LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz 802.11g **Wireless-G**

WIRELESS

USB Network Adapter with Wi-Fi Finder

User Guide

Model No. **WUSBF54G**

CISCO SYSTEMS

Copyright and Trademarks

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

This User Guide has been designed to make understanding networking with the Wireless-G USB Network Adapter with Wi-Fi Finder 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 Wireless-G USB Network Adapter with Wi-Fi Finder.

This exclamation point means there is a Caution or warning and is something that could damage your property or the Wireless-G USB Network Adapter with Wi-Fi Finder.

This question mark provides you with a reminder about something you might need to do while using the Wireless-G USB Network Adapter with Wi-Fi Finder.

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

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G USB Network Adapter with Wi-Fi Finder. With this Adapter, your wireless networking experience will be faster and easier than ever.

How does the Adapter do this? Like all wireless products, the Adapter allows for greater range and mobility within your wireless network. Connecting to your PC via the USB port means that this Adapter leaves the PC's slots open for other purposes. This adapter communicates over the 802.11g wireless standard, one of the newest wireless standards, to communicate with your network. It also has a convenient Wi-Fi Finder that enables you to find an available wireless network to connect to with just a click of a button.

But what does all of this mean?

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

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.

Use the instructions in this Guide to help you connect the Adapter, set it up, and configure it for your network. These instructions should be all you need to get the most out of the Adapter.

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.*

802.11g: *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.*

What's in this Guide?

This user guide covers the steps for setting up and using the Wireless-G USB Network Adapter with Wi-Fi Finder.

- 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: Setting Up and Connecting the Wireless-G USB Network Adapter with Wi-Fi Finder.
  This chapter shows you how to setup and connect the Adapter.
- Chapter 4: 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: Using Windows XP Wireless Configuration
  This appendix describes how Windows XP users can use Window's built-in wireless configuration to monitor their Adapter.
- Appendix C: Wireless Security
  This appendix discusses security issues regarding wireless networking and measures you can take to help protect your wireless network.
- Appendix D: Windows Help
  This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix F: Specifications
  This appendix provides the Adapter's technical specifications.
- Appendix G: Warranty Information
  This appendix supplies the Adapter's warranty information.

- Appendix H: Regulatory Information
  This appendix supplies the Adapter's regulatory information.

- Appendix I: 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.

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

***access point**: device that allows wireless-equipped computers and other devices to communicate with a wired network.*

***infrastructure**: Configuration in which a wireless network is bridged to a wired network via an access point.*

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.

***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 at 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 for more information about wireless products.

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*: an IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.* It is backward compatibility with 802.11b devices.

switch*: device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds.*

router*: a networking device that connects multiple networks together, such as a local network and the Internet.*

Chapter 3: Getting to Know and Using the Wireless-G Network Adapter with Wi-Fi Finder

The Front Panel

The Network Adapter's LEDs and Wi-Fi Finder LCD screen are located on the Front Panel.

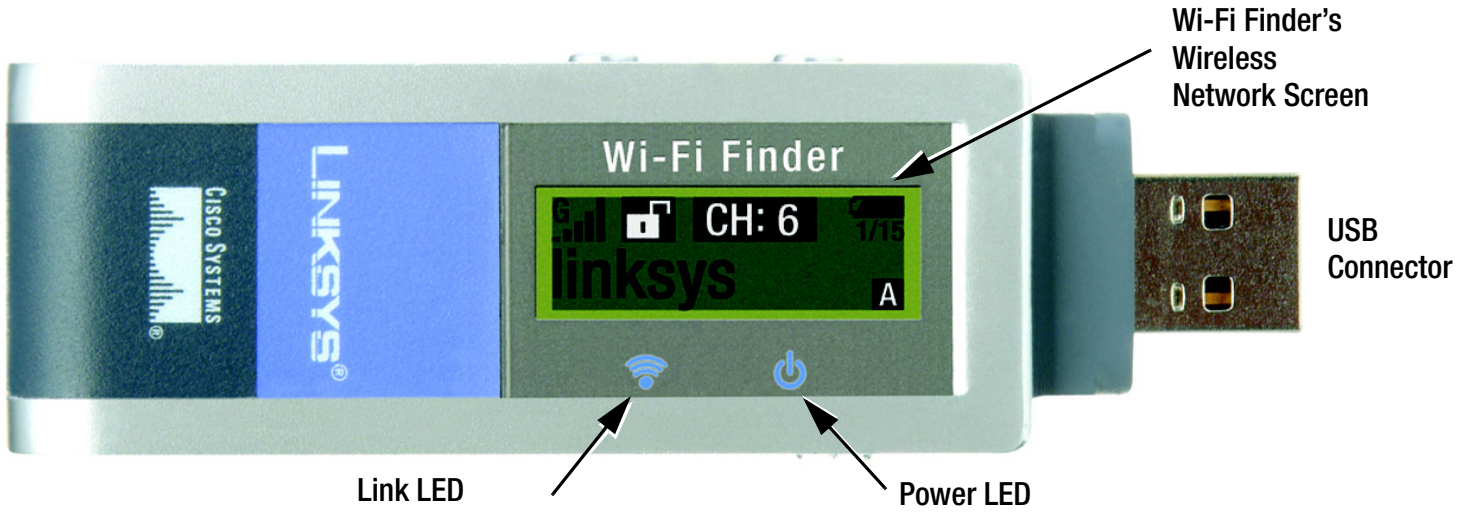

Figure 3-1: Front Panel

LEDs

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

Link *Green*. The Link LED lights up when there is wireless activity.

