

# LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz **Wireless-G**  
802.11g

Access Point

User Guide

WIRELESS

Model No. **WAP54G v2**

CISCO SYSTEMS



## Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2003 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

<b>Chapter 1: Introduction</b>	<b>1</b>
Welcome	1
What's in this Guide?	2
<b>Chapter 2: Planning your Wireless Network</b>	<b>4</b>
Network Topology	4
Roaming	4
Network Layout	5
<b>Chapter 3: Getting to Know the Wireless-G Access Point</b>	<b>6</b>
The Back Panel	6
The Front Panel	7
<b>Chapter 4: Connecting the Wireless-G Access Point</b>	<b>8</b>
Hardware Installation	8
<b>Chapter 5: Setting Up the Wireless-G Access Point</b>	<b>11</b>
<b>Chapter 6: Configuring the Wireless-G Access Point</b>	<b>16</b>
Overview	16
Navigating the Utility	17
Accessing the Utility	18
The Setup Tab	19
The Status Tab	27
The Advanced Tab	28
The Help Tab	32
<b>Appendix A: Troubleshooting</b>	<b>33</b>
Frequently Asked Questions	33
<b>Appendix B: Wireless Security</b>	<b>37</b>
A Brief Overview	37
What Are The Risks?	37
Maximizing Wireless Security	39
<b>Appendix C: Upgrading Firmware</b>	<b>45</b>
<b>Appendix D: Windows Help</b>	<b>46</b>
<b>Appendix E: Glossary</b>	<b>47</b>
<b>Appendix F: Specifications</b>	<b>51</b>

<b>Appendix G: Warranty Information</b>	<b>53</b>
<b>Chapter H: Regulatory Information</b>	<b>54</b>
<b>Appendix I: Contact Information</b>	<b>57</b>

# 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	11
Figure 5-2: Connecting the Access Point	12
Figure 5-3: Select an Access Point	12
Figure 5-4: Enter the Password	13
Figure 5-5: The Configure Network Address Settings screen	13
Figure 5-6: The Wireless Settings screen	14
Figure 5-7: The Security Settings screen	14
Figure 5-8: The Confirmation screen	15
Figure 5-9: The Congratulations screen	15
Figure 6-1: Password Screen	18
Figure 6-2: The Basic Setup Screen	19
Figure 6-3: WPA Pre-Shared Key Settings	21
Figure 6-4: WPA Radius Settings	21
Figure 6-5: Radius Settings	22
Figure 6-6: WEP Settings	22
Figure 6-7: The Password Screen	23
Figure 6-8: The AP Mode Screen	24
Figure 6-9: The Site Survey screen	24
Figure 6-10: Wireless Repeater diagram	25
Figure 6-11: Wireless Bridge diagram	25
Figure 6-12: The Log screen	26
Figure 6-13: The Status Screen	27
Figure 6-14: The Filters Screen	28
Figure 6-15: The Advanced Wireless screen	29
Figure 6-16: The SNMP screen	31
Figure 6-17: The Help screen	32

<b>Figure B-1: The WEP Screen</b>	<b>43</b>
<b>Figure B-2: The WPA Pre-Shared Key Screen</b>	<b>44</b>
<b>Figure B-3: The WPA Radius Screen</b>	<b>44</b>
<b>Figure B-4: The Radius Screen</b>	<b>44</b>
<b>Figure C-1: Upgrade Firmware</b>	<b>45</b>

# 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.
- **Chapter 6: 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.
- **Appendix F: Specifications**  
This appendix provides the Access Point's technical specifications.



## Wireless-G Access Point

- **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](http://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](http://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

- |              |   |
|--------------|---|
| <b>Power</b> | Green. The <b>Power</b> LED lights up when the Access Point is powered on.  |
| <b>Act</b>   | Green. If the <b>Act</b> LED is flickering, the Access Point is actively sending or receiving data to or from one of the devices over the LAN port. |
| <b>Link</b>  | Green. The <b>Link</b> 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

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

- 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

- 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.

