

LINKSYS[®]
A Division of Cisco Systems, Inc.



2.4GHz
802.11g **Wireless-G**



Access Point

User Guide

Model No. **WAP54G v2**



Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2004 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

How to Use this Guide

Your 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 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 in the "Table of Contents".

Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this Guide?	2
Chapter 2: Planning your Wireless Network	4
Network Topology	4
Roaming	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-G Access Point	6
The Back Panel	6
The Front Panel	7
Chapter 4: Connecting the Wireless-G Access Point	8
Hardware Installation	8
Chapter 5: Setting Up the Wireless-G Access Point	9
Setup Wizard	9
Linksys Wireless Guard Setup	15
Chapter 6: Linksys Wireless Guard	18
Client Software Installation	18
Network Access	21
Your Account	22
Chapter 7: Configuring the Wireless-G Access Point	29
Overview	29
Navigating the Utility	30
Accessing the Utility	31
The Setup Tab	32
The Status Tab	40
The Advanced Tab	41
The Help Tab	45
Appendix A: Troubleshooting	46
Frequently Asked Questions	46
Appendix B: Wireless Security	50
Security Precautions	50
Security Threats Facing Wireless Networks	50

Appendix C: Upgrading Firmware	53
Appendix D: Windows Help	54
Appendix E: Glossary	55
Appendix F: Specifications	59
Appendix G: Warranty Information	61
Appendix H: Regulatory Information	62
Appendix I: Contact Information	64

List of Figures

Figure 3-1: The Access Point's Back Panel	6
Figure 3-2: Front Panel	7
Figure 5-1: The Setup Wizard's Welcome Screen	9
Figure 5-2: Connecting the Access Point	10
Figure 5-3: Select an Access Point	10
Figure 5-4: Enter the Password	11
Figure 5-5: The Configure Network Address Settings Screen	11
Figure 5-6: The Wireless Settings Screen	12
Figure 5-7: The Security Settings Screen	12
Figure 5-8: The WEP Settings Screen	13
Figure 5-9: The WPA-PSK Screen	13
Figure 5-10: The Congratulations Screen	14
Figure 5-11: The Attention Screen	15
Figure 5-12: The Linksys Wireless Guard Setup Screen	15
Figure 5-13: The Securing your Access Point Screen	16
Figure 5-14: Note the New Password Screen	16
Figure 5-15: The Adding Authorized Users Screen	17
Figure 5-16: The Congratulations Screen	17
Figure 6-1: Note	18
Figure 6-2: Configuring Windows Installer	18
Figure 6-3: Exit Applications	19
Figure 6-4: License Agreement	19
Figure 6-5: Destination Location	20
Figure 6-6: Copying Files	20
Figure 6-7: Restart your Computer	21
Figure 6-8: The Network Access Screen	21
Figure 6-9: Member Login	22
Figure 6-10: Home	23

Figure 6-11: Network Administration	23
Figure 6-12: Modify Access Control	24
Figure 6-13: Add Guest	24
Figure 6-14: Add Member	25
Figure 6-15: Welcome	25
Figure 6-16: Subscriber Information	26
Figure 6-17: Account Finances	26
Figure 6-18: Credentials Information	27
Figure 6-19: Congratulations	27
Figure 7-1: Password Screen	31
Figure 7-2: The Basic Setup Screen	32
Figure 7-3: WPA Pre-Shared Key Settings	34
Figure 7-4: WPA Radius Settings	34
Figure 7-5: Radius Settings	35
Figure 7-6: WEP Settings	35
Figure 7-7: The Password Screen	36
Figure 7-8: The AP Mode Screen	37
Figure 7-9: The Site Survey screen	37
Figure 7-10: Wireless Repeater diagram	38
Figure 7-11: Wireless Bridge diagram	38
Figure 7-12: The Log screen	39
Figure 7-13: The Status Screen	40
Figure 7-14: The Filters Screen	41
Figure 7-15: The Advanced Wireless screen	42
Figure 7-16: The SNMP screen	44
Figure 7-17: The Help screen	45
Figure C-1: Upgrade Firmware	53

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. Being a dual-band access point, not only does the Access Point bring you these benefits, it also allows two wireless standards, 802.11g and 802.11b, to communicate with each other. This means that PCs with different wireless standards can communicate with each other and with a wired network.

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.

network: a series of computers or devices connected together

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.

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

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

adapter: a device that adds network functionality to your PC

What's in this Guide?

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

- **Chapter 1: Introduction**
This chapter describes the Wireless-G 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 Web-Based Utility to configure the settings on the Access Point and how to install the setup on the Access Point for the Linksys Wireless Guard.
- **Chapter 6: The Linksys Wireless Guard**
This chapter explains how to install the client software for Linksys Wireless Guard and other information on the service.
- **Chapter 7: Configuring the Wireless-G Access Point**
This chapter explains the use of the Access Point's Web-based Utility.
- **Appendix A: Troubleshooting**
This appendix describes some frequently asked questions regarding installation and use of the Wireless-G 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.

Wireless-G Access Point

- **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.

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.

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.

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

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

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

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

ssid: your wireless network's name

Network Layout

The Wireless-G Access Point has been designed for use with 802.11g and 802.11b products. With 802.11g products communicating with the 802.11b standard, products using these standards can communicate with each other. The Access point is compatible with 802.11g and 802.11b adapters, such as the PC Cards for your laptop computers, PCI Card for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with a 802.11g or 802.11b wireless PrintServer.

When you wish to connect your wired network with your wireless network, the Access Point's network port can be used to connect to any of Linksys's switches or routers.

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

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

The Back Panel

The Access Point's ports, where the power cord and network cable are connected, are located on the back panel.

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



Figure 3-1: The Access Point's Back Panel



Important: Resetting the Access Point will erase all of your settings (WEP Encryption, Wireless and LAN settings, etc.) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

- | | |
|---------------------|---|
| LAN | This LAN (Local Area Network) port connects to Ethernet network devices, such as a switch or router. |
| Power | The Power port is where you will connect the power adapter. |
| Reset Button | There are two ways to Reset the Access Point's factory defaults. Either press the Reset Button , for approximately ten seconds, or restore the defaults from the Password tab in the Access Point's Web-Based Utility. |

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about products that work with the Access Point.

The Front Panel

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



Figure 3-2: Front Panel

Power	Green. The Power LED lights up when the Access Point is powered on.
Act	Green. If the Act LED is flickering, the Access Point is actively sending or receiving data to or from one of the devices over the LAN port.
Link	Green. The Link LED lights whenever the Access Point is successfully connected to a device through the LAN port.

Chapter 4: Connecting the Wireless-G Access Point

Hardware Installation

1. Locate an optimum location for the Access Point. The best place for the Access Point is usually at the center of your wireless network, with line of sight to all of your PCs and wireless accessories.
2. Fix the direction of the antenna. Try to place it in a position that will best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
3. Connect a standard Ethernet network cable to the Access Point. Then, connect the other end of the Ethernet cable to a switch or router. The Access Point will then be connected to your 10/100 Network.
4. Connect the AC Power Adapter to the Access Point's Power Socket. Only use the power adapter supplied with the Access Point. Use of a different adapter may result in product damage.

Now that the hardware installation is complete, proceed to Chapter 5: Setting Up the Wireless-G Access Point, for directions on how to set up the Access Point.

hardware: the physical aspect of computers, telecommunications, and other information technology devices



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.



NOTE: If you are setting up an Infrastructure Network, all of your wireless devices must be in Infrastructure mode in order to function within the network. Similarly, if your network is an Ad-Hoc Network, all of your wireless devices must operate in Ad-hoc mode in order for all other wireless devices to communicate.

Chapter 5: Setting Up the Wireless-G Access Point

Setup Wizard

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.

1. Insert the Setup Wizard CD into your PC's CD-ROM drive. Your PC must be on your wired network to set up the Access Point.
2. The Setup Wizard's Welcome screen should appear on your monitor. If it does not, this means the Setup Wizard is not automatically running as it should. Start the Setup Wizard manually by clicking the **Start** button, selecting **Run**, and typing **d:\setup.exe** (where "D" is your PC's CD-ROM drive). Click the **Setup** button to continue this Setup Wizard. Clicking the **User Guide** button opened this Guide. To exit this Setup Wizard, click the **Exit** button.



Note: The Access Point should be set up through a wired network connection as shown in Chapter 4: Connecting the Wireless-G Access Point. If you wish to set up the Access Point wirelessly, the wireless computer will require you to use the Linksys default settings. These settings can then be changed with the Setup Wizard or Web-based Browser Utility



Figure 5-1: The Setup Wizard's Welcome Screen

Wireless-G Access Point

3. The next screen displayed displays how the Access Point should be connected while running this Setup Wizard. Optimally, you should perform this setup through a PC on your wired network. Click the **Next** button to continue or **Exit** to exit the Setup Wizard.



Figure 5-2: Connecting the Access Point

4. 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 each 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 and click the **Yes** button to continue or **No** to exit the Setup Wizard.

