LINKSYS®

A Division of Cisco Systems, Inc.

2.4 GHz 802.11g

Wireless-G

CompactFlash Card

User Guide

WIRELESS

CISCO SYSTEMS

Model No. WCF54G

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 © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

> **WARNING:** This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. *Wash hands after handling.*

How to Use this User Guide

The user guide to the CompactFlash Card has been designed to make understanding networking with the Access Point easier than ever. Look for the following items when reading this User Guide:

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

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

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

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.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G CompactFlash Card.

The Wireless-G CompactFlash Card installs directly into your Pocket PC using a CompactFlash Type II slot. The user-friendly software makes it a snap to set up, and you're ready to share data, printers, or high-speed Internet access over your existing wireless network at speeds up to 54Mbps. It's also compatible with Wireless-B (802.11b) wireless networks.

Use the Wireless CompactFlash Card to connect your PDA to wireless networks at the office, at home, or in any of the growing number of public wireless hotspot venues springing up in coffee shops, airport lounges, hotels and convention centers.

Use the instructions in this Guide to help you connect the CompactFlash Card, set it up, and configure it to communicate with your PDA and PC. These instructions should be all you need to get the most out of the CompactFlash Card.

What's in this Guide?

This user guide covers the steps for setting up and using the Dual-Band Wireless A+G Notebook Adapter.

- Chapter 1: Introduction
  This chapter describes the Adapter's applications and this User Guide.

- Chapter 2: Getting to Know the Wireless-G CompactFlash Card
  This chapter describes the physical features of the Adapter.

- Chapter 3: Setting Up the PDA
  This chapter instructs you on how to use the Card's Setup Wizard.

- Chapter 4: Installing the CompactFlash Card
  This chapter shows you how to install CompactFlash Card into your PDA.

- Chapter 5: Connecting to a Wireless Network
  This chapter shows you how to connect the CompactFlash Card to a wireless network.

- Chapter 6: Configuring the Wireless-G CompactFlash Card with the Wireless Network Monitor
  This chapter show you how to use the CompactFlash Card's Wireless Network Monitor.

- Appendix A: Troubleshooting
  This appendix describes some potential problems and solutions, as well as frequently asked questions, regarding installation and use of the CompactFlash Card.

- 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 CompactFlash Card's technical specifications.

- Appendix F: Warranty Information
  This appendix supplies the CompactFlash Cards warranty information.

- Appendix G: Regulatory Information
  This appendix supplies the CompactFlash Card's regulatory information.

- Appendix H: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Getting to Know the Wireless-G CompactFlash Card

The Front Panel

The CompactFlash Card's LEDs, where information about network activity is displayed, are located on the front panel.

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

Link   Green. If the **Link** LED is flickering, the CompactFlash Card is actively sending or receiving data to or from one of the devices on the network.

Figure 2-1: Front Panel

Chapter 3: Setting Up the PDA

Overview

This Setup Wizard will take you through all the steps necessary to install the Card's software on your PC so it can communicate with the PDA.

Connect your PDA to your PC. Make sure you have the Microsoft ActiveSync software installed on your PC. Refer to your PDA's documentation for information on Microsoft ActiveSync software.

⚠️ **IMPORTANT:** Do not insert the Card before installing the Setup Wizard or the setup will not work.

Setup Wizard

1. Insert the Setup Wizard CD into your PC's CD-ROM drive.

2. The Setup Wizard's Welcome screen should appear automatically on your monitor. If this screen does not appear automatically, you can access it by clicking the Start button and choosing Run. In the drop-down box, type d:\setup.exe (if "d" is the letter of your CD-ROM drive) and click **OK**.

   Click the **Install** button to continue this Setup Wizard. Clicking the User Guide button opened this Guide. To exit this Setup Wizard, click the **Exit** button.

3. The following screen displays the License Agreement. Read the agreement, then if you agree, click **Next** to continue.

   Click **Cancel** if you want to close the Setup Wizard.

Figure 3-1: PDA to PC Installation

Figure 3-2: Welcome
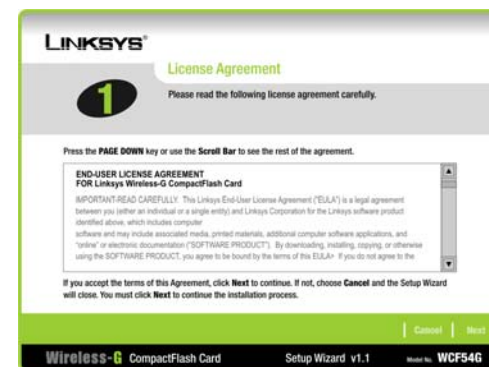
Figure 3-3: License Agreement

4. When asked if you want to install the Linksys Wireless-G CompactFlash Card using the default application install directory, click **Yes** to continue.

