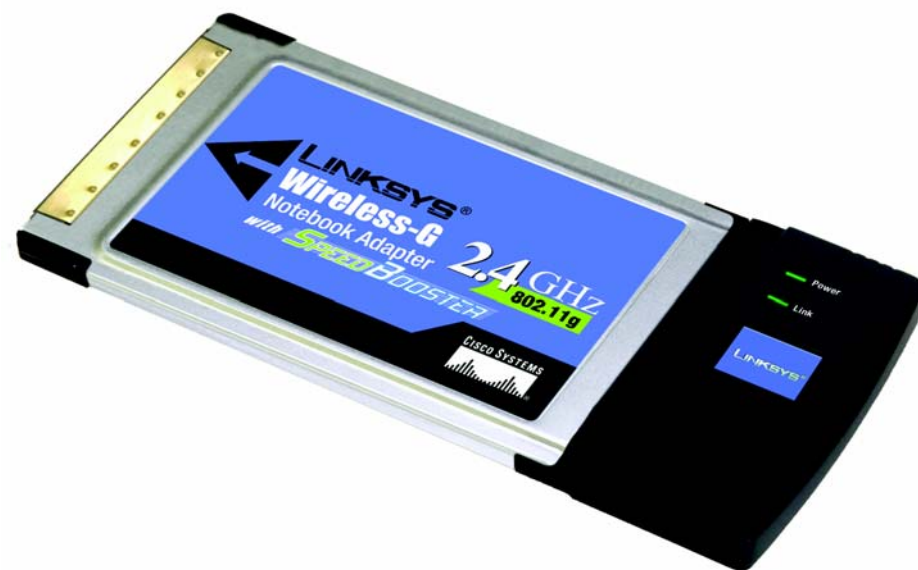


LINKSYS®

A Division of Cisco Systems, Inc.



2,4GHz
802.11g

Wireless-G

Notebook Adapter with SpeedBooster

User Guide



Model No. **WPC54GS (EU/UK/LA)**

CISCO SYSTEMS



Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

This User Guide

The User Guide to the Wireless-G Notebook Adapter with SpeedBooster has been designed to make understanding networking easier than ever. Look for the following items when reading this guide:



This checkmark means there is a note of interest and is something you should pay special attention to while using the Adapter.



This exclamation point means there is a caution or warning and is something that could damage your property or the Adapter.



This question mark provides you with a reminder about something you might need to do while using the Adapter.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: definition.

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the "List of Figures" section in the "Table of Contents".

Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this Guide?	2
Chapter 2: Planning your Wireless Network	4
Network Topology	4
Roaming	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-G Notebook Adapter	6
The LED Indicators	6
Chapter 4: Setting up and Connecting the Wireless-G Notebook Adapter	7
Starting the Setup	7
Connecting the Adapter	8
Setting up the Adapter	8
Chapter 5: Using the Wireless Network Monitor	20
Accessing the Wireless Network Monitor	20
Link Information Screens	20
Link Information	20
SecureEasySetup	23
Site Survey	25
Profiles	26
Creating a New Profile	27
Click Exit to close the Setup Wizard.	27
Appendix A: Troubleshooting	39
Common Problems and Solutions	39
Frequently Asked Questions	40
Appendix B: Wireless Security	43
Security Precautions	43
Security Threats Facing Wireless Networks	43
Appendix C: Windows Help	46
Appendix D: Glossary	47
Appendix E: Specifications	54

Appendix F: Warranty Information	55
Appendix G: Regulatory Information	56
Appendix H: Contact Information	63

List of Figures

Figure 3-1: Front Panel	6
Figure 4-1: Setup Wizard's Welcome Screen	7
Figure 4-2: Setup Wizard's License Agreement	7
Figure 4-3: Connecting the Adapter	8
Figure 4-4: Available Wireless Network	8
Figure 4-5: SecureEasySetup Screen	9
Figure 4-6: SecureEasySetup Logo	9
Figure 4-7: SecureEasySetup Logo Location	9
Figure 4-8: SecureEasySetup Congratulations	10
Figure 4-9: Available Wireless Network	10
Figure 4-10: WEP Key Needed for Connection	11
Figure 4-11: WPA - Personal Needed for Connection	11
Figure 4-12: Automatic Setup's Congratulations	12
Figure 4-13: Available Wireless Network	12
Figure 4-14: Network Settings	13
Figure 4-15: Wireless Mode	13
Figure 4-16: Ad-Hoc Mode Settings	14
Figure 4-17: Wireless Security - WEP	14
Figure 4-18: Wireless Security - WPA Personal	15
Figure 4-19: Wireless Security - WPA Enterprise - EAP-TLS	16
Figure 4-20: Wireless Security - WPA Enterprise - PEAP	16
Figure 4-21: Wireless Security - RADIUS - EAP-TLS	17
Figure 4-22: Wireless Security - RADIUS - PEAP	17
Figure 4-23: Wireless Security - LEAP	18
Figure 4-24: Confirm New Settings	18
Figure 4-25: Congratulations screen	19
Figure 5-1: Wireless Network Monitor Icon	20
Figure 5-2: Link Information	20
Figure 5-3: More Information - Wireless Network Status	21
Figure 5-4: More Information-Network Statistics	22

Figure 5-5: The SecureEasySetup button	23
Figure 5-6: Locate the Cisco Logo	23
Figure 5-7: Where can I find the button?	23
Figure 5-8: The SecureEasySetup Logo and Location	24
Figure 5-9: SecureEasySetup	24
Figure 5-10: Site Survey	25
Figure 5-11: WEP Key Needed for Connection	25
Figure 5-12: WPA-Personal Needed for Connection	25
Figure 5-13: Profiles	26
Figure 5-14: Import a Profile	26
Figure 5-15: Export a Profile	26
Figure 5-16: Create a New Profile	27
Figure 5-17: Available Wireless Network	27
Figure 5-18: Available Wireless Network	28
Figure 5-19: Available Wireless Network	28
Figure 5-20: Available Wireless Network	28
Figure 5-21: Available Wireless Network	29
Figure 5-22: Available Wireless Network	29
Figure 5-23: Available Wireless Network	30
Figure 5-24: WEP Key Needed for Connection	30
Figure 5-25: WPA Personal Needed for Connection	31
Figure 5-26: Network Settings for New Profile	31
Figure 5-27: Wireless Mode for New Profile	32
Figure 5-28: Ad-Hoc Mode Settings for New Profile	32
Figure 5-29: Wireless Security for New Profile	33
Figure 5-30: Wireless Security - WEP for New Profile	33
Figure 5-31: Wireless Security - WPA Personal for New Profile	34
Figure 5-32: Wireless Security - WPA Enterprise Using EAP-TLS for New Profile	35
Figure 5-33: Wireless Security - WPA Enterprise Using PEAP for New Profile	35
Figure 5-34: Wireless Security - RADIUS Using EAP-TLS for New Profile	36
Figure 5-35: Wireless Security - RADIUS Using PEAP for New Profile	36
Figure 5-36: Wireless Security - LEAP for New Profile	37
Figure 5-37: Confirm New Settings for New Profile	37

Figure 5-38: Congratulations for New Profile

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Notebook Adapter with SpeedBooster. With this Adapter, your wireless networking experience will be faster and easier than ever.

Like all wireless products, the Adapter allows for greater range and mobility within your wireless network. This adapter communicates over the 54Mbps 802.11g wireless standard, which is almost five times faster than 802.11b. But since they share the same 2.4GHz radio band, the Adapter can also communicate with the widely used 11Mbps 802.11b standard.

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network.

The included Setup Wizard will walk you through configuring the adapter to your network's settings, step by step. Then just slide it into your notebook's PC Card slot and enjoy network access with your notebook computer, while retaining true mobility.

Once you're connected, you can keep in touch with your e-mail, access the Internet, and share files and other resources such as printers and network storage with other computers on the network. At home, you can surf the web or use instant messaging to chat with friends while sitting out on the patio. Your wireless connection is protected by up to 128-bit WEP encryption.

You'll also be able to connect with any of the growing number of public wireless hotspots springing up in coffee shops, airport lounges, hotels and convention centers. And as those hotspots upgrade to the new high-speed Wireless-G standard, you'll be ready to take advantage of the increased speeds.

