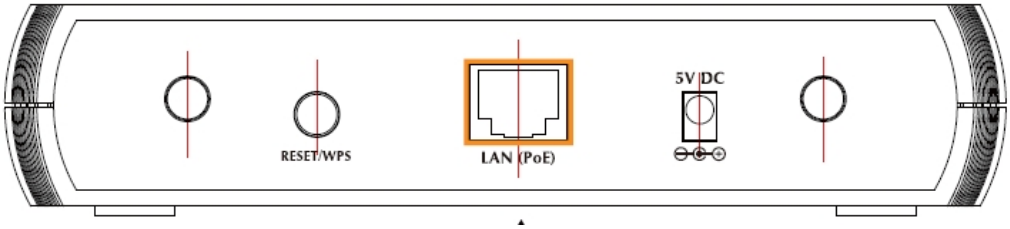
Figure: Rear Panel of 11N AP (example on WNAP-1120PE)

The **11N AP** provides a Reset button on the rear panel for user to restart or set **11N AP** configuration to factory default.

RST / WPS Button	This button has two functions: **To Clear All Data and restore the factory default values:** Press the RST (reset) button for longer than 20 seconds until the LED of power flash, and then the **11N AP** will reset itself to the factory default settings. (**Warning**: your original configurations will be replaced with the factory default settings) **To make Wi-Fi Protected Setup (WPS) simple and easier:** Press the WPS button (for less than 3 seconds); machine will start WPS function to build connection between wireless network clients and this wireless router.

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the **11N AP**.



1. **Locate an optimum location for the 11N AP.** The best place for your **11N AP** is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. **Assemble the antenna to the 11N AP.** Try to place them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
3. **Connect RJ-45 cable to 11N AP.** Connect this **11N AP** to your LAN switch/hub or a single PC.

Note:	The **WNAP-1120PE** also with IEEE802.3af Power over Ethernet PD (Powered Device) compliant, you can connect WNAP-1120 to an IEEE802.3af compliant PSE (Power Sourcing Equipment). The IEEE802.3af complied PSE shall provide the power for the WNAP-1120 after connected.

4. **Plug in power adapter and connect to power source**. After power on, the **11N AP** will start to work.

Note:	1. ONLY use the power adapter supplied with the **11N AP**. Otherwise, the product may be damaged. 2. ONLY use one power sources for your **WNAP-1120PE**. That is for **WNAP-1120**, either power it from 802.3af PoE or from DC power source. 3. If you want to reset your **11N AP** to default settings after it is powered on, press the Reset button for 20 seconds. Then release the button and wait for 10 seconds for rebooting.

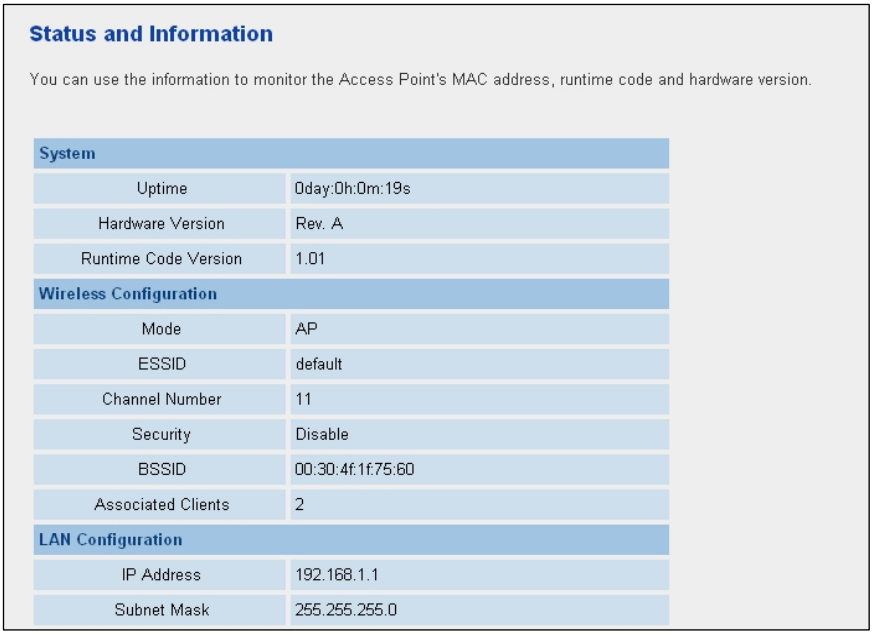
Chapter 3 Web Configuration

Web configuration provides a user-friendly graphical user interface (web pages) to manage your **11N AP**. An AP with an assigned IP address (e.g. **http://192.168.1.1**) will allow you to monitor and configure (via web browser e.g., MS Internet Explorer or Netscape).

1. Open your web browser.
2. Enter **11N AP** IP address (default IP address is **http://192.168.1.1**) into the address field. Please also make sure your PC's IP address is in the same IP range with **11N AP**.
3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. Default User Name and Password are "**admin**". Click "OK" to access the management page.

3.1 Home

In this screen, you can check all the information of the **11N AP**.



Here are descriptions of every item:

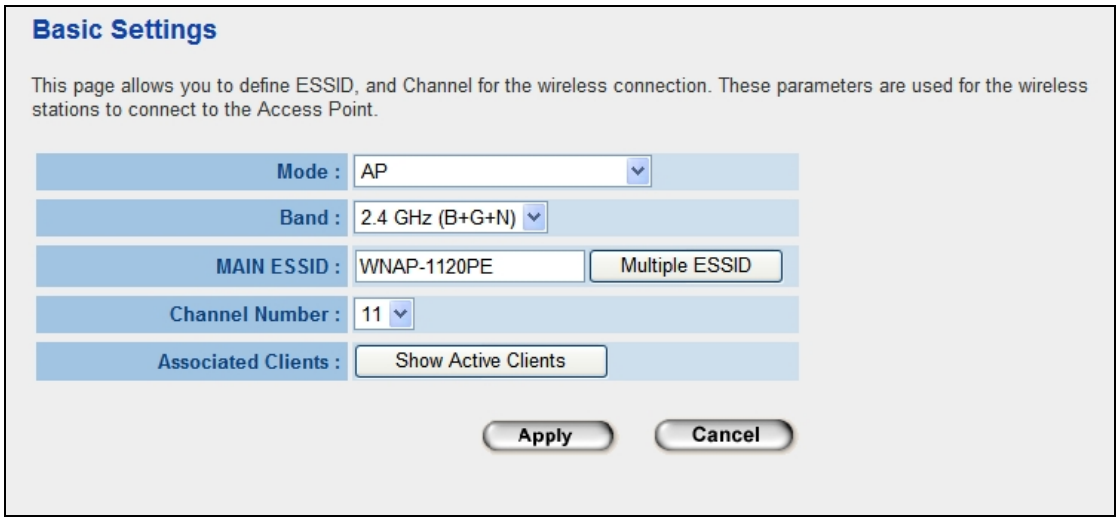
Up time	Displays the total passed time since the wireless access point is powered.
Hardware Version	Displays hardware version.
Runtime Code Version	Displays current firmware version. If you want to perform firmware upgrade, this number will help you to determine if you need such upgrade.
Mode	Displays the current wireless operating mode (see next Section)
ESSID	Displays current ESSID (the name used to identify this wireless access point)
Channel Number	Displays current wireless channel number
Security	Displays current wireless security setting
BSSID	Displays current BSSID (a set of unique identification name of this access point, it can not be modified by user)
Associated Clients	Displays the number of connected wireless client
IP Address	Displays the IP address of this wireless access point
Subnet Mask	Displays the net mask of IP address
Default Gateway	Displays the IP address of default gateway
MAC address	Displays the MAC address of LAN interface

3.2 Basic Setting

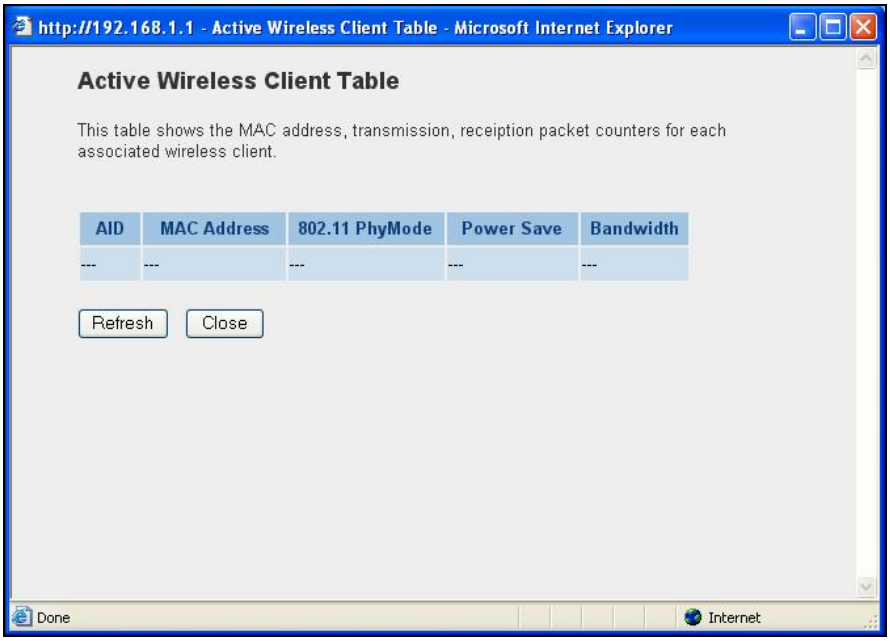
In this screen, you can configure the **11N AP** to work in different operating mode. Please refer to below sections to know the details configuration of each operating mode.

3.2.1 AP Mode

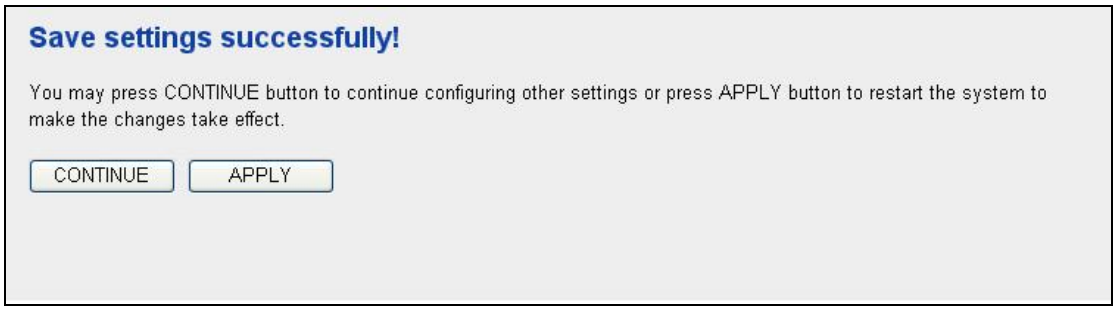
This mode is set to **11N AP** by default. It served as a transparent Media Access Control (MAC) bridge between wired and wireless network.



