LINKSYS®

A Division of Cisco Systems, Inc.

2,4GHz 802.11g

Wireless-G

Access Point

User Guide

WIRELESS

Model No. **WAP54G (EU/LA/UK)**

CISCO SYSTEMS

Copyright and Trademarks

How to Use this User Guide

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

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section.

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Access Point. This Access Point will allow you to network wirelessly better than ever.

How does the Access Point do all of this? An access point allows for greater range and mobility within your wireless network while also allowing you to connect the wireless network to a wired environment.

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 on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired".

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. This is sometimes called a WLAN, or Wired Local Area Network. The Access Point bridges wireless networks of both 802.11g and 802.11b standards and wired networks.

Use the instructions in this Guide to help you connect the Access Point, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Access Point.

***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.*

***network:** a series of computers or devices connected together.*

***lan** (local area network): the computers and networking products that make up your local network.*

***ethernet:** network protocol that specifies how data is placed on and retrieved from a common transmission medium.*

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

***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.*

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

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Access Point.

- Chapter 1: Introduction
  This chapter describes the Access Point's applications and this User Guide.
- Chapter 2: Planning your Wireless Network
  This chapter describes the basics of wireless networking.
- Chapter 3: Getting to Know the Wireless-G Access Point
  This chapter describes the physical features of the Access Point.
- Chapter 4: Connecting the Wireless-G Access Point
  This chapter instructs you on how to connect the Access Point to your network.
- Chapter 5: Setting Up the Wireless-G Access Point
  This chapter explains how to use the Setup Wizard to configure the settings on the Access Point.
- Chapter 6: Configuring the Wireless-G Access Point
  This chapter explains how to use the Access Point's Web-based Utility for advanced configuration.
- Appendix A: Troubleshooting
  This appendix describes some frequently asked questions regarding installation and use of the Access Point.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the Access Point's firmware.
- Appendix D: Windows Help
  This appendix describes some of the ways Windows can help you with wireless networking.
- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix F: Specifications
  This appendix provides the Access Point's technical specifications.
- Appendix G: Warranty Information
  This appendix supplies the Access Point's warranty information.

- Appendix H: Regulatory Information
  This appendix supplies the Access Point'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.

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

Linksys wireless adapters also provide users access to a wired network when using an access point, such as the Wireless-G 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.

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

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may 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 may be doubled.

Roaming

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

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

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

***ssid**: your wireless network's name*

Network Layout

The Wireless-G Access Point has been designed for use with 802.11g and 802.11b products. The Access Point is compatible with 802.11g and 802.11b adapters, such as the Notebook Adapters for your laptop computers, PCI Adapters for your desktop PCs, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with a 802.11g or 802.11b Wireless PrintServer.

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router.

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

Chapter 3: Getting to Know the Wireless-G Access Point

The Front Panel

The Access Point's LEDs, which indicate activity and status information, are located on the front panel.

Figure 3-1: Front Panel

(Cisco logo) Orange/White. The Cisco logo is the Access Point's SecureEasySetup button. It lights up when the Access Point is powered on. The Cisco logo is orange when the SecureEasySetup feature is not used, while the color white indicates that the SecureEasySetup feature is being used. When the Access Point enters SecureEasySetup mode, the Cisco logo will turn white and start flashing. Then the Access Point will generate its SSID (network name) and WPA-Personal (also called WPA-PSK) key. If the Access Point successfully associates with a client using SecureEasySetup, the Cisco logo will stop flashing and stay white. If the association is unsuccessful, then the Cisco logo will stop flashing and stay orange.

To clear the SSID and WPA-Personal key, press and hold down the Cisco logo for ten seconds. The Cisco logo will turn orange to indicate a successful reset.

Power Red. The **Power** LED lights up when the Access Point is powered on.

Act Green. The **Act** LED lights up when the Access Point is ready for wireless use. It flashes when the Access Point is transmitting or receiving data wirelessly.

Link Orange. The **Link** LED lights up when the Access Point is successfully connected to a device through the Ethernet network port. The LED flashes when the Access Point is transmitting or receiving data through the Ethernet network port.

NOTE: SecureEasySetup is a feature that makes it easy to set up your wireless network. If you have SecureEasySetup devices, run the Setup Wizard on the Access Point's Setup Wizard CD-ROM. Then follow the on-screen instructions.

The Back Panel

The Access Point's Ethernet network and power ports, as well as the Reset button, are located on the back panel.

port: *the connection point on a computer or networking device used for plugging in cables or adapters*

Figure 3-2: Back Panel

LAN Port The Ethernet network port connects to an Ethernet network device, such as a switch or router.

Reset Button There are two ways to reset the Access Point's factory defaults. Either press the **Reset** button, for approximately ten seconds, or use the *Administration - Factory Defaults* screen of the Access Point's Web-based Utility.

IMPORTANT: Resetting the Access Point will erase all of your settings (including wireless security, IP address, and power output) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Power Port The Power port connects to the Access Point's power adapter.

Chapter 4: Connecting the Wireless-G Access Point

Overview

This chapter explains how to connect the Access Point for setup.

Connections for Setup

1. Connect your Ethernet network cable to your network router or switch. Then connect the other end of the network cable to the Access Point's LAN (Ethernet network) port.
2. Connect the included power adapter to the Access Point's Power port. Then plug the power adapter into an electrical outlet. The LEDs on the front panel will light up as soon as the Access Point's powers on.

Proceed to "Chapter 5: Setting Up the Wireless-G Access Point."

Figure 4-1: Connect the Ethernet Network Cable

Figure 4-2: Connect the Power

Chapter 5: Setting up the Wireless-G Access Point

Overview

Now that you've connected the Access Point to your wired network, you are ready to begin setting it up. This Setup Wizard will take you through all the steps necessary to configure the Access Point.

Using the Setup Wizard

1. 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).