.
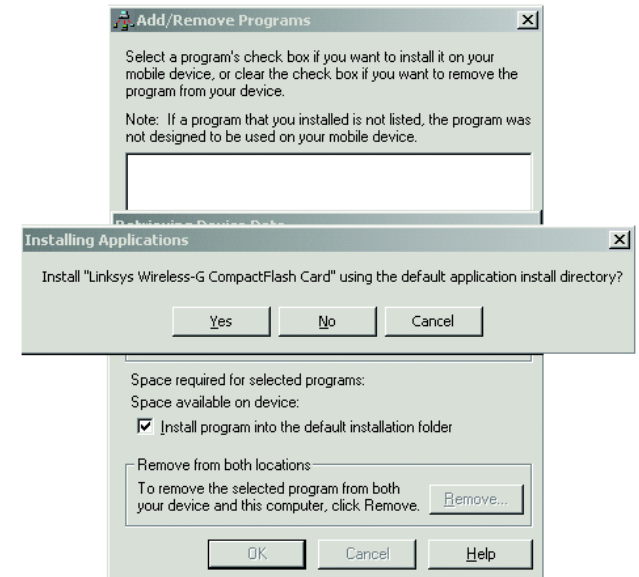
Figure 3-4: Click Yes

5. A screen will appear to show that the application is being installed. Do **NOT** cancel.
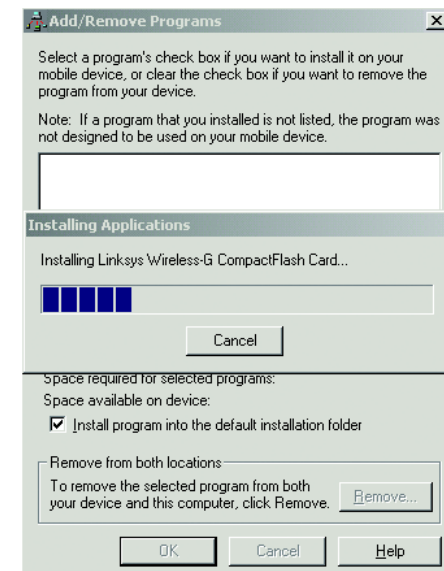
Figure 3-5: Application Being Installed

6. When asked to check your mobile device screen to see if additional steps are necessary to complete this installation, click **OK**.
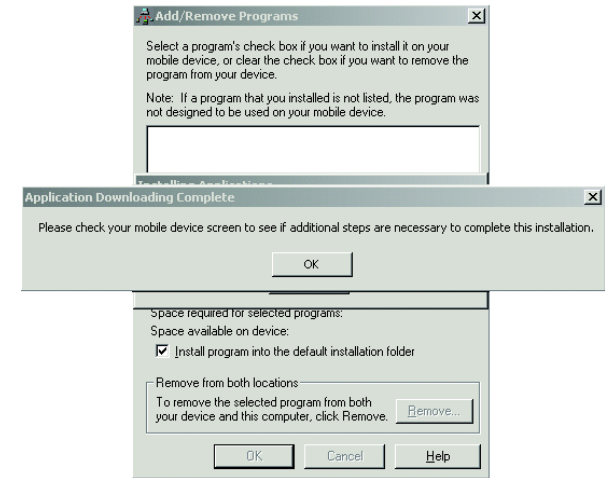
Figure 3-6: Mobile Device

7. The Congratulations screen will appear when the installation is complete. Click **Exit** to exit the Setup Wizard.

Figure 3-7: Congratulations

Chapter 4: Installing the CompactFlash Card

Overview

This chapter explains the steps to install the CompactFlash Card. Make sure that you have installed the Setup Wizard software before installing the Card.

⚠️ **IMPORTANT:** Make sure that the Setup Wizard software is installed before installing the Card.

Installing the Card

1. After installing the Setup Wizard software, the *Installation has completed successfully* screen will appear on your PDA. Click **OK**.

2. Disconnect the PDA from your PC.

3. Insert the Wireless CompactFlash Card into your PDA.

Figure 4-1: Successful Installation

Figure 4-2: CompactFlash Installation into PDA

4. The *Start* screen in will appear for Pocket PC 2002 users. The default setting is *Use server-assigned IP address*. In most cases, you should keep the default setting. However, if you are using fixed IP addresses on your wireless network, then click the radio button next to *Use specific IP address*, and complete the IP address, Subnet mask, and Default gateway fields. Click the **OK** button to close the screen.
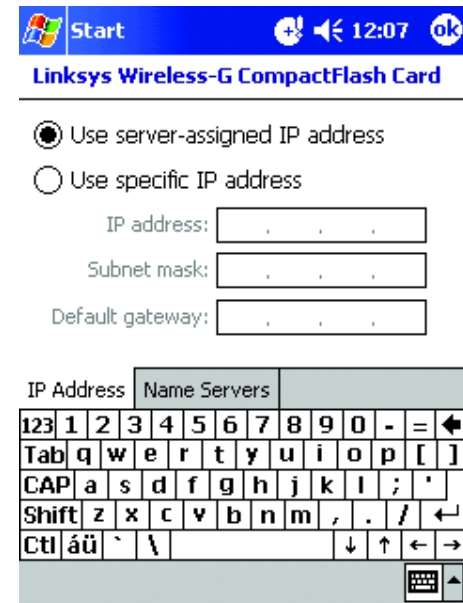
Figure 4-3: Start Screen

5. The Wireless Network Monitor icon will appear on the desktop of your PDA.

Figure 4-4: Wireless Network Monitor Icon

Uninstalling the Card

To uninstall the Card, on your PDA, click **Start**, **Settings**, then click **Remove Programs**. Select **Linksys Wireless-G CompactFlash Card**, and click **Remove**.

Chapter 5: Connecting to a Wireless Network

Overview

This chapter explains how to connect your PDA to a wireless network.

