



802.11n Wireless Access Point

User Manual
ver.1.0

WLn-501



COPYRIGHT

Copyright ©2005/2006 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

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

CATALOG

<i>Chapter I: Product Information</i>	4
1-1 Product Introduction	4
1-2 Safety Information	6
1-3 System Requirements	7
1-4 Package Contents	8
1-5 Familiar with your new wireless access point	9
<i>Chapter II: System and Network Setup</i>	11
2-1 Setup Network Connection between Wireless Access Point and your Computer	11
2-2 Connecting to wireless access point by web browser	12
2-2-1 Windows 95/98/Me IP address setup	12
2-2-2 Windows 2000 IP address setup	14
2-2-3 Windows XP IP address setup	16
2-2-4 Windows Vista IP address setup	18
2-2-5 Connecting to Web Management Interface	21
2-3 View System Status and Information	23
2-4 Select an Operating Mode for Wireless Access Point	25
2-4-1 AP Mode	27
2-4-2 AP Bridge-Point to Point Mode	29
2-4-3 AP Bridge-Point to Multi-Point Mode	31
2-4-4 AP Bridge-WDS Mode	33
2-5 WPS Setting	36
2-6 Advanced Wireless Settings	39
2-7 Wireless Security (Data Encryption)	42
2-7-1 Disable Security	44
2-7-2 WEP	45
2-7-3 WPA Pre-shared Key	47
2-7-4 WPA RADIUS	49
2-7-5 802.1x Authentication	51
2-8 Radius Server	53
2-9 MAC Filtering	56
2-10 System Utilities	58
2-10-1 Change Password	58
2-10-2 IP Address of the Wireless Access Point	59
2-10-3 DHCP Server	61

<i>Chapter III: Advanced Configuration</i>	63
3-1 Configuration Backup and Restore.....	63
3-2 Firmware Upgrade.....	64
3-3 System Reset.....	65
<i>Chapter IV: Appendix</i>	66
4-1 Hardware Specification	66
4-2 Troubleshooting	67
4-3 Glossary	69
4-4 FCC Statement.....	73

Chapter I: Product Information

1-1 Product Introduction

Thank you for purchasing this wireless access point! With this high cost-efficiency wireless access point, computers and wireless devices which are compatible with 802.11 Draft-N wireless network standard can connect to existing wired Ethernet network via this wireless access point, at the speed of 300Mbps.

Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

This access point is also capable to operate in 'Wireless Bridge' mode. You can use it to expand the scope of your network wirelessly! When you want to build connection between two wired networks, you can use this function to establish connection by a pair or more wireless access point, to connect all networks together.

Other features of this access point including:

- Compatible with IEEE 802.11b/g/Draft-N wireless network standard - works with other 802.11b/g/Draft-N wireless access points.
- High speed wireless network, six times faster than conventional 802.11g wireless network (300Mbps)
- Allow wireless devices to connect to existing wired network and share Internet and other network resources.
- Five wired Ethernet LAN ports (10/100M)
- Supports DHCP server function.
- Supports wireless data encryption (WEP/WPA).
- Supports MAC address filtering (Only allow specific wireless device of your choice to connect to this access point).

- Supports RADIUS server, only allow users listed in your authorization server to use wireless network.
- Supports WPS (Wi-Fi Protected Setup), simplifies wireless client setup procedures. Even inexperienced user can setup wireless network without network technician's help!
- Easy to use web-based GUI (Graphical User Interface) for network configuration and management purposes.
- Remote management function allows configuration and upgrades from a remote computer (over the Internet)
- Auto MDI / MDI-X function for all wired Ethernet ports.
- Three high-gain antenna (antenna angle adjustable).

1-2 Safety Information

In order to keep the safety of users and your properties, please follow the following safety instructions:

1. This access point is designed for indoor use only; DO NOT place this access point outdoor.
2. DO NOT put this access point at or near hot or humid places, like kitchen or bathroom. Also, do not left this access point in the car in summer.
3. DO NOT pull any connected cable with force; disconnect it from the access point first.
4. If you want to place this access point at high places or hang on the wall, please make sure the access point is firmly secured. Falling from high places would damage the access point and its accessories, and warranty will be void.
5. Accessories of this access point, like antenna and power supply, are danger to small children under 3 years old. They may put the small parts in their nose or month and it could cause serious damage to them. **KEEP THIS ACCESS POINT OUT THE REACH OF CHILDREN!**
6. The access point will become hot when being used for long time (***This is normal and is not a malfunction***), DO NOT put this access point on paper, cloth, or other flammable materials.
7. There's no user-serviceable part inside the access point. If you found that the access point is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the access point, warranty will be void.
8. If the access point falls into water when it's powered, DO NOT use your hand to pick it up. Switch the electrical power off before you do anything, or contact an experienced electrical technician for help.
9. If you smell something strange or even see some smoke coming out from the access point or power supply, remove the power supply or switch the electrical power off immediately, and call dealer of purchase for help.

1-3 System Requirements

- Computer or network devices with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser*).
- An available AC power socket (100 – 240 V, 50/60Hz)

1-4 Package Contents

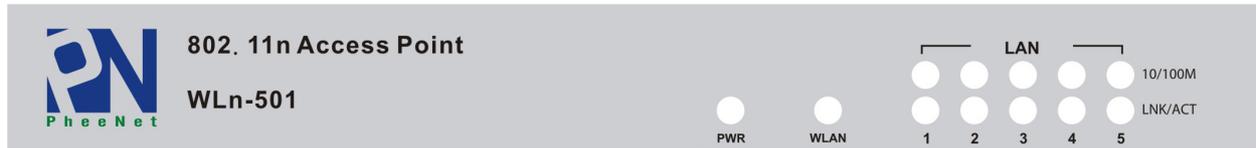
Before you starting to use this access point, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- Wireless Access point (main body, 1 pcs)..... 1
- User manual (1 pcs) 2
- A/C power adapter (1 pcs) 3



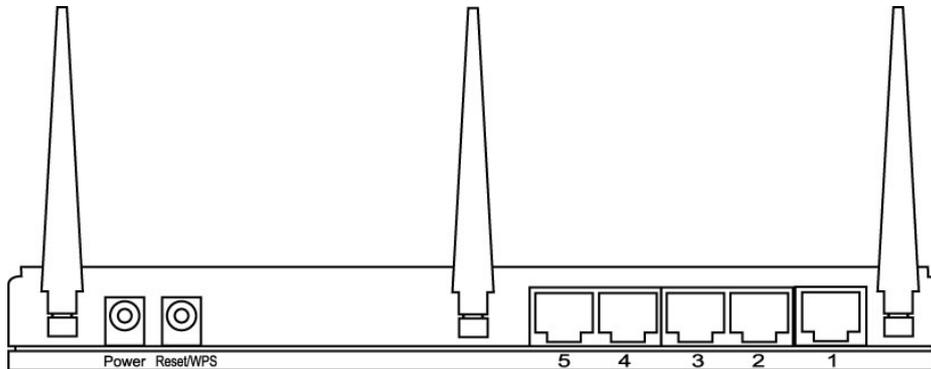
1-5 Familiar with your new wireless access point

Front Panel



LED Name	Light Status	Description
PWR	ON	Access point is switched on and correctly powered
WLAN	On	Wireless network is switched on
	Off	Wireless network is switched off
	Flashing	Wireless LAN activity (transferring data)
LAN 10/100M 1-5	On	LAN port is running at 100Mbps
	Off	LAN port is running at 10Mbps
LAN LNK/ACT 1-5	On	LAN port is connected
	Off	LAN port is not connected
	Flashing	LAN activity (transferring data)

Back Panel



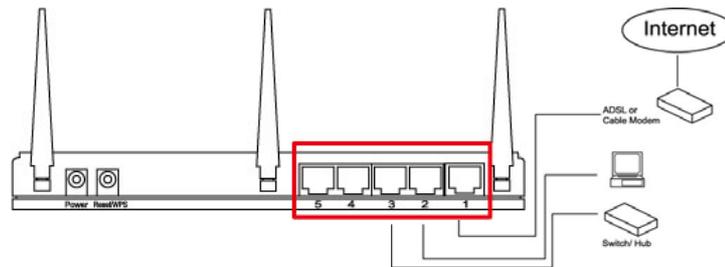
Item Name	Description
Antenna A to C	Antenna A, B and C
Power	Power connector, connects to A/C power adapter
Reset / WPS	Reset the router to factory default settings (clear all settings) or start WPS function. Press and hold this button for 2 seconds to activate WPS function; press and hold this button for more than 20 seconds to clear all settings.
LAN 1 - 5	Local Area Network (LAN) ports 1 to 5

Chapter II: System and Network Setup

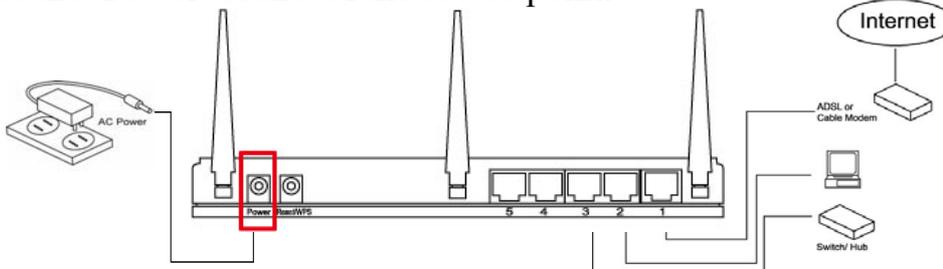
2-1 Setup Network Connection between Wireless Access Point and your Computer.

Please follow the following instruction to build the network connection between your new wireless access point and your computers, network devices:

1. Connect all your computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub) to the LAN port of the access point by Ethernet cable.



2. Connect the A/C power adapter to the wall socket, and then connect it to the 'Power' socket of the access point.



3. Please check all LEDs on the front panel. 'PWR' LED should be steadily on, LAN LEDs should be on if the computer / network device connected to the respective port of the access point is powered on and correctly connected. If PWR LED is not on, or any LED you expected is not on, please recheck the cabling, or jump to **'4-2 Troubleshooting'** for possible reasons and solution.

2-2 Connecting to wireless access point by web browser

After the network connection is built, the next step you should do is setup the access point with proper network parameters, so it can work properly in your network environment.

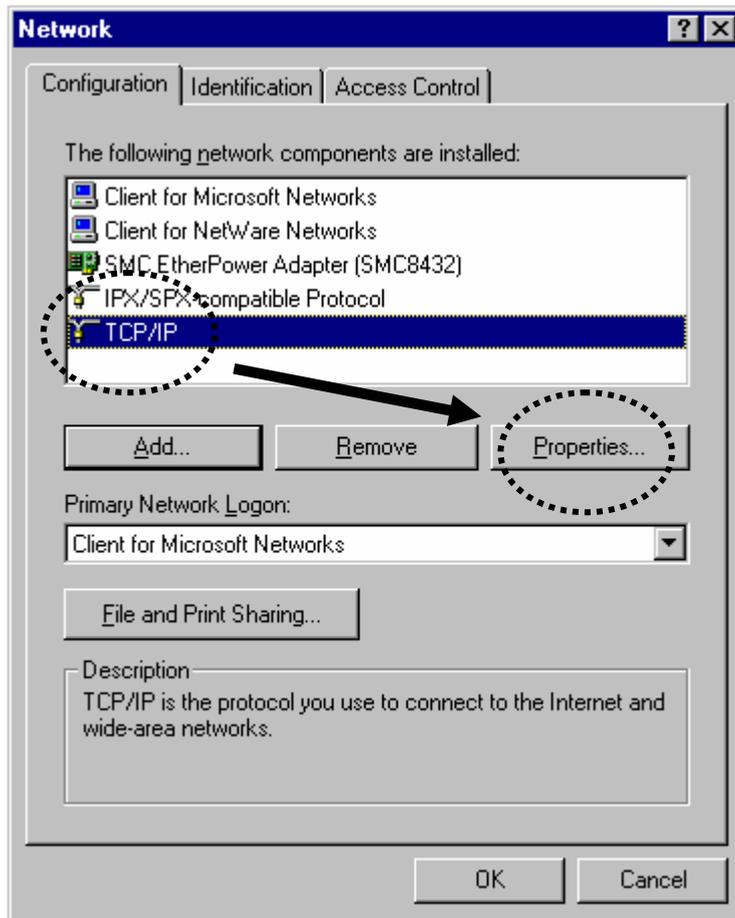
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address:

If the operating system of your computer is....