Using the Wi-Fi Finder

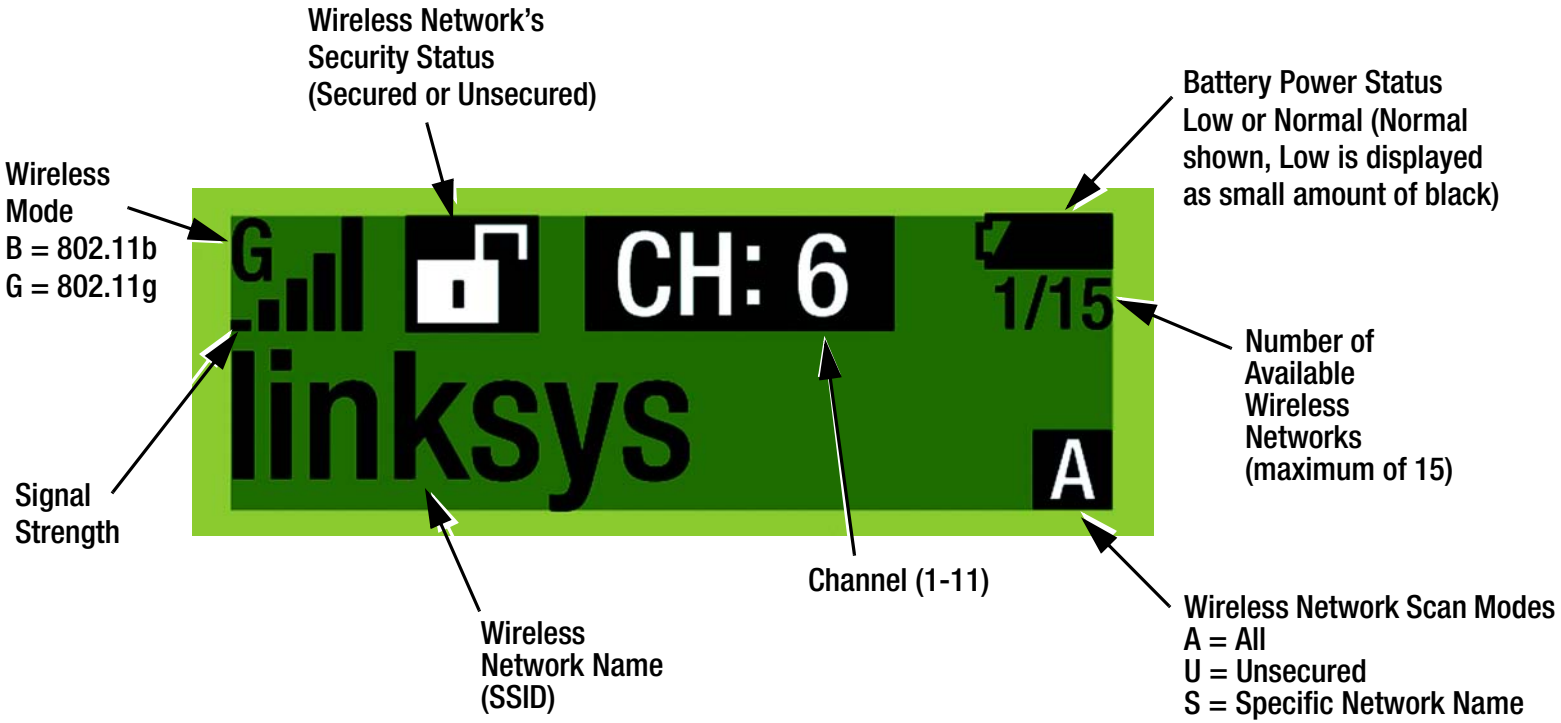

Figure 3-2: Wi-Fi Finder's Wireless Network Screen

Figure 3-3: Wi-Fi Finder's ON/OFF Switch and Buttons

ON/OFF Switch The ON/OFF switch is located on the side panel. Slide the button to the right side to turn on the Wi-Fi Finder.

Scan The Scan button is located on the side panel. Push the **Scan** button to scan for a wireless network.

There are three Wireless Network Scan Modes (shown in bottom right corner of screen): A = All Networks (default mode), U = Unsecured Networks, S = Specific Network Name

To change the mode, push and hold the **Scan** button.

- All Networks: This default mode scans and displays all secure and unsecure networks.
- Unsecured Networks: This mode scans and displays only unsecured networks.
- Specific Network Name: This mode scans and displays any networks with a selected specific network name. First, while in the All Networks mode, use the **Scroll** button and scroll until the network that you want is on your screen, then push and hold the **Scan** button to change the icon to S. Then, push the **Scan** button again to scan for any network with the selected name.

Scroll The Scroll button is located on the side panel. Push the **Scroll** button to view the next available wireless network, which will be displayed in the order of strongest to weakest signal strength. A maximum of fifteen wireless networks can be viewed.

Chapter 4: Setting up and Connecting the Wireless-G USB Network Adapter with Wi-Fi Finder

The Wireless-G USB Network Adapter with Wi-Fi Finder is set up with the Setup Wizard that comes on the CD enclosed with the Adapter. This chapter will guide you through the setup procedure.

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

Starting the Setup Wizard

To begin the setup process, 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).

Figure 4-1: Setup Wizard's Welcome Screen

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 this User Guide.

Exit - Click **Exit** 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 **Next** if you agree and want to continue the installation, or click **Cancel** to end the installation.

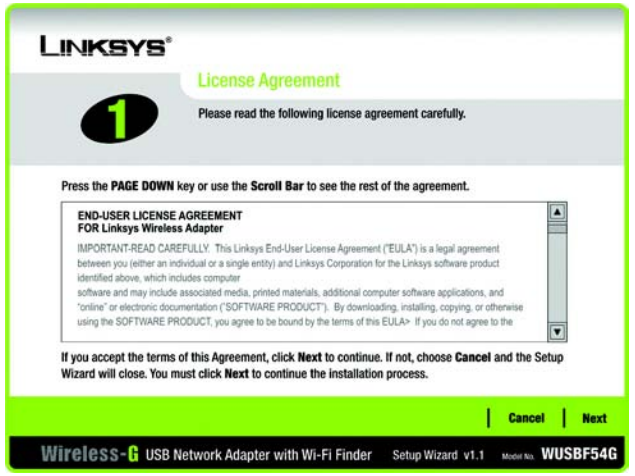

Figure 4-2: Setup Wizard's License Agreement

3. Windows will begin copying the files onto your PC.

4. The Setup Wizard will now prompt you to connect the Adapter to your PC's USB port. Once you've connected, click **Next**.

5. If prompted by Windows, Windows 98SE and ME users will need to restart their PCs.

Connecting the Adapter

1. Insert the USB connector end of the Adapter into the USB port of the PC.
2. The Power LED should light up when the Adapter is plugged in.

Figure 4-3: The Connecting the Adapter Screen

Setting Up the Adapter

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

This screen provides two options for setting up the Adapter

- **Available Wireless Network. (For most users.)** Use this option if you have already set up a network and the network is listed on the screen. Select the network and click the **Connect** button to connect to it. If you need to update the Available Wireless Network list, click the **Refresh** button.
- **Manual Setup.** If 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.

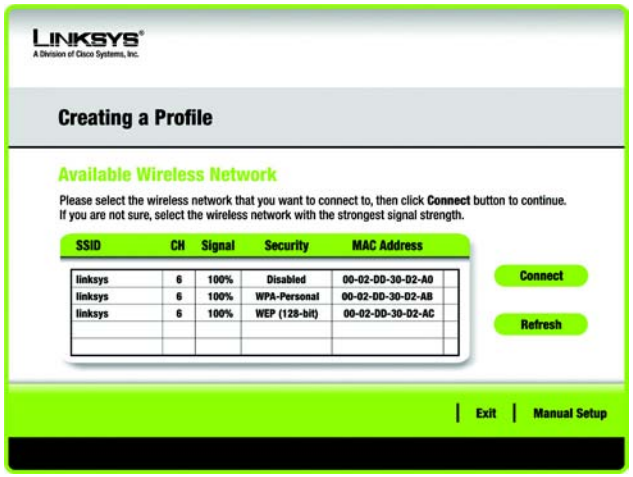

Figure 4-4: Available Wireless Network

Setting Up the Adapter with Available Networks

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 wireless security has been enabled on this network, you will see a wireless security screen. If your network utilizes WEP (Wired Equivalent Privacy) encryption, the *WEP Key Needed for Connection* screen will appear. If your network utilizes WPA-Personal (Wi-Fi Protected Access) encryption, the *WPA-Personal Needed for Connection* screen will appear.

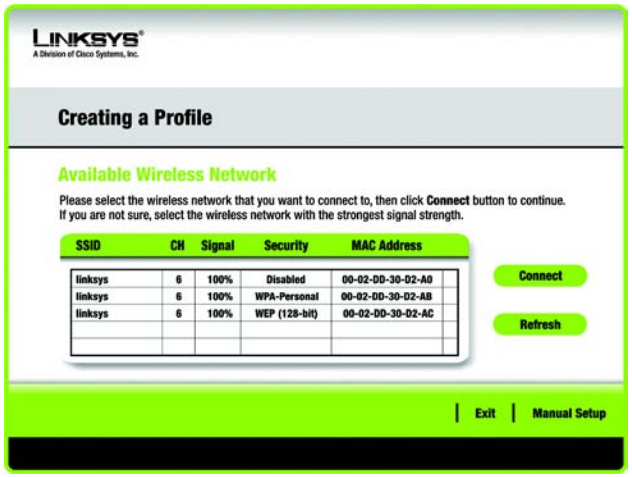

Figure 4-5: Available Wireless Network

WEP Key Needed for Connection

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** and proceed to the *Congratulations* screen. To cancel the connection, click **Cancel**.

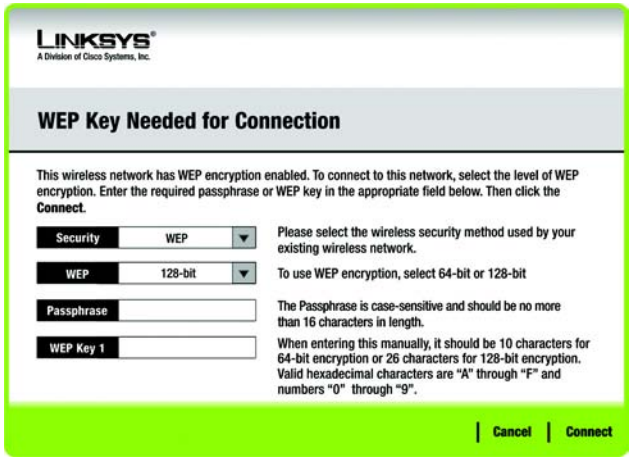

Figure 4-6: Wireless Security - WEP

WPA-Personal Needed for Connection

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 passphrase must match the devices on your wireless network.

