9. On the *SECURITY TYPE* screen, select the appropriate level of WEP encryption, **64-BIT WEP** or **128-BIT WEP**.

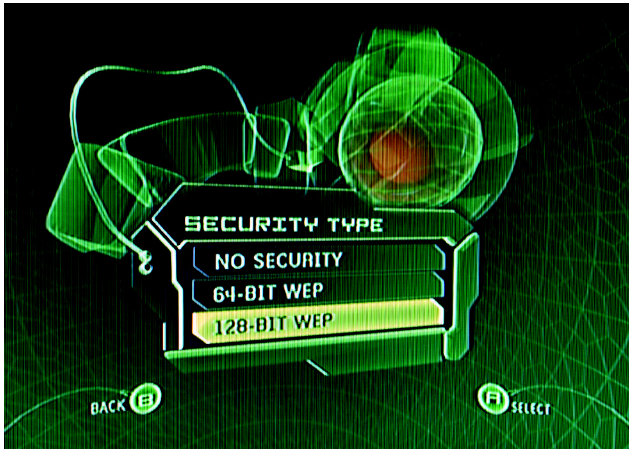
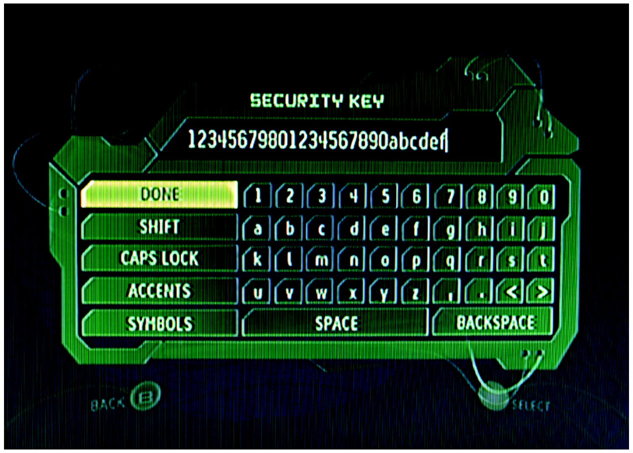


Figure 6-11: Xbox's SECURITY TYPE Screen

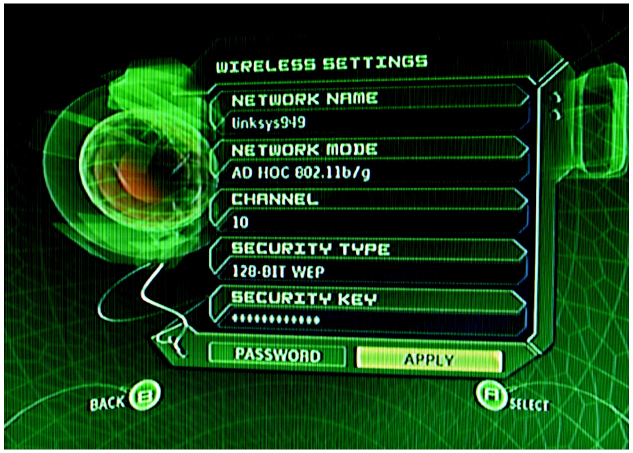
10. On the *SECURITY KEY* screen, enter the WEP key in hexadecimal characters and then select **DONE**. The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.