2. On the *Welcome* screen, click the **Click Here to Start** or **Setup** button if this is the first time you are running the Setup Wizard. These are your other choices:

   Install Linksys Wireless Guard - Linksys Wireless Guard is a subscription service that secures your network; it is available only in the USA and Canada.

   NOTE: The Linksys Wireless Guard service is available only in the USA and Canada.

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

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

Figure 5-1: Welcome Screen

3. Optimally, you should set up the Access Point using a PC on your wired network. Connect a network cable to your network router or switch. Then click the **Next** button.

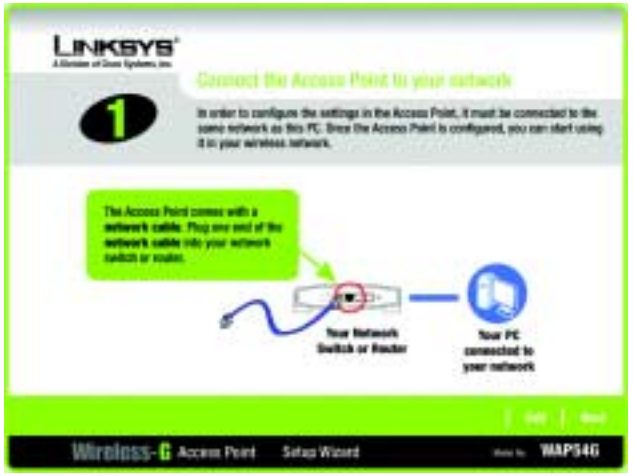


Figure 5-2: Connect the Network Cable to the Router or Switch Screen

4. The screen shows how the Access Point should be connected as you run the Setup Wizard. Connect the other end of the network cable to the Access Point's Ethernet network port. Then click the **Next** button.

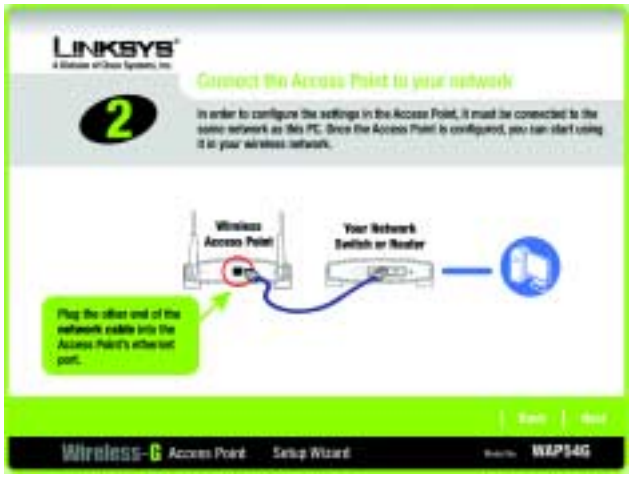


Figure 5-3: Connect the Network Cable to the Access Point Screen

5. Connect the power adapter to the Access Point and an electrical outlet. Then click the **Next** button.

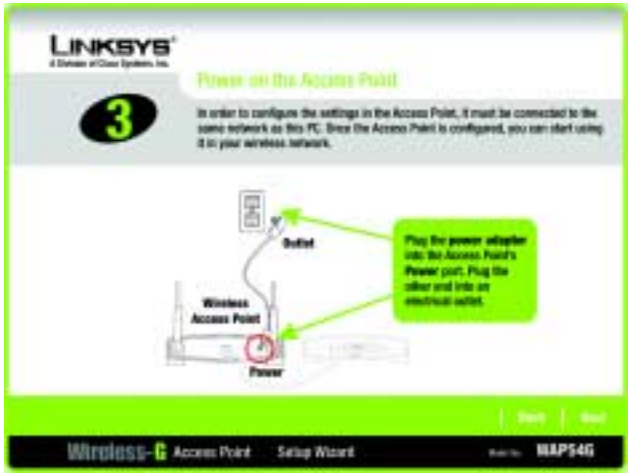


Figure 5-4: Power on the Access Point Screen

6. Make sure the Access Point's Power, Act, and Link LEDs are lit on its front panel. If they are not, check your cable connections. Then click the **Next** button to continue.

Figure 5-5: Check the Access Point's Status Screen

7. The Setup Wizard will run a search for the Access Point within your network and then display a list along with the status information for the selected access point. If this is the only access point on your network, it will be the only one displayed. If there are more than one displayed, select the Access Point by clicking on it. Click the **Yes** button to change any settings, or click the **No** button to keep these settings.

Figure 5-6: Select the Access Point Screen

8. You will be asked to sign onto the Access Point you have selected. Enter the default password, **admin**. Then, click **Enter**. (This password can be changed from the Web-based Utility's Administration - Management tab.)

Figure 5-7: Password Screen

9. The *Basic Settings* screen will appear next. Enter a descriptive name in the *Device Name* field. Create a password that will control access to the Access Point's Web-based Utility and Setup Wizard.

   If your network router will automatically assign an IP address to the Access Point, then select **Automatic-DHCP**.

   If you want to assign a static or fixed IP address to the Access Point, then select **Static IP**. Enter the IP Address, Subnet Mask, and Default Gateway settings. If you are not sure what changes you should make, then keep the default values.

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

   Device Name - Enter a descriptive name for the Access Point.

   Password - Enter a password that will control access to the Utility and Setup Wizard.

   IP Address - This IP address must be unique to your network. (The default IP address is **192.168.1.245**.)

   Subnet Mask - The Access Point's Subnet Mask must be the same as the subnet mask of your Ethernet network.

   Default Gateway - Enter the IP address of your network gateway (usually your router).

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

Figure 5-8: Basic Settings Screen

10. There are two ways to configure the Access Point's wireless settings, SecureEasySetup and manual configuration.

    If you have other SecureEasySetup devices, such as notebook adapters or printers, then you can use the Access Point's SecureEasySetup feature to configure your wireless network. Proceed to the section, "Using the Access Point's SecureEasySetup Feature."