Windows 95/98/Me	- please go to section 2-2-1
Windows 2000	- please go to section 2-2-2
Windows XP	- please go to section 2-2-3
Windows Vista	please go to section 2-2-4

2-2-1 Windows 95/98/Me IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Double-click *Network* icon, and *Network* window will appear. Select 'TCP/IP', then click 'Properties'.

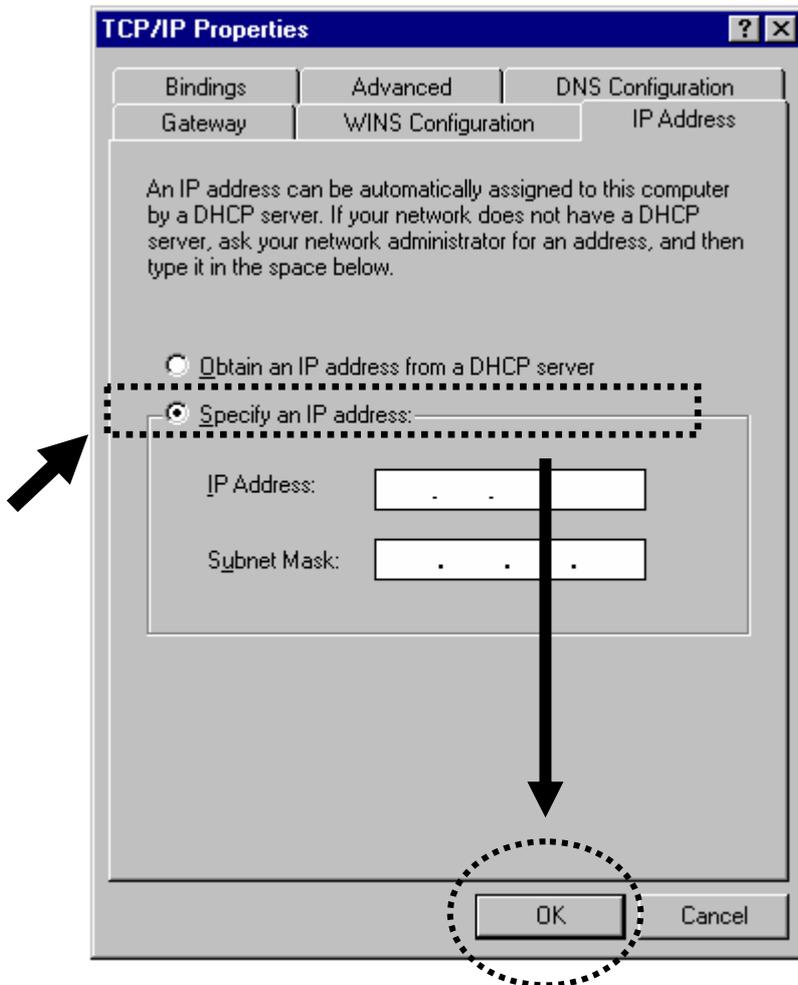


2. Select 'Specify an IP address', then input the following settings in respective field:

IP address: 192.168.2.2

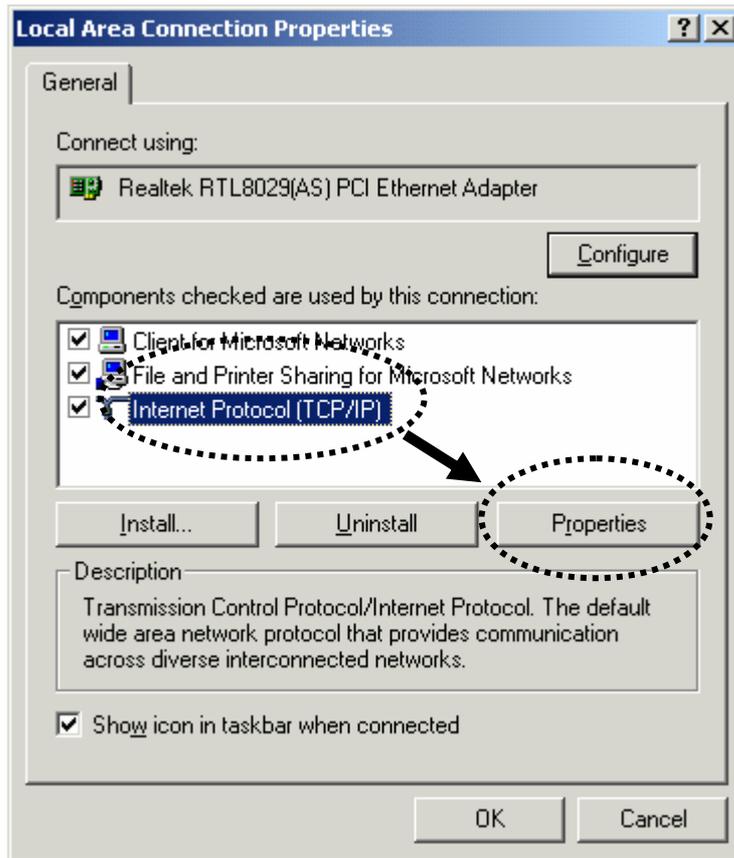
Subnet Mask: 255.255.255.0

click 'OK' when finish.



2-2-2 Windows 2000 IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection**, and **Local Area Connection Properties** window will appear. Select 'Internet Protocol (TCP/IP)', then click 'Properties'

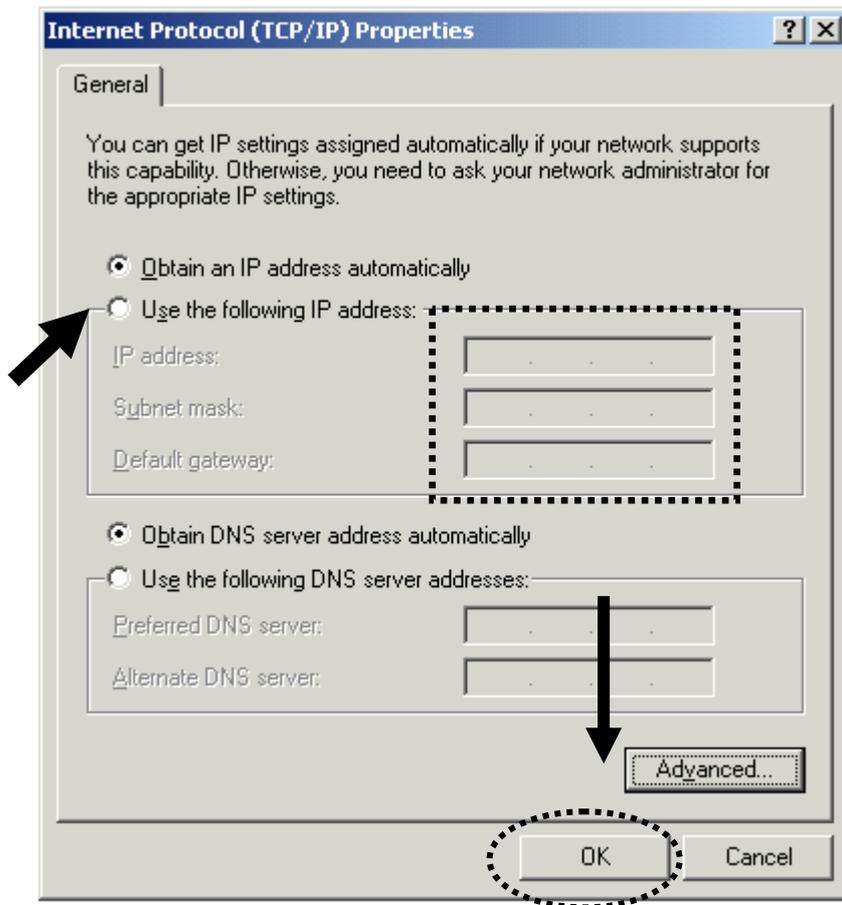


2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.2

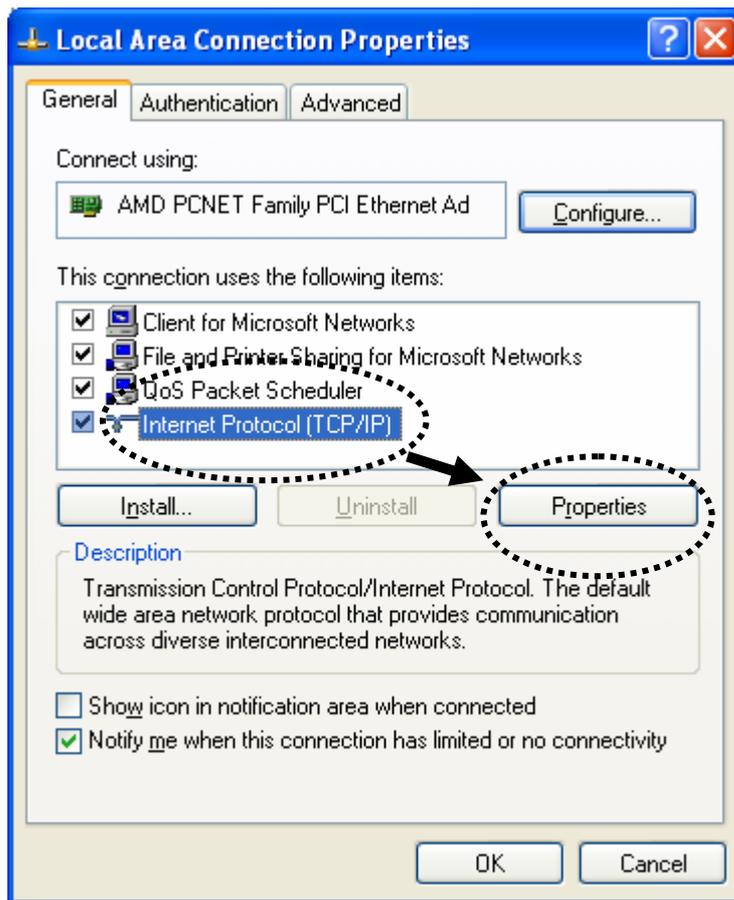
Subnet Mask: 255.255.255.0

click 'OK' when finish.