Then, click **Connect** and proceed to the *Congratulations* screen. To cancel the connection, click **Cancel**.

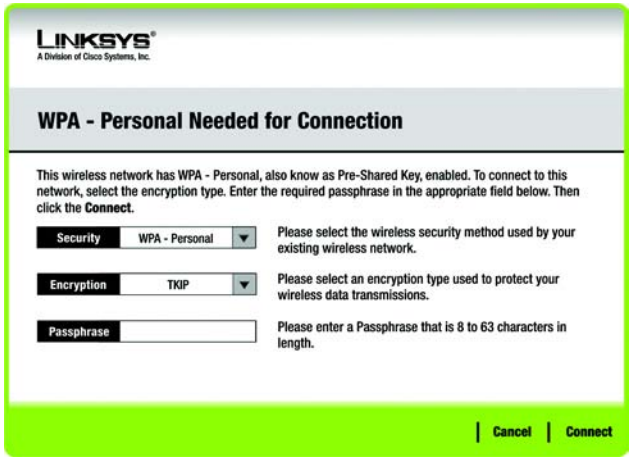

Figure 4-7: Wireless Security - WPA Personal

2. After the Adapter has been configured for the network, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network.

Figure 4-8: Congratulations

Congratulations! 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*

Setting Up the Adapter with Manual Setup

If your network is not listed with the available networks, click **Manual Setup** on the *Available Wireless Network* screen to set up the Adapter manually.

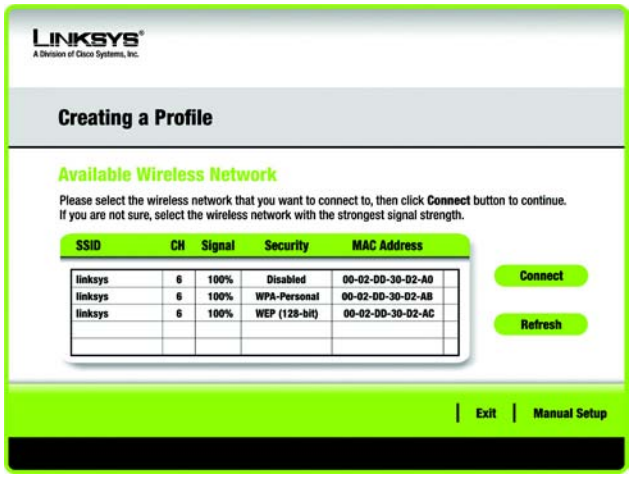

Figure 4-9: Available Wireless Network

1. After clicking **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 Router or 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 **Next** to continue, or click **Back** to return to the *Available Wireless Network* screen.

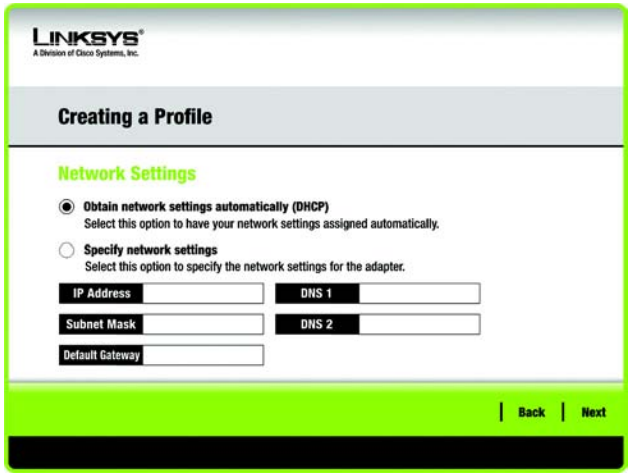

Figure 4-10: Network Settings

2. 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. Then, 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 **Next** to continue or **Back** to return to the previous screen.

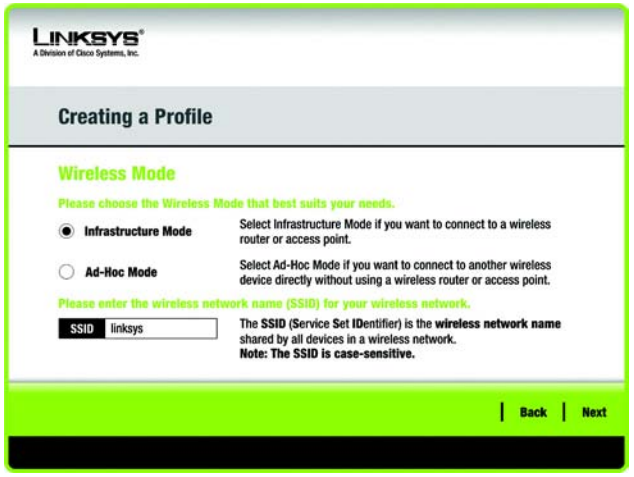

Figure 4-11: Wireless Mode

3. 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 **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.

   Then, select the **Network Mode** in which your wireless network will operate. In **Mixed Mode**, Wireless-B and Wireless-G devices can both operate on the network, though at a slower speed. In **G-Only Mode**, no Wireless-B devices can operate in the network.

   Click **Next** to continue or click **Back** to change any settings.

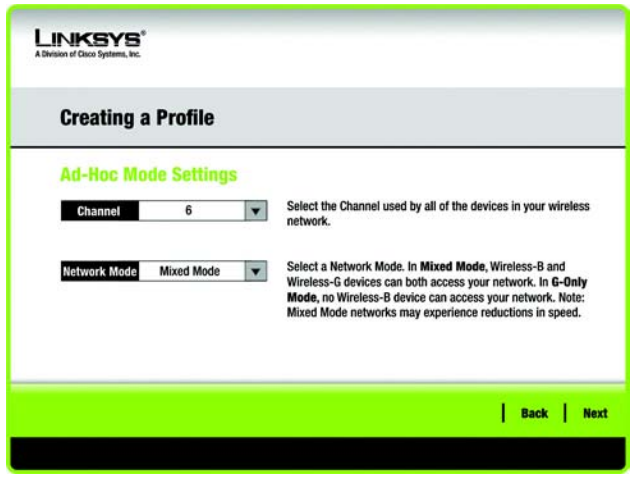

Figure 4-12: Ad-Hoc Mode Settings

4. The *Wireless Security* screen will appear. This step will configure wireless security.

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

   Select **WEP**, **WPA-Personal**, **WPA-Enterprise**, or **Radius** for the Encryption Method. WEP stands for Wired Equivalent Privacy, WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption, and RADIUS stands for Remote Authentication Dial-In User Service. If you don't want to use encryption, select **Disabled**.

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

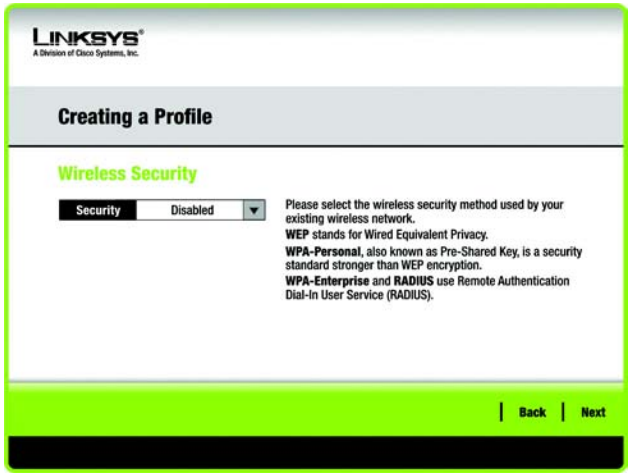

Figure 4-13: Wireless Security

encryption: *encoding data transmitted in a network.*

WEP

WEP - To use WEP encryption, select 64-bits or 128-bit characters from the drop-down menu, and enter a passphrase or key.

