

LINKSYS®

A Division of Cisco Systems, Inc.

Dual-Band
5GHz +

802.11a

2.4GHz

802.11g

Dual-Band
Wireless A+G
Access Point



User Guide

Model No. **WAP55AG**



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 © 2005 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 Dual-Band Wireless A + G Access Point has been designed to make understanding networking with the Access Point easier than ever. Look for the following items when reading this guide:



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



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



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

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

word: definition.

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

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the "List of Figures" section in the "Table of Contents".

Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this Guide?	2
Chapter 2: Planning your Wireless Network	4
Network Topology	4
Roaming	4
Network Layout	5
Chapter 3: Getting to Know the Dual-Band Wireless A + G Access Point	6
The Back Panel	6
The Front Panel	7
Chapter 4: Connecting the Dual-Band Wireless A + G Access Point	8
Hardware Installation	8
Chapter 5: Setting Up the Dual-Band Wireless A + G Access Point	9
Setup Wizard	9
Chapter 6: Configuring the Dual-Band Wireless A + G Access Point	17
Overview	17
Navigating the Utility	17
Accessing the Utility	19
The Setup Tab	19
The Wireless Tab	20
The Wireless Tab - Basic Wireless Settings	20
The Wireless Tab - Wireless Security	22
The Wireless Tab - Wireless MAC Filter	24
The Wireless Tab - Advanced Wireless Settings	25
The Administration Tab - Password	28
The Administration Tab - Log	28
The Administration Tab - Factory Defaults	29
The Administration Tab - Firmware Upgrade	29
The Status Tab - Local Network	30
The Status Tab - Wireless	31
Appendix A: Troubleshooting	32
Frequently Asked Questions	32

Appendix B: Wireless Security	36
Security Precautions	36
Security Threats Facing Wireless Networks	36
Appendix C: Upgrading Firmware	39
Appendix D: Windows Help	40
Appendix E: Glossary	41
Appendix F: Specifications	45
Appendix G: Warranty Information	46
Appendix H: Regulatory Information	47
Appendix I: Contact Information	49

List of Figures

Figure 3-1: The Access Point's Back Panel	6
Figure 3-2: Front Panel	7
Figure 5-1: The Setup Wizard's Welcome Screen	9
Figure 5-2: Connect to the Router	9
Figure 5-3: Connect to the Ethernet Port	10
Figure 5-4: Connect to the Power	10
Figure 5-5: Check the LEDs	10
Figure 5-6: Select the Access Point	11
Figure 5-7: Enter the Password	11
Figure 5-8: Basic Settings	12
Figure 5-9: Wireless-A Settings	12
Figure 5-10: Wireless-A Security - WEP	13
Figure 5-11: Wireless-A Security - PSK	13
Figure 5-12: Wireless-G Settings	14
Figure 5-13: Wireless-G Security - WEP	14
Figure 5-14: Wireless-G Security - PSK	15
Figure 5-15: Confirm New Settings	15
Figure 5-16: Congratulations	16
Figure 6-1: Automatic Configuration - DHCP	19
Figure 6-2: Static IP Address	19
Figure 6-3: Basic Wireless Settings	20
Figure 6-4: WEP	22
Figure 6-5: Pre-Shared Key	22
Figure 6-6: Pre-Shared Key + Radius	23
Figure 6-7: Wireless MAC Filter	24
Figure 6-8: Wireless Client List	24
Figure 6-9: Advanced Wireless	25
Figure 6-10: Password	28

Figure 6-11: Log	28
Figure 6-12: Factory Defaults	29
Figure 6-13: Firmware Upgrade	29
Figure 6-14: Status - Local Network	30
Figure 6-15: Status - Wireless Network	30
Figure C-1: Upgrade Firmware	39

Chapter 1: Introduction

Welcome

Thank you for choosing the Dual-Band Wireless A + 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 three wireless standards, 802.11a, 802.11b and 802.11g, 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

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

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

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

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 Dual-Band Wireless A + G Access Point.

