

Black Box Tech Support: FREE! Live. 24/7.

Tech support the
way it should be.



Great tech support is just 20 seconds away at 724-746-5500 or blackbox.com.



About Black Box

Black Box Network Services is your source for more than 118,000 networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 20 seconds or less.

© Copyright 2009. All rights reserved.

724-746-5500 | blackbox.com

802.11N 2T2R Wireless Access Point

Connect 802.11N Draft-N compatible computers and wireless devices to an existing wired Ethernet network.

Operates at speeds up to 300 Mbps.



**Customer
Support
Information**

Order toll-free in the U.S.: Call 877-877-BBOX (outside U.S. call 724-746-5500) •
FREE technical support 24 hours a day, 7 days a week: Call 724-746-5500 or fax 724-746-0746
• Mailing address: Black Box Corporation, 1000 Park Drive, Lawrence, PA 15055-1018 •
Web site: www.blackbox.com • E-mail: info@blackbox.com

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

We're here to help! If you have any questions about your application or our products, contact Black Box Tech Support at **724-746-5500** or go to **blackbox.com** and click on "Talk to Black Box." You'll be live with one of our technical experts in less than 20 seconds.

1. Specifications	8
2. Overview.....	9
2.1 Introduction	9
2.2 Features	9
2.3 Safety Information	9
2.4 System Requirements	10
2.5 What's Included	10
2.6 Front Panel.....	10
2.7 Back Panel.....	11
3. Installation and Configuration	12
3.1 Installation.....	12
3.2 Using a Web Browser to Configure the Wireless Access Point.....	12
3.2.1 Windows 95/98/Me IP Address Setup	12
3.2.2 Windows 2000 IP Address Setup	14
3.2.3 Windows XP IP Address Setup.....	16
3.2.4 Windows Vista IP Address Setup	18
3.2.5 Connecting to the Web Management Interface.....	19
3.3 View System Status and Information	20
3.4 Select an Operating Mode for the Wireless Access Point	22
3.4.1 AP Mode.....	22
3.4.2 Station Infrastructure	25
3.4.3 AP Bridge-Point to Point Mode	27
3.4.4 AP Bridge-Point to Multipoint Mode	28
3.4.5 AP Bridge-WDS Mode.....	30
3.4.6 Universal Repeater	31
3.5 WPS Setting	33
3.6 Advanced Wireless Settings.....	35
3.7 Wireless Security	37
3.7.1 Disable Security	38
3.7.2 WEP	39
3.7.3 WPA Pre-shared Key	40
3.7.4 WPA RADIUS.....	41
3.7.5 802.1x Authentication	43
3.8 Radius Server	44
3.9 MAC Filtering.....	45

- 3.10 System Utilities 47
 - 3.10.1 Change Password 47
 - 3.10.2 IP Address of the Wireless Access Point 48
 - 3.10.3 DHCP Server 49
- 4. Advanced Configuration 51
 - 4.1 Configuration Backup and Restore 51
 - 4.2 Firmware Upgrade 52
 - 4.3 System Reset..... 52
- Appendix A. Troubleshooting..... 54
 - A.1 Problems/Solutions 54
 - A.2 Calling Black Box 55
 - A.3 Shipping and Packaging..... 55
- Appendix B. Glossary 56

Federal Communications Commission and Industry Canada Radio Frequency Interference Statements

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular 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. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

Caution:

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

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Instrucciones de Seguridad

(Normas Oficiales Mexicanas Electrical Safety Statement)

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá de lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - A: El cable de poder o el contacto ha sido dañado; u
 - B: Objetos han caído o líquido ha sido derramado dentro del aparato; o
 - C: El aparato ha sido expuesto a la lluvia; o
 - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - E: El aparato ha sido tirado o su cubierta ha sido dañada.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces 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 for this equipment must therefore be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

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

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

EU Countries Not Intended for Use

None.

11N 2T2R Wireless Access Point

1. Specifications

Antenna: (2) 3-dBi Detachable Dipole Antennas (2T2R Spatial Multiplexing MIMO configuration) used for signal transmitting and receiving

Certification: FCC Class B, CE Flash: 4MB

SoC (System on Chip): Ralink RT3052 (single-chip AP/router)

SDRAM: 16MB

User Controls: (1) Reset/WPS button

Connectors: (1) 10/100-Mbps UTP RJ-45, (1) barrel connector for power, center positive (+)

Indicators: (3) LEDs: Pwr, WLAN, LAN

Temperature: 32–104° F (0–40° C)

Humidity: 10-90% (Noncondensing)

Transmit Power: 11n: 14dBm \pm 1.5dBm, 11g: 15dBm \pm 1.5dBm, 11b: 17 \pm 1.5dBm

Power: 5 VDC, 1A Switching Power Adapter

Size: 1.2"H x 5"W x 3.8"D (3 x 12.7 x 9.6 cm)

Weight: 0.4 lb. (0.2 kg)

2. Overview

2.1 Introduction

Use the 11N 2T2R Access Point to connect computers and wireless devices that are compatible with 802.11n/g/Draft-N to an existing wired Ethernet network at speeds of up to 300 Mbps.

Even inexperienced users can setup a network environment in a very short time (within minutes). Simply follow the setup procedure described in Section 3.2.

2.2 Features

- Compatible with IEEE 802.11b/g/Draft-N wireless network standard, so it works with other 802.11b/g/Draft-N wireless devices.
- High speed wireless network runs six times faster than a conventional 802.11g wireless network (up to 300Mbps).
- Allows wireless devices to connect to an existing wired network and share network resources.
- Supports DHCP server function.
- Supports 64/128-bit WEP, WPA, and WPA2 wireless data encryption.
- Supports MAC address filtering (only allows a specific wireless device of your choice to connect to this access point).
- Supports RADIUS server (only allows users listed in your authorization server to use the wireless network).
- Supports WPS (Wi-Fi Protected Setup) and simplifies wireless client setup procedures. Even an inexperienced user can set up a wireless network without a network technician's help.
- Easy to use web-based GUI (Graphical User Interface) for network configuration and management purposes.

2.3 Safety Information

For safety, follow these instructions:

1. This access point is designed for indoor use only; DO NOT place this access point outdoors.
2. DO NOT put this access point in or near hot or humid places, such as a kitchen or bathroom. Also, do not leave 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 in high places or hang it on the wall, make sure the access point is firmly secured. Falling from high places would damage the access point and its accessories, and void its warranty.
5. The access point contains small parts, so keep it out of reach of children under 3 years old.
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 are no user-serviceable parts inside the access point. If the access point is not working properly, contact Black Box Technical Support at 724-746-5500. DO NOT disassemble the access point, or its warranty will be void.
8. If the access point falls into water when it's powered, DO NOT pick it up with your hand. Switch the electrical power off before you do anything, or contact an experienced electrical technician for help.
9. If you smell something strange or see smoke coming out from the access point or power supply, remove the power supply or switch the electrical power off immediately, and call Black Box Technical Support at 724-746-5500.

2.4 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)

2.5 What’s Included

Your package should include the following items. If anything is missing or damaged, please contact Black Box Technical Support at 724-746-5500.

- Wireless Access Point
- 3-dBi dipole antenna (2 pcs)
- AC power adapter
- This user’s manual

2.6 Front Panel

The Wireless Access Point’s front panel is shown in Figure 2-1. Table 2-1 describes its components.



Figure 2-1. Front panel.

Table 2-1. Front panel components.

Number	Component	Light Status	Description
1	PWR LED	ON	The access point is switched on and correctly powered.
2	WLAN LED	ON	Wireless WPS mode is enabled.
		OFF	Wireless network is switched off.
		Flashing	Wireless access point is transferring or receiving data.
3	LAN LED	ON	The LAN port is connected.
		OFF	The LAN port is not connected.
		Flashing	The LAN is transferring or receiving data.

2.7 Back Panel

The Wireless Access Point's back panel is shown in Figure 2-2. Table 2-2 describes its components.

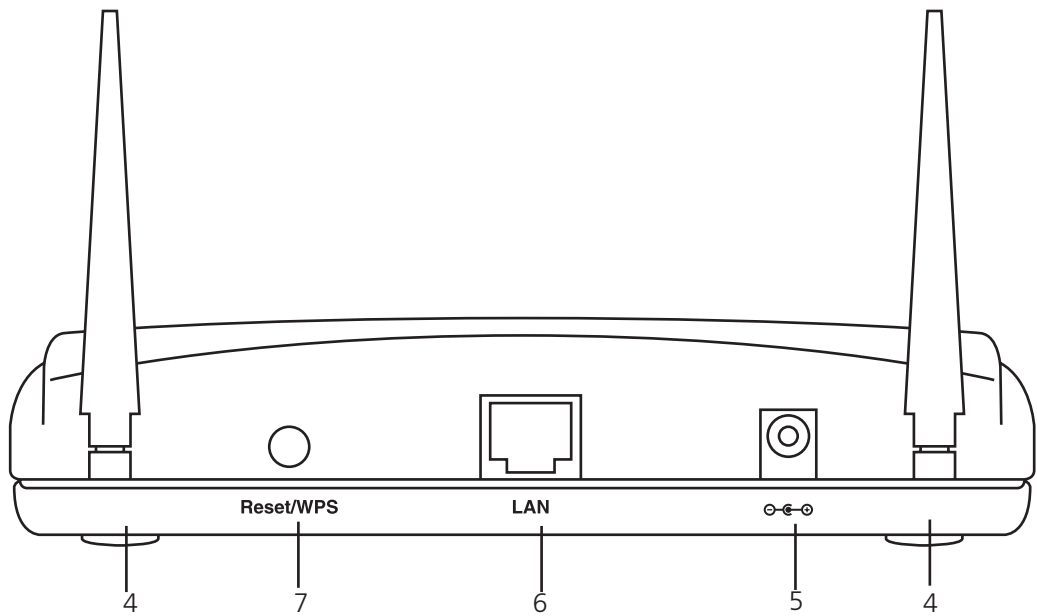


Figure 2-2. Back panel.

Table 2-2. Back panel components.

Number	Component	Description
4	Antennas	Included detachable 3-dBi antennas connect here.
5	Power connector	Connects to an A/C power adapter.
6	RJ-45 connector	Local Area Network (LAN) port.
7	Reset/WPS	Resets the router to its factory default settings (clears all settings), or starts the WPS function. Press and hold this button for 10 seconds to restore all settings to factory defaults. Press and hold this button for less than 5 seconds to start the WPS function.

3. Installation and Configuration

3.1 Installation

Please follow these instructions to connect the wireless access point to your computers and network devices:

1. Using an Ethernet cable, connect the access point to an ADSL modem, router, or switch/hub in your network.
2. Connect the A/C power adapter to the wall socket, and then connect it to the access point's power socket.
3. Check all the LEDs on the front panel. The PWR LED should be steadily on, and the LAN LEDs should be on if the access point is correctly connected to the ADSL modem, router, or switch/hub. If PWR LED is not on, or if any LED you expected to be on is not on, recheck the cabling, or go to Appendix A, Troubleshooting, for possible causes and solutions.

3.2 Using a Web Browser to Configure the Wireless Access Point

After connecting the access point to the network, you will set up the access point's network parameters so that 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 a static IP address, or you're unsure, follow the instructions below to configure your computer to use a dynamic IP address:

If your computer's operating system is:

- Windows 95/98/Me, go to Section 3.2.1
- Windows 2000, go to Section 3.2.2
- Windows XP, go to Section 3.2.3
- Windows Vista, go to Section 3.2.4

3.2.1 Windows 95/98/Me IP Address Setup

1. Click on the Start button (located at lower-left corner of your computer), then click on control panel. Double-click the Network icon, and the Network window will appear. Select TCP/IP, then click on Properties. See Figure 3-1.

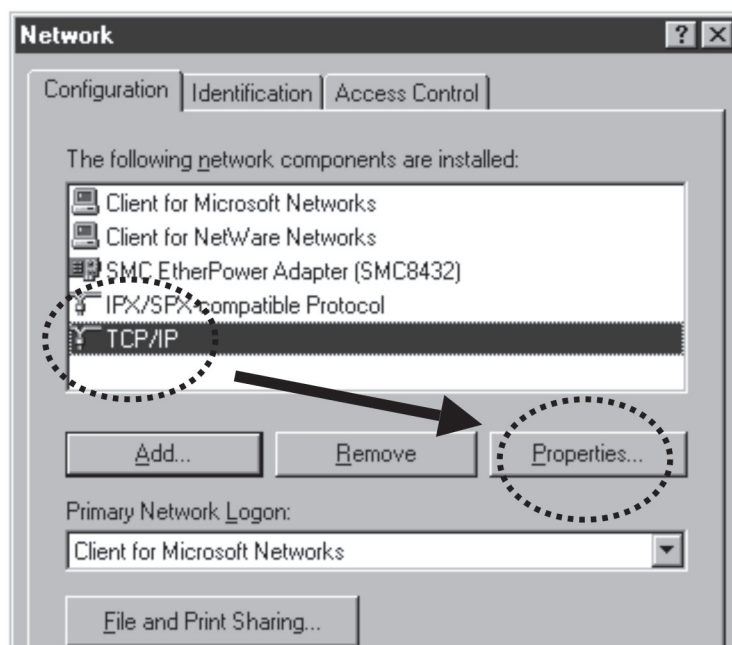


Figure 3-1. Network screen, Configuration tab, TCP/IP, Properties selected.