WEP Key- The WEP key you enter must match the WEP key of your wireless network. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Passphrase - Instead of manually entering a WEP key, you can enter a passphrase in the Passphrase field, so a WEP key is automatically generated. This case-sensitive 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.)

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**, where it auto-detects for **Shared Key** or **Open** systemNetshared Key is when both the sender and the recipient share a WEP key for authentication. Open key is when the sender and the recipient do not share a WEP key for authentication. All points on your network must use the same authentication type.

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

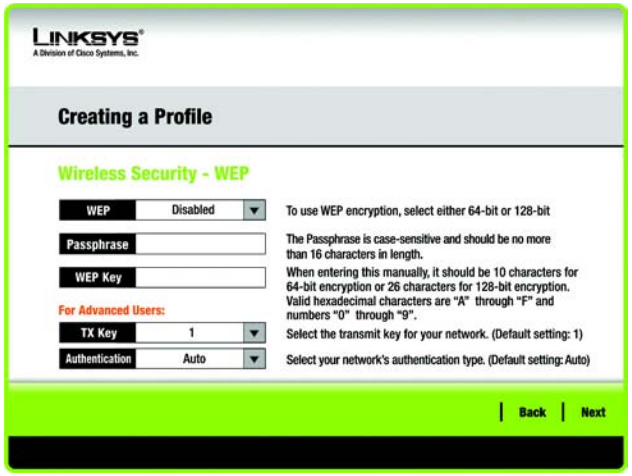

Figure 4-14: Wireless Security - WEP

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

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 passphrase must match the devices on your wireless network.

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

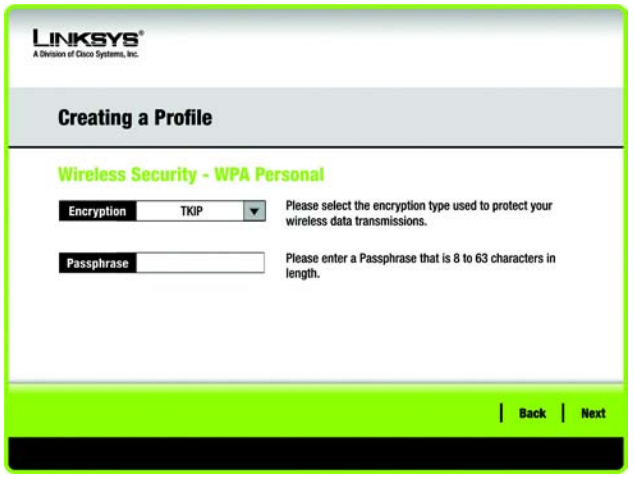

Figure 4-15: Wireless Security - WPA Personal

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.

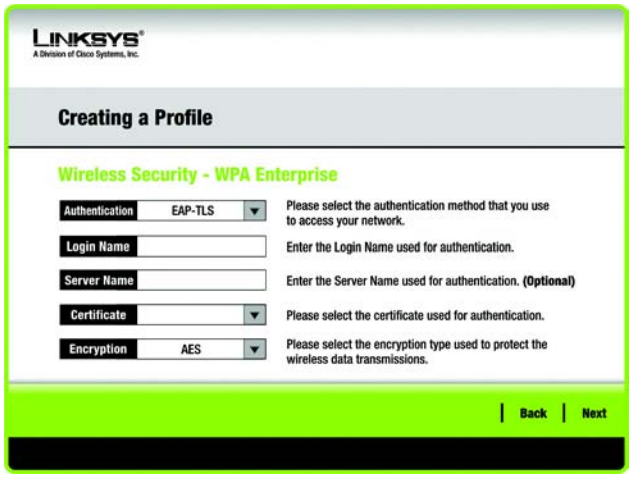

Figure 4-16: Wireless Security - WPA Enterprise - EAP-TLS

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 (Inner Authen.) used inside the PEAP tunnel. Select **EAP-MSCHAP v2**. Then, 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.

Figure 4-17: Wireless Security - WPA Enterprise - PEAP

RADIUS

RADIUS uses the security of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) It offers two authentication methods: EAP-TLS and PEAP.

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

EAP-TLS

Enter the Login name of your wireless network in the *Login Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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 (Inner Authen.) used inside the PEAP tunnel. Select **EAP-MSCHAP v2**.

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

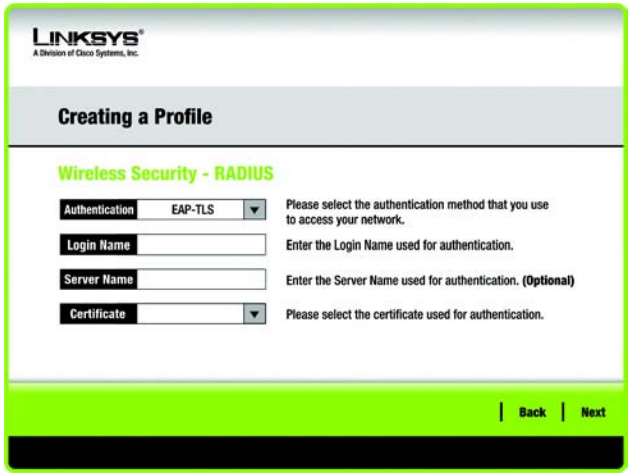

Figure 4-18: Wireless Security - RADIUS - EAP-TLS

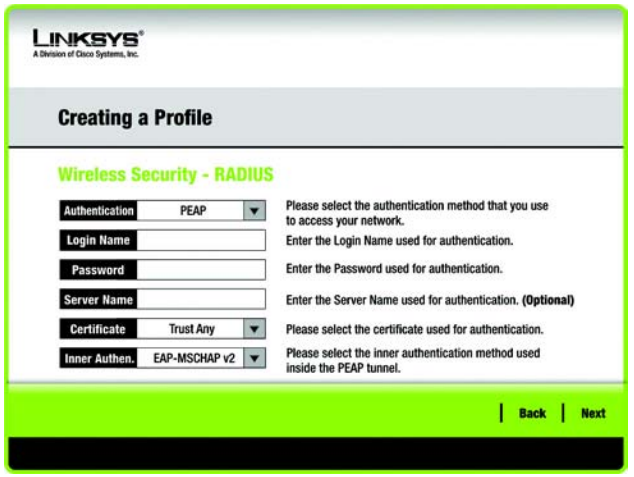

Figure 4-19: Wireless Security - RADIUS - PEAP

5. The next screen displays all of the Adapter's settings. If these are correct, you can save these settings to your hard drive by clicking **Save**. Click **Next** to continue and finish the setup. If these settings are not correct, click **Back** to change your settings. To exit the setup, click **Exit**.

Figure 4-20: Confirm New Settings

6. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network. Clicking **Return to Profiles screen** 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! 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 4-21: Congratulations

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 setting up and connecting the Adapter, the Wireless Network Monitor icon will appear in your PC's system tray. 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.

NOTE: The Wireless Network Monitor should only be accessed AFTER connecting the Adapter. For more information on Setting Up and Connecting the Adapter, refer to *Chapter 4: Setting Up and Connecting the USB Network Adapter.*

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

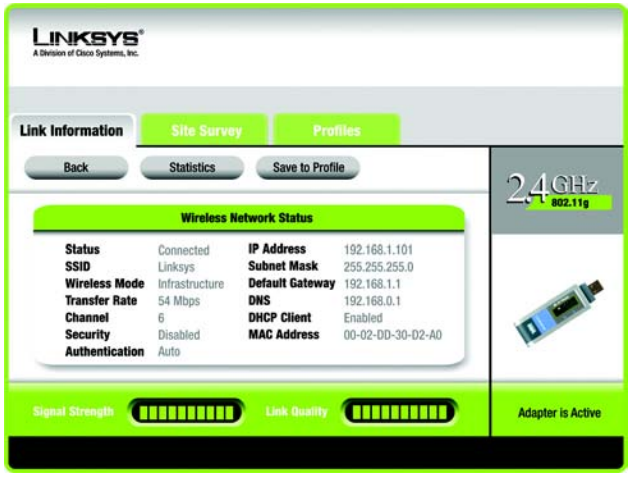

Figure 5-3: More Information - Wireless Network Status

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.