2-2-3 Windows XP IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections**, and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then click 'Properties'

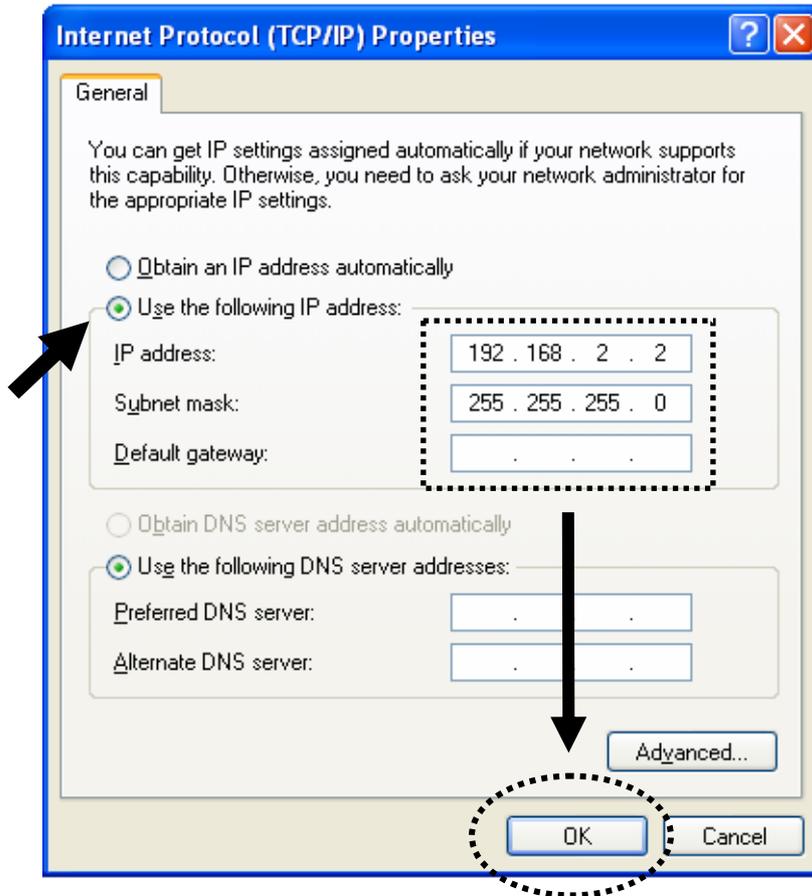


2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.2

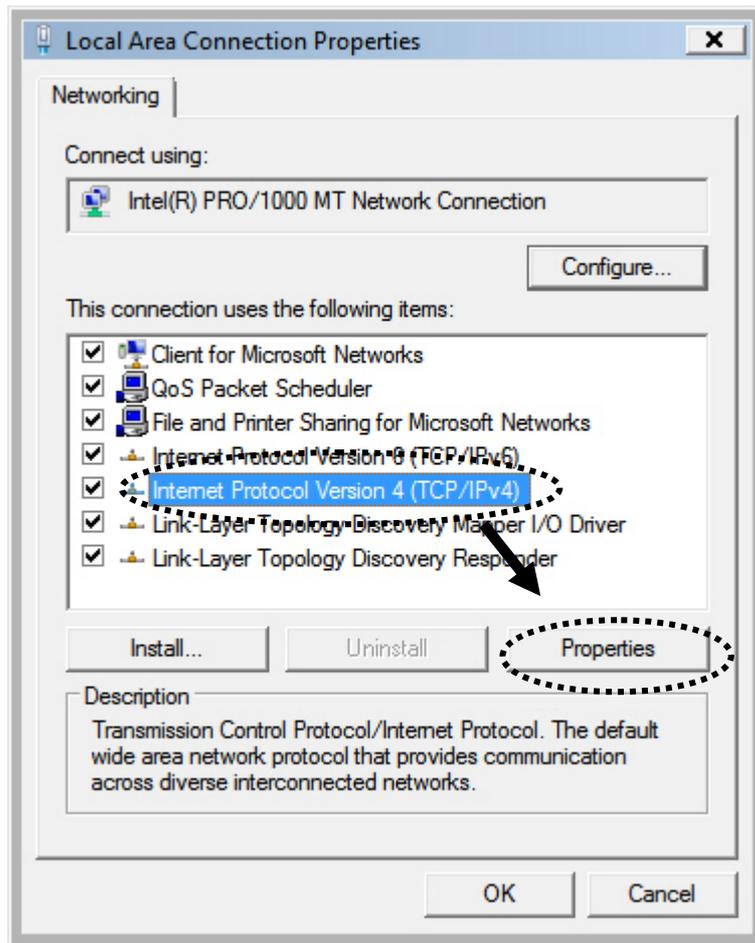
Subnet Mask: 255.255.255.0

click 'OK' when finish.



2-2-4 Windows Vista IP address setup

1. Click 'Start' button (it should be located at lower-left corner of your computer), then click control panel. Click *View Network Status and Tasks*, then click *Manage Network Connections*..Right-click *Local Area Network*, then select '*Properties*'. *Local Area Connection Properties* window will appear, select 'Internet Protocol Version 4 (TCP / IPv4), and then click 'Properties'

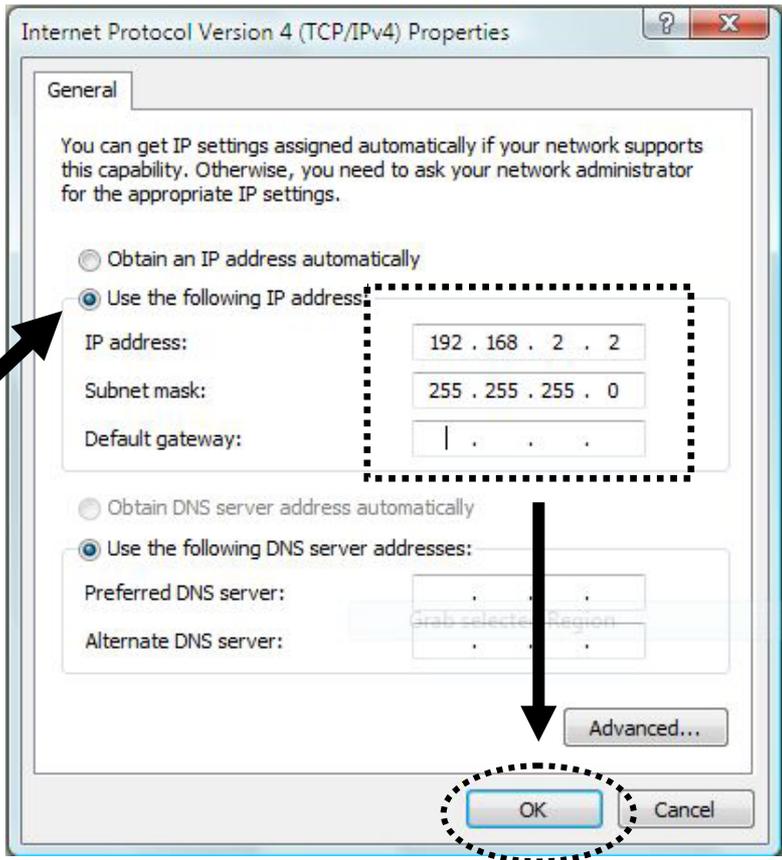


2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.2

Subnet Mask: 255.255.255.0

click 'OK' when finish.

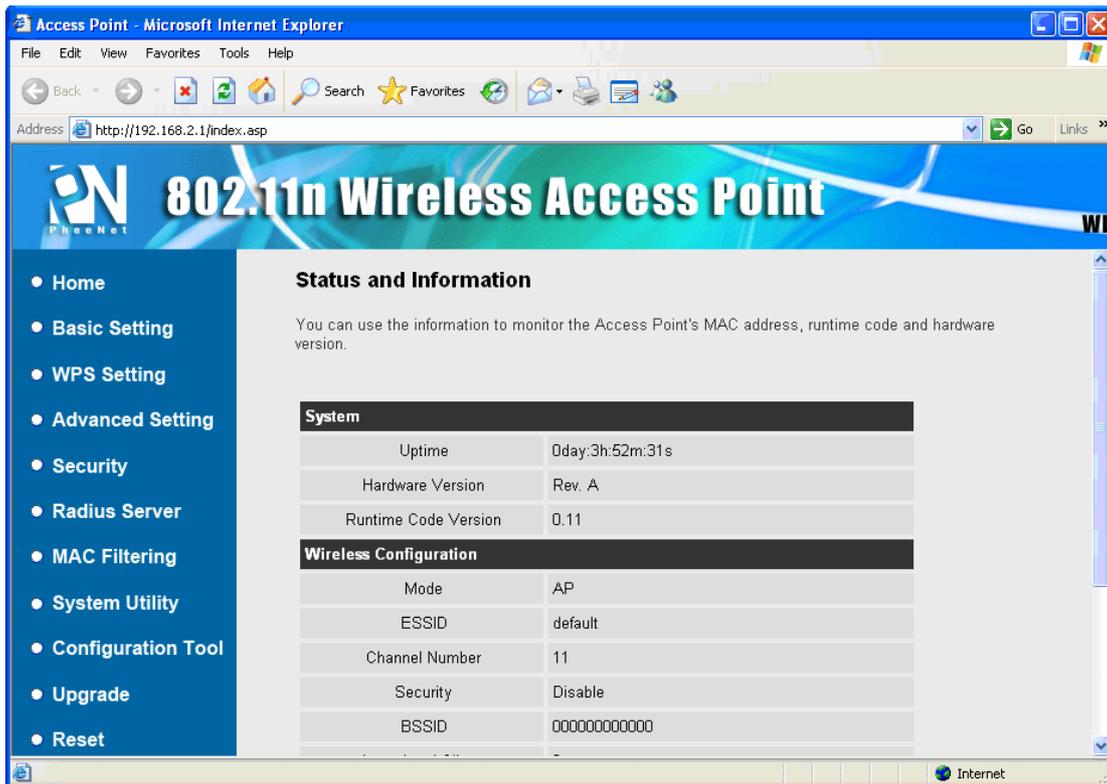


2-2-5 Connecting to Web Management Interface

All functions and settings of this access point must be configured via web management interface. Please start your web browser, and input '192.168.2.1' in address bar, then press 'Enter' key. The following message should be shown:



Please input user name and password in the field respectively, default user name is 'admin', and default password is '1234', then press 'OK' button, and you can see the web management interface of this access point:



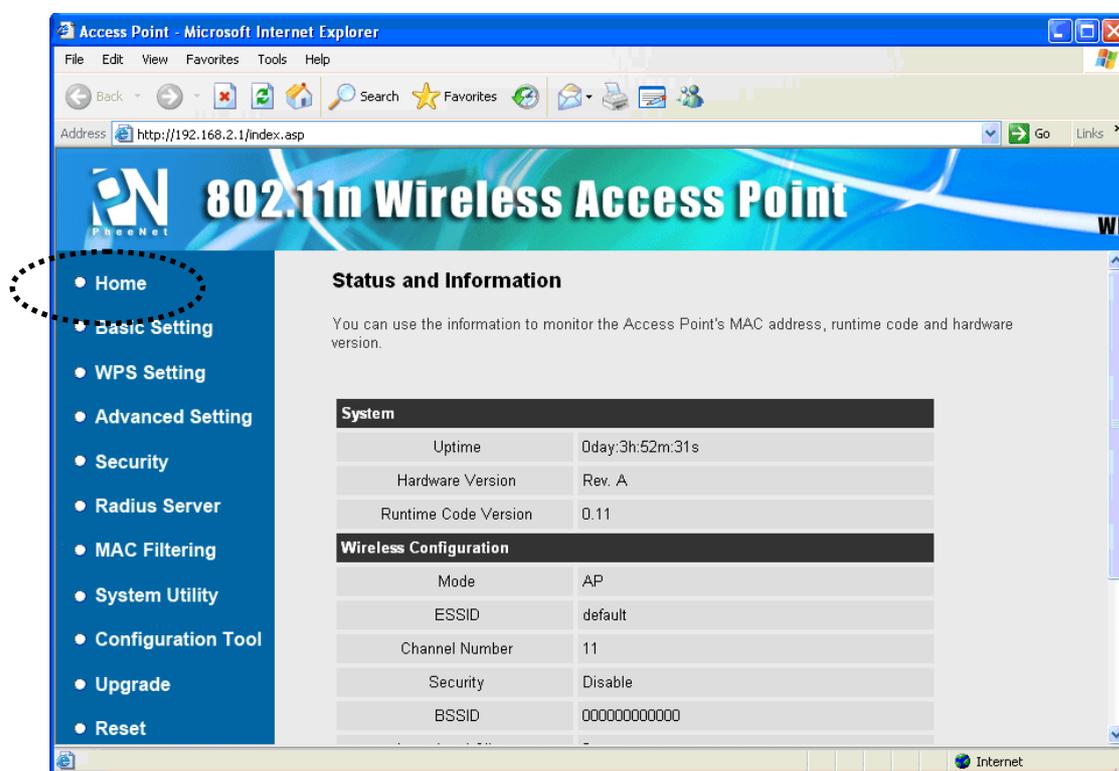
NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you didn't input username and password correctly. Please retype user name and password again. If you're certain about the user name and password you type are correct, please go to '4-2 Troubleshooting' (page 67) to perform a factory reset, to set the password back to default value.