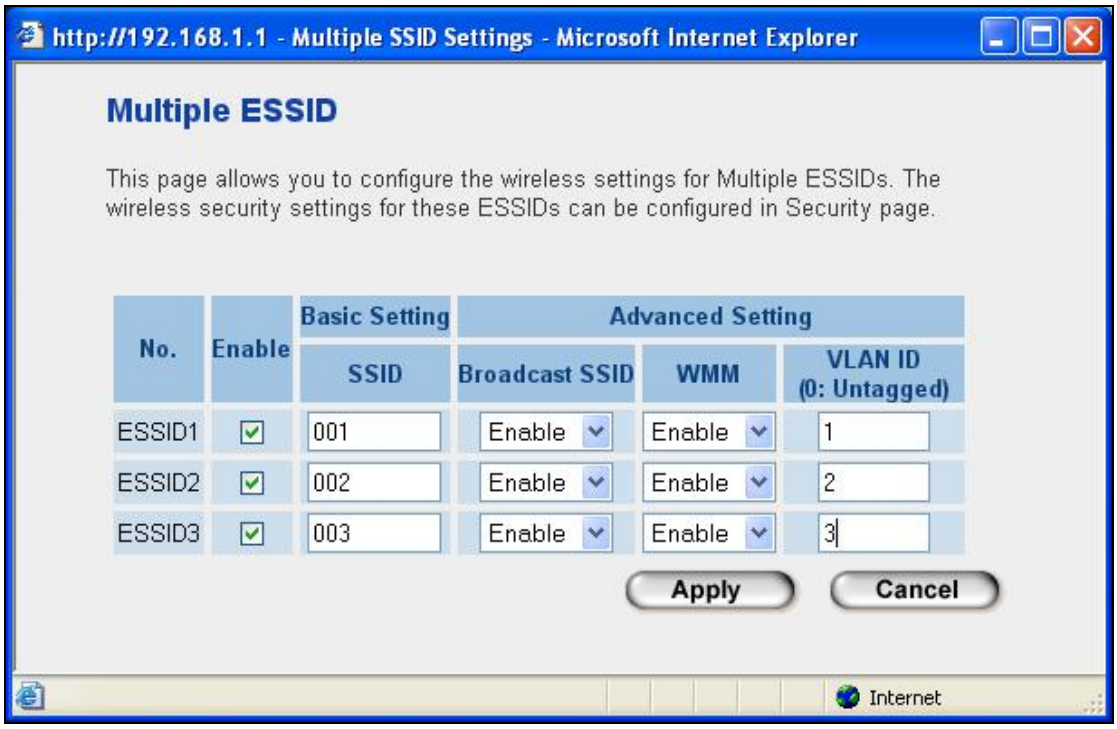
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (B+G):** It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously.
MAIN ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLAN. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Multiple ESSID	The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, please click this button. For detailed descriptions of the function, please refer to Section 3-2-1-1.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)

Associated Clients	You may press "**Show Active Clients**" button to check the connected client information. After the button pressed, you will see the dialog box as below.  You may press "**Refresh**" to get the new client table or "**Close**" to close this dialog box.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen below to prompt you the settings are saving successfully. If you press "Continue", you can proceed to configure other settings. However, the new configurations are not take effect at this time. You must click "Apply", and then the **11N AP** will restart with new configuration. You may check the LED status to make sure **11N AP** finishes the restart.



3.2.1.1 MULTIPLE ESSID SETTING

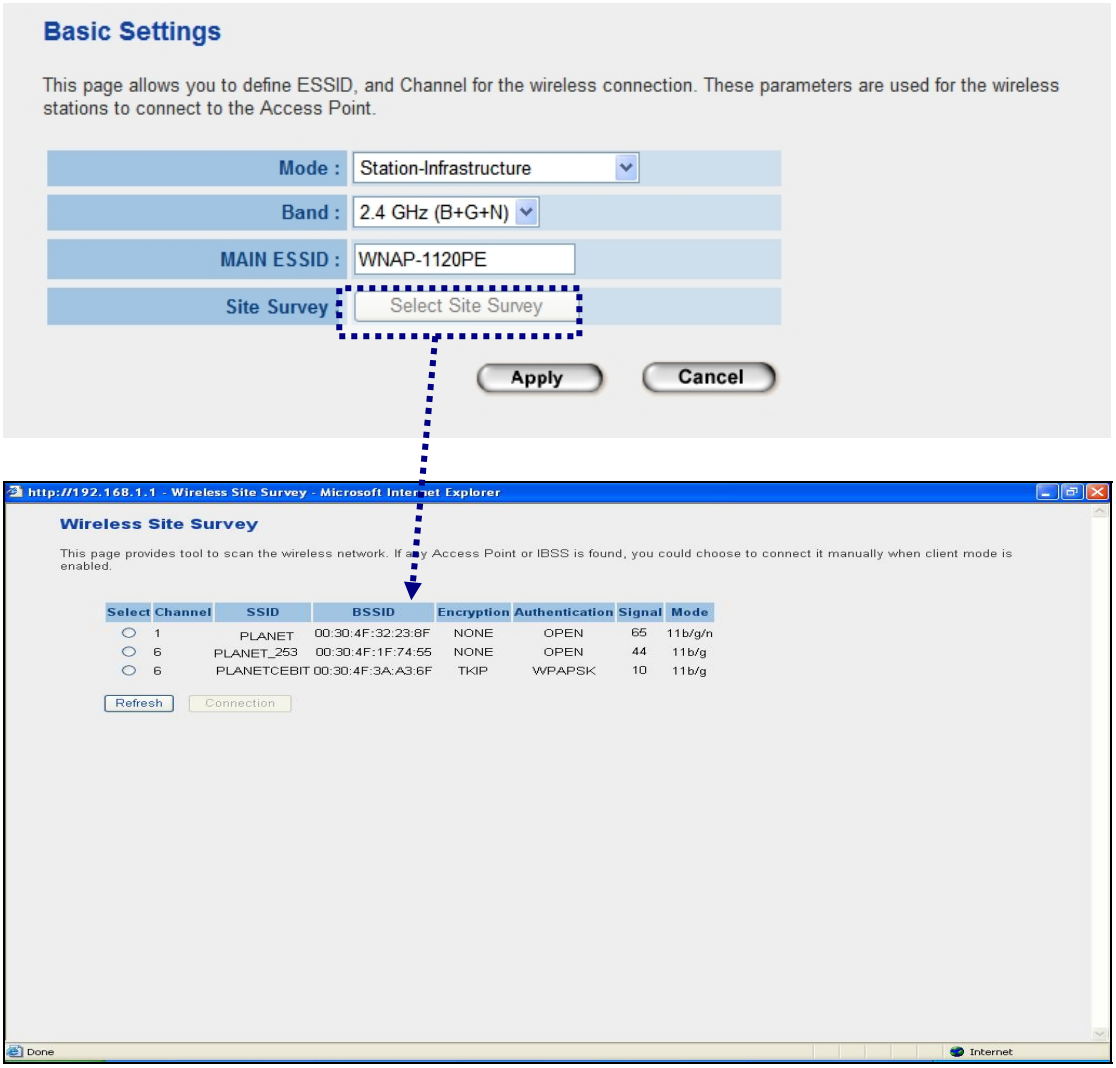


Here are descriptions of every setup item:

No.	Except Main SSID, you can configure additional three ESSID here.
Enable	Select the box to enable the different additional ESSID.
SSID	Please input the SSID name (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. PLEASE NOTE THAT ESSID IS **CASE SENSITIVE**.
Broadcast SSID	Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only people those who know the ESSID of your wireless access point can get connected.
WMM	WMM (Wi-Fi Multimedia) technology, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
VLAN ID (0:Untagged)	If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 1 to 4094. The VLAN ID is 0 by default (VID range is "0~4904"), it means that disable the VLAN function for the ESSID.

3.2.2 Station - Infrastructure Mode

11N AP serves as a wireless station (infrastructure) in this mode. Connected to a PC or a small LAN (no more than 2 PCs), it allows the PC or small LAN able to access the wireless network via Access Point.



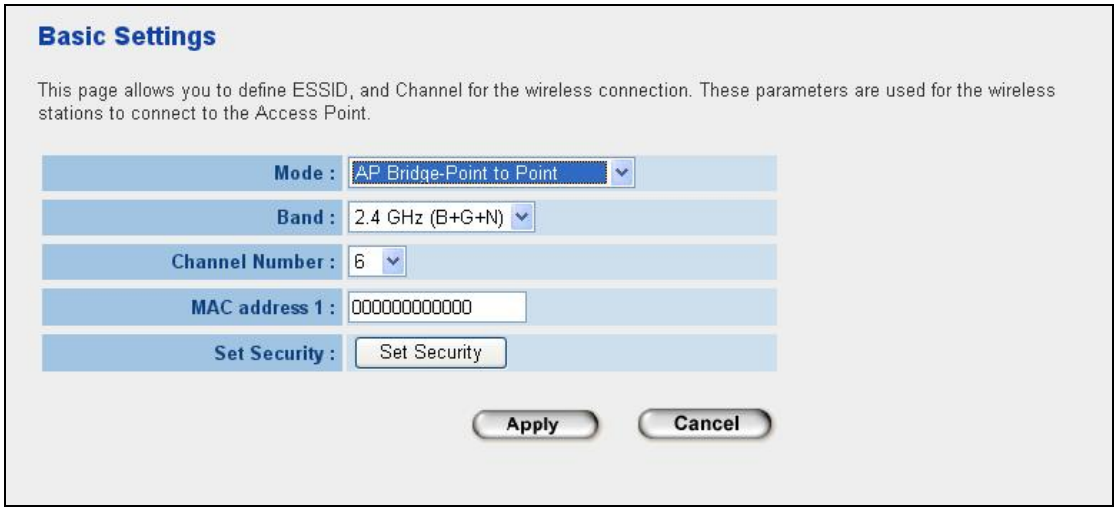
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (N):** It forces the **11N AP** to operate in 802.11n only. **2.4GHz (B+G):** It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the **11N AP** to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	Please make sure the ESSID of the wireless network that you will connect

	and enter the correct value in this field. The default SSID is "**default**".
WLAN MAC	**Keep default setting**: **11N AP** will use its own MAC address to access the wireless LAN. **Press "MAC Clone" button**: It will use PC's MAC address to access the wireless LAN.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart the **11N AP** with new configuration.

3.2.3 AP Bridge - Point to Point Mode

This function allows **11N AP** to bridge 2 wired Ethernet networks wirelessly.