Get connected to current-standard 802.11b networks today, and be prepared for the future with the Wireless-G Notebook Adapter with SpeedBooster from Linksys.

network: *a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.*

adapter: *a device that adds network functionality to your PC.*

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 and an operating frequency of 2.4GHz.*

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G Notebook Adapter with SpeedBooster.

- **Chapter 1: Introduction**
This chapter describes the Adapter's applications and this User Guide.
- **Chapter 2: Planning Your Wireless Network**
This chapter discusses a few of the basics about wireless networking.
- **Chapter 3: Getting to Know the Wireless-G Notebook Adapter**
This chapter describes the physical features of the Adapter.
- **Chapter 4: Setting Up and Connecting the Wireless-G Notebook Adapter**
This chapter shows you how to setup and connect the Adapter.
- **Chapter 5: Using the Wireless Network Monitor**
This chapter show you how to use the Adapter's Wireless Network Monitor.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Adapter.
- **Appendix B: Wireless Security**
This appendix discusses security issues regarding wireless networking and measures you can take to help protect your wireless network.
- **Appendix C: Windows Help**
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix D: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix E: Specifications**
This appendix provides the Adapter's technical specifications.
- **Appendix F: Warranty Information**
This appendix supplies the Adapter's warranty information.
- **Appendix G: Regulatory Information**
This appendix supplies the Adapter's regulatory information.

- **Appendix H: Contact Information**

This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network.

Linksys wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and can double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network can be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same channel and SSID.

Before enabling you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

topology: the physical layout of a network.

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

infrastructure: a wireless network that is bridged to a wired network via an access point.

roaming: the ability to take a wireless device from one access point's range to another without losing the connection.

ssid: your wireless network's name.

Network Layout

Linksys wireless access points and wireless routers have been designed for use with 802.11a, 802.11b, and 802.11g products. With 802.11g products communicating with the 802.11b standard and some products incorporating both “a” and “g”, products using these standards can communicate with each other.

Access points and wireless routers are compatible with 802.11a, 802.11b and 802.11g adapters, such as the PC Cards for your laptop computers, PCI Card for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity. Wireless products will also communicate with the wireless PrintServer.

When you wish to connect your wired network with your wireless network, network ports on access points and wireless routers can be connected to any of Linksys's switches or routers.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com/international for more information about wireless products.

Chapter 3: Getting to Know the Wireless-G Notebook Adapter

The LED Indicators

The Network Adapter's LEDs display information about network activity.



Figure 3-1: Front Panel

Power *Green.* The Power LED lights up when the Adapter is powered on.

Link *Green.* The Link LED lights up when the Adapter has an active connection.

Chapter 4: Setting up and Connecting the Wireless-G Notebook Adapter

Starting the Setup

The Wireless-G Notebook Adapter Setup Wizard will guide you through the installation procedure. The Setup Wizard will install the driver and Wireless Network Monitor, as well as connect and configure the Adapter.



IMPORTANT: Do not connect the Adapter until you are instructed to do so or the setup will not work.

Insert the **Setup Wizard CD-ROM** into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if “D” is the letter of your CD-ROM drive).

On the *Welcome* screen, you have the following choices:

Click Here to Start- Click the **Click Here to Start** button to begin the software installation process.

User Guide - Click the **User Guide** button to open the PDF file of this User Guide.

Exit - Click the **Exit** button to exit the Setup Wizard.

1. To install the Adapter, click the **Click Here to Start** button on the *Welcome* screen.
2. After reading the License Agreement, click the **Next** button if you agree and want to continue the installation, or click the **Cancel** button to end the installation.
3. Windows will begin copying the files onto your PC.



Figure 4-1: Setup Wizard's Welcome Screen

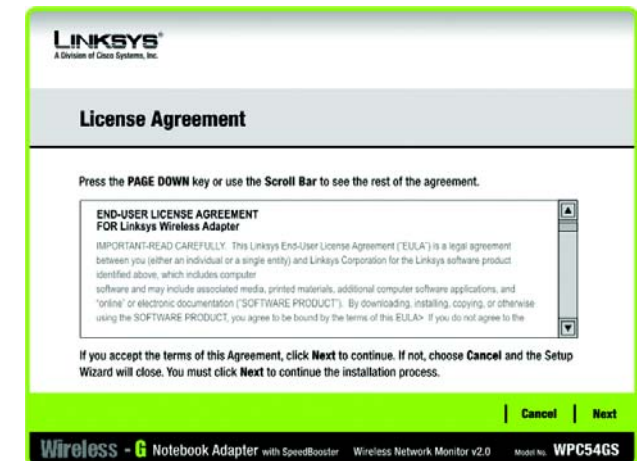


Figure 4-2: Setup Wizard's License Agreement

Connecting the Adapter

1. Locate an available CardBus slot on your notebook PC.
2. With the connector pin end facing the CardBus slot and the label facing up, slide the Adapter into the CardBus slot until it locks in place.
3. Windows 98 and Windows Me users may need to restart their PCs again when prompted to do so. The Power LED should light up when the Adapter is installed correctly.
4. Windows will begin copying the driver files to your computer. If Windows asks you for the original Windows CD-ROM, insert the CD-ROM, and direct Windows to its correct location (e.g., D:\).
5. Then, click **Next**.

Setting up the Adapter

The next screen to appear will be the *Available Wireless Network* screen.

This screen provides three options for setting up the Adapter

- **SecureEasySetup.** This Adapter features SecureEasySetup. This means that you can set it up with just the press of a button when connecting to wireless routers or access points that also feature SecureEasySetup. Both devices on the network must feature SecureEasySetup for this to work.
- **Available Wireless Network. (For most users.)** Use this option if you already have a network set up with devices that do not have SecureEasySetup. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If you are not taking advantage of SecureEasySetup and your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for Advanced Users only.

The setup for each option is described, step by step, under the appropriate heading on the following pages.

Click **Exit** to close the Setup Wizard, if you wish to set up the Adapter later.



Figure 4-3: Connecting the Adapter

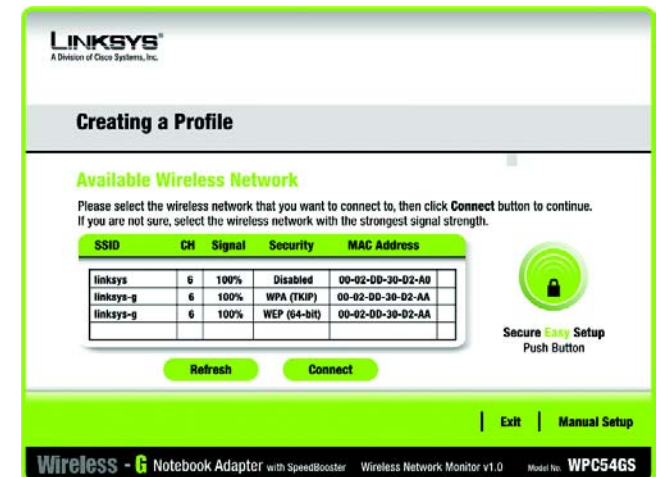


Figure 4-4: Available Wireless Network

Setting Up the Adapter with SecureEasySetup

With SecureEasySetup, setting up the Adapter is as simple as pushing a couple of buttons. Before you press any buttons, though, you should locate the SecureEasySetup button on the device you're connecting the Adapter to, such as a wireless router or access point.

1. Starting from the *Available Wireless Network* screen, click the **SecureEasySetup** button on the right hand side.

2. You will be asked to locate the **SecureEasySetup** button on the device with which the Adapter will be communicating. If you are not sure where to find this button, click **Where can I find the button?**.

This will walk you through a couple of screens to help you find the button, which is usually located on the front of the wireless router or access point.

3. Press the Router or Access Point's SecureEasySetup button on its front panel. After approximately two to ten seconds, the button will turn white and begin to blink.

If your other **SecureEasySetup device is not yet installed**, Click the **Next** button to continue and finish the Router's installation. Then, to install the other device, follow the instructions provided with that device for SecureEasySetup.

If your other **SecureEasySetup device is already installed**, press the SecureEasySetup button on that device within two minutes. (The button on that device may be on the device's software that you will have to click on-screen.) Click the **Next** button to continue and finish the Router's installation.