TIP: This page shows the four major setting categories: QuickSetup, General Setup, Status, and Tools. You can find the shortcut which leads to these setting categories at the upper-right corner of every page, and you can jump to another category directly by clicking the link, and don't have to go back to the first page.

2-3 View System Status and Information

After you connected to the access point by web browser, the first thing you see is ‘Status and Information’ page. All system and network related information of this access point will be displayed here. These information are very helpful when you want to know the detailed information of your access point, and when you try to fix the communication problem between this access point and other wired / wireless computer / devices.

You can click ‘Home’ on the left, and the system status and information will be displayed, as shown below:



Here are descriptions of every items:

<i>Up time</i>	<i>Displays the total passed time since the wireless access point is powered.</i>
<i>Hardware Version</i>	<i>Displays hardware version. This information is helpful when you need online help from the dealer of purchase.</i>
<i>Runtime Code Version</i>	<i>Displays current firmware version. If you want to perform firmware upgrade, this number will help</i>

	<i>you to determine if you need such upgrade.</i>
<i>Mode</i>	<i>Displays current wireless operating mode (see next chapter)</i>
<i>ESSID</i>	<i>Displays current ESSID (the name used to identify this wireless access point)</i>
<i>Channel Number</i>	<i>Displays current wireless channel number</i>
<i>Security</i>	<i>Displays current wireless security setting</i>
<i>BSSID</i>	<i>Displays current BSSID (a set of unique identification name of this access point, can not be modified by user)</i>
<i>Associated Clients</i>	<i>Displays the number of connected wireless client</i>
<i>IP Address</i>	<i>Displays the IP address of this wireless access point</i>
<i>Subnet Mask</i>	<i>Displays the net mask of IP address</i>
<i>Default Gateway</i>	<i>Displays the IP address of default gateway</i>
<i>MAC address</i>	<i>Displays the MAC address of LAN interface</i>

2-4 Select an Operating Mode for Wireless Access Point

This access point can be operated in different modes; you can click ‘Basic Setting’ on the left of web management interface to select a operating mode you want to meet different needs:



You can click ‘Mode’ dropdown menu to select operating mode, and there are 4 operating modes available:

<i>AP</i>	<i>Access point mode, allows wireless clients to connect to access point and exchange data with computers connected to wired Ethernet ports of access point.</i>
<i>AP Bridge-Point to Point</i>	<i>Establish wireless connection with another wireless access point using the same mode, and link the wired network which these two wireless access points connected to together. Only one access point can be connected in this mode.</i>
<i>AP Bridge-Point to Multi-Point</i>	<i>Establish wireless connection with other wireless access points using the same mode, and link the</i>

	<i>wired network which these wireless access points connected to together. Up to 4 access points can be connected in this mode.</i>
<i>AP Bridge-WDS</i>	<i>This mode is similar to 'AP Bridge to Multi-Point', but access point is not work in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.</i>

Please select one wireless operating mode, for detailed descriptions of every operating mode, please refer to chapter 2-4-1 to 2-4-4 listed below.

2-4-1 AP Mode

This is the most common mode. When in AP mode, this access point acts as a bridge between 802.11b/g/Draft-N wireless devices and wired Ethernet network, and exchange data between them.

When you select 'AP', the following options will be displayed:

The screenshot shows a configuration window for an access point in AP mode. The settings are as follows:

- Mode: AP (selected in a dropdown menu)
- Band: 2.4 GHz (B+G+N) (selected in a dropdown menu)
- ESSID: default (text input field)
- Channel Number: 11 (selected in a dropdown menu)
- Associated Clients: Show Active Clients (button)

At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Here are descriptions of every setup items:

<i>Band</i>	<p><i>Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.</i></p> <p><i>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point.</i></p> <p><i>If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.</i></p> <p><i>If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).</i></p>
<i>ESSID</i>	<p><i>Please input the ESSID (the name used to identify</i></p>

	<i>this wireless access point) here. You can input up to 32 alphanumerical characters. PLEASE NOTE THAT ESSID IS CASE SENSITIVE.</i>
<i>Channel Number</i>	<i>Please select a channel number you wish to use. If you know a certain channel number is being used by other 802.11a wireless access points nearby, please refrain from using the same channel number</i>
<i>Associated Clients</i>	<i>Click 'Show Active Clients' button and a new popup window will appear, which contains the information about all wireless clients connected to this access point. You can click 'Refresh' button in popup window to keep information up-to-date</i>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-4-2 AP Bridge-Point to Point Mode

In this mode, this wireless access point will connect to another wireless access point which uses the same mode, and all wired Ethernet clients of both wireless access points will be connected together. You can use this mode to connect a network to another network which is physically isolated.

Please note that when you set your access point to this mode, it will not accept regular wireless clients anymore.

When you select 'AP Bridge-Point to Point', the following options will be displayed:

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

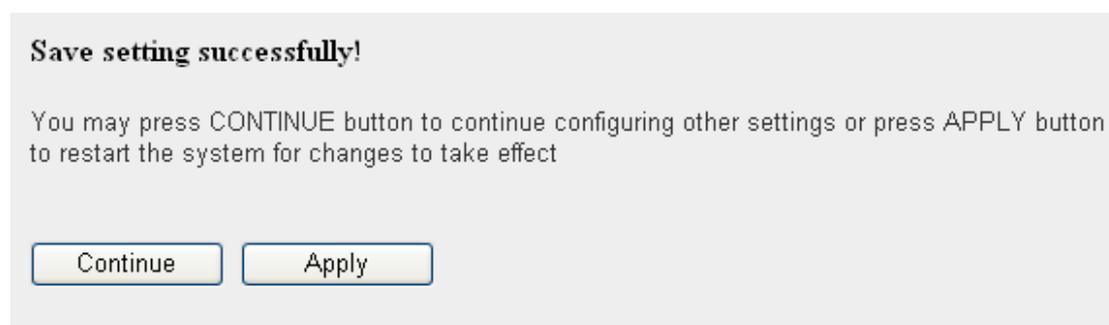
Mode :	AP Bridge-Point to Point
Band :	2.4 GHz (B+G+N)
Channel Number :	11
MAC address 1 :	000000000000
Set Security :	<input type="button" value="Set Security"/>

Here are descriptions of every setup items:

<i>Band</i>	<p><i>Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.</i></p> <p><i>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point.</i></p>
-------------	--

	<p><i>If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.</i></p> <p><i>If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).</i></p>
<i>Channel Number</i>	<i>Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect</i>
<i>MAC address 1</i>	<i>Please input the MAC address of the wireless access point you wish to connect</i>
<i>Set Security</i>	<i>Click this button to select an encryption mode for this wireless link, a new popup window will appear. Please refer to chapter 2-7 for detailed descriptions.</i>

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made is successfully saved, You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-4-3 AP Bridge-Point to Multi-Point Mode

In this mode, this wireless access point will connect to up to four wireless access points which uses the same mode, and all wired Ethernet clients of every wireless access points will be connected together. You can use this mode to connect a network to other networks which is physically isolated.

Please note that when you set your access point to this mode, it will not accept regular wireless clients anymore.

When you select ‘AP Bridge-Point to Multi-Point’, the following options will be displayed:

The screenshot shows a configuration window with the following fields and controls:

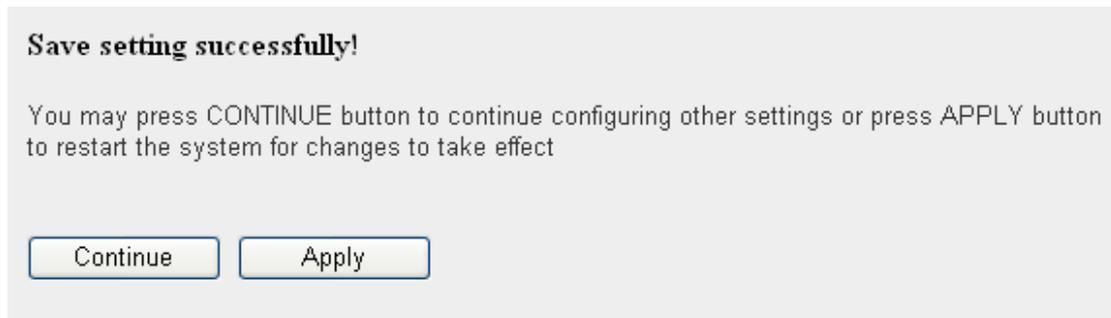
- Mode :** A dropdown menu set to "AP Bridge-Point to Multi-Point".
- Band :** A dropdown menu set to "2.4 GHz (B+G+N)".
- Channel Number :** A dropdown menu set to "11".
- MAC address 1 :** A text input field containing "000000000000".
- MAC address 2 :** A text input field containing "000000000000".
- MAC address 3 :** A text input field containing "000000000000".
- MAC address 4 :** A text input field containing "000000000000".
- Set Security :** A button labeled "Set Security".
- Apply** and **Cancel** buttons at the bottom right.

Here are descriptions of every setup items:

<i>Band</i>	<p><i>Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.</i></p> <p><i>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g)</i></p>
-------------	--

	<p><i>will be able to connect to this access point.</i></p> <p><i>If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.</i></p> <p><i>If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).</i></p>
<i>Channel Number</i>	<i>Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect</i>
<i>MAC address 1-4</i>	<i>Please input the MAC address of the wireless access point you wish to connect</i>
<i>Set Security</i>	<i>Click this button to select an encryption mode for this wireless link, a new popup window will appear. Please refer to chapter 2-7 for detailed descriptions.</i>

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-4-4 AP Bridge-WDS Mode

In this mode, this wireless access point will connect to up to four wireless access points which uses the same mode, and all wired Ethernet clients of every wireless access points will be connected together. You can use this mode to connect a network to other networks which is physically isolated.

When you use this mode, this access point is still able to accept wireless clients.

When you select ‘AP Bridge-WDS’, the following options will be displayed:

The screenshot displays a configuration window for 'AP Bridge-WDS' mode. The settings are as follows:

- Mode :** AP Bridge-WDS (dropdown menu)
- Band :** 2.4 GHz (B+G+N) (dropdown menu)
- ESSID :** default (text input field)
- Channel Number :** 11 (dropdown menu)
- Associated Clients :** Show Active Clients (button)
- MAC address 1 :** 000000000000 (text input field)
- MAC address 2 :** 000000000000 (text input field)
- MAC address 3 :** 000000000000 (text input field)
- MAC address 4 :** 000000000000 (text input field)
- Set Security :** Set Security (button)

At the bottom right, there are two buttons: **Apply** and **Cancel**.