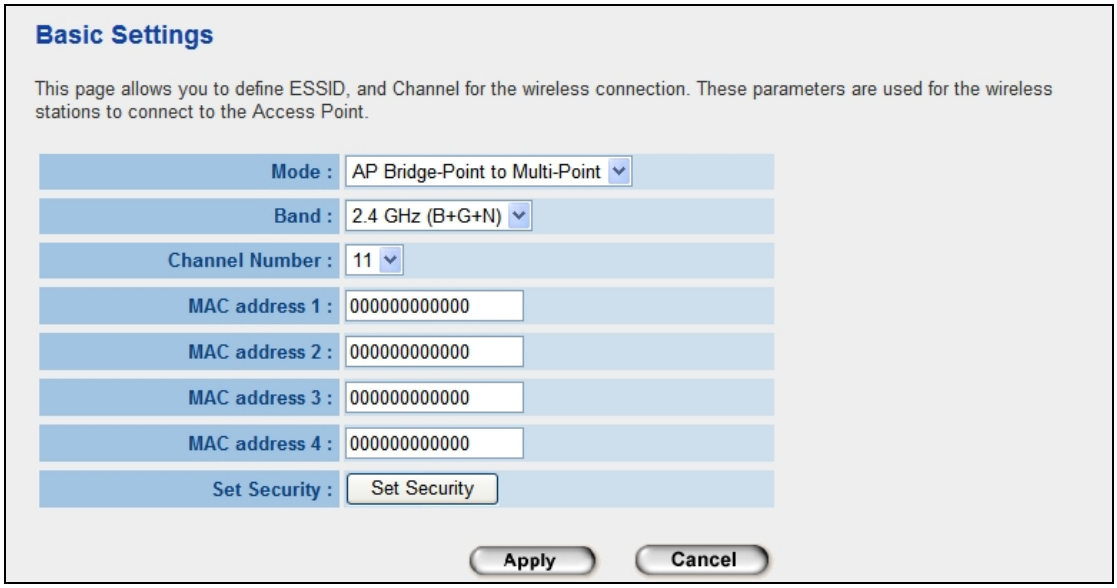
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (N):** It forces the **11N AP** to operate in 802.11n only. **2.4GHz (B+G):** It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the **11N AP** to operate in 802.11b, 802.11g, and 802.11n simultaneously.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)

MAC Address 1	**Keep default setting**: The **11N AP** will use its own MAC address to access the wireless LAN..
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section "3.2.8 Security setting for bridge mode" to configure the detail settings.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart the **11N AP** with new configuration.

3.2.4 AP Bridge - Point to Multipoint Mode

This function allows **11N AP** to bridge more than 2 wired Ethernet networks together by wireless connection.



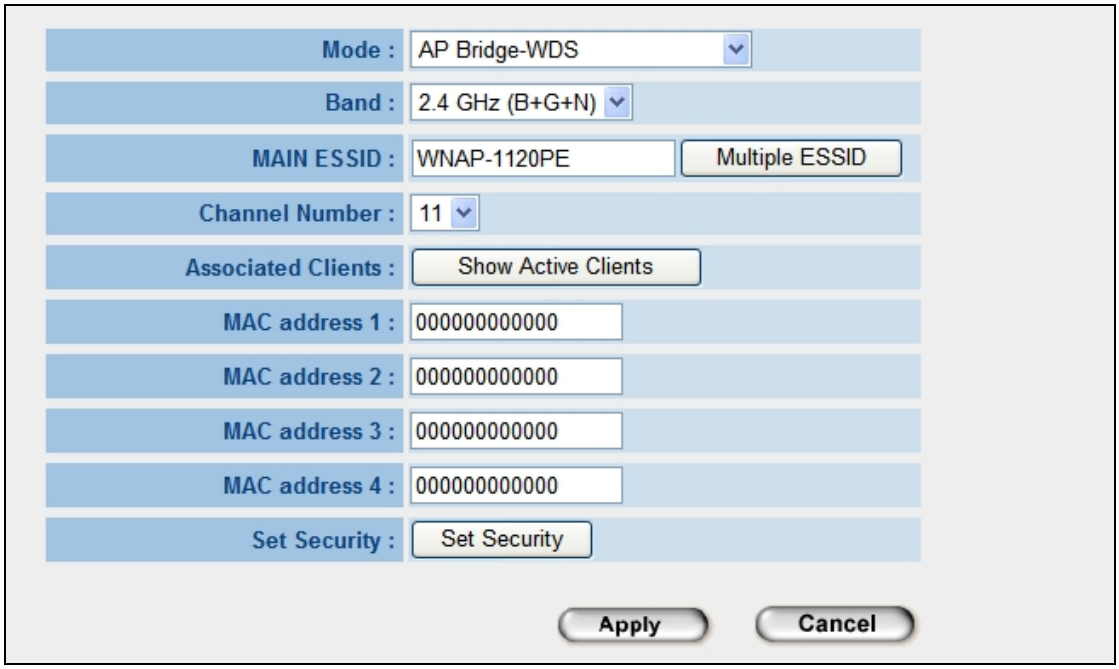
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (N):** It forces the **11N AP** to operate in 802.11n only. **2.4GHz (B+G):** It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the **11N AP** to operate in 802.11b, 802.11g, and 802.11n simultaneously.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country.

	Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
MAC Address 1~4	If you want to bridge multiple **11N AP** in this mode, you have to enter the MAC addresses of other **11N AP** into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section "3.2.8 Security setting for bridge mode" to configure the detail settings.

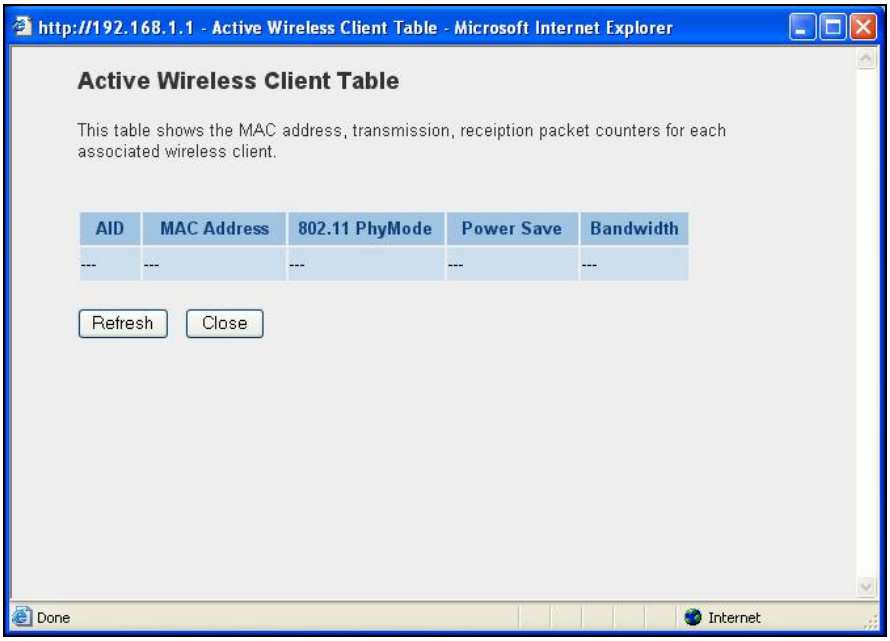
After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart the **11N AP** with new configuration.

3.2.5 AP Bridge - WDS Mode

If you want **11N AP** to bridge to other **11N AP** and provide access for other wireless clients at the same time, you have to set the **11N AP** to "AP Bridge - WDS". Simply speaking, "AP Bridge - WDS" function is the combination of "AP mode" and "AP Bridge-Point to Multi-Point mode".



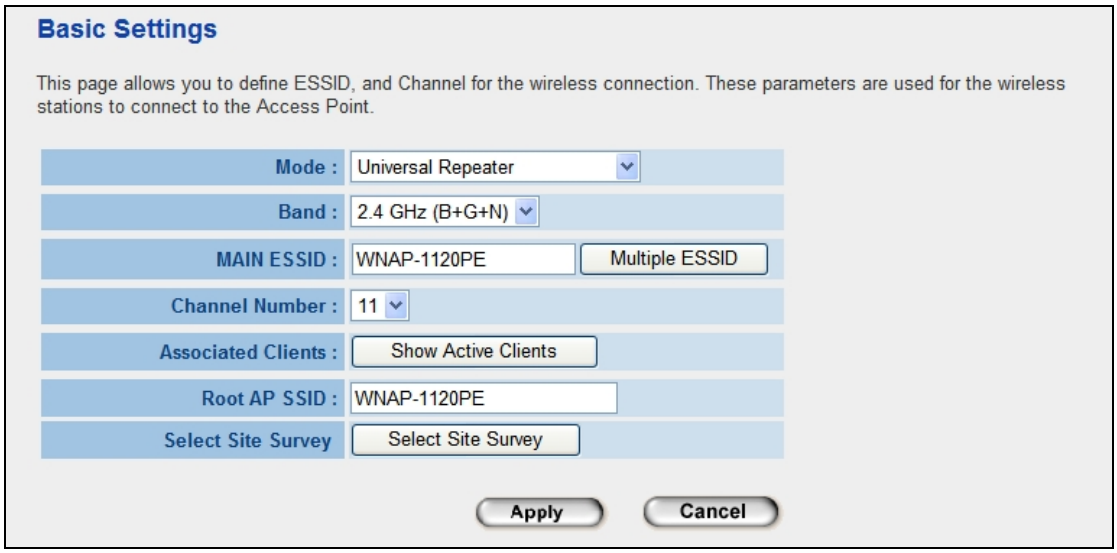
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (N):** It forces the **11N AP** to operate in 802.11n only.

	2.4GHz (B+G): It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the **11N AP** to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
Associated Clients	You may press "Show Active Clients" button to check the connected client information. After the button pressed, you will see the dialog box as below:  You may press "Refresh" to get the new client table or "Close" to close this dialog box.
MAC Address 1 ~4	If you want to bridge multiple **11N AP** in this mode, you have to enter the MAC addresses of other **11N AP** into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press "Set Security" button and refer to section "3.2.7 Security setting for bridge mode" to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.2.6 Universal Repeater Mode

This mode allows you to extend the range of your wireless network. When the AP is configured to repeater mode, it will repeat the wireless signal from wireless client to access point. Thus, the wireless connection distance can be extended. However, the performance will become half of normal performance when client connect to a Repeater. Besides, when the **11N AP** is configured to repeater mode, you can only manage the AP through LAN interface and the PC(s) connected to its LAN port cannot communicate with other wireless clients.