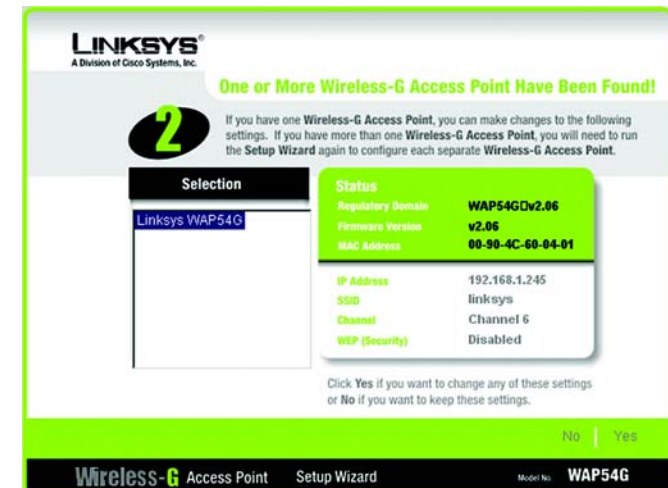


Figure 5-3: Select an Access Point



## Wireless-G Access Point

- 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.)

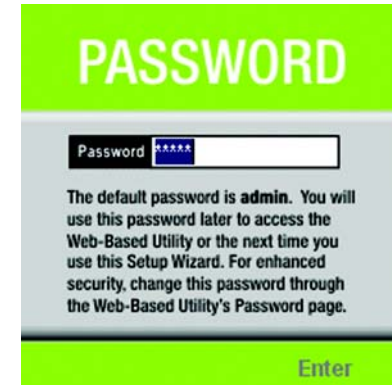


Figure 5-4: Enter the Password

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

- 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.

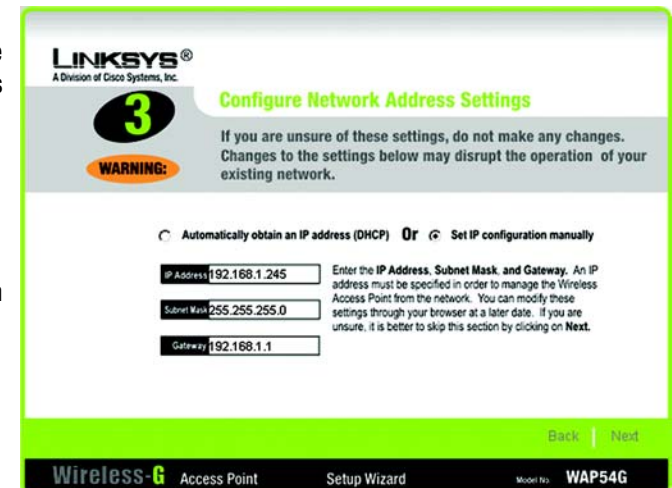


Figure 5-5: The Configure Network Address Settings screen

***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. Enter, also, 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.

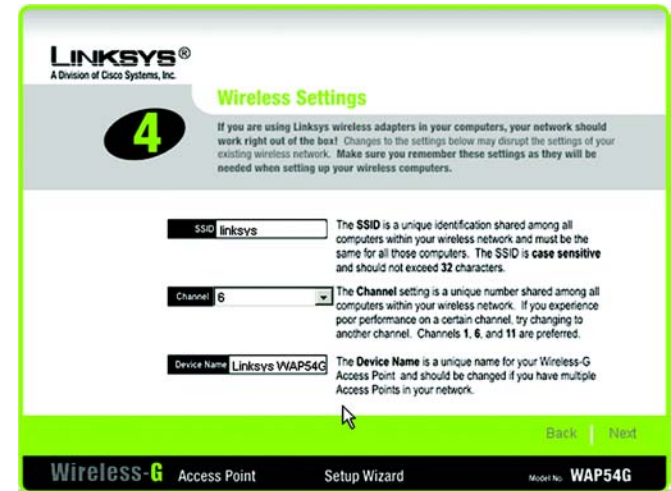


Figure 5-6: The Wireless Settings screen

*encryption: encoding data transmitted in a network*

8. The (optional) Security Settings screen will appear next. From this screen, you can set the level of encryption you desire for your network, along with selecting Passphrases and/or encryption keys.

With 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 WPA Shared Key of 8-32 characters.

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. All points in your wireless network must use the same WEP key to utilize WEP encryption.