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

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

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

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.

Transmit Power - This is the power output at which the Adapter is transmitting.

Up Time - This indicates the length of the most recent connection to a wireless network.

Total Up Time - This indicates the cumulative total of the Adapter's connection time.

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 - Wireless Network Statistics

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, a screen appear requiring security information.

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. To connect to the network, click **Connect**. To cancel the connection, click **Cancel**.

If the network has WPA-Personal wireless 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. To connect to the network, click **Connect**. To cancel the connection, click **Cancel**.

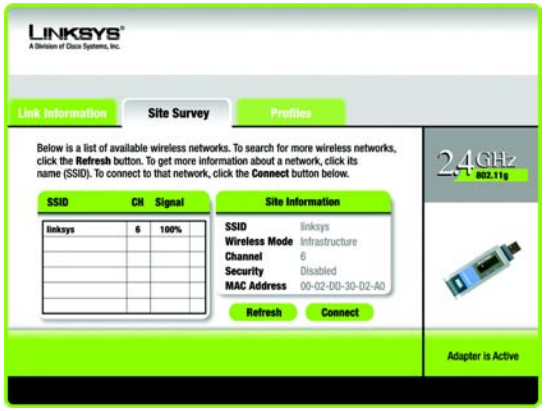

Figure 5-5: Site Survey

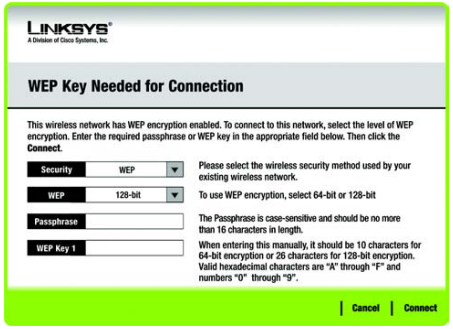

Figure 5-6: WEP Key Needed for Connection

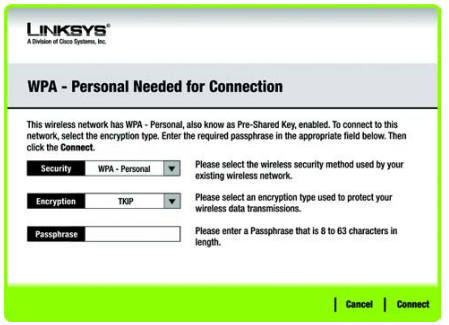

Figure 5-7: WPA-Personal Needed for Connection

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.

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 **New** 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 **Edit**.

Import - Click **Import** 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 **Export**. Direct Windows to the appropriate folder, and click the **Save** button.

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

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

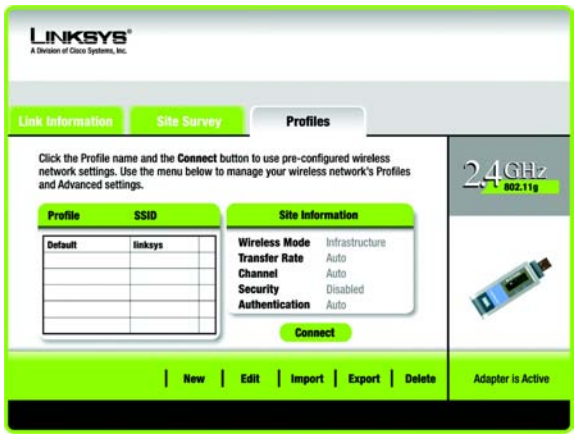

Figure 5-8: Profiles

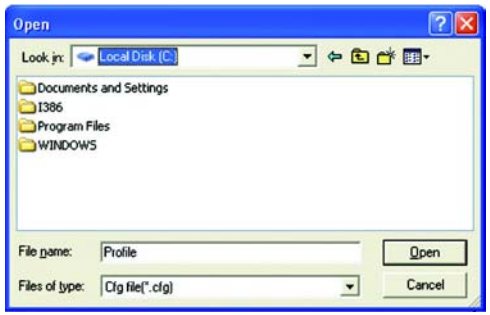

Figure 5-9: Import a Profile

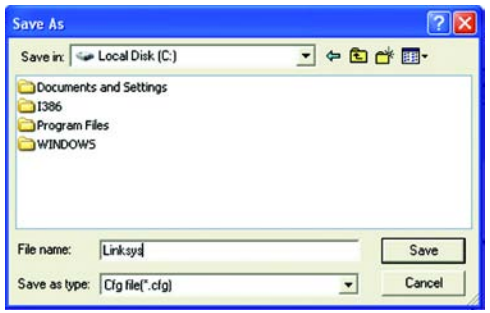

Figure 5-10: Export a Profile

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 two options for setting up the Adapter

- **Available Networks.** Use this option if you already have a network set up. The networks available to this Adapter will be listed on this screen. Select the network and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If 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 5-11: Create a New Profile

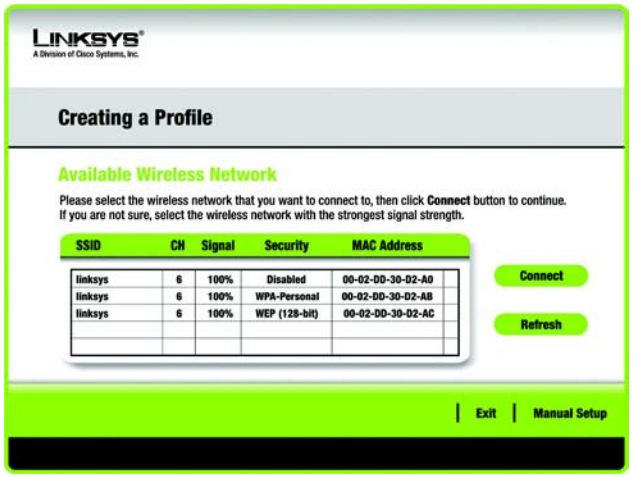

Figure 5-12: Available Wireless Network

Setting Up the Adapter with Available Networks

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.

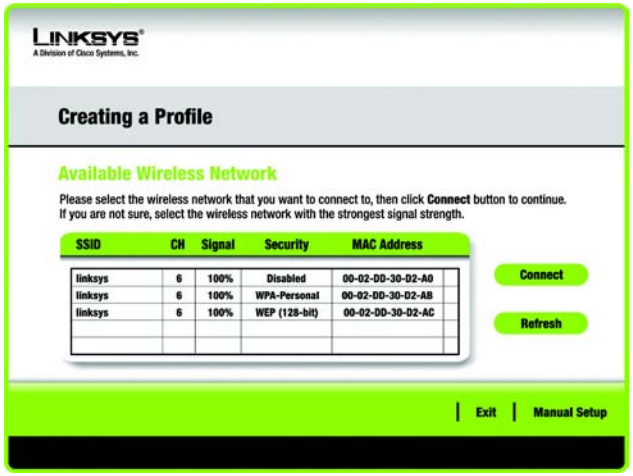

Figure 5-13: Available Wireless Network

1. If wireless security has been enabled on this network, you will see a wireless security screen. If your network utilizes WEP (Wired Equivalent Privacy) encryption, the *WEP Key Needed for Connection* screen will appear. If your network utilizes WPA-Personal (Wi-Fi Protected Access) encryption, the *WPA-Personal Needed for Connection* screen will appear.

   WEP Key Needed for Connection

   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** and proceed to the *Congratulations* screen. To cancel the connection, click **Cancel**.

