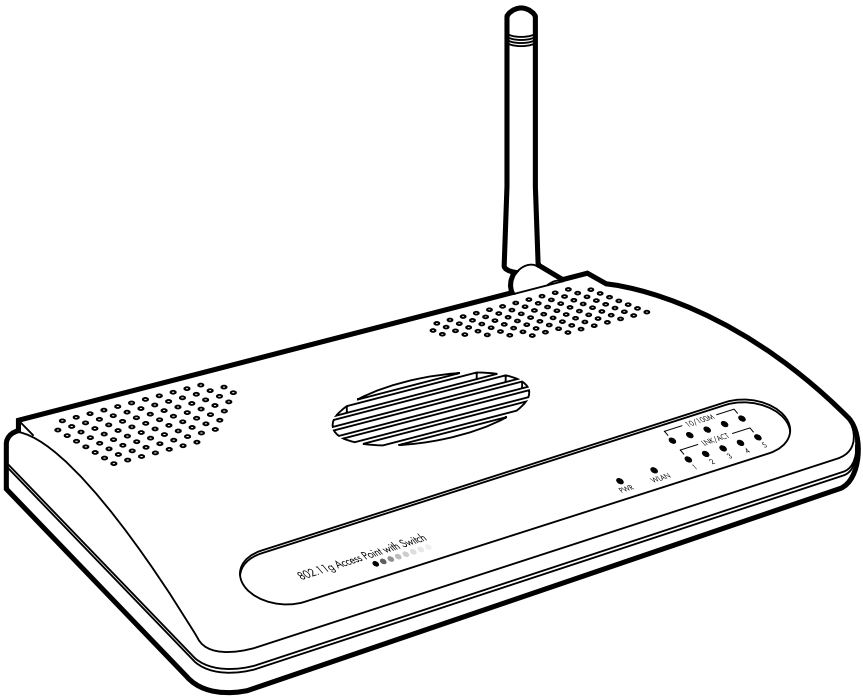
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

DECEMBER 2004
LW6004A
LW6004A-EU
LW6004A-UK

Pure Networking 802.11g Wireless Access Point with Switch



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**

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.

EUROPEAN UNION DECLARATION OF CONFORMITY

This equipment complies with the requirements of the European EMC Directive 89/336/EEC.

CE

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

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 a 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 deber 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 connectado 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 fisica 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 lineas de energia.

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 objectos liquidos 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: Objectos 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.

TRADEMARKS USED IN THIS MANUAL

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

Contents

Chapter **Page**

1. Specifications

Antenna: (1) RP-SMA detachable

CPU: ADMtek 5120 175-MHz MIPS R400

Distance (Maximum): 328 ft. (100 m)

Memory: 2 MB Flash, 8 MB DRAM

Operating System: Compatible with all major operating systems; Drivers included for Windows® 98 SE/Me/XP, Windows NT®, Windows 2000, and Linux®

Speed: Wireless: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps with auto fallback; Ethernet: 10/100 Mbps, autosensing

Standards: IEEE 802.11b, 802.11g, IEEE 802.3, IEEE 802.3u

Security: 64-, 128-, 152-bit WEP Data Encryption

Frequency Band: 2.400–2.4835 GHz

Radio Technology: Direct Sequence Spread Spectrum (DSSS)

Connectors: (5) RJ-45 LAN, (1) RP-SMA

Indicators: (12) LEDs: (1) Power, (1) WLAN, (5) LAN, (5) 10/100

Temperature Tolerance: *Operating:* 32 to 131°F (0 to 55°C);
Storage: -4 to +158°F (-20 to +70°C)

Humidity: Up to 90%, noncondensing

Size: 1.2"H x 5"W x 3.6"D (3 x 12.7 x 9.1 cm)

2. Introduction

2.1 Overview

The Pure Networking 802.11g Wireless Access Point with Switch is an access point for an IEEE 802.11g/b 2.4-GHz wireless network. Any wireless LAN station can join the wireless network by using the infrastructure mode. The access point supports 54-, 11-, 5.5-, 2-, and 1-Mbps network speeds. It automatically falls back to a slower speed in case of obstacles or interference. Also included is an internal 5-port Fast Ethernet switch for wired Ethernet connection.

The access point supports Web-based configuration. It has a built-in DHCP server to allow multiple wireless and wired users to get their IP address automatically. These versatile features allow you to integrate your wireless and wired Ethernet LAN network seamlessly.

With the access point's ESSID authentication, 64-/128-/152-bit WEP encryption, and MAC address filtering, you can prevent unauthorized wireless stations from accessing your wireless network.

Attach the access point's dipole antenna to an RP-SMA connector. Install a high-gain antenna for better network link quality so that you can build a wireless network with more flexibility.

2.2 What's Included

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

- (1) Pure Networking 802.11g Wireless Access Point with Switch
- (1) 2.2-dBm dipole antenna
- (1) power adapter
- (1) CD-ROM containing this users' manual in PDF format

2.3 Physical Description

2.3.1 Front Panel

The front panel contains LED indicators that tell you the access point's current status. Numbers 1–4 in Figure 2-1 correspond to numbers 1–4 in Table 2-1.

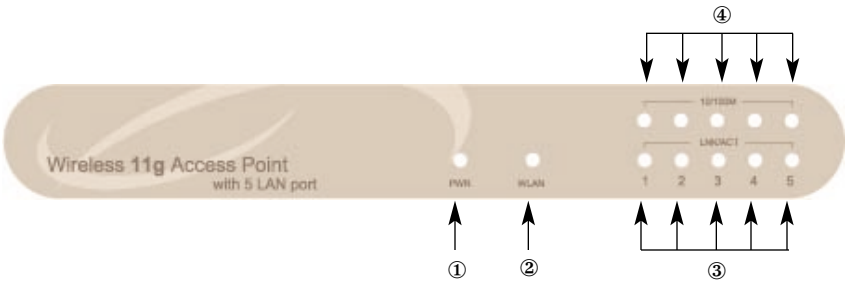


Figure 2-1. Front panel.

Table 2-1. Indicators.

LED	Color	Status	Description
① Power	Green	Lit	Power is supplied.
		Off	No power.
② Wireless Activity	Green	Flash	The antenna is transmitting or receiving data.
		Off	The antenna is not transmitting or receiving data.
③ LAN Link/Activity	Green	On	A valid link is established.
		Flash	The access point is transmitting or receiving data.
		Off	No link is established.

Table 2-1 (continued). Indicators.

LED	Color	Status	Description
④10/100 Mbps	Green	On	Network speed is 100 Mbps.
		Off	Network speed is 10 Mbps.

2.3.2 Back Panel

The access point's connection ports are located on the back panel (see Figure 2-2). Numbers 1–4 in Figure 2-2 correspond to numbers 1–4 in Table 2-2.

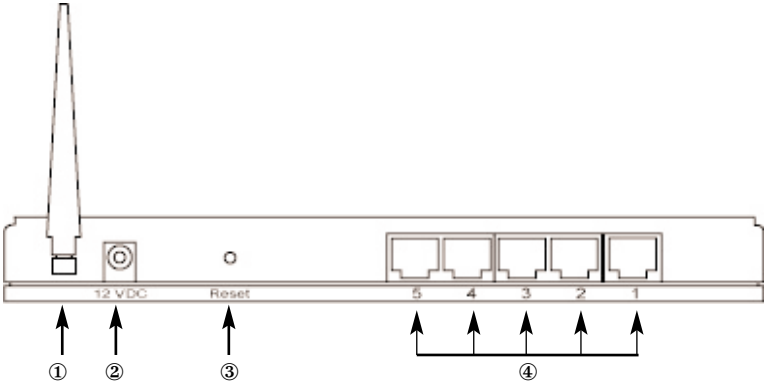


Figure 2-2. Back panel.