2. Select Specify an IP address, then input the following settings (see Figure 3-2):

IP address: 192.168.2.2

Subnet Mask: 255.255.255.0

Click OK when finished

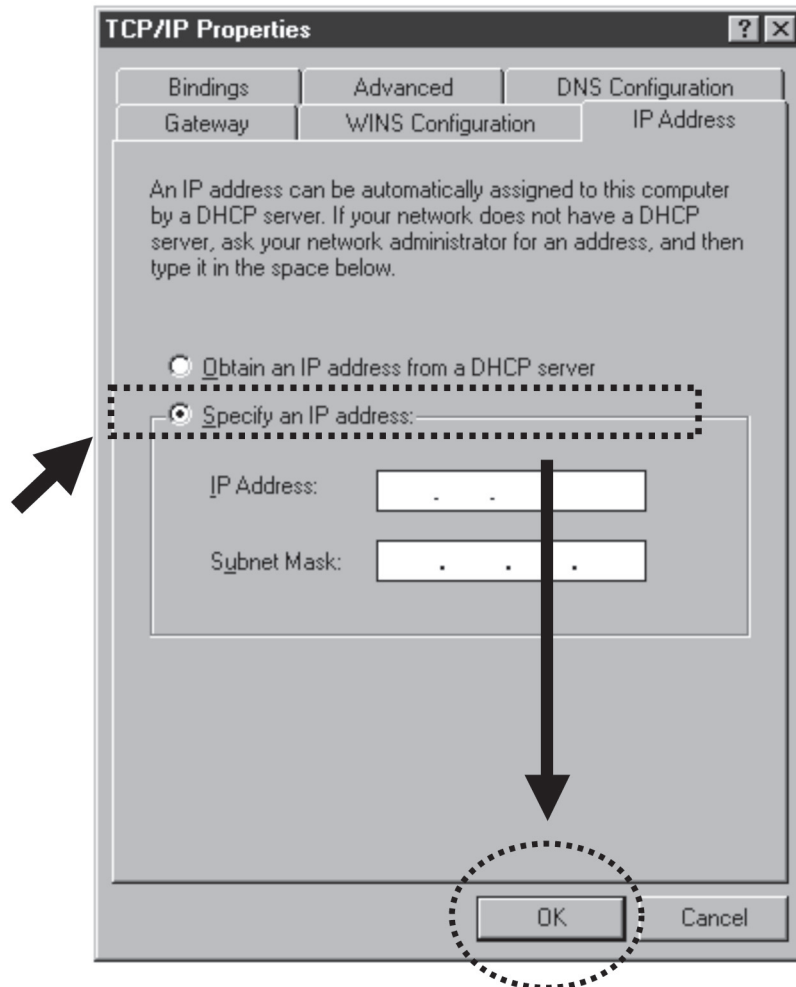


Figure 3-2. Input IP address and subnet mask.

3.2.2 Windows 2000 IP Address Setup

1. Click on the Start button (located at the lower-left corner of your computer), then click on control panel. Double-click on the Network and Dial-up Connections icons, double click Local Area Connection, and the Local Area Connection Properties window will appear. Select Internet Protocol (TCP/IP), then click on Properties (see Figure 3-3).

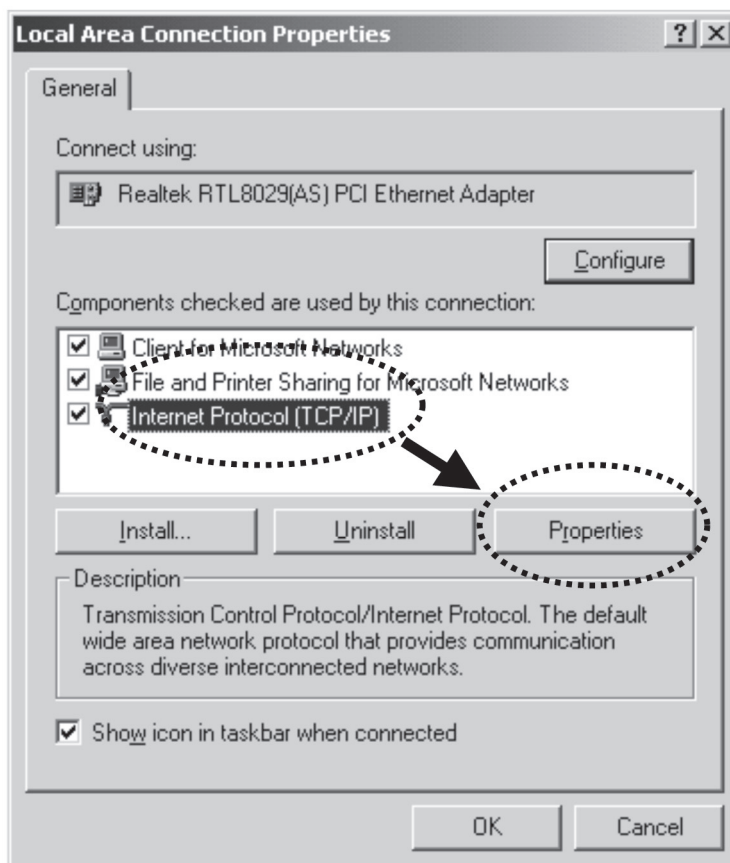


Figure 3-3. Local area connection properties screen.

2. Select Use the following IP address, then input the following settings:

IP address: 192.168.2.2

Subnet Mask: 255.255.255.0

Click OK when finished. See Figure 3-4.

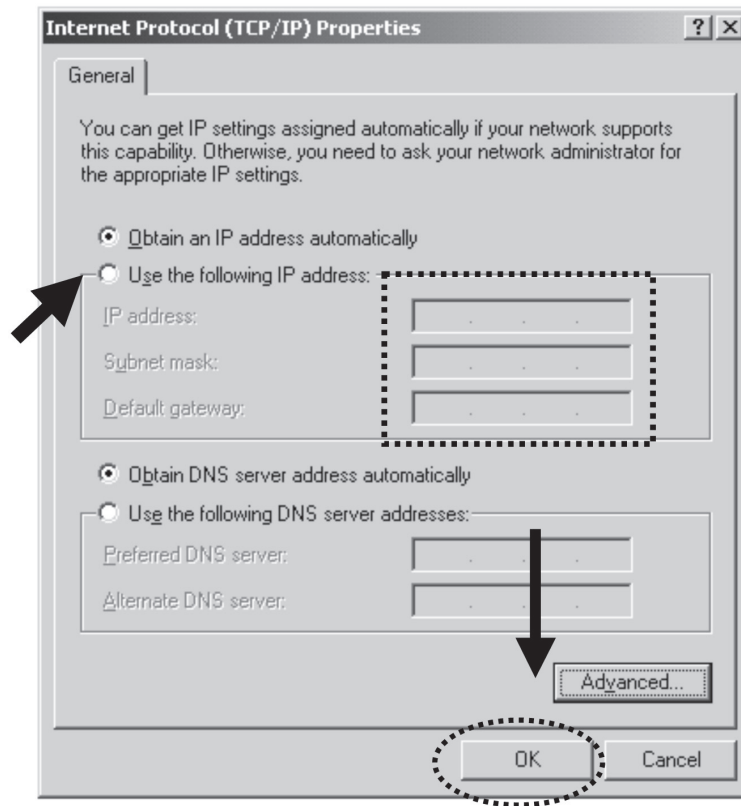


Figure 3-4. Internet protocol (TCP/IP) properties screen.

3.2.3 Windows XP IP Address Setup

1. Click on the Start button (located at lower-left corner of your computer), then click on the control panel. Double-click the Network and Internet Connections icon, click on Network Connections, and then double-click on Local Area Connection. The Local Area Connection Properties window will appear (see Figure 3-5). Then click on Properties.

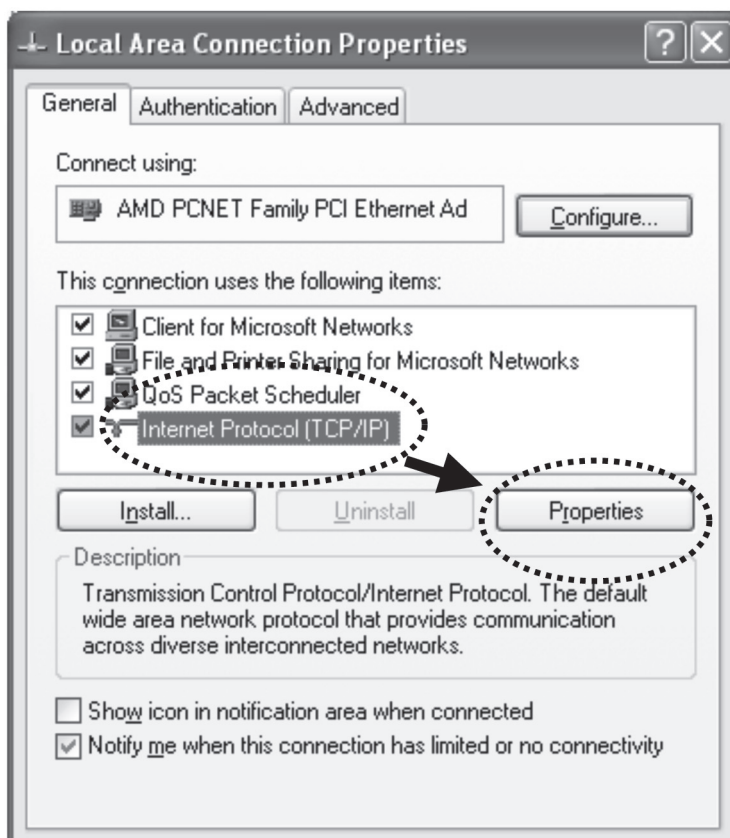


Figure 3-5. Local area connection properties screen, General tab.

2. Select Use the following IP address (see Figure 3-6), then input the following settings:

IP address: 192.168.2.2

Subnet Mask: 255.255.255.0

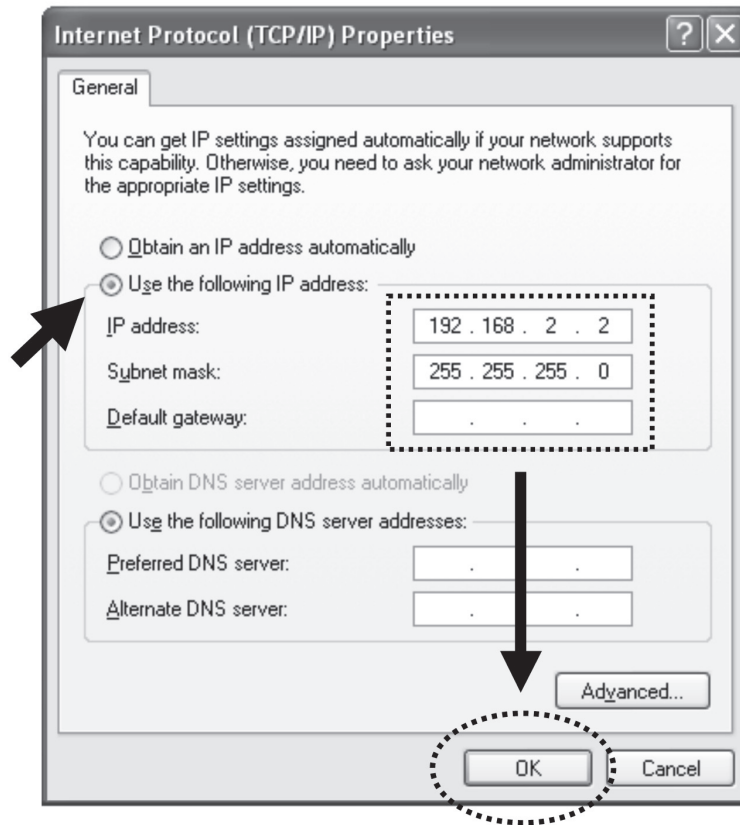


Figure 3-6. Internet protocol (TCP/IP) properties.

Click OK when finished.

3.2.4 Windows Vista IP Address Setup

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

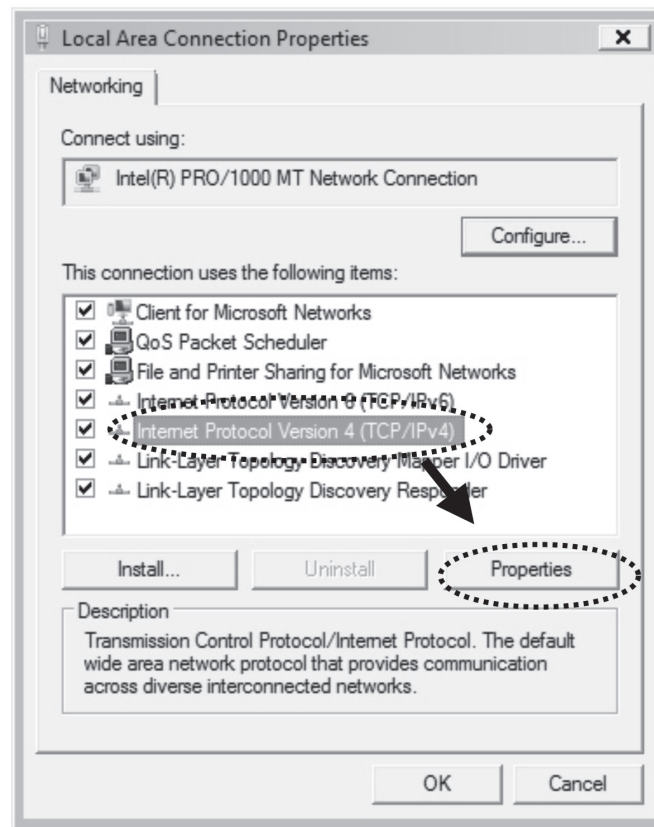


Figure 3-7. Local Area Connection Properties screen, Networking tab.