    NOTE: If you have already set up your network using your router's SecureEasySetup feature, then you cannot use the Access Point's SecureEasySetup feature. You must manually configure the Access Point's wireless settings to match your existing network's settings.

    If you do not have other SecureEasySetup devices, then proceed to the section, "Manually Configuring the Access Point's Wireless Settings."

Figure 5-9: Configure Wireless Settings Screen

Using the Access Point's SecureEasySetup Feature

Read these instructions before you press any SecureEasySetup buttons. You should locate the SecureEasySetup buttons of your devices before using the Access Point's SecureEasySetup feature.

NOTE: SecureEasySetup uses WPA-Personal encryption. If your current wireless devices do not support WPA-Personal security, then you cannot use SecureEasySetup on your network. You will need to manually configure your network security using the encryption supported by your existing devices.

1. Before you push any button, locate the SecureEasySetup button for each of your other SecureEasySetup devices. If you are not sure where to find this button, click **Where is my other SecureEasySetup button?**

   You will see a screen showing the SecureEasySetup logo. Click the **Next** button to continue or the **Close** button to return to the *Configure Wireless Settings* screen.

   You will see a screen with instructions on how to locate the SecureEasySetup hardware button. If your device does not have a hardware button, it most likely will have a software button. Click the **Next** button for instructions to locate the software button, or click the **Close** button to return to the *Configure Wireless Settings* screen.

   You will see a screen with instructions on how to locate the SecureEasySetup software button. Click the **Close** button to return to the *Configure Wireless Settings* screen.

Figure 5-10: SecureEasySetup Screen

Figure 5-11: SecureEasySetup Logo

Figure 5-12: Additional Information - Hardware Button

Figure 5-13: Additional Information - Software Button

2. Press the Access Point's Cisco logo for only one to two seconds and then release it.

NOTE: If you accidentally press the Cisco logo for five to eight seconds, then the Access Point's SSID and WPA-Personal settings will be changed, and you will have to re-configure all of your wireless client devices.

3. Wait five to ten seconds. When the logo turns white and begins to flash, press the SecureEasySetup button on another device. The Access Point's Cisco logo will stop flashing when the device has been added to the wireless network.

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

4. Then repeat this procedure for each additional SecureEasySetup device.

   When you have finished configuring the devices in your wireless network, click the **Next** button to continue.

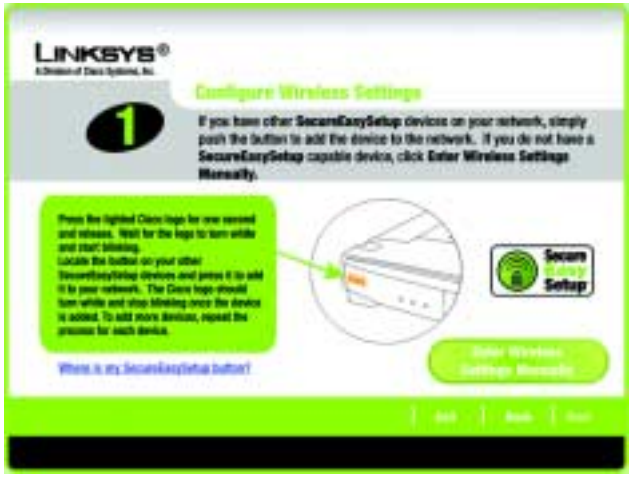


Figure 5-14: Configure Wireless Settings Screen

5. The Setup Wizard will ask you to review your settings before it saves them. Write down these settings in case you need to manually configure non-SecureEasySetup devices in the future.

   Click the **Yes** button if you are satisfied with your settings, or click the **No** button if you do not want to save your new settings.

Figure 5-15: Confirm New Settings Screen

6. The *Congratulations* screen will appear. Click the **Online Registration** button to register the Access Point, or click the **Exit** button to exit the Setup Wizard.

Congratulations! The installation of the Wireless-G Access Point is complete.

If you need to configure a non-SecureEasySetup device, proceed to the next section, "Configuring a Non-SecureEasySetup Device."

If you want to make advanced configuration changes, proceed to "Chapter 6: Configuring the Wireless-G Access Point."

Configuring a Non-SecureEasySetup Device

If you need to configure a non-SecureEasySetup device, then proceed with the setup of your non-SecureEasySetup device. When you have to configure its wireless settings, enter the settings you wrote down when you saw the *Confirm New Settings* screen at the end of the Setup Wizard.

If you did not write down these settings, then you will use the Access Point's Web-based Utility. Follow these instructions:

1. Launch Internet Explorer or Netscape Navigator. In the *Address* field, enter the Access Point's default IP address, **192.168.1.245**, or the IP address you entered during the Setup Wizard. (Should you need to learn what IP address the Access Point presently uses, run the Setup Wizard again. It will scan the Access Point and give you its IP address.) Press the **Enter** key.

2. The login screen will appear. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

3. Click the **Wireless** tab. The Access Point's Network Name (SSID) will appear on the *Basic Wireless Settings* screen. Write down the Network Name (SSID) for the Access Point.

4. Click the **Wireless Security** tab. The Access Point's WPA-Personal settings will appear on the *Wireless Security* screen. Write down the Passphrase for the Access Point.

5. When you configure the wireless settings for your non-SecureEasySetup devices, enter the Access Point's Network Name (SSID) and Passphrase when you are asked for them.

If you want additional information about the Web-based Utility, proceed to "Chapter 6: Configuring the Wireless-G Access Point."

Figure 5-16: Congratulations Screen

NOTE: Some devices may call the Passphrase a Pre-Shared Key instead. They are different names for the same key.