Here are descriptions of every setup items:

<i>Band</i>	<i>Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz</i>
-------------	--

	<p><i>(G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point.</i></p> <p><i>If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.</i></p> <p><i>If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).</i></p>
<i>ESSID</i>	<p><i>Please input the ESSID (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.</i></p>
<i>Channel Number</i>	<p><i>Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect</i></p>
<i>Associated Clients</i>	<p><i>Click 'Show Active Clients' button and a new popup window will appear, which contains the information about all wireless clients connected to this access point. You can click 'Refresh' button in popup window to keep information up-to-date</i></p>
<i>MAC address 1-4</i>	<p><i>Please input the MAC address of the wireless access point you wish to connect</i></p>
<i>Set Security</i>	<p><i>Click this button to select an encryption mode for this wireless link, a new popup window will appear. Please refer to chapter 2-7 for detailed descriptions.</i></p>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue

Apply

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-5 WPS Setting

WPS (Wi-Fi Protected Setup) provides a new way to configure wireless clients; for conventional wireless access points, users have to setup data encryption options manually, and repeat encryption settings on every wireless client by using special configure software, so the data transferred over air is protected by data encryption mechanism. This is generally considered as a boring job when one has a great amount of wireless clients to set.

When using WPS, the procedure is much simpler! You can just press a button on wireless network card (software or physical button), or input a special number (called as 'PIN' number) in the setup menu of this access point, the access point and wireless client will cooperate to setup an encrypted wireless connection. The whole setup procedure will be completed in less than 1 minute, even inexperienced users can setup the encrypted wireless connection with the help of network technician!

Note: WPS function of this access point will not work for those wireless clients do not support WPS.

To use WPS function to set encrypted connection between this access point and WPS-enabled wireless client by WPS, click 'WPS Setting' on the left of web management menu, and the following information will be displayed:

Enable WPS

• **Wi-Fi Protected Setup Information**

WPS Status:	unConfigured
Self PinCode:	0
SSID:	default
Authentication Mode:	Disable
Passphrase Key:	

• **Device Configure**

Configure via Push Button:	<input type="button" value="Start PBC"/>
Configure via Client PinCode:	<input type="text"/> <input type="button" value="Start PIN"/>

Here are descriptions of every setup items:

<i>Enable WPS</i>	<i>Check this box to enable or disable WPS function</i>
<i>Wi-Fi Protected Setup Information</i>	<p><i>All information related to WPS will be displayed here, they're helpful when you're setting up connections by WPS. They are:</i></p> <p><i>WPS Status: Displays WPS status. If data encryption settings of this access point has never been set, 'unConfigured' message will be displayed her. (see chapter 2-7 for detailed information); if data encryption settings has been set before, 'Configured' message will be displayed here.</i></p> <p><i>Self PinCode: Displays the PIN code of this access point. You'll need this number when requested by the wireless client's setup software.</i></p> <p><i>SSID: Displays the SSID (ESSID) of this access point.</i></p> <p><i>Authentication Mode: Displays the authentication mode of this access point.</i></p>

	<i>Passphrase Key: Displays the WPA passphrase here, all characters will be replaced by asterisk for security reason. If encryption is not set on this access point, nothing will be displayed here.</i>
<i>Start PBC</i>	<i>Click this button to start PBC type WPS setup (PBC stands for 'Push Button Configuration')</i>
<i>Start PIN</i>	<i>Click this button to start PIN type WPS setup, the PIN number of wireless client must be inputted in the field located at the left of 'Start PIN' button.</i>

This access point also provides a hardware PBC button for WPS setup. You can press and hold 'Reset/WPS' button for 2 seconds to use PBC type WPS setup, the hardware button's function is the same as 'Start PBC' software button described above. Do not press and hold 'Reset/WPS' button for longer than 20 seconds, or this will reset the access point and remove all settings inside!

NOTE: When you're using PBC type WPS setup, you must press 'PBC' button (hardware or software) of wireless client within 90 seconds; if you didn't press PBC button of wireless client within this time period, please press 'PBC' button (hardware or software) of this access point again.

2-6 Advanced Wireless Settings

This wireless access point has many advanced wireless features and can be configured by yourself. Please note that all settings listed here are for experienced users only, if you're not sure about the meaning and function of these settings, please don't modify them, or the wireless performance will be reduced.

You can click 'Advanced Setting' on the left to enter advanced settings menu, and the following message will be displayed:

Fragment Threshold:	<input type="text" value="2346"/>	(256-2346)
RTS Threshold:	<input type="text" value="2347"/>	(0-2347)
Beacon Interval:	<input type="text" value="100"/>	(20- 1024 ms)
DTIM Period:	<input type="text" value="3"/>	(1-10)
Data Rate:	Auto <input type="button" value="v"/>	
N Data Rate:	Auto <input type="button" value="v"/>	
Channel Width:	<input checked="" type="radio"/> Auto 20/40 MHZ <input type="radio"/> 20 MHZ	
Preamble Type:	<input checked="" type="radio"/> Short Preamble <input type="radio"/> Long Preamble	
Broadcast ESSID:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
CTS Protect:	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None	
Tx Power:	100 % <input type="button" value="v"/>	

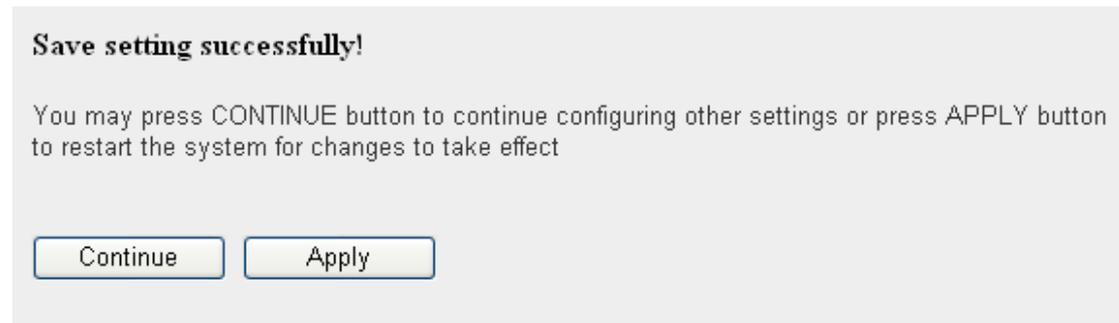
Here are descriptions of every setup items:

<i>Fragment Threshold</i>	<i>Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346</i>
<i>RTS Threshold</i>	<i>Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347</i>
<i>Beacon Interval</i>	<i>Set the beacon interval of wireless radio. Do not</i>

	<i>modify default value if you don't know what it is, default value is 100</i>
<i>DTIM Period</i>	<i>Set the DTIM period of wireless radio. Do not modify default value if you don't know what it is, default value is 3</i>
<i>Data Rate</i>	<i>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.</i>
<i>N Data Rate</i>	<i>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.</i>
<i>Channel Width</i>	<i>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.</i>
<i>Preamble Type</i>	<i>Set the type of preamble of wireless radio, Do not modify default value if you don't know what it is, default setting is 'Short Preamble'.</i>
<i>Broadcast ESSID</i>	<i>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.</i>
<i>CTS Protect</i>	<i>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' or 'Always'. However, if you set to 'None', your wireless access point should be able to work fine, too.</i>
<i>Tx Power</i>	<i>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</i>

<p><i>power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless access point).</i></p>

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



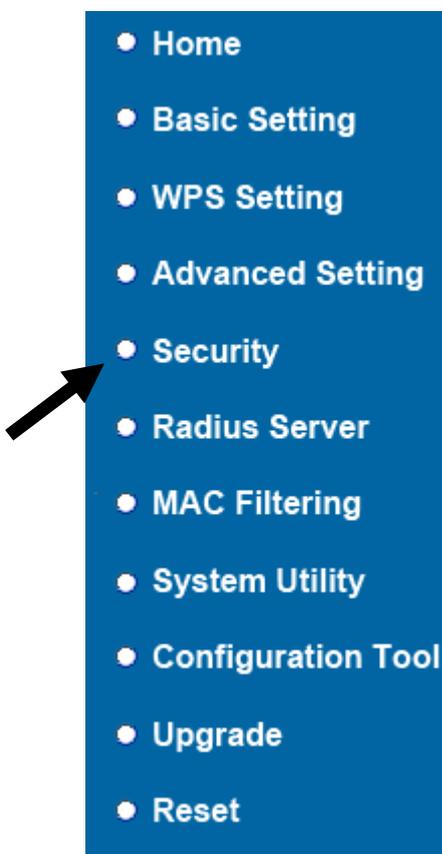
When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-7 Wireless Security (Data Encryption)

This wireless access point provides many types of wireless security (wireless data encryption). When you use data encryption, data transferred by radio signals in the air will become unreadable for those people who don't know correct encryption key (encryption password).

There are two ways to set wireless security:

1. Click 'Security' on the left of web management interface.



2. Click 'Set Security' button when the wireless operating mode you selected is 'AP Bridge-Point to Point', 'AP Bridge-Point to Multi-Point', or 'AP Bridge-WDS'.

Mode :	AP Bridge-Point to Point
Band :	2.4 GHz (B+G+N)
Channel Number :	11
MAC address 1 :	000000000000
Set Security :	<input type="button" value="Set Security"/>

There are four types of security level you can select: Disable (no security - data encryption disabled), WEP, WPA Pre-shared Key, and WPA Radius. Please refer to the following chapters for detailed instructions.

Please remember it's very important to set wireless security settings properly! Without a proper setting, hackers and intruders may gain access to your local network and do something bad to your computers and servers, which could cause serious problem.

There are several things you can do to improve wireless security:

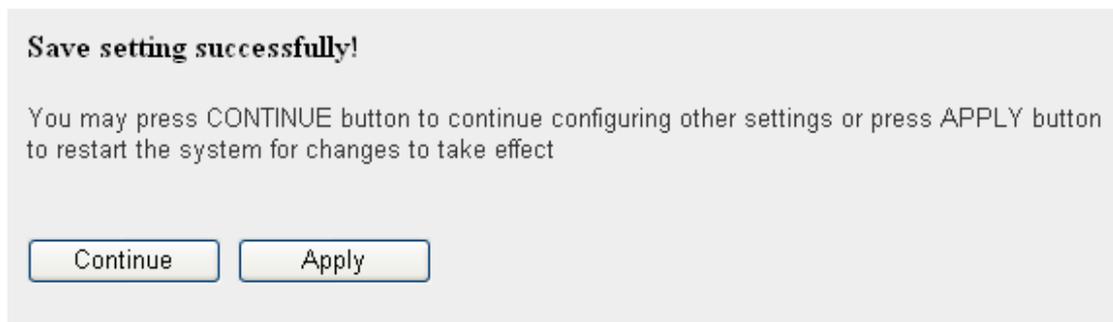
1. Always enable data encryption. Only disable it when you want to open your wireless access point to the public.
2. Never use simple words as encryption password. Use the random combination of symbols, numbers, and alphabets will greatly improve security.
3. Use WPA when possible - it's much safer than WEP.
4. Change encryption password when you've used it for too long time.

2-7-1 Disable Security

When you select 'Disable', wireless encryption is disabled. As mentioned before, you should only select this when you know what you're doing.