Table 2-2. Connection ports.

Connector or Port	Description
① Antenna Connector	This round connector is a standard reverse SMA connector. Any antenna with a reverse SMA connector can connect to the access point.
② Power Adapter Port	Insert the power adapter's power jack into this port.
③ Reset	The reset button allows you to do one of two things: 1. If problems occur with your access point, press the reset button with a pencil tip (for less than 4 seconds). The access point will reboot itself, keeping your original configurations. 2. If problems persist, you experience extreme problems, or you forgot your password, press the reset button for longer than four seconds. The access point will reset itself to the factory default settings.
④ LAN Port	The access point's LAN ports are where you connect to your LAN's network devices.

WARNING

If you press the reset button for longer than four seconds, your original configurations will be replaced with the factory-default settings.

3. Installation

1. Decide where to place the Pure Networking 802.11g Wireless Access Point with Switch. The best access point location is usually at the center of your wireless network with line-of-sight to all of your mobile stations.

2. Connect the access point to your router, hub, or switch. Attach one end of standard UTP cable to the access point's LAN port and connect the other end of the cable to a switch, a router, or a hub. The access point will then be connected to your existing wired LAN network.

3. Connect the power adapter to the access point's power socket. Use only the access point's included power adapter. Using a different adapter may damage the access point.

The hardware installation is complete.

4. Configuration Utility

4.1 Getting Started

This access point provides a Web-based configuration tool, allowing you to configure it from wired or wireless stations. Follow the instructions below.

From a wired station:

1. Make sure your wired station is in the access point's subnet.

   The access point's default IP address and subnet mask:

   Default IP address: 192.168.2.1

   Default subnet: 255.255.255.0

2. Configure your PC to be in the access point's subnet.

   2a. Windows 95/98/Me

   1. Click on the **Start** button and select **Settings**, then click on **Control Panel**. The Control Panel window will appear.

   2. Double-click on the **Network** icon. The Network window will appear.

   3. Check the Network Components list. If TCP/IP is not installed, click on the **Add** button to install it now. If TCP/IP is installed, go to step 6.

   4. In the Network Component Type dialog box, select **Protocol** and click on the **Add** button.

   5. In the **Select Network Protocol** dialog box, select **Microsoft**® and **TCP/IP**, then click on the **OK** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

   6. After installing TCP/IP, go back to the Network dialog box. Select **TCP/IP** from the list of network components and then click on the **Properties** button.

7. Check each of the tabs and verify the following settings:

   - Bindings: Check **Client** for Microsoft networks and **File and Printer Sharing** for Microsoft networks.
   - Gateway: All fields are blank.
   - DNS Configuration: Select **Disable DNS**.
   - WINS Configuration: Select **Disable WINS Resolution**.
   - IP Address: Select **Specify an IP Address**. Specify the IP address and subnet mask.

     IP Address: 192.168.2.3 (any IP address within 192.168.2.2–192.168.2.254 is available, do not set up 192.168.2.1)

     Subnet Mask: 255.255.255.0

8. Reboot the PC. It will now have the IP address you specified.

2b. Windows 2000

1. Click on the **Start** button and select **Settings**, then click on **Control Panel**. The Control Panel window will appear.
2. Double-click on the **Network and Dial-up Connections** icon. In the Network and Dial-up Connection window, double-click on the **Local Area Connection** icon. The Local Area Connection window will appear.
3. In the Local Area Connection window, click on the **Properties** button.
4. Check the Network Components list. You should see **Internet Protocol [TCP/IP]** on your list. Select it, then click on the **Properties** button.
5. In the Internet Protocol (TCP/IP) Properties window, select **Use the following IP address** and specify the IP address and subnet mask as follows:

   IP Address: 192.168.2.3 (any IP address within 192.168.2.2–192.168.2.254 is available, do not set up 192.168.2.1)

   Subnet Mask: 255.255.255.0

6. Click on **OK** to confirm the setting. Your PC will now have the IP address you specified.

2c. Windows NT

1. Click on the **Start** button and select **Settings**, then click on **Control Panel.** The Control Panel window will appear.

2. Double-click on the **Network** icon. The Network window will appear. Select the **Protocol** tab from the Network window.

3. Make sure the **TCP/IP Protocol** is on the Network Protocols list. If TCP/IP is not installed, click on the **Add** button to install it now. If TCP/IP is installed, go to step 5.

4. In the Select Network Protocol window, select **TCP/IP Protocol** and click on the **OK** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

5. After you install TCP/IP, go back to the Network window. Select **TCP/IP** from the list of network protocols, then click on the **Properties** button.

6. Check each of the tabs and verify the following settings:

   - IP Address: In the Specify an IP address window, type in the IP address and subnet mask as follows.

     IP Address: 192.168.2.3 (any IP address within 192.168.2.2–192.168.2.254 is available, do not set up 192.168.2.1)

     Subnet Mask: 255.255.255.0

   - DNS: Leave all fields blank.

   - WINS: Leave all fields blank.

   - Routing: Leave all fields blank.

7. Click on **OK** to confirm the setting. Your PC will now have the IP address you specified.

3. Enter `192.168.2.1` from the Web browser to get into the access point's configuration tool.

4. A screen (see Figure 4-1) will pop up and request that you enter the user name and password. The default user name and password are as follows.

   User Name: admin

   Password: 1234

   Enter the default user name and password, then click on the **OK** button. See Figure 4-1.

5. You can start configuring the access point.

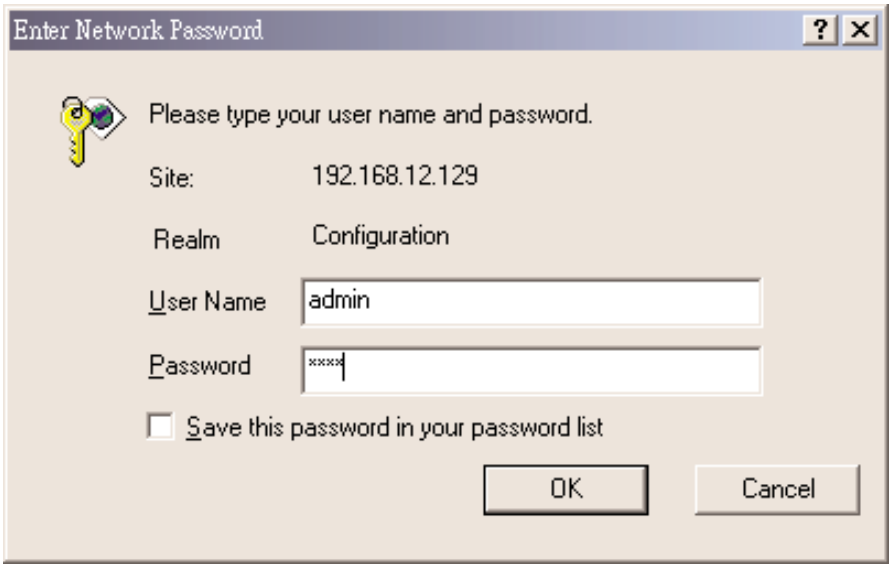


Figure 4-1. Enter Network Password screen.

From a wireless station:

1. Make sure your wireless station is in the access point's subnet. Refer to step 1 at the beginning of **Section 4.1** for configuring the wireless station's IP address and sub mask.