Manually Configuring the Access Point's Wireless Settings

1. If you do not have other SecureEasySetup devices, then click the **Enter Wireless Settings Manually** button.

Figure 5-17: Configure Wireless Settings Screen

2. The Setup Wizard will ask you to enter the SSID, Channel, and Network Mode settings for your wireless network.

   SSID - Enter the name of your wireless network. The SSID must be identical for all devices in the network. The default setting is **linksys** (all lowercase).

   Channel - Select the operating channel for your wireless network. All of your wireless devices will use this channel to communicate.

   Network Mode - Select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed Mode**. If you have only 802.11g devices, select **G-Only**. If you have only 802.11b devices, select **B-Only**. If you want to disable your wireless network, select **Disable**.

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

Figure 5-18: Wireless Settings Screen

3. Select the level of security you want to use: **WEP**, **WPA/WPA2 Personal**, **WPA-Enterprise**, or **Linksys Wireless Guard**, which is available only in the USA and Canada. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. Click the **Next** button and proceed to step 4.

   If you want to use WPA-Enterprise, then you should select **Disabled** and use the Access Point's Web-based Utility to configure your wireless security settings. (Refer to "Chapter 6: Configuring the Wireless-G Access Point.") Click the **Next** button and proceed to step 5.

   If you do not want to use any wireless security method, select **Disabled** and then click the **Next** button. Proceed to step 5.

4. Proceed to the appropriate section for your security method.

WEP (64-Bit)

To use 64-bit WEP encryption, select **WEP (64-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. Valid hexadecimal characters are "0" to "9" and "A" to "F".

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

WEP (128-Bit)

To use 128-bit WEP encryption, select **WEP (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 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

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

Figure 5-19: Security Settings Screen

Figure 5-20: WEP Settings Screen

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

encryption: *encoding data transmitted in a network.*

WPA Personal

To use WPA Personal security, select **WPA Personal** from the *Security* drop-down menu. 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 8-32 characters in length.

Encryption - Select **TKIP** or **AES** from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

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

Figure 5-21: WPA Personal Settings

wpa *(wi-fi protected access: a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.*

WPA2 Personal

To use WPA2 Personal security, select **WPA2 Personal** from the *Security* drop-down menu. WPA2 Personal uses AES encryption with dynamic keys. Enter a Passphrase that is 8-32 characters in length.

Encryption - The default for WPA2 Personal, **AES**, is automatically selected.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

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

Figure 5-22: WPA2 Personal Settings Screen

WPA2 Mixed Mode

To use WPA2 Mixed Mode security, select **WPA2 Mixed Mode** from the *Security* drop-down menu. WPA2 Mixed Mode uses TKIP and AES for encryption. Enter a Passphrase that is 8-32 characters in length.

Encryption - The default for WPA2 Personal, **TKIP +AES**, is automatically selected.

Passphrase - Enter a Passphrase, also called a pre-shared key, of 8-32 characters in the *Passphrase* field. The longer and more complex your Passphrase is, the more secure your network will be.

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

WPA Enterprise

If you want to use WPA-Enterprise, then you should select **Disabled** and use the Access Point's Web-based Utility to configure your wireless security settings. (Refer to "Chapter 6: Configuring the Wireless-G Access Point.") Click the **Next** button and proceed to step 5.

Linksys Wireless Guard

This subscription service gives you WPA Enterprise security without the work of building your own RADIUS server; it is available only in the USA and Canada.

NOTE: The Linksys Wireless Guard service is available only in the USA and Canada.

Figure 5-23: WPA2 Mixed Mode Settings Screen

radius *(remote authentication dial-in user service): a protocol that uses an authentication server to control network access.*

5. The Setup Wizard will ask you to review your settings before it saves them. Click the **Yes** button if you are satisfied with your settings, or click the **No** button if you do not want to save your new settings.

Figure 5-24: Confirm New Settings Screen

6. The *Congratulations* screen will appear. Click the **Online Registration** button to register the Access Point, or click the **Exit** button to exit the Setup Wizard.

Congratulations! The installation of the Wireless-G Access Point is complete.

If you want to make advanced configuration changes, proceed to "Chapter 6: Configuring the Wireless-G Access Point."

Figure 5-25: Congratulations Screen

Chapter 6: Configuring the Wireless-G Access Point

Overview

The Access Point has been designed to be functional right out of the box, with the default settings in the Setup Wizard. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the Web-based Utility. This chapter explains how to use the Utility.

The Utility can be accessed via Microsoft Internet Explorer or Netscape Navigator through use of a computer that is networked with the Access Point.

For a basic network setup, most users only have to use the following screens of the Utility:

- Setup
  On the *Network Setup* screen, enter your basic network settings here.
- Management
  Click the **Administration** tab and then select the **Management** screen. The Access Point's default password is **admin**. To secure the Access Point, change the AP's Password from its default.

HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.

tcp/ip: *a set of instructions PCs use to communicate over a network.*

browser: *an application that provides a way to look at and interact with all the information on the World Wide Web.*

NOTE: The Access Point is designed to function properly after using the Setup Wizard. This chapter is provided solely for those who wish to perform more advanced configuration or monitoring.

Navigating the Utility

There are four main tabs: Setup, Wireless, Administration, and Status. Additional screens will be available from most of the main tabs.

Setup

Enter the network and AP mode settings for the Access Point.

- *Network Setup*. Enter the settings for the Access Point and your Internet connection on this screen.
- *AP Mode*. Set up how the Access Point will work with other access points in your network.

Wireless

You will use the Wireless tabs to enter a variety of wireless settings for the Access Point.

- *Basic Wireless Settings*. Enter the network mode, SSID, and other basic settings on this screen.
- *Wireless Security*. Use this screen to configure the Access Point's wireless security settings.
- *Wireless MAC Filter*. From this screen, you can allow or block access to your wireless network.
- *Advanced Wireless Settings*. Configure the Access Point's more advanced wireless settings.