To add other SecureEasySetup devices to your network, follow the instructions provided with each device.



NOTE: You can only add one SecureEasySetup device at a time.

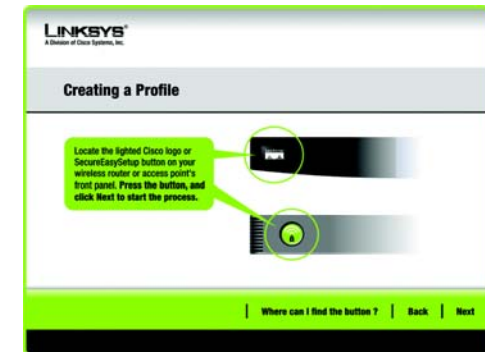


Figure 4-5: Locate the Button



Figure 4-6: SecureEasySetup Logo



Figure 4-7: SecureEasySetup Logo Location

4. When SecureEasySetup is complete, you may save your configuration to a text file by clicking the **Save** button, or print the configuration by clicking the **Print** button. Click **Connect to Network** to connect to your network.

Congratulations! The setup is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, refer to *Chapter 5: Using the Wireless Network Monitor*.

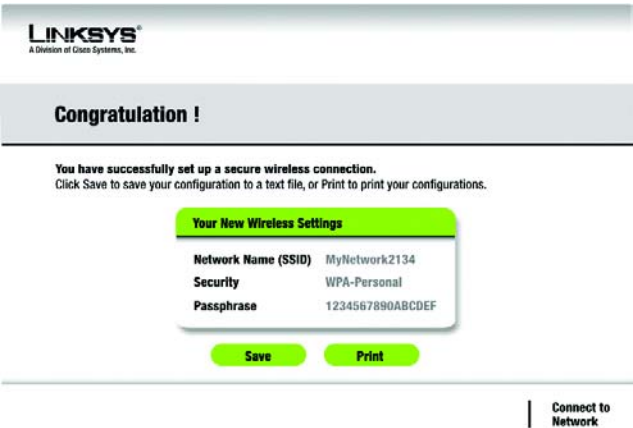


Figure 4-8: SecureEasySetup Congratulations

Setting Up the Adapter with Available Wireless Network

If you're not setting up the Adapter with SecureEasySetup, another method for setting up the Adapter is with the available networks listed on the *Available Wireless Network* screen. The available networks are listed in the table on the center of the screen by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If you do not see your network listed, you can click the **Refresh** button to bring the list up again.) If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If you have wireless security enabled on your network, continue to step 2. If you don't have wireless security enabled, continue to step 3.

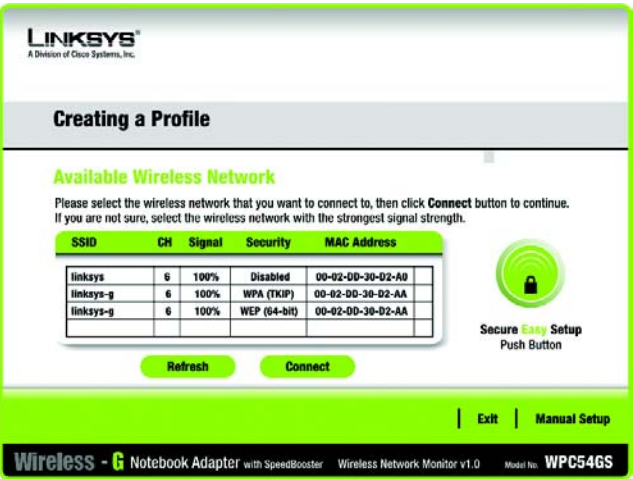


Figure 4-9: Available Wireless Network

- If your network has the wireless security WEP (Wired Equivalent Privacy) enabled, this screen will appear. Select **64-bit** or **128-bit**.

Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer 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.)

WEP Key - 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. For 152-bit encryption, enter exactly 32 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Then click **Connect** and proceed to Step 3.

If your network has the wireless security WPA Personal (Wi-Fi Protected Access) enabled, this screen will appear.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Then click **Connect** and proceed to Step 3.

LINKSYS
A Division of Cisco Systems, Inc.

WEP Key Needed for Connection

This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then press **Connect**.

Security WEP Please select the wireless security method used by your existing wireless network.

WEP 128-bit To use WEP encryption, select 64-bit, 128-bit or 152-bit encryption. (152-bit encryption is available for 802.11a networks only.)

Passphrase The Passphrase is case-sensitive and should be no more than 16 characters in length.

WEP Key 1 When entering this manually, it should be 10 hexadecimal characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".

Cancel **Connect**

Figure 4-10: WEP Key Needed for Connection

LINKSYS
A Division of Cisco Systems, Inc.

WPA - Personal Needed for Connection

This wireless network has WPA - Personal, also known as Pre-Shared Key, enabled. To connect to this network, select the encryption type. Enter the required passphrase in the appropriate field below. Then press **Connect**.

Security WPA - Personal Please select the wireless security method used by your existing wireless network.

Encryption TKIP Please select an encryption type used to protect your wireless data transmissions.

Passphrase Please enter a Passphrase that is 8 to 63 characters in length.

Cancel **Connect**

Figure 4-11: WPA - Personal Needed for Connection

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.

encryption: encoding data transmitted in a network.

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.

3. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network. For more information about the Wireless Network Monitor, refer to *Chapter 5: Using the Wireless Network Monitor*.

Congratulations! The setup is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, proceed to Chapter 5: Using the Wireless Network Monitor.



Figure 4-12: Automatic Setup's Congratulations

Setting Up the Adapter with Manual Setup

If you are not taking advantage of SecureEasySetup and your network is not listed with the available networks, you can use Manual Setup.

1. Click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.

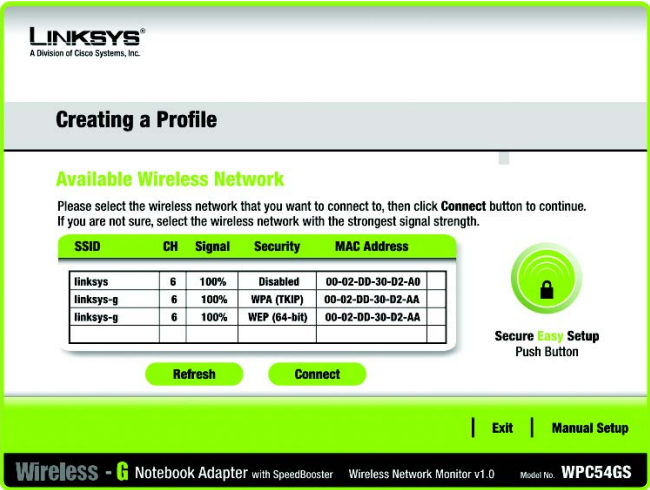


Figure 4-13: Available Wireless Network

2. The *Network Settings* screen from the Wireless Network Monitor will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

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 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

Click the **Next** button to continue, or click the **Back** button to return to the *Profiles* screen.

Figure 4-14: Network Settings

3. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

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

Figure 4-15: Wireless Mode

4. If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. 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, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.

- If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 6.

If your wireless network has wireless security, select the method of security used: **WEP**, **WPA-Personal**, **WPA-Enterprise**, **RADIUS**, or **LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA is a stronger security method than WEP. RADIUS stands for Remote Authentication Dial-In User Service, and LEAP stands for Lightweight Extensible Authentication Protocol. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA-Personal, WPA-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit** or **128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so 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 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.)

WEP Key - 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".

LINKSYS
A Division of Cisco Systems, Inc.

Creating a Profile

Ad-Hoc Mode Settings

Channel: Auto ▼ Select the Channel used by all of the devices in your wireless network.

Back Next

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-16: Ad-Hoc Mode Settings

LINKSYS
A Division of Cisco Systems, Inc.

Creating a Profile

Wireless Security - WEP

WEP: 128-bit ▼ To use WEP encryption, select 64-bit, 128-bit or 152-bit encryption. (152-bit encryption is available for 802.11a networks only.)

Passphrase: The Passphrase is case-sensitive and should be no more than 16 characters in length.

WEP Key: When entering this manually, it should be 10 hexadecimal characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".