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

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

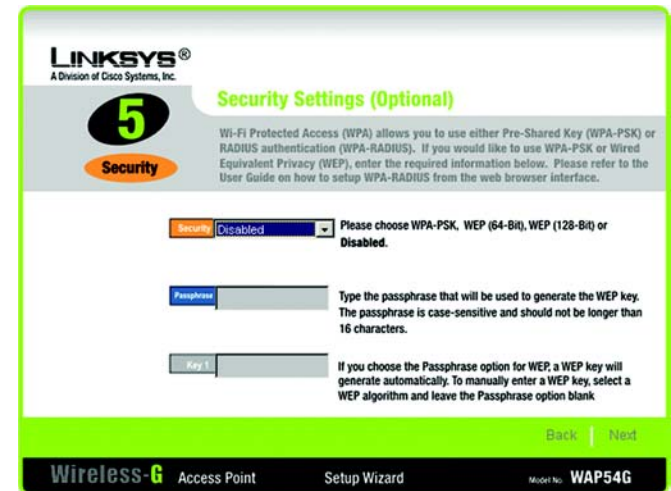


Figure 5-7: The Security Settings screen

*bit: a binary digit*

## Wireless-G Access Point

9. You should now review the settings you've chosen. If these settings are correct, click the **Yes** button to save these settings. If you wish to change any of the settings, click the **No** button. You will exit the Setup Wizard and can start it again to revise your settings.

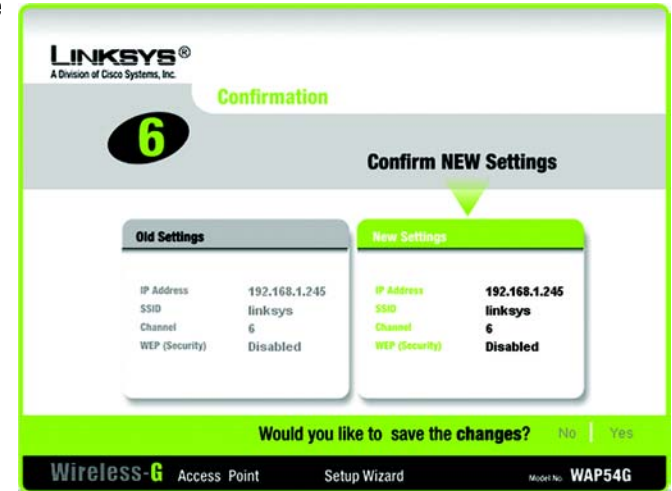


Figure 5-8: The Confirmation screen

10. 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.



Figure 5-9: The Congratulations screen

# Chapter 6: Configuring the Wireless-G Access Point

## Overview

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

### 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.

### Help

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

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

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

## 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 6-1: 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.



Figure 6-2: 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.

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

The screenshot shows the 'WPA Pre-Shared Key' configuration page. At the top, a blue header contains the text: 'The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.' Below this, the 'Security Mode' is set to 'WPA Pre-Shared Key'. The 'WPA Algorithm' is set to 'TKIP'. There is a text input field for the 'WPA Shared Key'. The 'Group Key Renewal' is set to '300 seconds'. At the bottom, there are three buttons: 'Save Settings', 'Cancel Changes', and 'Help'.

Figure 6-3: 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

The screenshot shows the 'WPA Radius' configuration page. At the top, a blue header contains the text: 'The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.' Below this, the 'Security Mode' is set to 'WPA RADIUS'. The 'WPA Algorithm' is set to 'TKIP'. The 'Radius Server Address' is set to '0 . 0 . 0 . 0'. The 'RADIUS Port' is set to '1812'. There is a text input field for the 'Shared Key'. The 'Key Renewal Timeout' is set to '300 seconds'. At the bottom, there are three buttons: 'Save Settings', 'Cancel Changes', and 'Help'.

Figure 6-4: WPA Radius Settings

## Wireless-G Access Point

**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 header contains the text: 'The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.' Below this, the 'Radius' tab is selected. The form includes the following fields and controls:

- Security Mode:** A dropdown menu set to 'RADIUS'.
- Radius Server Address:** A dotted IP address field with '0' in each segment.
- RADIUS Port:** A text input field containing '1812'.
- Shared Key:** A text input field.
- Default Transmit Key:** Radio buttons for keys 1, 2, 3, and 4, with key 1 selected.
- WEP Encryption:** A dropdown menu set to '64 bits 10 hex digits'.
- Passphrase:** A text input field with a 'Generate' button to its right.
- Key 1, Key 2, Key 3, Key 4:** Four text input fields for manual key entry.
- Buttons:** 'Save Settings', 'Cancel Changes', and 'Help' buttons at the bottom.