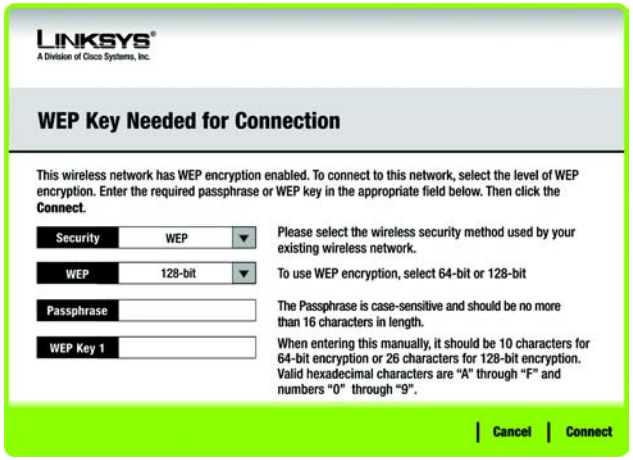

Figure 5-14: WEP Key Needed for Connection

WPA-Personal Needed for Connection

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 passphrase must match the devices on your wireless network.

Then, click **Connect** and proceed to the *Congratulations* screen. To cancel the connection, click **Cancel**.

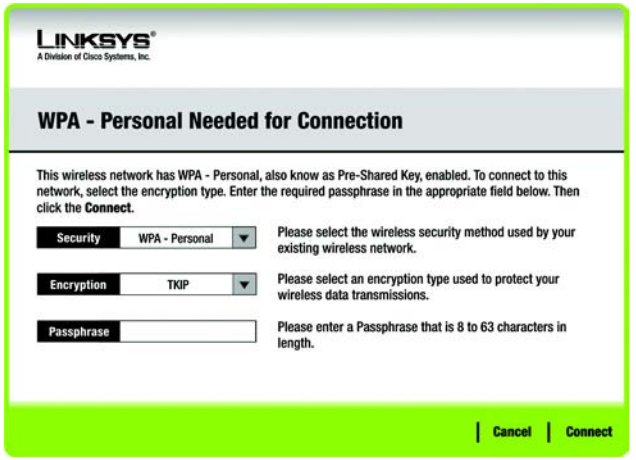

Figure 5-15: WPA-Personal Needed for Connection

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

Congratulations! The profile has been configured.

Figure 5-16: The Congratulations Screen

Setting Up the Adapter with Manual Setup

If your network is not listed among the available networks, click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.

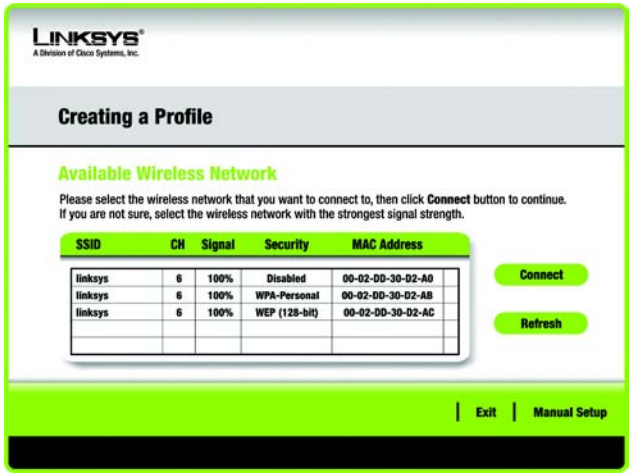

Figure 5-17: Available Wireless Network

1. After clicking **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 Router or 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 **Next** to continue, or click **Back** to return to the *Available Wireless Network* screen.

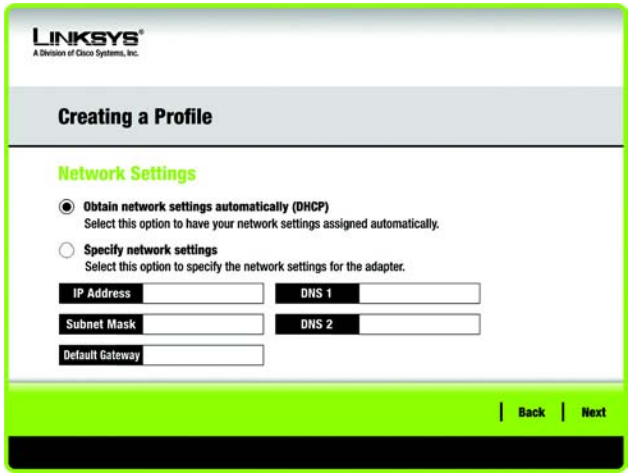

Figure 5-18: Network Settings

2. 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. Then, 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 **Next** to continue or **Back** to return to the previous screen.

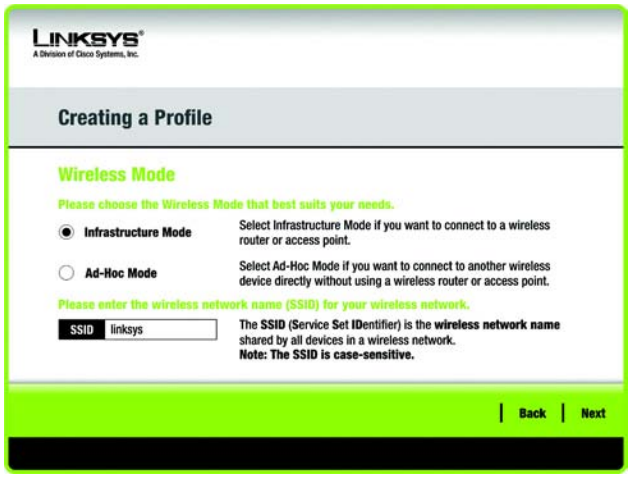

Figure 5-19: Wireless Mode

3. 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 **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.

   Then, select the **Network Mode** in which your wireless network will operate. In **Mixed Mode**, Wireless-B and Wireless-G devices can both operate on the network, though at a slower speed. In **G-Only Mode**, no Wireless-B devices can operate in the network.

   Click **Next** to continue or click **Back** to change any settings.

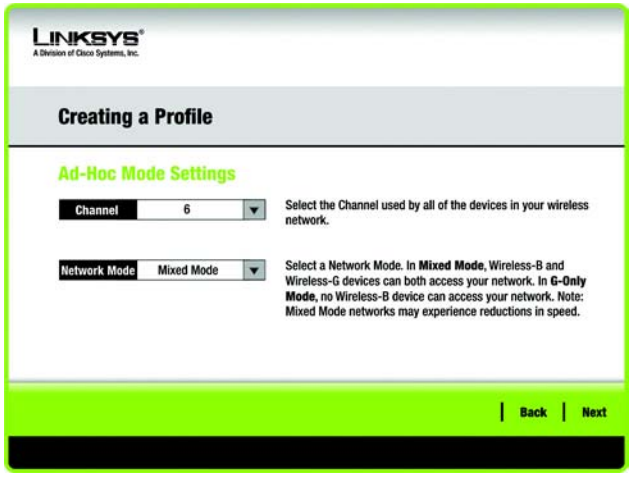

Figure 5-20: Ad-Hoc Mode Settings

4. The *Wireless Security* screen will appear. This step will configure wireless security.

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

   Select **WEP**, **WPA-Personal**, **WPA-Enterprise**, or **Radius** for the Encryption Method. WEP stands for Wired Equivalent Privacy, WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption, and RADIUS stands for Remote Authentication Dial-In User Service. If you don't want to use encryption, select **Disabled**.

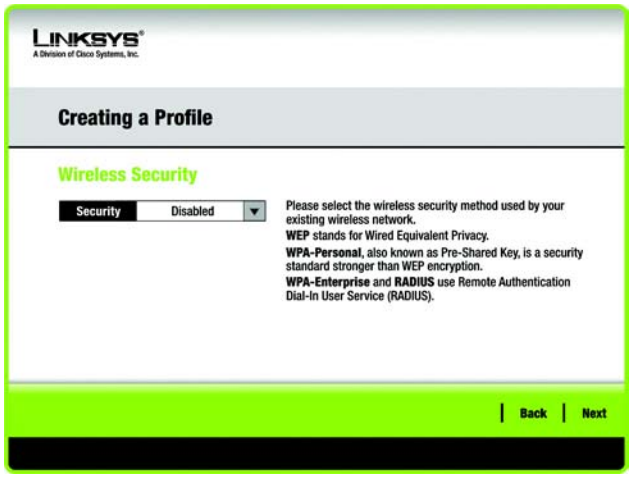

Figure 5-21: Wireless Security

WEP

WEP - To use WEP encryption, select 64-bits or 128-bit characters from the drop-down menu, and enter a passphrase or key.