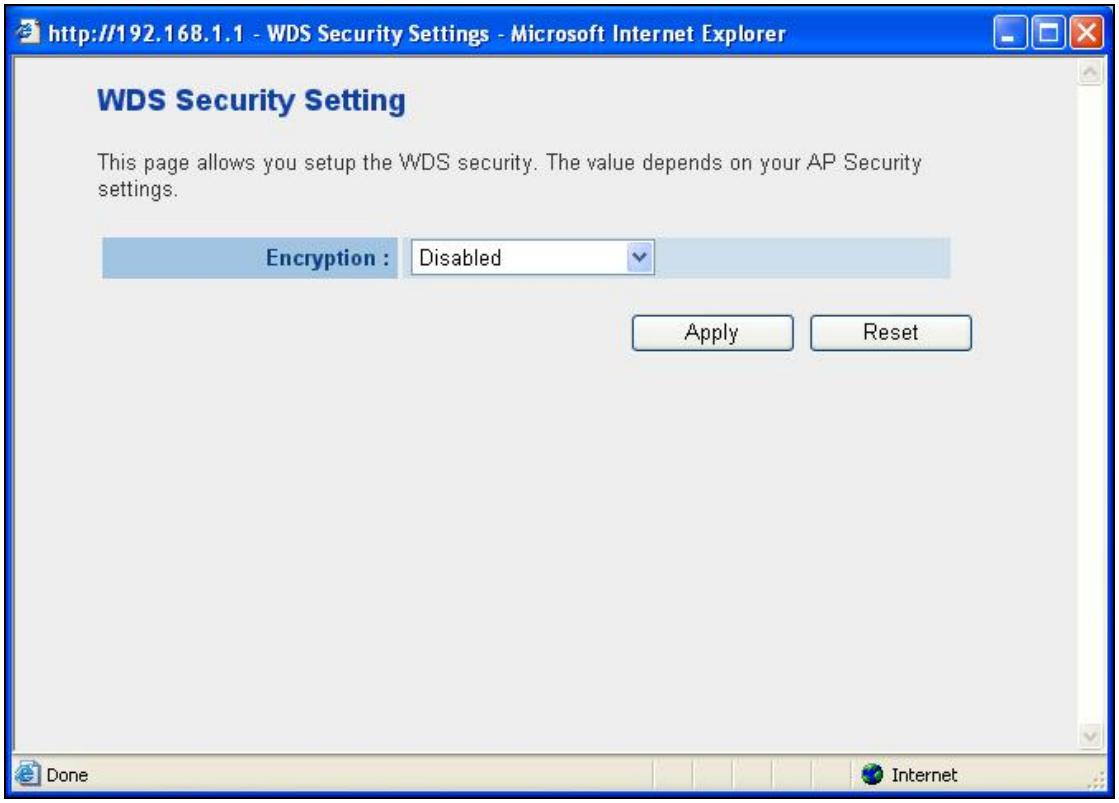
Parameter	Description
Mode	Shows the current operation mode.
Band	**2.4GHz (B):** It forces the **11N AP** to operate in 802.11b only. **2.4GHz (G):** It forces the **11N AP** to operate in 802.11g only. **2.4GHz (N):** It forces the **11N AP** to operate in 802.11n only. **2.4GHz (B+G):** It allows the **11N AP** to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the **11N AP** to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is “**default**”.

Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
Associated Clients	You may press “Show Active Clients” button to check the connected client information. After the button pressed, you will see the dialog box as below.  You may press “Refresh” to get the new client table or “Close” to close this dialog box.
WLAN MAC	**Keep default setting**: **11N AP** will use its own MAC address to access the wireless LAN. **Press “MAC Clone” button**: It will use PC’s MAC address to access the wireless LAN.
Root AP SSID	In “Universal Repeater mode”, this device can act as a station to connect to a Root AP. You should enter the SSID of the Root AP here.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.2.7 Security setting of bridge mode

In “AP Bridge-Point to Point mode”, “AP Bridge-Point to Multi-Point mode” and “AP Bridge-WDS mode”, you can click “Set Security” to add encryption for the communication between the bridged access points. This can protect your wireless network.



Parameter	Description
Encryption	You can select “None”, “WEP 64bits”, “WEP 128bits”, “WPA (TKIP)” or “WPA2 (AES)” of this option . It is set to “None” by default.
Key Format	This is only used when you select “WEP 64bits” or “WEP 128bits” encryption method. You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
WEP Key	This is only used when you select “WEP 64bits” or “WEP 128bits” encryption method. The WEP key is used to encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Pre-shared Key Format	This is only used when “WPA” or “WPA2” is selected. You may use Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.

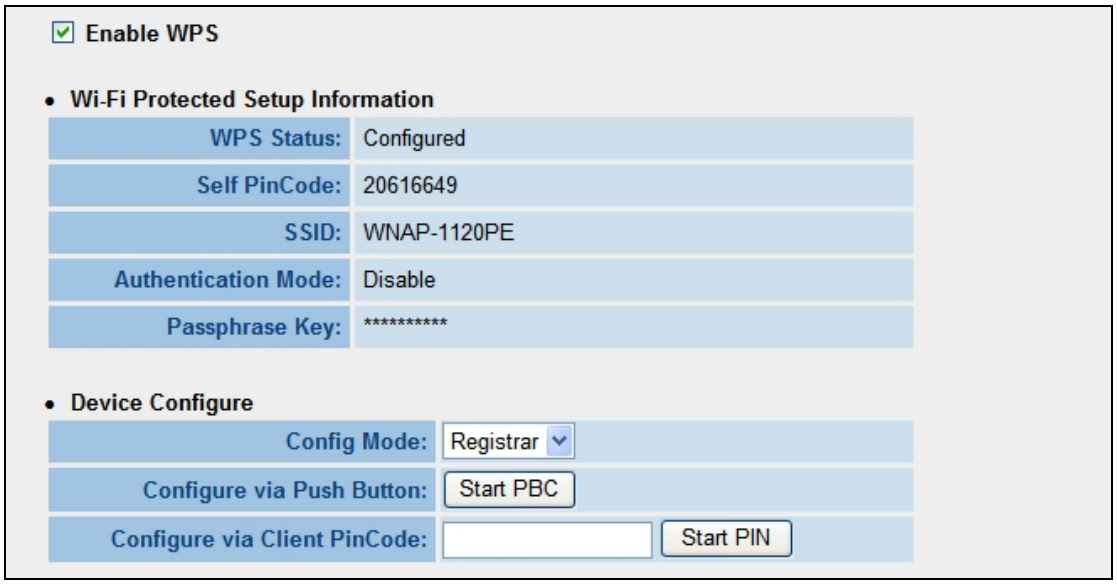
Pre-shared Key	This is only used when “WPA” or “WPA2” is selected. The Pre-shared key is used to authenticate and encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. Hex (64 characters): input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) Passphrase: at least 8 characters.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.3 WPS Settings

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless router. You don’t have to select encryption mode and input a long encryption pass phrase every time when you need to setup a wireless client, you only have to press a button on wireless client and router, and the WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode too. You can push RET/WPS button of this wireless router, or click ‘Start PBC’ button in the web configuration interface to do this. If you want to use PIN code, you can see the setup as below.



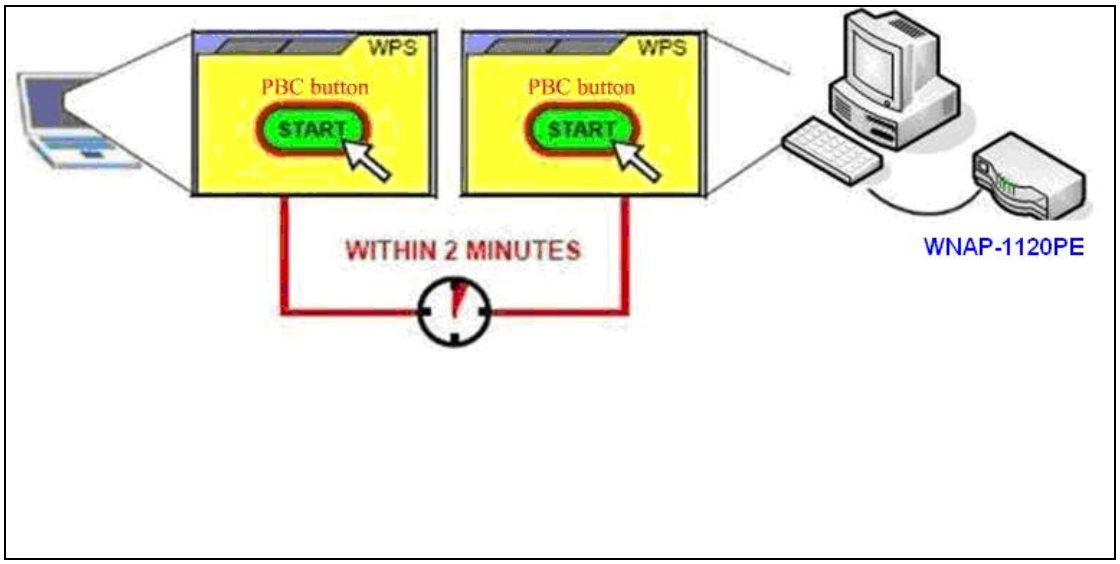
Parameters	Description
Enable WPS	Check this box to enable WPS function, uncheck it to disable WPS.
Wi-Fi Protected Setup Information	WPS-related system information will be displayed here.

WPS Status	If the wireless security (encryption) function of this wireless router is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'unConfigured'.
Self PIN code	This is the WPS PIN code of this wireless router. This code is useful when **11N AP** router sets as Enrollee, you need to fill this number into the web page of the other device.
SSID	The SSID of this wireless router will be displayed here.
Authentication Mode	The wireless security authentication mode of this wireless router will be displayed here.
Passphrase Key	Confirming your Identity Key Store Pass-phrase. It is allowed you to easily remember the key what you may want to remember is that if the passphrase is used,

Device Configure	
Config Mode:	"Registrar", "Enrollee", please see the setup step as below.
Configure via Push Button	Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.
Configure via Pin Code	Please input the PIN code of the other device you wish to connect, and click 'Start PIN' button. The 'WLAN' led on the wireless router will be steady on when this wireless router is waiting for incoming WPS request. (Please see the detail as below.)

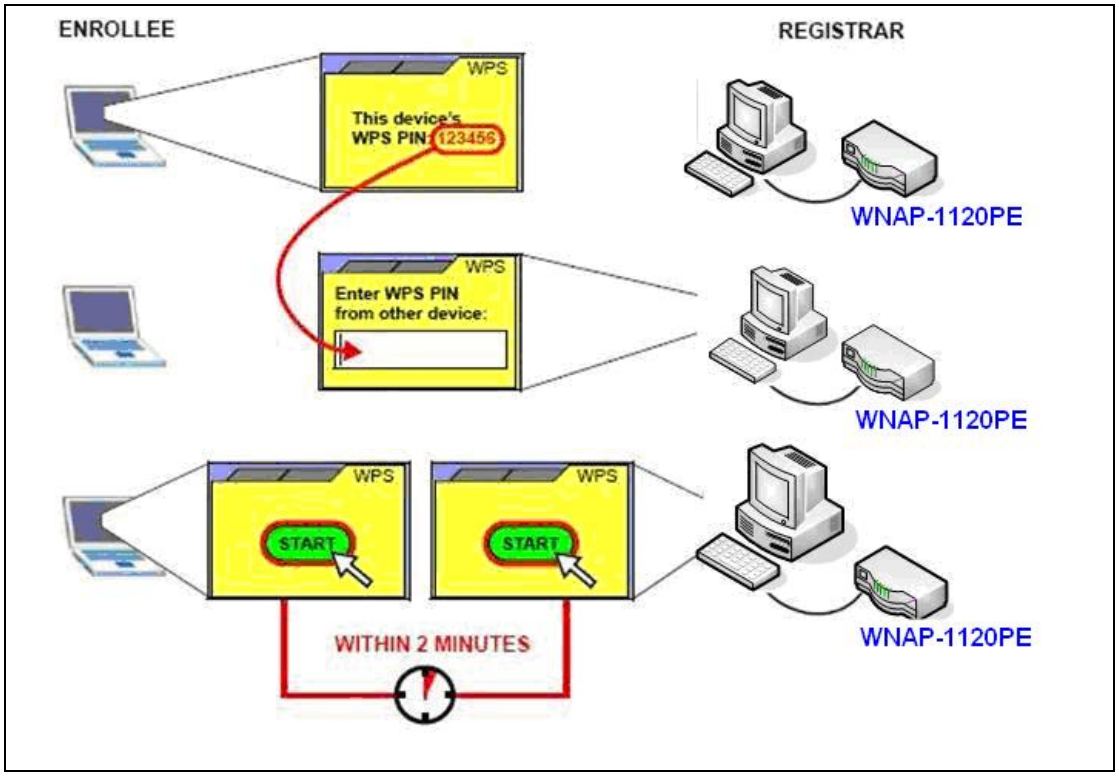
PBC setup step:

1. Ensure you have set the security setting on the **11N AP** (as Registrar).
2. Click the WPS button on **11N AP** (or the “Start PBC” button on the web interface of **11N AP**) and the other device (supports PBC function) in 2 minutes.
3. **11N AP** (Registrar) would send SSID and security key to the other device (Enrollee) through tunnel to connect.
4. If you see the wireless client in the list, WPS-PBC setting is successful.