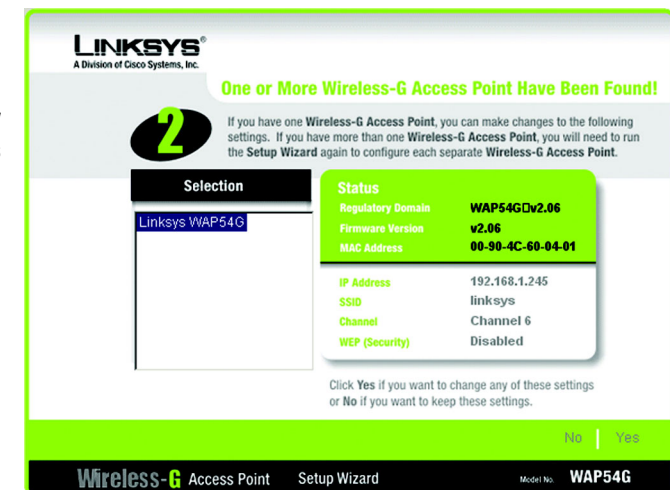


Figure 5-3: Select an Access Point

5. You will be asked to sign onto the Access Point you've selected. Enter the Password you've assigned. If none has been assigned, enter the default password: **admin**. Then, click the **OK** button. (This password can be changed from the Web-based Utility's Password tab.)

Figure 5-4: Enter the Password

ip (internet protocol): a protocol used to send data over a network

6. The Configure Network Address Settings screen will appear next. Enter an IP Address, Subnet Mask, and the IP Address of your network Gateway. Then, click the **Next** button to continue or **Back** to return to the previous page.
 - 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 your Ethernet network.
 - Gateway. This IP address should be the IP address of the gateway device that allows for contact between the Internet and the local network.

Figure 5-5: The Configure Network Address Settings Screen

ip address: the address used to identify a computer or device on a network

gateway: a device that interconnects networks with different, incompatible communications protocols

7. The Wireless Settings screen should now appear. Enter your wireless network's SSID and select the channel at which the network broadcasts its wireless signal. Also enter a Device Name to prevent any confusion when using multiple Access Points. Then, click the **Next** button to continue or **Back** to return to the previous page.

- **SSID.** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Channel.** Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11. All points in your wireless network must use the same channel in order to function correctly.
- **Device Name.** The Device Name is a unique name given to the Access Point to prevent confusion when using multiple Access Points.

LINKSYS®
A Division of Cisco Systems, Inc.

Wireless Settings

4 If you are using Linksys wireless adapters in your computers, your network should work right out of the box! Changes to the settings below may disrupt the settings of your existing wireless network. Make sure you remember these settings as they will be needed when setting up your wireless computers.

SSID linksys The SSID is a unique identification shared among all computers within your wireless network and must be the same for all those computers. The SSID is **case sensitive** and should not exceed **32** characters.

Channel 6 The Channel setting is a unique number shared among all computers within your wireless network. If you experience poor performance on a certain channel, try changing to another channel. Channels 1, 6, and 11 are preferred.

Device Name Linksys WAP54G The Device Name is a unique name for your Wireless-G Access Point and should be changed if you have multiple Access Points in your network.

Back | Next

Wireless-G Access Point Setup Wizard Model No. WAP54G

Figure 5-6: The Wireless Settings Screen

8. The Security Settings screen will appear next. From this screen, you can set the level of security you desire for your network. Select from WEP, WPA-Personal, WPA Enterprise, and Linksys Wireless Guard. All points in your wireless network must use the same security method.

LINKSYS®
A Division of Cisco Systems, Inc.

Security Settings

5 At this point, you have the opportunity to enable wireless security, which prevents unauthorized access to your wireless network. For your own security, please read and choose from the following options.

Security

weak **strong**

Disabled If you are setting up a publicly available network, you can leave wireless security disabled.

WEP Wired Equivalent Privacy (WEP) is a security system that encrypts the data sent over the wireless network so that only users that know the encryption key can access the network.

WPA-Personal The Pre-Shared Key mode of Wi-Fi Protected Access (WPA-PSK) is similar to WEP but stronger, with longer and constantly changing encryption keys.

WPA-Enterprise The RADIUS mode of Wi-Fi Protected Access (WPA-RADIUS) secures corporate wireless networks by authorizing each device against a master list held in a special authentication server.

Linksys Wireless Guard Linksys Wireless Guard is a subscription service that gives small businesses the industrial-strength security of WPA-RADIUS, without the hassle of building your own RADIUS server. [Learn more](#)

Back | Next

Wireless-G Access Point Setup Wizard Model No. WAP54G

Figure 5-7: The Security Settings Screen

- WEP. From this screen, you can set the level of encryption you desire for your network, along with selecting Passphrases and/or encryption keys.

The WEP key can consist of the letters "A" through "F" and the numbers "0" through "9" and should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

Figure 5-8: The WEP Settings Screen

bit: a binary digit

encryption: encoding data transmitted in a network

- WPA Personal. With WPA Personal (WPA PSK, or Pre-Shared Keys) you have two encryption options, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. Enter a Pre-Shared Key of 8-32 characters.
- WPA-Enterprise. This option is for corporate wireless networks only and uses a special authentication server. To choose this option, select **Disable**. You will need to enable the option in the web-based utility. Refer to Chapter 7: Configuring the Wireless-G Access Point.
- Linksys Wireless Guard. With this subscription service, you get the highest security of WPA RADIUS, but without having to build your own RADIUS network. If you select this option, follow the step-by-step instructions in the next section, Linksys Wireless Guard.

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

For more information on wireless security, refer to Appendix B: Wireless Security.

Figure 5-9: The WPA-PSK Screen

Wireless-G Access Point

9. At this point, the configuration performed with the Setup Wizard is complete. To configure any other Access Points in your network, you can run this Setup Wizard again.

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

For more advanced configuration, you can go to Chapter 7: Configuring the Wireless-G Access Point.



Figure 5-10: The Congratulations Screen

Linksys Wireless Guard Setup

Linksys Wireless Guard is a subscription service that gives you WPA RADIUS without having to build your own RADIUS network. Follow the instructions below. To learn more about Linksys Wireless Guard, go to www.linksys.com/wirelessguard. If you need help with setting up Linksys Wireless Guard, contact us at wirelessguard@linksys.com or call 888-231-5506.

1. After clicking on *Linksys Wireless Guard* for your security selection, this screen will appear. Before you continue with the setup, make sure your computer meets the following requirements.

- Windows XP or Windows 2000 operating system
- 128 MB RAM
- 50MB free disk space
- A wireless network interface with a driver that supports WPA security
- Must be connected to the Internet through a broadband connection (DSL, cable, other)

If you meet these requirements, click **Continue** to sign up for the Linksys Wireless Guard service, or click **Cancel** to cancel the setup.

2. This screen guides you through the registration process. Enter your user name, password, first and last name, E-mail address, and a security question and answer below. Then, click **Next** to continue or **Exit** if you want to quit the Setup Wizard.

- User Name and Password. Enter the user name you want to use into the *User Name* field. Enter the Password you want to use in the *Password* field.
- Confirm Password. Enter the password again into the *Confirm Password* field.
- First and Last Name. Enter your first and last names into the fields.
- E-mail address. Enter your E-mail address into the field.
- Security Question and Answer. Select a security question from the *Security Question* drop-down menu to help identify you if you forget your password. Enter the answer to your selected question in the *Security Answer* field.

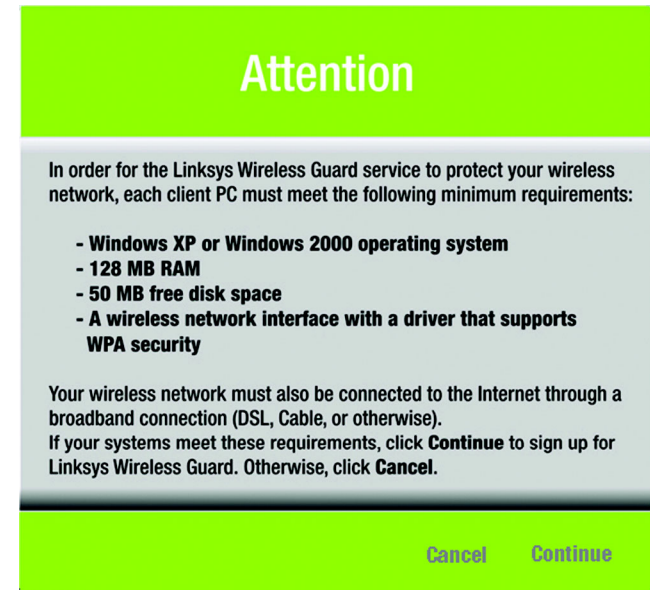


Figure 5-11: The Attention Screen

Figure 5-12: The Linksys Wireless Guard Setup Screen

Wireless-G Access Point

- When the next screen appears, your Access Point will be automatically configured. Make sure that the correct access point is selected and that the name is correct. Also, make sure that the SSID is correct. Click **Next** to add this Access Point to your network or click **Back** to return to the previous screen.

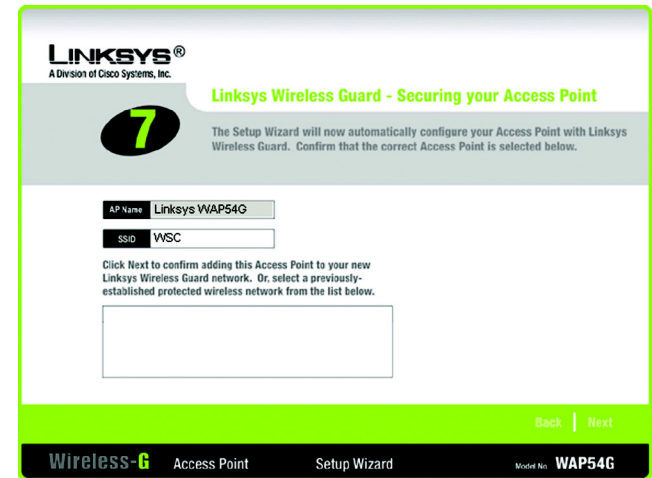


Figure 5-13: The Securing your Access Point Screen

- For security reasons, the password has been automatically changed. Please note the new password before continuing or you won't be able to access the Access Point later. After writing down the new password, select **I have noted the new password**, then click **OK**.