After you finish with setting, please click 'Apply', and the following message will be displayed:



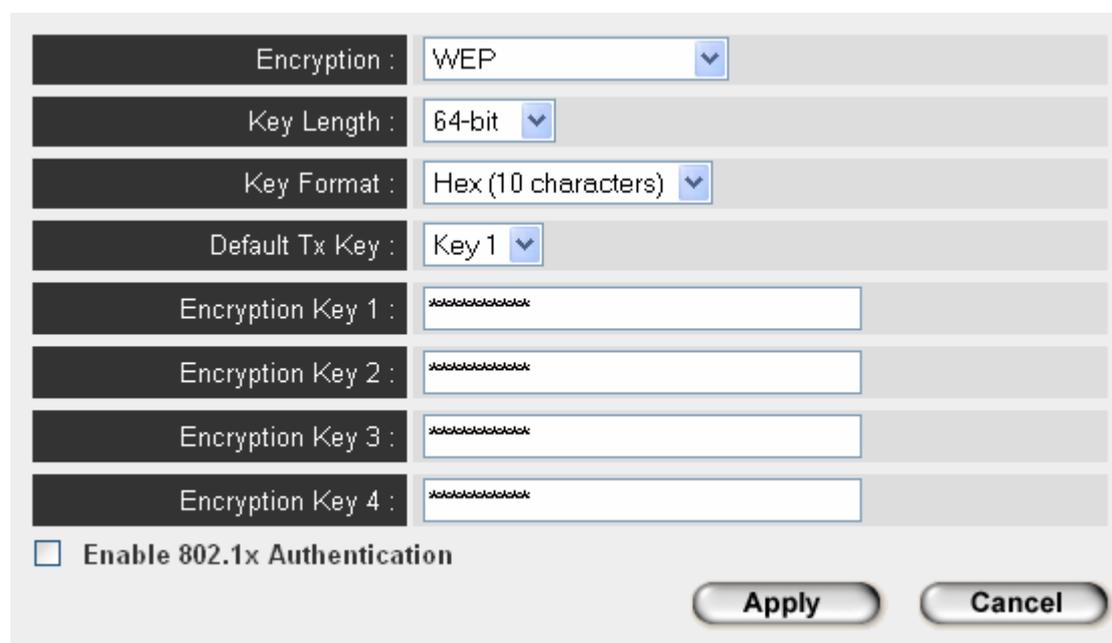
When you see this message, the settings you made is successfully save, You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-7-2 WEP

WEP (Wired Equivalent Privacy) is a common encryption mode, it's safe enough for home and personal use. But if you need higher level of security, please consider using WPA encryption (see next chapter).

However, some wireless clients don't support WPA, but only support WEP, so WEP is still a good choice for you if you have such kind of client in your network environment.

When you select 'WEP' as encryption type, the following messages will be displayed:



The screenshot shows a configuration window for WEP encryption. It includes the following fields and options:

- Encryption : WEP (dropdown)
- Key Length : 64-bit (dropdown)
- Key Format : Hex (10 characters) (dropdown)
- Default Tx Key : Key1 (dropdown)
- Encryption Key 1 : [masked]
- Encryption Key 2 : [masked]
- Encryption Key 3 : [masked]
- Encryption Key 4 : [masked]
- Enable 802.1x Authentication
- Buttons: Apply, Cancel

Here are descriptions of every setup items:

<i>Key Length</i>	<i>There are two types of WEP key length: 64-bit and 128-bit. Using '128-bit' is safer than '64-bit', but will reduce some data transfer performance.</i>
<i>Key Format</i>	<i>There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select '64-bit' as key length, and 'Hex' as key format, you'll see the message at the right of 'Key</i>

	<i>Format' is 'Hex (10 characters), which means the length of WEP key is 10 characters.</i>
<i>Default Tx Key</i>	<i>You can set up to four sets of WEP key, and you can decide which key is being used by default here. If you don't know which one you should use, select 'Key 1'.</i>
<i>Encryption Key 1 to 4</i>	<i>Input WEP key characters here, the number of characters must be the same as the number displayed at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same with each other.</i>
<i>Enable 802.1x Authentication</i>	<i>Check this box to enable 802.1x user authentication. Please refer to chapter 2-7-5 for detailed instructions.</i>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

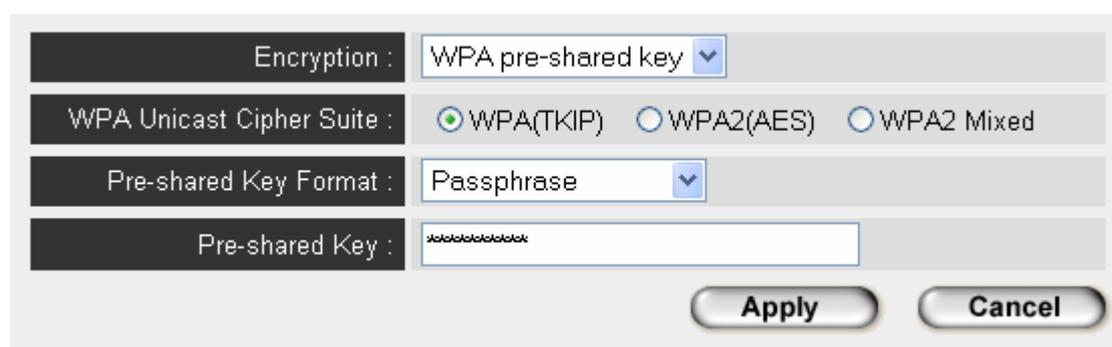
Continue
Apply

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-7-3 WPA Pre-shared Key

WPA Pre-shared key is the safest encryption method currently, and it's recommended to use this encryption method to ensure the safety of your data.

When you select 'WPA pre-shared key' as encryption type, the following messages will be displayed:



The screenshot shows a configuration dialog box for WPA settings. It has four rows of controls:

- Encryption :** A dropdown menu with 'WPA pre-shared key' selected.
- WPA Unicast Cipher Suite :** Three radio buttons: 'WPA(TKIP)' (selected), 'WPA2(AES)', and 'WPA2 Mixed'.
- Pre-shared Key Format :** A dropdown menu with 'Passphrase' selected.
- Pre-shared Key :** A text input field containing a masked key (asterisks).

At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Here are descriptions of every setup items:

<i>WPA Unicast Cipher Suite</i>	<i>You can select WPA encryption type here. AES is safer than TKIP, but not every wireless client supports it. Please refer to the specification of your wireless client to decide which encryption type you should use.</i>
<i>Pre-shared Key Format</i>	<i>Please select the format of pre-shared key here, available options are 'Passphrase' (8 to 63 alphanumerical characters) and 'Hex (64 hexadecimal characters – 0 to 9 and a to f).</i>
<i>Pre-shared Key</i>	<i>Please input pre-shared key according to the key format you selected here. For security reason, don't use simple words).</i>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue

Apply

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-7-4 WPA RADIUS

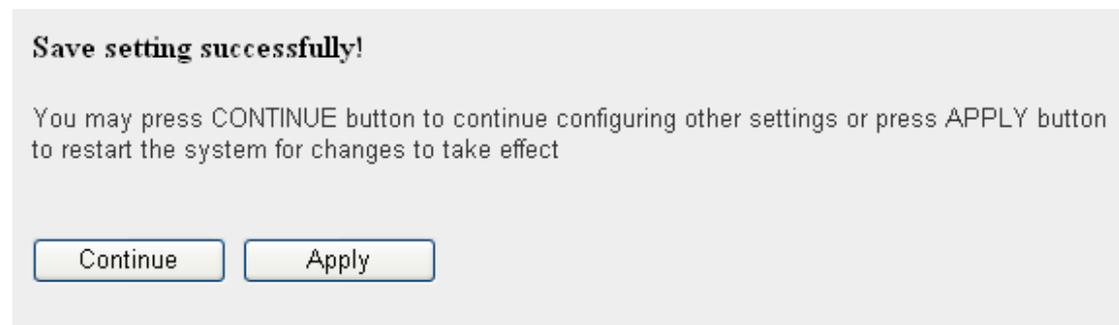
WPA Radius is the combination of WPA encryption method and RADIUS user authentication. If you have a RADIUS authentication server, you can check the identify of every wireless clients by user database.

When you select ‘WPA RADIUS’ as encryption type, the following messages will be displayed:

Here are descriptions of every setup items:

<i>WPA Unicast Cipher Suite</i>	<i>You can select WPA encryption type here. AES is safer than TKIP, but not every wireless client supports it. Please refer to the specification of your wireless client to decide which encryption type you should use.</i>
<i>Use internal MD5 RADIUS Server</i>	<i>Uses built-in RADIUS Server (refer to chapter 2-8) instead of external RADIUS server. If you check this box, the value in following three fields will be ignored.</i>
<i>RADIUS Server IP address</i>	<i>Please input the IP address of RADIUS authentication server here.</i>
<i>RADIUS Server Port</i>	<i>Please input the port number of RADIUS authentication server here. Default value is 1812.</i>
<i>RADIUS Server Password</i>	<i>Please input the password of RADIUS authentication server here.</i>

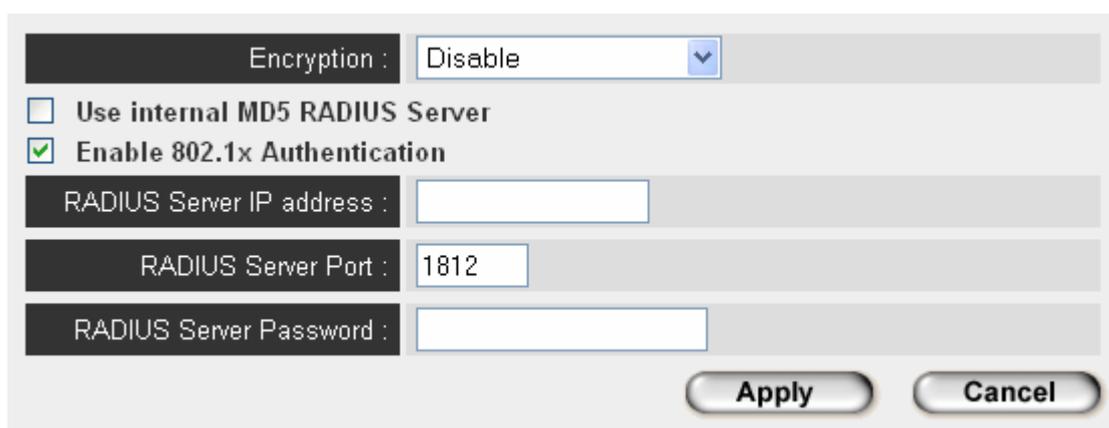
After you finish with setting, please click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-7-5 802.1x Authentication

You can enable 802.1x user identification (based on RADIUS user authentication server) by checking 'Enable 802.1x Authentication' box when you select 'Disable' or 'WEP' as encryption type, and the following message will be displayed:



Encryption :

Use internal MD5 RADIUS Server

Enable 802.1x Authentication

RADIUS Server IP address :

RADIUS Server Port :

RADIUS Server Password :

Here are descriptions of every setup items:

<i>Use internal MD5 RADIUS Server</i>	<i>Uses built-in RADIUS Server (refer to next chapter) instead of external RADIUS server. If you check this box, the value of internal RADIUS server fields will be ignored.</i>
<i>Enable 802.1x Authentication</i>	<i>Enable or disable the use of 802.1x user authentication.</i>
<i>RADIUS Server IP address</i>	<i>Please input the IP address of RADIUS authentication server here.</i>
<i>RADIUS Server Port</i>	<i>Please input the port number of RADIUS authentication server here. Default value is 1812.</i>
<i>RADIUS Server Password</i>	<i>Please input the password of RADIUS authentication server here.</i>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue

Apply

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-8 Radius Server

Comparing to other wireless security measures, radius server provides user-based authentication. If your wireless client supports 802.1x user authentication, you can use the 'Radius Server' function to use the internal mini radius server to improve security and wireless user control.

The internal radius server only supports 96 users and 16 IP addresses. If the number of user and/or IP address you need is more than this, please use external radius server.