2. Select Use the following IP address, then input the following settings (see Figure 3-8):

IP address: 192.168.2.2

Subnet Mask: 255.255.255.0

Click OK when finished.

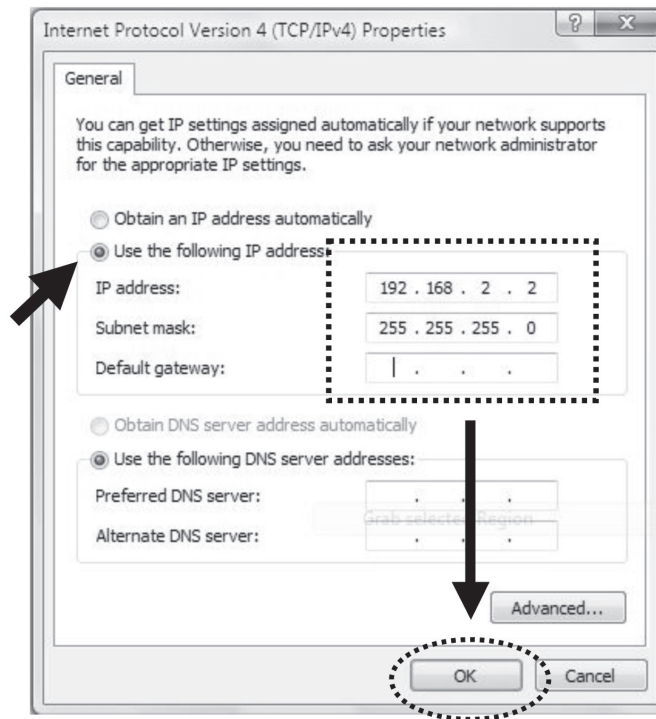


Figure 3-8. Properties window, General tab.

3.2.5 Connecting to the Web Management Interface

All functions and settings of this access point must be configured via the web management interface. Start your Web browser, and input 192.168.2.1 in the address bar, then press the Enter key. The following message appears (see Figure 3-9):

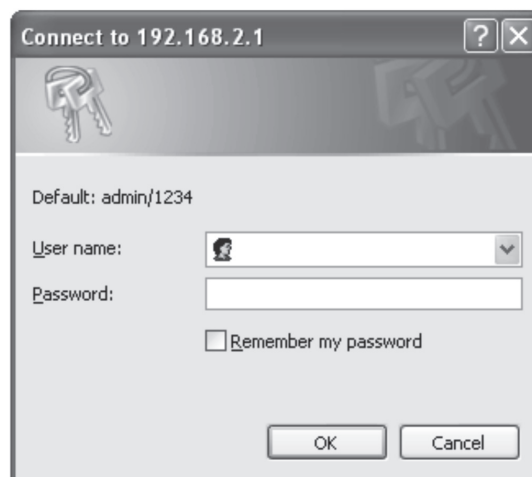


Figure 3-9. Connect to web management interface screen.

Type in the user name and password in the respective fields. (The default user name is admin, and the default password is 1234). Press the OK button, and the access point's Web management interface appears (see Figure 3-10):

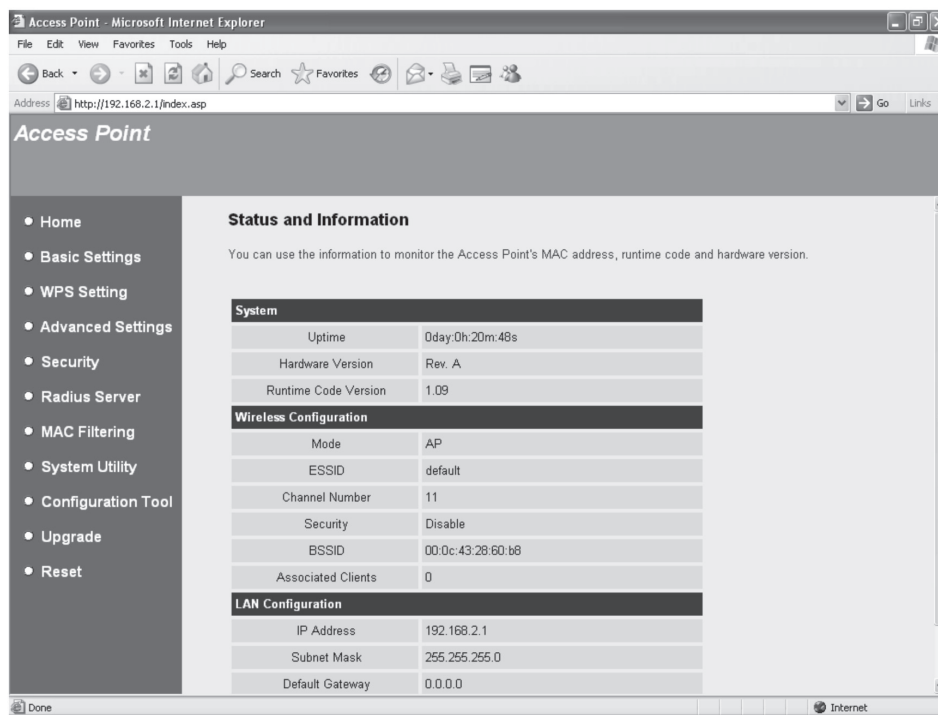


Figure 3-10. Web management interface.

NOTE: If you can't see the Web management interface, and you're prompted to input the user name and password again, you need to retype the user name and password correctly. If you're certain that the user name and password you typed are correct, see Appendix A, Troubleshooting.

3.3 View System Status and Information

After you connect to the access point via a Web browser, the first thing you see is the Status and Information page. All system and network related information for this access point will be displayed here. The information provides detailed information for your access point that will enable you to fix communication problems between this access point and other wired/wireless computers/devices.

Click Home on the left, and the system status and information displays, as shown below (see Figure 3-11).

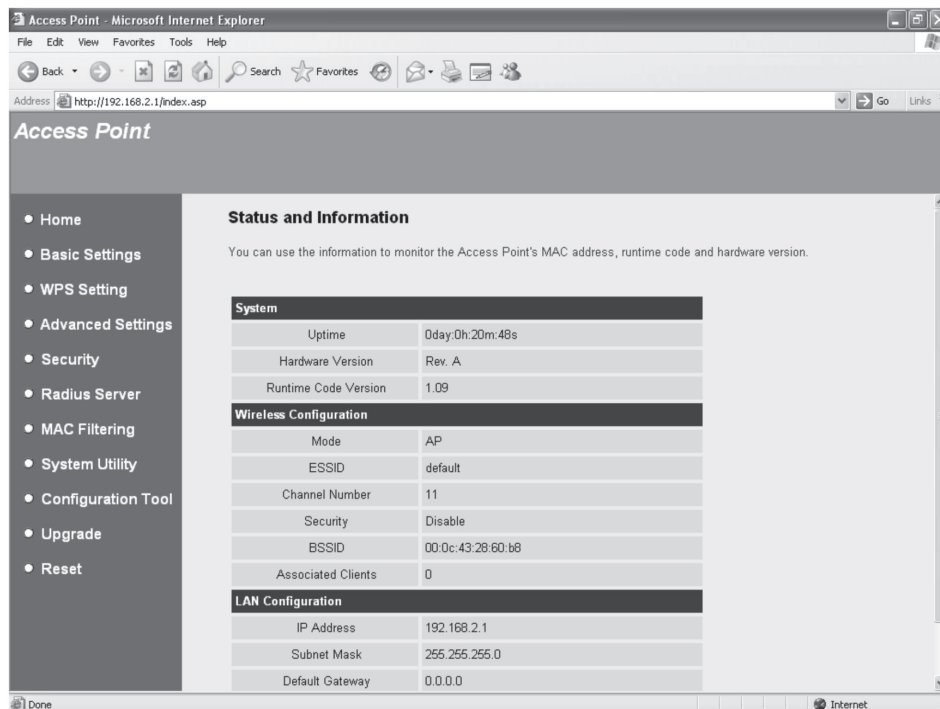


Figure 3-11. Status and information screen.

Table 3-1. Status and information screen options.

Option	Description
Up Time	Displays the total time passed since the wireless access point was powered on.
Hardware Version	Displays the hardware version. Use this information when you need online help from Black Box Technical Support.
Runtime Code Version	Displays the current firmware version. If you want to perform firmware upgrade, this number will help you to determine if you need an upgrade.
Mode	Displays the current wireless operating mode (see Section 3.4).
ESSID	Displays the current ESSID (the name used to identify this wireless access point).
Channel Number	Displays the current wireless channel number.
Security	Displays the current wireless security setting.
BSSID	Displays the current BSSID (a unique identification name for this access point, it cannot be modified by user).
Associated Clients	Displays the number of connected wireless clients.
IP Address	Displays the wireless access point's IP address.
Subnet Mask	Displays the IP address' net mask.
Default Gateway	Displays the default gateway's IP address.
MAC address	Displays the LAN interface's MAC address.

3.4 Select an Operating Mode for the Wireless Access Point

This access point operates in different modes; click on Basic Setting on the left of the Web management interface screen to select an operating mode for different needs:

Click on the Mode dropdown menu to select an operating mode. Six operating modes are available:

Table 3-2. Operating mode options.

Option	Description
AP	Access point mode, allows wireless clients to connect to the access point and exchange data with the devices connected to the wired network.
Station-Infrastructure	Enables an Ethernet device (such as a TV and game player) that's connected to a wireless client via the access point.
AP Bridge-Point to Point	Establishes a wireless connection with another wireless access point using the same mode, and links both access points to the wired network. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	Establishes a wireless connection with other wireless access points using the same mode, and links the wired network to these wireless access points. Up to 4 access points can be connected in this mode.
AP Bridge-WDS	This mode is similar to AP Bridge to Multi-Point, but the access point does not work in bridge-dedicated mode. It accepts wireless clients while working as a wireless bridge.
Universal Repeater	The AP acts as a wireless range extender to extend the networking wirelessly. It acts as a station and an AP at the same time. The AP can use the station function to connect to a root AP and use the AP function to service all wireless clients within its coverage area.

Select one wireless operating mode. For detailed descriptions of every operating mode, please refer to Sections 3.4.1 through 3.4.6.

3.4.1 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 exchanges data between them.

When you select AP, the following screen will be displayed:

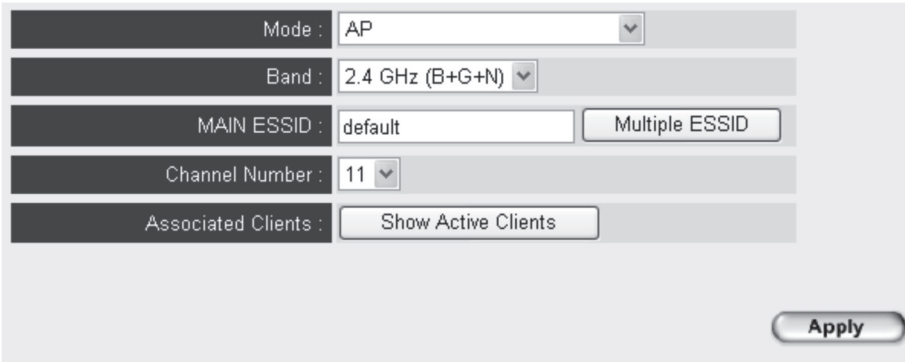


Figure 3-12. AP mode screen.

Table 3-3. AP mode setup options.