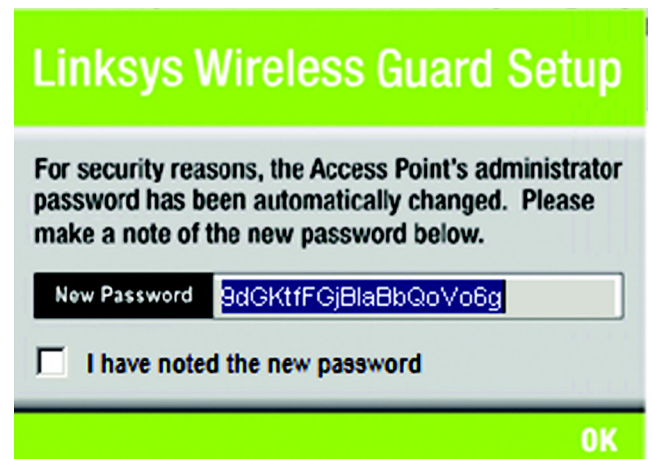


Figure 5-14: Note the New Password Screen

Wireless-G Access Point

- When the next screen appears, you will specify which users you will allow access to this protected network. Enter the E-mail address, User Name, Password, then Confirm Password for each user. Then, click **Add**. To remove a user from the list, select the user, then click **Remove**.

LINKSYS®
A Division of Cisco Systems, Inc.

Linksys Wireless Guard - Adding Authorized Users

Please specify which users are authorized to access this protected wireless network by entering their information below, then clicking **Add**. If a user is already registered with Linksys Wireless Guard, you only need to fill in their e-mail address.

Access control list for network: WSCWSC

Email Address	User Name	Network Owner
<div><div>Email Address</div><div>User Name</div><div>Password</div><div>Confirm Password</div></div>		

Remove **Add**

Back **Next**

Wireless-G Access Point Setup Wizard Model No: WAP54G

Figure 5-15: The Adding Authorized Users Screen

- The Access Point is now configured for Linksys Wireless Guard. To finish configuring your wireless network, you will need to install the Linksys Wireless Guard client software for each PC that will have access. Click **Main Menu**, then click **Linksys Wireless Guard Client**.

To add more Access Points to your Linksys Wireless Guard network,
run the Linksys Wireless Guard Setup again for each Access Point.



Figure 5-16: The Congratulations Screen

Chapter 6: Linksys Wireless Guard

This chapter is only for users who have signed up for Linksys Wireless Guard to secure their network and have configured the Access Point for Linksys Wireless Guard. (Refer to Chapter 5: Setting up the Wireless-G Access Point.)

You will now need to install the client software needed to securely connect a PC to your Access Point that is protected by Linksys Wireless Guard. This chapter will also show you how to access your protected network, and manage your account.

Client Software Installation

1. If you haven't already done so, on the Main Menu of the Setup-CD-ROM, click **Linksys Wireless Guard Client**. The screen in Figure 6-1 will appear. To install the software on this PC, click **Continue**. Click **Cancel** to cancel the installation.
2. A screen will appear to notify you that the setup is in process. Wait until the next screen appears. Only if you want to end the installation process, click **Cancel**.



IMPORTANT: Make sure that you have signed up for Linksys Wireless Guard and that you have configured the Access Point for Linksys Wireless Guard before starting the installation of the client software.

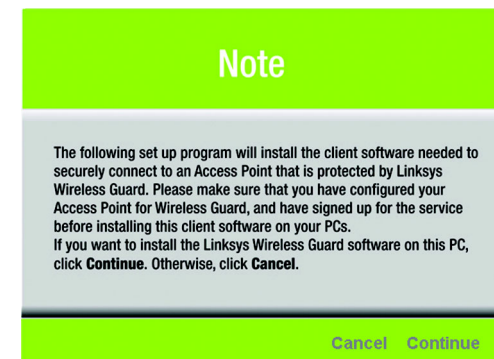


Figure 6-1: Note

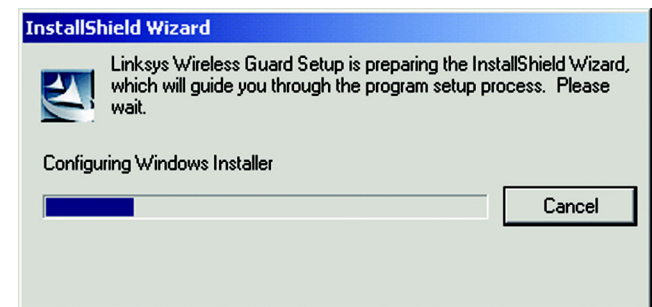


Figure 6-2: Configuring Windows Installer

Wireless-G Access Point

3. The next screen informs you to close all other applications before continuing. If no other applications are open, click **Next** to continue. If you want to exit to close your other applications, click **Cancel**.

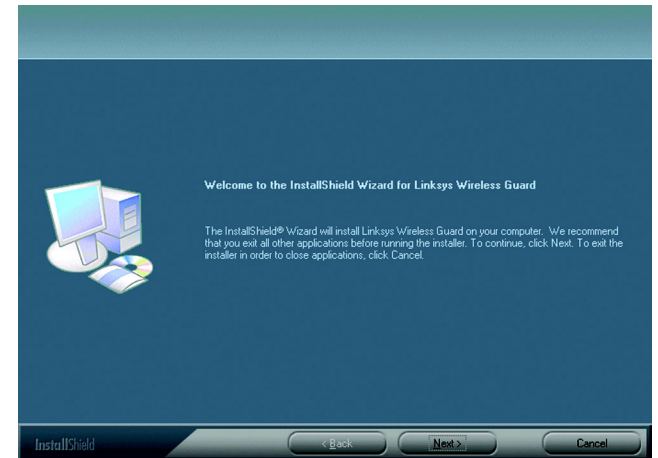


Figure 6-3: Exit Applications

4. A license agreement will appear next. Scroll down or press PAGE DOWN to read the entire agreement. To accept the terms and continue the installation, click **Yes**. To quit the installation, Click **No**.

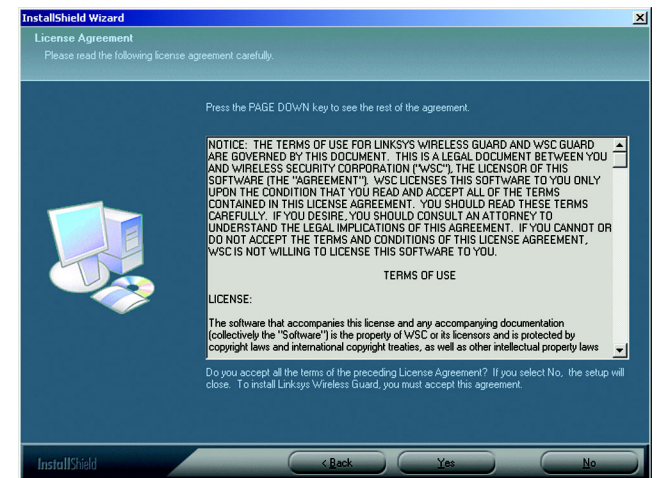


Figure 6-4: License Agreement

5. On this screen, you will be informed where the Linksys Wireless Guard will be installed. To install to the folder, click **Next**. If you want to choose a different location for the folder, click the **Browse** button and select the location.

Click **Back** to return to the previous screen. Click **Cancel** to cancel the installation.

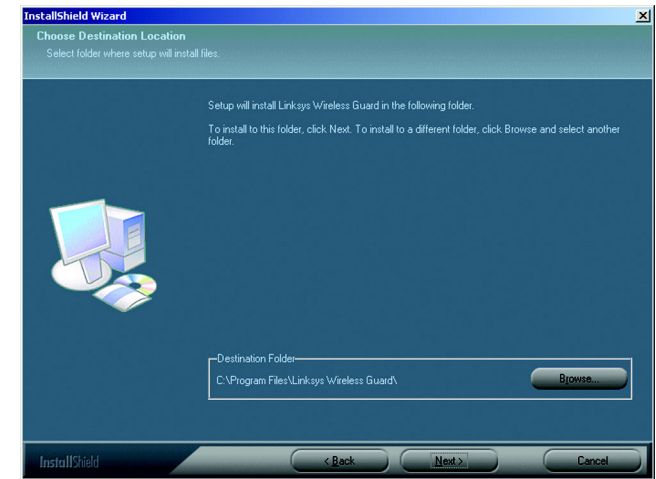


Figure 6-5: Destination Location

6. The program files will start copying. Click **Next** to continue.

Click **Back** to return to the previous screen. Click **Cancel** to cancel the installation.