SECURITY KEY

12345679801234567890abcdef

Figure 6-12: Xbox's SECURITY KEY Screen

11. On the *WIRELESS SETTINGS* screen, select **APPLY** to save your new settings.



WIRELESS SETTINGS

NETWORK NAME
linksys949

NETWORK MODE
AD HOC 802.11b/g

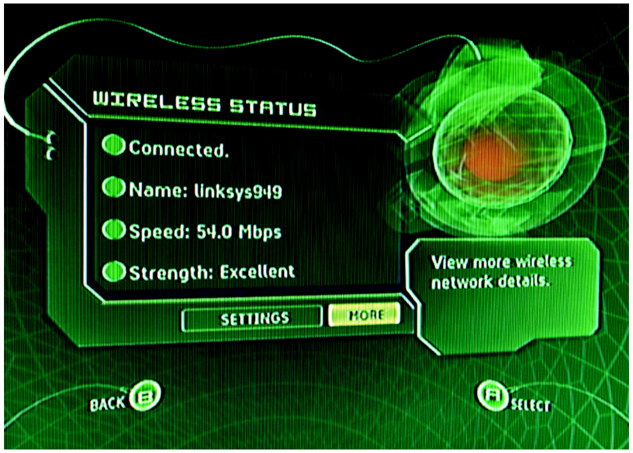
CHANNEL
10

SECURITY TYPE
128-BIT WEP

SECURITY KEY
••••••••••••

Figure 6-13: Xbox's WIRELESS SETTINGS Screen

12. On the *WIRELESS STATUS* screen, click **MORE** to see additional details.



WIRELESS STATUS

Connected.

Name: linksys949

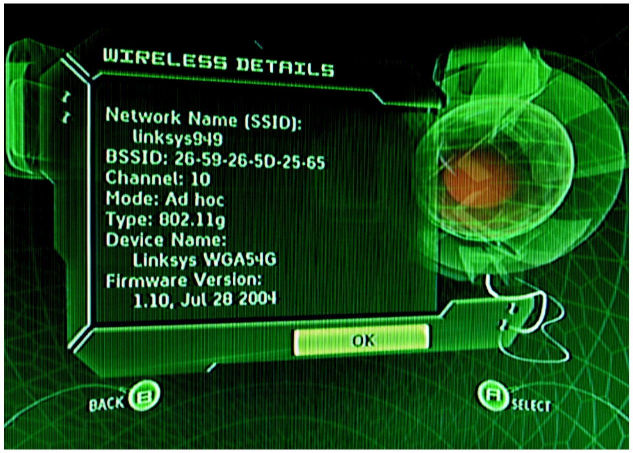
Speed: 54.0 Mbps

Strength: Excellent

View more wireless network details.

Figure 6-14: Xbox's WIRELESS STATUS Screen

13. After you have reviewed the network settings, click **OK** to exit this screen,



WIRELESS DETAILS

Network Name (SSID):
linksys949
BSSID: 26-59-26-5D-25-65
Channel: 10
Mode: Ad hoc
Type: 802.11g
Device Name:
Linksys WGA54G
Firmware Version:
1.10, Jul 28 2004

Figure 6-15: Xbox's WIRELESS DETAILS Screen

14. Go back to the Xbox main menu, and set your Xbox to multiplayer gaming.

Congratulations! The installation of the Wireless A/G Game Adapter is complete.

Chapter 7: Using the Wireless A/G Game Adapter Web Configuration Utility

Overview

This chapter will describe each web page of the Utility and each page's key functions. You can use the Utility to change the Game Adapter's settings. You can also restore the Game Adapter to its factory default settings, change the password used to access its Utility, and upgrade its firmware.

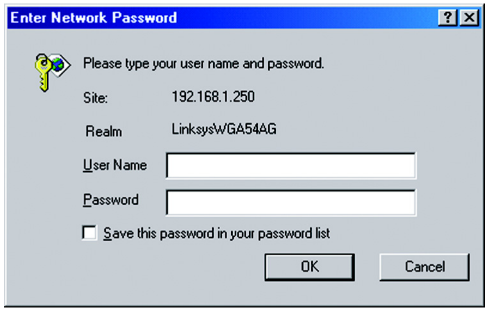
Accessing the Web Configuration Utility

To access the Game Adapter's Utility, launch Internet Explorer or Netscape Navigator, and enter the Game Adapter's default IP address, **192.168.1.250**, in the *Address* field. Press the **Enter** key.

NOTE: If your network router automatically assigns IP addresses, then the Game Adapter's IP address may have changed. Refer to your router's documentation for instructions on how to find the Game Adapter's current IP address (you may need to view the router's DHCP client table).

A screen will appear asking you for your User Name and Password. Leave the *User Name* field blank, and enter **admin** in the *Password* field. Then click the **OK** button.

Make the necessary changes through the Utility. When you have finished making changes to a screen, click the **Apply** button to save the changes, or click the **Cancel** button to undo your changes. For help information on a tab, click **Help**.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.250

Realm LinksysWGA54AG

User Name

Password

□ Save this password in your password list

Figure 7-1: Utility's Enter Network Password Screen

The Setup Tab

The *Basic Setup* screen is the first screen you see when you access the Utility.