2. Connect to the access point. The access point's ESSID is "default" and the WEP encryption function is disabled. Make sure your wireless station is using the access point's ESSID and associate your wireless station to the access point.

3. Enter `192.168.2.1` from the Web browser to get into the access point's configuration tool.

4. Enter the user name and password, then click on the **OK** button. The Status and Information screen (see Figure 4-2) appears. You can now configure the access point from this screen.

4.2 Menu Options

The screen shown in Figure 4-2 lists menu options vertically on the left-hand side. To get to this screen, enter the user name and password in the Enter Network Password screen (see Figure 4-1), then click on the **OK** button. These menu options (described in **Sections 4.2.2** through **4.2.9**) enable you to set the access point's functions. You don't have to set the functions in the order they are presented here. Just choose the menu option you want to set and go to the corresponding numbered section.

4.2.1 Status and Information

On this screen (see Figure 4-2 and Table 4-1), you can see the general access point information.

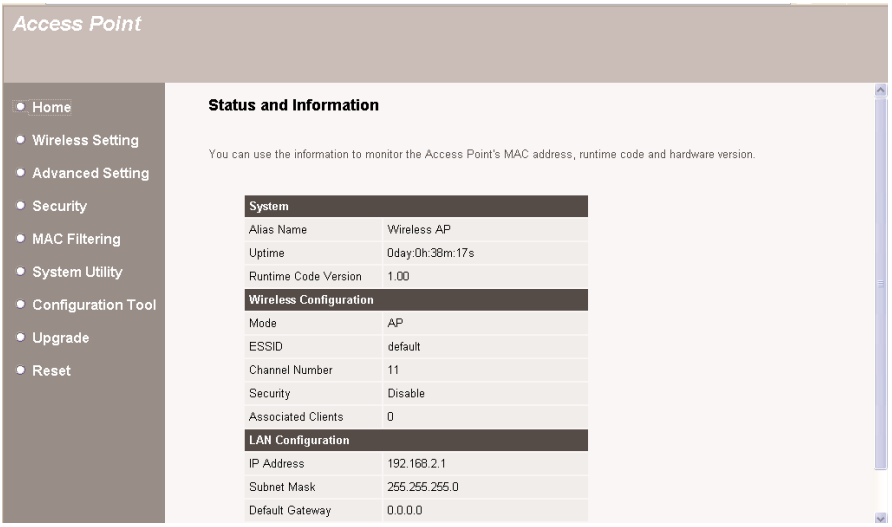


Figure 4-2. Status and information screen.

Table 4-1. Status and information screen options.

Parameter	Description
Alias Name	The access point's alias name. Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode. See **Section 4.2.2** for a description of each mode.
Uptime	The amount of time that the access point has been active since the last reboot or power on.
Runtime Code Version	This is the current operating code version.
Mode	AP (Access Point), station, bridge, or WDS (Wire Distributed System Repeater) mode.
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Make sure that all stations' ESSIDs in the same WLAN network are the same. The default ESSID is "default". Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channel 1–11 Assign an alias name in AP mode, station-ad hoc mode, AP bridge-point to point mode, AP bridge-point to multipoint mode, and AP bridge-WDS mode.
Security	This selects whether WEP is enabled or disabled.

Table 4-1 (continued). Status and information screen options.

Parameter	Description
Associated Clients	Click on the **Show Active Clients** button at the bottom of the screen (not visible in Figure 4-2, since you must scroll down to see it), then an Active Wireless Client table will pop up. You can see the status of all active wireless stations that are connecting to the access point.
IP Address	This is the access point's LAN IP address.
Subnet Mask	This is the subnet mask for the attached LAN segment.
Default Gateway	This is your local LAN's default router address.

Click on the **Apply** button at the bottom of the screen (not shown in Figure 4-2, since you must scroll down to see it) to save the above configurations. You can now configure other advanced sections or start using the access point.

4.2.2 Wireless Setting

This access point supports AP mode, station ad-hoc mode, station-infrastructure mode, and AP bridge-WDS mode. AP mode provides pure access point function. Station ad-hoc mode enables a wired Ethernet network device to communicate with a wireless LAN. Station-infrastructure mode links two wired Ethernet networks together via a wireless LAN. AP bridge-WDS mode enables the access point to bridge a wired Ethernet network and connect to other wireless stations at the same time.

The simplest way to build up a wireless LAN is to use AP mode (see Figure 4-3 and Table 4-2).

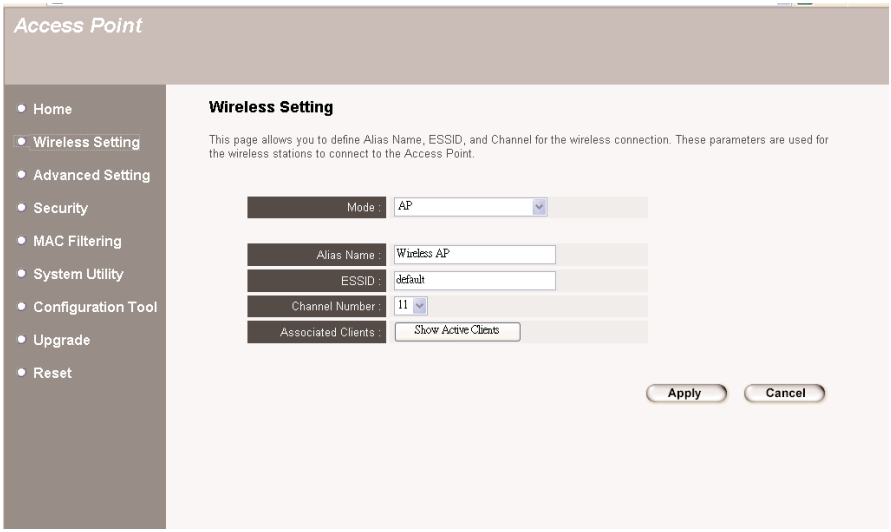


Figure 4-3. AP mode setting page.

Table 4-2. AP mode setting parameters.

Parameter	Description
Mode	AP (Access Point), station, bridge, or WDS.
Alias Name	The access point's alias name. Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Make sure that all stations' ESSIDs in the same WLAN network are the same. The default ESSID is "default". Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.

Table 4-2 (continued). AP mode setting parameters.

Parameter	Description
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channel 1–11 Assign an alias name in AP mode, station-ad hoc mode, AP bridge-point to point mode, AP bridge-point to multipoint mode, and AP bridge-WDS mode.
Associated Clients	Select **Show Active Clients** from the Associated Clients drop-down menu, then an Active Wireless Client table will pop up. You can see the status of all active wireless stations that are connecting to the access point.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

AP mode is used to allow a network device with only wired Ethernet function to have wireless LAN communication capability. It provides both ad-hoc (without access points) and infrastructure (with access points) applications.

Station-ad hoc mode enables your network device to join multiple PCs together to form a wireless LAN.

Station-infrastructure mode enables your network device to join a wireless LAN through an access point.

AP bridge mode-WDS bridges more than two wired Ethernet networks together via a wireless LAN. You can use two access points with AP bridge-point to point mode to bridge two wired Ethernet networks together. See Figure 4-4 and Table 4-3.