Connect to a Wireless Network

1. On your PDA's desktop, click the **Wireless Network Monitor icon** at the bottom of the desktop.

Figure 5-1: Wireless Network Monitor Icon

2. The Status screen will appear. Click **Configure Wireless Networks** near the bottom of the screen.
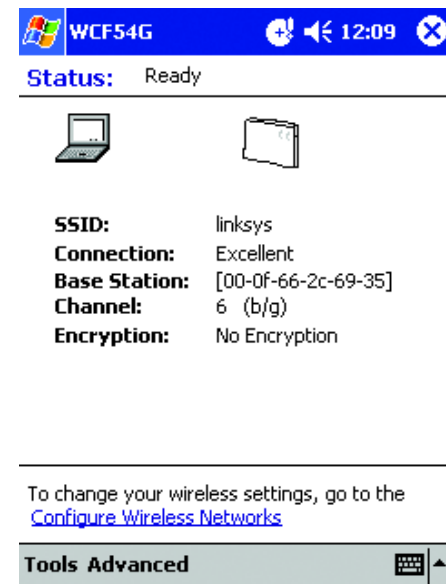
3. Continue to the section for the Pocket PC operating system that your PDA uses.

Figure 5-2: Status Screen

Pocket PC 2003

1. Select your wireless network from the list and click **Connect**.
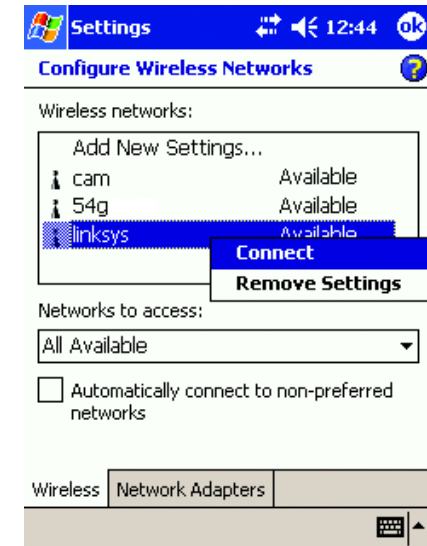
Figure 5-3: Configure Wireless Networks

2. On the Settings screen, if your wireless network does <u>not</u> have Wireless Security-WEP, click **OK**, then go to step D.

    If your wireless network has Wireless Security-WEP, click **Authentication**.
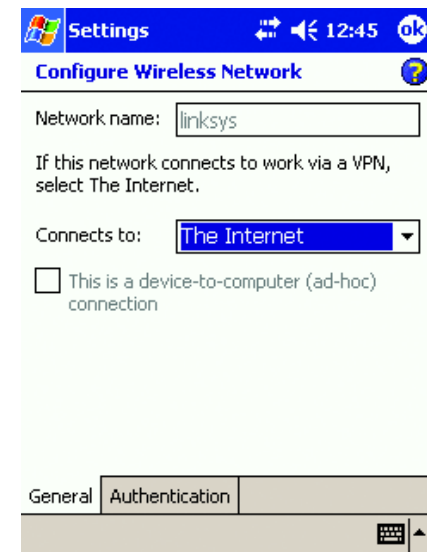
Figure 5-4: Settings

3. When the *Configure Network Authentication* screen appears, Check the box for **Data encryption (WEP Enabled)** and uncheck the box for **The Key is provided for me automatically.** Enter the *Network key* in the field and click **OK**.
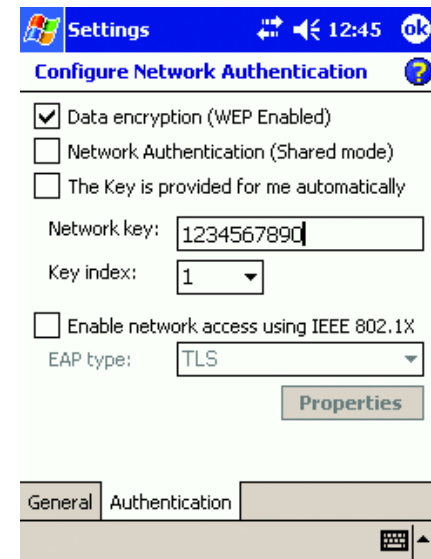
Figure 5-5: Configure Network Authentication

4. The next screen will show that the PDA is connected to the wireless network. Click **OK**.

The installation of the Wireless-G CompactFlash Card is complete.
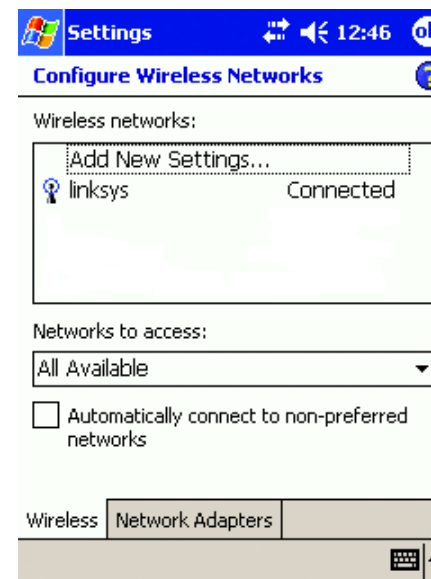
Figure 5-6: PDA Connected