**Figure 6-5: 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 header contains the text: 'The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.' Below this, the 'WEP' tab is selected. The form includes the following fields and controls:

- Security Mode:** A dropdown menu set to 'WEP'.
- Default Transmit Key:** Radio buttons for keys 1, 2, 3, and 4, with key 1 selected.
- WEP Encryption:** A dropdown menu set to '64 bits 10 hex digits'.
- Passphrase:** A text input field with a 'Generate' button to its right.
- Key 1, Key 2, Key 3, Key 4:** Four text input fields for manual key entry.
- Buttons:** 'Save Settings', 'Cancel Changes', and 'Help' buttons at the bottom.

**Figure 6-6: 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 6-7: 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 6-8: The AP Mode Screen



Figure 6-9: The Site Survey screen

## Wireless-G Access Point

**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.

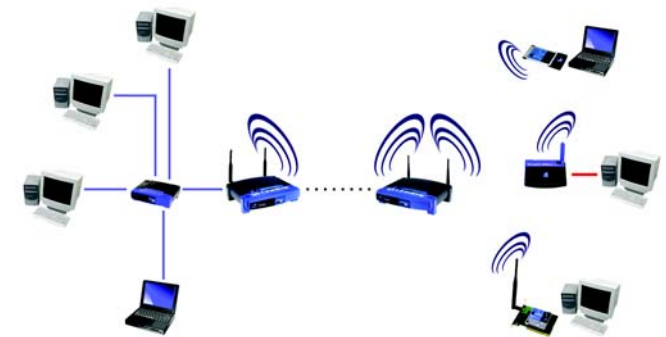


Figure 6-10: Wireless Repeater diagram

**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.

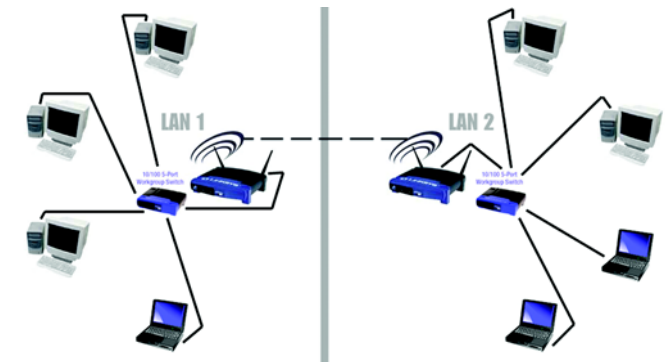


Figure 6-11: Wireless Bridge diagram



**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](http://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 6-12: 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.