Option	Description
Band	<p>Select the wireless band you want to use. By selecting different band settings, you'll be able to allow or deny access to the wireless client on a certain band.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), then 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.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band will be able to connect to this access point.</p> <p>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).</p>
Main ESSID	<p>Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters.</p> <p>NOTE: ESSID IS CASE SENSITIVE.</p>
Multiple ESSID	<p>The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, click on this button.</p>
Channel Number	<p>Please select a channel number you wish to use. If you know a certain channel number is being used by other wireless access points nearby, don't use the same channel number.</p>
Associated Clients	<p>Click on the Show Active Clients button and a new popup window will appear that contains information about all wireless clients connected to this access point. Click on the Refresh button in the popup window to keep information up-to-date.</p>

After you finish the settings, click on Apply. The following message will be displayed:

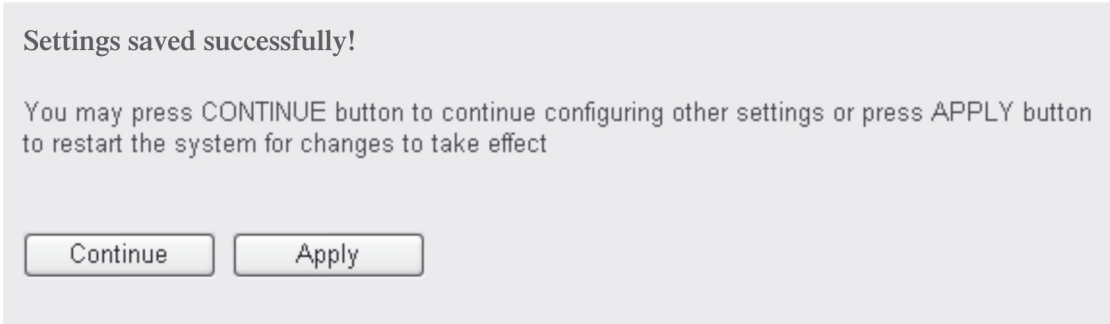


Figure 3-13. Settings saved successfully prompt.

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

Multiple ESSID

This access point supports four SSIDs. Configure the main SSID in the Basic Setting page, then configure another three SSIDs here. With different SSIDs, you can separate the wireless networks with different SSID names, wireless security, WMM, and VLAN settings.

NOTE: If you want to configure the wireless security for a different SSID, go to Section 3.7, Wireless Security.

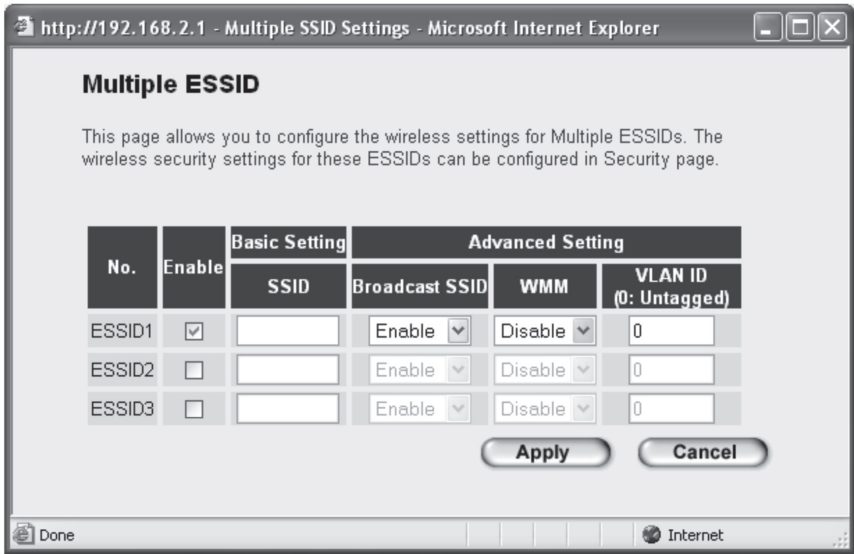


Figure 3-14. Mutliple SSID screen.

Table 3-4. Multiple SSID screen options.

Option	Description
No.	Except for the Main SSID, you can configure an additional three ESSIDs here.
Enable	Select the box to enable the different additional ESSIDs.
SSID	Input the SSID name (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. NOTE: ESSID IS CASE SENSITIVE.
Broadcast SSID	Decide if the wireless access point will broadcast its own ESSID or not. You can hide your wireless access point's ESSID (set the option to Disable), so only people who know the ESSID can connect.
WMM	WMM (Wi-Fi Multimedia) technology improves the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable the WMM function, the access point will define the priority of different kinds of data, and give higher priority to applications that require instant responding. This improves 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, and it disables the VLAN function for the ESSID.

3.4.2 Station-Infrastructure

In this mode, you can connect the access point to an Ethernet device such as a TV and game player to enable the Ethernet device to be a wireless station and join a wireless network through an access point or AP router.

Mode :	Station-Infrastructure
Band :	2.4 GHz (B+G+N) ▼
MAIN ESSID :	default
Site Survey :	Select Site Survey

Figure 3-15. Station infrastructure mode screen.

Table 3-5. Station infrastructure mode settings.

Option	Description
Band	<p>Select the wireless band you wish to use. By selecting a different band setting, you'll be able to allow or deny the wireless client of a certain band.</p> <p>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) can connect to this access point.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band can connect to this access point.</p> <p>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).</p>
Main ESSID	<p>Input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters.</p> <p>NOTE: ESSID IS CASE SENSITIVE.</p>
Site Survey	<p>When you use this access point as a wireless station for an Ethernet network device to have wireless capability, you have to associate it with a working access point. Click on the Select Site Survey button, and a Wireless Site Survey Table will pop up. The table lists all available access points nearby. You can select one access point in the table and it will join the wireless LAN through this access point.</p>

After you finish the settings, click on the Apply button, and the following message will be displayed:

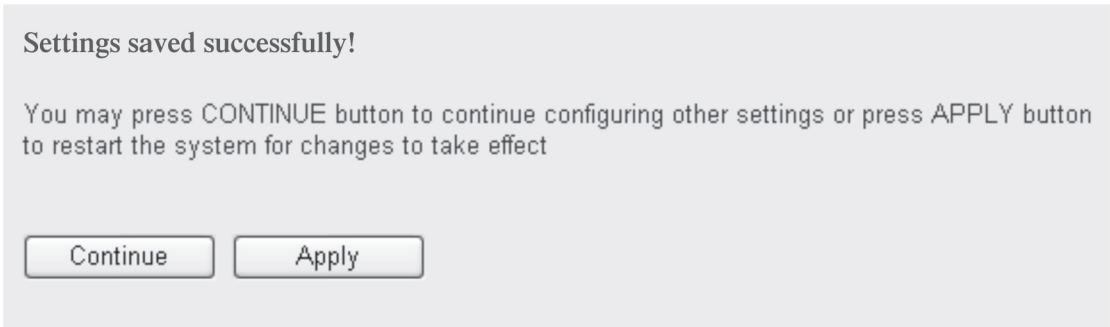


Figure 3-16. Settings saved successfully prompt.

When you see this message, the settings you made are successfully saved. Click on the Continue button to go back to the previous page and continue setting items, or click on the Apply button to restart the wireless access point. The changes will take effect after about 30 seconds.

Wireless Site Survey

The table lists the access points nearby that are set to station mode; select one of these access points to associate.

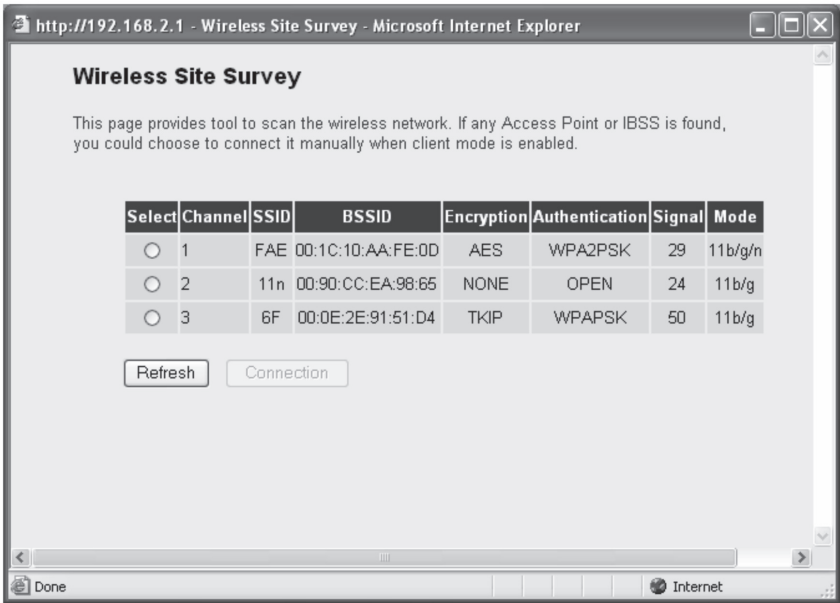


Figure 3-17. Wireless site survey screen.

Table 3-6. Wireless site survey options.

Option	Description
Select	Click on the radio button to select the access point.
Channel	Displays the access point’s channel number.
SSID	Displays the access point’s SSID name.

Table 3-6 (continued). Wireless site survey options.

Option	Description
BSSID	Displays the access point's BSSID (MAC Address).
Encryption	Displays the access point's encryption setting. If you selected the access point with a security setting, go to Section 3.7, Wireless Security, to set the same security for the access point you want to associate.
Authentication	Displays the AP's authentication type.
Signal	Each access point's signal strength displays here. When the signal strength is stronger, the connection quality is better.
Mode	Displays the access point's wireless modes, including 11b, 11b/g, 11b/g/n, or 11n only.
Refresh	Click this button to refresh the table.
Connection	Select an access point and click this button to choose the network. The SSID name of the access point you have selected will be displayed in the Main SSID in the Basic Setting page.

3.4.3 AP Bridge-Point to Point Mode

In this mode, the wireless access point will connect to another wireless access point that 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 that is physically isolated.

NOTE: 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 screen will be displayed:

The screenshot shows a web-based configuration interface for an access point. The 'Mode' dropdown is set to 'AP Bridge-Point to Point'. The 'Band' dropdown is set to '2.4 GHz (B+G+N)'. The 'Channel Number' dropdown is set to '11'. The 'MAC address 1' field contains '000000000000'. There is a 'Set Security' button next to the MAC address field. At the bottom right of the configuration panel are 'Apply' and 'Cancel' buttons.

Figure 3-18 AP Bridge-Point to Point Mode setup screen.

Table 3-7. AP bridge-point to point mode options.

Option	Description
Band	<p>Select the wireless band you want to use. By selecting different band settings, you'll be able to allow or deny the wireless client of a certain band.</p> <p>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.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band will be able to connect to this access point.</p> <p>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).</p>

Table 3-7 (continued). AP bridge-point to point mode options.

Option	Description
Channel Number	Select a channel number you want to use. The channel number must be same as another wireless access point you want to connect.
MAC address	Input the MAC address of the wireless access point you want to connect.
Set Security	Click on this button to select an encryption mode for this wireless link, and a new popup window will appear. Please refer to Section 3.7 for detailed descriptions.

After you finish the settings, click on the Apply button, and the following message will be displayed:

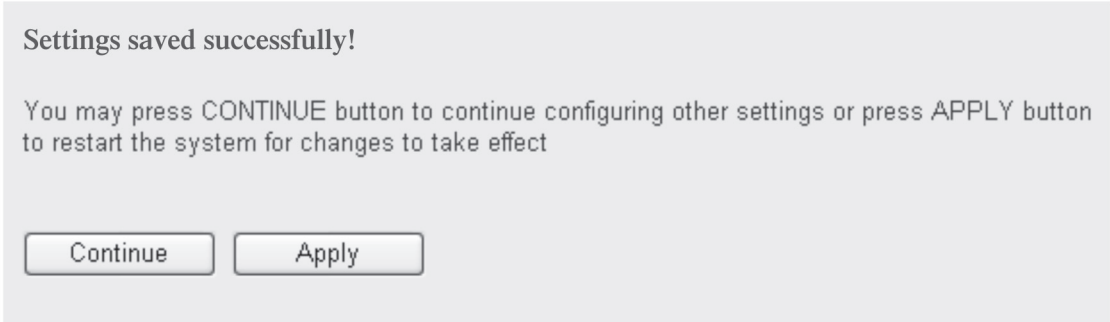


Figure 3-19. Settings saved successfully prompt.

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

3.4.4 AP Bridge-Point to Multi-Point Mode

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

NOTE: 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 screen will be displayed:

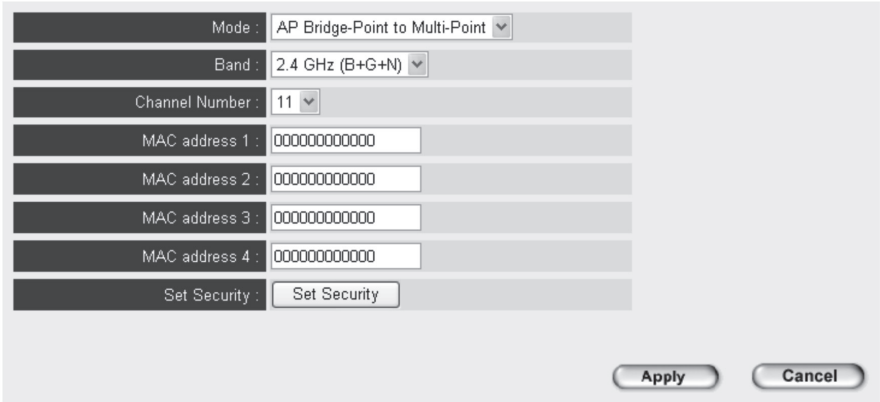


Figure 3-20. AP bridge-point to multi-point mode screen.

Table 3-8. AP bridge-point to multi-point mode options.