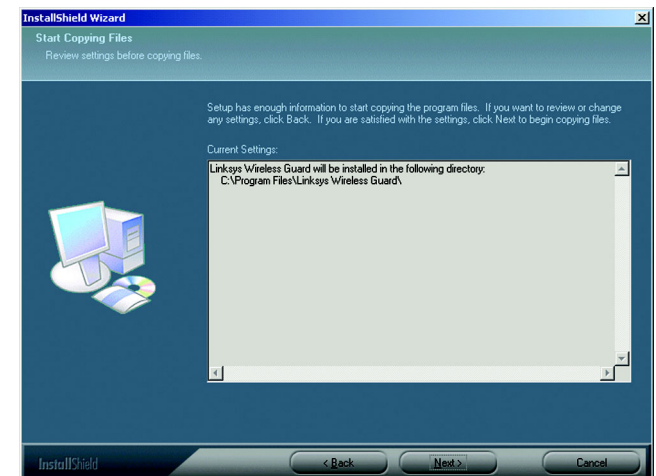


Figure 6-6: Copying Files

Wireless-G Access Point

7. The Linksys Wireless Guard is successfully installed. Before you can use the program, you must restart your computer. Select **Yes** to restart your computer now. Select **No** to restart your computer at a later time. Remove any disks that are in their drives, then click **Finish**.
8. After the Linksys Wireless Guard is installed, a key icon will be installed on the right-side of the system tray at the bottom of your screen. The color of the key will change with the status of the network connection. The most common colors are described below.



Green - Connected.

Green with Red X - Connected, but waiting for authentication.

Gray - Not connected.

Red - Connected to a network that is not protected by Linksys Wireless Guard.

Network Access

After Linksys Wireless Guard is installed, any time you access a Linksys Wireless Guard protected network, this screen will appear. To access your network, click **Login as a Wireless Guard Member**, or if you are a guest, click **Login as a Wireless Guard Guest**. Enter your user name and password, then click **Login**.

Login as a Wireless Guard Member. Select this option if you are a registered member.

Login as a Wireless Guard Guest. Select this option if you are a registered guest member. The guest must first be added as a guest in the **Membership and Network Administration Website**. See the Add a Guest section, below.

Save Password. Select this if you want the system to remember your password so you don't have to enter it when you log in.

Enable Auto Login. Select this if you want the system to bypass the log in.

Click **Cancel** to cancel the login or if you forget your password, click **Lost Password**.

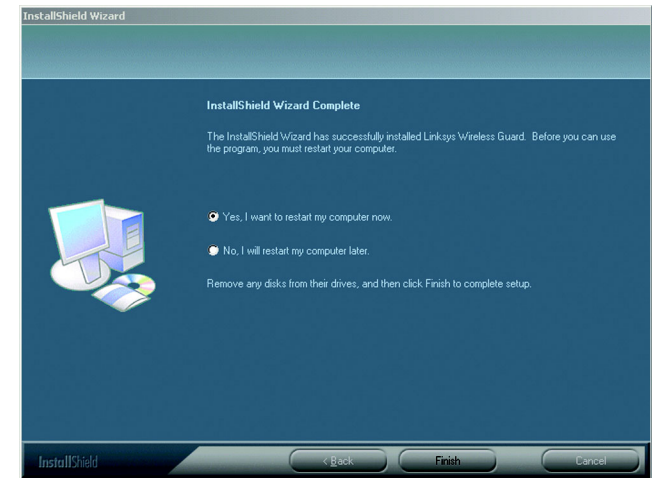


Figure 6-7: Restart your Computer



Figure 6-8: The Network Access Screen

Your Account

This section explains how to access your account, how to add a guest, how to add another member to your account, and how to secure and unprotect the Linksys Wireless Guard network.

For more detailed information on your account and the website, click on your computer's **Start** button, select the **Linksys Wireless Guard** folder, then click **Linksys Wireless Guard Help**. For further information on the Linksys Wireless Guard only, you can contact Linksys Wireless Guard Technical Support at 888 231-5506 or E-mail us at wirelessguard@linksys.com.

Accessing your Account

Right-click on the green Wireless Guard Network key icon, then click **View Membership and Network Administration Website** to log in to the Linksys Wireless Guard website.

You can also click on your computer's **Start** button, select the **Linksys Wireless Guard** folder, then click **Membership and Network Administration Website**.

1. The screen in Figure 6-9 will appear. Enter the administrator's user name and password in the fields. Click **Login**.
2. The Wireless Guard Member Website home screen will appear. From this website, you can modify your member or billing profile, view information about your account or subscription, add or remove members, modify access to members and guests, change network settings, and download updates and documentation. There is an extensive Help tab to help you with everything on the website. The instructions for adding a guest or member, or securing and unprotecting your network are also explained below.



The screenshot shows the Linksys Wireless Guard Member Login page. At the top, there is a blue header with the Linksys logo on the left and 'Wireless Guard Member Website' on the right. Below the header, the page title is 'Linksys Wireless Guard Member Login'. The main content area contains a login form with the text 'If you already created a user account, please log in.' followed by 'User Name:' and 'Password:' labels, each with a corresponding text input field. Below these fields is a 'Login' button. At the bottom of the form, there is a link: 'Forgot your password? [Click here.](#)'. At the very bottom of the page, there are links for 'Terms of Use', 'Privacy Policy', and 'Contact Us', and a copyright notice: 'Copyright © 2004 WSC - all rights reserved.'

Figure 6-9: Member Login

Add a Guest

1. On the Wireless Guard Member Website home screen, Figure 6-10, click the **Network Admin** tab.



Figure 6-10: Home

2. The screen in Figure 6-11 will appear. Under Network Administration, click **Modify Access Control**.

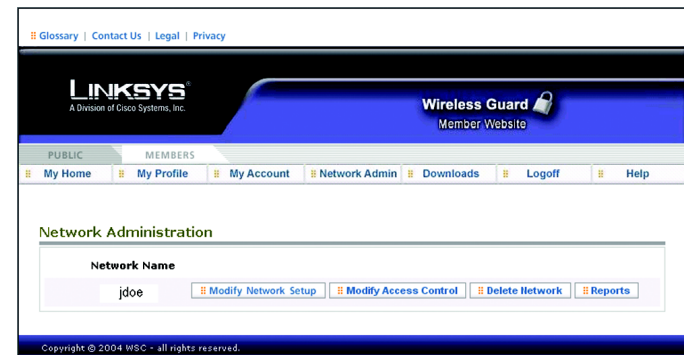


Figure 6-11: Network Administration

3. The screen in Figure 6-12 will appear. Under *Guests*, click **Add Guest**.

The screenshot shows the 'Modify Access Control' page for a network named 'wsc'. It features a table for 'Members' with columns: Full Name, User Name, Access Beginning, Duration, Status, and Last Access. One member, John (jdoe), is listed with an access beginning of 04/13/04 17:24 PDT, a 10-year duration, and an active status. There are 'Modify' and 'Remove' buttons for this member. Below the members table is a section for 'Guests' with an 'Add Guest' button. The page also includes a navigation bar with links like 'My Home', 'My Profile', 'My Account', 'Network Admin', 'Downloads', 'Logoff', and 'Help'.

Figure 6-12: Modify Access Control

4. The screen in Figure 6-13 will appear. Enter the Guest User Name, Guest First Name, Guest Last Name, Password, Password Verify, Access Duration, then click **Submit**.

Guest User Name. Enter a user name of the guest you want to add.

Guest First Name. The first name of the guest you want to add.

Guest Last Name. The last name of the guest you want to add.

Password. Enter a password that's at least six characters for the guest you want to add.

Password Verify. Enter the password again.

Access Duration. Enter the length of time that the guest will be on the network in hours.

The screenshot shows the 'Add Guest' page for a network named 'wsc'. It contains several input fields: 'Guest User Name', 'Guest First Name', 'Guest Last Name', 'Password' (with a note '(6 characters min.)'), 'Password Verify', and 'Access Duration' (with a dropdown menu showing '1' and 'Hour'). There are 'Submit' and 'Cancel' buttons at the bottom. The page also includes the same navigation bar as Figure 6-12.

Figure 6-13: Add Guest

5. The guest will need to install the Linksys Wireless Guard Client software on his PC. The software can be downloaded from the Setup CD-ROM or from Linksys.com/support. Refer to *Client Software Installation* at the beginning of this chapter.

Add a Member

To add a member, follow instructions for Add a Guest, steps 1 through 3 above, except in step 3, click **Add Member**.

The screen in Figure 6-14 will appear. Registered members can enter their Email address in the field and select the duration for access from the drop-down menu. If you want this network member to have the authority to put the network into Fallback Mode in case network security is lost, select **Permission to Initiate Network Fallback**. When finished, click **Submit**.

To register as a member for Linksys Wireless Guard, refer to the following instructions, then when finished with registration, return to this screen.

The member will need to install the Linksys Wireless Guard Client software on his PC. The software can be downloaded from the Setup CD-ROM or from Linksys.com/support. Refer to *Client Software Installation* at the beginning of this chapter.

Member Registration

1. Right-click on the green Wireless Guard Network key icon, then click **Register Member**.
2. The Welcome screen will appear. Click **Next**.

The screenshot shows the 'Add Member' page of the Linksys Wireless Guard Member Website. The page has a blue header with the Linksys logo and 'Wireless Guard Member Website'. A navigation bar includes links for PUBLIC and MEMBERS, with sub-links like My Home, My Profile, My Account, Network Admin, Downloads, Logoff, and Help. The main content area is titled 'Add Member' and shows the network name 'wsc'. There is a text input field for 'Member Email Address', a dropdown menu for 'Access Duration' set to '1 Hour', and a checkbox for 'Permission to Initiate Network Fallback'. At the bottom are 'Submit' and 'Cancel' buttons. A footer note says 'Copyright © 2004 WSC - all rights reserved.'