Firmware - This shows the version number and date of the firmware that is currently installed.

MAC - The MAC address of the Game Adapter is displayed here.

Network Type - Select the type of network you are using, **Wireless-G Mode** (for 802.11g and/or 802.11b networking) or **Wireless-A Mode** (for 802.11a networking).

SSID - Enter the SSID or name of your wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not include more than 32 keyboard characters.

Network Type - Select the mode of your wireless network, **Infrastructure** or **Ad-Hoc**. Infrastructure mode is used when wireless and wired devices communicate using a wireless access point. Ad-Hoc mode is used when multiple wireless devices communicate directly with each other, such as when playing head-to-head games.

If you have selected Ad-Hoc for the Network Type, then select the channel of your wireless network from the *Channel* drop-down menu.

Security - If you do not want to use wireless security, keep the default setting, **Disabled**. If you want to use WEP encryption, select **Enabled** and click the **Edit Wireless Security** button. For instructions on how to configure the security settings, refer to the following section about the *WEP Encryption* screen.

Status - This indicates the status of the Game Adapter's connection to your wireless network.

A list of wireless networks is displayed at the bottom of the screen. Their SSIDs, MAC addresses, Channel settings, Signal Strength ratings, and Modes are shown.

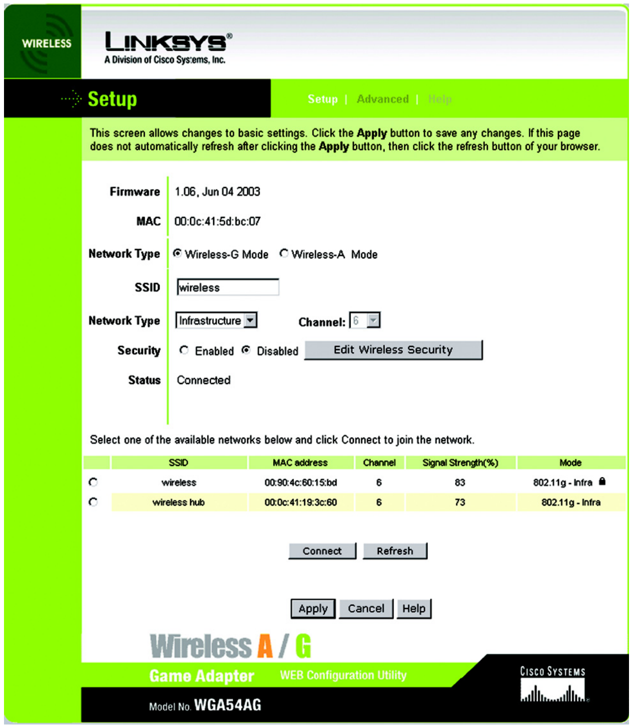
SSID - This is the name of the wireless network.

MAC Address - This is the MAC address of the network's access point.

Channel - The Channel setting of the wireless network is shown here.

Signal Strength (%) - Displayed here is the percentage of wireless signal strength available.

Mode - Shown here are the wireless standard and mode used by the network. A lock is displayed if the network has its wireless security enabled.



This screen allows changes to basic settings. Click the **Apply** button to save any changes. If this page does not automatically refresh after clicking the **Apply** button, then click the refresh button of your browser.

Firmware 1.06, Jun 04 2003

MAC 00:0c:41:5d:bc:07

Network Type ● Wireless-G Mode ○ Wireless-A Mode

SSID wireless

Network Type Infrastructure Channel: 6

Security ○ Enabled ● Disabled

Status Connected

Select one of the available networks below and click Connect to join the network.