PIN (as Registrar) setup step:

1. Select Config Mode: “Registrar” on **11N AP**.
2. Fill the PIN code of the other device (as Enrollee that support WPS-PIN setting) into the “configure via Client Pin code” of **11N AP**.
3. Click the PIN buttons on **11N AP** and the other device in 2 minutes.
4. If you see the wireless client in the list, WPS-PIN setting is successful.



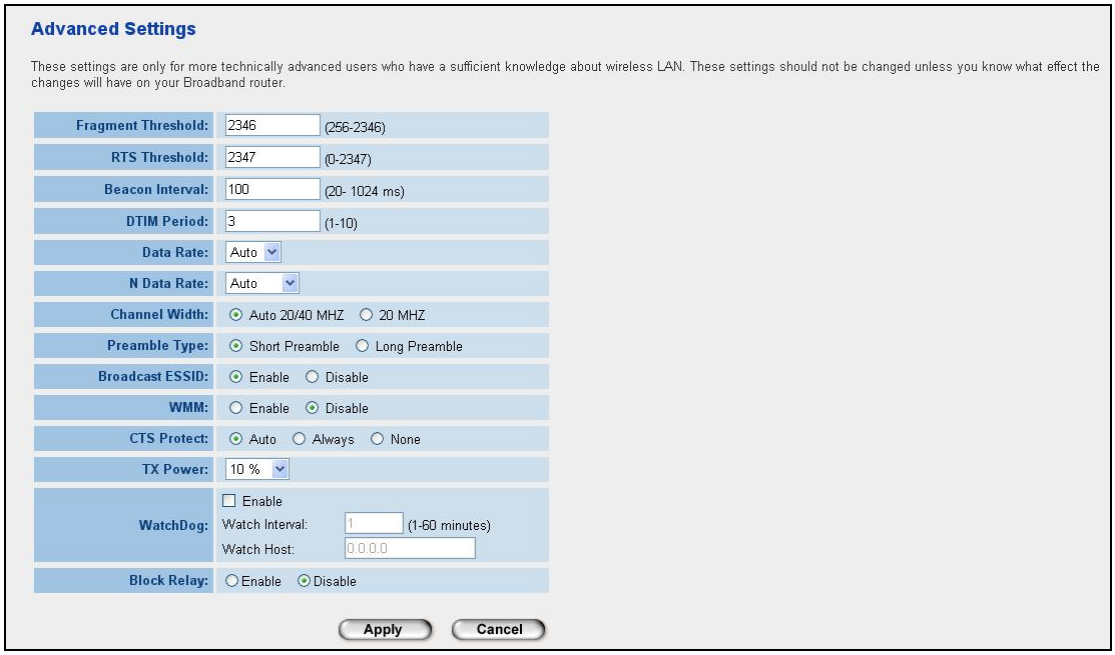
PIN (as Enrollee) setup step:

1. Select Config Mode: “Enrollee” on **11N AP**.
2. Fill the PIN code of **11N AP** into the other device (as Registrar).
3. Click the PIN buttons on **11N AP** and the other device in 2 minutes.
4. If you see the wireless client in the list, WPS-PIN setting is successful.

**** As the figure as above, just change two roles.**

3.4 Advanced Settings

You should not change these advanced parameters unless you know what effect the changes will have on this access point.



Parameter	Description
Fragment Threshold	"Fragment Threshold" specifies 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. ***Do not modify default value if you don't know what it is, default value 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. ***Do not modify default value if you don't know what it is, default value is 2347***
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network. ***Do not modify default value if you don't know what it is, default value is 100***
Data Rate	The "Data Rate" is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
N Data Rate	Set the data rate of 802.11 Draft-N clients, available options are MCS 0 to MCS 15, it's safe to set this option to 'Auto' and it's not necessary to change this value unless you know what will happen after modification.
Channel Width	Select wireless channel width (bandwidth taken by wireless signals of this access point). It's suggested to select 'Auto 20/40MHz'. Do not change to '20 MHz' unless you know what it is.

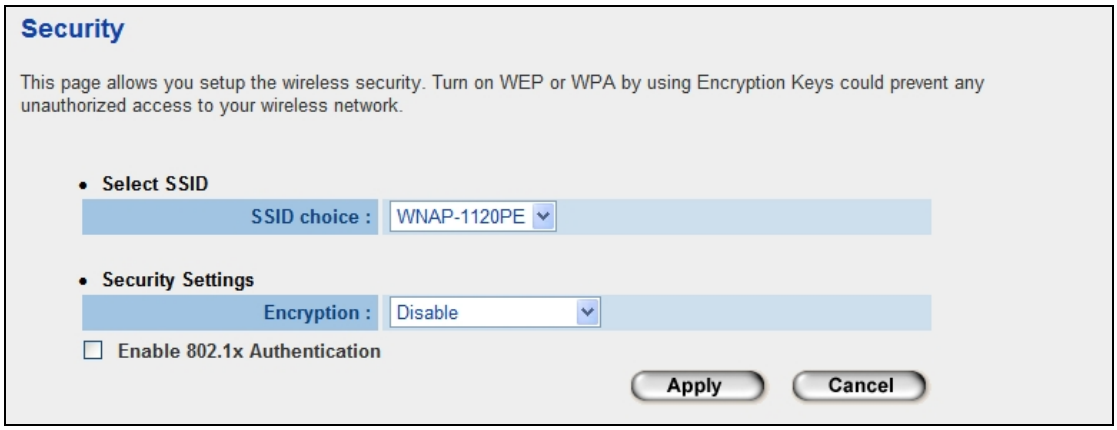
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “Short Preamble” is suitable for high traffic wireless network. “Long Preamble” can provide more reliable communication.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.
WMM	WMM (Wi-Fi Multimedia) technology, which can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It’s recommended to set this option to ‘Auto’.
TX Power	You can set the output power of wireless radio. Unless you’re using this wireless access point in a really big space, you may not have to set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless access point).
Watch dog	When you set the important Server in the same IP range topology , key the IP address in the Watch host space and set the time (1~60 minutes). When there is large traffic in the topology, you can not login the server during the setting time. The **11N AP** will reboot to solve the traffic jam status.
Block Relay	When you enable the function, the **11N AP** wireless users can not ping each other.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart the **11N AP** with new configuration.

3.5 Security

This Access Point provides complete wireless LAN security functions, includes WEP, 802.1x, 802.1x with WEP, WPA-PSK and WPA RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security mechanism. In default, the security option is “Disable”.

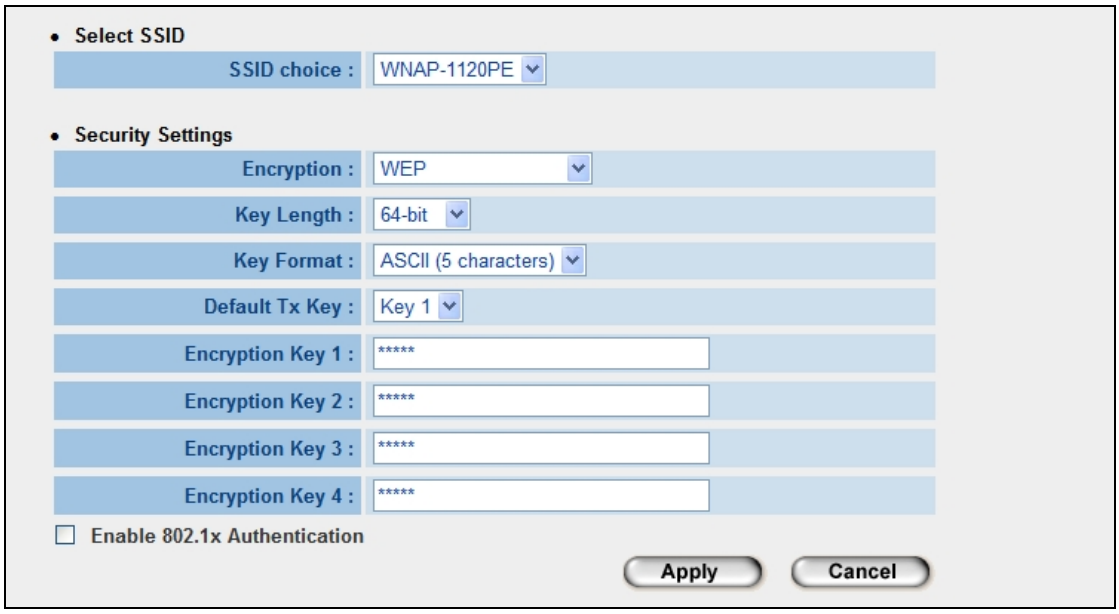
Note: This access point can act as a station and an AP at the same time in “Universal Repeater” mode. The security settings only apply to AP operation in “Universal Repeater” mode. The station operation has no security.



3.5.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can enter four WEP keys and select one of them as default key. Then the access point will only allow the clients configured with the same encryption keys for association. You can use WEP encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode”, “AP Bridge-WDS mode” and “Universal Repeater mode”.

If you would like to enable 802.1x Authentication also, please check the “Enable 802.1x Authentication” and refer to section 3.4.2 for the detail settings.