- **Chapter 1: Introduction**
This chapter describes the Dual-Band Wireless A + 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 Dual-Band Wireless A + G Access Point**
This chapter describes the physical features of the Access Point.
- **Chapter 4: Connecting the Dual-Band Wireless A + G Access Point**
This chapter instructs you on how to connect the Access Point to your network.
- **Chapter 5: Setting Up the Dual-Band Wireless A + G Access Point**
This chapter explains how to use the Web-Based Utility to configure the settings on the Access Point and how to install the setup on the Access Point for the Linksys Wireless Guard.
- **Chapter 6: Configuring the Dual-Band Wireless A + 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 Dual-Band Wireless A + 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.

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

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

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

Chapter 3: Getting to Know the Dual-Band Wireless A + 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.

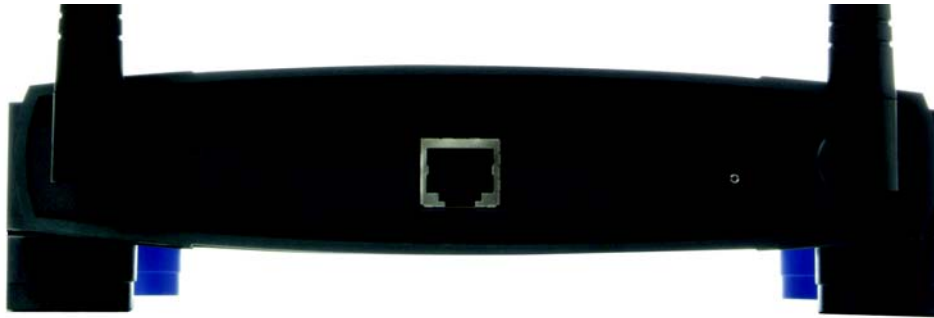


Figure 3-1: The Access Point's Back Panel

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

- | | |
|---------------------|---|
| Ethernet | The Ethernet 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 Administration tab in the Access Point's Web-Based Utility. |

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



Important: Resetting the Access Point will erase all of your settings (Wireless Security, 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.

The Front Panel

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



Figure 3-2: Front Panel

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

Wireless-A WLAN Green. When the **WLAN** LED is blinking, the Wireless-A network is operating.

Wireless-G WLAN Green. When the **WLAN** LED is blinking, the Wireless-G network is operating.

Ethernet Green. The **Ethernet** LED serves two purposes. If the LED is continuously lit, the Access Point is successfully connected to a device through the Ethernet port. If the LED is flickering, it is an indication of any network activity.

Chapter 4: Connecting the Dual-Band Wireless A + 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 wired Network.
4. Connect the AC Power Adapter to the Access Point's Power port and to an electrical outlet. 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 Dual-Band Wireless A + 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 Dual-Band Wireless A + G Access Point

Setup Wizard

This Setup Wizard will take you through all the steps necessary to set up and 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 **Click Here to Start** button to continue this Setup Wizard. Clicking the **User Guide** button opened this User Guide. To exit this Setup Wizard, click the **Exit** button.
3. The next screen shows how to start connecting the Access Point. Optimally, you should perform this setup through a PC on your wired network. Connect one end of the network cable to your network switch or router.

Click the **Next** button to continue or **Exit** to exit the Setup Wizard.



Note: The Access Point will be set up in the Setup Wizard through a wired network connection. You may refer to Chapter 4: Connecting the Dual-Band Wireless A + G Access Point.