	SSID	MAC address	Channel	Signal Strength(%)	Mode
○	wireless	00:90:4c:60:15:bd	6	83	802.11g - Infra 🔒
○	wireless hub	00:0c:41:19:3c:60	6	73	802.11g - Infra

Model No. WGA54AG

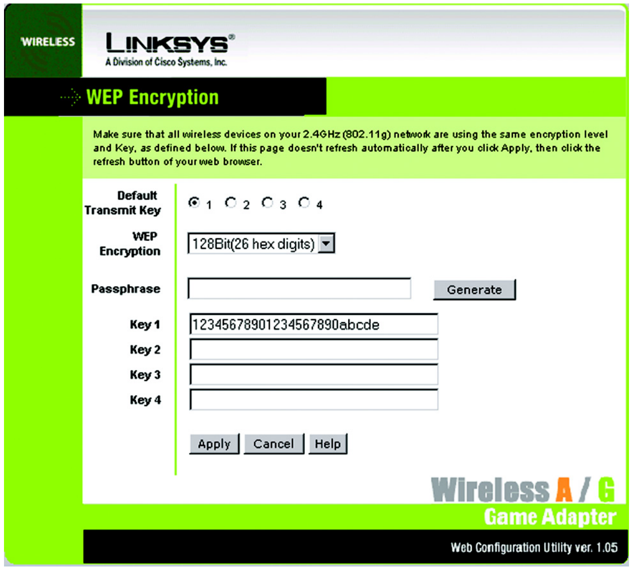
Figure 7-2: Utility's Setup Screen

To connect to one of these networks, select a network and then click the **Connect** button. If you want to update this list of wireless networks, click the **Refresh** button.

When you have finished making changes, click the **Apply** button to save your changes, or click the **Cancel** button to undo your changes. For help information, click **Help**.

WEP Encryption

Use the *WEP Encryption* screen to change the Game Adapter's wireless security settings.



Make sure that all wireless devices on your 2.4GHz (802.11g) network are using the same encryption level and Key, as defined below. If this page doesn't refresh automatically after you click Apply, then click the refresh button of your web browser.

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

WEP Encryption: 128Bit(26 hex digits)

Passphrase:

Key 1: 12345678901234567890abcde

Key 2:

Key 3:

Key 4:

Figure 7-3: Utility's WEP Encryption Screen

Default Transmit Key - The default transmit key number is 1. If your network's access point uses transmit key number 2, 3, or 4, select the appropriate radio button.

WEP Encryption- Select the level of WEP encryption, **64Bit (10 hex digits)** or **128Bit (26 hex digits)**, from the drop-down menu.

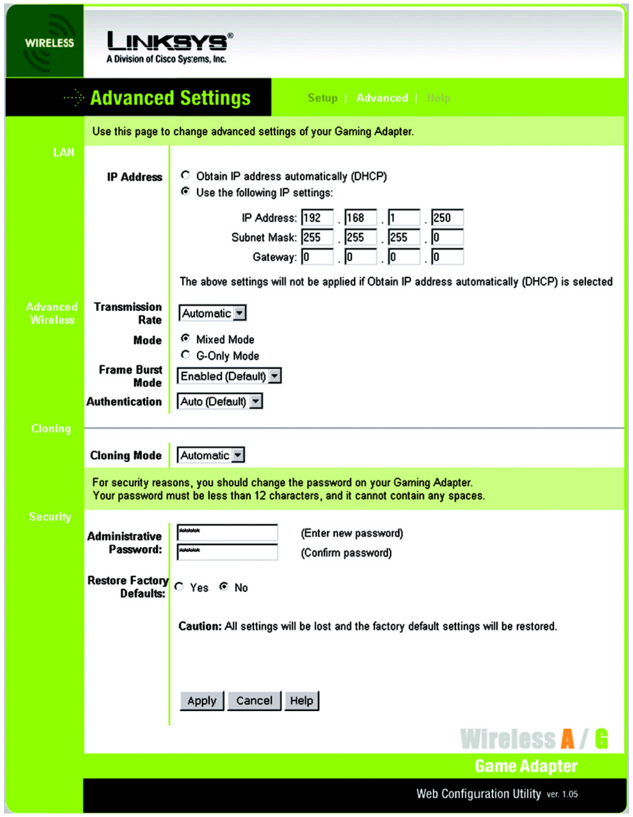
Passphrase - To automatically generate one or more WEP keys, enter a passphrase in the *Passphrase* field and click the **Generate** button. The passphrase is case-sensitive and should not have more than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

Key 1-4 - If you want to manually enter the WEP key, enter it in the appropriate field. The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

When you have finished making changes, click the **Apply** button to save your changes, or click the **Cancel** button to undo your changes. For help information, click **Help**.