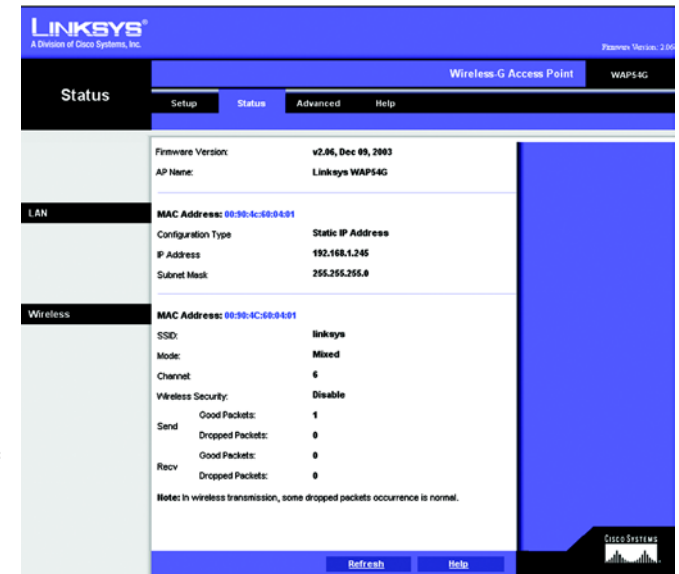


Figure 6-13: The Status Screen

**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.

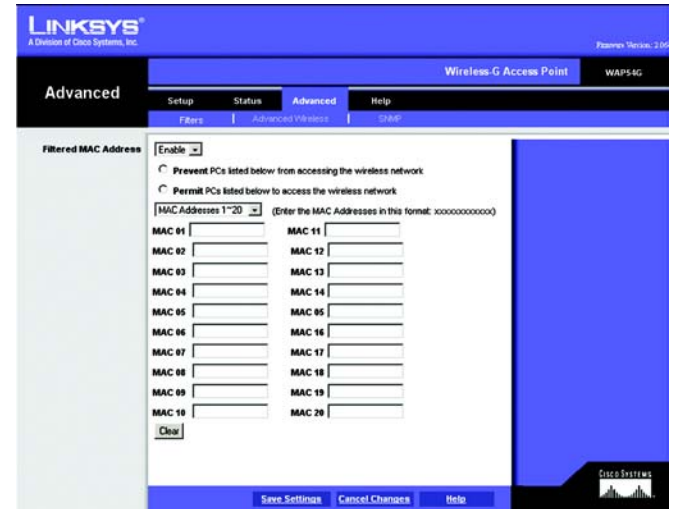


Figure 6-14: The Filters Screen



## 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.

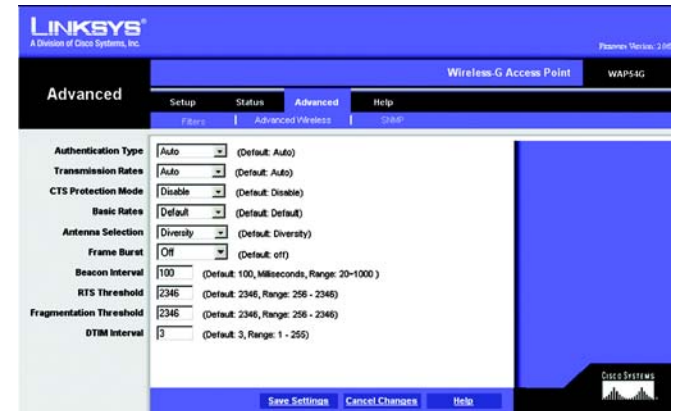


Figure 6-15: The Advanced Wireless screen

*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.*

## Wireless-G Access Point

**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 6-16: 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](http://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.

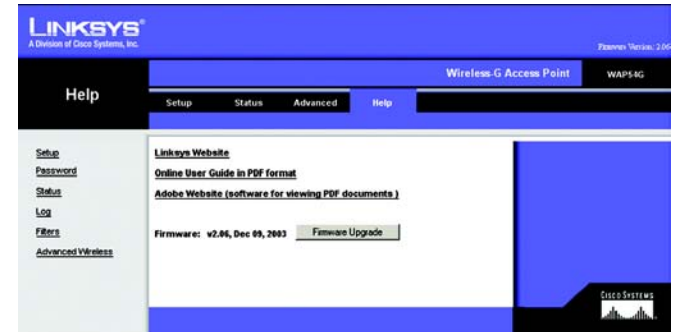


Figure 6-17: The Help screen

**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](http://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

## A Brief Overview

Whenever data - in the form of files, emails, or messages - is transmitted over your wireless network, it is open to attacks. Wireless networking is inherently risky because it broadcasts information on radio waves. Just like signals from your cellular or cordless phone can be intercepted, signals from your wireless network can also be compromised. What are the risks inherent in wireless networking? Read on.

## What Are The Risks?

Computer network hacking is nothing new. With the advent of wireless networking, hackers use methods both old and new to do everything from stealing your bandwidth to stealing your data. There are many ways this is done, some simple, some complex. As a wireless user, you should be aware of the many ways they do this.

Every time a wireless transmission is broadcast, signals are sent out from your wireless PC or access point, but not always directly to its destination. The receiving PC or access point can hear the signal because it is within that radius. Just as with a cordless phone, cellular phone, or any kind of radio device, anyone else within that radius, who has their device set to the same channel or bandwidth can also receive those transmission.

Wireless networks are easy to find. Hackers know that, in order to join a wireless network, your wireless PC will typically first listen for "beacon messages". These are identifying packets transmitted from the wireless network to announce its presence to wireless nodes looking to connect. These beacon frames are unencrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier) and the IP address of the network PC or access point. The SSID is analogous to the network's name. With this information broadcast to anyone within range, hackers are often provided with just the information they need to access that network.

One result of this, seen in many large cities and business districts, is called "Warchalking". This is the term used for hackers looking to access free bandwidth and free Internet access through your wireless network. The marks they chalk into the city streets are well documented in the Internet and communicate exactly where available wireless bandwidth is located for the taking.