Pocket PC 2002

1. When the *Configure Wireless Networks* screen appears, select the **Default** profile and click **Edit**.
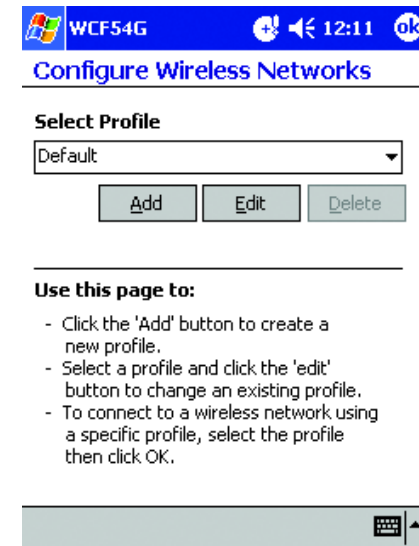
Figure 5-7: Configure Wireless Networks

2. On the *Add/Edit Configuration* screen, select **Access Point** from the drop-down menu for *Wireless Mode*. Click **Next**.
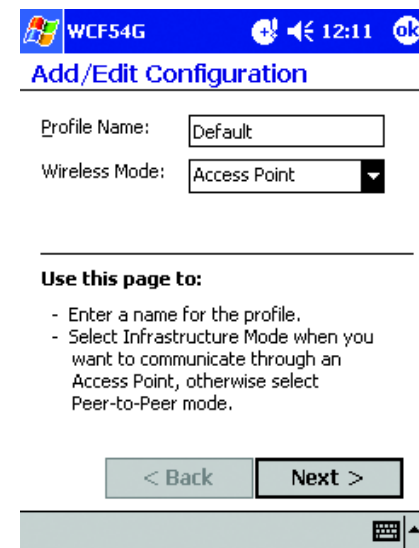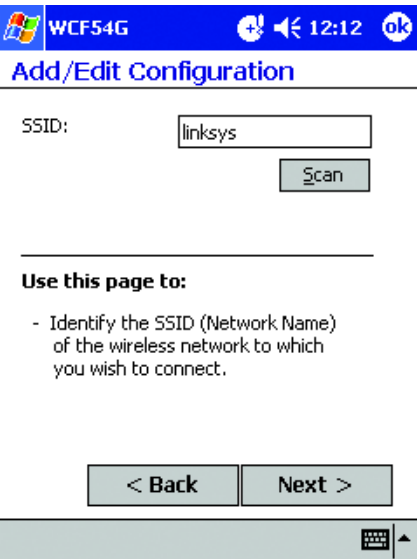
Figure 5-8: Add/Edit Configuration
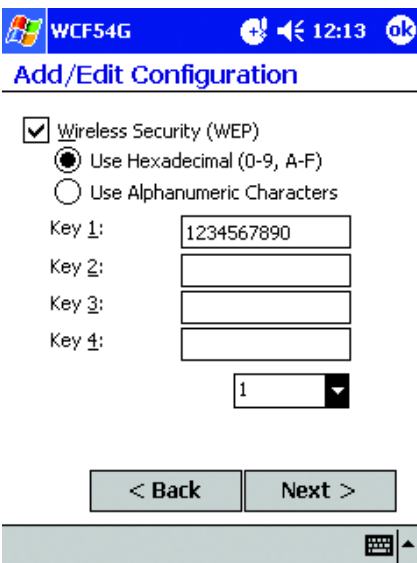
3. On the next screen, enter the name of your wireless network in the *SSID* field. You can click **Scan** to search for an existing wireless network name. Click **Next**.

Figure 5-9: SSID

4. If your wireless network has Wireless Security-WEP, check **Wireless Security (WEP)**. Then select **Use Hexadecimal (0-9, A-F)** and enter the WEP key in a *Key* field. Click **Next**.

Figure 5-10: Wireless Security (WEP)

5. *Power Management* is a power saving mode. The lower power consumption may also lower the wireless performance. To enable Power Management, select **On**. To disable Power Management, select **Off**. Then, click **Finish.**
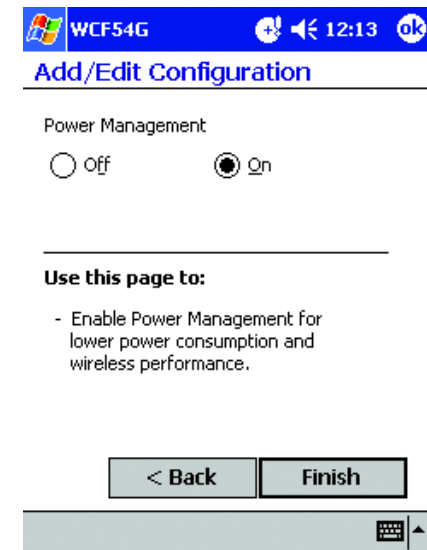
Figure 5-11: Power Management

6. You will return to the *Select Profile* screen. Click **OK**.

The installation of the Wireless-G CompactFlash Card is complete.
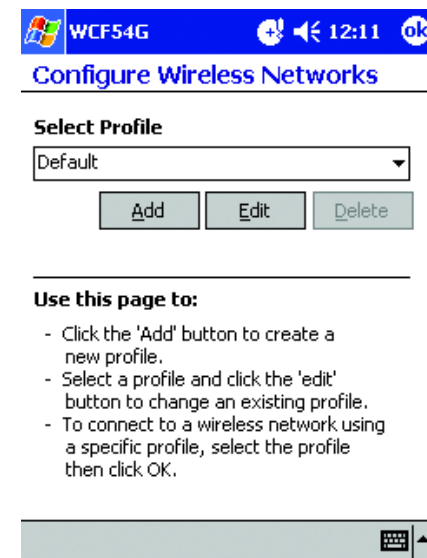
Figure 5-12: Select Profile

Chapter 6: Configuring the Wireless-G CompactFlash Card with the Wireless Network Monitor

Overview

the CompactFlash Card can be configured with the Wireless Network Monitor. This chapter explains how to configure the CompactFlash Card in this manner.