Option	Description
Band	<p>Select the wireless band you want to use. Selecting a different band setting will enable the AP to allow or deny the wireless client of a certain band.</p> <p>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.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band will be able to connect to this access point.</p> <p>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).</p>
Channel Number	Select a channel number you want to use. The channel number must be the same as another wireless access point you want to connect.
MAC Address 1-4	Input the MAC address of the wireless access point you want to connect.
Set Security	Click on this button to select an encryption mode for the wireless link, and a new popup window will appear. Refer to Section 3.7 for detailed descriptions.

After you finish the settings, click on Apply, and the following message will be displayed:

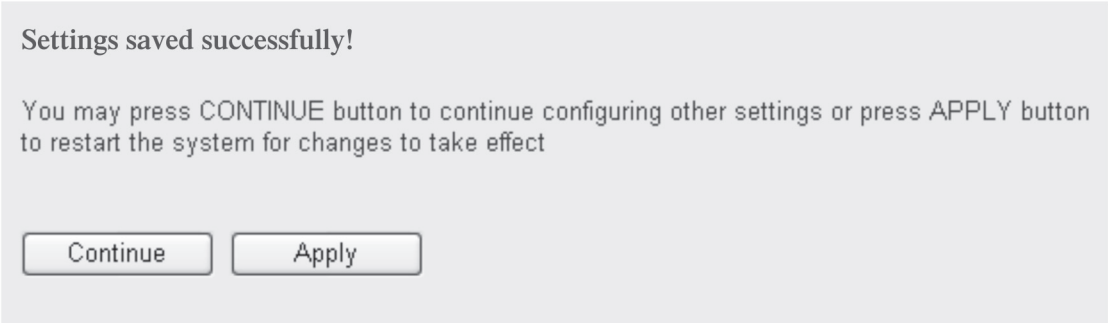


Figure 3-21. Settings saved successfully prompt.

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

3.4.5 AP Bridge-WDS Mode

In this mode, this wireless access point connects to up to four wireless access points that use the same mode, and all wired Ethernet clients of every wireless access point will be connected together. Use this mode to connect a network to other networks that are physically isolated.

When you use this mode, this access point can still accept wireless clients.

When you select AP Bridge-WDS, the following screen will be displayed:

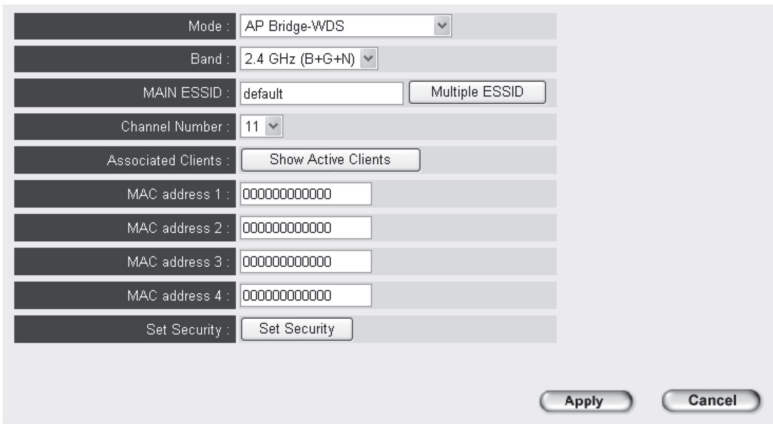


Figure 3-22. AP bridge-WDS mode.

Table 3-9. AP bridge-WDS mode options.

Option	Description
Band	<p>Select the wireless band you want to use. Selecting different band settings will enable you to allow or deny the wireless client of a certain band.</p> <p>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.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band will be able to connect to this access point.</p> <p>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).</p>
MAIN ESSID	<p>Input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters.</p> <p>NOTE: ESSID IS CASE SENSITIVE.</p>
Multiple ESSID	<p>The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, click on this button..</p>
Channel Number	<p>Select a channel number you want to use. The channel number must be the same as another wireless access point you want to connect.</p>
Associated Clients	<p>Click on the Show Active Clients button and a new popup window will appear. It contains the information about all wireless clients connected to this access point. Click on the Refresh button in the popup window to keep information up-to-date.</p>

Table 3-9 (continued). AP bridge WDS mode options.

Option	Description
MAC Address 1-4	Input the MAC address of the wireless access point you want to connect.
Set Security	Click on this button to select an encryption mode for this wireless link, and a new popup window will appear. Refer to Section 3.7 for detailed descriptions.

After you finish the settings, click on the Apply button. The following message will be displayed:

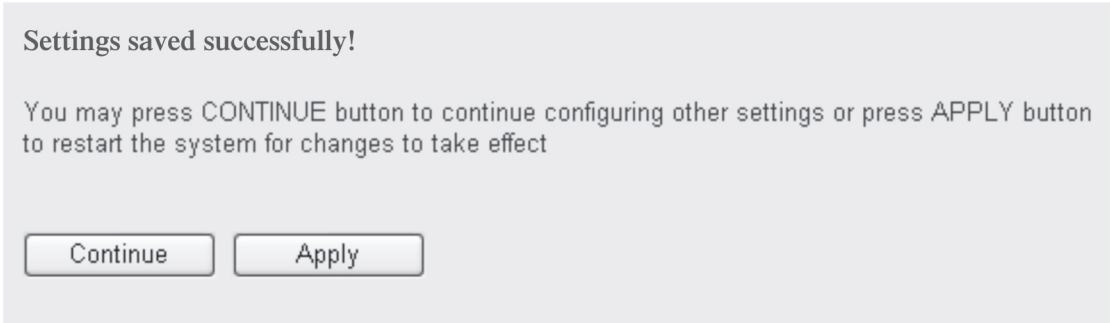


Figure 3-23. Settings saved successfully prompt.

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

3.4.6 Universal Repeater

In this mode, the access point acts as a wireless repeater; it can be configured as station and AP at the same time. It uses the station function to connect to a Root AP and it uses the AP function to service all wireless stations within its coverage.

NOTE: In repeater mode, this access point will demodulate the received signal and check if it is noise for the operating network, then modulate and amplify the signal again. This mode’s output power is the same as that of WDS and normal AP mode.

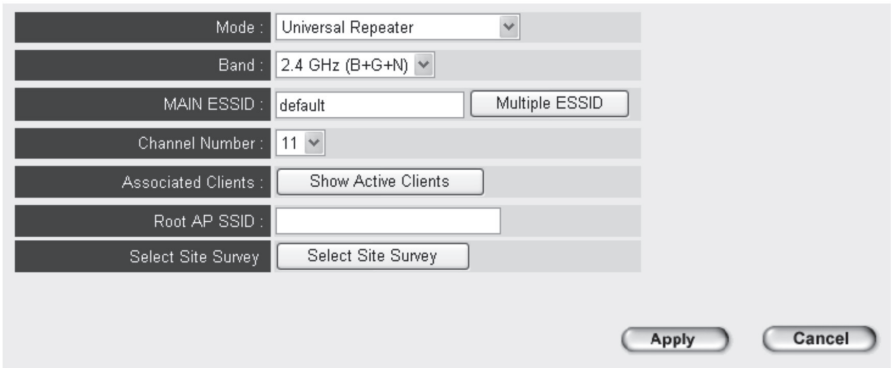


Figure 3-24. Universal repeater screen.

Table 3-10. Universal repeater options.

Option	Description
Band	<p>Select the wireless band you want to use. Selecting different band settings enables you to allow or deny the wireless client of a certain band.</p> <p>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.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g band will be able to connect to this access point.</p> <p>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).</p>
MAIN SSID	<p>Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters</p> <p>NOTE: ESSID IS CASE SENSITIVE.</p>
Multiple ESSID	<p>The access point supports multiple SSID functions; up to four SSIDs can be set. If you want to configure additional SSIDs, click on this button.</p>
Channel Number	<p>Select a channel number you want to use. The channel number must be the same as another wireless access point you want to connect.</p>
Associated Clients	<p>Click on the Show Active Clients button. A new popup window will appear that contains the information about all wireless clients connected to this access point. You can click on the Refresh button in the popup window to keep information up to date.</p>
Root AP SSID	<p>In Universal Repeater mode, this device acts as a station to connect to a root AP. Assign the root AP's SSID here or click on the Select Site Survey button to choose a Root AP.</p>
Select Site Survey	<p>Click on the Select Site Survey button, and a Wireless Site Survey Table pops up. It lists all available access points nearby. Select one access point in the table and the access point will join the wireless LAN through this access point.</p>

After you finish the settings, click on the Apply button, and the following message will be displayed:

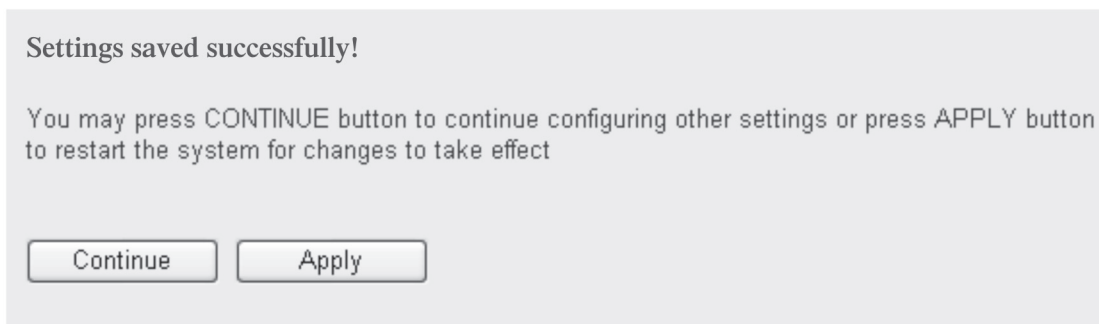


Figure 3-25. Settings saved successfully prompt.

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

3.5 WPS Setting

Wi-Fi Protected Setup (WPS) is the simplest way to connect wireless network clients to this access point. You don't have to select encryption mode and input a long encryption passphrase every time you need to setup a wireless client; just press a button on the wireless client and this access point and the WPS will do the setup for you.

This access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch this access point to WPS mode and push a specific button on the wireless client to start WPS mode. To do this, press the AP's Reset/WPS button, or click on the Start PBC button in the Web configuration interface. If you want to use a PIN code, you have to provide the PIN code of the wireless client you want to connect to this access point and then switch the wireless client to WPS mode. Detailed instructions are listed follow:

To use the WPS function to set an encrypted connection between this access point and the WPS-enabled wireless client by WPS, click on 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:	Configured
Self PinCode:	0
SSID:	default
Authentication Mode:	Disable
Passphrase Key:	

• Device Configure

Config Mode:	Registrar ▼
Configure via Push Button:	Start PBC
Configure via Client PinCode:	<input type="text"/> Start PIN

Figure 3-26. Enable WPS screen.

Table 3-11. Enable WPS options.

Option	Description
Enable WPS	Check this box to enable or disable WPS function.
Wi-Fi Protected Setup Information	<p>All information related to WPS will be displayed here. It's helpful when you're setting up connections by WPS.</p> <p>WPS Status: Displays WPS status. If this access point's data encryption settings have never been set, an unConfigured message will be displayed here. (see Section 3.7 for detailed information). If data encryption settings have been set before, a Configured message will be displayed here.</p> <p>Self PinCode: This is the access point's WPS PIN code. Use it when you need to build wireless connection by WPS with other WPS-enabled wireless devices.</p> <p>SSID: Displays the access point's SSID (ESSID).</p> <p>Authentication Mode: The access point's wireless security authentication mode will be displayed here. If you don't enable the access point's security function before WPS is activated, the access point will auto set the security to WPA (AES) and generate a set of passphrase keys for WPS connection.</p> <p>Passphrase Key: Displays the WPA passphrase. All characters will be replaced by asterisks for security. If encryption is not set on this access point, nothing will be displayed here.</p>
Config Mode	There are Registrar and Enrollee modes for the WPS connection. When Registrar is enabled, the wireless clients will follow the access point's wireless settings for WPS connection. When Enrollee mode is enabled, the access point will follow the wireless settings of wireless client for WPS connection.
Start PBC	Click on the Start PBC button to start Push-Button style WPS setup procedure. This access point will wait for WPS requests from wireless clients for 2 minutes. The WLAN LED on the access point will be steady on for 2 minutes when this access point is waiting for incoming WPS request.
Start PIN	<p>Input the PIN code of the wireless client you want to connect, and click on the Start PIN button. The WLAN LED on the access point will be steady on when this access point is waiting for an incoming WPS request.</p> <p>NOTE: When you're using PBC type WPS setup, press the wireless client's PBC button (hardware or software) within 120 seconds. If you don't press the wireless client's PBC button within this timeframe, press it again.</p>

3.6 Advanced Wireless Settings

This wireless access point has many advanced wireless features.

NOTE: All settings listed here are for experienced users only. If you’re not sure about the meaning and function of these settings, don’t modify them, or the wireless performance will be adversely affected.

Click on Advanced Setting on the left to enter the Advanced Settings screen. The following message will be displayed:

Advanced Settings

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

Fragment Threshold:

2346

(256-2346)

RTS Threshold:

2347

(0-2347)

Beacon Interval:

100

(20- 1024 ms)

DTIM Period:

3

(1-10)

Data Rate:

Auto

N Data Rate:

Auto

Channel Width:

☒ Auto 20/40 MHZ

☐ 20 MHZ

Preamble Type:

☒ Short Preamble

☐ Long Preamble

Broadcast ESSID:

☒ Enable

☐ Disable

WMM:

☐ Enable

☒ Disable

CTS Protect:

☒ Auto

☐ Always

☐ None

TX Power:

100 %

Apply

Cancel

Figure 3-27. Advanced settings screen.