Even keeping your network settings, such as the SSID and the channel, secret won't prevent a hacker from listening for those beacon messages and stealing that information. This is why most experts in wireless networking strongly recommend the use of WEP (Wired Equivalent Privacy). WEP encryption scrambles your wireless signals so they can only be recognized within your wireless network.

## Wireless-G Access Point

But even WEP has its problems. WEP's encryption algorithm is referred to as "simple", which also means "weak", because the technology that scrambles the wireless signal isn't too hard to crack for a persistent hacker.

There are five common ways that hackers can break into your network and steal your bandwidth as well as your data. The five attacks are popularly known as:

1. Passive Attacks
2. Jamming Attacks
3. Active Attacks
4. Dictionary-building or Table Attacks
5. Man-in-the-Middle Attacks

### Passive Attacks

There's no way to detect a passive attack because the hacker is not breaking into your network. He is simply listening (eavesdropping, if you will) to the information your network broadcasts. There are applications easily available on the Internet that can allow a person to listen into your wireless network and the information it broadcasts. Information such as MAC addresses, IP addresses, usernames, passwords, instant message conversations, emails, account information, and any data transmitted wirelessly, can easily be seen by someone outside of your network because it is often broadcast in clear text. Simply put, any information transmitted on a wireless network leaves both the network and individual users vulnerable to attack. All a hacker needs is a "packet sniffer", software available on the Internet, along with other freeware or shareware hacking utilities available on the Internet, to acquire your WEP keys and other network information to defeat security.

### Jamming Attacks

Jamming Attacks, when a powerful signal is sent directly into your wireless network, can effectively shut down your wireless network. This type of attack is not always intentional and can often come about simply due to the technology. This is especially possible in the 2.4 GHz frequency, where phones, baby monitors, and microwave ovens can create a great deal of interference and jam transmissions on your wireless network. One way to resolve this is by moving your wireless devices into the 5 GHz frequency, which is dedicated solely to information transmissions.



**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.

## Active Attacks

Hackers use Active Attacks for three purposes: 1) stealing data, 2) using your network, and 3) modifying your network so it's easier to hack in the next time.

In an Active Attack, the hacker has gained access to all of your network settings (SSID, WEP keys, etc.) and is in your network. Once in your wireless network, the hacker has access to all open resources and transmitted data on the network. In addition, if the wireless network's access point is connected to a switch, the hacker will also have access to data in the wired network.

Further, spammers can use your Internet connection and your ISP's mail server to send tens of thousands of e-mails from your network without your knowledge.

Lastly, the hacker could make hacking into your network even easier by changing or removing safeguards such as MAC address filters and WEP encryption. He can even steal passwords and user names for the next time he wants to hack in.

## Dictionary-Building or Table Attacks

Dictionary-building, or Table attacks, is a method of gaining network settings (SSID, WEP keys, etc.) by analyzing about a day's worth of network traffic, mostly in the case of business networks. Over time, the hacker can build up a table of network data and be able to decrypt all of your wireless transmissions. This type of attack is more effective with networks that transmit more data, such as businesses.

## Man-in-the-Middle Attacks

A hacker doesn't need to log into your network as a user - he can appear as one of the network's own access points, setting himself up as the man-in-the-middle. To do this, the hacker simply needs to rig an access point with your network's settings and send out a stronger signal than your access point. In this way, some of your network's PCs may associate with this rogue access point, not knowing the difference, and may begin sending data through it and to this hacker.

The trade-off for the convenience and flexibility wireless networking provides is the possibility of being hacked into through one of the methods described here. With wireless networks, even with WEP encryption, open to the persistent hacker, how can you protect your data? The following section will tell you how to do just that.

## Maximizing Wireless Security

Security experts will all tell you the same thing: Nothing is guaranteed. No technology is secure by itself. An unfortunate axiom is that building the better mousetrap can often create a better mouse. This is why, in the

## Wireless-G Access Point

examples below, your implementation and administration of network security measures is the key to maximizing wireless security.

No preventative measure will guarantee network security but it will make it more difficult for someone to hack into your network. Often, hackers are looking for an easy target. Making your network less attractive to hackers, by making it harder for them to get in, will make them look elsewhere.

How do you do this? Before discussing WEP and WPA, let's look at a few security measures often overlooked.