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

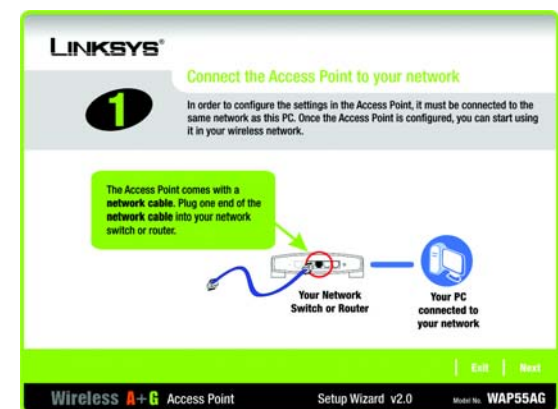


Figure 5-2: Connect to the Router

Dual-Band Wireless A + G Access Point

4. Connect the other end of the network cable to the Ethernet port on the back of the Access Point.

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

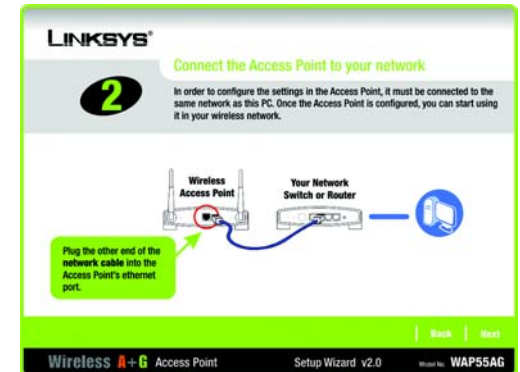


Figure 5-3: Connect to the Ethernet Port

5. Connect the power adapter to the Access Point's Power port. Then connect the other end to an electrical outlet. Only use the power adapter supplied with the Access Point. Use of a different adapter can cause product damage.



IMPORTANT: Make sure that you use the power adapter that is supplied with the Access Point. Use of a different power adapter could damage the Access Point.

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

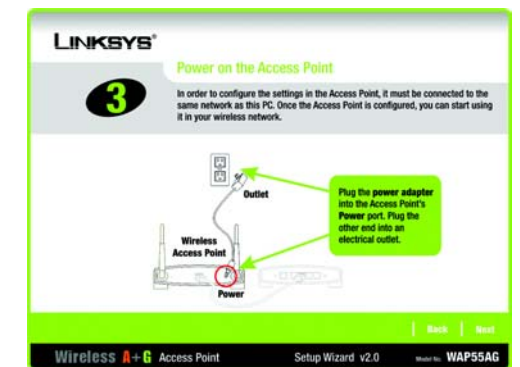


Figure 5-4: Connect to the Power

6. The Access Point's LEDs should be lit. If not, re-check the connections.

Click the **Next** button to continue or **Exit** to exit the Setup Wizard.

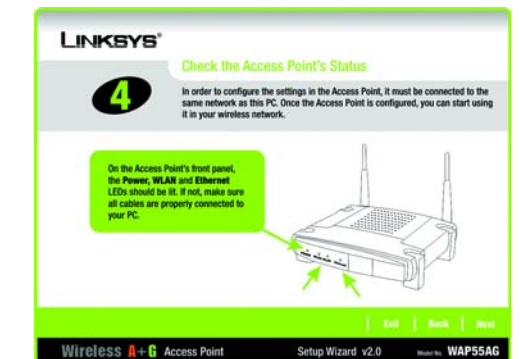


Figure 5-5: Check the LEDs

Dual-Band Wireless A + G Access Point

7. The Setup Wizard will run a search for the Access Point within your network and then display a list along with the status information for each access point. If there are more than one displayed, select the Access Point by clicking on it and click the **Next** button to continue, the Back button to return to a previous screen, or **Exit** to exit the Setup Wizard.



Figure 5-6: Select the Access Point

8. 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 **Enter** button. (This password can be changed on the next screen.)



Figure 5-7: Enter the Password

9. The Basic Settings screen will appear next. Enter the Device Name and new Password. Then, click the **Next** button to continue or **Back** to return to the previous page.

- **Device Name.** The Device Name is a unique name given to the Access Point to prevent confusion when using multiple Access Points.
- **Password.** Enter a new password that will be used to access the web-based utility or Setup Wizard.
- **Network.** Select **Automatically** if your network has a router or DHCP server. Select **Static IP** if your network requires a static IP address.
- **IP Address.** This IP address must be unique to your network. (The default IP address is 192.168.1.246) Leave the default IP address, unless you know your network's IP address is different.
- **Subnet Mask.** The Access Point's Subnet Mask must be the same as your Ethernet network. Leave the default Subnet Mask, unless you know your network's subnet mask is different.
- **Default Gateway.** This IP address should be the IP address of the gateway device that allows for contact between the Internet and the local network. Leave the default Default Gateway blank, unless you know your network's default gateway.

