User's Manual

HAWKING TECHNOLOGY

HWBA54G

Rev. R

Wireless-G
Access Point / Bridge

website | www.hawkingtech.com
e-mail | techsupport@hawkingtech.com

CE MARK WARNING

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

LIMITED WARRANTY

Hawking Technology guarantees that every HWBA54G Wireless-G AP / Bridge is free from physical defects in material and workmanship under normal use for two (2) years from the date of purchase. If the product proves defective during this two-year warranty period, call Hawking Customer Service in order to obtain a Return Authorization number. Warranty is for repair or replacement only. Hawking Technology does not issue any refunds. BE SURE TO HAVE YOUR PROOF OF PURCHASE. RETURN REQUESTS CAN NOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization number clearly on the outside of the package and include your original proof of purchase.

IN NO EVEN SHALL HAWKING TECHNOLOGY'S LIABILTY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE OR ITS DOCUMENTATION. Hawking Technology makes no warranty or representation, expressed, implied or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Hawking Technology reserves the right to revise or updates its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to: techsupport@hawkingtech.com

TRADEMARKS AND COPYRIGHT

FCC WARNING

Federal Communication Commission Interference Statement

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

- **Reorient or relocate the receiving a ntenna.**
- **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 the dealer or an experienced radio/TV technician for help.**

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

Table of Contents

Chapter 1 Introduction

Thank you for purchasing the Hawking Technologies Hi-Speed 54M Wireless-G Access Point and Ethernet Bridge. The HWBA54G is compliant with the IEEE 802.11g/b wireless standards.

The **Hi-Speed 54G Wireless AP/Bridge** utilizes the highest wireless security standards (WPA) to protect your network from outside intruders, including WPA-PSK, WEP, ESSID and MAC address filter functions. With ESSID authentication, WPA-PSK, 64-/128-bit WEP encryption and MAC address filtering, unauthorized outside access into your wireless network is prevented.

The unique multi-function feature of the HWBA54G puts two solutions into one compact unit, saving you time and money. You may setup your HWBA54G as a Wireless Access Point to provide wireless access to any wired network or you may choose to set up your device as an Ethernet Bridge to make any Ethernet-ready device wireless.

The HWBA54G's dipole antenna is detachable by connecting to a RP-SMA connector. Users can attach an optional Hawking Technologies Hi-Gain antenna to the connector for better network range and signal quality.

1.1 Package Contents

The HWBA54G includes the following items:

- One HWBA54G Access Point/Bridge
- One Power Adapter
- One Quick Installation Guide
- One Setup CD
- One Dipole Antenna

1.2 Features

- Complies with the IEEE 802.11b/g (DSSS) 2.4GHz specification.
- Multiple Functions: Access Point, Ethernet Bridge, WDS Bridge etc…
- High wireless data rate 54Mbps network speed.
- Seamlessly integrates wireless and wired Ethernet networks.
- Auto rate fallback in case of obstacles or interferences.
- Provide 64/128-bit WEP and WPA Data Encryption function to protect the wireless data transmissions.
- Built-in DHCP server supports auto IP addresses assignment.
- Supports Web-based configuration.
- Easy Setup Wizard for simple configuration

1.3 Specifications

- Standards: IEEE 802.11b/g (Wireless), IEEE 802.3 (Wired)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP and WPA Data Encryption
- Frequency Band: 2.400~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps and DBPSK@1Mbps
- Radio Technology: Direct Sequence Spread Spectrum (DSSS)
- Antenna: External detachable dipole antenna (with RP-SMA connector) Compatible with Hawking Technologies Hi-Gain Wireless Range Extending Antennas and Boosters.
- Connectors: 10/100Mbps RJ-45 x 1
- Power: 12VDC, 0.5A

- Transmit Power: 15dBm (Typical)
- LEDs: Power, LAN Link/Activity, Wireless Activity
- Dimension: 30(H) x 127(W) x 96(D) mm
- Temperature:

  Operating: 32~131°F (0~55°C)

  Storage: -4~158°F(-20~70°C)
- Humidity: 10-90% (Noncondensing)
- Certification: FCC, CE

1.4 Physical Description

Front Panel

Located on the HWBA54G's front panel are LED status lights that inform you of the unit's current status. Below is an explanation of each LED.

LED	Color	Status	Description
Power	Green	Lit Off	Power is supplied. No Power.
Wireless Activity	Green	Flash Off	Antenna is transmitting or receiving data. Antenna is not transmitting or receiving data.
LAN Link/Activity	Green	On Flash Off	A valid link is established. It is transmitting or receiving data. No link is established.

Back Panel

Access Point's connection ports are located on the back panel. Below is the description of each connection port.

- Antenna Connector
  This round connection is standard Reverse SMA connector where any antennas with Reverse SMA connector can connect to the Access Point.

- DC Adapter Port
  Insert the power jack of the power adapter into this port.

- LAN Port
  The Access Point's LAN port is where you connect to your LAN's network devices.

- 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) and the Access Point will re-boot itself, keeping your original configurations.

2) If problems persist or you experience extreme problems or you forgot your password, press the reset button for longer than 4 seconds and the Access Point will reset itself to the factory default settings (warning: your original configurations will be replaced with the factory default settings).

Chapter 2 Wireless LAN Access Point Connection

1. **Locate an optimum location for the Wireless Access Point.**
   The best location for your Access Point is usually at the center of your wireless network, with line of sight to all of your mobile computers. A higher location is also preferable. (i.e. the second story of a house versus the first level)

2. **Connect the Wireless LAN Access Point to your router, hub or switch.**
   Connect one end of included Ethernet 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 existed wired LAN Network.

3. **Connect the DC Power Adapter to the Wireless LAN Access Point's Power Socket.**
   Only use the power adapter supplied with the Access Point. Using a different adapter may damage the product.

The Hardware Installation is complete.

Chapter 3 Wireless LAN Access Point Configuration

3.1 Getting Started

This Access Point provides web-based configuration tool allowing you to configure from wired or wireless computers. Follow the instructions below to get started configuration.

From Wired Computer

1. Make sure your wired computer is in the same subnet with the Access Point.
   The default IP Address and Sub Mask of the Access Point is:
   Default IP Address: 192.168.1.240
   Default Subnet: 255.255.255.0

   Configure your PC to be in the same subnet with the Access Point.
   1a) Windows 95/98/Me
   1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
   2. Double-click *Network* icon. The *Network* window will appear.
   3. Check your list of *Network Components*. If TCP/IP is not installed, click 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 *Add* button.
   5. In the *Select Network Protocol* dialog box, select *Microsoft and TCP/IP* and then dick 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 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 as following example.
    1. IP Address: 192.168.1.20 (any IP address within 192.168.1.1~192.168.1.253 is available, **do not setup 192.168.1.1 or 192.168.1.254**)
        - ✓ Subnet Mask: 255.255.255.0

8. Reboot the PC. Your PC will now have the IP Address you specified.

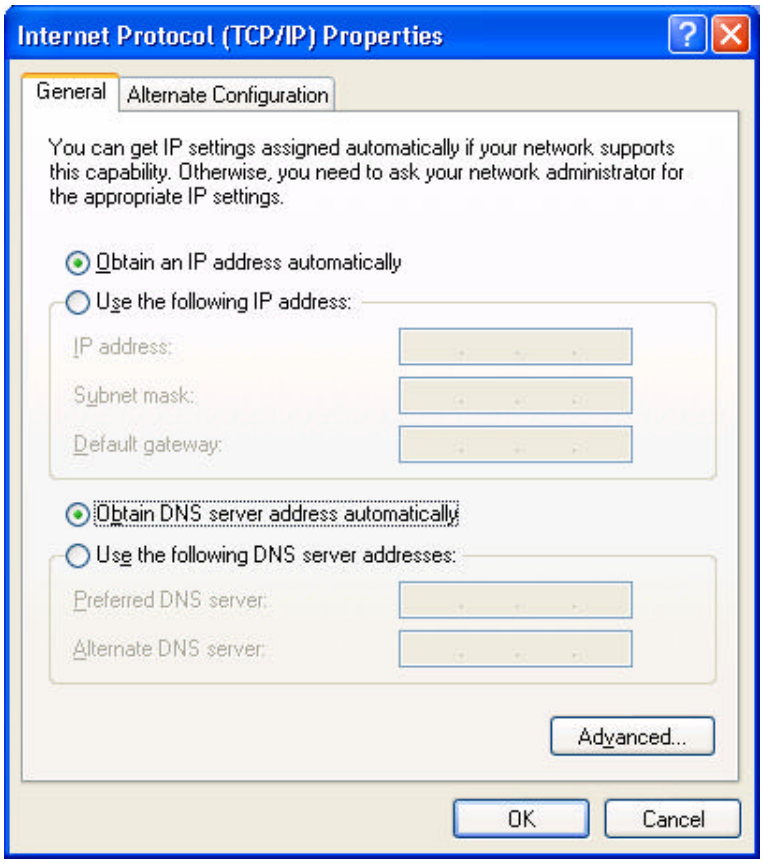
1b) Windows XP

1: Click the *Start* button and select *Settings*, then click *Network Connections.* The *Network Connections* window will appear.

