

## The Profiles Tab

The Profiles screen lets you save different configuration profiles for different network setups. You can also import or export profiles. The default profile holds the initial configuration saved when you ran the Setup Wizard.

**Profile** - Name of the connection profile.

**SSID** - The wireless network's unique name, as set in the connection profile.

### Profile Information

**Wireless Mode** - The mode of the wireless network currently in use.

**Transfer Rate** - The data transfer rate of the current connection. (In Auto mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)

**Channel** - The channel to which the wireless network devices are set.

**WEP** - The status of the WEP encryption security feature.

**Authentication** - The authentication setting for the network.

**Connect** - To connect to a wireless network using a specific profile, select the profile, and click the **Connect** button.

**New** - Click the **New** button to create a new profile. See the next section, "Creating a New Profile," for detailed instructions.

**Edit** - Select a profile, and click the **Edit** button to change an existing profile.

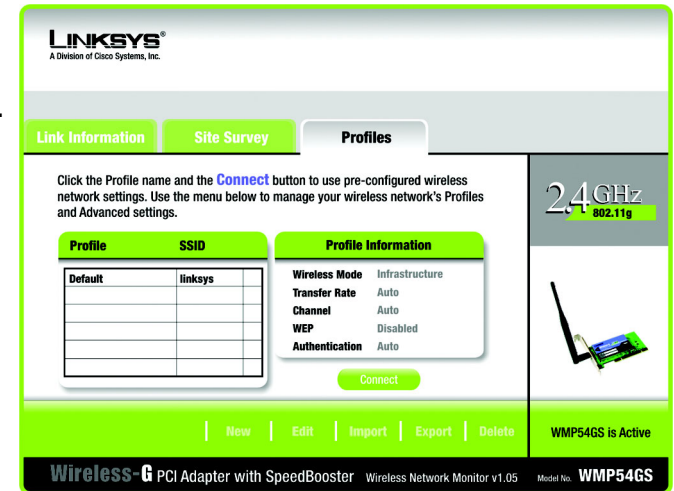


**Figure 6-5: The Profiles Tab**

**Import** - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file and click the **Open** button.

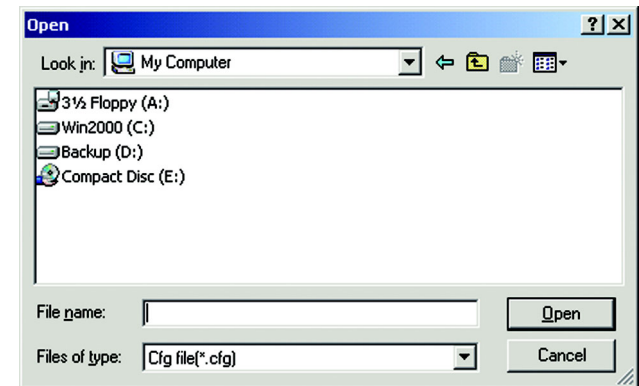


Figure 6-6: Importing a Profile

**Export** - To save the profile(s) in a different location, click the **Export** button. Direct Windows to the appropriate folder and click the **OK** button.

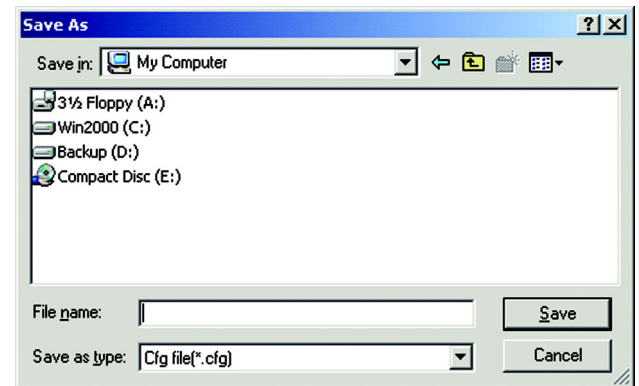


Figure 6-7: Exporting a Profile

**Delete** - Click the **Delete** button to delete a profile.

Click the **X** (Close) button in the upper right corner to exit the Wireless Network Monitor.