To setup internal radius server, click 'Radius Server' on the left of web management interface, and the following information will be displayed:

Enable Radius Server

Users Profile (up to 96 users)

Username	Password	Re-Type Password	Configure
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Reset"/>

NO.	Username	Select
1	chen	<input type="checkbox"/>

Authentication Client (up to 16 clients)

Client IP	Secret Key	Re-Type Secret Key	Configure
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Reset"/>

NO.	Client IP	Select
1	192.168.2.25	<input type="checkbox"/>

Here are descriptions of every setup items:

<i>Enable Radius Server</i>	<i>Check this box to enable internal radius server function.</i>
<i>User Profile</i>	<p><i>You can add or delete radius user here. Please input username, password, re-type password in corresponding field, and click 'Add' button to add the user to radius server database. You can click 'Reset' to clear the text you typed in above three fields.</i></p> <p><i>All current radius users will be listed here. If you want to delete one or more users, check 'Select' box of that user, and click 'Delete Selected' button; you can click 'Delete All' button to delete all users in radius server database. You can also click 'Reset' button to uncheck all 'Select' boxes.</i></p>
<i>Authentication Client</i>	<p><i>You can add allowed radius client IP address here. Please input client IP, secret key, re-type secret key in corresponding field, and click 'Add' button to add the IP address to radius server database. You can click 'Reset' to clear the text you typed in above three fields.</i></p> <p><i>All current IP addresses will be listed here. If you want to delete one or more addresses, check 'Select' box of that address, and click 'Delete Selected' button; you can click 'Delete All' button to delete all addresses in radius server database. You can also click 'Reset' button to uncheck all 'Select' boxes.</i></p>

After you finish with setting, please click 'Apply', and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue

Apply

When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-9 MAC Filtering

Another security measure you can use to keep hackers and intruders away is 'MAC filtering'. You can pre-define a so-called 'white-list', which contains MAC addresses of the wireless clients you trust. All other wireless client with the MAC address which is not in your list will be denied by this wireless access point.

To setup MAC filtering, please click 'MAC Filtering' on the left of web management interface, and the following messages will be displayed:

• MAC Address Filtering Table
It allows to entry 20 sets address only.

NO.	MAC Adres	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable Wireless Access Control

New MAC Address: Comment:

Address filtering table (1)

Add new entry here (2)

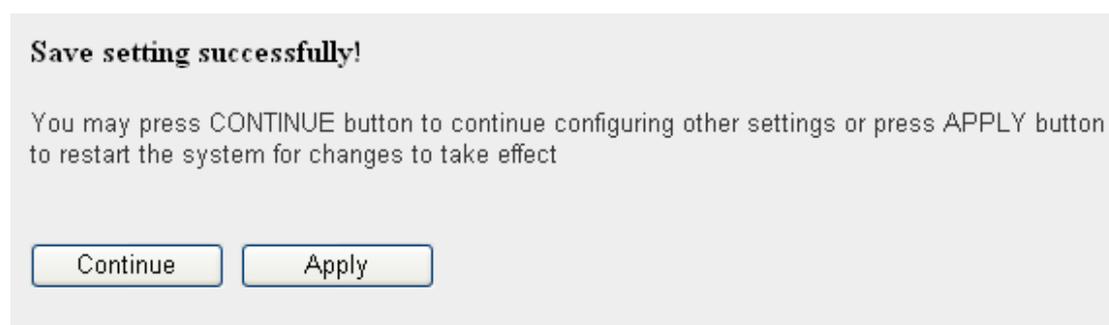
This page contains 2 parts of MAC filtering information. All allowed MAC addresses will be listed in upper part (1), and you can add new MAC addresses by components in lower part (2).

Here are descriptions of every setup items:

<i>Select</i>	<i>Check this box to select one or more MAC address(es) to delete.</i>
<i>Delete Selected</i>	<i>Click this button to delete all selected MAC address(es).</i>
<i>Delete All</i>	<i>Delete all MAC address entries.</i>
<i>Reset</i>	<i>Uncheck all selected MAC address entries.</i>
<i>Enable Wireless</i>	<i>Check this box to enable MAC address restriction,</i>

<i>Access Control</i>	<i>if unchecked, no restriction will be enforced (any wireless client with proper encryption setting will be able to connect to this wireless access point).</i>
<i>MAC address</i>	<i>Input MAC address allowed to use this wireless access point here. You don't have to add colon (:), or hyphen (-) by yourself, just input 0 to 9 and a to f here, like 112233445566 or aabbccddeeff.</i>
<i>Comment</i>	<i>You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid. This is optional.</i>
<i>Add</i>	<i>When you finish inputting MAC address and (optional) Comment, click this button to add the MAC address to the list.</i>
<i>Clear</i>	<i>Remove all characters in 'MAC address' and 'Comments' field.</i>

After you finish with setting, please click 'Apply', and the following message will be displayed:



When you see this message, the settings you made is successfully save., You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

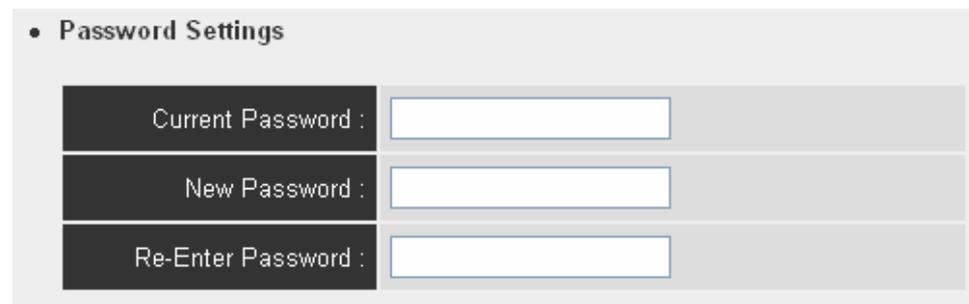
2-10 System Utilities

This access point provides some control functions include password, IP address management, and DHCP server function. Please click ‘System Utility’ on the left of web management interface to access these functions. Below are detailed descriptions of every control function.

2-10-1 Change Password

You can change the password used to enter the web configuration menu of this wireless access point.

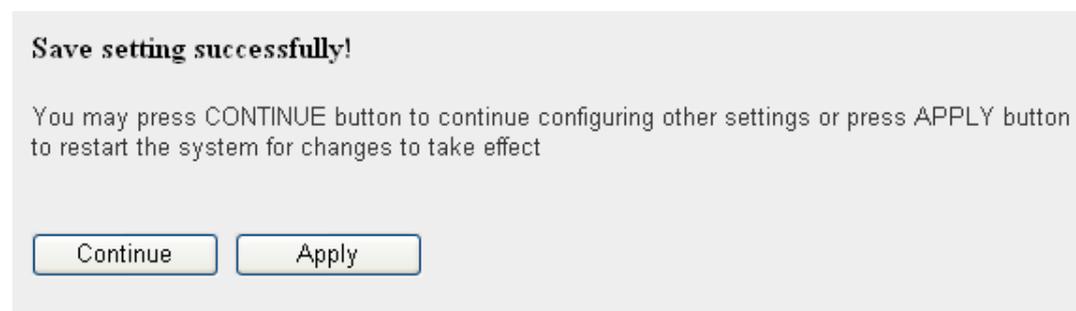
Please click ‘System Utility’ on the left, and the following message will be displayed:



The screenshot shows a web form titled "Password Settings" with three input fields:

- Current Password :** A text input field.
- New Password :** A text input field.
- Re-Enter Password :** A text input field.

Please input current password in ‘Current Password’ field, then input new password in both ‘New Password’ and ‘Re-Enter Password’ field. After you finish, please go to the bottom of this page and click ‘Apply’, and the following message will be displayed:



The screenshot shows a message box with the following content:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue Apply

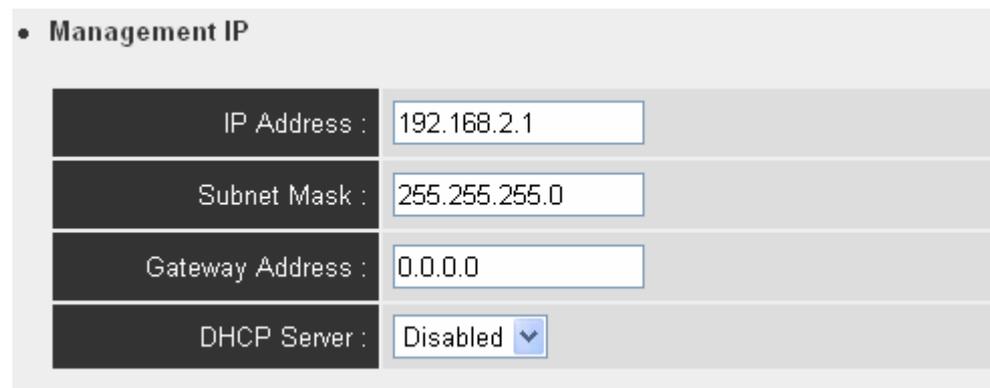
When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-10-2 IP Address of the Wireless Access Point

You can change the IP address of this wireless access point, so it can become a part of your local network. Please remember this address, you will not be able to connect the configuration menu of this wireless access point if you forget it.

Default IP address is: 192.168.2.1 / Subnet Mask 255.255.255.0, you can press and hold 'Reset' button to change the IP address back to default value if you forget the IP address you set.

To change IP address, please click 'System Utility' on the left, and the following message will be displayed:



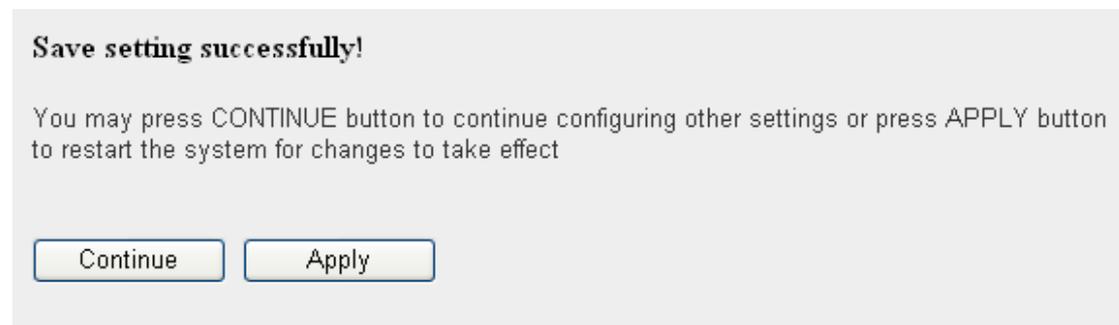
The screenshot shows a configuration window titled "Management IP". It contains four rows of configuration options:

IP Address :	<input type="text" value="192.168.2.1"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Address :	<input type="text" value="0.0.0.0"/>
DHCP Server :	<input type="button" value="Disabled"/> ▾

Please input IP address and Subnet Mask in corresponding field, and you can input the IP address of gateway in 'Gateway Address' field, if you need to manage this wireless access point from other network (like Internet).

If you want to activate the DHCP server function of this wireless access point, please select 'Enabled' in 'DHCP Server' option, and see next chapter for detailed instructions; if you don't want to use DHCP server function of this wireless access point, or there's another DHCP server on the network this access point connects to, please select 'Disable'.

After you finish, please go to the bottom of this page and click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2-10-3 DHCP Server

This wireless access point is capable to act as a DHCP server for your network, and it's disabled by default. If you want to activate this function, please click 'System Utility' on the left, and the following message will be displayed:

• DHCP Server

Default Gateway IP :	<input type="text" value="0.0.0.0"/>
Domain Name Server IP :	<input type="text" value="0.0.0.0"/>
Start IP :	<input type="text" value="192.168.2.100"/>
End IP :	<input type="text" value="192.168.2.200"/>
Domain Name :	<input type="text"/>
Lease Time :	<input type="text" value="Forever"/>

NOTE: Please remember to select 'Enable' in 'DHCP Server' option as described in last chapter, or all DHCP-related fields will be grayed out, and you will not be able to input any DHCP parameter.