2: Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.

3: Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.

4: In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



5: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

1c) Windows 2000

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

- ✓ IP Address: 192.168.1.20 (any IP address within 192.168.1.1~192.168.1.253 is available, **do not setup 192.168.1 .1 or 192.168.1.254**)
- ✓ Subnet Mask: 255.255.255.0

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

1d) Windows NT

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.
3. Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If *TCP/IP* is not installed, click the *Add* button to install it now. If *TCP/IP* is installed, go to **step 5**.
4. In the Select *Network Protocol* window, select the *TCP/IP Protocol* and click 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* and then click the *Properties* button.
6. Check each of the tabs and verify the following settings:

- **IP Address:** Select *Specify an IP address.* Specify the IP Address and Subnet Mask as following example.
  1. IP Address: 192.168.1.20 (any IP address within 192.168.1.1~192.168.1.253 is available, **do not setup 192.168.1.1 or 192.168.1.254**)
     - ✓ Subnet Mask: 255.255.255.0
- **DNS:** Let all fields are blank.
- **WINS:** Let all fields are blank.
- **Routing:** Let all fields are blank.

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

2. Enter **192.168.1.240** from a Web Browser to get into the Access Point's configuration tool.
3. A screen will be popped up and request you to enter user name and password. The default user name and password is as follows.
   User Name: Admin
   Password: 1234

Enter the default user name and password, then press **OK** button directly.

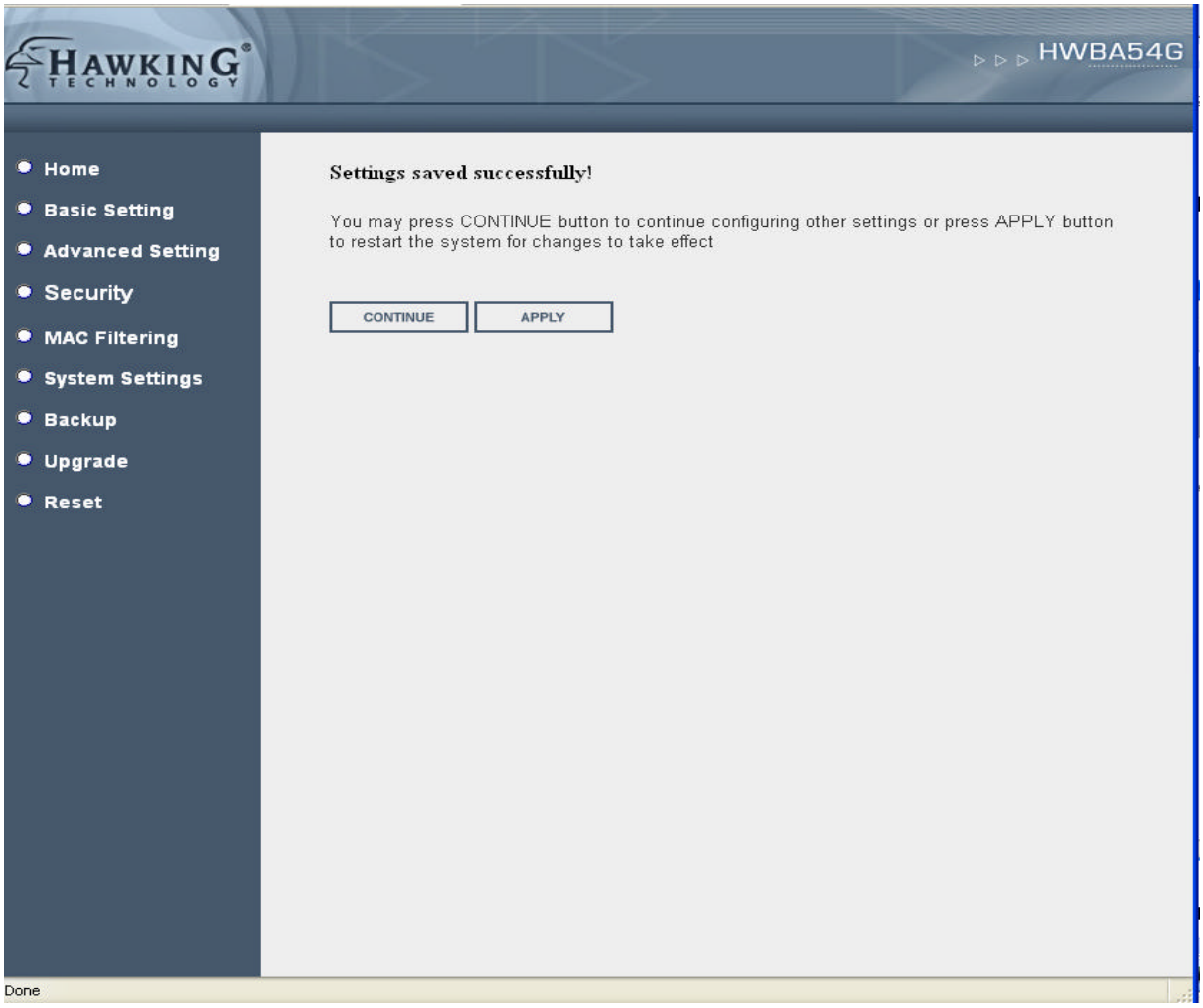
4. You can start configuring the Access Point once you enter the management screen.

From a Wireless computer

1. Make sure your wireless computer is in the same subnet with the Access Point. Please refer to the **step 1** above for configuring the IP Address and Sub Mask of the wireless computer.

2. Connect to the Access Point.
   The Access Point's default ESSID is "**hawkingap**" and the WEP Encryption function is disabled. Make sure your wireless computer is using the same ESSID as the Access Point and associate your wireless computer to the Access Point.
3. Enter **192.168.1.240** from a Web Browser to get into the Access Point's configuration tool.
4. Enter the user name and password and then press the **OK** button and you will be able to configure the Access Point.

3.2 Configuring the Access Point



When modifying a settings page always click the “Apply” button after your changes have been made. The above page will appear. Click “Continue” if you wish to continue making more changes. When all of your changes have been made, click “Apply” at the above pop-up page to save your settings and restart the device.

3.2.1 Status and Information

On this screen, you can see the general information of the Access Point including Alias Name, Firmware Version, ESSID, Channel Number, Status, IP Address, MAC Address, etc.

3.2.2 Wireless Setting

The HWBA54G supports multiple modes of operation. (Access Point, Ethernet Bridge – Ad Hoc, Ethernet Bridge - Client, WDS and Point to Point or Point to Multi Point Bridge modes.

Access Point Mode enables wireless access to any wired network. The simplest way to build up a wireless LAN is to use “Access Point Mode”.

Ethernet Bridge Mode is used to enable wireless access for a wired Ethernet device (i.e. an Game Console, wired computer etc...) It provides both device to device access (Ad-Hoc) or network access (Client).

With “Ethernet Bridge - Ad Hoc mode”, your network device can join a wireless LAN using peer-to-peer communication.

With “Ethernet Bridge - Client mode”, your network device joins a network by connecting to an existing wireless network.