Figure 6-14: Add Member

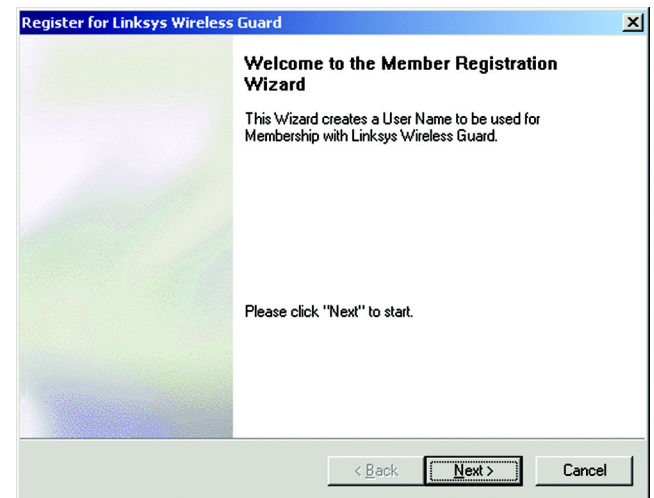
The screenshot shows a 'Welcome to the Member Registration Wizard' window. The title bar says 'Register for Linksys Wireless Guard'. The text inside says 'Welcome to the Member Registration Wizard' and 'This Wizard creates a User Name to be used for Membership with Linksys Wireless Guard.' Below this, it says 'Please click "Next" to start.' At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a dashed border.

Figure 6-15: Welcome

3. When the *Enter subscriber information* screen appears, enter the first and last names, the phone number, if desired, then the E-mail address of the new member. Click **Next**.

Click **Back** to return to the previous screen. Click **Cancel** to cancel the member registration.

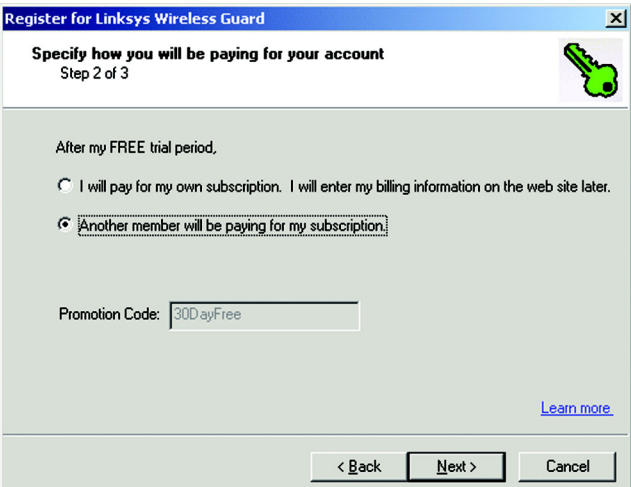


The screenshot shows a web browser window titled "Register for Linksys Wireless Guard". The main heading is "Enter subscriber information" with the subtitle "Step 1 of 3". A green key icon is in the top right corner. Below the heading are four text input fields: "First Name:", "Last Name:", "Phone (optional):", and "Email Address:". Below these fields is a paragraph of text: "Linksys Wireless Guard uses your email address to provide you with status messages regarding your Wireless Guard account. To receive valuable offers from Linksys Wireless Guard and its partners, uncheck the checkbox below." Below this text is a checkbox labeled "Do not send me any promotional email." which is currently checked. A link for "Privacy Policy" is located at the bottom right. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Figure 6-16: Subscriber Information

4. When the next screen appears, choose who will be paying for the account. If the new member will be paying for the account, click **I will pay for my own subscription. I will enter my billing information on the web site later**. If the administrator will be paying for the account, click **Another member will be paying for my subscription**. Click **Next**.

Click **Back** to return to the previous screen. Click **Cancel** to cancel the member registration.



The screenshot shows a web browser window titled "Register for Linksys Wireless Guard". The main heading is "Specify how you will be paying for your account" with the subtitle "Step 2 of 3". A green key icon is in the top right corner. Below the heading is the text "After my FREE trial period," followed by two radio button options: "I will pay for my own subscription. I will enter my billing information on the web site later." and "Another member will be paying for my subscription." The second option is selected. Below these options is a text input field for "Promotion Code:" containing the text "30DayFree". A link for "Learn more" is located at the bottom right. At the bottom of the window are three buttons: "< Back", "Next >", and "Cancel".

Figure 6-17: Account Finances

Wireless-G Access Point

5. When this screen appears, enter the information you will be using with the account. Enter a user name, password, then the password again. Also select a security question and answer in case you forget your password in the future. Click **Next** to continue.

Click **Back** to return to the previous screen. Click **Cancel** to cancel the member registration.

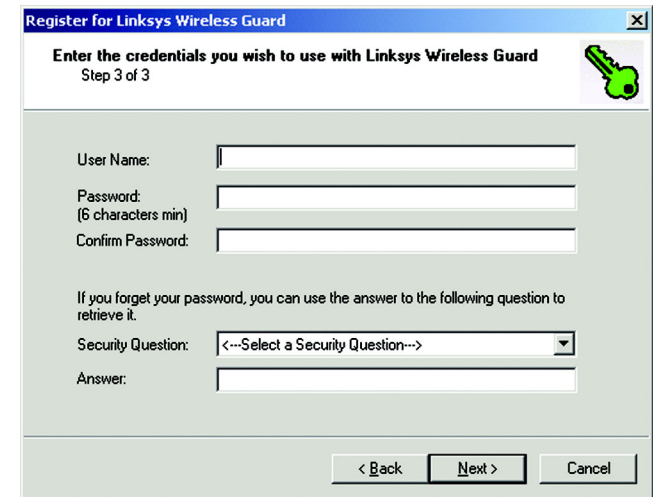


Figure 6-18: Credentials Information

6. When the congratulations screen appears you will be successfully registered for Linksys Wireless Guard. Click **Finish**.
7. You should now ask the administrator to add you to his Wireless Guard Protected Network's Access Control List. To do so, The network administrator needs to return to the *Add Member* screen in Figure 6-14, above.

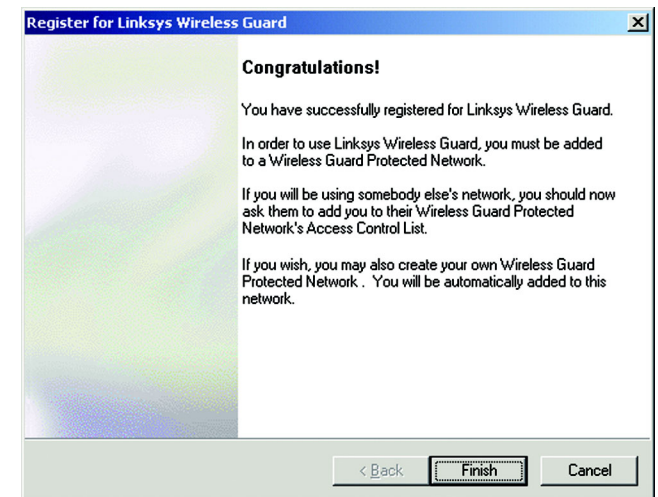


Figure 6-19: Congratulations

Securing or Unprotecting your Wireless Guard Network

There may be some instances where you would want to completely unprotect your network connection so it is not using the Wireless Guard security. For example, if you take your laptop to another location to give a presentation, and connect to a network that is running 802.1x security, the Linksys Wireless Guard software on your laptop will prevent you from logging in to another network. You will need to manually unprotect your network connection so you can log in. When you come back to your own network, you won't have to manually re-secure the network connection. Linksys Wireless Guard will recognize it and automatically reinstate security.

To unprotect a network

Right-click on the green Wireless Guard Network key icon on the right-side of the system tray at the bottom of your screen. Select **Unprotect this Network Connection** from the menu.

When the screen asks if you're sure you want to unprotect the network, click **Yes**.

To secure an unprotected network

Right-click on the green Wireless Guard Network key icon. Select **Secure this Network Connection** from the menu.

When the screen asks if you're sure you want to secure the network. Click **Yes**.

For more detailed information on your account and the website, click on your computer's **Start** button, select the **Linksys Wireless Guard** folder, then click **Linksys Wireless Guard Help**.

Chapter 7: 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 configure the Access Point in this manner.

For your convenience, use the Access Point's Web-based Utility to administer it. This chapter will explain all of the functions in this Utility. The Utility can be accessed via Microsoft Internet Explorer or Netscape Navigator through use of a computer connected with an Ethernet cable to the Access Point.

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

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

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, Status, Advanced, and Help. Additional screens will be available from the main tabs.

Setup

- *Basic Setup.* Enter the Internet connection and network settings on this screen.
- *Password.* Change the Access Point's Password and change its settings back to their defaults from this screen.
- *AP Mode.* From this screen, you can configure how the Access Point will work with other access points in your network.
- *Log.* You can view or save, even email, activity logs from this screen.

firmware: the programming code that runs a networking device

Status

- This screen will display current information on the Access Point, its settings, and its performance.