## Creating a New Profile

1. On the *Profiles* tab, click the **New** button to create a new profile.

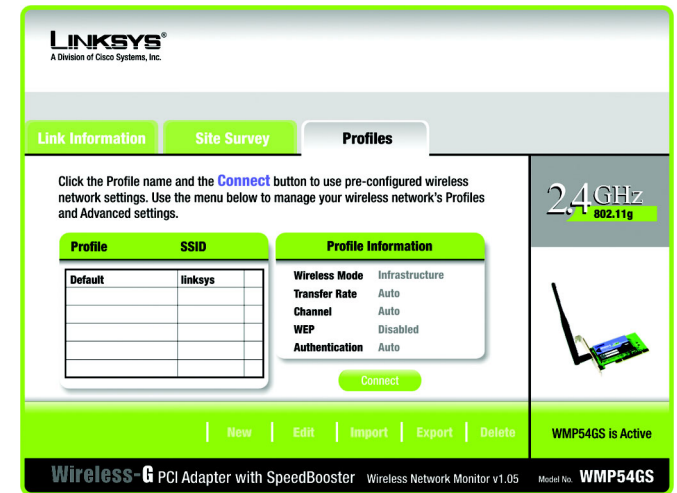


Figure 6-8: The Profiles Tab

2. When the Create connection profile screen appears, enter a name for the new profile. Click **OK** to save the profile name or click **Cancel** to return to the previous screen.



Figure 6-9: Create Connection Profile

3. Enter your network's settings on the *Network Settings* screen, which appears next.

If your network has a DHCP server (or Router), click the radio button next to **Obtain an IP address automatically (DHCP)** and click the **Next** button to continue.

If your network does not have a DHCP server (or router), click the radio button next to **Specify the IP address**. Enter an **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS** appropriate for your network. Enter each address in this format: xxx.xxx.xxx.xxx (the x's represent the numbers that make up each address). You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, then leave these fields alone.

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

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

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

**DNS** - Enter the DNS addresses of your network here.

Click the **Next** button to continue or the **Cancel** button to return to the previous screen.

Figure 6-10: Profiles - Network Settings

4. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want your wireless computers to communicate with computers on your wired network via a wireless access point, and continue to Step 6. Click the **Ad-Hoc Mode** radio button if you want multiple wireless computers to communicate directly with each other. Click the **Next** button to continue or the **Back** button to return to the previous screen.

**SSID** - The SSID is the unique name shared among all devices in your wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which can be any keyboard character.

**Infrastructure Mode** - This mode allows wireless and wired networks to communicate through an access point. Continue to Step 6 if selecting this mode.

**Ad-Hoc Mode** - This mode allows wireless-equipped computers to communicate directly with each other. No access point is used.

Figure 6-11: Profiles - Wireless Mode

5. The *Ad-Hoc Mode Settings* screen, for those who chose an Ad-hoc network, will appear next. Select the correct operating channel for your network from the Channel drop-down menu. Then, select the Network Mode from the drop-down menu. Click the **Next** button to continue or click the **Back** button to change any settings.

**Channel** - The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, select the default channel (Channel 6).

**Network Mode** - Select Mixed Mode, and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed will be reduced. Select G-Only Mode for maximum speed, but no Wireless-B users will be allowed on the network.

The screenshot shows the 'Ad-Hoc Mode Settings' screen in the Linksys Wireless Network Monitor v1.05. The 'Channel' is set to 6, and the 'Network Mode' is set to Mixed Mode. The screen includes instructions for selecting the channel and network mode, and a 'Next' button.

Figure 6-12: Profiles - Ad-Hoc Settings

6. The *Security Settings* screen allows you to set the security level for your network. Enable or disable Wired Equivalent Privacy (WEP) encryption for your wireless network. If you enable WEP, enter a Passphrase or WEP key. Click the **Next** button to continue or the **Back** button to return to the previous screen. For more information about the information on this screen, you can also click the **Help** button.