On your PDA's desktop, click the **Wireless Network Monitor icon** at the bottom of the screen.

Wireless Network Monitor

The *Status* screen appears first. It displays the status of your wireless connection.

SSID. The network name.

Connection. The strength of the wireless connection is displayed.

Base Station. The MAC Address of the device you are connected to.

Channel. The wireless network channel, between 1 and 11 in North America will be displayed.

Encryption. The Wireless Security-WEP option is displayed.

Three options are available. Select from Tools, Advanced, Configure Wireless Networks. The options are described below.

Tools

There are many tools available for your use. They are described below.

Exit. Select **Exit** to exit the Wireless Network Monitor.

Turn Radio. Select **Turn Radio Off** to disable the wireless connection. Select **Turn Radio On** to enable the wireless connection.

Figure 6-1: Wireless Network Monitor Icon
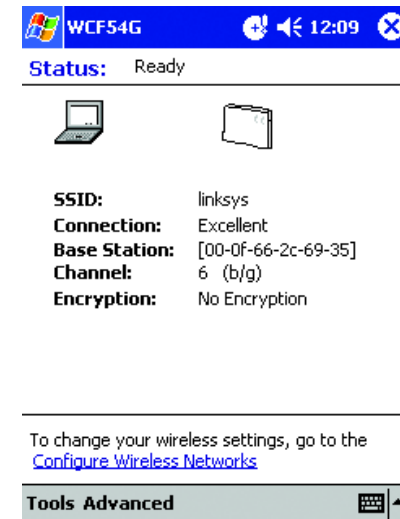
Figure 6-2: Status Screen

Power Management. **Power Management** is a power saving mode. The lower power consumption may lower the wireless performance. Select **On** to enable Power Management. Select **Off** to disable Power Management.

Version Information. Select **Version Information** to view information about the driver. Included is the Client, Driver Name, Driver Version, Primary Firmware Version, and Station Firmware Version.

Wireless Advanced. The advanced wireless settings are displayed on this screen.

Country. This is used to send 802.11d country information when an access Point or IBSS operation is used. 802.11d is a specification used in countries where the 802.11 family is not allowed to operate. IBSS, Independent Basic Service Set, is also referred to as peer-to-peer mode or Ad-hoc mode. Select the location.

Power Mode. This is a power management mode. Select **Disabled** or **Automatic**.

Cell Size. The smaller the cell-size system, the modem will hand over quicker to the access point than in a large cell-size system. Select from **Large**, **Medium**, **Small**, **Minicell**, **Microcell**.

Tx Power. You can select the power output used to transmit data. Select from **8**, **10**, **12**, **14**, **16**, **18**, **20**.

Tx Rates. You can select the rates that the device will use to transmit data. Select from **1Mbps**, **2Mbps**, **5.5Mbp**s, **11Mbps**, **6Mbps**, **9Mbps**, **12Mbps**, **18Mbps**, **24Mbps**, **36Mbps**, **48Mbps** and **54Mbps**.

Force long preamble. This forces a long wireless signal that synchronizes network traffic. Select **Force long preamble** only when there is an interoperability issue with an access point.

Allow 802.11g Operation in IBSS. IBSS mode uses only CCK data rates. IBSS, Independent Basic Service Set, is also referred to as peer-to-peer mode or Ad-hoc mode. Select this option to support the extended OFDM data rates.

Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS)

Reset to Default Values. Reset to the default values on this page by clicking the **Defaults** button.
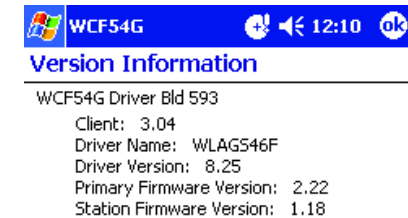
Figure 6-3: Version Information Screen
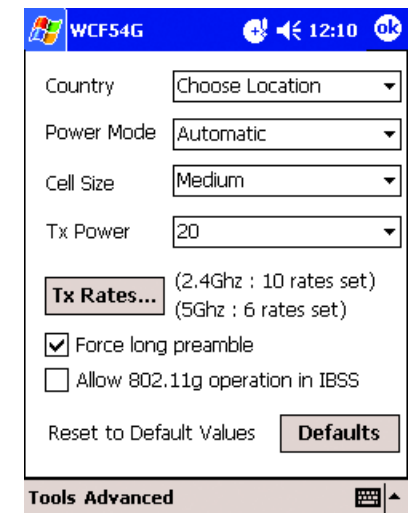
Figure 6-4: Wireless Advanced Screen

Advanced

These advanced options are offered: Network Troubleshooting and Site Survey. See below for descriptions.

Network Troubleshooting. The IP address and Gateway address of the CompactFlash Card is displayed.

For information on the connection, click **More Info**. The *More Information* screen will appear. The MAC Address, IP Address, Subnet Mask, DHCP Server, Gateways, and DNS are displayed. The IP Forward Table displays the Destination, Mask, Interface, Next Hop, Policy, Type Protocol, Age, Next Hop AS, Metric 1, Metric 2, Metric 3, and Metric 4.

The MAC Address. The MAC address of the Card is displayed.

IP Address. The IP address of the Card is displayed.

Subnet Mask. The Subnet Mask of the Card is displayed.