Advanced

- *Filters.* From this screen, you can allow or prevent access to your network.
- *Advanced Wireless.* From this screen, you can configure the Access Point's more advanced wireless settings.
- *SNMP.* This screen allows you to customize the Simple Network Management Protocol (SNMP) settings.

snmp: the standard e-mail protocol on the Internet

Help

- For help on the various tabs in this Web-based Utility, go to this screen.

Accessing the Utility

To access the Web-based Utility of the Access Point, launch Internet Explorer or Netscape Navigator, and enter the Access Point's default IP address, **192.168.1.245**, in the *Address* field. Press the **Enter** key.

Open your web browser and type the IP Address you entered in the Setup Wizard. (The default IP address is 192.168.1.245.) (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 and the following screen will appear. Leave the User Name field blank. The first time you open the Web-Based Utility, use the default password **admin**. You can set a new password from the Password tab.

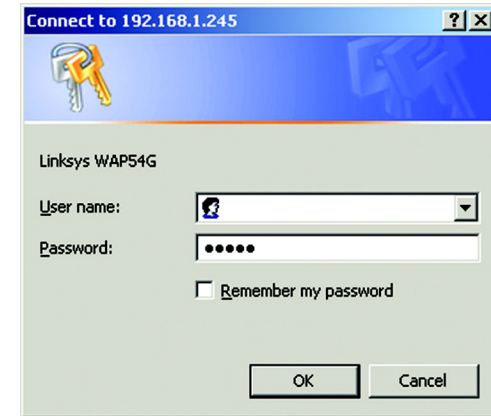


Figure 7-1: Password Screen

static ip address: a fixed address assigned to a computer or device connected to a network

The Setup Tab

Basic Setup

The first screen that appears displays the *Basic Setup* screen. This allows you to change the Access Point's general settings. Change these settings as described here and click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. If you require online help, click **Help**.

- **Firmware.** This will display the Access Point's current firmware version. Firmware can be upgraded from the Help tab.
- **AP Name.** You may assign any name to the Access Point. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. Verify this is the name you wish to use and click **Save Settings** to set it.

LAN

The selections under this heading allow you to configure the Access Point's connection to your Ethernet (wired) network.

- **Configuration Type.** Select **Static IP Address** if your ISP provided you with the IP Address, Subnet Mask, and Gateway address or select **Automatic Configuration - DHCP** if your ISP assigns IP addresses via a DHCP server.

The following fields apply **ONLY** when the Static IP Address option is selected:

- **IP Address.** The IP address must be unique to your network. We suggest you use the default IP address of 192.168.1.245. This is a private IP address, so there is no need to purchase a separate IP address from your service provider.
- **Subnet Mask.** The Subnet Mask must be the same as that set on your Ethernet network.
- **Gateway.** If you have assigned a static IP address to the Access Point, then enter the IP address of your network's Gateway, such as a router, in the Gateway field. If your network does not have a Gateway, then leave this field blank.

The screenshot shows the Linksys Basic Setup interface. The top navigation bar includes 'Setup', 'Status', 'Advanced', and 'Help'. The 'Setup' tab is active, with sub-tabs for 'Basic Setup', 'Password', 'AP Mode', and 'Log'. The 'Firmware Version' is v2.06, Dec 09, 2003. The 'AP Name' is Linksys WAP54G. Under the 'LAN' section, 'Configuration Type' is set to 'Static IP Address'. The 'IP Address' is 192.168.1.245, 'Subnet Mask' is 255.255.255.0, and 'Gateway' is 192.168.1.1. Under the 'Wireless' section, 'Mode' is 'Mixed', 'SSID' is 'Linksys', 'Channel' is '6', and 'Wireless Security' is 'Disable'. The 'Save Settings', 'Cancel Changes', and 'Help' buttons are at the bottom.

Figure 7-2: The Basic Setup Screen

firmware: programming code that runs a networking device

dhcp: 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.

isp (internet service provider): a company that provides access to the Internet

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

subnet mask: an address code that determines the size of the network

Wireless

The selections under this heading allow you to configure the Access Point's connection to your wireless network.

- **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.
- **SSID.** The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network. For added security, you should change the SSID from the default name, **linksys**, to a unique name.
- **SSID Broadcast.** Allows the SSID to be broadcast on your network. 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 network. Click **Enable** to broadcast the SSID to all wireless devices in range. Click **Disable** to increase network security and prevent the SSID from being seen on networked PCs.
- **Channel.** Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11. All points in your wireless network must use the same channel in order to function correctly.
- **Wireless Security.** To enable wireless security, through WPA or WEP encryption, select the **Enable** radio button. To disable such security, select the radio button by **Disable**. To change the security settings for your network, click the **Edit Security Settings** button. A notification window will ask if you wish to change the settings. Click **OK** to continue or **Cancel** to return to the *Basic Setup* tab.

software: instructions for the computer

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

wep: a method of encrypting network data transmitted on a wireless network for greater security

Wireless Security Settings

The Wireless Security settings configure the security of your wireless network. There are four wireless security mode options supported by the Access Point: WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These four are briefly discussed here. For detailed instructions on configuring wireless security for the Access Point, turn to “Appendix B: Wireless Security.”

WPA Pre-Shared Key. WPA gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. Enter a WPA Shared Key of 8-32 characters. Then enter a Group Key Renewal period, which instructs the Access Point how often it should change the encryption keys.

WPA RADIUS. 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.) First, select the type of WPA algorithm you want to use, **TKIP** or **AES**. Enter the RADIUS server’s IP Address and port number, along with a key shared between the Access Point and the server. Last, enter a Key Renewal Timeout, which instructs the Access Point how often it should change the encryption keys.

If you want to get the security of WPA RADIUS, but without having to build your own RADIUS network, Linksys offers Linksys Wireless Guard, a subscription service. For more information, click **CLICK HERE**.

***tkip:** a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted*

Figure 7-3: WPA Pre-Shared Key Settings

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

Figure 7-4: WPA Radius Settings

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.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the Access Point and the server. Then, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Last, either generate a WEP key using the Passphrase or enter the WEP key manually.

The screenshot shows the 'Radius' configuration page. At the top, a blue banner states: 'The Access Point supports 4 different types of security modes. WEP, WPA Pre-Shared Key, RADIUS, and WPA RADIUS. An easy way to utilize the maximum security of WPA Radius is to sign up for the Linksys Wireless Guard service. To learn more, [CLICK HERE](#).' Below this, the 'Radius' tab is selected. The form includes fields for 'Security Mode' (set to RADIUS), 'Radius Server Address' (0.0.0.0), 'RADIUS Port' (1812), and 'Shared Key'. Below these are radio buttons for 'Default Transmit Key' (1, 2, 3, 4) and a 'WEP Encryption' dropdown (set to 64 bits 10 hex digits). There is a 'Passphrase' field with a 'Generate' button, and four 'Key' fields (Key 1 through Key 4). At the bottom are 'Save Settings', 'Cancel Changes', and 'Help' buttons.

Figure 7-5: Radius Settings

***passphrase:** used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products*

WEP. WEP is a basic encryption method, which is not as secure as WPA. To use WEP, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. Then either generate a WEP key using the Passphrase or enter the WEP key manually.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. For help on any of these settings, click the **Help** button. For detailed instructions on configuring wireless security for the Access Point, turn to "Appendix B: Wireless Security."

The screenshot shows the 'WEP' configuration page. At the top, a blue banner states: 'The Access Point supports 4 different types of security modes. WEP, WPA Pre-Shared Key, RADIUS, and WPA RADIUS. An easy way to utilize the maximum security of WPA Radius is to sign up for the Linksys Wireless Guard service. To learn more, [CLICK HERE](#).' Below this, the 'WEP' tab is selected. The form includes fields for 'Security Mode' (set to WEP), 'Default Transmit Key' (radio buttons 1, 2, 3, 4), 'WEP Encryption' (dropdown set to 64 bits 10 hex digits), 'Passphrase' with a 'Generate' button, and four 'Key' fields (Key 1 through Key 4). At the bottom are 'Save Settings', 'Cancel Changes', and 'Help' buttons.

Figure 7-6: WEP Settings

Password

The Password screen allows you to change the Access Point's password and restore factory defaults.

Changing the sign-on password for the Access Point is as easy as typing the password into the AP Password field. Then, type it again into the second field to confirm.

To restore the Access Point's factory default settings, click the **Yes** button beside Restore Factory Defaults.

To back up your Access Point configuration, click the **Backup** button. To restore the backed-up configuration, click the **Restore** button.

Click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. If you require online help, click the **Help** button.

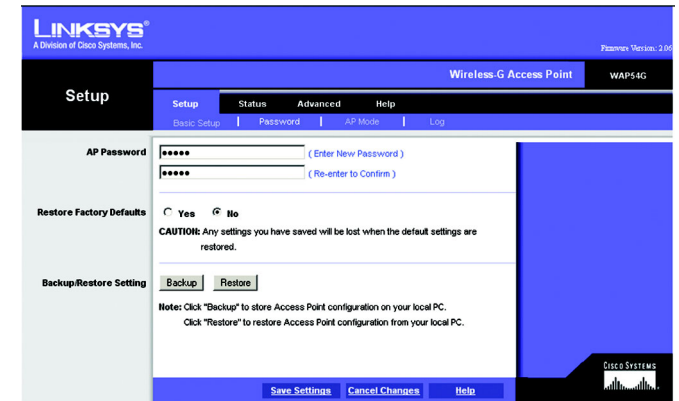


Figure 7-7: The Password Screen

AP Mode

LAN MAC Address

The Access Point offers five modes of operation: Access Point, AP (Access Point) Client, Wireless Repeater, and Wireless Bridge. For the bridging mode and Repeater mode, make sure the channel, SSID, and WEP keys are the same.