Administration

You will use the Administration tabs to manage the Access Point.

- *Management*. This screen allows you to customize the password settings, as well as back up or restore the Access Point's configuration file.
- *SNMP*. Configure the Simple Network Management Protocol (SNMP) settings on this screen.
- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Defaults*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.

snmp: *the standard e-mail protocol on the Internet.*

firmware: *the programming code that runs a networking device.*

Status

You will be able to view status information for your local and wireless network.

- *Local Network*. This screen will display current information on the Access Point and its local network.
- *Wireless Network*. This screen will display current information on the Access Point and its wireless network.

Accessing the Utility

To access the Web-based Utility of the Access Point, launch Internet Explorer or Netscape Navigator. In the *Address* field, enter the Access Point's default IP address, **192.168.1.245**, or the IP address you entered during the Setup Wizard. (Should you need to learn what IP address the Access Point presently uses, run the Setup Wizard again. It will scan the Access Point and give you its IP address.) Press the **Enter** key.

The login screen will appear. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

Figure 6-1: Login Screen

The Setup - Network Setup Tab

The first screen that appears is the *Network Setup* screen. This allows you to change the Access Point's general settings.

Network Setup

Device Name

You may assign any Device Name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network.

Configuration Type

Select **Automatic Configuration - DHCP** if your network router will assign an IP address to the Access Point.

The Access Point's IP Address, Subnet Mask, and Default Gateway address are displayed here.

Figure 6-2: Setup - Automatic Configuration - DHCP Screen

Select **Static IP** if you want to assign a static or fixed IP address to the Access Point. Then complete the following:

IP Address. The IP address must be unique to your network. We suggest you use the default IP address of **192.168.1.245**.

Subnet Mask. The Subnet Mask must be the same as that set on your Ethernet network.

Default Gateway. Enter the IP address of your network's gateway. The gateway is the device that enables communication between your computers and the Internet. In most cases, your router acts as your gateway.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-3: Setup - Static IP Screen

static ip address: *a fixed address assigned to a computer or device that is connected to a network.*

The Setup - AP Mode Tab

On this screen you can change the Access Point's mode of operation. In most cases, you can keep the default, **Access Point**. You may wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless repeater to extend the range of your wireless network. You may also wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless bridge; for example, you can use two Access Points in Wireless Bridge mode to connect two wired networks that are in two different buildings.

IMPORTANT: For the AP Client and Wireless Bridge modes, the remote access point must be a second Linksys Wireless-G Access Point (model number: WAP54G). For the Wireless Repeater mode, the remote wireless bridge must be a second Linksys Wireless-G Access Point (model number: WAP54G) or Wireless-G Router (model number: WRT54G).

AP Mode

The Access Point offers four modes of operation: Access Point, AP Client, Wireless Repeater, and Wireless Bridge. For the Repeater and Bridge modes, make sure the SSID, channel, and security settings are the same for the other wireless access points/devices.

LAN MAC Address

The MAC address of the Access Point is displayed here.

Access Point. The Mode is set to **Access Point** by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary.

AP (Access Point) Client. When set to AP Client mode, the AP Client is able to talk to one remote access point within its range. This feature only works with another Wireless-G Access Point (model number: WAP54G).

This mode allows the AP Client to act as a client of a remote access point. The AP Client cannot communicate directly with any wireless clients. A separate network attached to the AP Client can then be wirelessly bridged to the remote access point.

To use this mode, select **AP Client** and enter the LAN MAC address of the remote access point in the *Remote Access Point's LAN MAC Address* field. If you do not know the remote access point's MAC address, click the **Site Survey** button. Select the access point you want to use and click the **Close** button. If you do not see the access point you want, click the **Refresh** button to search for access points again.

Figure 6-4: Setup - AP Mode Screen

Figure 6-5: Site Survey Screen

Wireless Repeater. When set to Wireless Repeater mode, the Wireless Repeater is able to talk to up a remote access point within its range and retransmit its signal. This feature only works with the Linksys Wireless-G Router (model number: WRT54G) or another Wireless-G Access Point (model number: WAP54G).

Figure 6-6: Wireless Repeater Diagram

To configure a Wireless Repeater environment, select **Wireless Repeater** and enter the MAC address of the remote access point in the *Remote Access Point's LAN MAC Address* field.

Wireless Bridge. This mode connects two physically separated wired networks using two access points (use additional access points to connect more wired networks). This feature only works with another Wireless-G Access Point (model number: WAP54G).

IMPORTANT: In Wireless Bridge mode, the Access Point can ONLY be accessed by another access point in Wireless Bridge mode. In order for your other wireless devices to access the Access Point, you must reset it to Access Point mode. The two modes are mutually exclusive.

Figure 6-7: Wireless Bridge Diagram

To configure a Wireless Bridge environment, select **Wireless Bridge**, and enter the MAC addresses of the wireless bridges/access points in the *Remote Wireless Bridge's LAN MAC Addresses* fields. You will also need to set the remote wireless bridges/access points to Wireless Bridge mode.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

The Wireless - Basic Wireless Settings Tab

Change the wireless network settings on this screen.

Basic Wireless Settings

Configure the Access Point using the available settings.

Mode. Select **Mixed** and both Wireless-G and Wireless-B computers will be allowed on the network, but the speed will be reduced. Select **G-Only** for maximum speed with Wireless-G products only. The final selection, **B-Only**, allows only Wireless-B products on the network. To disable wireless performance, select **Disabled**.

Network Name (SSID). Enter the name of the Access Point's wireless network.

Channel. Select the appropriate channel from the list provided; this will be the channel that all of your wireless devices will use.

SSID Broadcast. This feature allows the SSID to be broadcast by the Access Point. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software and gain unauthorized access to your main network. Click **Enabled** to broadcast the SSID to all wireless devices in range. Click **Disabled** to increase network security and block the SSID from being seen on networked PCs.