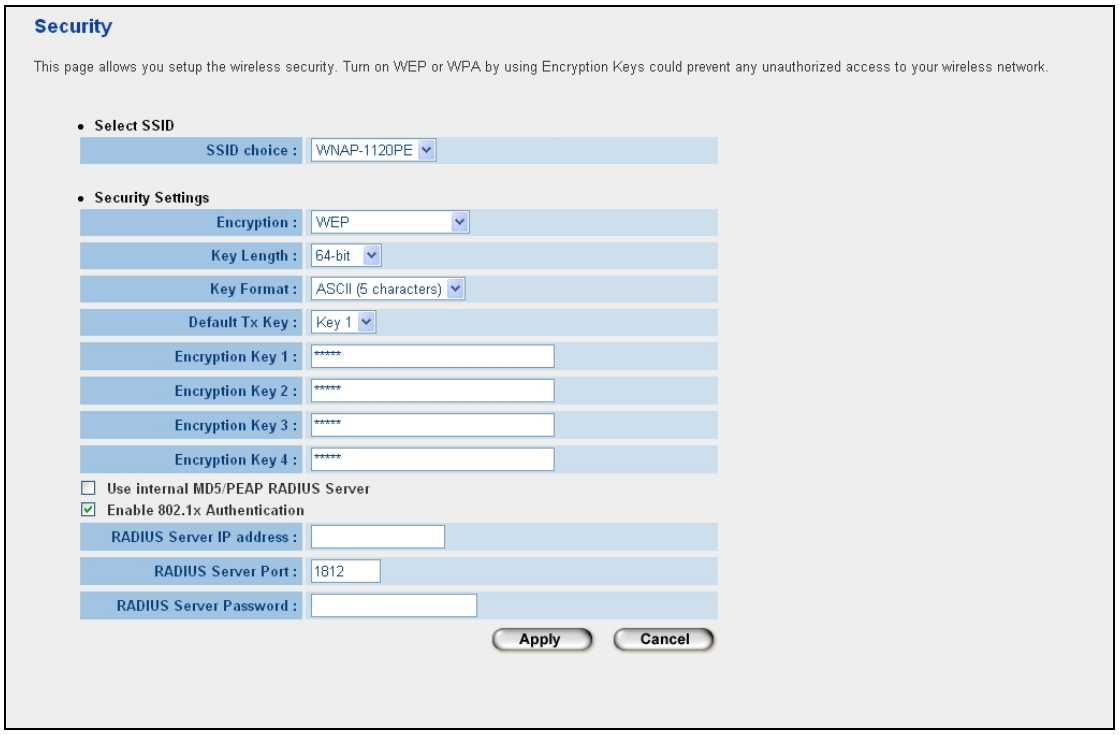


Parameter	Description
Encryption	Select “WEP” in this option.
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Enable 802.1x Authentication	Check this box when you want to enable 802.1x authentication with WEP encryption. You may refer to section 3.4.2 for detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart the **11N AP** with new configuration.

3.5.2 802.1x

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. It is suggested to enable 802.1x and WEP at the same time.

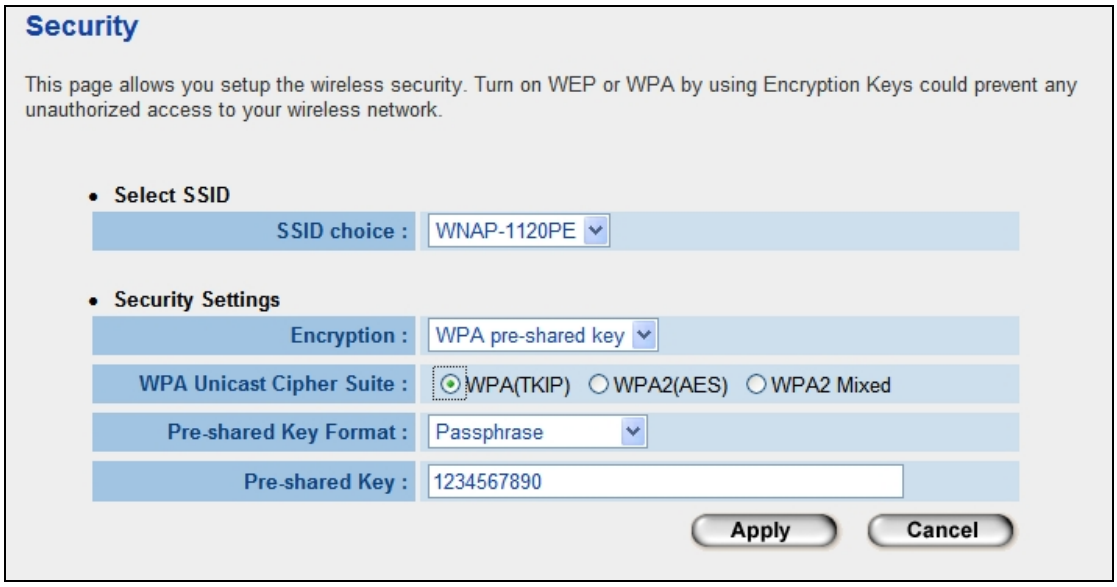


Parameter	Description
Encryption	If you want to use 802.1x only, keep this setting in “Disable”.
Enable 802.1x Authentication	Check this option to enable 802.1x function.
Use Internal MD5/PEAP RADIUS Server	**11N AP** has built in a RADIUS server. You can check this option to make the 802.1x authentication work with **11N AP** internal RADIUS server. If you would like to work with an external RADIUS Server, just leave this box blank and fill the fields below.
RADIUS Server IP Address	Enter RADIUS Server IP address.
RADIUS Server Port	Leave the default port setting or assign a new port number for this option.
RADIUS Server Password	Enter the password that is configured in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.5.3 WPA pre-shared key

WiFi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

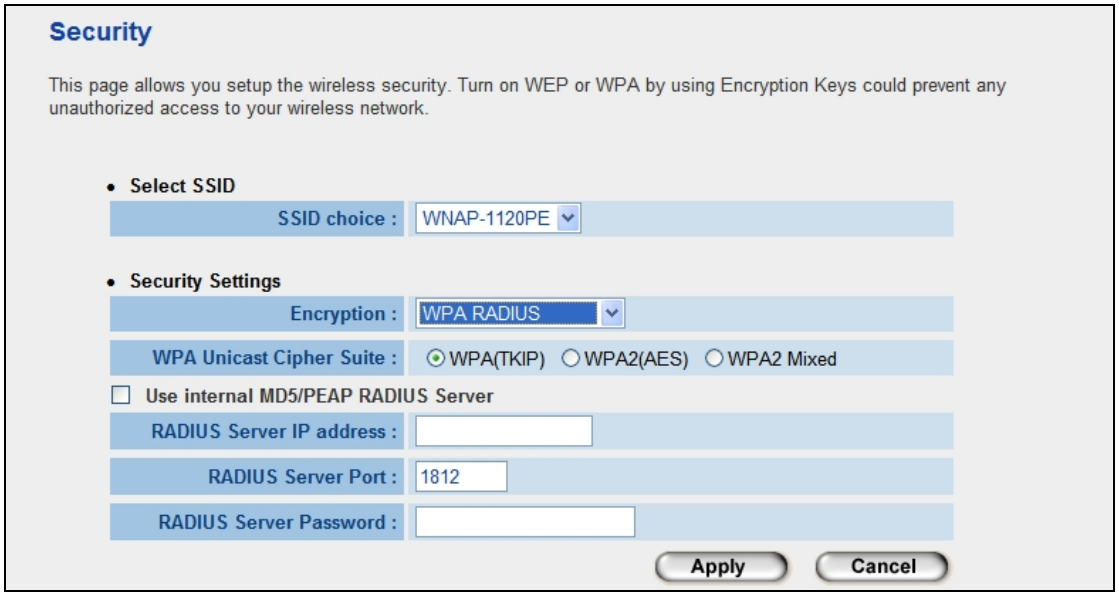


Parameter		Description
Encryption		Select “WPA pre-shared key” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) Passphrase: at least 8 characters.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.5.4 WPA RADIUS

You can use a RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. **11N AP** also provides an internal RADIUS server for user's convenience.

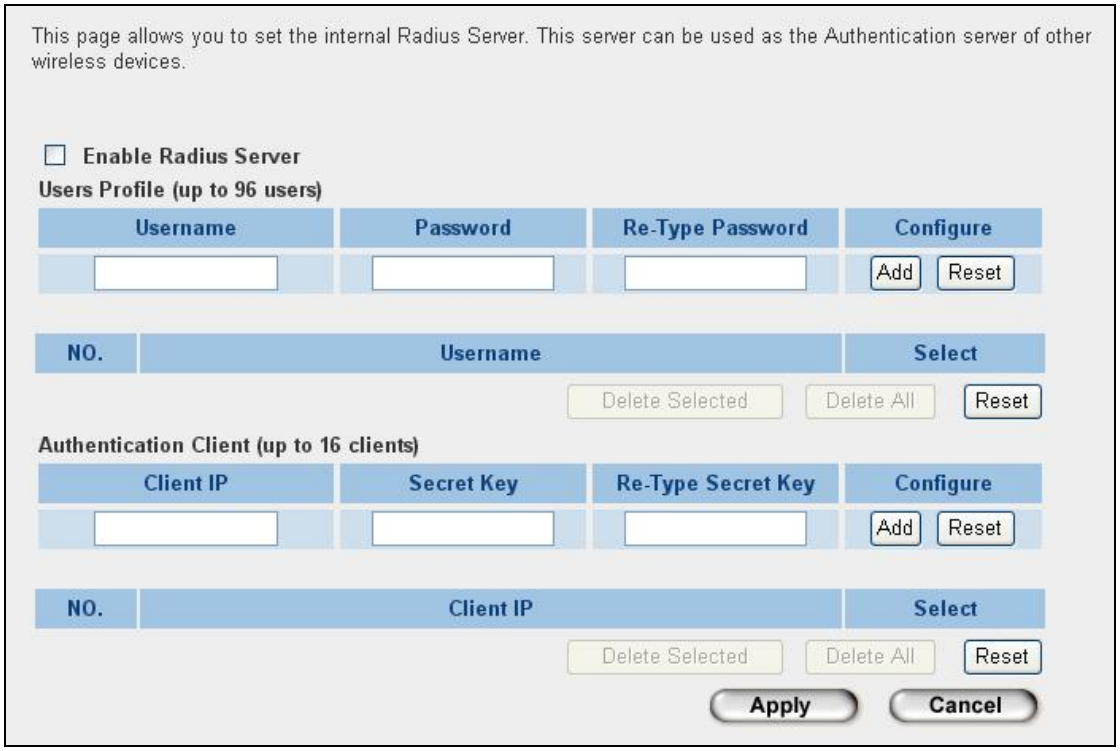


Parameter		Description
Encryption		Select "WPA RADIUS" in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Use Internal MD5/PEAP RADIUS Server		**11N AP** has built in a RADIUS server. You can check this option to make the 802.1x authentication work with **11N AP** internal RADIUS server. If you would like to work with an external RADIUS Server, just leave this box blank and fill the fields below.
RADIUS Server IP Address		Enter RADIUS Server IP address.
RADIUS Server Port		Leave the default port setting or assign a new port number for this option.
RADIUS Server Password		Enter the password that is configured in RADIUS Server.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart the **11N AP** with new configuration.

3.6 RADIUS Server

The **11N AP** has provided an internal RADIUS server to authenticate wireless station users. You have to add user accounts to the RADIUS server manually. The wireless station user will use one of these accounts to login to the Access Point before access the wireless LAN. You also have to add secret key to the RADIUS server. RADIUS server client has to use one of these secret keys to login the RADIUS server before asking for the authentication.