DHCP Server. The assigned IP, Subnet Mask, Gateway, and DNS address of your network's server.

Gateway. The network's Gateway IP address is displayed.

DNS. The Domain Name Server (DNS) address of the Card is displayed.

IP Forwarding Table

Destination. The destination IP address is displayed.

Mask. The Subnet Mask of the destination IP address is displayed.

Interface. The interface of the destination IP address is displayed.

Next Hop. On remote routes, this is the address of the next system on the route.

Policy. The general set of conditions that would cause the selection of a multi-path route.

Type. This is the type of route.

Age. The time in seconds since the route was last updated.

Next Hop AS. This is the Autonomous System number of the Next Hop.
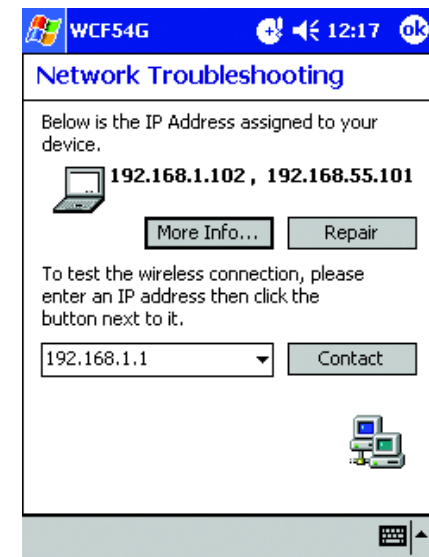
Figure 6-5: Network Troubleshooting Screen
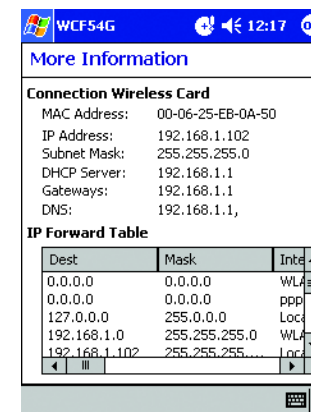
Figure 6-6: More Information Screen
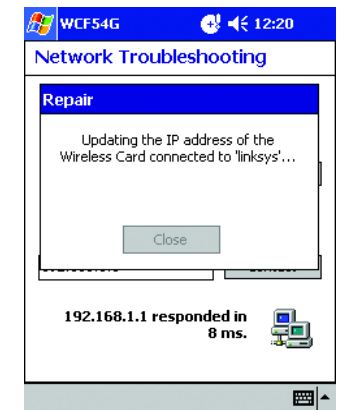
Figure 6-7: Repair Screen

Metric 1- 4. This is a routing metric.

To update the IP address for the Card, click **Repair**. The *Repair* screen will appear.

You can check the connection by entering the IP Address into the field, then clicking **Contact**. The *Contact* screen will appear.
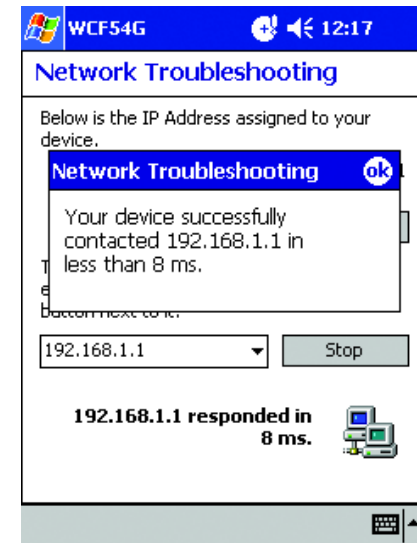
Figure 6-8: Contact Screen

Site Survey. To search for an existing wireless network, select **Site Survey**. To view more information on an wireless network, select the wireless network, then click **Open**. The SNR, Signal Noise, Channel, and Privacy of the wireless network will be displayed.

SNR. SNR, signal-to-noise ratio, is the ratio of the amplitude of a data signal to the amplitude of noise in a transmission channel. SNR is displayed in decibels (dB).

Signal Noise. The transmission signal noise of the wireless network is displayed.

Channel. The wireless network transmission channel is displayed.

Privacy. The privacy of the wireless network is displayed.
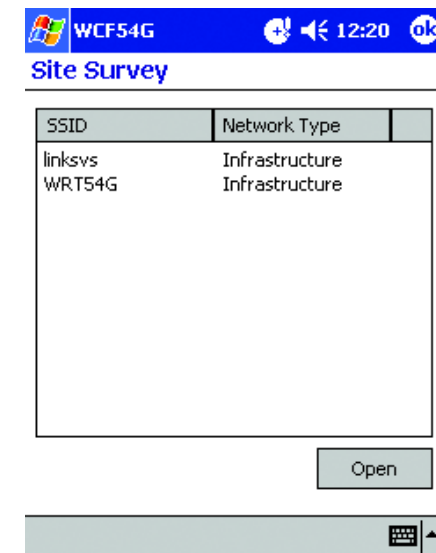
Figure 6-9: Site Survey Screen

Configure Wireless Networks

To configure or connect to a wireless network for a Pocket PC 2002, click Configure Wireless Networks. If you use a Pocket PC 2003, on your PDA, click **Start**, **Help**, then **Connections** or refer to Chapter 5: Connecting to a Wireless Network.

Through the Configure Wireless Networks screen, you can create a new profile, edit an existing profile, or connect to a wireless network using an existing profile. To use a profile to connect, select a profile, then click **OK**. To create a new profile, enter a profile name, then click **Add**. To edit a profile, select the profile, then click **Edit**. To delete a profile, select the profile, then click **Delete**.