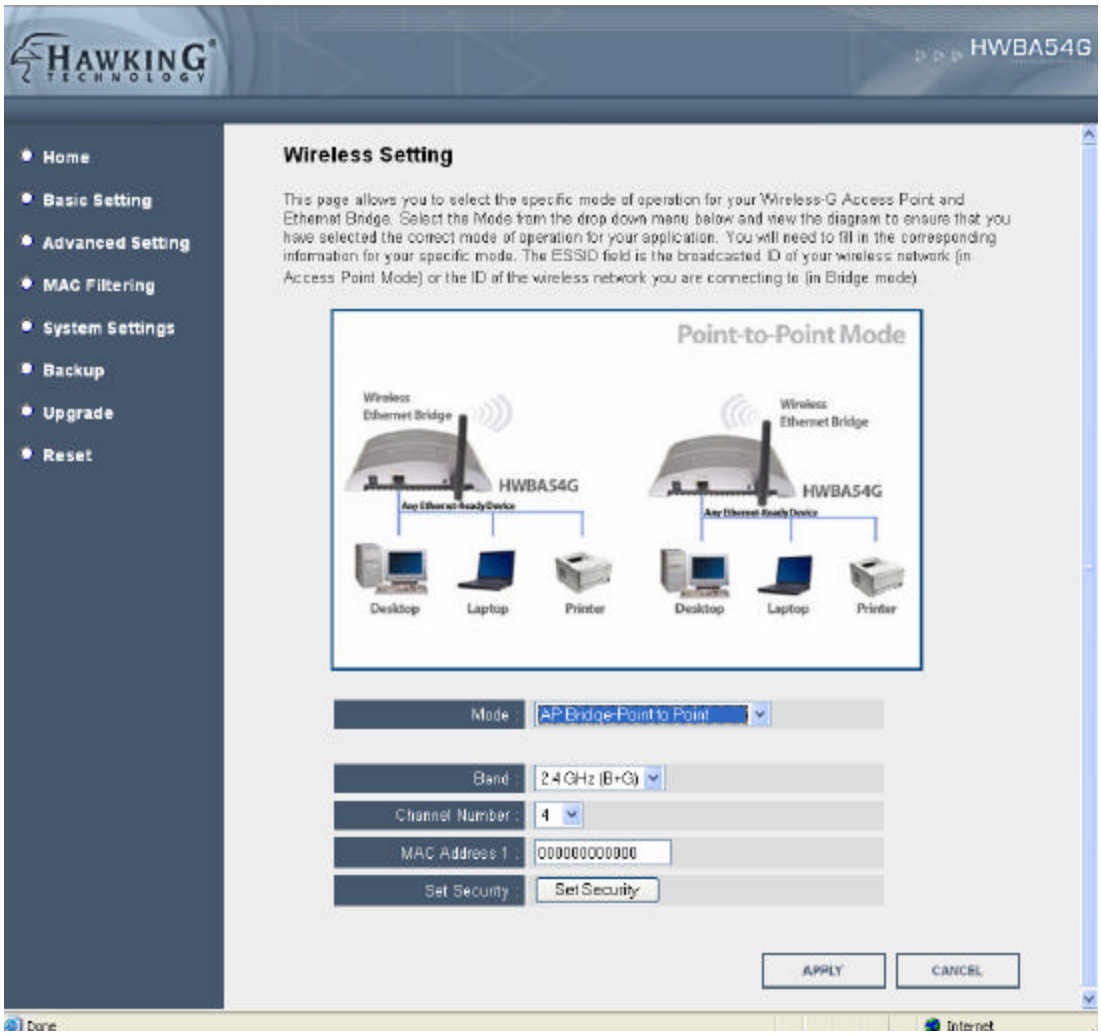
AP Bridge Mode provides the function to bridge more than two wired Ethernet networks together wirelessly. You can use two access points with “AP Bridge-Point to Point mode” to bridge two wired Ethernet networks together. If you want to bridge more than two wired Ethernet networks together, you will need to utilize enough HWBA54G access points with “AP Bridge-Point to Multi-Point mode” to suffice your application. An access point with “AP Bridge-Point to Point mode” or “AP Bridge-Point to Multi-Point mode” can only be used to bridge wired Ethernet networks together. It cannot accept connections from other wireless computer simultaneously. If you want an access point to bridge a wired Ethernet network and provide wireless access to local computers simultaneously, you need to set the access point mode to “AP Bridge-WDS mode”. AP Bridge-WDS mode combines “Access Point mode” and “AP Bridge-Point to Multi-Point mode” together as one mode. AP.

Access Point mode settings page:

Ethernet Bridge – Ad Hoc mode settings page:

Ethernet Bridge - Client mode settings page:

AP Bridge - Point to Point mode settings page:



AP Bridge - Point to Multi-Point mode settings page:

AP Bridge - WDS mode settings page:

Parameter	Description
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique identifying name of a wireless network. The ID prevents the unintentional merging of two co-located wireless networks. Please make sure that the ESSID of all computers in the same WLAN network are the same. The default ESSID is "**hawkingap**". You will need to assign an ESSID in "Access Point mode", "Bridge-Ad Hoc mode", "Bridge-Client mode", and "AP Bridge-WDS mode."
Band	Select 802.11b or 802.11g operating modes. You also can select B+G mode to allow the AP to select 802.11b and 802.11g connection automatically (recommended).
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe) There are 14 channels available. You should assign Channel Number in "Access Point mode", "Ethernet Bridge - Ad Hoc mode", "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" and "AP Bridge-WDS mode."
MAC Address	If you want to bridge more than one wired Ethernet networks together wirelessly, you have to set the access point to "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" or "AP Bridge-WDS mode". You will need to enter the MAC addresses of the other access points you wish to connect to.
WLAN MAC	In "Ethernet Bridge - Ad Hoc mode" and "Ethernet Bridge - Client mode" this device need a WLAN MAC address to act as a computer to connect to other peers or access points. You can also click the "Clone MAC" button to let this device copy the MAC address of the PC that you are using to configure this device.
Set Security	In "AP Bridge-Point to Point mode", ""AP Bridge-Point to Multi-Point mode" and "AP Bridge-WDS mode", you can click "Set Security" to add encryption for the communication between the bridged access points.

	This can protect your wireless network.
Associated Clients	Click the "Show Active Clients" button, to view your "Active Wireless Client Table." You can see the status of all active wireless computers that are connecting to the access point here.
Wireless Site Survey	When using the HWBA54G in Bridge mode the HWBA54G will need to connect to a specific wireless access point of your choosing. Click the "Select Site Survey" button to do a local search of wireless networks. When the one you wish to connect to appears, select the button next to it to connect.

Click **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.

Set Security

Wireless security provides protection from outside intruders into your network. The HWBA54G offers the latest in wireless security in all modes: "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" or "AP Bridge-WDS mode". "WEP 64bits", "WEP 128bits", "WPA (TKIP)", "WPA2 (AES)" encryption methods are offered. Each mode will have its own security settings page.

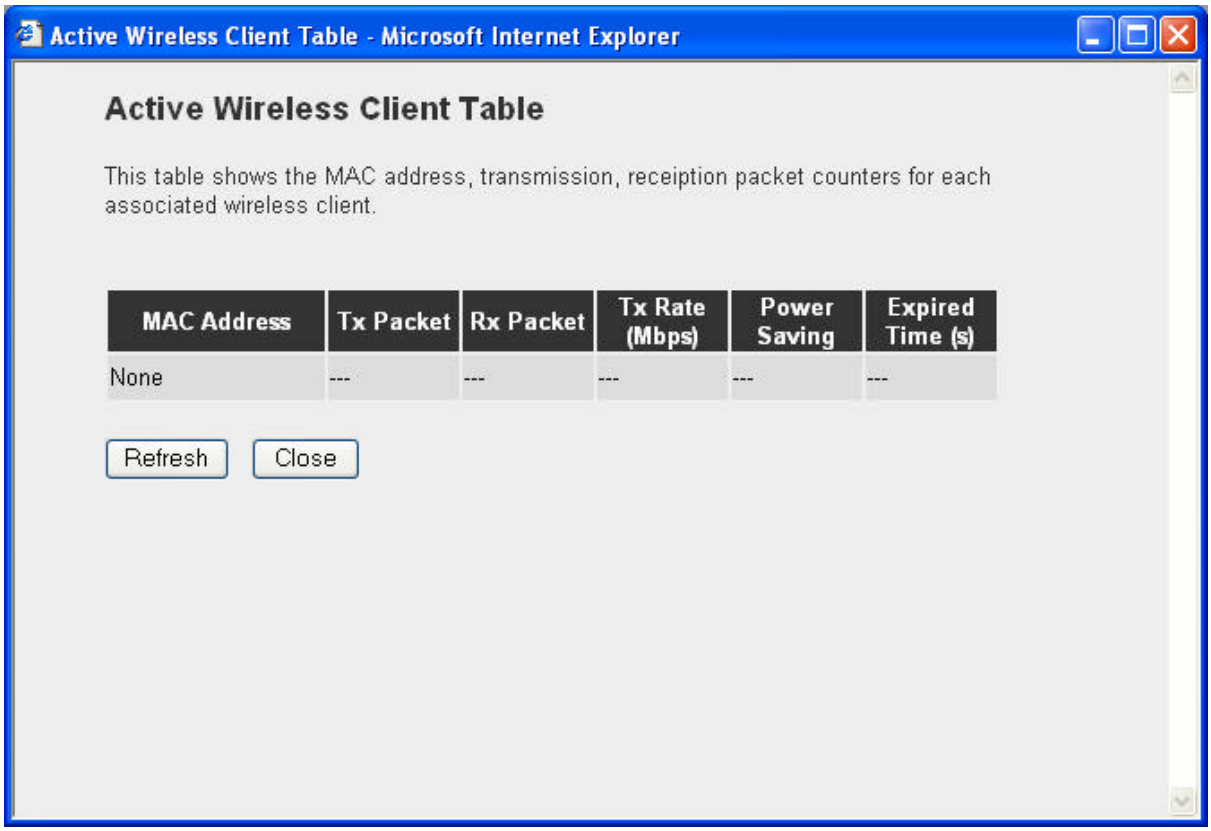
Parameter	Description
Encryption	You can select "No encryption","WEP 64bits", "WEP 128bits", "WPA (TKIP)" or "WPA2 (AES)" encryption methods.
Key Format	This is only used when you select "WEP 64bits" or "WEP 128bits" encryption method. You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example:

	ASCII Characters: guest Hexadecimal Digits: 12345abcde
WEP Key	This is only used when you select "WEP 64bits" or "WEP 128bits" encryption method. The WEP key is used to encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 10-digit ASCII characters as the encryption keys.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. Hex WEP: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Click **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.