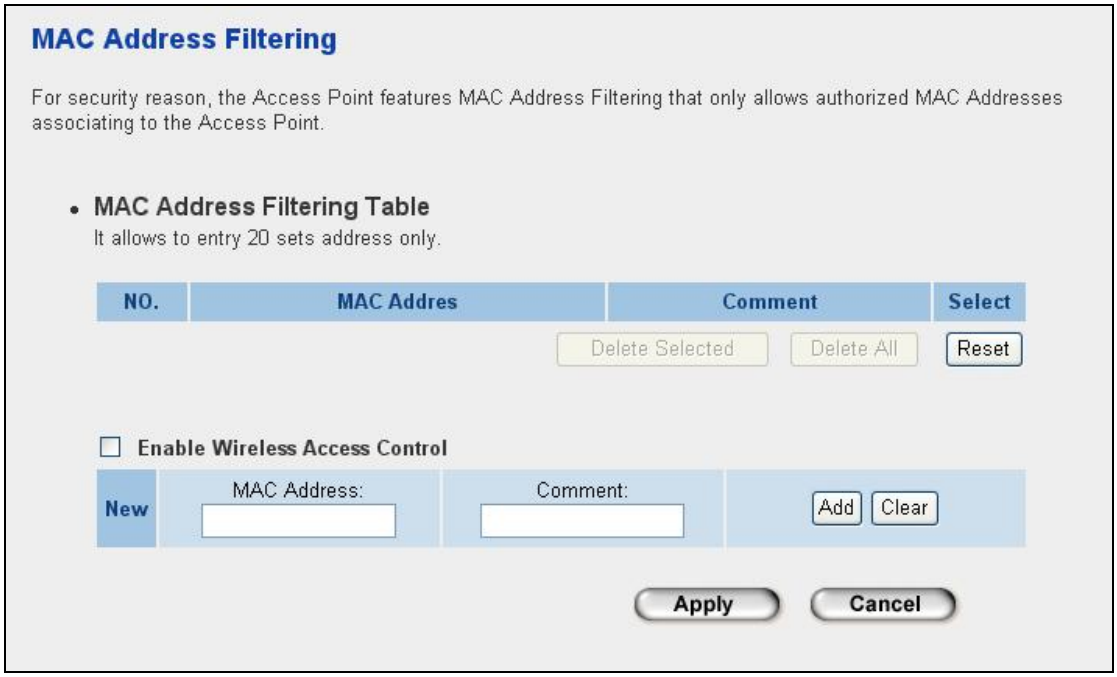


Parameter	Description
Enable Radius Server	Select to enable the RADIUS server.
User Profile	
User Profile table	This table records the accounts of users who are allowed to access your wireless network. An account includes the “User name” and “Password”. A wireless LAN user has to enter correct “Username” and “Password” before he/she accesses the wireless LAN.
Add an user account	Fill in the “Username”, “Password” and “Re-Type Password” and then click “Add”. This new account will be added into the account table below. Click “Reset” to clear the fields.
Remove user account from the table	If you want to remove an account from the table, select the account in the table and then click “Delete Selected”. If you want remove all user accounts from the table, just click “Delete All” button.

Reset	Click “Reset” will clear your current selections.
Authentication Client	
Authentication Client table	This table records the clients of the RADIUS server that need to authenticate wireless LAN users. Authentication client information includes the “Client IP” and “Secret Key”. An authentication client has to use the “Secret Key” to login to the RADIUS server before it starts to authenticate wireless LAN users. An authentication client can be an access point.
Add an authentication client	Fill in the “Client IP”, “Secret Key” and “Re-Type Secret Key” of the new authentication client and then click “Add”. This new authentication client will be added into the table below. Click “Reset” to clear the fields.
Remove authentication client from the table	If you want to remove an authentication client from the table, select the authentication client in the table and then click “Delete Selected”. If you want remove all user authentication clients from the table, just click “Delete All” button.
Reset	Click “Reset” will clear your current selections.

3.7 MAC Filtering

Enabling the MAC Filtering feature would allow only authorized clients associating to the Access Point.

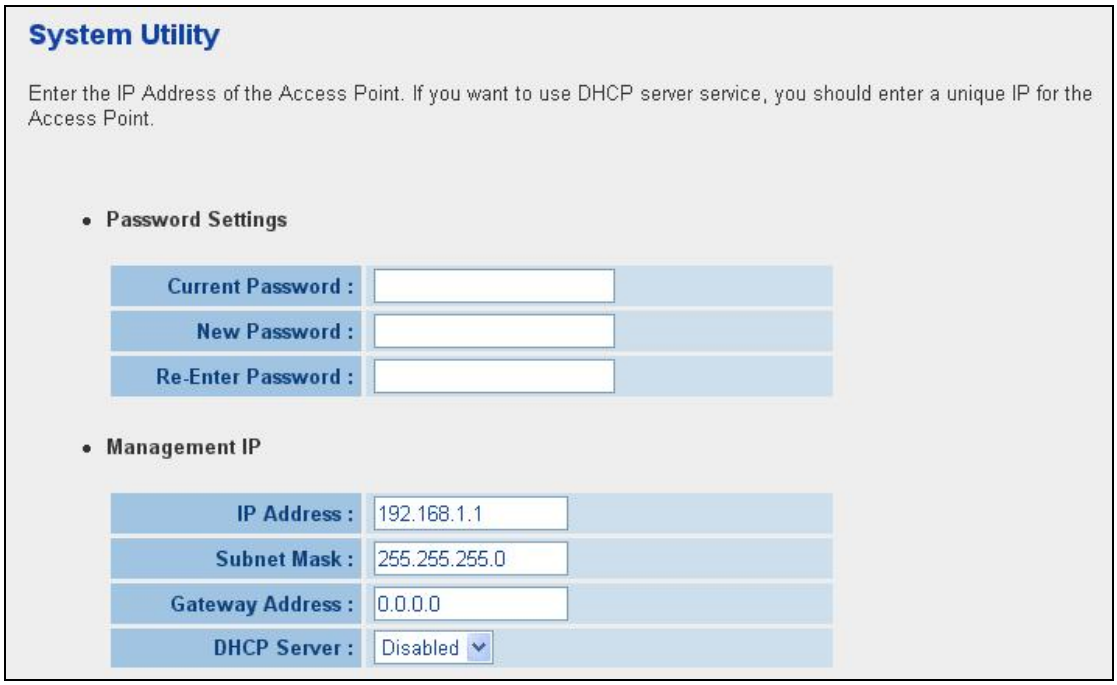


Parameter	Description
MAC Address Filtering Table	This table records the MAC addresses of wireless stations you allow to access your network. The “Comment” field is the description of the wireless station and is helpful for you to recognize the wireless station.
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
Add MAC address into the table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless station, and then click “Add”. This wireless station will be added into the “MAC Address Filtering Table” above.
Remove MAC address from the table	If you want to remove a MAC address from the “MAC Address Filtering Table”, select the MAC address in the table and then click “Delete Selected”. If you want to remove all MAC addresses from the table, just click “Delete All” button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart **11N AP** with new configuration.

3.8 System Utility

In this page, you can define the Access Point’s IP Address, Login Password and enable the DHCP Server feature.

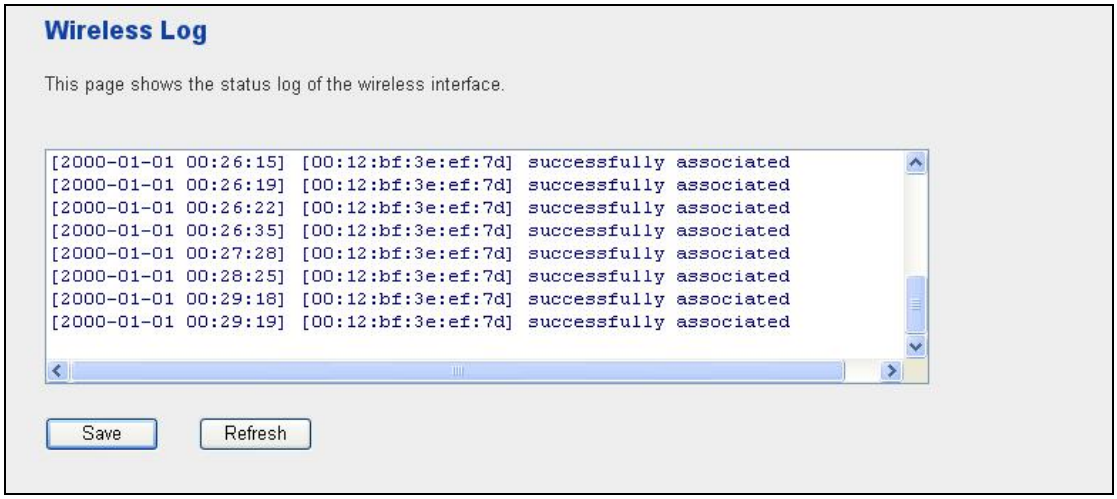


Parameter	Description
Password Settings	
Current Password	Enter the current password (up to 15-digit alphanumeric string) of the Access Point. The default password for the **11N AP** is **admin**. Note that the password is case-sensitive.
New Password	Enter the password (up to 15-digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
Re-Enter Password	Reconfirm the password (up to 15-digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
Management IP	
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.1.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The default Subnet Mask of the Access Point is **255.255.255.0**.
Gateway Address	The IP address of the default gateway of the subnet that this access point resides in. It allows this access point be accessed by PC from deferent subnet to do configuration.
DHCP Server	Enable or disable the DHCP Server.
DHCP Server	
Default Gateway IP	Specify the gateway IP in your network. This IP address should be different from the Management IP.
Domain Name Server IP	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.1.100** to End IP **192.168.1.200**.
Domain Name	You can specify the Domain Name for your Access Point.
Lease Time	The DHCP Server when enabled will temporarily give your LAN client an IP address. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN clients. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart **11N AP** with new configuration.

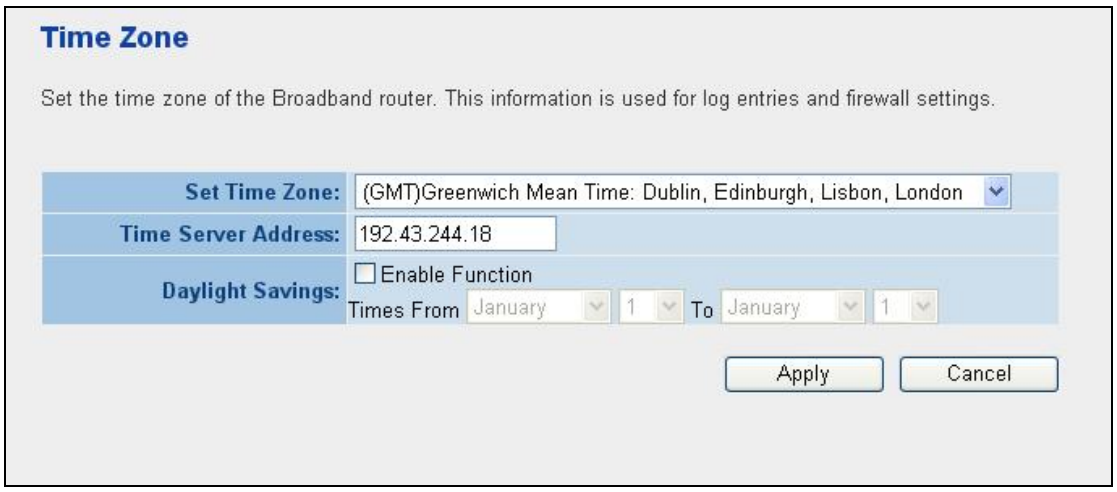
3.9 Wireless Log

This screen is displayed when the Wireless client Status Log in the **11N AP** information on the screen.