Figure 6-10: Select Profile Screen

Add/Edit Configuration

Profile Name. Enter a name for your profile.

Wireless Mode. Select from Access Point, Peer-to-Peer Group, or Act as a BaseStation.

Access Point. If you want to connect to an access point, select **Access Point**.

Peer-to-Peer Group. If you want to connect to a wireless network that doesn't use an access point, select **Peer-to-Peer**.

Act as BaseStation. If you want other users to connect to your PDA as an Access Point, select **Act as BaseStation**.

Click **Next** to continue.

Figure 6-11: Add/Edit Configuration Screen

Chapter 6: Configuring the Wireless-G CompactFlash Card with the Wireless Network Monitor
Wireless Network Monitor

21

Access Point

Enter the name of your wireless network in the *SSID* field. You can click **Scan** to search for an existing wireless network name. Click **Next**.

Figure 6-12: SSID Screen

If your wireless network has Wireless Security-WEP, check **Wireless Security (WEP)**.

For most wireless networks, select **Use Hexadecimal (0-9, A-F)** and enter the WEP key. For 64-bit encryption, enter exactly 10 hexadecimal characters, in a *Key* field. For 128-bit encryption, enter 26 hexadecimal characters. Hexadecimal characters are the numbers "0-9", and the letters "a-f".

If your network uses Alphanumeric characters, select Use **Alphanumeric Characters**. For 64-bit encryption, enter any 5 characters in a *Key* field. For 128-bit encryption, enter any 13 characters.

Select the same number for a Transmit Key from the numbered drop-down menu that was selected for the key number. Click **Next**.

Figure 6-13: Wireless Security (WEP) Screen

Power Management is a power saving mode. The lower power consumption may lower the wireless performance. To enable power management, select **On**. To disable Power Management, select **Off**. Click **Finish**, then you will return to the *Select Profile* screen. Click **OK**.
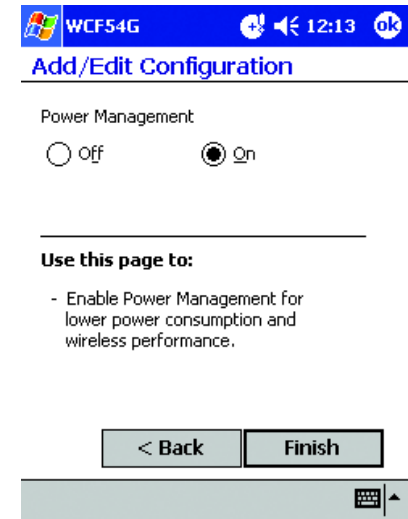
Figure 6-14: Power Management Screen

Peer-to-Peer and Act as a BaseStation

Enter the SSID or network name used by your network. Select the channel used by your network. The choice is 1-11 in North America. Click **Next** to continue. Click **Back** to return to the previous screen.
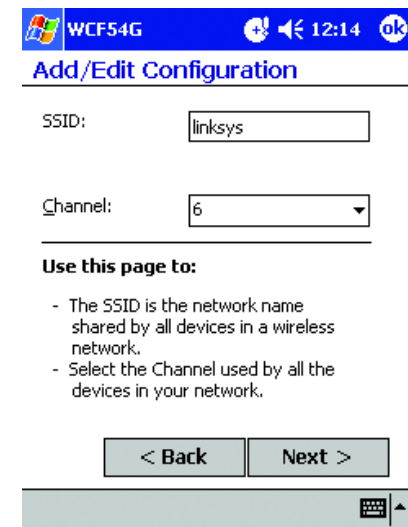
Figure 6-15: SSID/Channel Screen

Chapter 6: Configuring the Wireless-G CompactFlash Card with the Wireless Network Monitor
Wireless Network Monitor

23

If your wireless network has Wireless Security-WEP, check **Wireless Security (WEP)**.

For most wireless networks, select **Use Hexadecimal (0-9, A-F)** and enter the WEP key. For 64-bit encryption, enter exactly 10 hexadecimal characters, in a *Key* field. For 128-bit encryption, enter 26 hexadecimal characters. Hexadecimal characters are the numbers "0-9", and the letters "a-f".

If your network uses Alphanumeric characters, select Use **Alphanumeric Characters**. For 64-bit encryption, enter any 5 characters in a *Key* field. For 128-bit encryption, enter any 13 characters.

Click **Finish**.
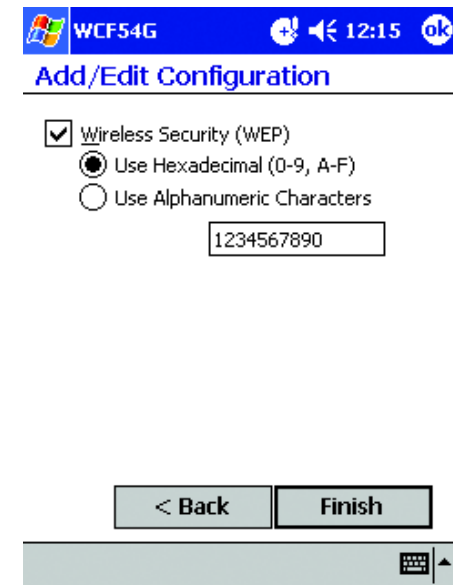
Figure 6-16: Wireless Security (WEP) Screen

Chapter 6: Configuring the Wireless-G CompactFlash Card with the Wireless Network Monitor
Wireless Network Monitor

24

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 this product. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Common Problems and Solutions

1. **My PDA does not recognize the Wireless CompactFlash Card.**
   - Make sure that the Wireless CompactFlash Card is properly inserted into the CompactFlash port.
   - Make sure the Link LED is solidly lit.