### A. Common Sense Solutions

#### 1) Network Content

Now that you know the risks assumed when networking wirelessly, you should view wireless networks as you would the Internet. Don't host any systems or provide access to data on a wireless network that you wouldn't put on the Internet.

#### 2) Network Layout

When you first lay out your network, keep in mind where your wireless PCs are going to be located and try to position your access point(s) towards the center of that network radius. Remember that access points transmit indiscriminately in a radius; placing an access point at the edge of the physical network area reduces network performance and leaves an opening for any hacker smart enough to discover where the access point is transmitting.

This is an invitation for a man-in-the-middle attack, as described in the previous section. To perform this type of attack, the hacker has to be physically close to your network. So, monitoring both your network and your property is important. Furthermore, if you are suspicious of unauthorized network traffic, most wireless products come with a log function, with which you can view activity on your network and verify if any unauthorized users have had access.

#### 3) Network Devices

With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. If they get into the hands of a hacker, so do all of your settings. So keep an eye on them.

#### 4) Administrator passwords

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.

## 5) SSID

There are a few things you can do to make your SSID more secure:

- a. Disable Broadcast
- b. Make it unique
- c. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. This is a option for convenience, allowing anyone to log into your wireless network. In this case, however, anyone includes hackers. So don't broadcast the SSID.

A default SSID is set on your wireless devices 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.

Changing your SSID regularly will force any hacker attempting to gain access to your wireless network to start looking for that new SSID.

With these three steps in mind, please remember that while SSIDs are good for segmenting networks, they fall short with regards to security. Hackers can usually find them quite easily.

## 6) MAC addresses

Enable MAC address filtering if your wireless products allow it. 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 using a random MAC address or spoofing (faking) a MAC address.

## 7) Firewalls

Once a hacker has broken into your wireless network, if it is connected to your wired network, they'll have access to that, too. This means that the hacker has effectively used your wireless network as a backdoor through your firewall, which you've put in place to protect your network from just this kind of attack via the Internet.

You can use the same firewall technology to protect your wired network from hackers coming in through your wireless network as you did for the Internet. Rather than connecting your access point to an unprotected switch, swap those out for a router with a built-in firewall. The router will show the access point coming in through its WAN port and its firewall will protect your network from any transmissions entering via your wireless network.

## Wireless-G Access Point

PCs unprotected by a firewall router should at least run firewall software, and all PCs should run up-to-date antiviral software.

### B. WEP

Wired Equivalent Privacy (WEP) is often looked upon as a panacea 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.

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

Programs exist on the Internet that are designed to defeat WEP. The best known of these is AirSnort. In about a day, AirSnort can analyze enough of the wireless transmissions to crack the WEP key. Just like a dictionary-building attack, the best prevention for these types of programs is by not using static settings, periodically changing WEP keys, SSID, etc.

There are several ways that WEP can be maximized:

- a) Use the highest level of encryption possible
- b) Use multiple WEP keys
- c) Change your WEP key regularly

Current encryption technology offers 64-bit and 128-bit WEP encryption. If you are using 64-bit WEP, swap out your old wireless units for 128-bit encryption right away. Where encryption is concerned, the bigger and more complex, the better. A WEP key is a string of hexadecimal characters that your wireless network uses in two ways. First, nodes in your wireless network are identified with a common WEP key. Second, these WEP keys encrypt and decrypt data sent over your wireless network. So, a higher level of security ensures that hackers will have a harder time breaking into your network.

Setting one, static WEP key on your wireless network leaves your network open the threats even as you think it is protecting you. While it is true that using a WEP key increases wireless security, you can increase it further by using multiple WEP keys.

Keep in mind that WEP keys are stored in the firmware of wireless cards and access points and can be used to hack into the network if a card or access point falls into the wrong hands. Also, should someone hack into your network, there would be nothing preventing someone access to the entire network, using just one static key.

## Wireless-G Access Point

The solution, then, is to segment your network up into multiple groups. If your network had 80 users and you used four WEP keys, a hacker would have access to only ¼ of your wireless network resources. In this way, multiple keys reduce your liability.

Finally, be sure to change your WEP key regularly, once a week or once a day. Using a "dynamic" WEP key, rather than one that is static, makes it even harder for a hacker to break into your network and steal your resources.