3.10 System Time Zone

The time information is used for Log entries and Firewall settings. You can keep the default Time Server address or set a new IP address for your router to synchronize its time.

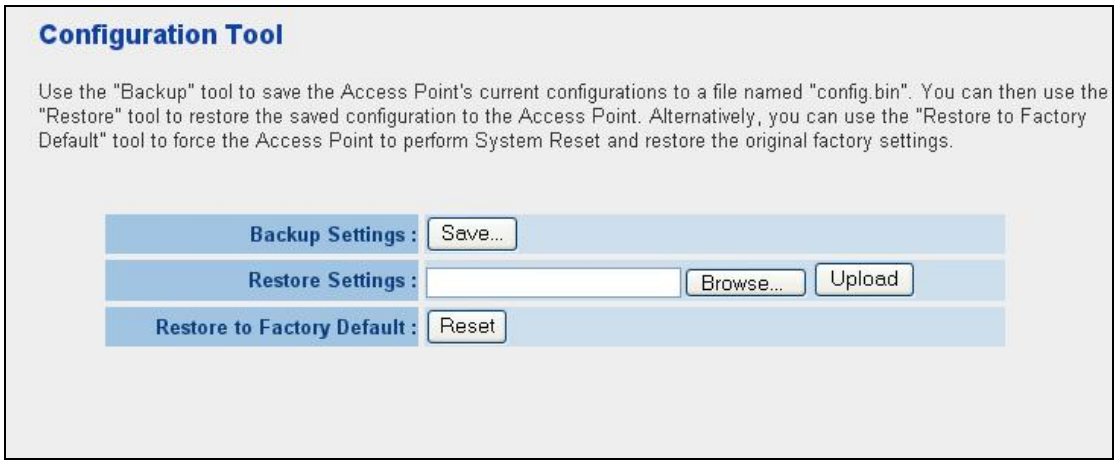


Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address	Remain it as default or, you can manually assign an IP address of the Time Server. The information of Timer Server can be found in the following URL link: http://www.eecis.udel.edu/~mills/ntp/servers.html or http://www.ntp.org.
Enable Daylight Savings	The router can also take Daylight savings into account. To enable this function, check/tick the “Enable Function” box and select which days this function will work.

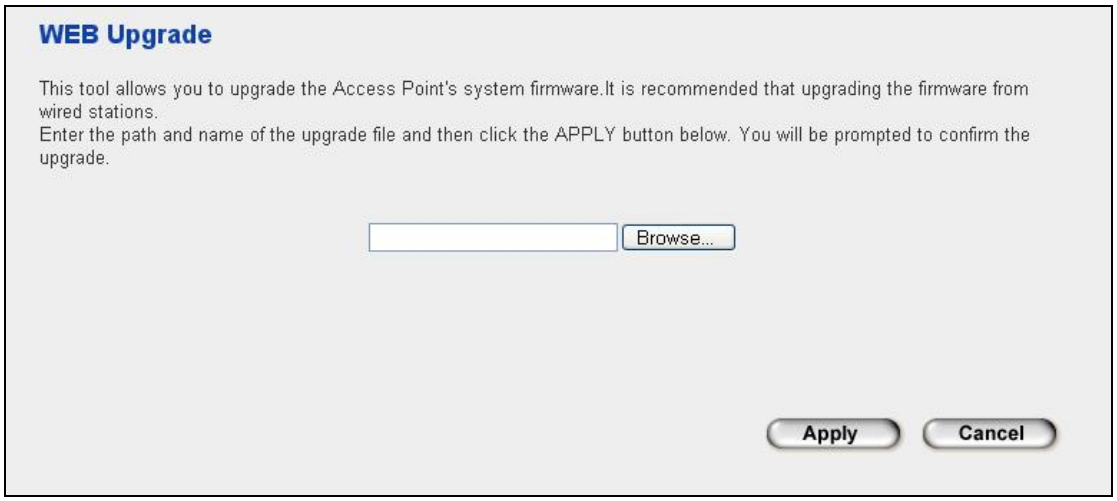
3.11 Configuration

The Configuration Tools screen allows you to save (**Backup**) the **11N AP** current settings. Saving settings provides an added protection and convenience for system backup. When you save the configuration setting (Backup), you can re-load the saved configuration into the **11N AP** through the **Restore** button. If extreme problems occur you can use the **Restore to Factory Default** button. This will set all configurations to original default settings (e.g. when you first purchased the Access Point).



3.12 Upgrade

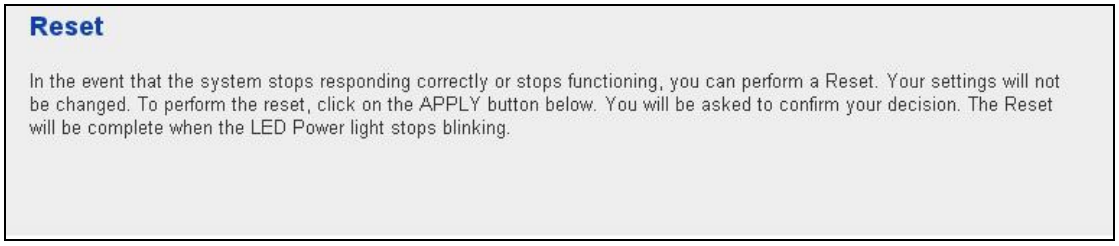
This page allows you to upgrade **11N AP** with latest firmware.



Parameter	Description
Firmware Upgrade	To upgrade the firmware of **11N AP**, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the "**Browse…**" button to find out the firmware file on your PC. Press Apply button to start upgrade process. When the upgrade process is complete, we suggest you to power off/on **11N AP** to make the new firmware effect.

3.13 Reset

You can reset the **11N AP** system if necessary. The reset function essentially reboots your **11N AP** system.



Parameter	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed by reset procedure**. To perform the reset, click on the **Apply** button. You will be asked to confirm your decision. Once the reset process is complete you may start using the Access Point again.

Appendix A Specification

Standard	IEEE 802.11b/g , 802.11n Draft 2.0 , IEEE802.3af compliant (**WNAP-1120PE**)
Frequency Band	2.400~2.4835GHz
Transfer Rate	IEEE 802.11b: 11/5.5/2/1 Mbps IEEE 802.11g: 54/48/36/24/18/12/9/6 Mbps IEEE 802.11n: 300/270/243/240/216/180/162/120/108Mbps in 40Mhz mode 145/130/117/104/ 78Mbps in 20Mhz mode
Modulation	11b mode: CCK, DQPSK, DBPSK 11g mode: 64 QAM, 16 QAM, QPSK, BPSK 11n mode: 64 QAM, 16 QAM, QPSK, BPSK
Radio Technology	Direct Sequence Spread Spectrum (DSSS)
Antenna	RP-SMA connector with two 3dBi dipole antennas
Transmit Power	18dBm (max.)
LAN Interface	1-port RJ-45 UTP, Auto-MDI/MDI-X
Cabling	Category 5/5e or above, 1-pair
LED Indicators	PWR, WLAN, LNK
Power	5V DC, 1A
Temperature	Operating :0 ~ 40 Degree C Storage: -20 ~ 60 Degree C
Humidity	Storage: 10 ~ 90% Non-Condensing Storage Humidity: Max. 95% (Non-Condensing)
Dimension	144 x 88 x 32 mm
Weight	305g
Emission	FCC Class B, CE-mark

Appendix B Frequently Ask Question

This chapter provides answer to problems usually encountered during the *installation* and operation of the *Wireless Network Access Point*. Read the description below to solve your problems.

Q. Can I run an application from a remote computer over the wireless network?

A. This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Q. What is the 11N AP IEEE 802.11n throughput?

A. The **11N AP** Wireless LAN is 300Mbps in the 11n 2T2R theory. According to the distance and real wireless environment, you will get the different throughput. The real throughput is 70~80 Mbps in the clear wireless lab environment.

Q. What IEEE 802.11 features are supported?

A. The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

Q. What is Infrastructure?

A. An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

Q. What is Roaming?

A. Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Wireless Network Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number with the Wireless Network Access Point of dedicated coverage area.

Q. When 11N AP works with WDS mode, can wireless connect to it?

A. Yes, WDS mode is work as the AP and Bridge at the same time. So the wireless client can access to WDS mode **11N AP** without problem. When wireless client connect to the remote site via WDS mode, the performance will be 50% then access to the connected WDS mode **11N AP**. Just like connect to AP via a repeater.

Q. How much wired client can connect to Station mode 11N AP?

A. We will suggest you connect max. 2 wired clients to a **11N AP**. This more is not suit to connect a large wired network. If you have much more clients has to connect via wireless, please set **11N AP** to Bridge mode. Bridge mode will be suit to connect wired LANs together.

Q. Is 11N AP Bridge mode compatible with other bridge mode device?

A. Yes. **11N AP** Bridge mode is compatible with **11N AP** and WNRT-625, WNRT-620 v2. They are designed with the same chipset. So their bridge mode is compatible to each other.

Q. When I set 11N AP to Universal Repeater mode, the PCs that connect to 11N AP LAN port cannot access to wireless network. Why?

A. Since Repeater is used to extend the AP's coverage, the LAN port is for configuration purpose only. The computer connected to the Repeater's LAN port cannot access to wireless network.

EC Declaration of Conformity

For the following equipment:

*Type of Product : 802.11n Wireless Access Point with POE
*Model Number : WNAP-1120PE

* Produced by:
Manufacturer's Name : **Planet Technology Corp.**
Manufacturer's Address: 11F, No 96, Min Chuan Road
Hsin Tien, Taipei, 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.
For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.7.1	(2006-05)
EN 301 489-1 V1.6.1	(2005-09)
EN 301 489-17 V1.2.1	(2002-08)
EN 50385	(2002)
EN 60950-1	

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: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Tom Shih**

Position / Title : **Product Manager**

Taiwan	**31 March, 2009**	
Place	*Date*	*Legal Signature*

EC Declaration of Conformity

For the following equipment:

*Type of Product : 802.11n Wireless Access Point
*Model Number : WNAP-1120

* Produced by:
Manufacturer‘s Name : **Planet Technology Corp.**
Manufacturer‘s Address: 11F, No 96, Min Chuan Road
Hsin Tien, Taipei, 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.
For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.7.1	(2006-05)
EN 301 489-1 V1.6.1	(2005-09)
EN 301 489-17 V1.2.1	(2002-08)
EN 50385	(2002)
EN 60950-1	

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: **11F, No.96, Min Chuan Road, Hsin Tien, Taipei, Taiwan, R.O.C**

Person responsible for making this declaration

Name, Surname **Tom Shih**

Position / Title : **Product Manager**

Taiwan	**31 March, 2009**	
Place	*Date*	*Legal Signature*