Current Encryption. This shows the encryption method currently used by the Access Point.

SecureEasySetup Button. The status of the Access Point's SecureEasySetup feature is displayed here. If you want to use the Access Point's SecureEasySetup feature, click the **SecureEasySetup** button.

NOTE: If you have already set up your network using your router's SecureEasySetup feature, then you cannot use the Access Point's SecureEasySetup feature. You must manually configure the Access Point's wireless settings to match your existing network's settings.

NOTE: SecureEasySetup uses WPA Personal encryption. If your current wireless devices do not support WPA Personal security, then you cannot use SecureEasySetup on your network. You will need to manually configure your network security using the encryption supported by your existing devices.

You will be asked to press the SecureEasySetup button (hardware or software) on your wireless client (computer or other network device) within two minutes to complete the SecureEasySetup process. Click the **OK** button to continue.

Figure 6-8: Wireless - Basic Wireless Settings Screen

Figure 6-9: Press the SecureEasySetup Button for Your Wireless Client

A new screen will be displayed while the Access Point is waiting for you to push the SecureEasySetup button on your wireless client.

When the SecureEasySetup process is complete, the *Basic Wireless Settings* screen will appear, and the Current Encryption and Status information will be updated.

NOTE: You can only add one SecureEasySetup device at a time. For additional devices, click the **SecureEasySetup** button on the *Basic Wireless Settings* screen and repeat the process.

Reset Security. If you already set up the network using the Access Point's SecureEasySetup feature and you want to replace your current settings with new SecureEasySetup settings, click the **Reset Security** button. A new screen will appear. You will be asked to confirm that you want to reset your wireless security settings. Click the **OK** button to continue.

The Access Point will generate a new network name (SSID) and set of keys. To configure your wireless network using SecureEasySetup, return to the previous page of this User Guide and follow the instructions for the SecureEasySetup button.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

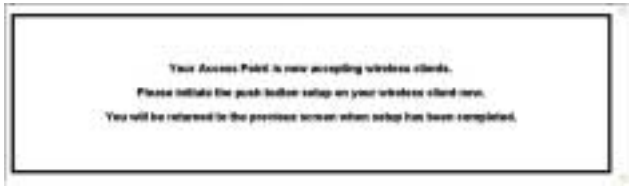


Figure 6-10: Waiting for Completion of SecureEasySetup

Figure 6-11: SecureEasySetup Completed Screen

Figure 6-12: Confirm Reset

The Wireless - Wireless Security Tab

Change the Access Point's wireless security settings on this screen.

Wireless Security

Security Mode. Select the security method you want to use, **WPA-Personal**, **WPA2-Personal**, **WPA2-Mixed**, **WPA-Enterprise**, **RADIUS**, or **WEP**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WPA2 is a stronger version of WPA. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below. For detailed instructions on configuring wireless security for the Access Point, turn to "Appendix B: Wireless Security." To disable such security, select **Disabled**.

WPA-Personal

Encryption. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. Enter a Key Renewal timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-13: Wireless - Wireless Security (WPA-Personal) Screen

encryption: *encoding data transmitted in a network.*

WPA2-Personal

Encryption. **AES** is automatically selected as the encryption method.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. Enter a Key Renewal timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-14: Wireless Security - WPA2-Personal Screen

WPA2-Mixed

Encryption. **TKIP + AES** is automatically selected so both methods can be used.

Passphrase. Enter a Passphrase (also called a WPA Shared Key) of 8-32 characters.

Key Renewal. Enter a Key Renewal timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-15: Wireless Security - WPA2-Mixed Screen

WPA-Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Access Point.)

Encryption. WPA offers you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm you want to use, **TKIP** or **AES**.

RADIUS Server. Enter the RADIUS server's IP address.

RADIUS Port. Enter the port number used by the RADIUS server.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal. Enter a Key Renewal timeout period, which instructs the Access Point how often it should change the encryption keys.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-16: Wireless Security - WPA-Enterprise Screen

radius: *a protocol that uses an authentication server to control network access.*

server: *any computer whose function in a network is to provide user access to files, printing, communications, and other services.*

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Access Point.)

RADIUS Server. Enter the RADIUS server's IP address.

RADIUS Port. Enter the port number used by the RADIUS server.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Encryption. Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, enter the Passphrase and click the **Generate** key.

Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

TX Key. Select which Key to use for data transmissions.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-17: Wireless Security - RADIUS Screen

WEP

Encryption. Select a level of WEP encryption, **40/64 bits (10 hex digits)** or **128 bits (26 hex digits)**.

Passphrase. To generate WEP keys using a Passphrase, enter the Passphrase and click the **Generate** key.

Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

TX Key. Select which Key to use for data transmissions.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-18: Wireless Security - WEP Screen

The Wireless - Wireless MAC Filter Tab

This screen allows you to permit or block wireless access for computers with specific MAC addresses.

Wireless MAC Filter

Access Restriction

If you want to control access to your wireless network, select **Enable**. If you do not wish to filter users by MAC address, select **Disable**.

To deny access, click **Prevent PCs listed below from accessing the wireless network**. To permit access, click **Permit PCs listed below to access the wireless network**.

MAC 01-25. Enter the MAC addresses of the computers whose access you want to control. If you want to list more than 25 MAC addresses, then select **MAC Addresses 26~50** from the drop-down menu.

Click **Clear** to delete the MAC addresses you have entered.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-19: Wireless - Wireless MAC Filter Screen

mac address: *the unique address that a manufacturer assigns to each networking device.*

The Wireless - Advanced Wireless Settings Tab

This screen allows you to configure the advanced settings for the Access Point. In most cases, these settings do not need to be changed.

Figure 6-20: Wireless - Advanced Wireless Settings Screen

Advanced Wireless

You can change the data transmission and output power settings for the Access Point.