Active Wireless Client Table

The “Active Wireless Client Table” records the status of all active wireless devices and computers that connect to the access point. You can lookup the MAC Address, Number of Transmitted Packets, Number of Received Packets and Encryption Status of each active wireless client in this table.

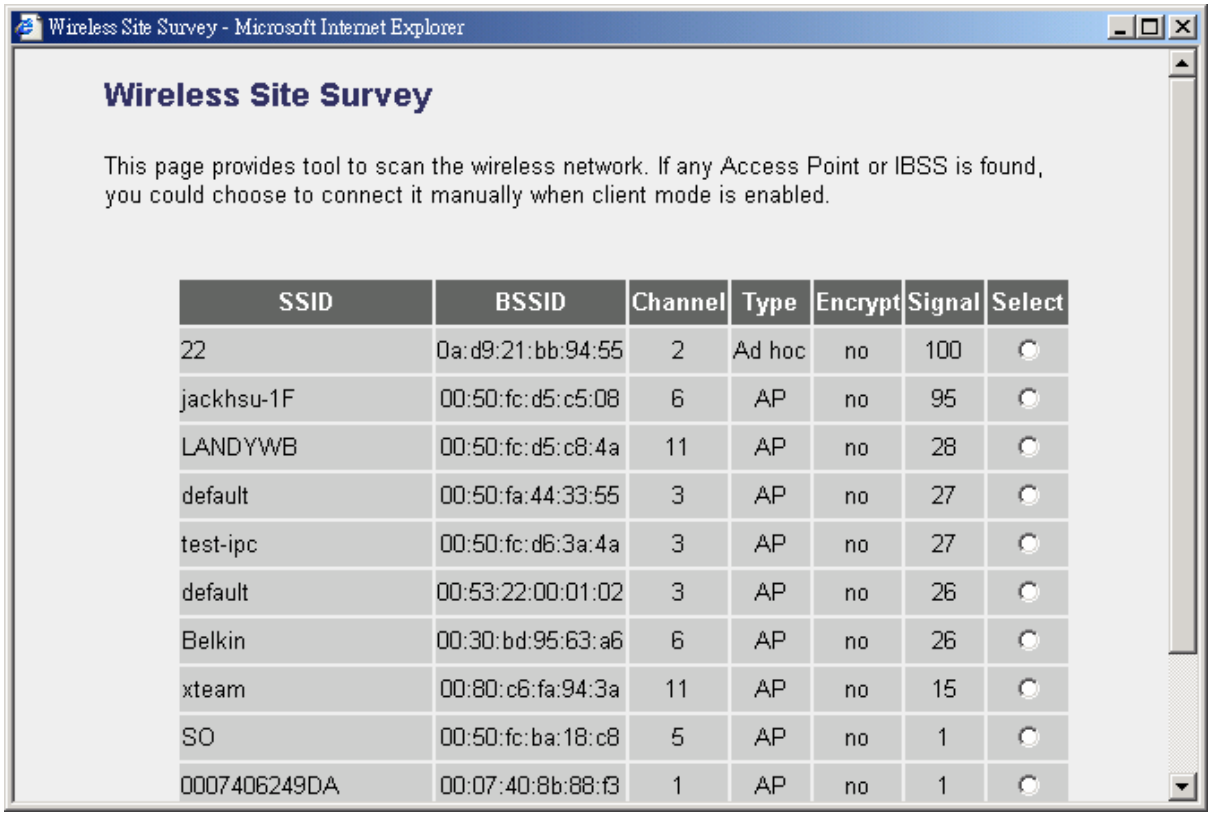


Parameter	Description
MAC Address	MAC address of this active wireless computer.
Tx Packet	The number of transmitted packets that are sent out from this active wireless computer.
Rx Packet	The number of received packets that are received by this active wireless computer.
TX Rate	The transmission rate in Mbps.

Power Saving	Shows if the wireless client is in Power Saving mode.
Expired Time	The time in second before dissociation. If the wireless keeps idle long than the expired time, this access point will dissociate it. The wireless client computer has to associate again when it become active.
Refresh	Refresh the "Active Wireless Client Table".
Close	Refresh the "Active Wireless Client Table".

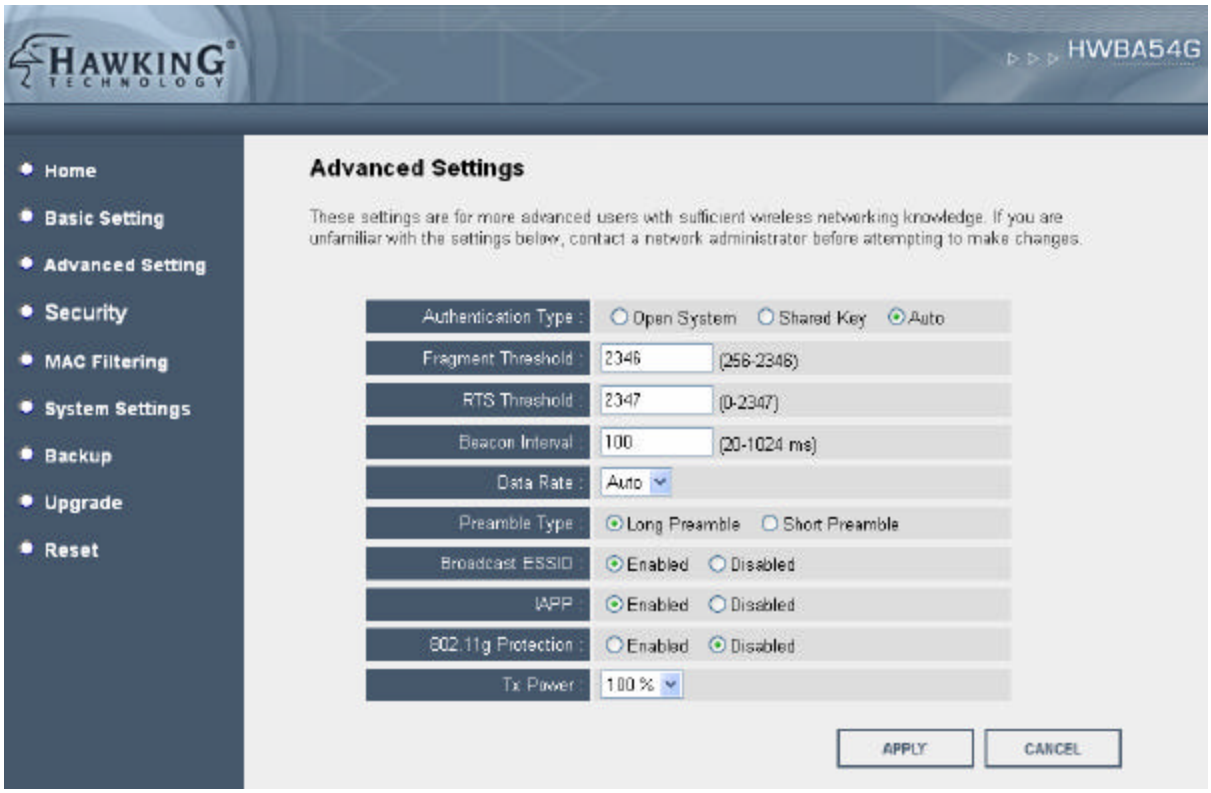
Wireless Site Survey

When using "Ethernet Bridge - Ad Hoc mode" or "Ethernet Bridge - Client mode" the HWBA54G requires a connection to a wireless network to work correctly. Below is a view of the Site Survey tool used to select a network to connect to.



3.2.3 Advanced Settings

For more technical users the HWBA54G offers a wide selection of advanced options. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Tx Operation Rate, Tx Basic Rate, Preamble Type, Broadcast ESSID. If you are unfamiliar with any of these settings, it is strongly recommended that you do not change them.