Table 3-12. Advanced Settings screen options.

Option	Description
Fragment Threshold	Sets the wireless radio’s Fragment threshold. Do not modify the default value if you don’t know what it is; the default value is 2346.
RTS Threshold	Sets the wireless radio’s RTS threshold. Do not modify the default value if you don’t know what it is; the default value is 2347.
Beacon Interval	Sets the wireless radio’s beacon interval. Do not modify the default value if you don’t know what it is; the default value is 100.
DTIM Period	Sets the wireless radio’s DTIM period. Do not modify the default value if you don’t know what it is; the default value is 3.
Data Rate	Sets the wireless data transfer rate to a certain value. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically, you don’t need to change this value unless you know what will happen after modification.
N Data Rate	Sets the 802.11 Draft-N clients’ data rate. Available options are MCS 0 to MCS 15. It’s safe to set this option to Auto. Don’t change this value unless you know what will happen after you modify it.

Table 3-12 (continued). Advanced Settings screen options.

Option	Description
Channel Width	Selects the wireless channel width (bandwidth taken by wireless signals of this access point). We suggest setting Auto 20/40MHz. Do not change this to 20 MHz unless you know what it is.
Preamble Type	Sets the wireless radio's preamble type. Do not modify the default value if you don't know what it is; the default setting is Short Preamble.
Broadcast ESSID	Decides if the wireless access point will broadcast its own ESSID or not. You can hide the wireless access point's ESSID (set the option to Disable), so only people who know your wireless access point's ESSID can connect.
WMM	WMM (Wi-Fi Multimedia) technology improves the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable the WMM function, the access point will define the priority of different kinds of data, and give higher priority to applications which require instant responding. This improves 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. We recommend setting this option to Auto.
TX Power	You can set the wireless radio's output power. 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 will not be able to reach your wireless access point).

After you finish the settings, click on the Apply button, and the following message will be displayed:

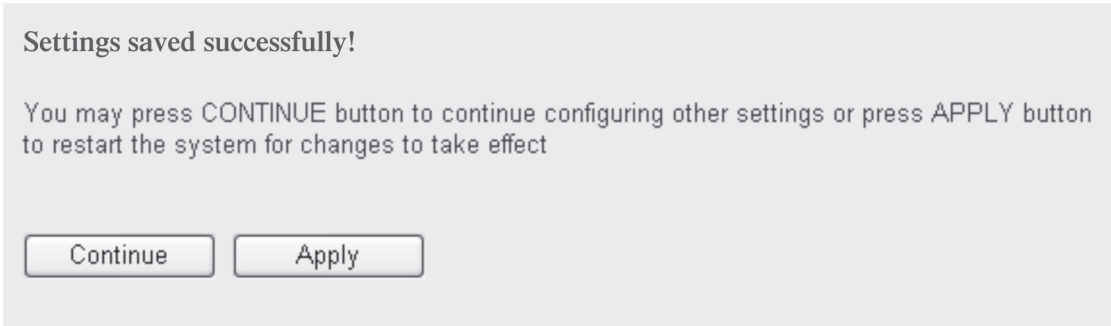


Figure 3-28. Settings saved successfully prompt.

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

3.7 Wireless Security

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 the correct encryption key (encryption password).

There are two ways to set wireless security:

1. Click on Security on the left of the Web management interface.

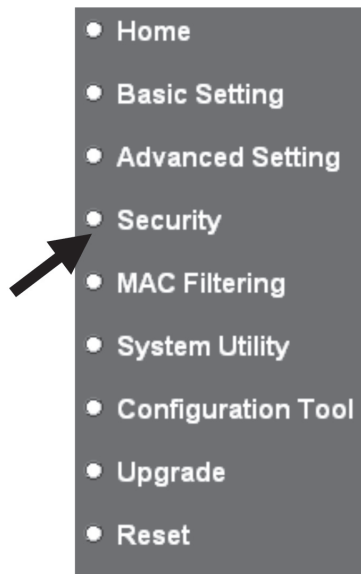


Figure 3-29. Web management interface.

2. Click on the 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.

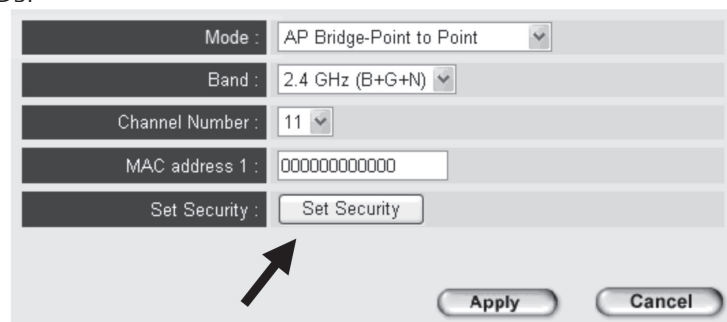


Figure 3-30. AP bridge-point to point screen.

Select from four security levels: disable (no security—data encryption disabled), WEP, WPA pre-shared key, and WPA radius. Refer to the following sections for detailed instructions.

NOTE: If multiple SSIDs are enabled, select the SSID network you want to configure in advance.

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 cause serious problems with your computers and servers.

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 an encryption password. Using a random combination of symbols, numbers, and alphabets will greatly improve security.
3. Use WPA when possible—it's much safer than WEP.
4. Change the encryption password periodically.

3.7.1 Disable Security

Select the SSID you wish to configure. When you select Disable, wireless encryption for the network is disabled.



• Select SSID

SSID choice : default ▼

• Security Settings

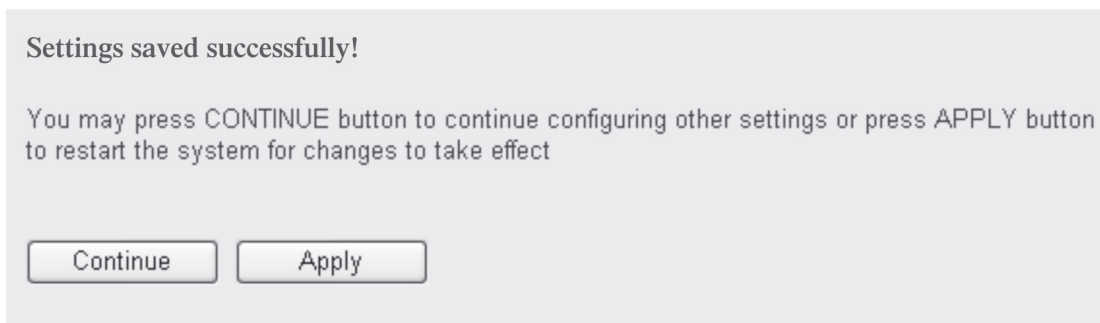
Encryption : Disable ▼

☐ Enable 802.1x Authentication

Apply Cancel

Figure 3-31. Enable/disable security screen.

After you finish the setting, click on the Apply button, and the following message will be displayed:



Settings saved 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

Figure 3-32. Settings saved successfully prompt.

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

3.7.2 WEP

WEP (Wired Equivalent Privacy) is a common encryption mode that’s safe enough for home and personal use. If you need a higher level of security, consider using WPA encryption.

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

When you select WEP as an encryption type, the following screen will be displayed:

The screenshot shows a configuration window for WEP. It contains the following elements:

- Encryption :** A dropdown menu set to "WEP".
- Key Length :** A dropdown menu set to "64-bit".
- Key Format :** A dropdown menu set to "Hex (10 characters)".
- Default Tx Key :** A dropdown menu set to "Key 1".
- Encryption Key 1 :** A text input field containing "sksksksksksksksk".
- Encryption Key 2 :** A text input field containing "sksksksksksksksk".
- Encryption Key 3 :** A text input field containing "sksksksksksksksk".
- Encryption Key 4 :** A text input field containing "sksksksksksksksk".
- Enable 802.1x Authentication :** An unchecked checkbox.
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

Figure 3-33. WEP screen.

Table 3-13. WEP options.

Option	Description
Key Length	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.
Key Format	There are two types of key format: ASCII and Hex. When you select a key format, the number of key characters 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 Format is Hex (10 characters), which means the length of WEP key is 10 characters.
Default Tx Key	You can set up to four WEP keys, 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.
Encryption Key 1 to 4	Input WEP key characters here. The number of characters must be the same as the number displayed in the Key Format field. Use any alphanumerical characters (0-9, a-z, and A-Z) if you select ASCII key format, and use characters 0-9, a-f, and A-F if you select Hex as key format. Enter at least one encryption key here. If you entered multiple WEP keys, they should not be the same as each other.

Table 3-13 (continued). WEP options.

Option	Description
Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. Refer to Section 3.7.5 for detailed instructions.

After you finish the settings, click on the Apply button, and the following message will be displayed:

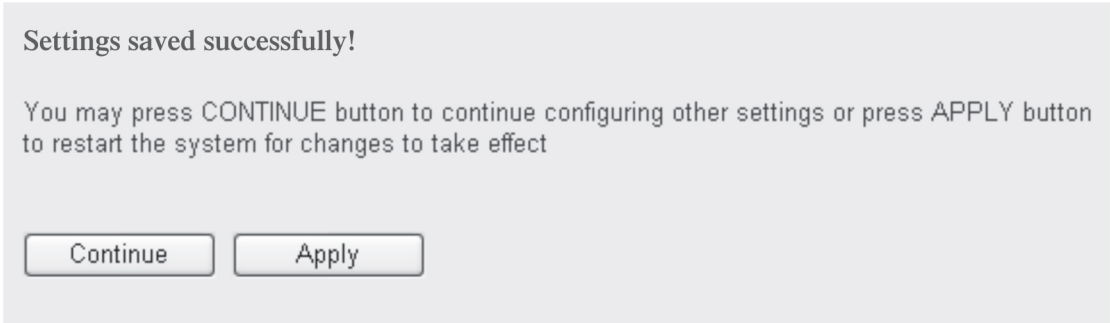


Figure 3-34. Settings saved successfully prompt.

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

3.7.3 WPA Pre-shared Key

WPA Pre-shared key is the safest encryption method. Use it to ensure the safety of your data.

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

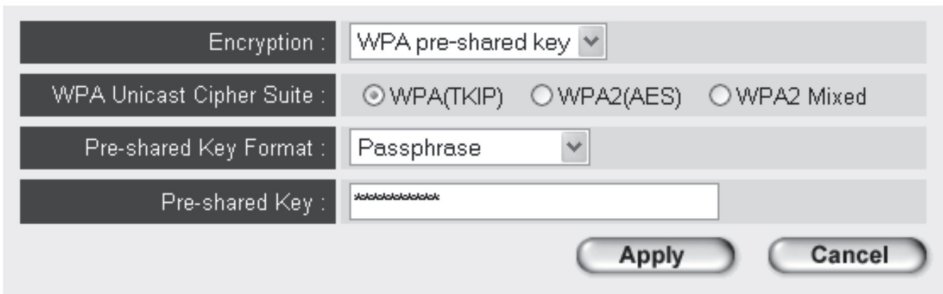


Figure 3-35. WPA pre-shared key screen.

Table 3-14. WPA pre-shared key options.

Option	Description
WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client supports the cipher you selected.
Pre-shared Key Format	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).
Pre-shared Key	Input the pre-shared key according to the key format you selected here. (For security reasons, don't use simple words).

After you finish the settings, click on the Apply button. The following message will be displayed:

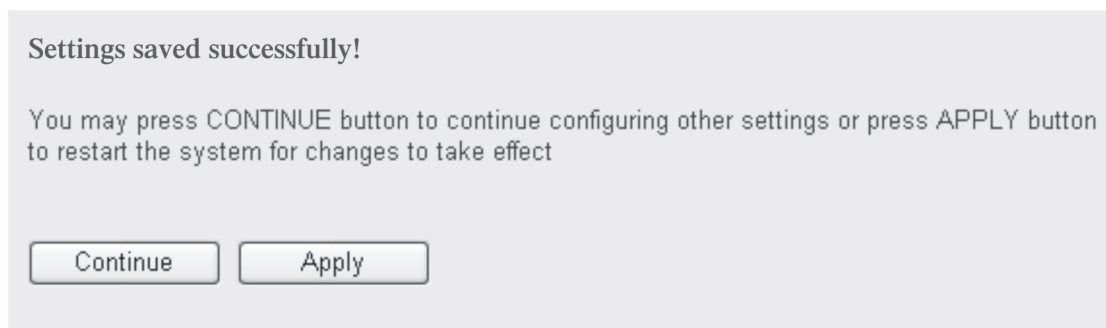


Figure 3-36. Settings saved successfully prompt.

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

3.7.4 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 identity of every wireless client with the user database.