### WEP Encryption

WEP encryption for the Access Point is configured through the Web-Utility's Setup tab. Select **WEP** from the drop-down menu of Security Mode, which will open the WEP screen.

Select which WEP key (1-4) will be used when the Access Point sends data, then select that number as the Default Transmit Key. Make sure the receiving device is using the same key.

If you wish to use a WEP Passphrase, it can be a maximum of 16 alphanumeric characters. This passphrase may not work with non-Linksys products due to possible incompatibility with other vendors' passphrase generators. The WEP Key can be generated using your Passphrase or you can enter it manually.

If you wish to enter the WEP Key manually, type the key into the appropriate Key field on the left. The WEP key must 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. All points in your wireless network must use the same WEP key to utilize WEP encryption.

Once the Passphrase is entered, click the **Generate** key to generate a WEP key.

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

### C. WPA

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

WPA is accessed through the Web-Utility's Security Tab. Choose one of the following Security Modes from the drop-down menu:

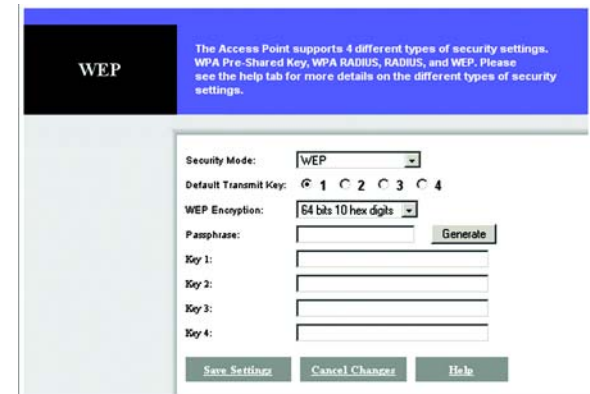


Figure B-1: The WEP Screen

### 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 8-32 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Access Point how often it should change the encryption keys.

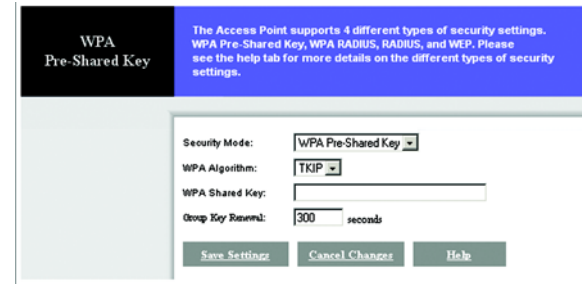


Figure B-2: The WPA Pre-Shared Key Screen

### WPA RADIUS

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

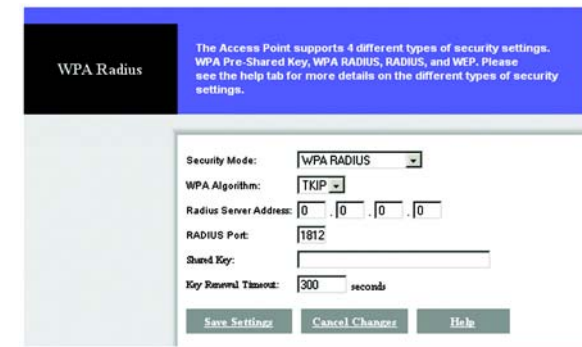


Figure B-3: The WPA Radius Screen

### RADIUS

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 WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

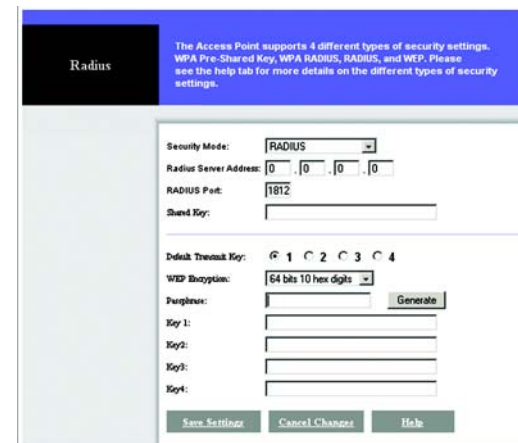


Figure B-4: The Radius Screen



# 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](http://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.

## Wireless-G Access Point

**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 soumis à autorisation préalable et très restreint.

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

## FCC PART 68 STATEMENT

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

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

## Wireless-G Access Point

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

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

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

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

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

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

## 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](ftp://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](mailto: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