The Advanced Settings Tab

Use the *Advanced Settings* screen to change the Game Adapter's advanced wireless settings, clone a MAC address onto the Game Adapter, change the password, or restore its default settings.



Use this page to change advanced settings of your Gaming Adapter.

IP Address: ○ Obtain IP address automatically (DHCP) ● Use the following IP settings:

IP Address: 192 . 168 . 1 . 250
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 0 . 0 . 0 . 0

The above settings will not be applied if Obtain IP address automatically (DHCP) is selected

Transmission Rate: Automatic
Mode: ● Mixed Mode ○ G-Only Mode
Frame Burst Mode: Enabled (Default)
Authentication: Auto (Default)

Cloning Mode: Automatic

For security reasons, you should change the password on your Gaming Adapter.
Your password must be less than 12 characters, and it cannot contain any spaces.

Administrative Password: ****** (Enter new password)
****** (Confirm password)

Restore Factory Defaults: ○ Yes ● No

Caution: All settings will be lost and the factory default settings will be restored.

Figure 7-4: Utility's Advanced Settings Screen

LAN

IP Address - Select **Obtain IP address automatically (DHCP)** if your network router automatically assigns IP addresses. Select **Use the following IP settings** if you want to assign a static or fixed IP address to the Game Adapter. Then enter the IP Address, Subnet Mask, and Gateway address in the fields provided.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Game Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Gateway - Enter the IP address of your network's Gateway here.

Advanced Wireless

Transmission Rate - The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or keep the default setting, **Automatic**, to have the Game Adapter automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Game Adapter and your wireless router or access point.

Mode - This setting is available only for Wireless-G (2.4GHz, 802.11g) and/or Wireless-B (2.4GHz, 802.11b) networking. From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-G and Wireless-B devices in your network, keep the default setting, **Mixed Mode**. If you have only Wireless-G devices in your network, select **G-Only Mode** for maximum network speeds.

Frame Burst Mode - Enabling this mode should improve your network's performance by reducing packet overhead, depending on which wireless products you are using. If you are not sure how to use this option, keep the default, **Enabled**. Otherwise, select **Disabled** if you do not want to use the Frame Burst Mode.

Authentication - The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. For Open System authentication, the sender and recipient do NOT use a WEP key for authentication. For Shared Key authentication, the sender and recipient use a WEP key for authentication. Select the authentication method your network is using, **Open System** or **Shared Key**. If you are not sure which method to select, keep the default, **Auto**.

Cloning

Cloning Mode - The MAC cloning feature allows you to clone the MAC address of the device currently connected to the Game Adapter's Network port. The Game Adapter will actively scan for a new MAC address to be cloned whenever you disconnect and re-connect the Game Adapter through its Network port. The default setting, **Automatic**, enables the MAC cloning feature. To disable MAC address cloning, select **Disabled**.

Security

Administrative Password - You should always change the Game Adapter's password from its factory default, **admin**. All users who try to access the Game Adapter's Utility will be prompted for the Game Adapter's password. Enter the new password in the first field, and then re-enter the password in the second field to confirm it.

Restore Factory Defaults - To clear all of the Game Adapter's settings and reset them to their factory defaults, click the **Yes** radio button. If you do not want to restore the factory defaults, keep the default setting, **No**.

NOTE: Before restoring the Game Adapter's factory defaults, write down its current settings in case you need these settings later.

When you have finished making changes, click the **Apply** button to save your changes, or click the **Cancel** button to undo your changes. For help information, click **Help**.

The Help Tab

The *Help* screen offers links to the Linksys website, the online version of this User Guide, and the Adobe website. You can also use this screen to upgrade the Game Adapter's firmware.

NOTE: Firmware should be upgraded ONLY if you experience problems with the Game Adapter.

Linksys Website - Click this link to visit *www.linksys.com*.

Online manual in PDF format - Click this link to view the online version of this User Guide. It is in Adobe Acrobat Portable Document File (pdf) format, so you will need the free Adobe Acrobat Reader to view the pdf. If you do not have the Reader, click the **Adobe Website** link to download it.

Adobe Website (to obtain a PDF reader if required) - If you need to download the Adobe Acrobat Reader to view the pdf of the User Guide, then click this link.

Firmware Upgrade - Before upgrading the Game Adapter's firmware, write down its settings because they may be reset to their factory defaults when the firmware is upgraded.