For Advanced Users:

TX Key: 1 ▼ Select the transmit key for your network. (Default setting: 1)

Authentication: Auto ▼ Select your network's authentication type. (Default setting: Auto)

Back Next

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-17: Wireless Security - WEP

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select **TKIP** or **AES** for encryption. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

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



The screenshot shows the Linksys configuration interface for 'Wireless Security - WPA Personal'. At the top, the Linksys logo is displayed. Below it, the title 'Creating a Profile' is centered. The main section is titled 'Wireless Security - WPA Personal'. It contains two fields: 'Encryption' with a dropdown menu currently set to 'TKIP', and 'Passphrase' with a text input field. To the right of the 'Encryption' dropdown is a note: 'Please select the encryption type used to protect your wireless data transmissions.' To the right of the 'Passphrase' field is a note: 'Please enter a Passphrase that is 8 to 63 characters in length.' At the bottom right, there are 'Back' and 'Next' buttons. The footer bar contains the text 'Wireless - G Notebook Adapter with SpeedBooster', 'Wireless Network Monitor v1.0', and 'Model No. WPC54GS'.

Figure 4-18: Wireless Security - WPA Personal

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. The 'Login Name' field is empty. The 'Server Name' field is empty. The 'Certificate' dropdown is empty. The 'Encryption' dropdown is set to 'AES'. To the right of each field is a descriptive instruction. At the bottom right are 'Back' and 'Next' buttons. The footer bar indicates 'Wireless - G Notebook Adapter with SpeedBooster', 'Wireless Network Monitor v1.0', and 'Model No. WPC54GS'.

Figure 4-19: Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. The 'Login Name' field is empty. The 'Password' field is empty. The 'Server Name' field is empty. The 'Certificate' dropdown is set to 'Trust Any'. The 'Inner Authen.' dropdown is set to 'EAP-MSCHAP v2'. The 'Encryption' dropdown is set to 'AES'. To the right of each field is a descriptive instruction. At the bottom right are 'Back' and 'Next' buttons. The footer bar indicates 'Wireless - G Notebook Adapter with SpeedBooster', 'Wireless Network Monitor v1.0', and 'Model No. WPC54GS'.

Figure 4-20: Wireless Security - WPA Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel.

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

LINKSYS
A Division of Cisco Systems, Inc.

Creating a Profile

Wireless Security - RADIUS

Authentication Please select the authentication method that you use to access your network.

Login Name Enter the Login Name used for authentication.

Server Name Enter the Server Name used for authentication. **(Optional)**

Certificate Please select the certificate used for authentication.

[Back](#) [Next](#)

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-21: Wireless Security - RADIUS - EAP-TLS

LINKSYS
A Division of Cisco Systems, Inc.

Creating a Profile

Wireless Security - RADIUS

Authentication Please select the authentication method that you use to access your network.

Login Name Enter the Login Name used for authentication.

Password Enter the Password used for authentication.

Server Name Enter the Server Name used for authentication. **(Optional)**

Certificate Please select the certificate used for authentication.

Inner Authn. Please select the inner authentication method used inside the PEAP tunnel.

[Back](#) [Next](#)

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-22: Wireless Security - RADIUS - PEAP

LEAP

If you selected LEAP, then enter the Username and Password that will authenticate you on your wireless network.

Username - Enter the username used for authentication.

Password - Enter the password used for authentication.

Confirm - Enter the password again.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

LINKSYS®
A Division of Cisco Systems, Inc.

Creating a Profile

Wireless Security - LEAP

User Name Enter the Login Name used for authentication.

Password Enter the Password used for authentication.

Confirm Re-enter the Password again.

Back Next

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-23: Wireless Security - LEAP

- The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button. To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.

LINKSYS®
A Division of Cisco Systems, Inc.

Confirm New Settings

Profile Settings

SSID	linksys
Wireless Mode	Infrastructure
Channel	6
Network Mode	Mixed Mode
Security	WEP (128-bit)
Authentication	Auto
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS	10.10.10.10

Exit Back Save

Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS

Figure 4-24: Confirm New Settings

7. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network. Clicking **Return to Profile** will open the Wireless Network Monitor's *Profiles* screen. For more information about the Wireless Network Monitor, refer to *Chapter 5: Using the Wireless Network Monitor*.

Congratulations! The setup is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, proceed to Chapter 5: Using the Wireless Network Monitor.

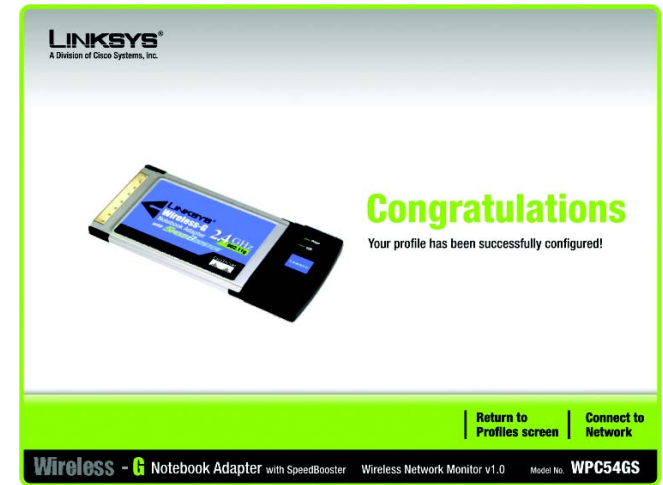


Figure 4-25: Congratulations screen

Chapter 5: Using the Wireless Network Monitor

Use the Wireless Network Monitor to check the link information, search for available wireless networks, or create profiles that hold different configuration settings.

Accessing the Wireless Network Monitor

After installing the Adapter, the Wireless Network Monitor icon will appear in the system tray of your computer. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.



Figure 5-1: Wireless Network Monitor Icon

Link Information Screens

The opening screen of the Wireless Network Monitor is the *Link Information* screen. From this screen, you can find out how strong the current wireless signal is and how good the connection's quality is. You can also click the **More Information** button to view additional status information about the current wireless connection. To search for available wireless networks, click the **Site Survey** tab. To perform configuration changes or create connection profiles, click the **Profiles** tab.

Link Information

The *Link Information* screen displays network mode, signal strength, and link quality information about the current connection. It also provides a button to click for additional status information.

Ad-Hoc Mode or Infrastructure Mode - The screen indicates whether the Adapter is currently working in ad-hoc or infrastructure mode.

Signal Strength - The Signal Strength bar indicates signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **More Information** button to view additional information about the wireless network connection on the *Wireless Network Status* screen.



Figure 5-2: Link Information

Wireless Network Status

The *Wireless Network Status* screen provides information on your current network settings.

Status - This shows the status of the wireless network connection.

SSID - This is the unique name of the wireless network.

Wireless Mode - The mode of the wireless network currently in use is displayed here.

Transfer Rate - The data transfer rate of the current connection is shown here.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

Authentication - This is your wireless network's authentication method.

IP Address - The IP Address of the Adapter is displayed here.

Subnet Mask - The Subnet Mask of the Adapter is shown here.

Default Gateway - The Default Gateway address of the Adapter is displayed here.

DNS - This is the DNS address of the Adapter.

DHCP Client - This displays the Adapter's status as a DHCP client.

MAC Address - The MAC address of the wireless network's access point or wireless router is shown here.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Statistics** button to go to the *Wireless Network Statistics* screen. Click the **Back** button to return to the initial *Link Information* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile.



Figure 5-3: More Information - Wireless Network Status

Wireless Network Statistics

The *Wireless Networks Statistics* screen provides statistics on your current network settings.

Transmit Rate - This is 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.)

Receive Rate - This is the rate at which data is received.

Packets Received - This shows the packets received by the Adapter, in real time, since connecting to the wireless network or since the *Refresh Statistics* button was last pressed.

Packets Transmitted - This shows the packets transmitted from the Adapter, in real time, since connecting to the wireless network or since the *Refresh Statistics* button was last pressed.

Noise Level - This shows the level of background noise affecting the wireless signal. A lower reading translates into a higher quality signal.

Signal Strength - This is the intensity of the wireless signal received by the Adapter.