**WEP** - If you do not want to use WEP encryption, choose Disabled. To use WEP encryption (recommended to increase network security), select 64-bit or 128-bit WEP from the drop-down menu, and enter either a Passphrase or WEP key.

**Passphrase** - Instead of manually entering WEP keys, you can enter a Passphrase, so that a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your wireless network and is compatible with other Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key(s) manually on those products.)

**WEP Key** - This WEP key must match the WEP key of your wireless network. If you are using 64-bit WEP encryption, then the key must consist of exactly ten hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

**TX Key** - This allows you to access different WEP keys used by different routers or access points in your network. Choose the TX Key used in that network. For instance, if the device uses TX Key 3, use TX Key 3. If you're not using multiple WEP Keys, leave this set at 1.

**Authentication** - Select the Authentication method used by your network. Open Authentication does not employ WEP keys. Shared Authentication employs WEP encryption. Auto (the default setting) chooses the method of the network to which you're connecting.

The screenshot shows the 'Wireless Security' screen in the Linksys Wireless Network Monitor v1.05. The 'WEP' is set to 128-bit, and the 'Authentication' is set to Auto. The screen includes instructions for selecting WEP encryption, entering a passphrase, and setting the TX key and authentication method.

Figure 6-13: Profiles - Security Settings

7. The *Confirm New Settings* screen will appear. To save the new settings, click the **Save** button. To cancel the settings and return to the Profiles screen, click the **Exit** button. To edit the new settings, click the **Back** button.

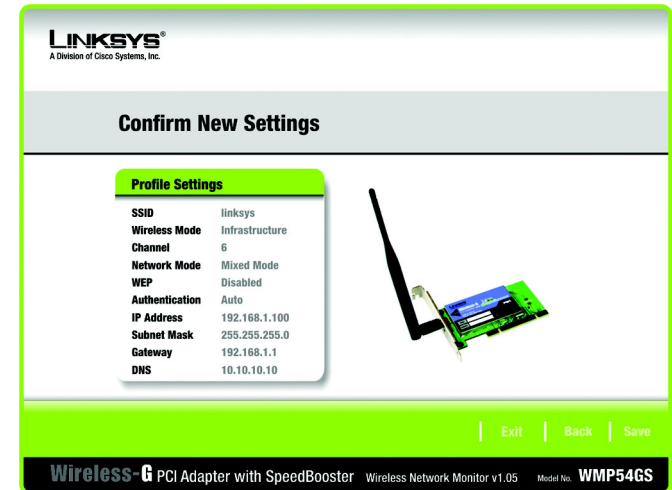


Figure 6-14: Profiles - Confirm New Settings

8. The Congratulations screen shows that the new Profile has successfully been configured. Click **Connect to Network** to implement the new settings immediately and return to the Link Information screen. Click **Return to Profiles Screen** to keep the current settings active, and return to the Profiles screen so that you can edit your profile or create another profile.

You have successfully created a connection profile. Click the X (Close) button in the upper right corner to exit the Wireless Network Monitor.



Figure 6-15: Profiles - Congratulations

# 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-G PCI 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](http://www.linksys.com).

## Common Problems and Solutions

### **1. *The Wireless-G PCI Adapter does not work properly.***

- Reinsert the Wireless-G PCI Adapter into your PC's PCI slot.
- Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find the Wireless-G PCI Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of the Wireless-G PCI Adapter. If there is a yellow question mark, please check the following:
- Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.)
- Make sure that you have inserted the right adapter and installed the proper driver.

If the Wireless-G PCI Adapter does not function after attempting the above steps, remove the adapter and do the following:

- Uninstall the driver software from your PC.
- Restart your PC and repeat the hardware and software installation as specified in this User Guide.

### **2. *I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.***

- Make sure that the PC to which the Wireless-G PCI Adapter is associated is powered on.
- Make sure that your Wireless-G PCI Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

## 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 802.11b 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 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 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.

### ***What is roaming?***

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

### ***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).

### ***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-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?***

The Adapter 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, the Adapter 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.

# 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 (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.

## 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

**WPA.** Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Three modes are available: Radius-PSK, WPA Radius, and Radius. Radius-PSK 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. WPA RADIUS offers two encryption methods, TKIP and AES, with dynamic encryption keys. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication.