To upgrade the Game Adapter's firmware, follow these instructions:

1. Download the Game Adapter's firmware upgrade zip file from *www.linksys.com*.

2. Extract the zip file on your computer.

3. On the *Help* screen, click the **Firmware Upgrade** button and follow the on-screen instructions.

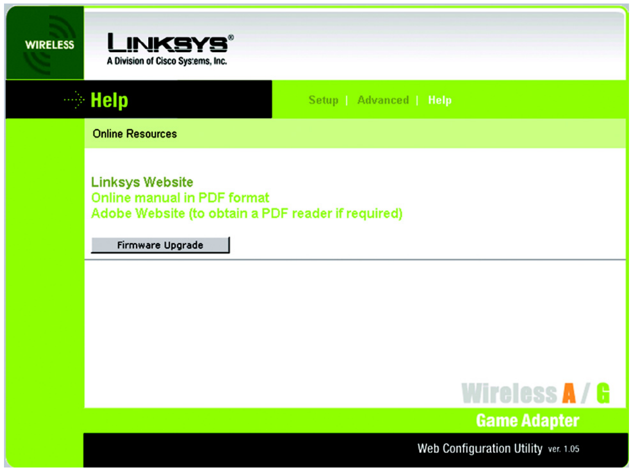

WIRELESS
LINKSYS®
A Division of Cisco Systems, Inc.
Help
Setup | Advanced | Help
Online Resources
Linksys Website
Online manual in PDF format
Adobe Website (to obtain a PDF reader if required)
Firmware Upgrade
Wireless A / G
Game Adapter
Web Configuration Utility ver. 1.05

Figure 7-5: Utility's Help Screen

Appendix A: Troubleshooting

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." This appendix provides solutions to problems that may occur during the installation and operation of the Wireless A/G Game Adapter. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. ***I cannot connect to the Game Adapter.***
   Follow these instructions:
   1. Open the Web Configuration Utility. (Refer to "Chapter 7: Using the Wireless A/G Game Adapter Web Configuration Utility" for more details.)
   2. On the *Setup* screen, make sure that the SSID is the same as the SSID of your wireless network.
   3. Click the **Edit Wireless Security** button.
   4. On the *WEP Encryption* screen, make sure that all of the WEP settings are the same as the WEP settings of your wireless network.

2. ***I don't know how to change the Game Adapter's IP address.***
   1. Open the Web Configuration Utility. (Refer to "Chapter 7: Using the Wireless A/G Game Adapter Web Configuration Utility" for more details.)
   2. On the *Advanced Settings* screen, select **Use the following IP settings**.
   3. Enter the Game Adapter's new IP address in the *IP Address* fields.
   4. Click the **Apply** button to save the new IP address.
   5. If you encounter problems, power the Game Adapter off and on again, or push the Reset button. Then try to change its IP address again.

3. ***The Setup Wizard doesn't seem to work properly.***
   Make sure that the Game Adapter's back panel switch is set the Infra position. Then run the Setup Wizard again.

4. ***I used the "Fast Setup" instructions for my two Adapters, but the multiplayer gaming doesn't work.***
   Follow these instructions:
   1. Unplug the power from both Adapters.
   2. Set the Game Adapter's back panel switch to the Adhoc A position if you are using a Wireless-A (802.11a) network, or set the switch to the Adhoc B position if you are using a Wireless-G and/or B (802.11g and/or 802.11b) network.
   3. Power on one Game Adapter.

4. Wait 30 seconds.
5. Set the second Game Adapter's back panel switch to the Adhoc A position if you are using a Wireless-A (802.11a) network, or set the switch to the Adhoc B position if you are using a Wireless-G and/or B (802.11g and/or 802.11b) network.
6. Power on the second Game Adapter.

The Game Adapter should now work properly.

Frequently Asked Questions

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play computer games with other members of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What is the IEEE 802.11a standard?
It is one of the IEEE standards for wireless networks. The 802.11a standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11a standard. The 802.11a standard states a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

mbps: *one million bits per second; a unit of measurement for data transmission.*

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11a features are supported?

The product supports the following IEEE 802.11a functions:

- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11b functions:

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

What IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

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

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

fragmentation: *breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.*

What is roaming?