Driver Version - This shows the version of the Adapter's driver.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Back** button to return to the initial *Link Information* screen. Click the **Status** button to go to the *Wireless Network Status* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile. Click the **Refresh** button to reset the statistics.

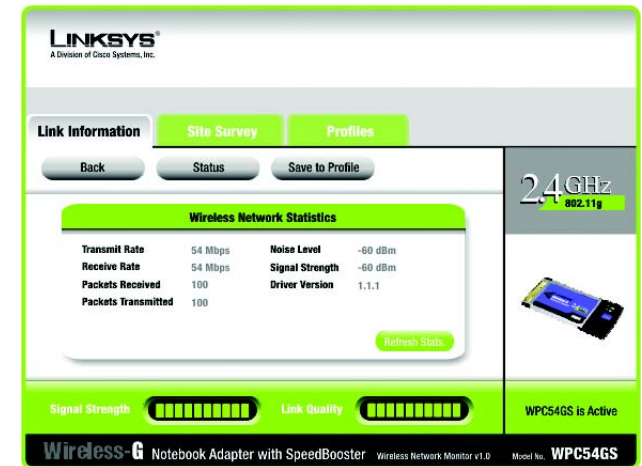


Figure 5-4: More Information-Network Statistics

SecureEasySetup

While using the Monitor, you might see the SecureEasySetup button on the right-hand side of the screen. This button can be used to set up the Adapter, if this has not already been done. With SecureEasySetup, setting up the Adapter is as simple as pushing a couple of buttons. Before you press any buttons, though, you should locate the SecureEasySetup button on the device you're connecting the Adapter to, such as a wireless router or access point.

1. After clicking the **SecureEasySetup** button, you will be asked to locate the **SecureEasySetup** button or Cisco logo button on the device with which the Adapter will be communicating. If you are not sure where to find this button, click **Where can I find the button?**.

This will walk you through a couple of screens to help you find the button, which is usually located on the front of the wireless router or access point.

If you've clicked the button by accident or do not wish to use SecureEasySetup, you can click **Back** to return to the previous screen.



**Secure Easy Setup
Push Button**

Figure 5-5: The SecureEasySetup button

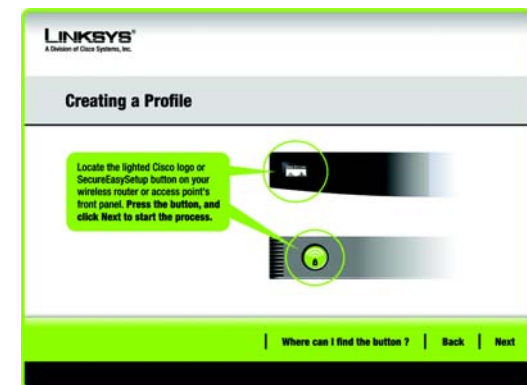


Figure 5-6: Locate the Button



Figure 5-7: Where can I find the button?

2. Press the Router or Access Point's SecureEasySetup button on its front panel. After approximately two to ten seconds, the button will turn white and begin to blink.

If your other **SecureEasySetup** device is **not yet installed**, Click the **Next** button to continue and finish the Router's installation. Then, to install the other device, follow the instructions provided with that device for SecureEasySetup.

If your other **SecureEasySetup** device is **already installed**, press the SecureEasySetup button on that device within two minutes. (The button on that device may be on the device's software that you will have to click on-screen.) Click the **Next** button to continue and finish the Router's installation.

To add other SecureEasySetup devices to your network, follow the instructions provided with each device.



NOTE: You can only add one SecureEasySetup device at a time.

3. SecureEasySetup is now complete and a configuration profile will has been created automatically. You may save your configuration profile to a text file by clicking the **Save** button, or print the configuration by clicking the **Print** button. Click **Connect to Network** to connect to your network.

Congratulations! SecureEasySetup is complete.



Figure 5-8: The SecureEasySetup Logo and Location

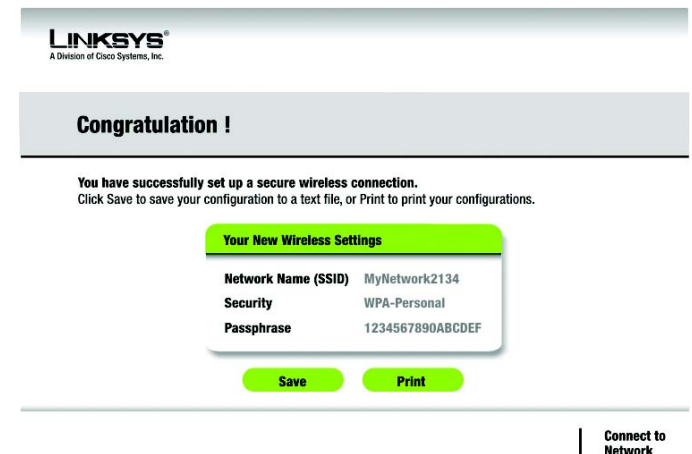


Figure 5-9: SecureEasySetup

Site Survey

The *Site Survey* screen displays a list of available networks in the table on the left. The table shows each network's SSID, Channel, and the quality of the wireless signal the Adapter is receiving. You may click **SSID**, **CH** (Channel), or **Signal**, to sort by that field.

SSID - The SSID or unique name of the wireless network is displayed here.

CH - This is the channel that the network uses.

Signal - This is the percentage of signal strength, from 0 to 100%.

Site Information

For each network selected, the following settings are listed:

SSID - This the SSID or unique name of the wireless network.

Wireless Mode - This is the mode of the wireless network currently in use.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

MAC Address- The MAC address of the wireless network's access point is displayed here.

Refresh - Click the **Refresh** button to perform a new search for wireless devices.

Connect - To connect to one of the networks on the list, select the wireless network, and click the **Connect** button. If the network has encryption enabled, then you will see a new screen appear.

If the network has the wireless security WEP encryption enabled, then you will see the *WEP Key Needed for Connection* screen. Select the appropriate level of WEP encryption, **64-bit** or **128-bit**). Then enter the network's Passphrase or WEP Key. Click the **Connect** button. To cancel the connection, click the **Cancel** button.

If the network has the wireless security WPA-Personal security enabled, then you will see the *WPA-Personal Needed for Connection* screen. Select the appropriate encryption type, **TKIP** or **AES**. Enter the network's Passphrase or pre-shared key in the *Passphrase* field. Then click the **Connect** button. To cancel the connection, click the **Cancel** button.

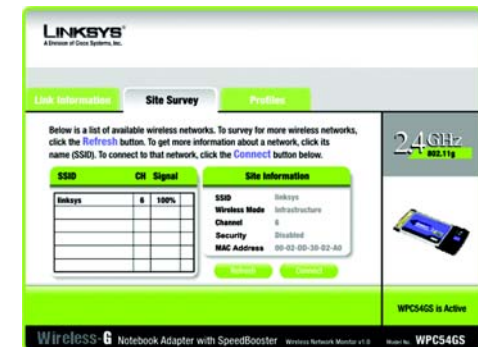


Figure 5-10: Site Survey

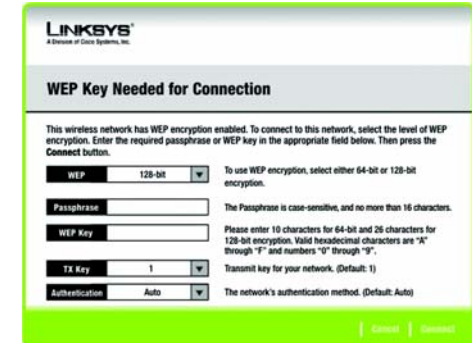


Figure 5-11: WEP Key Needed for Connection

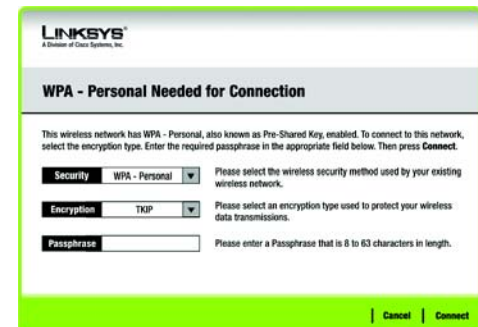


Figure 5-12: WPA-Personal Needed for Connection

Profiles

The *Profiles* screen lets you save different configuration profiles for different network setups. The table on the left displays a list of available profiles with their profile names and SSIDs.