Access Point - The Operational 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 Access Point Client mode, the Access Point Client is able to talk to one remote access point within its range. This mode allows the Access Point Client to act as a client of a remote access point. The Access Point Client cannot communicate directly with any wireless clients. A separate network attached to the Access Point Client can then be wirelessly bridged to the remote access point. Enter the required LAN MAC address of the remote access point in the Remote AP MAC Address field.

To select an available access point, click the Site Survey button and choose from the access points listed by clicking on the radio button for the appropriate access point and clicking the close button. If you do not see an access point listed, click the Refresh button and another survey will be performed.



IMPORTANT: For all modes of operation EXCEPT Access Point, the remote access point must be a second Linksys Wireless Network Access Point. The Access Point will not communicate with any other kind of remote access point.

Figure 7-8: The AP Mode Screen

Figure 7-9: The Site Survey screen

Wireless Repeater - When set to Wireless Repeater mode, the Wireless Repeater is able to talk to one remote access point within its range and retransmit its signal. (This feature only works with Linksys WAP54G and WRT54G.)

To configure a Wireless Repeater environment, click **Wireless Repeater** and enter the LAN MAC address of the remote access point in the Remote AP MAC Address field.

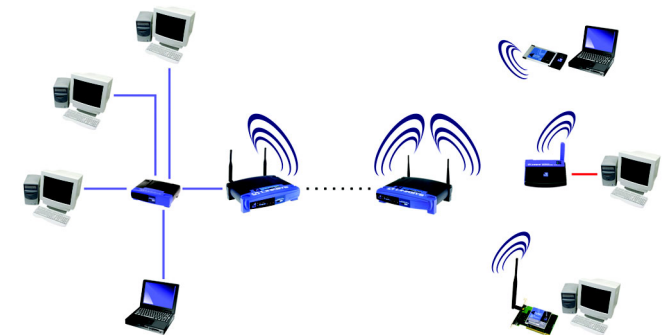


Figure 7-10: Wireless Repeater diagram

Wireless Bridge - If you are trying to make a wireless connection between two wired networks, select **Wireless Bridge**. This mode connects two physically separated wired networks with two access points.

To configure a Wireless Bridge environment, click **Wireless Bridge** and enter the LAN MAC address of the remote access point in the Remote Bridge MAC Address field. The remote access point also needs to be set up as a Wireless Bridge.

Click the **Save Changes** button to apply your changes or **Cancel Changes** to cancel your changes. If you require online help, click the **Help** button.



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.

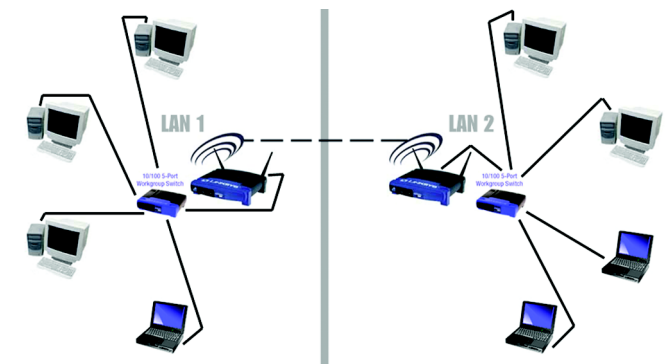


Figure 7-11: Wireless Bridge diagram



NOTE: All devices on each wired network must be connected through a hub or switch.

Log

To view a log of the Access Point's activity, select the **Log** tab.

To enable permanent logging activity, select **Enable**. The default setting for this function is **Disable**.

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 Send Log to field, 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.

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

Click the **Save Changes** button to apply your changes or **Cancel Changes** to cancel your changes. If you require online help, click the **Help** button.

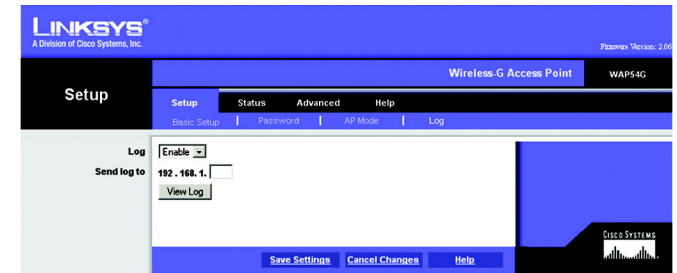


Figure 7-12: The Log screen

The Status Tab

The *Status* tab displays the Access Point’s current status.

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

AP Name. This is the Access Point name specified on the Basic Setup screen.

MAC Address. This is the Access Point’s MAC Address, as seen by your ISP.

Configuration Type. This displays how the Access Point is assigned an IP address, either **Automatic Configuration - DHCP**, if assigned by DHCP server, or **Static IP Address** and its IP Address and Subnet Mask, if assigned by Static IP Address server.

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

Subnet Mask. When the Access Point is using a Subnet Mask, it is shown here.

MAC Address. The MAC Address of the LAN interface is displayed here.

SSID. The unique name shared among all points in your wireless network is displayed here.

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

Channel. The wireless channel shared by all wireless devices connected to this Access Point is displayed here.

Wireless Security. The encryption method you chose in the Setup Wizard or changed from the Setup tab of this Web-based Utility is displayed here.

Send and Receive. The Send and Receive fields display the number of successful or dropped packets that have been sent or received. Some packet loss is normal in wireless networking.

To update the status information, click the **Refresh** button. If you require online help, click the **Help** button.

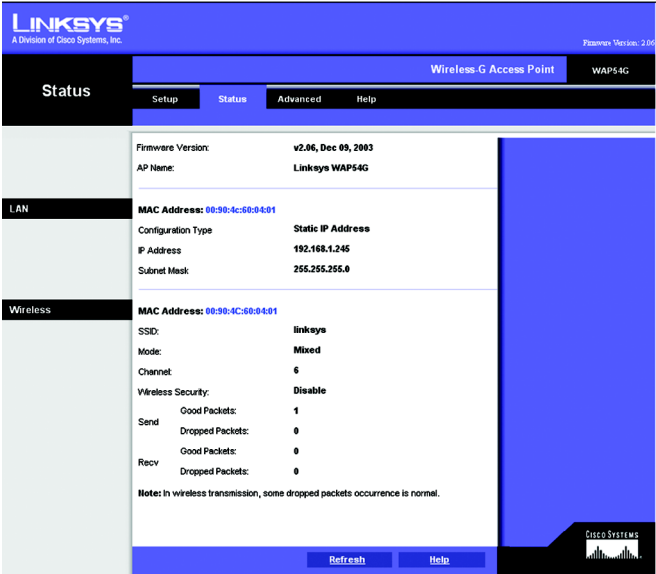


Figure 7-13: The Status Screen

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

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

The Advanced Tab

Filters

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

Wireless MAC Filter. To filter wireless users by MAC Address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC Address, select **Disable**.

Prevent. Clicking this button will block wireless access by MAC Address.

Permit Only. Clicking this button will allow wireless access by MAC Address.

Edit MAC Address Filter List. Clicking this button will open the MAC Address Filter List. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click the **Wireless Client MAC List** button to display a list of network users by MAC Address.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. If you require online help, click the **Help** button.

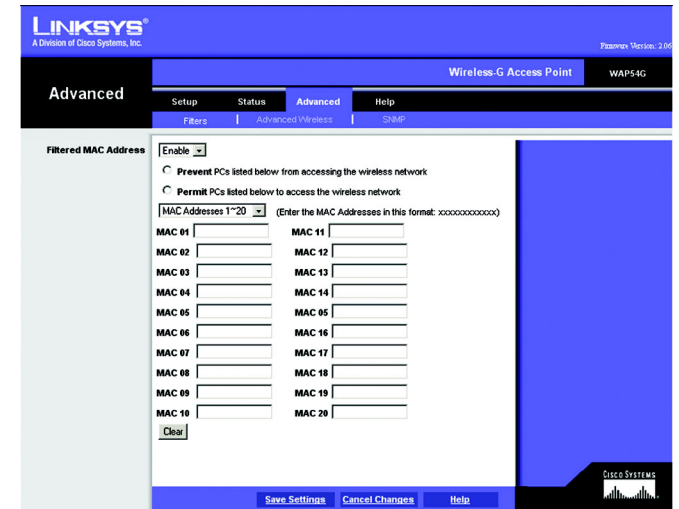


Figure 7-14: The Filters Screen

Advanced Wireless

Before making any changes to the Wireless tab, please check your wireless settings on other systems, as these changes will alter the effectiveness of the Access Point. In most cases, these settings do not need to be changed.

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

Transmission Rates. The default setting is **Auto**. 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, 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.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the Access Point in an environment with heavy 802.11b traffic. This function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance.

Basic Rate. The Basic Rate setting is not actually one rate of transmission but a series of rates, advertising to the other wireless devices in your network at what 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 of rates to advertise are **1-2Mbps**, for use with older wireless technology, and **All**, when you wish to make all rates advertised. The Basic Rate is not the rate transmitted; that is the Transmission Rate.