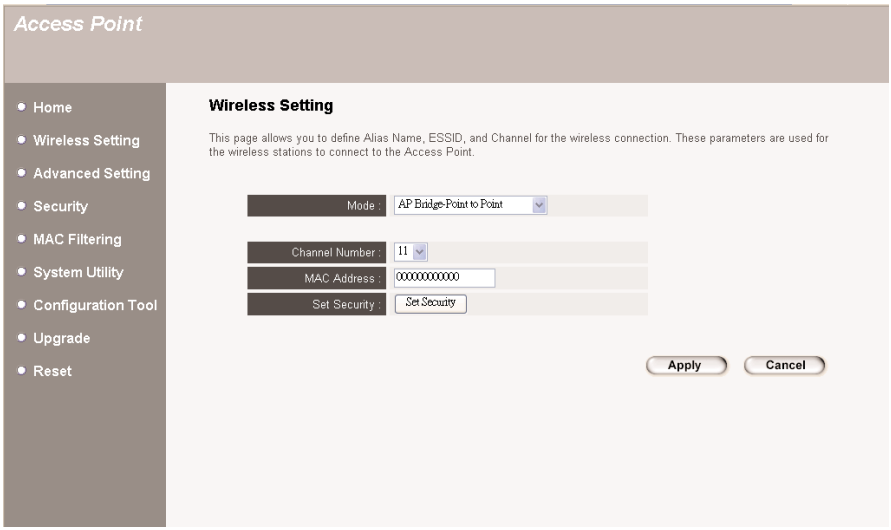


Figure 4-4. AP bridge-point to point mode setting page.

Table 4-3. AP bridge-point to point mode parameters.

Parameter	Description
Mode	AP (Access Point), station, bridge, or WDS.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channel 1–11 Assign an alias name in AP mode, station-ad hoc mode, AP bridge-point to point mode, AP bridge-point to multipoint mode, and AP bridge-WDS mode.

Table 4-3 (continued). AP bridge-point to point mode parameters.

Parameter	Description
MAC Address	If you want to bridge more than one wired Ethernet network together with a wireless LAN, you have to set this access point to AP bridge-point-to-point mode, AP bridge-point-to-multipoint mode, or AP bridge-WDS mode. You have to enter the MAC addresses of other access points that join the bridging work.
Set Security	Enable or disable the security option.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

If you want to bridge more than two wired Ethernet networks together, you have to use enough access points with AP bridge-point to multipoint mode. An access point with AP bridge-point to point mode or AP bridge-point to multipoint mode can only be used to bridge wired Ethernet networks together. It can't accept connections from other wireless stations at the same time.

If you want an access point to bridge a wired Ethernet network and provide connection service for other wireless stations at the same time, you have to set the access point to AP bridge-WDS mode. See Figure 4-5 and Table 4-4. Simply speaking, AP bridge-WDS mode function is the combination of AP mode and AP bridge-point to multipoint mode.

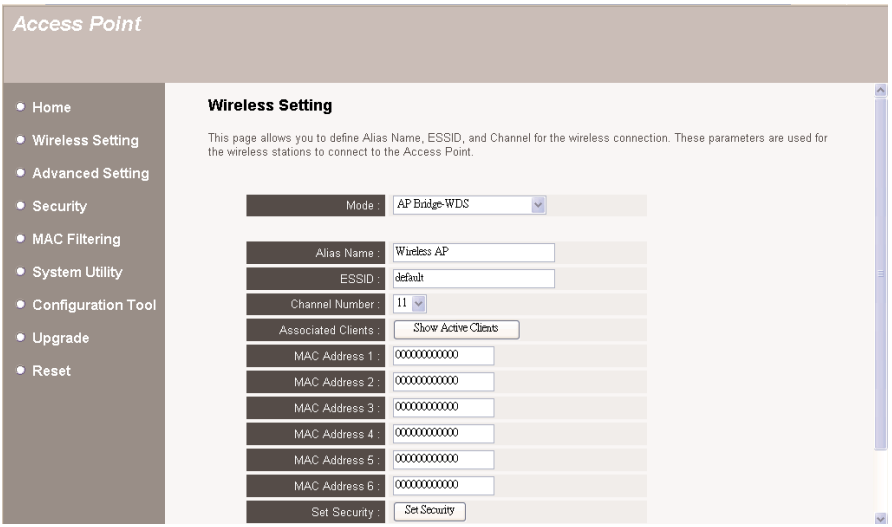


Figure 4-5. AP bridge-WDS mode setting page.

Table 4-4. AP bridge-WDS mode parameters.

Parameter	Description
Mode	AP (Access Point), station, bridge, or WDS.
Alias Name	The access point's alias name. Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Make sure that all stations' ESSIDs in the same WLAN network are the same. The default ESSID is "default". Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.

Table 4-4 (continued). AP bridge-WDS mode parameters.

Parameter	Description
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channel 1–11 Assign an alias name in AP mode, station-ad hoc mode, AP bridge-point to point mode, AP bridge-point to multipoint mode, and AP bridge-WDS mode.
Associated Clients	Click on the **Show Active Clients** button, then an Active Wireless Client table will pop up. You can see the status of all active wireless stations that are connecting to the access point.
MAC Address	If you want to bridge more than one wired Ethernet network together with a wireless LAN, you have to set this access point to AP bridge-point-to-point mode, AP bridge-point-to-multipoint mode, or AP bridge-WDS mode. You have to enter the MAC addresses of other access points that join the bridging work.
Set Security	Enable or disable the security option.

Active Wireless Client Table

The Active Wireless Client table (see Figure 4-6 and Table 4-5) records the status of all active wireless stations that connect to the access point. To get to this screen, select the Show Active Clients option from the drop-down menu in Figure 4-5.

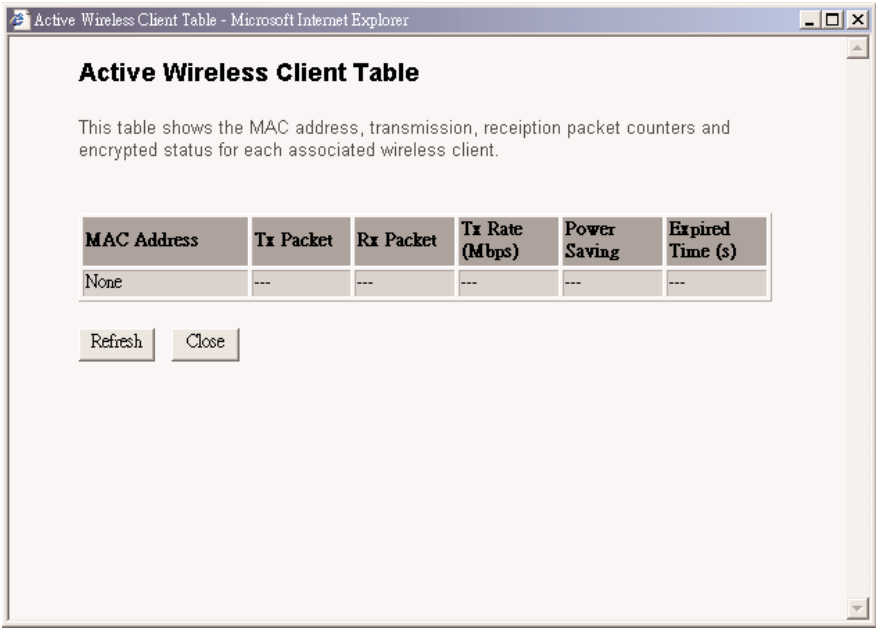


Figure 4-6. Active wireless client table.

Table 4-5. Active wireless client table options.