Authentication Type. Select the authentication method you want the Access Point to use, **Shared Key** or **Open System (Default)**. Shared Key is when both the sender and the recipient share a WEP key for authentication. Open System is when the sender and the recipient do not share a WEP key for authentication. All devices on your network must use the same authentication type. In most cases, keep the default, **Open System (Default)**.

Basic Rates. This setting is not actually one rate of transmission but a series of rates that are advertised to the other wireless devices in your network, so they know at which rates the Access Point can transmit. At the **Default** setting, the Access Point will advertise that it will automatically select the best rate for transmission. Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when you wish to have all rates advertised. The Basic Data Rates are not the rates transmitted; the rates transmitted can be configured through the Transmission Rates setting on this screen.

Transmission Rates. The range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can keep the default setting, **Auto (Default)**, to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client.

Transmission Power. You can adjust the output power of the Access Point to get the appropriate coverage for your wireless network. Select the level you need for your environment. If you are not sure which setting to choose, then keep the default setting, **Full (Default)**.

CTS Protection Mode. The CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance. Select **Enable** if you want to permanently enable this feature, or keep the default, **Disable**, if you want to permanently disable this feature. In most cases, CTS Protection Mode should remain disabled, unless the Wireless-G products are experiencing severe problems trying to transmit to the Access Point in an environment with heavy 802.11b traffic.

***cts** (clear-to-send): a signal sent by a wireless device, signifying that it is ready to receive data.*

Frame Burst Mode. Enabling this option should reduce overhead and enhance your network performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Disabled**.

Antenna Selection. This selection is for choosing which antenna transmits data, left or right. If you are not sure which antenna to use, keep the default, **Diversity**, to increase reception.

Beacon Interval. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless networks service area, the Access Point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

packet: *a unit of data sent over a network.*

beacon internal: *data transmitted on your wireless network that keeps the network synchronized.*

DTIM Interval. This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.

dtim *(delivery traffic indication message): a message included in data packets that can increase wireless efficiency.*

Fragmentation Threshold. This specifies the maximum size a data packet can be before splitting and creating a new packet. It should remain at its default setting of **2346**. A smaller setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

fragmentation: *breaking a packet into smaller units when transmitting over a network.*

RTS Threshold. This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications are recommended.

rts *(request to send): a networking method of coordinating large packets through the RTS Threshold setting.*

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

The Administration - Management Tab

On this screen you can configure the password as well as back up or restore the Access Point's configuration file.

Figure 6-21: Administration - Management Screen

Management

You should change the password that controls access to the Access Point's Web-based Utility.

AP's Password

Password. Create a Password for the Access Point's Web-based Utility.

Re-enter to Confirm. To confirm the new Password, enter it again in this field.

Backup and Restore

On this screen you can create a backup configuration file or save a configuration file to the Access Point.

Backup Settings. To save a backup configuration file on a computer, click the **Backup Settings** button and follow the on-screen instructions.

Restore Settings. To upload a configuration file to the Access Point, click the **Restore Settings** button and follow the on-screen instructions.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

The Administration - SNMP Tab

SNMP is a popular network monitoring and management protocol. It provides network administrators with the ability to monitor the status of the Access Point and receive notification of any critical events as they occur on the Access Point.

Figure 6-22: Administration - SNMP Screen

SNMP V1/V2c

To enable the SNMP support feature, select **Enable**. Otherwise, select **Disable**.

Contact. Enter the name of the contact person, such as a network administrator, for the Access Point.

Device Name. Enter the name you wish to give to the Access Point.

Location. Enter the location of the Access Point.

SNMP Community

You can have up to two passwords. Then select the level of access you want to assign to each password.

(**public**.) Enter the first password that allows access to the Access Point's SNMP information. The default is **public**. Then select the level of access you want to assign, **Read-Only** or **Read/Write**.

(**private**.) Enter the second password that allows access to the Access Point's SNMP information. The default is **private**. Then select the level of access you want to assign, **Read-Only** or **Read/Write**.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

The Administration - Log Tab

On this screen you can configure the log settings.

Management

You can have logs that keep track of the Access Point's activities.

Log

To enable the Log support feature, select **Enabled**. Otherwise, select **Disabled**.

Logviewer IP Address. If you have chosen to monitor the Access Point's traffic, then you can designate a PC that will receive permanent log files periodically. In the field provided, enter the IP address of this PC. To view these permanent logs, you must use Logviewer software, which can be downloaded free of charge from *www.linksys.com/international*.

View Log. To see a temporary log of the Access Point's most recent activities, click this button.

On the *View Log* screen, click the **First Page** button to see the first page of log entries. Click the **Last Page** button to see the last page of log entries. Click the **Previous Page** button to see the previous page of log entries, and click the **Next Page** button to see the next page of log entries. To delete all log entries, click the **Clear Log** button. To update the log with the most recent activities, click the **Refresh** button.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Help** for more information.

Figure 6-23: Administration - Log Screen

Figure 6-24: View Log Screen

The Administration - Factory Defaults Tab

On this screen you can restore the Access Point's factory default settings.

Management

Write down any custom settings before you restore the factory defaults. Once the Access Point is reset, you will have to re-enter all of your configuration settings.

Factory Defaults

Restore Factory Defaults. To restore the Access Point's factory default settings, click this button. Then follow the on-screen instructions.

Click **Help** for more information.

Figure 6-25: Administration - Factory Defaults Screen

The Administration - Firmware Upgrade Tab

On this screen you can upgrade the Access Point's firmware. Do not upgrade the firmware unless you are experiencing problems with the Access Point or the new firmware has a feature you want to use.

Firmware Upgrade

Before you upgrade the Access Point's firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings. To upgrade the Access Point's firmware:

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com/international*.
2. Extract the firmware upgrade file on your computer.
3. On the *Firmware Upgrade* screen, enter the location of the firmware upgrade file in the field provided, or click the **Browse** button to find the file.
4. Click the **Upgrade** button, and follow the on-screen instructions. You can also click the **Cancel** button to cancel the upgrade, or click the **Help** button for more information.