WEP Key - The WEP key you enter must match the WEP key of your wireless network. If you are using 64-bit WEP encryption, then the key must consist of exactly 10 hexadecimal characters. If you are using 128-bit WEP encryption, then the key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Passphrase - Instead of manually entering a WEP key, you can enter a passphrase in the Passphrase field, so a WEP key is automatically generated. This case-sensitive 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.)

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**, where it auto-detects for **Shared Key** or **Open** system. Shared Key is when both the sender and the recipient share a WEP key for authentication. Open key is when the sender and the recipient do not share a WEP key for authentication. All points on your network must use the same authentication type.

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

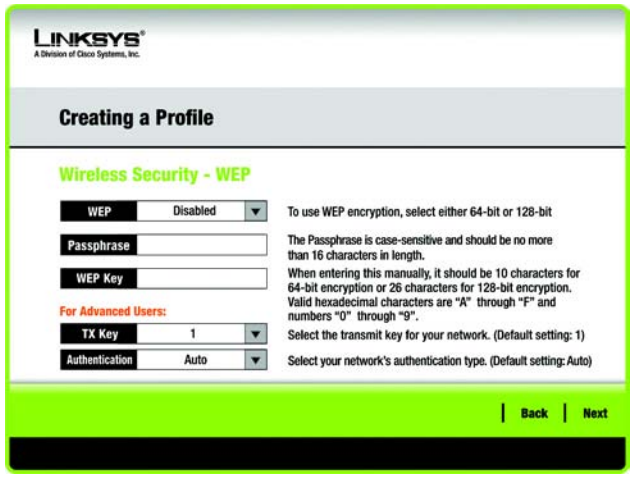

Figure 5-22: Wireless Security - WEP

WPA Personal

WPA Personal offers two encryption methods, *TKIP* and *AES*, with dynamic encryption keys.

Select the type of algorithm, **TKIP** or **AES**, for the *Encryption Type*. Enter a Passphrase of 8-63 characters in the *Passphrase* field. The passphrase must match the devices on your wireless network.

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

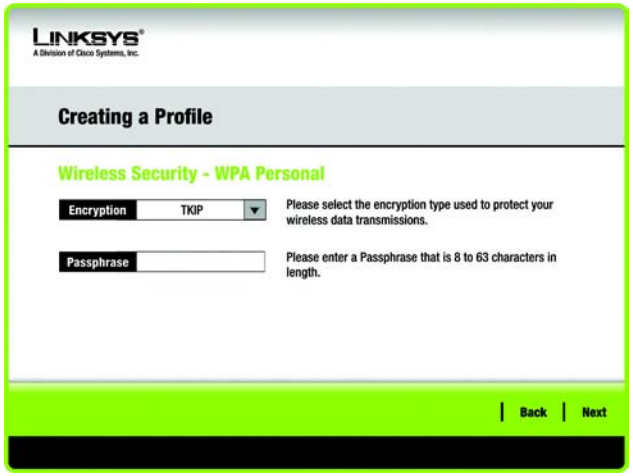

Figure 5-23: Wireless Security - WPA Personal

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.

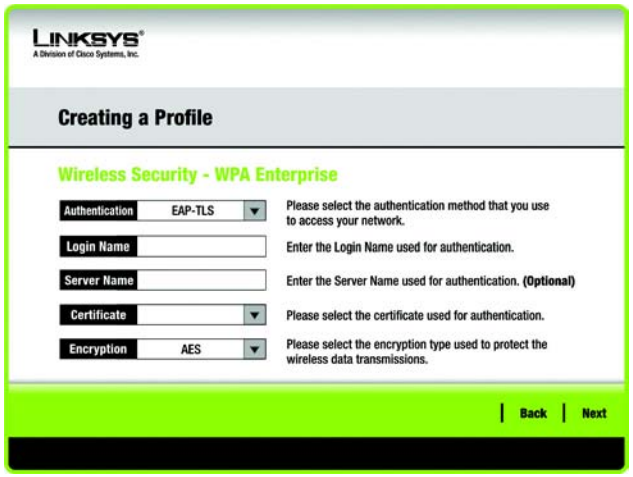

Figure 5-24: Wireless Security - WPA Enterprise - EAP-TLS

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 (Inner Authen.) used inside the PEAP tunnel. Select **EAP-MSCHAP v2**. Then, 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.

Figure 5-25: Wireless Security - WPA Enterprise - PEAP

RADIUS

RADIUS uses the security of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) It offers two authentication methods: EAP-TLS and PEAP.

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

EAP-TLS

Enter the Login name of your wireless network in the *Login Name* field. From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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 (Inner Authen.) used inside the PEAP tunnel. Select **EAP-MSCHAP v2**.

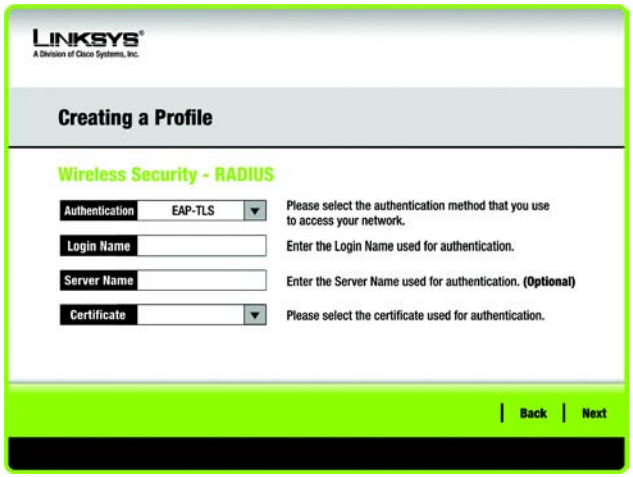

Figure 5-26: Wireless Security - RADIUS - EAP-TLS

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

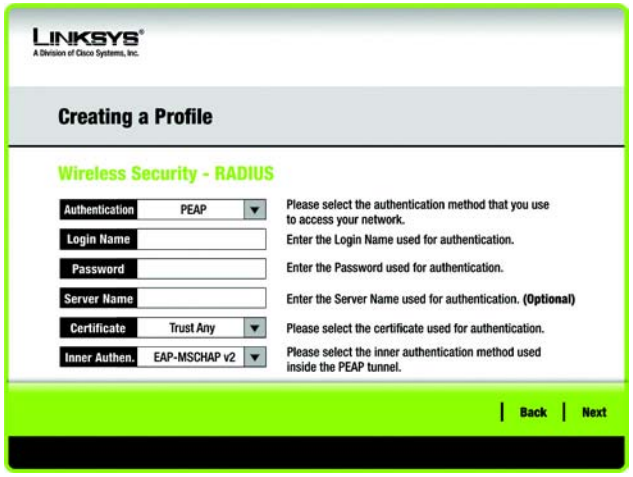

Figure 5-27: Wireless Security - RADIUS - PEAP

5. The next screen displays all of the Adapter's settings. If these are correct, you can save these settings to your hard drive by clicking **Save**. Click **Next** to continue. If these settings are not correct, click **Back** to change your settings.

Figure 5-28: Confirm New Settings

6. 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.

Congratulations! The profile has been configured.

Figure 5-29: The Congratulations Screen

Appendix A: Troubleshooting

This appendix provides solutions to problems usually encountered during the installation and operation of the Adapter. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

1.My computer does not recognize the USB Network Adapter.

- Make sure that the USB Network Adapter is properly inserted into the USB port.
- Also, make sure that the USB Controller is enabled in the BIOS. Check with your motherboard User Guide for more information.