Parameter	Description
MAC Address	The active wireless station's MAC address.
Tx Packet	The number of transmitted packets that are sent out from this active wireless station.
Rx Packet	The number of received packets that are received by this active wireless station.
TX Rate	The transmission rate in Mbps.
Power Saving	Shows if the wireless client is in power-saving mode.
Expired Time	The time in seconds before dissociation. If the wireless station stays idle longer than the expired time, this access point will dissociate it. The wireless client station has to associate again when it becomes active.
Refresh	Refresh the Active Wireless Client table.
Close	Close the Active Wireless Client table.

Wireless Site Survey

When one access point is in station-ad hoc mode or station-infrastructure mode, it should associate with another access point and connect to your wireless LAN through the associated access point. The wireless site survey (see Figure 4-7) searches for all available access points nearby. To get to this screen, select Station mode from the drop-down mode menu in Figure 4-3. The wireless site survey will appear; select one access point listed in this table.

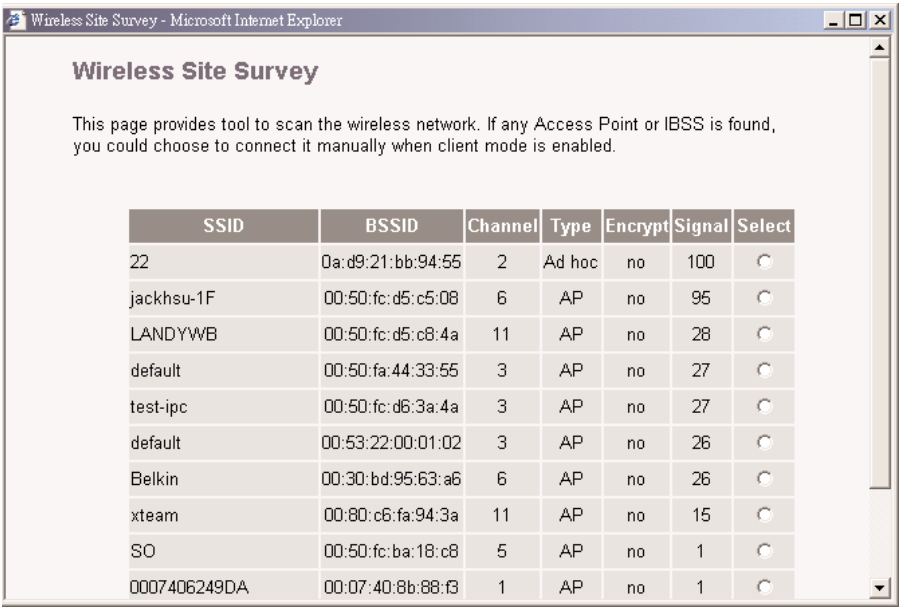


Figure 4-7. Wireless site survey screen.

4.2.3 Advanced Setting

You can set the access point's advanced parameters (see Figure 4-8 and Table 4-6). You should not change these parameters unless you know what effect the changes will have on this access point.

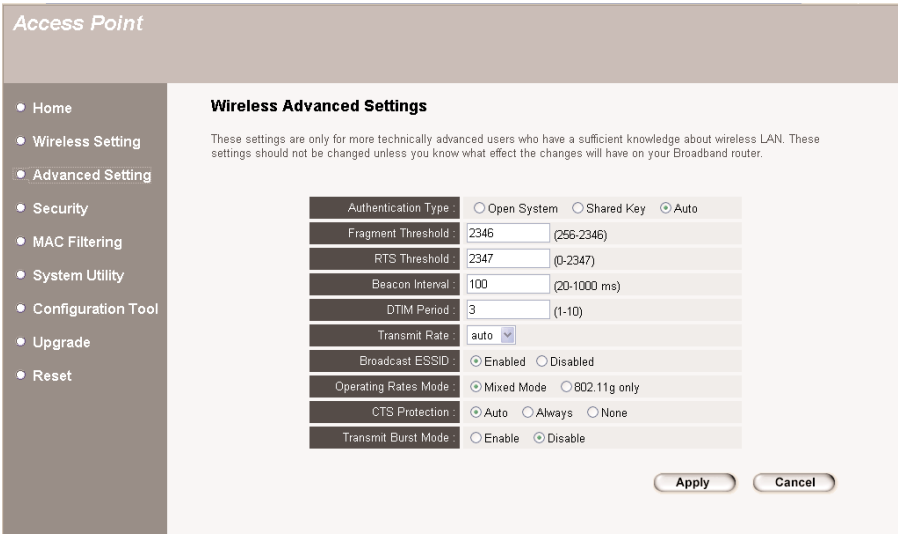


Figure 4-8. Advanced settings selected.

Table 4-6. Advanced setting options.

Parameter	Description
Authentication Type	There are two authentication types: open system and shared key. When you select open system, wireless stations can associate with this access point without WEP encryption. When you select shared key, you should also set up WEP key in the encryption page, and wireless stations should use WEP encryption in the authentication phase to associate with this access point. If you select both, the wireless client can associate with this access point by using either one of these two authentication types.

Table 4-6 (continued). Advanced setting options.

Parameter	Description
Fragment Threshold	Fragment threshold specifies the maximum data packet size to be transmitted during data fragmentation. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcasts a beacon. A beacon is used to synchronize the wireless network.
DTM Period	This is a delivery traffic indication message. It tells clients when the next interval is so it can listen for broadcasts.
Transmit Rate	The data rate is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate.
Broadcast ESSID	If you enable broadcast ESSID, every wireless station located within this access point's coverage can discover this access point easily. If you are building a public wireless network, enable this feature. Disabling broadcast ESSID can provide better security.
Operating Rates Mode	Operates in a pure 802.11g (54 Mbps) environment or a mix of 11-Mbps (802.11b) and 54-Mbps devices.
CTS Protection	Locks out access so that 802.11b frames and 802.11g frames are not mixed up.
Transmit Burst Mode	Provides short-lived bursts of data to 54-Mbps devices.

Table 4-6 (continued). Advanced setting options.

Parameter	Description
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the configurations. You can now configure other advanced sections or start using the access point.

4.2.4 Security

This access point provides complete wireless LAN security functions. With these functions, you can protect your wireless LAN from illegal access. Make sure your wireless stations use the same security function.

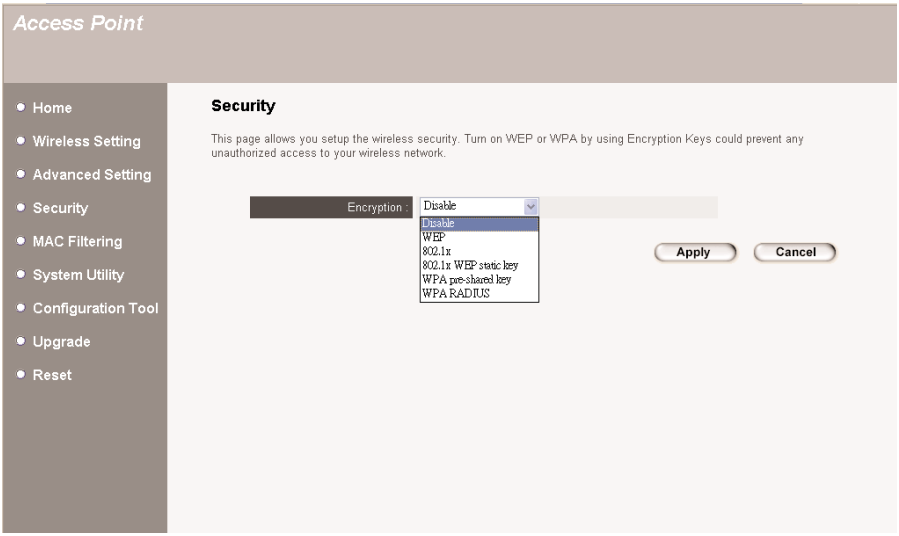


Figure 4-9. Security functions.