Profile - The name of the profile is displayed here.

SSID - The SSID or unique name of the wireless network is displayed here.

Profile Information

For each profile selected, the following are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Transfer Rate - The data transfer rate of the current connection is shown here.

Channel - This is the channel to which the wireless network devices are set.

Security - The status of the wireless security feature is displayed here.

Authentication - The authentication setting for the network is shown here.

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 the profile you want to change, and then click the **Edit** button.

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.

Export - Select the profile you want to save in a different location, and click the **Export** button. Direct Windows to the appropriate folder, and click the **Save** button.

Delete - Select the profile you want to delete, and then click the **Delete** button.



NOTE: If you want to export more than one profile, you have to export them one at a time.

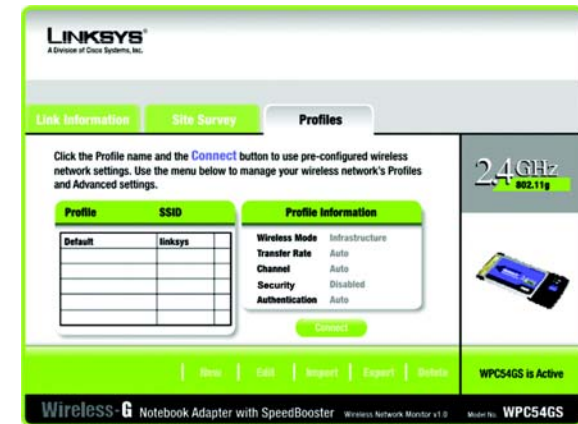


Figure 5-13: Profiles



Figure 5-14: Import a Profile

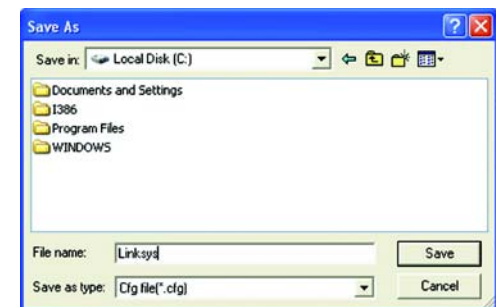


Figure 5-15: Export a Profile

Creating a New Profile

On the *Profiles* screen, click the **New** button to create a new profile. Enter a name for the new profile, and click the **OK** button. Click the **Cancel** button to return to the *Profiles* screen without entering a name.

The *Available Wireless Network* screen will appear. This screen provides three options for setting up the Adapter

- **SecureEasySetup.** This Adapter features SecureEasySetup. This means that you can set it up with just the press of a button when connecting to wireless routers or access points that also feature SecureEasySetup. Both point on the network must feature SecureEasySetup for this to work.
- **Available Networks.** (For most users.) Use this option if you already have a network set up with devices that do not have SecureEasySetup. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If you are not taking advantage of SecureEasySetup and your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for Advanced Users only.

The setup for each option is described, step by step, under the appropriate heading on the following pages.

Click **Exit** to close the Setup Wizard.



Figure 5-16: Create a New Profile

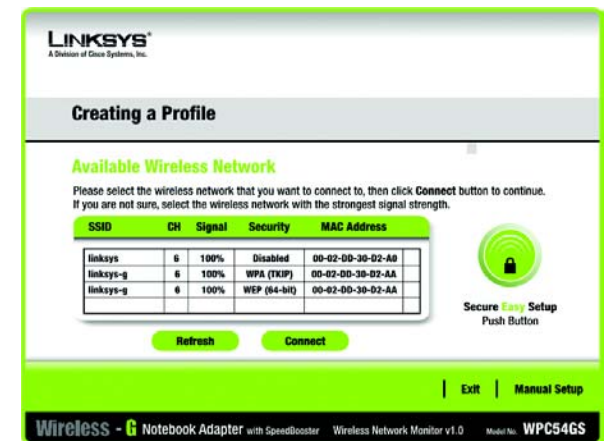


Figure 5-17: Available Wireless Network

Setting Up the Adapter with SecureEasySetup

While using the Monitor, you might see the SecureEasySetup button on the right-hand side of the screen. This button can be used to set up the Adapter, if this has not already been done. With SecureEasySetup, setting up the Adapter is as simple as pushing a couple of buttons. Before you press any buttons, though, you should locate the SecureEasySetup button on the device you're connecting the Adapter to, such as a wireless router or access point.

1. After clicking the **SecureEasySetup** button, you will be asked to locate the **SecureEasySetup** button or Cisco logo button on the device with which the Adapter will be communicating. If you are not sure where to find this button, click **Where can I find the button?**.

This will walk you through a couple of screens to help you find the button, which is usually located on the front of the wireless router or access point.

If you've clicked the button by accident or do not wish to use SecureEasySetup, you can click **Back** to return to the previous screen.



**Secure Easy Setup
Push Button**

Figure 5-18: Available Wireless Network

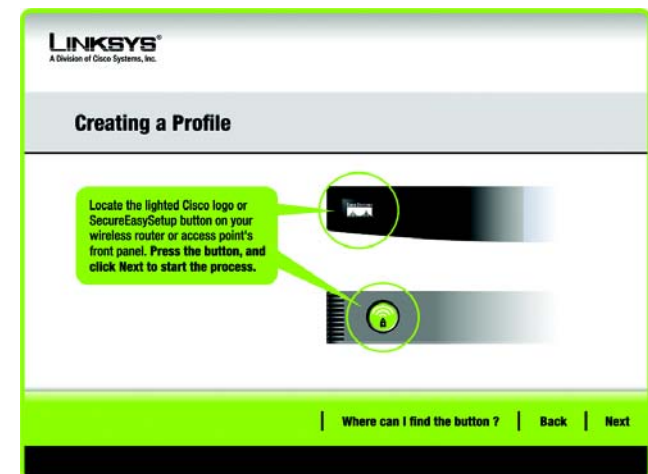


Figure 5-19: Locate the Button

2. Press the Gateway's SecureEasySetup button on its front panel. After approximately two seconds, the button will turn white and begin to blink.

If your other **SecureEasySetup** device is **not yet installed**, Click the **Next** button to continue and finish the Router's installation. Then, to install the other device, follow the instructions provided with that device for SecureEasySetup.

If your other **SecureEasySetup** device is **already installed**, press the SecureEasySetup button on that device within two minutes. (The button on that device may be on the device's software that you will have to click on-screen.) Click the **Next** button to continue and finish the Router's installation.

To add other SecureEasySetup devices to your network, follow the instructions provided with each device.



NOTE: You can only add one SecureEasySetup device at a time.

3. SecureEasySetup is now complete and a configuration profile will has been created automatically. You may save your configuration profile to a text file by clicking the **Save** button, or print the configuration by clicking the **Print** button. Click **Connect to Network** to connect to your network.

Congratulations! SecureEasySetup is complete.



Figure 5-20: SecureEasySetup Location

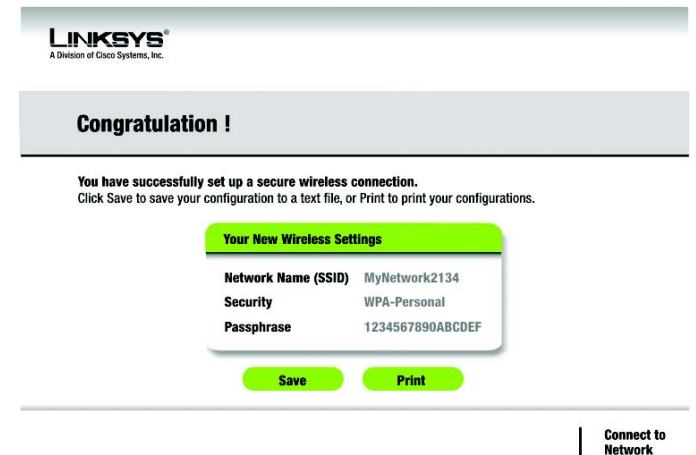


Figure 5-21: Congratulations

Setting Up the Adapter with Available Networks

If you're not setting up the Adapter with SecureEasySetup, another method for setting up the Adapter is with the available networks listed on the *Available Wireless Network* screen. The available networks are listed in the table on the center of the screen by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If you do not see your network listed, you can click the **Refresh** button to bring the list up again.) If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If your network has the wireless security WEP (Wired Equivalent Privacy) enabled, this screen will appear. Select **64-bit or 128-bit**.

Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer 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.)

WEP Key - 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".

Then click **Connect**.

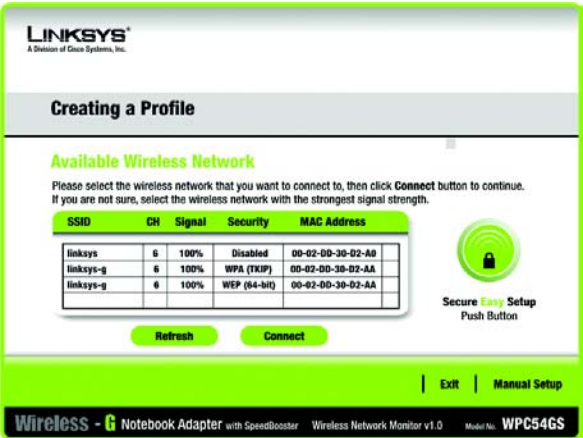


Figure 5-22: Available Wireless Network

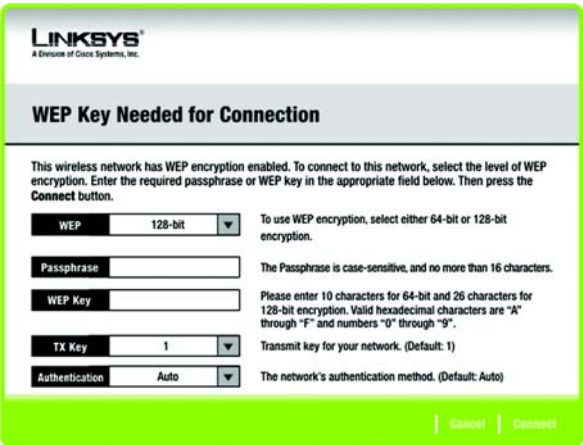


Figure 5-23: WEP Key Needed for Connection

If your network has the wireless security WPA Personal (Wi-Fi Protected Access) enabled, this screen will appear.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

Then click **Connect**.

- After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network.

Congratulations! The setup is complete.

Setting up the Adapter with Manual Setup

- The *Network Settings* screen will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

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.



Figure 5-24: WPA Personal Needed for Connection



Figure 5-25: Congratulations

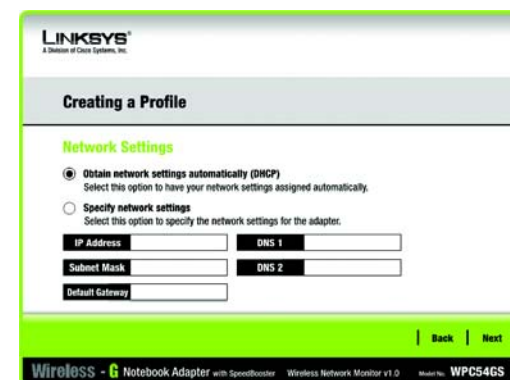


Figure 5-26: WPA Personal Needed for Connection

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

- The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

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

- If you chose **Infrastructure Mode**, go to Step 4 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. 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, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.



Figure 5-27: Network Settings for New Profile

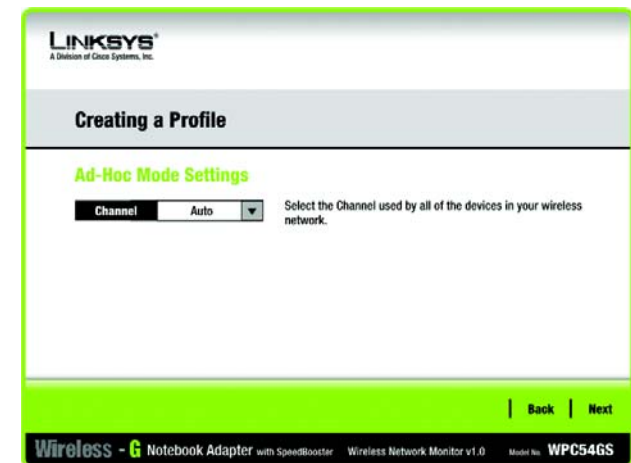


Figure 5-28: Wireless Mode for New Profile

If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 5.

If your wireless network has wireless security, select the method of security used: **WEP**, **WPA-Personal**, **WPA-Enterprise**, **RADIUS**, or **LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA is a stronger security method than WEP. RADIUS stands for Remote Authentication Dial-In User Service, and LEAP stands for Lightweight Extensible Authentication Protocol. Click the **Next** button to continue or the **Back** button to return to the previous screen.

4. Proceed to the appropriate section for your security method: WEP, WPA-Personal, WPA-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit** or **128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so 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 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.)

WEP Key - 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".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication - The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.



Figure 5-29: Ad-Hoc Mode Settings for New Profile

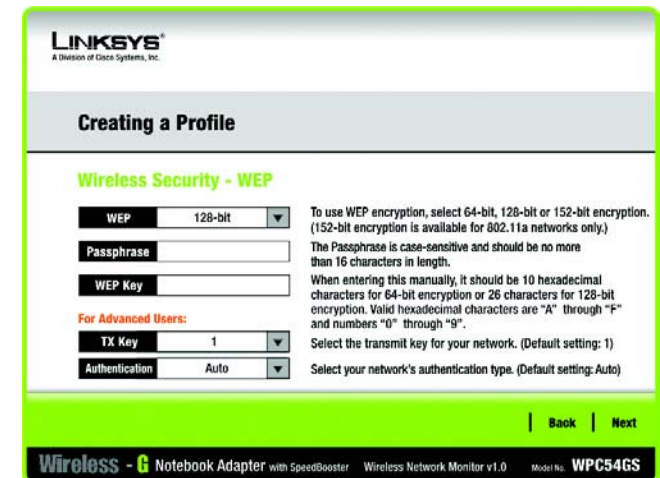


Figure 5-30: Wireless Security for New Profile

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. Select **TKIP** or **AES** for encryption. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-63 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

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



The screenshot shows the 'Creating a Profile' screen in the Linksys Wireless Network Monitor v1.0. The title bar at the top reads 'LINKSYS A Division of Cisco Systems, Inc.' Below the title bar, the main heading is 'Creating a Profile'. Underneath, the section is titled 'Wireless Security - WPA Personal'. There are two main input areas: 'Encryption' with a dropdown menu currently set to 'TKIP', and 'Passphrase' with a text input field. To the right of the 'Encryption' dropdown, there is a note: 'Please select the encryption type used to protect your wireless data transmissions.' To the right of the 'Passphrase' field, there is a note: 'Please enter a Passphrase that is 8 to 63 characters in length.' At the bottom right of the main content area, there are two buttons: 'Back' and 'Next'. The footer of the window contains the text 'Wireless - G Notebook Adapter with SpeedBooster Wireless Network Monitor v1.0 Model No. WPC54GS'.

Figure 5-31: Wireless Security - WEP for New Profile

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. The 'Login Name' field is empty. The 'Server Name' field is empty. The 'Certificate' dropdown is set to 'Trust Any'. The 'Encryption' dropdown is set to 'AES'. The 'Back' and 'Next' buttons are at the bottom right. The footer shows 'Wireless - G Notebook Adapter with SpeedBooster', 'Wireless Network Monitor v1.0', and 'Model No. WPC54GS'.

Figure 5-32: Wireless Security - WPA Personal for New Profile

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. The 'Login Name' field is empty. The 'Password' field is empty. The 'Server Name' field is empty. The 'Certificate' dropdown is set to 'Trust Any'. The 'Inner Authen.' dropdown is set to 'EAP-MSCHAP v2'. The 'Encryption' dropdown is set to 'AES'. The 'Back' and 'Next' buttons are at the bottom right. The footer shows 'Wireless - G Notebook Adapter with SpeedBooster', 'Wireless Network Monitor v1.0', and 'Model No. WPC54GS'.