2. The USB Network Adapter does not work properly.

- Reinsert the USB Network Adapter into the notebook or desktop's USB port.
- Right-click on My Computer, and select Properties. Select the Adapter, then chose the Device Manager tab, and click on the Network Adapter. You will find the USB Network 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 or desktop is powered on.
- Make sure that your USB Network Adapter is configured on the same channel, SSID, and WEP as the other computers in the Infrastructure configuration.

Frequently Asked Questions

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

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

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

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

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11b functions:

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

What IEEE 802.11g features are supported?
The product supports the following IEEE 802.11g functions:

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

What is ad-hoc mode?

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

What is infrastructure mode?

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

What is roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that

the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

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

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

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

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Appendix B: Using Windows XP Wireless Configuration

If your computer is running Windows XP, then this choice will be available. If you want to use Windows XP Wireless Configuration to control the Adapter, instead of using the Wireless Network Monitor, then right-click on the Wireless Network Monitor and select **Use Windows XP Wireless Configuration**.

If you want to switch back to the Wireless Network Monitor, right-click the **Wireless Network Monitor** icon, and select **Use Linksys Wireless Network Monitor**.

Figure B-1: Wireless Network Monitor Icon

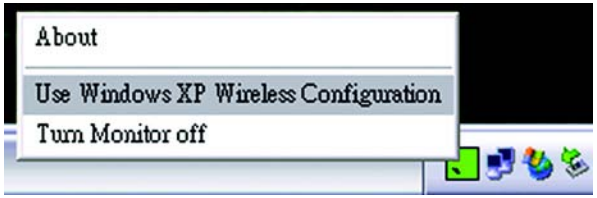

Figure B-2: Windows XP - Use Windows XP Wireless Configuration

1. After installing the Adapter, the Windows XP Wireless Configuration icon will appear in your computer's system tray. Double-click the icon.

NOTE: For more information about Windows XP Wireless Configuration, refer to Windows Help.

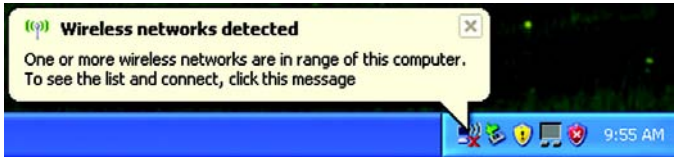

Figure B-3: Windows XP Wireless Configuration Icon

2. The screen that appears will show any available wireless network. Select the network you want. Click the **Connect** button.

   If your network does not have wireless security enabled, go to step 3.

   If your network does have wireless security enabled, go to step 4.

NOTE: Steps 2 and 3 are the instructions and screenshots for Windows XP with Service Pack 2 installed.

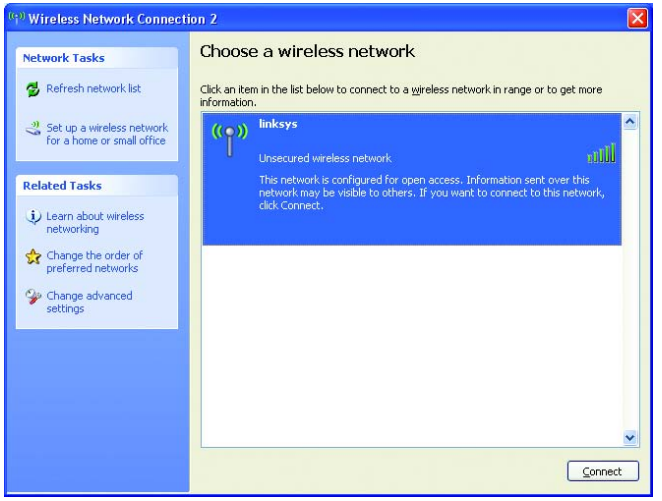

Figure B-4: Available Wireless Network

3. If your network does not have wireless security enabled, click the **Connect Anyway** button to connect the Adapter to your network.

Figure B-5: No Wireless Security

4. If your network uses wireless security WEP, enter the WEP Key used into the *Network Key* and *Confirm network key* fields. If your network uses wireless security WPA Personal, enter the Passphrase used into the *Network Key* and *Confirm network key* fields. Click the **Connect** button.

Figure B-6: Network Connection - Wireless Security

NOTE: Windows XP Wireless Configuration does not support the use of a passphrase. Enter the exact WEP key used by your wireless router or access point.

5. Your wireless network will appear as *Connected* when your connection is active.

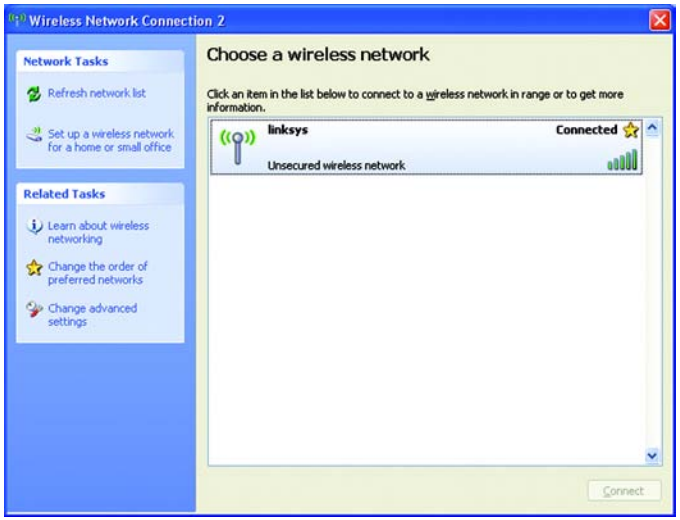

Figure B-7: Wireless Network Connection

For more information about wireless networking on a Windows XP computer, click the **Start** button, select **Help**, and choose **Support**. Enter the keyword wireless in the field provided, and press the **Enter** key.

The installation of the Windows XP Wireless Configuration is complete.

Appendix C: 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. Two modes are available: WPA-Personal and WPA-Enterprise. 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 Standard), which utilizes a symmetric 128-Bit block data encryption. WPA-Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys, and it uses a RADIUS (Remote Authentication Dial-In User Service) 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 you want to use, **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.

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 D: 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 the Access Point, 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 E: 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.

PEAP (**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.

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.

QoS (**Q**uality **o**f **S**ervice) - QoS ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

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

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

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

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

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects 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 (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

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

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

STUN (**S**imple **T**raversal of **U**DP through **N**ATs) - 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 (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

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

Upload - To transmit a file over a network.

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

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

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

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

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

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

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

Appendix F: Specifications

Model	WUSBF54G
Standards	IEEE 802.11b, 802.11g, USB 1.1, USB 2.0
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
LEDs	Power, Link
Transmitted Power	18dBm (Typical)@11Mbps 16dBm (Typical)@54Mbps
Receive Sensitivity	-73dBm (Typical)@54Mbps, -84dBm (Typical)@11Mbps
Power Consumption	Active: TX 380mA (Max.) & RX 200mA (Max.)
Battery	Built-in rechargeable Li-ion Polymer battery
Security features	WEP Encryption, WPA
Dimensions	3.78" x 0.63" x 1.14" (96 mm x 16 mm x 29 mm)
Unit Weight	0.05 lb (0.023 kg)
Certifications	FCC, WiFi
Operating Temp.	0°C ~ 40°C (32°F ~ 104°F)
Storage Temp.	-20°C ~ 70°C (-4°F ~ 158°F)
Operating Humidity	0% ~ 70% Non-Condensing
Storage Humidity	10% ~ 90% Non-Condensing

Appendix G: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser ("You") that, for a period of three years for the hardware and a period of one year for the battery, (the "Warranty Period"). Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's 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.

If the product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a 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.

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, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, 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 Section 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 USA.

Appendix H: 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 département. L'utilisation en extérieur est soumis à autorisation préalable et très restreint.

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

SAFETY NOTICES

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

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

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

Appendix I: 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: Or fax your request in to:	800-546-5797 (LINKSYS) 949-823-3002
If you experience problems with any Linksys product, you can call us at: Don't wish to call? You can e-mail us at:	800-326-7114 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: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000