Once you select a security function from the drop-down menu, click on the **Apply** button to save your changes, or click on the **Cancel** button to exit the screen without making any changes.

WEP

WEP is an authentication algorithm that protects authorized wireless LAN users against eavesdropping. The wireless stations' authentication type and WEP key must be the same as the access point's. This access point supports a 64-/128-/152-bit WEP encryption function. With this function, your data will be transmitted over the wireless network securely.

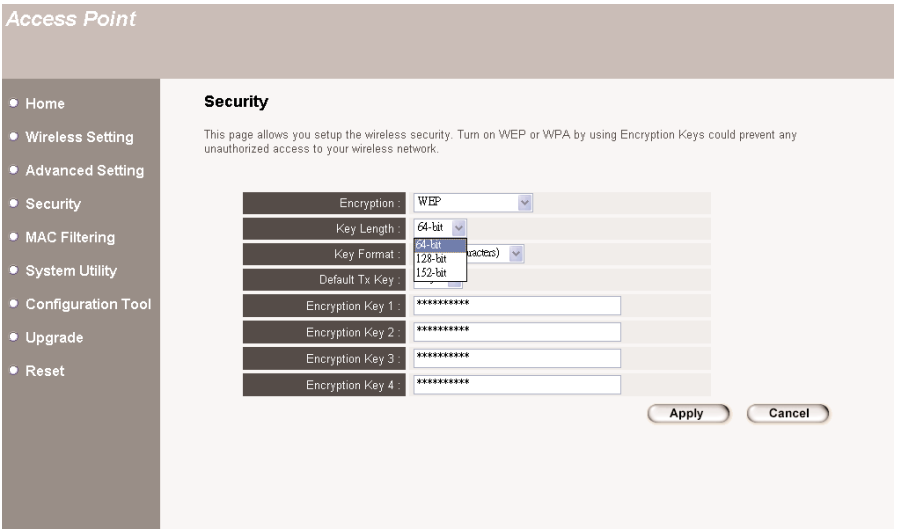


Figure 4-10. WEP security selected.

Table 4-7. WEP security options.

Parameter	Description
Key Length	Select the 64-, 128-, or 152-bit key to encrypt transmitted data. A larger WEP key length will provide a higher level of security, but the throughput will be lower. You can also select disable to transmit data without encryption.

Table 4-7 (continued). WEP security options.

Parameter	Description
Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the WEP key. For example: ASCII characters: guest Hexadecimal digits: 12345abcde
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select in the default key option will take effect.
Encryption Key 1–4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill in the text box, keeping in mind the points listed below. 64-bit WEP: Type in 10-digit hex values (in the A–F, a–f, and 0–9 range) or 5-digit ASCII characters as the encryption keys. For example, “0123456aef”. 128-bit WEP: Type in 26-digit hex values (in the A–F, a–f, and 0–9 range) or 13-digit ASCII characters as the encryption keys. For example, “01234567890123456789abcdef”. 152-bit WEP: Type in 32-digit hex values (in the A–F, a–f, and 0–9 range) or 16-digit ASCII characters as the encryption keys. For example, “01234567890123456789abcdef”.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

802.1x

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this access point before accessing the wireless LAN. The authentication is processed by a RADIUS server. You can use an external RADIUS server or use the access point's built-in RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

Figure 4-11. 802.1x security selected.

Table 4-8. 802.1x security options.

Parameter	Description
Use internal MD5 RADIUS Server	This is a checkbox that you can select to use the internal RADIUS server to process the authentication job. The internal RADIUS server uses the MD5 authentication method. Although this checkbox does not appear in Figure 4-11, it will appear on the software's screen.
RADIUS Server IP address	The external RADIUS server's IP address.
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The external RADIUS server's password.

Table 4-8 (continued). 802.1x security options.

Parameter	Description
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

802.1x WEP Static Key

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to the access point before accessing the wireless LAN. The authentication is processed by a RADIUS server. You can use an external RADIUS server or use the access point's built-in RADIUS server. This mode also uses WEP to encrypt the data during communication.

Figure 4-12. 802.1x WEP static key selected.

Table 4-9. 802.1x WEP static key selected options.

Parameter	Description
Key Length	Select 64-bit or 128-bit to encrypt transmitted data. A larger WEP key length will provide a higher level of security, but the throughput will be lower. You also can select Disable to transmit data without encryption.
Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the WEP key. For example: ASCII characters: guest Hexadecimal digits: 12345abcde
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select in the default key will take effect.
Encryption Key 1–4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill in the text box, keeping in mind the points listed below. 64-bit WEP: Type in 10-digit Hex values (in the A–F, a–f, and 0–9 range) or 5-digit ASCII character as the encryption keys. For example, “0123456abcdef”. 128-bit WEP: Type in 26-digit Hex values (in the A–F, a–f, and 0–9 range) or 10-digit ASCII characters as the encryption keys. For example, “01234567890012345678 90abcdef”.
Use internal MD5 RADIUS Server	You can select to use the internal RADIUS server to process the authentication job. This is a checkbox on the software screen (not shown in Figure 4-12).The internal RADIUS server uses the MD5 authentication method.

Table 4-9 (continued). 802.1x WEP static key selected options.

Parameter	Description
RADIUS Server IP address	The external RADIUS server's IP address.
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The external RADIUS server's password.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the access point.

WPA Pre-Shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP to change the encryption key frequently. This can improve security.

Figure 4-13. WPA pre-shared key security selected.

Table 4-10. WPA pre-shared key options.

Parameter	Description
WPA Unicast Cipher Suite	Select the TKIP checkbox to change the encryption key frequently to enhance the wireless LAN security. Select the AES (Advanced Encryption Standard) checkbox to keep the encryption key the same.
Pre-shared Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the Pre-shared Key. For example: ASCII characters: iamguest Hexadecimal digits: 12345abcde
Pre-shared Key	The pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex WEP: Type in 64-digit Hex values (in the A–F, a–f, and 0–9 range) or at least an 8-character pass phrase as the pre-shared keys.

Table 4-10 (continued). WPA pre-shared key options.

Parameter	Description
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the configurations. You can now configure other advanced sections or start using the access point.

WPA RADIUS

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP to change the encryption key frequently to improve security, or AES to keep the key the same.

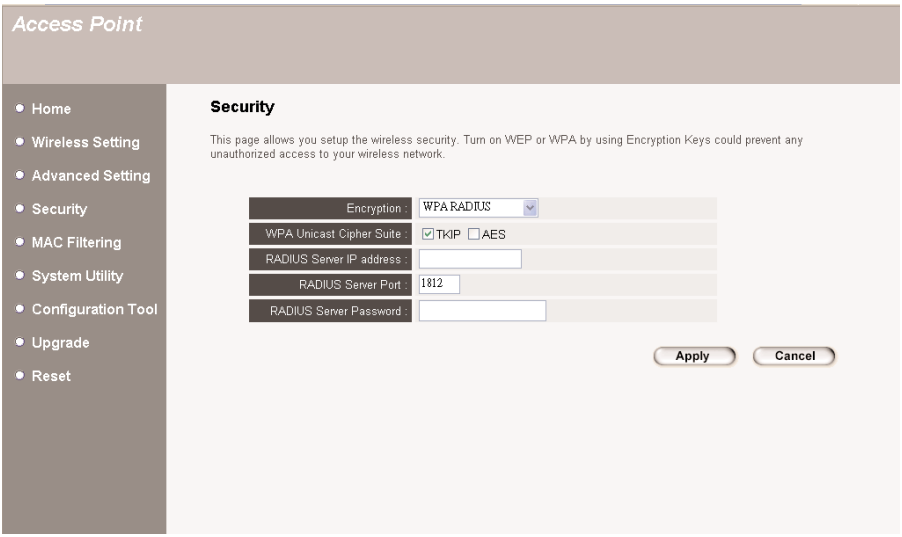


Figure 4-14. WPA security selected.