Figure 5-33: Wireless Security - WPA Enterprise Using EAP-TLS for New Profile

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel.

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

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'EAP-TLS'. Below it are fields for 'Login Name', 'Server Name', and a 'Certificate' dropdown. Instructions on the right side of the screen guide the user to select the authentication method, enter the login name, enter the server name (optional), and select a certificate. At the bottom, there are 'Back' and 'Next' buttons. The footer indicates the device is a 'Wireless - G Notebook Adapter with SpeedBooster' and the model number is 'WPC54GS'.

Figure 5-34: Wireless Security - WPA Enterprise Using PEAP for New Profile

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'PEAP'. Below it are fields for 'Login Name', 'Password', 'Server Name', a 'Certificate' dropdown (set to 'Trust Any'), and an 'Inner Authen.' dropdown (set to 'EAP-MSCHAP v2'). Instructions on the right side of the screen guide the user to select the authentication method, enter the login name, enter the password, enter the server name (optional), select a certificate, and select the inner authentication method. At the bottom, there are 'Back' and 'Next' buttons. The footer indicates the device is a 'Wireless - G Notebook Adapter with SpeedBooster' and the model number is 'WPC54GS'.

Figure 5-35: Wireless Security - RADIUS Using EAP-TLS for New Profile

LEAP

If you selected LEAP, then enter the Username and Password that will authenticate you on your wireless network.

Username - Enter the username used for authentication.

Password - Enter the password used for authentication.

Confirm - Enter the password again.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

3. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button. To edit the new settings, click the **Back** button. To exit the Wireless Network Monitor, click **Exit**.



Figure 5-36: Wireless Security - RADIUS Using PEAP for New Profile



Figure 5-37: Wireless Security - LEAP for New Profile

4. The *Congratulations* screen will appear next. 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.

You have successfully created a connection profile.



Figure 5-38: Confirm New Settings for New Profile

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 Notebook 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/international.

Common Problems and Solutions

1. *My computer does not recognize the Wireless-G Notebook Adapter.*

Make sure that the Wireless-G Notebook Adapter is properly inserted into the PC Card slot.

2. *The Wireless-G Notebook Adapter does not work properly.*

Reinsert the Wireless-G Notebook Adapter into the notebook.

Go to your Control Panel, and select **System**. Select the Hardware tab, then select **Device Manager**, and click on the **Network Adapter**. You will find the Wireless-G Notebook Adapter if it is installed successfully. If you see a yellow exclamation mark, the resources may be conflicting and you must follow the steps below:

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

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

Make sure that the notebook is powered on.

Make sure that the Wireless-G Notebook Adapter is configured with the same SSID and Security settings as the other computers and access point 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

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

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

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.

ism band: radio bandwidth utilized in wireless transmissions.

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

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

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.

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: WPA-Personal, WPA-Enterprise, and Radius. WPA-Personal 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-Enterprise 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-Personal. 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-Enterprise. 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-Enterprise 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.

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 (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.

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 (Dynamic Domain Name System) - 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 (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.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

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.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

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

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - 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 (File Transfer Protocol) - 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 (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

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.

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

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

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.

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

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.

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

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

NAT (Network Address Translation) - 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 (Network News Transfer Protocol) - 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 (Orthogonal Frequency Division Multiplexing) - 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 (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 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 over Ethernet (PoE) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - 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 (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.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - 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 (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

SPI (Stateful Packet Inspection) 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 (Service Set Identifier) - 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 (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.

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

TFTP (Trivial File Transfer Protocol) - 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 (Temporal Key Integrity Protocol) - 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 (User Datagram Protocol) - 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 (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network)- The Internet.

WEP (Wired Equivalent Privacy) - 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 (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

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	IEEE 802.11g, IEEE 802.11b, CardBus
Channels	11 Channels (Most of North, South, and Central America) 13 Channels (Most of Europe, and Asia)
LEDs	Power, Link
Transmit Power	18 dBm
Protocols	802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps); 802.11g: OFDM
Security Features	WEP, AES, TKIP, 802.1x
WEP Key Bits	64, 128 Bit
Dimensions	115 mm x 54 mm x 7.5 mm
Unit Weight	0.047 kg
Certifications	FCC, IC-03, CE
Operating Temp.	0°C to 55°C
Storage Temp.	-25°C to 70°C
Operating Humidity	5% to 95%, Non-Condensing
Storage Humidity	5% to 95%, Non-Condensing

Appendix F: Warranty Information

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.

This Warranty is valid and may be processed only in the country of purchase.

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 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.

Industry Canada (Canada)

This device complies with Canadian ICES-003 and RSS210 rules.

Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industry Canada.

Compliance Information for 2.4-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Wireless-G Notebook Adapter with SpeedBooster

Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

NOTE: For all products, the Declaration of Conformity is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit www.linksys.com/international and select your country or region. Then select your product.

If you need any other technical documentation, see the “Technical Documents on www.linksys.com/international” section, as shown later in this appendix.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

CE Marking

For the Linksys Wireless-B and Wireless-G products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.



Check the CE label on the product to find out which notified body was involved during the assessment.

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check <http://www.bipt.be> for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie <http://www.bipt.be> voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez <http://www.ibpt.be> pour de plus amples détails.

France

In case the product is used outdoors, the output power is restricted in some parts of the band. See Table 1 or check <http://www.art-telecom.fr/> for more details.

Dans la cas d'une utilisation en extérieur, la puissance de sortie est limitée pour certaines parties de la bande. Reportez-vous à la table 1 ou visitez <http://www.art-telecom.fr/> pour de plus amples détails.

Table 1: Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner's property, the use of this 2.4 GHz Wireless LAN product requires a 'general authorization'. Please check with <http://www.comunicazioni.it/it/> for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2.4 GHz richiede una "Autorizzazione Generale". Consultare <http://www.comunicazioni.it/it/> per maggiori dettagli.

Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended.

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

Power Output of Your Device

To comply with your country's regulations, you may have to change the power output of your wireless device. Proceed to the appropriate section for your device.

NOTE: The power output setting may not be available on all wireless products. For more information, refer to the documentation on your product's CD or <http://www.linksys.com/international>.

Wireless Adapters

Wireless adapters have the power output set to 100% by default. Maximum power output on each adapter does not exceed 20 dBm (100 mW); it is generally 18 dBm (64 mW) or below. If you need to alter your wireless adapter's power output, follow the appropriate instructions for your computer's Windows operating system:

Windows XP

1. Double-click the **Wireless** icon in your desktop's system tray.
2. Open the *Wireless Network Connection* window.
3. Click the **Properties** button.
4. Select the **General** tab, and click the **Configure** button.
5. In the *Properties* window, click the **Advanced** tab.
6. Select **Power Output**.
7. From the pull-down menu on the right, select the wireless adapter's power output percentage.

Windows 2000

1. Open the **Control Panel**.
2. Double-click **Network and Dial-Up Connections**.
3. Select your current wireless connection, and select **Properties**.
4. From the *Properties* screen, click the **Configure** button.
5. Click the **Advanced** tab, and select **Power Output**.
6. From the pull-down menu on the right, select the wireless adapter's power setting.

If your computer is running Windows Millennium or 98, then refer to Windows Help for instructions on how to access the advanced settings of a network adapter.

Wireless Access Points, Routers, or Other Wireless Products

If you have a wireless access point, router or other wireless product, use its Web-based Utility to configure its power output setting (refer to the product's documentation for more information).

Technical Documents on www.linksys.com/international

Follow these steps to access technical documents:

1. Browse to <http://www.linksys.com/international>.
2. Click the region in which you reside.
3. Click the name of the country in which you reside.
4. Click **Products**.
5. Click the appropriate product category.
6. Select a product.
7. Click the type of documentation you want. The document will automatically open in PDF format.

NOTE: If you have questions regarding the compliance of these products or you cannot find the information you need, please contact your local sales office or visit <http://www.linksys.com/international> for more details.

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/international>

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Denmark	support.dk@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Portugal	support.pt@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom & Ireland	support.uk@linksys.com

Outside of Europe	E-mail Address
Latin America	support.la@linksys.com
U.S. and Canada	support@linksys.com
Asia Pacific	asiasupport@linksys.com (English only)