Parameter	Description
Authentication Type	There are two authentication types: “Open System” and “Shared Key”. When you select “Open System”, wireless computers can associate with this access point without WEP encryption. When you select “Shared Key”, you should also setup a WEP key in the “Encryption” page and wireless computers should use WEP encryption in the authentication phase to associate with this access point. If you select “Auto”, the wireless client can associate with this access point by using any one of these two authentication types.

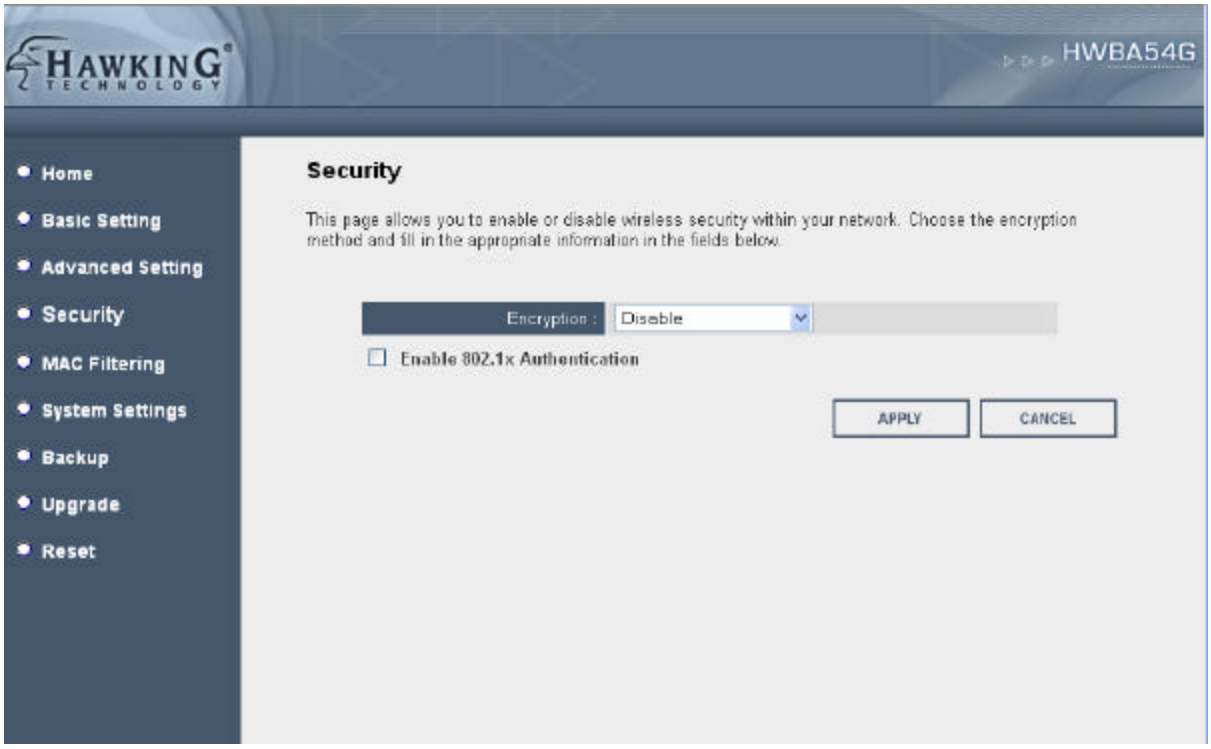
Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
Data Rate	The "Data Rate" is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. "Short Preamble" is suitable for high traffic wireless network. "Long Preamble" can provide more reliable communication.
Broadcast ESSID	If you enable "Broadcast ESSID", every wireless computer located within the coverage of this access point can discover this access point easily. If you are using this device in a public location for public access, enabling this feature is recommended. However, for a private network within close proximity to unauthorized neighboring users, Disabling "Broadcast ESSID" may be a secure option.
IAPP	If you enable "IAPP", the access point will automatically broadcast information of associated wireless computers to its neighbors. This will help wireless computer roaming smoothly between access points. If you have more than one access points in your wireless network and wireless computers have roaming requirements, enabling this feature is recommended. Disabling "IAPP" can provide better security.
802.11g Protection	This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless computers. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.

Click **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.

3.2.4 Security

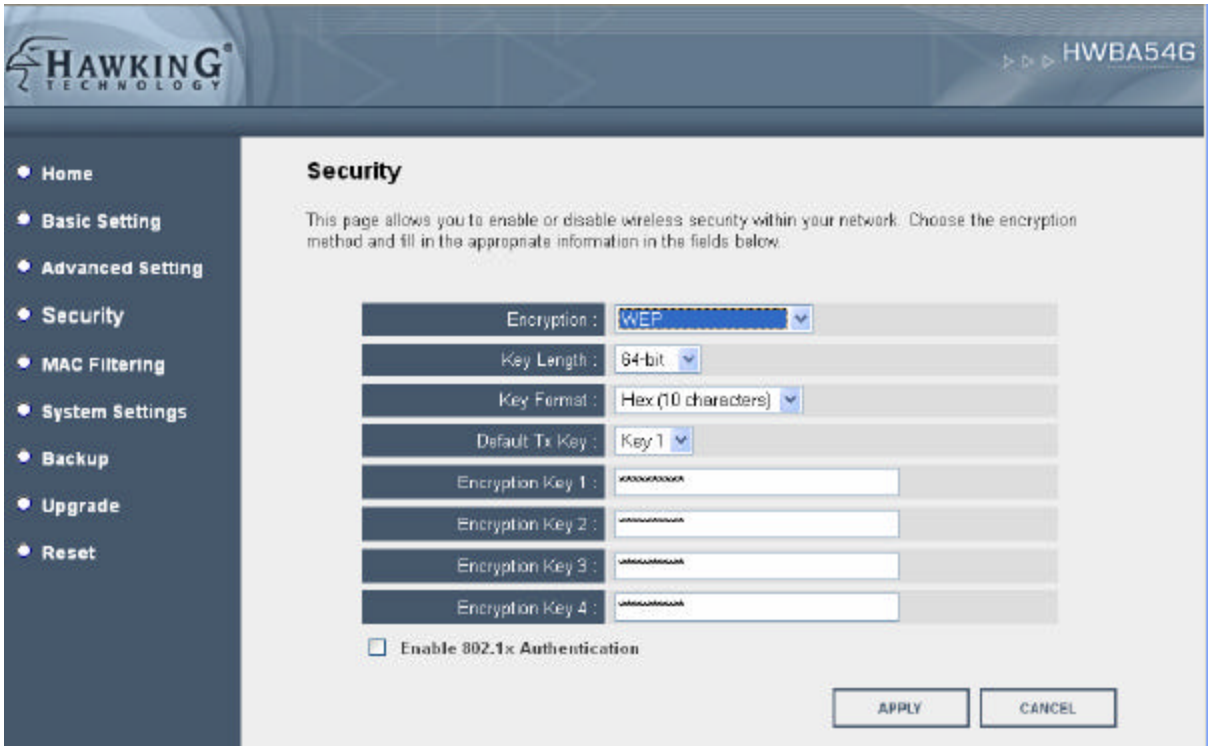
This Access Point provides a complete set of wireless LAN security functions, including WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security features, you can prevent your wireless network from outside intruders.

Note: When using wireless security all computers and devices on the same wireless network must use the same wireless security feature and key.



WEP

WEP encryption uses 64-bit and 128-bit keys to protect your data. You can generate the keys by yourself and enter it. You may enter up to four keys (only one is necessary to work). You can use WEP encryption in "Access Point mode", "Ethernet Bridge - Ad Hoc mode", "Ethernet Bridge - Client mode", and "AP Bridge-WDS mode."