**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-PSK.** If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, and enter a password in the Passphrase field of 8-63 characters.

**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.) WPA Radius offers two encryption methods, TKIP and AES, with dynamic 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.)

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: Windows Help

All wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

## TCP/IP

Before a computer can communicate with an access point or wireless router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

## Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

## Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

# Appendix D: 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 (Advanced Encryption Standard)** - 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.

**Bit** - A binary digit.

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

**CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)** - A method of data transfer that is used to prevent data collisions.

**CTS (Clear To Send)** - A signal sent by a wireless device, signifying that it is ready to receive data.

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

**DHCP (Dynamic Host Configuration Protocol)** - 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.

**DNS (Domain Name Server)** - 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.

**DSSS (Direct-Sequence Spread-Spectrum)** - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

**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.

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

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

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

**IEEE (The Institute of Electrical and Electronics Engineers)** - An independent institute that develops networking standards.

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

**IP (Internet Protocol)** - A protocol used to send data over a network.

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

**ISM band** - Radio bandwidth utilized in wireless transmissions.

**ISP (Internet Service Provider)** - A company that provides access to the Internet.

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

**MAC (Media Access Control) Address** - The unique address that a manufacturer assigns to each networking device.

**Mbps (MegaBits Per Second)** - One million bits per second; a unit of measurement for data transmission.

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

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

**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.

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

**RADIUS (Remote Authentication Dial-In User Service)** - A protocol that uses an authentication server to control network access.

**RJ-45 (Registered Jack-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 (Request To Send)** - 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.

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

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

**SSID (Service Set Identifier)** - Your wireless network's name.

**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 (Transmission Control Protocol)** - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - A set of instructions PCs use to communicate over a network.

**TKIP (Temporal Key Integrity Protocol)** - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

**Topology** - The physical layout of a network.

**WEP (Wired Equivalent Privacy)** - A method of encrypting network data transmitted on a wireless network for greater security.

**WPA (Wi-Fi Protected Access)** - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

# Appendix E: Specifications

|                    |                                                                         |
|--------------------|-------------------------------------------------------------------------|
| Standards          | 802.11g, 802.11b                                                        |
| LEDs               | Act: Solid when linked, flashes with traffic                            |
| Transmit Power     | 15dBm                                                                   |
| Sensitivity        | -80 dBm                                                                 |
| Security features  | WEP                                                                     |
| Modulation         | 802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)<br>802.11g: OFDM |
| WEP key bits       | 64Bit and 128Bit                                                        |
| Network Protocol   | TCP/IP, IPX, NetBEUI                                                    |
| Dimensions         | 6.18" x 8.66" x 0.910" (157 mm x 220 mm x 23 mm)                        |
| Unit Weight        | 3.53 oz. (0.1 kg.)                                                      |
| Certifications     | FCC                                                                     |
| Operating Temp.    | 0 C to 65 C (32 F to 150 F)                                             |
| Storage Temp.      | -40 C to 85 C (-40 F to 185 F)                                          |
| Operating Humidity | 0% to 95% Non-Condensing                                                |
| Storage Humidity   | 0% to 95% Non-Condensing                                                |

Cisco-Linksys, LLC declares that WMP54GS ( FCC ID: Q87-HGA7S-5) is limited in CH1~CH11 by specified firmware controlled in U.S.A.

# Appendix F: 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 G: 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: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## 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.

## 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.

## EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-G PCI Adapter 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 Wireless-G PCI Adapter tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group déclare la Passerelle ADSL sans fil-B 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 complètement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. 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.

## Also Available:

- **Linksys High Gain Antenna for SMA Connectors (HGA7S)**



## Appendix H: 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](ftp://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:  
Or fax your request in to:

800-546-5797 (LINKSYS)  
949-261-8868

If you experience problems with any Linksys product, you can call us at:

800-326-7114  
[support@linksys.com](mailto:support@linksys.com)

Don't wish to call? You can e-mail us at:

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:  
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)

949-261-1288