Table 4-11. WPA security options.

Parameter	Description
WPA Unicast Cipher Suite	Select the TKIP checkbox to change the encryption key frequently to enhance the wireless LAN security. Select the AES (Advanced Encryption Standard) checkbox to keep the encryption key the same.
RADIUS Server IP Address	The external RADIUS server's IP address.
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The external RADIUS server's password.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

4.2.5 MAC Address Filtering

This access point provides MAC address filtering, which prevents unauthorized MAC addresses from accessing your wireless network.

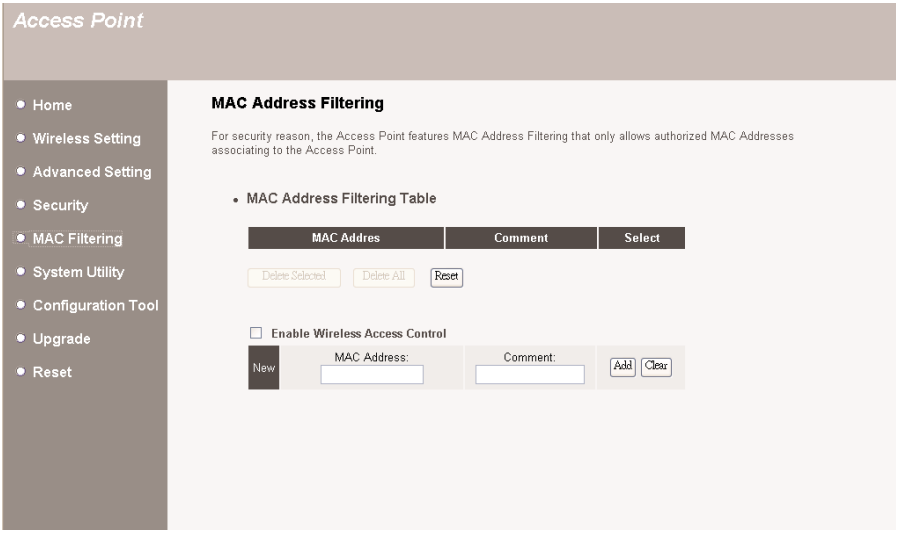


Figure 4-15. MAC address filtering selected.

Table 4-12. MAC address filtering options.

Parameter	Description
MAC Address Filtering Table	This table records the wireless stations' MAC addresses that you want to allow to access your network. The comment field describes the wireless station associated with the MAC address and is helpful for you to recognize the wireless station.
Delete Selected	Delete the selected MAC addresses.
Delete All	Delete all of the MAC addresses.
Reset	Reset the filtering table without saving changes.

Table 4-12 (continued). MAC address filtering options.

Parameter	Description
Enable Wireless Access Control	Check this checkbox to enable wireless access control.
MAC address	In the bottom new area, type in the MAC address for the wireless station to be added.
Comment	Type in the comment for the wireless station to be added.
Add button	Click on this button to add this wireless station into the MAC Address Filtering Table above.
Clear button	If you make a typing mistake and you have not hit the Add button, just click on this button. Both MAC Address and Comment fields will be cleared.

4.2.6 System Utility

From here, you can define the access point's IP address and login password and enable the access point to be a DHCP server.

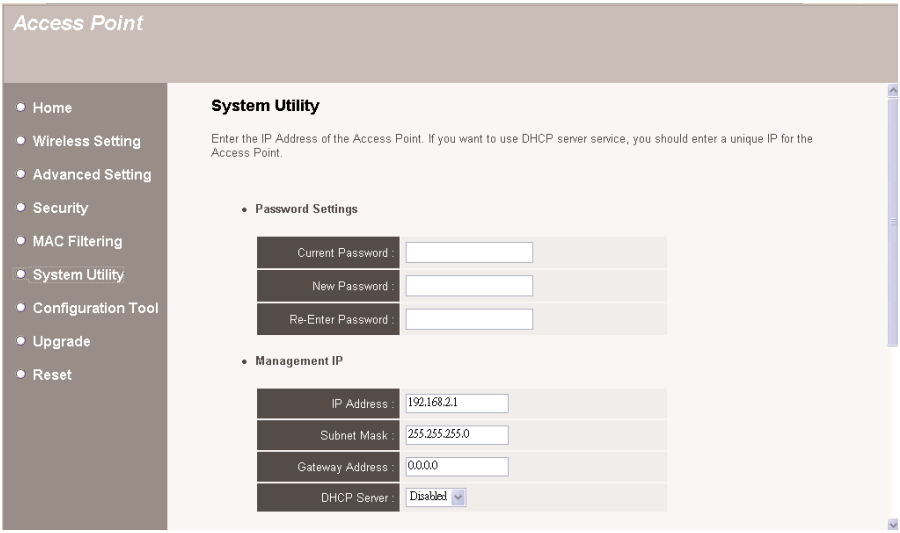


Figure 4-16. System utility selected.

Table 4-13. System utility options.

Parameter	Description
Current Password	Enter the current password (up to a 15-digit alphanumeric string) of the access point. The default password for the access point is `1234`.
New Password	Enter the password (up to a 15-digit alphanumeric string) that you want to use to login to the access point.
Re-Enter Password	Reconfirm the password (up to a 15-digit alphanumeric string) you want to login to the access point.

NOTE

All of the passwords listed above are case-sensitive.

Table 4-13 (continued). System utility options.

Parameter	Description
IP Address	Designate the access point's IP address. This IP address should be unique in your network. The default IP address is 192.168.2.1.
Subnet Mask	Specify a subnet mask for your LAN segment. The access point's subnet mask is fixed, and the value is 255.255.255.0.
Gateway Address	Specify the access point's gateway address.
DHCP Server	Enable or disable the DHCP server.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

DHCP Server Setting

A DHCP server will automatically give your LAN client an IP address. To enable DHCP, go to the System Utility initial configuration screen. If the DHCP is not enabled, you'll have to manually set your LAN client's IP address.

Table 4-14. DHCP server options.

Parameter	Description
Default Gateway IP	Specify the gateway IP in your network. This IP address should be different from the server IP.
Domain Name Server IP	This is the DNS server IP address that your ISP gave you; or you can specify your own preferred DNS server IP address.

Table 4-14 (continued). DHCP server options.

Parameter	Description
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default, the IP range is from: Start IP 192.168.2.100 to End IP 192.168.2.200.
Domain Name	You can specify the domain name for your access point.
Lease Time	The DHCP server, when enabled, will temporarily give your LAN client an IP address. Lease time allows you to specify the time period that the DHCP server lends an IP address to your LAN clients. The DHCP server will change your LAN client's IP address when this time threshold period is reached.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

4.2.7 Configuration Tool

The Configuration Tools screen allows you to backup the access point's current configuration setting. Saving the configuration settings provides an added protection and convenience if problems occur with the access point and you have to reset it to the factory default. When you back up the configuration setting, you can re-load the saved configuration into the access point through the restore selection. If extreme problems occur, you can use the Restore to Factory Default selection; this will set all configurations to the original default settings (for example, when you first purchased the access point).