When you select WPA RADIUS as the encryption type, the following screen will be displayed:

The image shows a configuration screen for WPA RADIUS. It has a dark gray header with "Encryption : WPA RADIUS" and a dropdown arrow. Below this, there are three radio buttons for "WPA Unicast Cipher Suite": "WPA(TKIP)" (selected), "WPA2(AES)", and "WPA2 Mixed". There is a checkbox labeled "Use internal MD5/PEAP RADIUS Server" which is currently unchecked. Below the checkbox, there are three input fields: "RADIUS Server IP address" (empty), "RADIUS Server Port" (1812), and "RADIUS Server Password" (empty). At the bottom right, there are two buttons: "Apply" and "Cancel".

Figure 3-37. WPS RADIUS screen.

Table 3-15. WPS RADIUS screen options.

Option	Description
Pre-shared Key	Input a pre-shared key according to the key format you selected here. For security, don't use simple words.
Use internal MD5/PEAP RADIUS Server	Uses a built-in RADIUS Server (refer to Section 3.8) instead of an external RADIUS server. If you check this box, the value in the following three fields will be ignored.
RADIUS Server IP address	Input the RADIUS authentication server's IP address here.
RADIUS Server Port	Input the RADIUS authentication server's port number here. The default value is 1812.
RADIUS Server Password	Input the RADIUS authentication server's password here.

After you finish the settings, click on the Apply button, and the following message will be displayed:

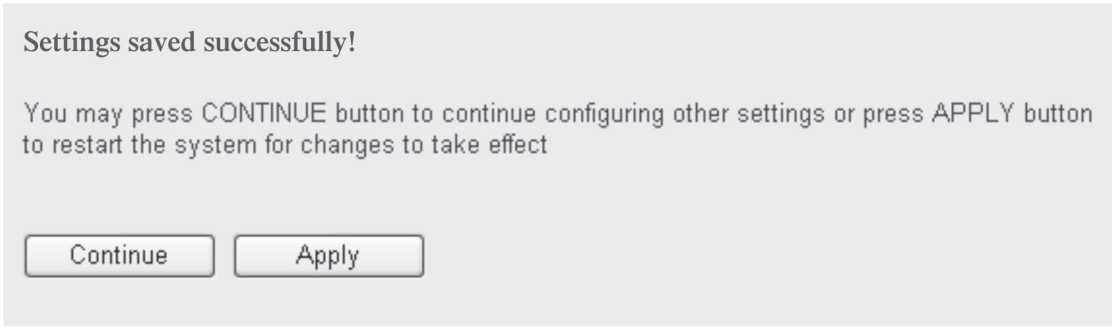


Figure 3-38. Settings saved successfully prompt.

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

3.7.5 802.1x Authentication

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

Select SSID

SSID choice : default

Security Settings

Encryption : Disable

☐ Use internal MD5/PEAP RADIUS Server

☒ Enable 802.1x Authentication

RADIUS Server IP address :

RADIUS Server Port : 1812

RADIUS Server Password :

Apply

Cancel

Figure 3-39. 802.1x screen.

Table 3-16. 802.1x options.

Option	Description
Select SSID	Choose the SSID you want to configure.
Use internal MD5/PEAP RADIUS Server	Uses a built-in RADIUS Server (refer to the next section) instead of an external RADIUS server. If you check this box, the value of the internal RADIUS server fields will be ignored.
Enable 802.1x Authentication	Enable or disable 802.1x user authentication.
RADIUS Server IP address	Input the RADIUS authentication server’s IP address here.
RADIUS Server Port	Input the RADIUS authentication server’s port number here. The default value is 1812.
RADIUS Server Password	Input the RADIUS authentication server’s password here.

After you finish the settings, click on the Apply button, and the following message will be displayed:

Settings saved 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

Figure 3-40. Settings saved successfully prompt.

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

3.8 Radius Server

Compared to other wireless security measures, a radius server provides user-based authentication. If your wireless client supports 802.1x user authentication, you can use the Radius Server function to enable 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 users and/or IP addresses you need is more than this, use the external radius server.

To set up the internal radius server, click Radius Server on the left of the 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"/>

Figure 3-41. Radius server screen.

Table 3-17. Radius server options.

Option	Description
Enable Radius Server	Check this box to enable internal radius server function.
User Profile	<p>You can add or delete a radius user here. Input the username and password, then re-type the password in the corresponding field, and click on the Add button to add the user to the radius server database. Click on Reset to clear the text you typed in above three fields.</p> <p>All current radius users will be listed here. If you want to delete one or more users, check the user's Select box, and click on the Delete Selected button. Click on the Delete All button to delete all users in the radius server database. You can also click on the Reset button to uncheck all Select boxes.</p>

Table 3-17 (continued). Radius server options.

Option	Description
Authentication Client	<p>Add an allowed radius client IP address here. Input client IP, secret key, then re-type the secret key in the corresponding field, and click on the Add button to add the IP address to the radius server database. Click on the Reset button to clear the text you typed in the above three fields.</p> <p>All current IP addresses will be listed here. If you want to delete one or more addresses, check the Select box for that address, and click on the Delete Selected button. Click on the Delete All button to delete all addresses in the radius server database. Click on the Reset button to uncheck all Select boxes.</p>

After you finish the settings, click on the Apply button, and the following message will be displayed:

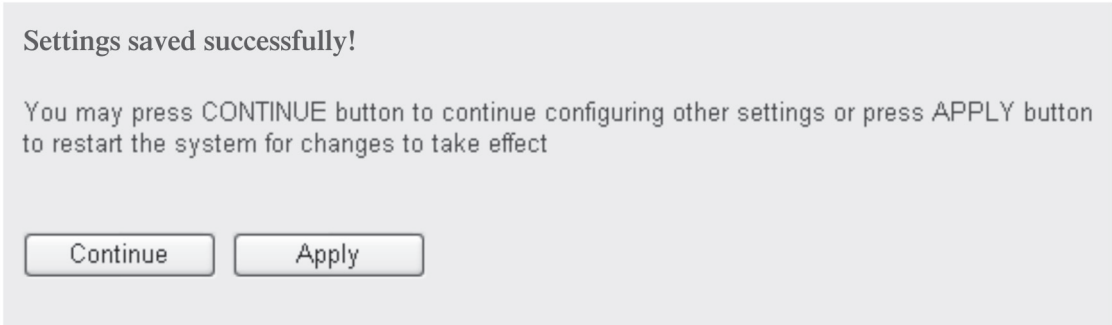


Figure 3-42. Settings saved successfully prompt.

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

3.9 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” that contains MAC addresses for the wireless clients you trust. All other wireless clients with a MAC address that is not in your list will be denied access by the wireless access point.

To set up MAC filtering, click MAC Filtering on the left of the Web management interface and the following screen will be displayed:

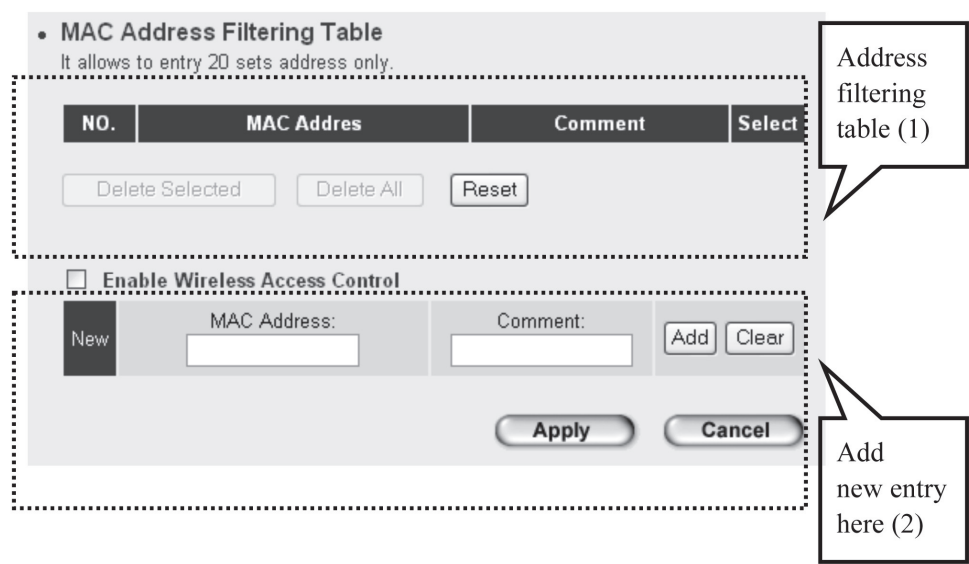


Figure 3-43. MAC address filtering table screen.

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

Table 3-18. MAC address filtering table options.

Option	Description
Select	Check this box to select one or more MAC address(es) to delete.
Delete Selected	Click on this button to delete all selected MAC address(es).
Delete All	Delete all MAC address entries.
Reset	Uncheck all selected MAC address entries.
Enable Wireless Access Control	Check this box to enable MAC address restriction. If unchecked, no restriction will be enforced (any wireless client with the proper encryption setting will be able to connect to this wireless access point).
MAC Address	Input the MAC address allowed using this wireless access point here. You don't have to add a colon (:) or a hyphen (-), just input 0 to 9 and a to f, for example, 112233445566 or aabbccddeeff.
Comment	Input any text here as comments for this MAC address, such as ROOM 2A Computer. You can input up to 16 alphanumerical characters. This is optional and you can leave it blank, however, we recommend using this field to write a comment for every MAC addresses as a memory aid.
Add	When you finish inputting the MAC address and (optional) comment, click on this button to add the MAC address to the list.
Clear	Remove all characters in the MAC address and Comments field.

After you finish the settings, click on the Apply button. The following message will be displayed:

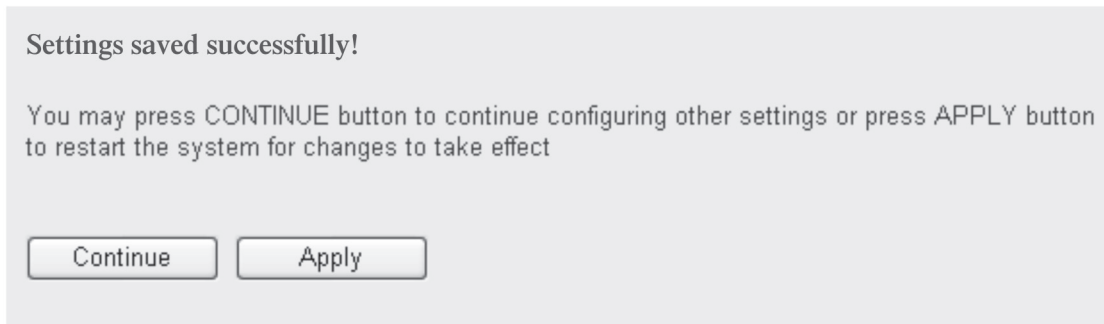


Figure 3-44. Settings saved successfully prompt.

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

3.10 System Utilities

This access point provides some control functions including password, IP address management, and DHCP server functions. Click System Utility on the left of the Web management interface to access these functions. Below are detailed descriptions of every control function.

3.10.1 Change Password

You can change the password used to enter the Web configuration menu for this wireless access point.

Click System Utility on the left, and the following screen will be displayed:

A web interface titled "• Password Settings". It contains three rows of input fields. The first row is labeled "Current Password :", the second "New Password :", and the third "Re-Enter Password :". Each label is in a dark gray box, and each has a corresponding white text input field to its right.

Figure 3-45. Password settings screen.

11N 2T2R Wireless Access Point

Input the current password in Current Password field, then input a new password in both the New Password and the Re-Enter Password field. After you finish, go to the bottom of this page and click on the Apply button. The following message will be displayed:

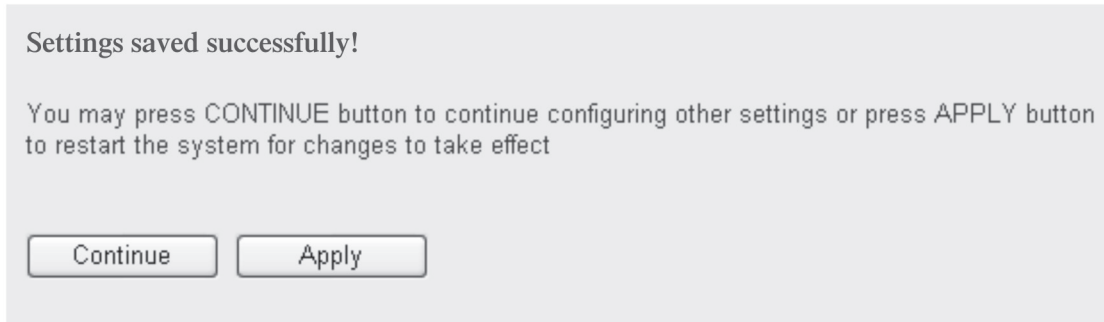


Figure 3-46. Settings saved successfully prompt.

When you see this message, the settings you made are successfully saved. Click on the Continue button to go back to the previous page and continue setting other items. Click on the Apply button to restart the wireless access point. The changes will take effect after about 30 seconds.

3.10.2 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. Remember this address or you will not be able to connect to this wireless access point's configuration menu.

The default IP address is: 192.168.2.1/subnet mask 255.255.255.0. Press and hold the Reset/WPS button for more than 10 seconds to change the IP address back to the default value if you forget the IP address you set.