Here are descriptions of every setup items:

<i>Default Gateway IP</i>	<i>Please input the IP address of default gateway of your network here. If not set, the IP address of this wireless access point will be provided to client.</i>
<i>Domain Name Server IP</i>	<i>Please input the IP address of domain name server (DNS) here. If not set, the IP address of this wireless access point will be provided to client.</i>
<i>Start IP</i>	<i>Please input the start IP address of the IP range.</i>
<i>End IP</i>	<i>Please input the end IP address of the IP range.</i>
<i>Domain Name</i>	<i>If you wish, you can also optionally input the domain name for your network. This is optional.</i>
<i>Lease Time</i>	<i>Please choose a lease time (the duration that every computer can keep a specific IP address) of every</i>

	<i>IP address assigned by this access point from dropdown menu.</i>
--	---

After you finish, please click ‘Apply’, and the following message will be displayed:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

When you see this message, the settings you made is successfully save., You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

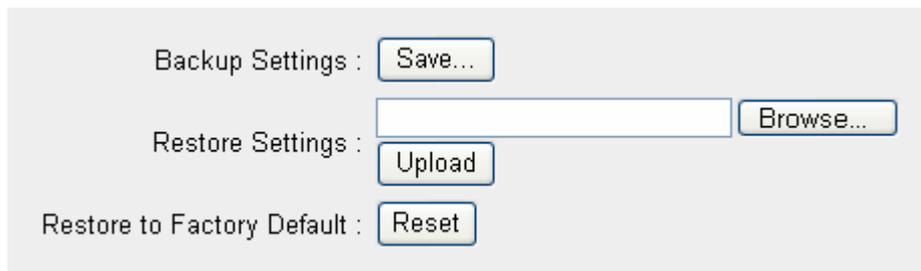
Chapter III: Advanced Configuration

3-1 Configuration Backup and Restore

You can backup all configurations of this access point to a file, so you can make several copied of access point configuration for security reason.

To backup or restore access point configuration, please follow the following instructions:

Please click ‘Configuration Tool’ on the left of web management interface, and the following message will be displayed on your web browser:



The screenshot shows a web interface for configuration management. It contains three sections: 'Backup Settings' with a 'Save...' button; 'Restore Settings' with a text input field and a 'Browse...' button; and 'Restore to Factory Default' with a 'Reset' button.

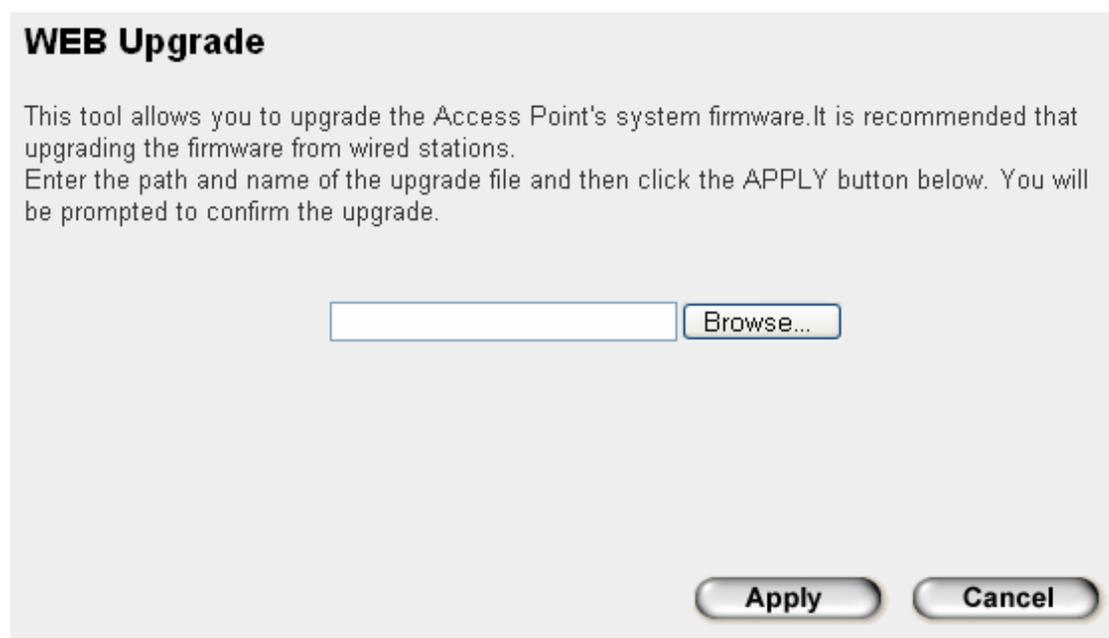
Here are descriptions of every buttons:

<i>Backup Settings</i>	<i>Press ‘Save...’ button, and you’ll be prompted to download the configuration as a file, default filename is ‘default.bin’, you can please save it as another filename for different versions, and keep it in a safe place.</i>
<i>Restore Settings</i>	<i>Press ‘Browse...’ to pick a previously-saved configuration file from your computer, and then click ‘Upload’ to transfer the configuration file to access point. After the configuration is uploaded, the access point’s configuration will be replaced by the file you just uploaded.</i>
<i>Restore to Factory Default</i>	<i>Click this button to remove all settings you made, and restore the configuration of this access point back to factory default settings.</i>

3-2 Firmware Upgrade

If there are new firmware of this wireless access point available, you can upload the firmware to the access point to change the firmware with new one, to get extra functions or problem fix.

To perform firmware upgrade, please click 'Upgrade' on the left of web management interface, and the following message will be displayed:



WEB Upgrade

This tool allows you to upgrade the Access Point's system firmware. It is recommended that upgrading the firmware from wired stations. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

Click 'Browse' button first, you'll be prompted to provide the filename of firmware upgrade file. Please download the latest firmware file from our website, and use it to upgrade your access point.

After a firmware upgrade file is selected, click 'Apply' button, and the access point will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

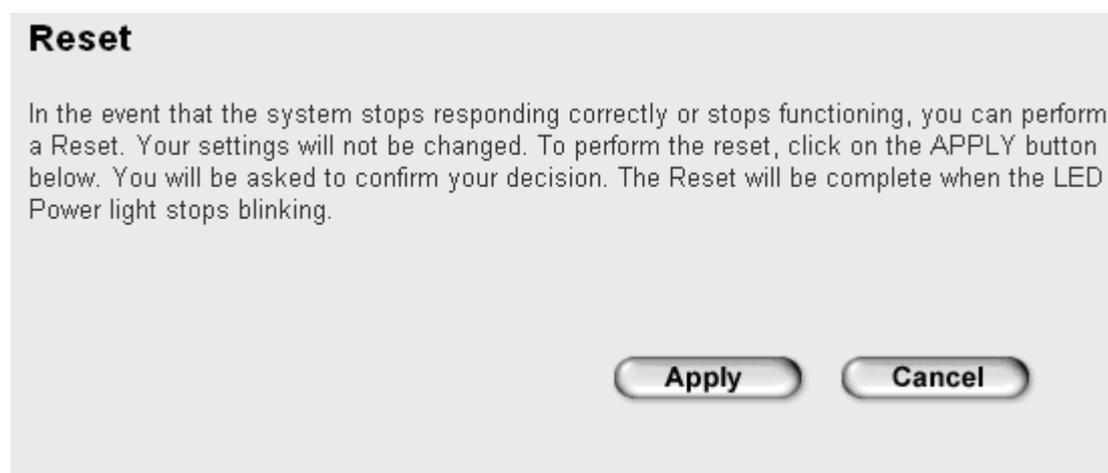
NOTE: Never interrupt the upgrade procedure by closing the web browser or physically disconnect your computer from access point. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may have to return this access point to the dealer of purchase to ask for help. (Warranty voids if you interrupted the

3-3 System Reset

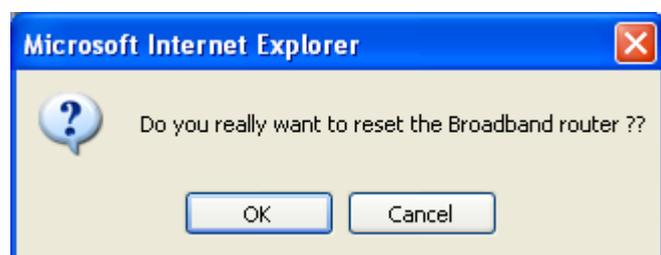
When you think the access point is not working properly, you can use this function to restart the access point, this may help and solve the problem.

This function is useful when the access point is far from you or unreachable. However, if the access point is not responding, you may have to switch it off by unplugging the power plug and plugging it back again after 10 seconds.

To reset your access point, please click 'Reset' on the left, and the following message will be displayed:



Please click 'Apply', and a popup message will ask you again, to make sure you really want to reset the access point:



Click 'OK' to reset the access point, or click 'Cancel' to abort. Please remember all connections between wireless client and this access point will be disconnected.

Chapter IV: Appendix

4-1 Hardware Specification

CPU: Ralink RT1310

Switch: Realtek RTL8305SC (5 Port Switch)

Wireless Module: Ralink RT2860+RT2820

Flash: 4MB

SDRAM: 16MB

WAN Port: 10/100M UTP Port x 1

LAN Ports: 10/100M UTP Port x 4

Antenna: Fixed Antenna x 3 (2T3R MIMO Technology)

Power: 12VDC, 1A Switching Power Adapter

Dimension: 30(H) x 187(W) x 100(D) mm

Temperature: 32~104°F (0 ~ 40°C)

Humidity: 10-90% (NonCondensing)

Certification: FCC, CE

4-2 Troubleshooting

If you found the access point is working improperly or stop responding to you, don't panic! Before you contact your dealer of purchase for help, please read this troubleshooting first. Some problems can be solved by yourself within very short time!

Scenario	Solution
Access point is not responding to me when I want to access it by web browser	<ol style="list-style-type: none">a. Please check the connection of power cord and network cable of this access point. All cords and cables should be correctly and firmly inserted to the access point.b. If all LEDs on this access point are out, please check the status of A/C power adapter, and make sure it's correctly powered.c. You must use the same IP address section which access point uses.d. Are you using MAC or IP address filter? Try to connect the access point by another computer and see if it works; if not, please perform a hard reset (pressing 'reset' button).e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help.g. If all above solutions don't work, contact the dealer of purchase for help.
Can't get connected to wireless access point	<ol style="list-style-type: none">a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client.b. Try to move closer to wireless access point.c. Unplug the power plug of access point, and plug it back again after 10 seconds.d. If all LEDs on this access point are out,

	<p>please check the status of A/C power adapter, and make sure it's correctly powered.</p>
<p>I can't locate my access point by my wireless client</p>	<ul style="list-style-type: none"> a. 'Broadcast ESSID' set to off? b. Is Antenna properly installed and secured? c. Are you too far from your access point? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled. e. If antenna is not installed, install them now and never remove them.
<p>File download is very slow or breaks frequently</p>	<ul style="list-style-type: none"> a. Try to reset the access point and see if it's better after that. b. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. c. Change channel number and see if this works.
<p>I can't log onto web management interface: password is wrong</p>	<ul style="list-style-type: none"> a. Make sure you're connecting to the correct IP address of the access point! 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.
<p>Access point become hot</p>	<ul style="list-style-type: none"> a. This is not a malfunction, if you can keep your hand on the access point's case. b. If you smell something wrong or see the smoke coming out from access point or A/C power adapter, please disconnect the access point and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

4-3 Glossary

Default Gateway (Access point): Every non-access point IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as `www.Broadbandaccess point.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "`Broadbandaccess point.com`" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: `192.168.2.1`. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": `aaa.aaa.aaa.aaa`, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".":

`bbbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb`, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading

1's followed by consecutive trailing 0's, such as

11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,

11011001.10110000.10010000.00000111, and if its network mask is,

11111111.11111111.11110000.00000000

It means the device's network address is

11011001.10110000.10010000.00000000, and its host ID is,

00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Access point: A access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and

Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

4-4 FCC Statement

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

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

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

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.