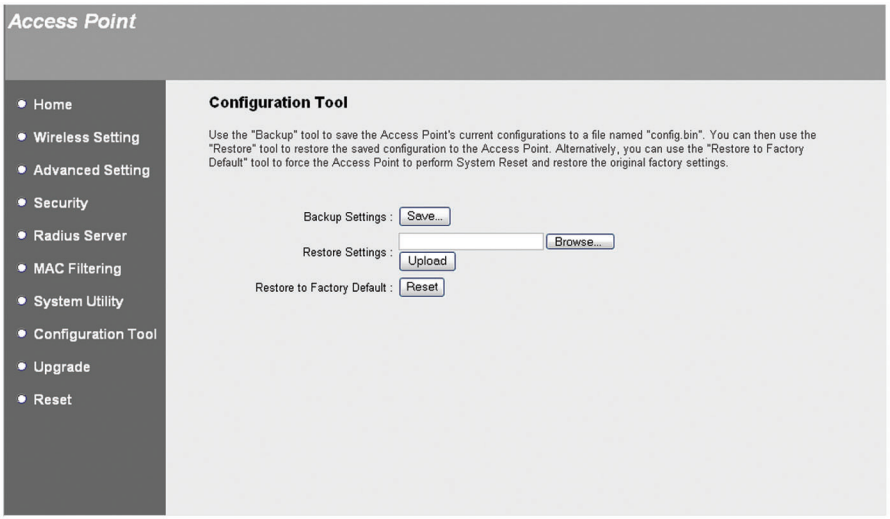


Figure 4-17. Configuration tool selected.

Table 4-15. Configuration tool options.

Parameter	Description
Backup Settings	Use the backup tool to save the access point's current configuration to a file named config.bin on your PC. Click on **Save** to save the changes.
Restore Settings	You can then use the Restore tool to upload and restore the saved configuration to the access point. Click on the **Upload** button.
Restore to Factory Default	Or, you can use the Restore to Factory Default tool to force the access point to perform a power reset and restore the original factory settings. Click on the **Reset** button.

4.2.8 Firmware Upgrade

This page allows you to upgrade the access point's firmware.

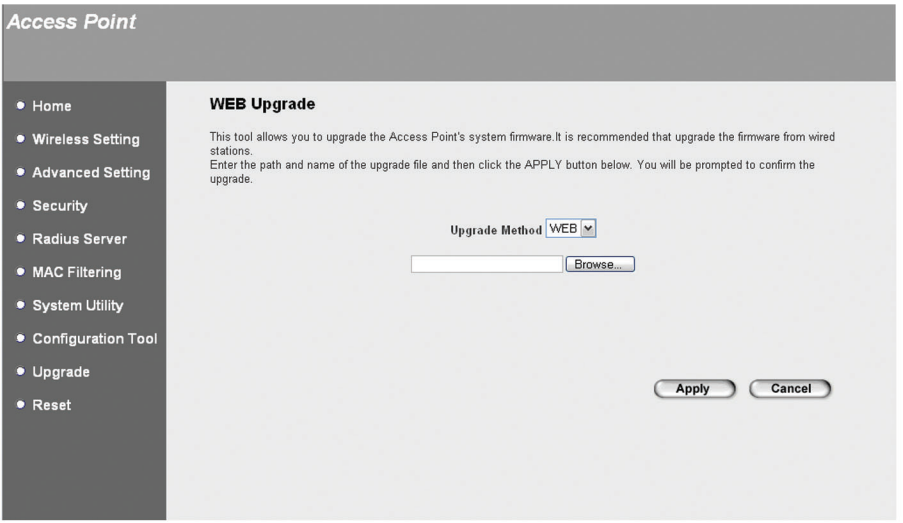


Figure 4-18. Upgrade selected.

Table 4-16. Upgrade option.

Parameter	Description
Upgrade Method	This tool allows you to upgrade the access point's system firmware. To upgrade your access point's firmware, download the firmware file to your local hard disk, and enter that file name and path in this field on this page.
Browse	Use this button to find the firmware file on your PC. Reset the access point when the upgrade is complete.
Apply	Click on this button to start the upgrade process.
Cancel	Click on this button to cancel the upgrade process.

Once you've selected the new firmware file, click on the **Apply** button at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete, you can start using the access point.

4.2.9 RESET

You can reset the access point's system if any problem exists. The reset function essentially reboots your access point's system.

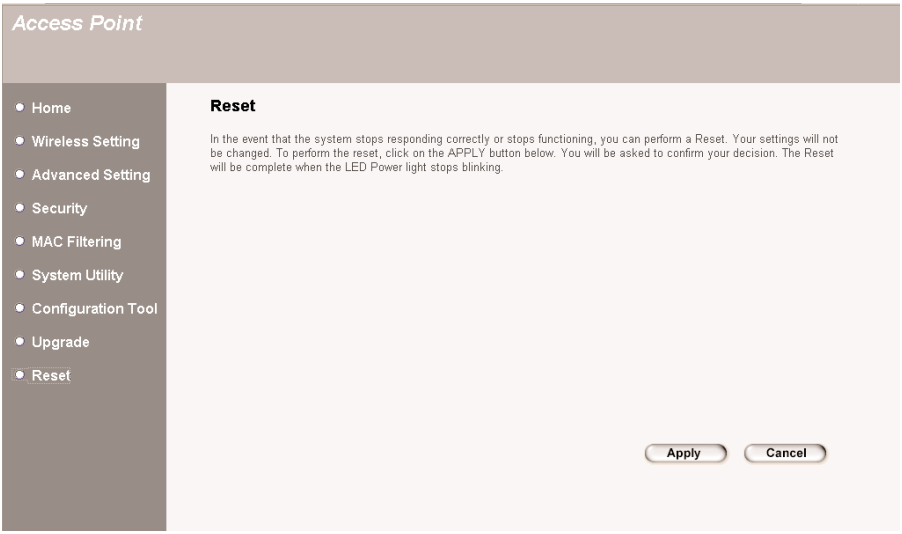


Figure 4-19. Reset selected.

If the system stops responding correctly or in some way stops functioning, perform a reset. Your settings will not be changed. To perform the reset, click on the **Apply** button. You will be asked to confirm your decision. Once the reset process is complete, you can start using the access point again.

Click on the **Cancel** button to cancel the reset.

5. Troubleshooting

5.1 Frequently Asked Questions

1. How do you manually find your PC's IP and MAC address?

   a. In Windows, open the Command Prompt program.

   b. Type `Ipconfig/all` and press **Enter**.

      Your PC's IP address is listed as "IP address."

      Your PC's MAC address is listed as "Physical Address."

2. What is BSS ID?

   A specific ad-hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

3. What is ESSID?

   An infrastructure configuration can also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS can roam freely between BSSs while maintaining a continuous connection to the wireless network stations and the access points.

4. Can data be intercepted while transmitting through the air?

   WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum (DSSS) technology, it has the inherent scrambling security feature. On the software side, the WLAN series offers the encryption function (WEP) to enhance security and access control.

5. What is WEP?

   WEP stands for Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared key algorithm, as described in the IEEE 802.11 standard.

6. What is a MAC Address?

   The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device (such as a network adapter) that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

5.2 Calling Black Box

If you determine that your Pure Networking 802.11g Wireless Access Point with Switch is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box 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.

5.3 Shipping and Packaging

If you need to transport or ship your Pure Networking 802.11g Wireless Access Point with Switch:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the access point for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.