Click **Help** for more information.

Figure 6-26: Administration - Firmware Upgrade Screen

upgrade: *to replace existing software or firmware with a newer version*

The Status - Local Network Tab

The *Local Network* screen displays the Access Point's current status information for the local network.

Figure 6-27: Status - Local Network Screen

AP's Information

Firmware Version. This is the version of the Access Point's current firmware.

Local Network

MAC Address. The MAC address of the Access Point's Local Area Network (LAN) interface is displayed here.

AP's IP Address. This shows the Access Point's IP Address, as it appears on your local network.

Subnet Mask. This shows the Access Point's Subnet Mask.

Default Gateway. Displayed here is the IP address of the Access Point's Default Gateway.

Click **Help** for more information.

The Status - Wireless Network Tab

The *Wireless Network* screen displays the Access Point's current status information for its wireless network.

Figure 6-28: Status - Wireless Network Screen

Wireless Network

MAC Address. The MAC Address of the Access Point's wireless interface is displayed here.

Mode. The Access Point's mode is displayed here.

Network Name (SSID). The Access Point's main SSID is displayed here.

Channel. The Access Point's Channel setting for wireless broadcast is shown here.

Security. The wireless security setting for the Access Point is displayed here.

SSID Broadcast. Shown here is the setting of the Access Point's SSID Broadcast feature.

Click **Help** for more information.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Access Point. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com/international*.

Frequently Asked Questions

Can the Access Point act as my DHCP server?
No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

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 multiplayer games with other users 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 802.11 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?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

What is roaming?

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

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

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

What is the 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?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers a variety of wireless security methods to enhance security and access control. Users can set it up depending upon their needs.

Can Linksys wireless products support file and printer sharing?

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

What is WEP?

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

What is a MAC Address?
The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I avoid interference?
Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, make sure to operate each one on a different channel (frequency).

How do I reset the Access Point?
Press the Reset button on the back of the Access Point for about ten seconds. This will reset the unit to its default settings.

How do I resolve issues with signal loss?
There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an Access Point and wireless PC will create signal loss. Leaded glass, metal, concrete floors, water, and walls will inhibit the signal and reduce range. Start with your Access Point and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, open the Access Point's Web-based Utility. Click the **Wireless** tab and then the **Advanced Wireless** tab. Make sure the Output Power is set to 100%.

Does the Access Point function as a firewall?
No. The Access Point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but I cannot see my network.
Wireless security, such as WEP or WPA, is probably enabled on the Access Point, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices in your wireless network.

What is the maximum number of users the Access Point can handle?
No more than 65, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.

Appendix B: Wireless Security

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

Security Precautions

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

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

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

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

Security Threats Facing Wireless Networks

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

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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Four modes are available: WPA-Personal, WPA2-Personal, WPA-Enterprise, and RADIUS. WPA-Personal gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption Standard), which utilizes a symmetric 128-Bit block data encryption. WPA2-Personal only uses AES encryption, which is stronger than TKIP. WPA-Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication.

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.

WPA2-Personal. 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. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

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

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

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

Appendix C: Upgrading Firmware

The Access Point's firmware is upgraded through the Web-based Utility's Administration - Firmware Upgrade tab. Follow these instructions:

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com/international*.
2. Extract the firmware upgrade file on your computer.
3. Open the Access Point's Web-based Utility.
4. Click the **Administration** tab.
5. Click the **Upgrade Firmware** tab.
6. On the *Firmware Upgrade* screen, enter the location of the firmware upgrade file in the field provided, or click the **Browse** button to find the file.
7. Click the **Upgrade** button, and follow the on-screen instructions.

Figure C-1: Firmware Upgrade

Appendix D: Windows Help

Almost 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

802.11b - 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 (**De**-**m**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.

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.

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

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

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

Router - A networking device that connects multiple networks together.

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

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

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

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

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

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

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects 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.

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	WAP54G
Standards	IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Ports/Buttons	One 10/100 Auto-Cross Over (MDI/MDI-X) port, power port, reset and SES button
LEDs	Power, Activity, Link, SecureEasySetup
Transmit Power	802.11g: Typ. 13.5 +/- 2dBm @ Normal Temp Range 802.11b: Typ: 16.5 +/- 2dBm @ Normal Temp Range
Security Features	WPA, WPA2, Linksys Wireless Guard (USA and Canada only), WEP Encryption, MAC Filtering, SSID Broadcast enable/disable
WEP Key Bits	64/128-bit
Dimensions (W x H x D)	186 mm x 48 mm x 169 mm
Unit Weight	0,46 kg
Power	External, 12V DC
Certifications	FCC, CE, IC-03
Operating Temp.	0ºC to 40ºC
Storage Temp.	0ºC to 70ºC

Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

Appendix G: Warranty Information

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

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

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

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

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

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

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

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

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

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

Declaration of Conformity with Regard to the EU Directive 1995/5/EC (R&TTE Directive)

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

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

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

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

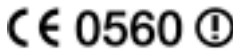
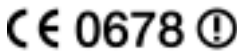
If you need any other technical documentation, see the "Technical Documents on www.linksys.com/international" section, as shown later in this appendix.

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

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

CE Marking

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

 or  or 

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

National Restrictions

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

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

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

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

Belgium

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

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

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

France

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

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

Table 1: Applicable Power Levels in France

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

Italy

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

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

Product Usage Restrictions

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

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

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

Power Output of Your Device

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

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

Wireless Adapters

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

Windows XP

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

Windows 2000

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

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

Wireless Access Points, Routers, or Other Wireless Products

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

Technical Documents on www.linksys.com/international

Follow these steps to access technical documents:

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

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

Appendix 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/international

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

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

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