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


A screenshot of the "Management IP" configuration screen. It has a title "• Management IP". Below the title are four rows of configuration fields: "IP Address" with value "192.168.2.1", "Subnet Mask" with value "255.255.255.0", "Gateway Address" with value "0.0.0.0", and "DHCP Server" with a dropdown menu set to "Disabled".

Figure 3-47. Management IP screen.

Input the IP address and the Subnet Mask in the corresponding fields. To manage this wireless access point from another network (such as the Internet), input the IP address of the gateway in Gateway Address field.

To activate the wireless access point's DHCP server, select Enabled in the DHCP Server option, and see Section 3.10.3 for detailed instructions. If you don't want to use the wireless access point's DHCP server function, or if there's another DHCP server on the network that this access point connects to, select Disable.

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

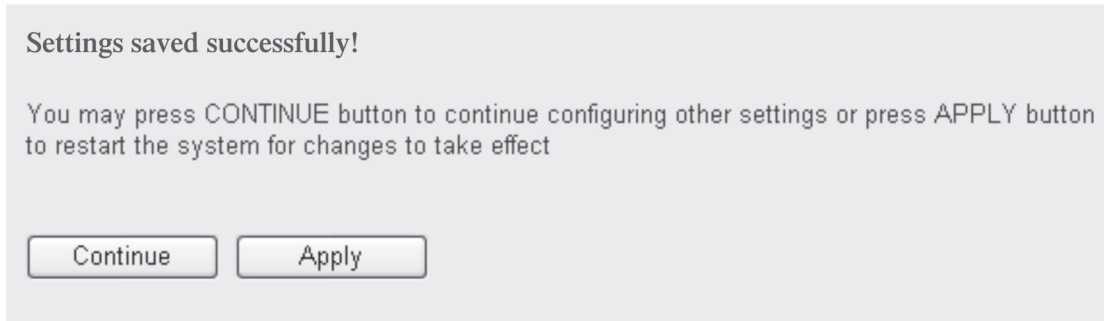
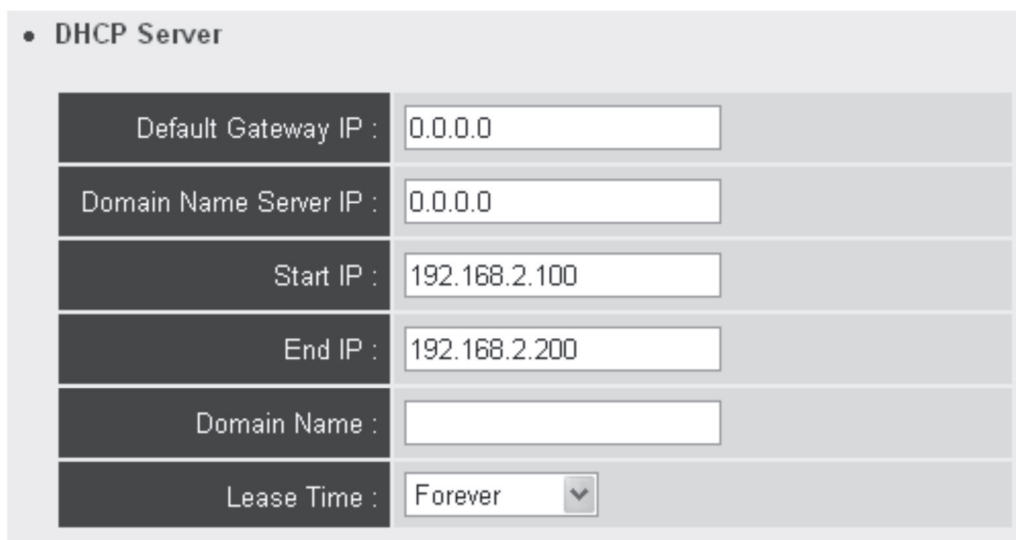


Figure 3-48. Settings saved successfully prompt.

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

3.10.3 DHCP Server

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

A screenshot of the DHCP Server configuration screen. It has a title "• DHCP Server". Below the title, there are six rows of configuration fields. Each row has a label on the left and a text input field on the right. The fields are: "Default Gateway IP" with value "0.0.0.0", "Domain Name Server IP" with value "0.0.0.0", "Start IP" with value "192.168.2.100", "End IP" with value "192.168.2.200", "Domain Name" which is empty, and "Lease Time" with a dropdown menu showing "Forever".

Label	Value
Default Gateway IP :	0.0.0.0
Domain Name Server IP :	0.0.0.0
Start IP :	192.168.2.100
End IP :	192.168.2.200
Domain Name :	
Lease Time :	Forever

Figure 3-49. DHCP server screen.

NOTE: Remember to select Enable in the DHCP Server option as described in Section 3.10.2, or all DHCP related fields will be grayed out, and you will not be able to input any DHCP parameters.

Table 3-19. DHCP server screen options.

Option	Description
Default Gateway IP	Input the network’s default gateway IP address.
Domain Name Server IP	Input the domain name server’s (DNS) IP address here.
Start IP	Input the start IP address of the IP range.
End IP	Input the end IP address of the IP range.
Domain Name	Input the domain name for your network. This is optional.
Lease Time	Choose a lease time (how long every computer can keep a specific IP address) for every IP address assigned by this access point from the drop-down menu.

After you finish, click on the Apply button, and the following message will be displayed:

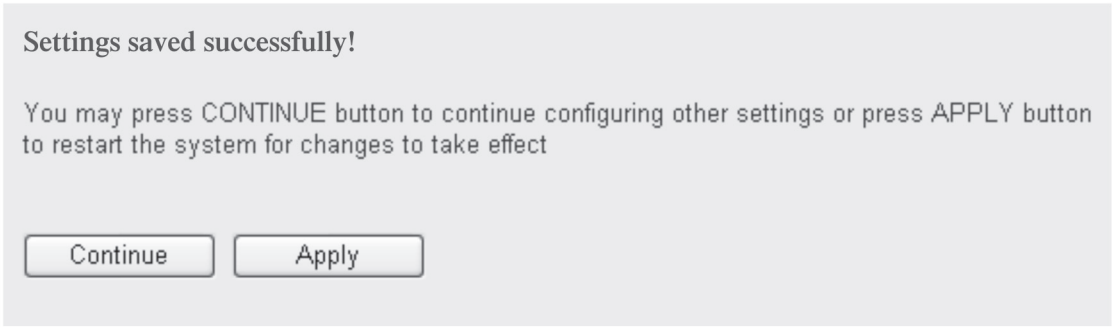


Figure 3-50. Settings saved successfully prompt.

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

4. Advanced Configuration

4.1 Configuration Backup and Restore

Backup all configurations of this access point to a file, so you can make several copies of the access point configuration for security reasons.

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

Click on the Configuration Tool on the left of the Web management interface, and the following screen will be displayed on your web browser:



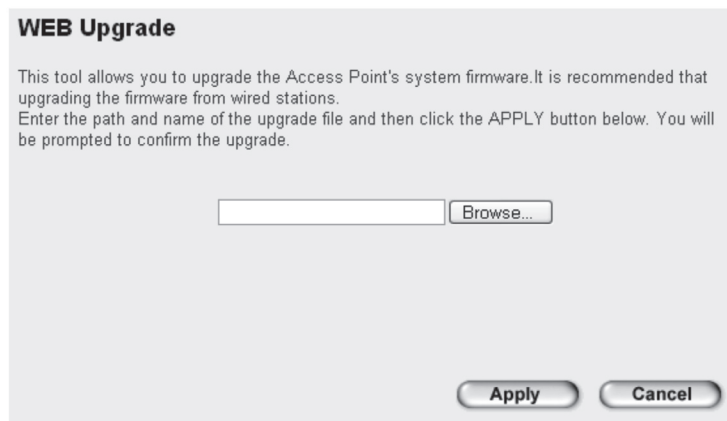
Figure 4-1. Backup or restore the access point’s configuration screen.

Table 4-1. Backup or restore the access point’s configuration options.

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

4.2 Firmware Upgrade

To upload the most recent firmware to the access point, click Upgrade on the left of the Web management interface, and the following screen 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.

Figure 4-2. Web upgrade screen.

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

After you select a firmware upgrade file, click on the Apply button, and the access point will start to upgrade the firmware automatically. The procedure may take several minutes.

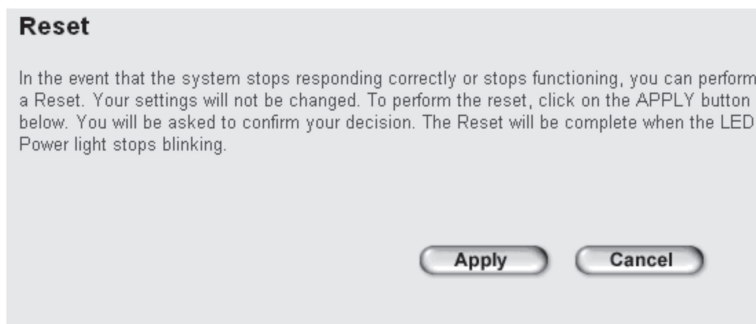
NOTE: Never interrupt the upgrade procedure by closing the Web browser or physically disconnecting your computer from the access point, since this could corrupt the firmware. If the firmware you uploaded is corrupt, the firmware upgrade will fail.

4.3 System Reset

If the access point is not working properly, use this function to restart the access point; this may help 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 in after 10 seconds.

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



Reset

In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.

Figure 4-3. System reset screen.

Click on the Apply button, and a popup message will ask you again, to make sure you really want to reset the access point:

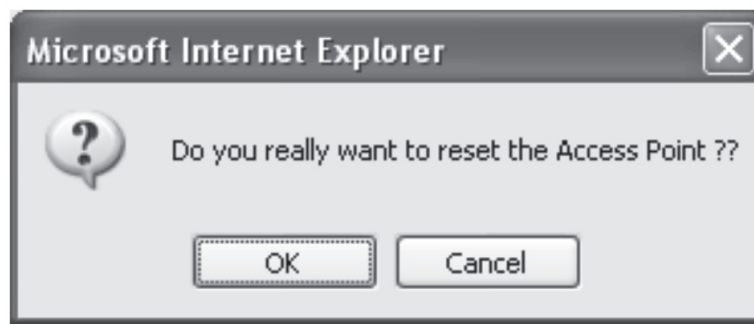


Figure 4-4. Confirm reset screen.

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

Appendix A. Troubleshooting

A.1 Problem/Solutions

If the access point is working improperly, read this section. If you still need help, contact Black Box Technical Support at 724-746-5500.

Problem: The access point is not responding to me when I want to access it by Web browser.

Possible Solution #1: Please check the access point's power cord and network cable connections. All cords and cables should be correctly and firmly inserted into the access point.

Possible Solution #2: If all LEDs on this access point are out, check the status of the A/C power adapter, and make sure it's correctly powered.

Possible Solution #3: You must use the same IP address section that the access point uses.

Possible Solution #4: Are you using a MAC or IP address filter? Try to connect the access point to another computer and see if it works; if not, press the reset button.

Possible Solution #5: Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address.

Possible Solution #6: If you upgraded the firmware and this happens, contact Black Box Technical Support.

Possible Solution #7: If all of the above solutions don't work, contact Black Box Technical Support at 724-746-5500.

Problem: I can't get connected to the wireless access point.

Solution #1: If encryption is enabled, please re-check the WEP or WPA passphrase settings on your wireless client.

Solution #2: Move closer to the wireless access point.

Solution #3: Unplug the access point's power plug, then plug it back in again after 10 seconds.

Solution #4: If all LEDs on this access point are out, check the the A/C power adapter's status, and make sure it's correctly powered.

Problem: I can't locate my access point via my wireless client.

Solution #1: Is the Broadcast ESSID set to off?

Solution #2: Is the antenna properly installed and secured?

Solution #3: Are you too far from your access point? Move closer.

Solutoin #4: Remember that you have to input ESSID on your wireless client manually if ESSID broadcast is disabled.

Problem: File download is very slow or breaks frequently.

Solution #1: Reset the access point and see if it improves.

Solution #2: Know what computers do on your local network. If someone's transferring big files, other people will think the Internet is too slow.

Solution #3: Change the channel number.

Problem: I can't log onto the Web management interface; the password is wrong.

Solution #1: Make sure you're connecting to the access point's correct IP address.

Solution #2: The password is case-sensitive. Make sure the Caps Lock light is not lit.

Solution #3: If you forget the password, do a hard reset (press the reset button).

Problem: Access point becomes hot.

Solution #1: This is not a malfunction if you can keep your hand on the access point's case.

Solution #2: If you smell something wrong or see smoke coming out from the access point or A/C power adapter, disconnect the access point and A/C power adapter from utility power (make sure it's safe before doing this!), and call Black Box Technical Support.

A.2 Calling Black Box

If you determine that your 11N 2T2R Access Point is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box Technical Support at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

2.3 Shipping and Packaging

If you need to transport or ship your 11N 2T2R Access Point:

- Package it carefully. We recommend that you use the original container.
- If you are returning the unit, make sure you include everything you received with it. Before you ship for return or repair, contact Black Box to get a Return Authorization (RA) number.

Appendix B. 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.Broadbandaccesspoint.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 "`Broadbandaccesspoint.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 on the Internet for a pre-configured amount of time, the connection will automatically disconnect.

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: An 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.