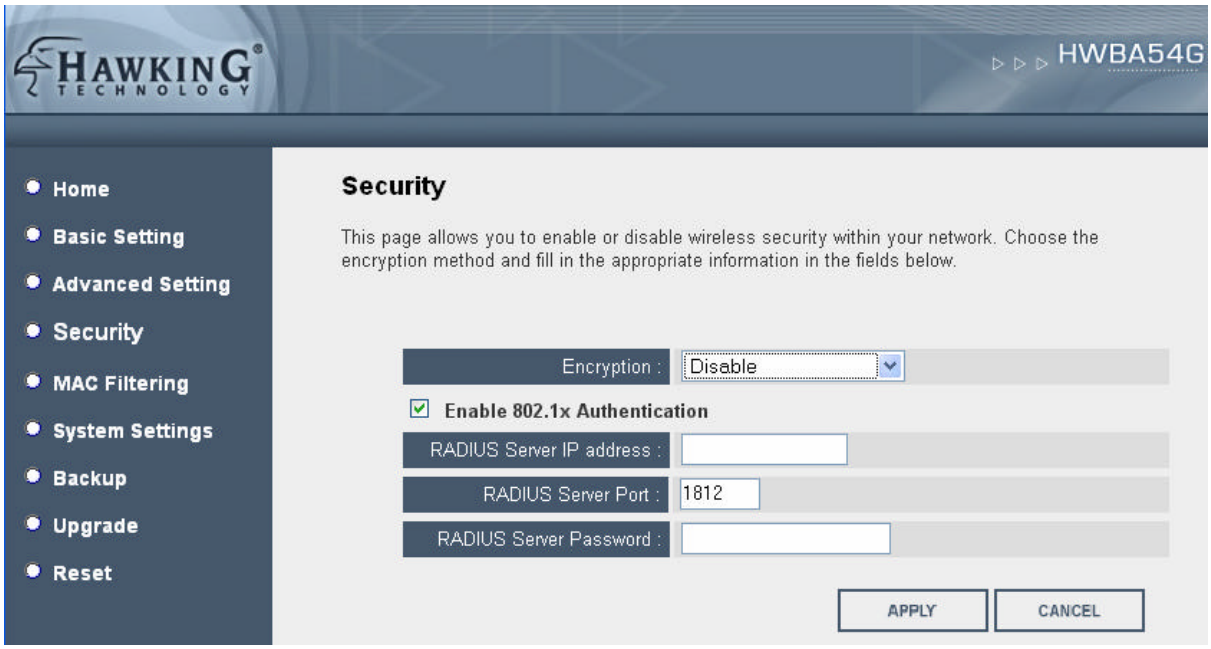
Parameter	Description
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. 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

	it in the “Default key” will take effect.
Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.

Click **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.

802.1x only

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encrypt the data during communication. You can use 802.1x without encryption in “AP mode” and “AP Bridge-WDS mode.”



Parameter	Description
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **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.

802.1x WEP static key

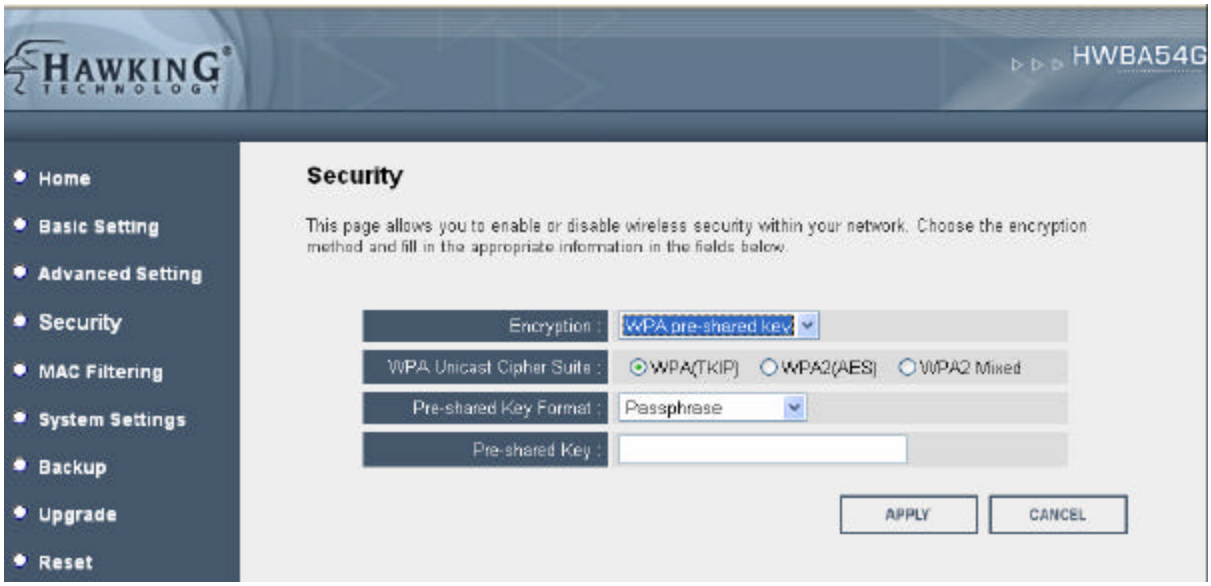
IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication. You can use 802.1x with WEP encryption in “AP mode” and “AP Bridge-WDS mode.”

For the WEP settings, please refer to section “WEP only”. For the 802.1x settings, please refer to section “802.1x only”.

Click **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 computers and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently, making it hard for hackers to crack the key. WPA is more secure than WEP encryption. You can use WPA pre-shared key encryption in “Access Point mode”, “Ethernet Bridge - Ad Hoc mode”, “Ethernet Bridge - Client mode” and “AP Bridge-WDS mode.”



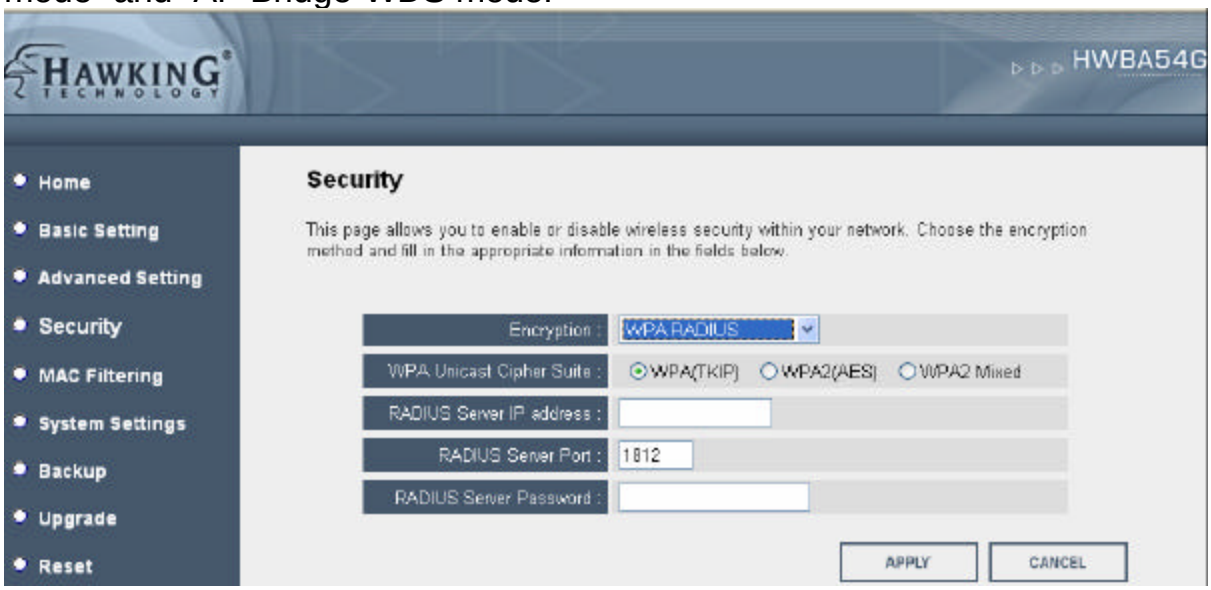
Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.

WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: 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: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Click **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 RADIUS

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless computers and provide the session key to encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. This can improve security very much. You can use WPA RADIUS encryption in "Access Point mode" and "AP Bridge-WDS mode."