2. **The Wireless CompactFlash Card does not work properly.**
   - Reinsert the Wireless CompactFlash Card into the PDA's CompactFlash port.
   - Uninstall the utility and driver software from your PC and PDA device.
   - Restart your PC, and repeat the software and hardware installation as specified in this User Guide.

3. **3. I cannot communicate with the Access Point in the Infrastructure network.**
   - Make sure that the Access Point is powered on.
   - Make sure that your Wireless CompactFlash Card is configured with the same channel, SSID, and WEP settings as the Access Point.

Frequently Asked Questions

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

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

What 802.11b features are supported?

The product supports the following 802.11b functions:

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

What 802.11g features are supported?

The product supports the following 802.11g functions:

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

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 set to the same channel number with the Access Point of the dedicated coverage area.

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

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

Can Wireless products support printer sharing?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with NetWare, Windows 2000, or other LAN operating systems to support printer or file sharing.

What is WEP?

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

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 or router.

Appendix B: Wireless Security

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

Security Precautions

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

1. Change the default SSID.

2. Disable SSID Broadcast.

3. Change the default password for the Administrator account.

4. Enable MAC Address Filtering.

5. Change the SSID periodically.

6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.

7. Change the WEP encryption keys periodically.

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

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

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

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

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

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

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

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

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

Appendix C: Glossary

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

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

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

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

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

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

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

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

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

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

Bit - A binary digit.

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

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

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

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

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

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

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

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

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

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

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

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

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

DMZ (**Dem**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

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

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

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

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

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

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

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

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

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

Firmware - The programming code that runs a networking device.

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

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

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

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

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

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

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

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

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

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

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

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

ISM band - Radio bandwidth utilized in wireless transmissions.

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

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

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

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

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

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

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

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

NAT (**N**etwork **A**ddress **T**ranslation) **Traversal** -A method of enabling specialized applications, such as Internet phone calls, video, and audio, to travel between your local network and the Internet. STUN is a specific type of NAT traversal.

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

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

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

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

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

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

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

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

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

Router - A networking device that connects multiple networks together.

RTP (**R**eal-time **T**ransport **P**rotocol) - A protocol that enables specialized applications, such as Internet phone calls, video, and audio, to occur in real time.

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

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

SMTP (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 incoming packets of information before allowing them 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.

STUN (Simple Traversal of UDP through NATs) - A protocol that enables specialized applications, such as Internet phone calls, video, and audio, to travel between your local network and the Internet. STUN is a specific type of NAT traversal.

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

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

Upload - To transmit a file over a network.

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

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

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

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

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

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

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

Appendix D: Specifications

Standards	IEEE 802.11b, IEEE 802.11g, Type II CompactFlash
LEDs	Link, Power
Transmit Power	802.11g: 15dBm Typical @ Normal Temp Range 802.11b: 20dBm Typical @ Normal Temp Range
TX Peak	350mA @ 54Mbps
RX Peak	270mA @ 54Mbps
Security Features	WEP Encryption
WEP key bits	64, 128
Dimensions	1.69" x 0.27" x 2.32" (43 mm x 6.9 mm x 59mm)
Unit Weight	0.86 oz. (0.025 kg)
Certifications	FCC
Operating Temp.	0ºC to 50ºC (32ºF to 122ºF)
Storage Temp.	-20ºC to 70ºC (-4ºF to 158ºF)
Operating Humidity	5% to 95% Non-Condensing
Storage Humidity	5% to 95% Non-Condensing

Appendix E: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix F: Regulatory Information

FCC STATEMENT

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

Reorient or relocate the receiving antenna

Increase the separation between the equipment or devices

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

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

FCC 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 Class B digital apparatus complies with Canadian ICES-003, RSS210.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.
The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

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

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

EN 609 50 Safety

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

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

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

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

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

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

Belgique:

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

France:

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

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

SAFETY NOTICES

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

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

41

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

FCC PART 68 STATEMENT

This equipment complies with Part 68 of the FCC Rules. A label is attached to the equipment that contains, among other information, its FCC registration number and ringer equivalence number. If requested, this information must be provided to the telephone company.

This equipment uses the following USOC Jack: RJ-11.

An FCC compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack, which is FCC Part 68 compliant. Connection to the telephone network should be made by using the standard modular telephone jack.

The REN is useful to determine the quantity of devices that may be connected to the telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of RENs should not exceed 5. To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area.

If this equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

In the event this equipment should fail to operate properly, disconnect the unit from the telephone line. Try using another FCC approved device in the same telephone jack. If the trouble persists, call the telephone company repair service bureau. If the trouble does not persist and appears to be with this unit, disconnect the unit from the telephone line and discontinue use of the unit until it is repaired. Please note that the telephone company may ask that you disconnect the equipment from the telephone network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. The user must use the accessories and cables supplied by the manufacturer to get optimum performance from the product.

No repairs may be done by the customer. If trouble is experienced with this equipment, please contact your authorized support provider for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you remove the equipment from the network until the problem is resolved. This equipment cannot be used on telephone company provided coin service. Connection to Party Line Service is subject to state tariffs.

Appendix G: Contact Information

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

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

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

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

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com