Roaming is the ability of a portable computer to communicate continuously while it and its user are moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the user must make sure that the workstation is set to the same channel number used by the access point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

ism band: *radio bandwidth utilized in wireless transmissions.*

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

spread spectrum: *wideband radio frequency technique used for more reliable and secure data transmission.*

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-

dsss: *Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.*

Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

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

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a shared key algorithm, as described in the IEEE 802.11 standard. For more information, refer to “Appendix B: Wireless Security.”

Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (as shown in this User Guide) (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

Note: Some of these security features are available only through the network router or access point. Refer to the router or access point's documentation for more information.

To ensure network security, steps one through five should be followed, at least.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for “beacon messages”. These messages can be easily decrypted and contain much of the network’s information, such as the network’s SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

Important: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

WPA Pre-Shared Key. If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA RADIUS. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - A method that uses up to 256-bit key encryption to secure data.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**D**e**mi**litarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation -Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack**-45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (**R**equest **T**o **S**end) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a “program”.

SOHO (**S**mall **O**ffice/**H**ome **O**ffice) - Market segment of professionals who work at home or in small offices.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects every incoming packet of information before allowing it to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (**U**ser **D**atagram **P**rotocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - A wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix D: Specifications

Model	WGA54AG
Standards	IEEE 802.11a, 802.11b, 802.11g
Ports	Power, Network
Button/Switch	Reset, Network Mode (Infra, AdHoc-A, AdHoc-B)
Cabling Type	Category 5
LEDs	Power, Ethernet, Wireless
Transmit Power	14dBm ± 1dBm
Security Features	WEP
WEP Key Bits	64, 128
Warranty	3 Years
Dimensions	6.30" x 3.94" x 1.42" (160 mm x 100 mm x 36 mm)
Unit Weight	6.98 oz. (0.20 kg)
Power	12V 1A
Certifications	FCC, IC-03
Operating Temp.	32 ~ 104°F (0 ~ 40°C)
Storage Temp.	-4 ~ 158°F (-20 ~ 70°C)

Operating Humidity	10~85% Non Condensing
Storage Humidity	5~90% Non Condensing

Appendix E: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of three years (the “Warranty Period”), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix F: Regulatory Information

FCC STATEMENT

This product has been tested and complies with the specifications 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 according to 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 is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna

Increase the separation between the equipment or devices

Connect the equipment to an outlet other than the receiver's

Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Operation within the 5150 to 5250GHz band is restricted to indoor use only.

•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.□
□
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.

Linksys declares that WGA54AG (FCC ID: Q87-WGA54AG) is limited in □
CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

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 and your body.
•This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
SAFETY NOTICES

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.

Do not use this product near water, for example, in a wet basement or near a swimming pool.

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

To prevent radio interference to the licensed service (i.e. □
co-channel Mobile Satellite systems) this device is intended to be
operated indoors and away from windows to provide maximum □
shielding. Equipment (or its transmit antenna) that is installed □
outdoors is subject to licensing.□
Because high power radars are allocated as primary users □
(meaning they have priority) in 5250-5350 MHz, these radars □
could cause interference and/or damage to license exempt LAN □
devices.□
Operation is subject to the following two conditions:□
1) This device may not cause interference and□
2) This device must accept any interference, including □
interference that may cause undesired operation of the device.□

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that this product conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.

EN 609 50 Safety

EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys vakuuttaa täten että dieses produkt tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys déclare que le produit est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France:

2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le départment. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

Appendix G: Contact Information

Need to contact Linksys?
Visit us online for information on the latest products and updates
to your existing products at: http://www.linksys.com or
ftp.linksys.com

Can't find information about a product you want to buy
on the web? Do you want to know more about networking
with Linksys products? Give our advice line a call at: 800-546-5797 (LINKSYS)
Or fax your request in to: 949-823-3002

If you experience problems with any Linksys product,
you can call us at: 800-326-7114
Don't wish to call? You can e-mail us at: support@linksys.com

If any Linksys product proves defective during its warranty period,
you can call the Linksys Return Merchandise Authorization
department for obtaining a Return Authorization Number at: 949-823-3000
(Details on Warranty and RMA issues can be found in the Warranty
Information section in this Guide.)