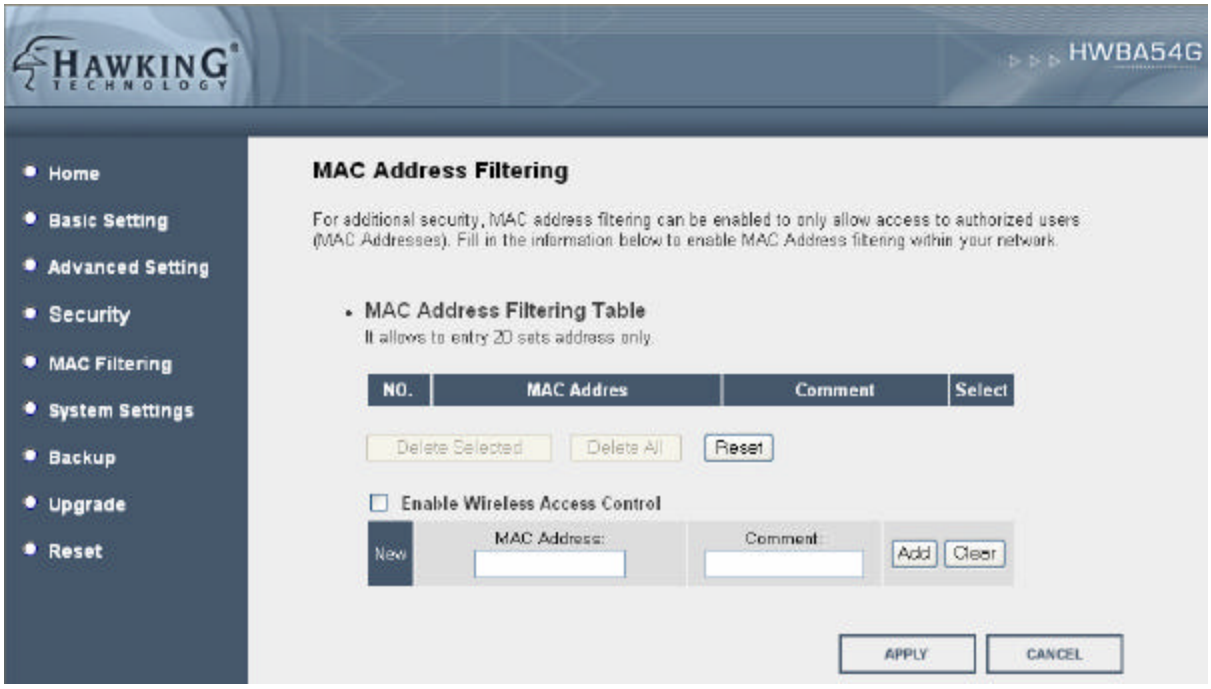


Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **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.

3.2.5 MAC Address Filtering

This Access Point provides MAC Address Filtering, which prevents computers and devices with unauthorized MAC Addresses from accessing your wireless network.



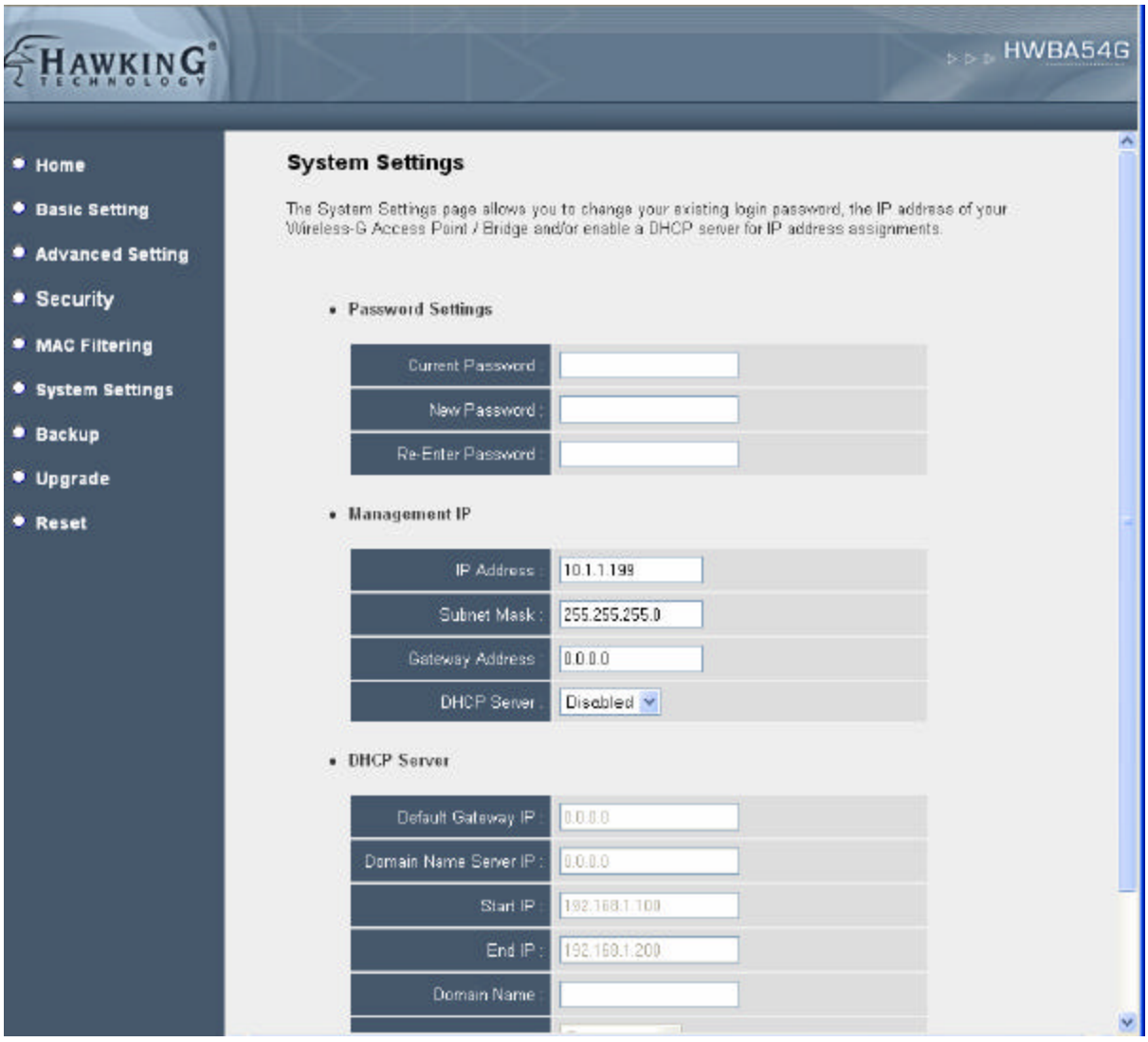
Parameter	Description
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
MAC Address Filtering Table	This table records the MAC addresses of wireless computers you want to allow to access your network. The “Comment” field is the description of the wireless computer associated with the “MAC Address” and is helpful for you to recognize the wireless computer.
Add MAC address into the table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless computer to be added and then click “Add”. Then this wireless computer will be added into the “MAC Address Filtering Table” above. If you find any typo before adding it and want to retype again. Just click “Clear” and both “MAC Address” and “Comment” fields will be cleared.

Remove MAC address from the table	If you want to remove some MAC address from the “MAC Address Filtering Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”. If yo u want remove all MAC addresses from the table, just click “Delete All” button.
Reset	Click “Reset” will clear your current selections.

Click **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.

3.2.6 System Settings

The System Settings page allows for configuration of your passwords, device IP address and DHCP Server.



Parameter	Description
Current Password	Enter the current password (up to 15-digit alphanumeric string) of the Access Point. The default password for the Access Point is **1234**. Note that the password is casesensitive.

New Password	Enter the password (up to 15 -digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
Re-Enter Password	Reconfirm the password (up to 15-digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
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 Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
Gateway Address	The IP address of the default gateway of the subnet that this access point resides in. It allows this access point be accessed by PC from deferent subnet to do configuration.
DHCP Server	Enable or disable the DHCP Server.

Click **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.

DHCP Server Setting

A DHCP Server automatically assigns IP addresses to devices or computers connecting to the Access Point. Before enabling this feature you should check to make sure that your network router does not already have a DHCP server running to avoid and conflicts.

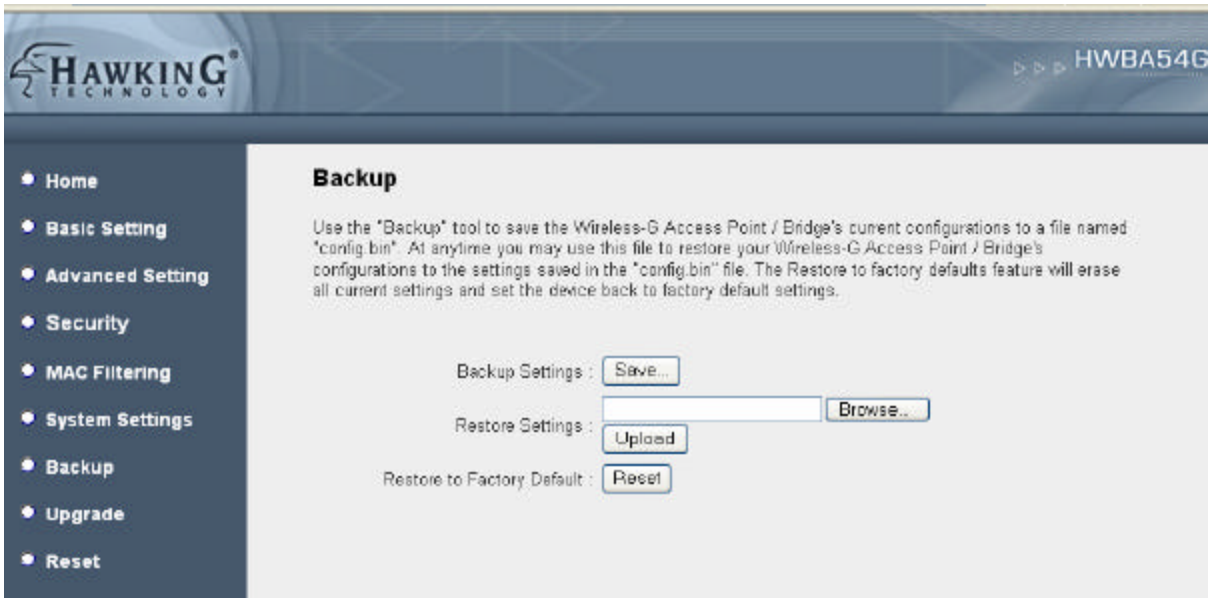
Parameter	Description
Default Gateway IP	Specify the gateway IP in your network. This IP address should be different from the Management IP.
Domain Name Server IP	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.

Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.1.100** to End IP **192.168.1.200**.
Domain Name	You can specify the Domain Name for your Access Point.
Lease Time	The DHCP Server when enabled will temporarily give your LAN client an IP address. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN clients. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

Click **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.

3.2.7 Backup Tool

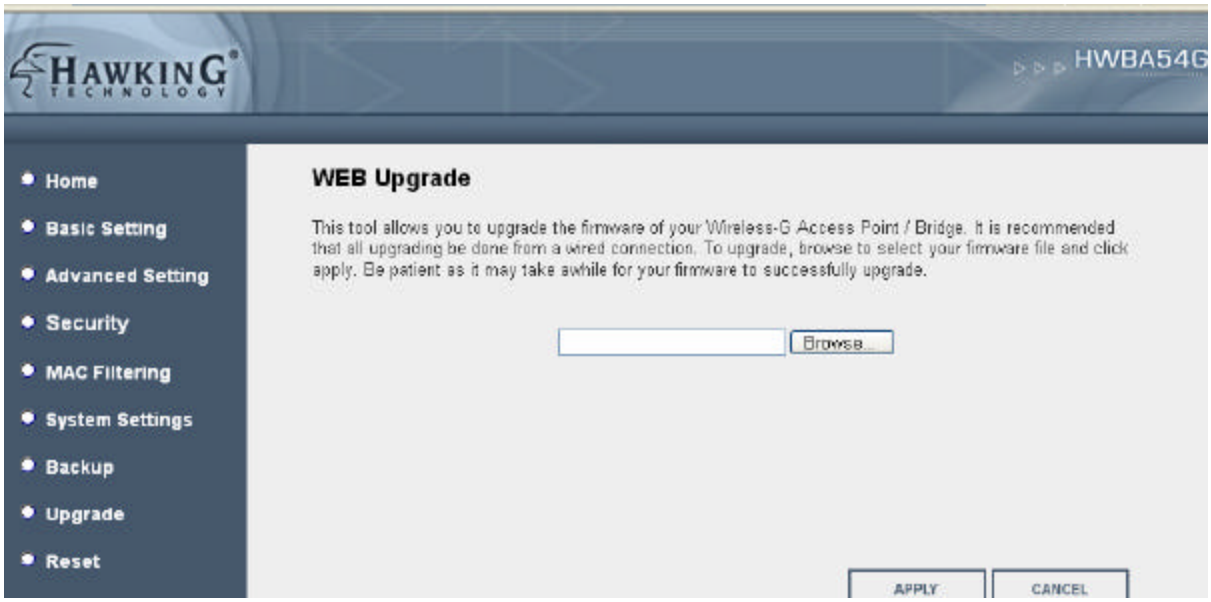
The Backup feature allows you to save (**Backup**) the Access Point's current configuration setting. Saving the configuration settings provides an added protection and convenience should problems occur with the Access Point and you have to reset to factory default. When you save the configuration setting (Backup) 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 its original default settings (e.g. when you first purchased the Access Point).



Parameter	Description
Configuration Tools	Use the "**Backup**" tool to save the Access Point's current configuration to a file named "config.bin" on your PC. You can then use the "**Restore**" tool to upload and restore the saved configuration to the Access Point. Alternatively, 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.

3.2.8 Firmware Upgrade

This page allows you to upgrade the Access Point's firmware.

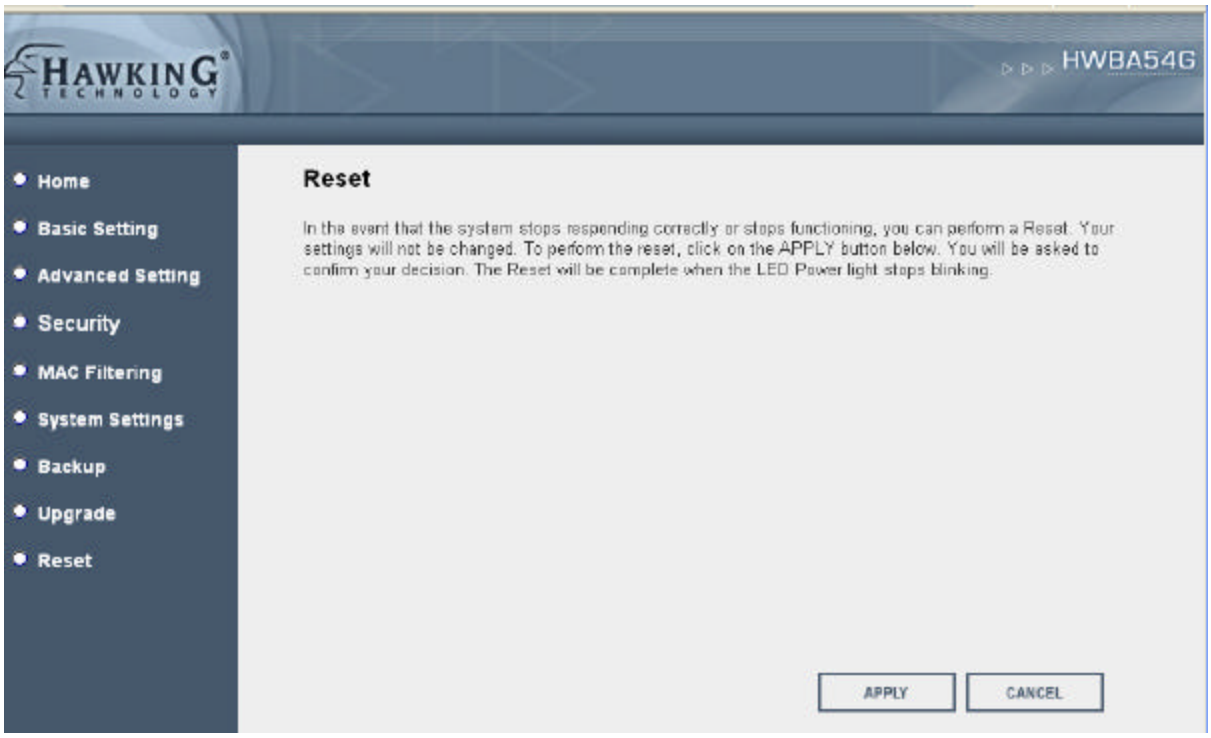


Parameter	Description
Firmware Upgrade	This tool allows you to upgrade the Access Point's system firmware. To upgrade the firmware of your Access Point, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the **Browse** button to find the firmware file on your PC. Please reset the Access Point when the upgrade process is complete.

Once you've selected the new firmware file, click **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.

3.2.9 Reset

You can reset the Access Point's system should any problem exist. The reset function essentially Re-boots your Access Point's system.



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

Chapter 4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the Access Point.

1. How to manually find your PC's IP and MAC Address?

1) In Windows, open the Command Prompt program
2) Type **Ipconfig /all** and **Enter**
   - Your PC's IP address is the one entitled **IP address**
   - Your PC's MAC Address is the one entitled **Physical Address**

2. What is Ad-hoc?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN without a central access point or router.

3. What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration.

4. What is BSS ID?

A group of wireless computers and an Access Point compose a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

5. What is ESSID?

An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while maintaining a continuous connection to the wireless network computers and the Wireless LAN Access Points.

6. 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 technology, it has the inherent scrambling security feature. On the software side, the WLAN series offers the encryption function (WEP, WPA, WPA2) to enhance security and access control.

7. What is WEP?

WEP stands for Wired Equivalent Privacy, a data privacy mechanism based on a 64(40)-bit shared key algorithm.

8. What is WPA?

WPA is an acronym for Wi-Fi Protected Access. It is a security protocol for 802.11 wireless networks. WPA can provide data protection with the use of encryption and the use of access controls and user authentication.

9. What is WPA2?

In addition to WPA, WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES).

10. 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.