Antenna Selection. This selection is for choosing which antenna transmits data, left or right. By default, the **Diversity** antenna selection, used to increase reception, is chosen.

Frame Burst. Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. If you are not sure how to use this option, keep the default, **Off**.

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 LAN service area, the AP address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

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 **2,346**. Should you encounter inconsistent data flow, only minor modifications are recommended.

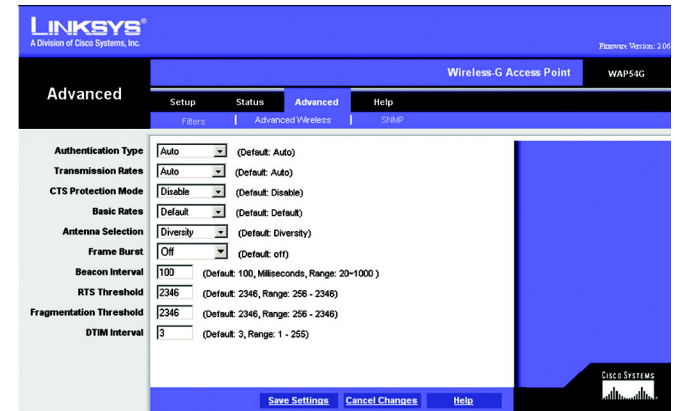


Figure 7-15: The Advanced Wireless screen

cts: a signal sent by a wireless device, signifying that it is ready to receive data.

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

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

Fragmentation Length. This specifies the maximum size a data packet will be before splitting and creating a new packet and should remain at its default setting of **2,346**. 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.

DTIM Interval. This value indicates how often the Access Point sends out a Delivery Traffic Indication Message. 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.

When you've completed making any changes on this tab, click the **Save Settings** button to save those changes or **Cancel Changes** to exit the Web-based Utility without saving changes. For more information on this tab, you can click the **Help** button.

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

dtim: a message included in data packets that can increase wireless efficiency

SNMP

The SNMP screen allows you to customize the Simple Network Management Protocol (SNMP) settings. SNMP is a popular network monitoring and management protocol.

The Identification settings let you designate the Contact, Device Name, and Location information for the Access Point. The SNMP Community settings allow names to be assigned to any SNMP communities that have been set up in the network. You can define two different SNMP communities, with the default names being Public and Private.

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

Identification. In the Contact field, enter contact information for the Access Point. In the Device Name field, enter the name of the Access Point. In the Location field, specify the area or location where the Access Point resides.

SNMP Community. You may change the name from its default, Public. Enter a new name in the Public field. Then configure the community's access as either Read-Only or Read-Write. You may change the name from its default, Private. Enter a new name in the Private field. Then configure the community's access as either Read-Only or Read-Write.

When you've completed making any changes on this tab, click the **Save Settings** button to save those changes or **Cancel Changes** to cancel your changes. For more information on this tab, you can click the **Help** button.

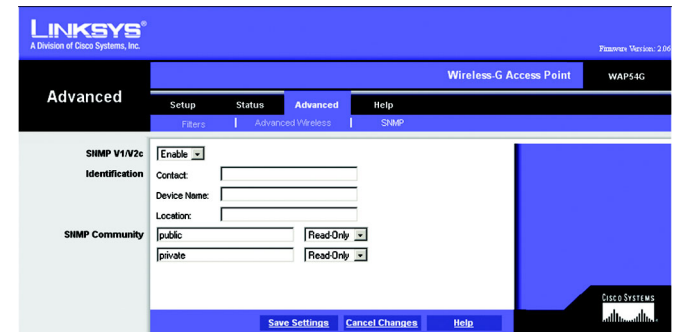


Figure 7-16: The SNMP screen

The Help Tab

For help on the various tabs in this Web-based Utility, along with upgrading the Access Point's firmware and viewing this User Guide, click the *Help* tab.

The help files for the various tabs in this Web-based Utility are listed by tab name on the lefthand side of the screen.

Click the *Linksys Website* link to connect to the Linksys homepage for Knowledgebase help files and information about other Linksys products, provided you have an active Internet connection.

For an Online manual in PDF format, click that text link. The User Guide will appear in Adobe pdf format. If you do not have the Adobe PDF Reader installed on your computer, click the **Adobe Website** link or go to the Setup Wizard CD-ROM to download this software. (To access the Adobe website, you will need an active Internet connection.) To download from the CD-ROM, click the **Start** button and select **Run**. Type **D:\Acrobat** (if "D" is the letter of your CD-ROM drive).

New firmware versions are posted at www.linksys.com and can be downloaded for free. If the Access Point is not experiencing difficulties, then there is no need to download a more recent firmware version, unless that version has a new feature that you want to use. Loading new firmware does not always enhance the speed or quality of your Internet connection.

To upgrade the Access Point's firmware:

1. Download the firmware upgrade file from the Linksys website.
2. Extract the firmware upgrade file.
3. Click the **Upgrade Firmware** button on the Help screen.
4. Enter the location of the firmware upgrade file in the File Path field, or click the **Browse** button to find the firmware upgrade file.
5. Double-click the firmware upgrade file.
6. Click the **Upgrade** button, and follow the on-screen instructions.

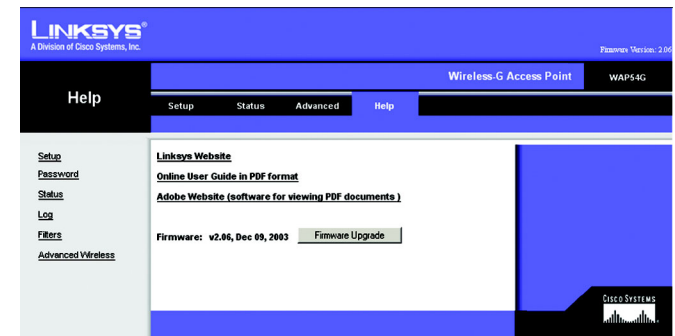


Figure 7-17: The Help screen

download: to receive a file transmitted over a network

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

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.

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 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 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 user to communicate continuously while moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number 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 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 the encryption function (WEP) 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, be 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, due to FCC regulations, more power may be transmitted, using 802.11a, on channels 52, 56, 60 and 64, than on the lower channels. Lastly, check the Advanced tab of the Web-Based Utility and make sure that FULL is selected in the Transmission Rate field.

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.

WEP is probably enabled on the Access Point, but not on your wireless adapter (or vice versa). Verify that the same WEP Keys and levels (64 or 128) are being used on all nodes on your wireless network.

What is the maximum number of users the Access Point facilitates?

No more than 65, but this depends on the volume of data and may be less if many users create a large amount of network traffic.

How many channels/frequencies are available with the Access Point?

Using 802.11b or draft 802.11g, there are eleven available channels, ranging from 1 to 11.

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.

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.



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.

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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



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.

Dual-Band Wireless Access Point

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

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

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

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

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

Appendix C: Upgrading Firmware

The Access Point's firmware is upgraded through the Web-Utility's Help tab. Follow these instructions:

1. Download the firmware from Linksys's website at www.linksys.com.
2. Click the Web-Utility's **Help** tab, and click the **Upgrade Firmware** button.
3. From the *Upgrade Firmware* screen, enter the location of the firmware's file or click the **Browse** button to find the file.
4. Then, click the **Upgrade** button to upgrade the firmware.



Figure C-1: Upgrade Firmware

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix E: Glossary

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

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

Adapter - This is 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.

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.

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

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

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

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

DHCP (Dynamic Host Configuration Protocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

Download - To receive a file transmitted over a network.

Wireless-G Access Point

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

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

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

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.

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

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

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

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

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

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

ISM band - Radio bandwidth utilized in wireless transmissions.

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

Router - A networking device that connects multiple networks together.

RTS (Request To Send) - A networking method of coordinating large packets through the RTS Threshold setting.

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

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

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

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

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

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

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

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

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

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

Wireless-G Access Point

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

Topology - The physical layout of a network.

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

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

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

Appendix F: Specifications

Standards	802.11g and 802.11b
Channels	802.11g 11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports/Buttons	One 10/100 RJ-45 Port, One Power Port, One Reset Button
Cabling Type	UTP CAT 5 or better
Data Rate	Up to 54Mbps
Transmit Power	15dBm
LEDs	Power, Act, Link
Dimensions (L x W x H)	7.31" x 1.88" x 6.88" (186 mm x 48 mm x 175 mm)
Antenna Height	4.5" (114 mm)
Unit Weight	15 oz. (0.42 kg)
Power	External, 12V DC
Certifications	FCC, Canada
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)

Wireless-G Access Point

Operating Humidity **10% to 85% Non-Condensing**

Storage Humidity **5% to 90% Non-Condensing**

Appendix G: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix H: Regulatory Information

FCC STATEMENT

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

Reorient or relocate the receiving antenna

Increase the separation between the equipment or devices

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that the Wireless-G ADSL Gateway conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

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

EN 609 50 Safety

Wireless-G Access Point

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

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

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

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

Linksys vakuuttaa täten että Wireless-G ADSL Gateway tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group déclare la Passerelle ADSL sans fil-G est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

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

France:

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

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

SAFETY NOTICES

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

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

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

Appendix I: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:

<http://www.linksys.com> or
<ftp.linksys.com>

Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:
Or fax your request in to:

800-546-5797 (LINKSYS)
949-823-3002

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

800-326-7114
support@linksys.com

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

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

949-823-3000