10. The Wireless-A Settings screen should now appear. Enter your wireless 802.11a network's SSID, select the channel at which the network broadcasts its wireless signal, and select the security. 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. All devices in your wireless network must broadcast on the same channel in order to communicate. If you want the Router to automatically scan for a clear channel, then select **Auto (DFS)**
- **SSID Broadcast.** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Access Point. To broadcast the Access Point's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Access Point's SSID, then select **Disabled**.
- **Security.** Two wireless security methods are available: WEP (Wired Equivalent Privacy) and PSK (Pre-Shared Key), which is the stronger security method. Select **WEP** or **PSK** from the drop-down menu. All devices in your wireless network must use the same security method.

Figure 5-8: Basic Settings

***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*

Figure 5-9: Wireless-A Settings

11. The next screen that appears will depend on your security selection. Make sure that the security mode is the same for all the devices on your network.

- WEP. From this screen, select the level of encryption, and enter a passphrase, which will generate the WEP key for you automatically, or you can enter the key manually.

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, 26 characters in length for 128-bit encryption, or 32 characters for 152-bit encryption.

Figure 5-10: Wireless-A Security - WEP

bit: a binary digit

encryption: encoding data transmitted in a network

- PSK (Pre-Shared Key) you have two encryption options, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. Enter a Passphrase of 8-32 characters.

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

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

Figure 5-11: Wireless-A Security - PSK

12. The Wireless-G Settings screen should now appear. Enter your wireless 802.11g network's SSID, select the channel at which the network broadcasts its wireless signal, and select the security. 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.
- **SSID Broadcast.** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Access Point. To broadcast the Access Point's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Access Point's SSID, then select **Disabled**.
- **Security.** Two wireless security methods are available: WEP (Wired Equivalent Privacy) and PSK (Pre-Shared Key), which is the stronger security method. Select **WEP** or **PSK** from the drop-down menu. All devices in your wireless network must use the same security method.

LINKSYS®

Wireless-G Settings

Make sure you write these settings down. They will be needed when setting up your wireless computers. **The wireless security settings must be the same on all devices on your wireless network, or they will not be able to communicate.**

8

SSID:

Channel:

SSID Broadcast:

Security:

2.4GHz
802.11g

[Back](#) [Next](#)

Wireless **A+G** Access Point Setup Wizard v2.0 Model No. **WAP55AG**

Figure 5-12: Wireless-G Settings

13. The next screen that appears will depend on your security selection. Make sure that the security mode is the same for all the devices on your network.

- **WEP.** From this screen, select the level of encryption, and enter a passphrase, which will generate the WEP key for you automatically, or you can enter the key manually.

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.

LINKSYS®

Wireless-G Security - WEP

Make sure you write these settings down. They will be needed when setting up your wireless computers. **The wireless security settings must be the same on all devices on your wireless network, or they will not be able to communicate.**

Security

Encryption:

Passphrase:

WEP Key 1:

2.4GHz
802.11g

[Back](#) [Next](#)

Wireless **A+G** Access Point Setup Wizard v2.0 Model No. **WAP55AG**

Figure 5-13: Wireless-G Security - WEP

Dual-Band Wireless A + G Access Point

- PSK (Pre-Shared Key) you have two encryption options, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. Enter a Passphrase of 8-32 characters.

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

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

LINKSYS® Wireless-G Security - PSK

Security Make sure you write these settings down. They will be needed when setting up your wireless computers. The wireless security settings must be the same on all devices on your wireless network, or they will not be able to communicate.

Encryption **TKIP** To utilize PSK encryption, select either TKIP or AES encryption.

Passphrase Enter the Passphrase that will be used by your wireless network. The Passphrase is case-sensitive and should be between 8 and 63 characters.

2.4GHz 802.11g

Back Next

Wireless A+G Access Point Setup Wizard v2.0 Model No. WAP55AG

Figure 5-14: Wireless-G Security - PSK

14. The Confirm New Settings screen will appear to allow you to check your settings. If you want to change a setting, click the **Back** button until you find the correct screen. If your settings are correct, click the **Save** button. If you want to cancel the installation, you may click **Exit**.

LINKSYS® Confirm New Settings

Confirm NEW Wireless Settings

Old Settings		New Settings	
Device Name	WAP55AG	Device Name	WAP55AG
IP Address	192.168.1.250	IP Address	192.168.1.250
Wireless-A		Wireless-A	
SSID	linksys-a	SSID	linksys-a
Channel	Auto (DFS)	Channel	Auto (DFS)
Security	Disabled	Security	Disabled
Wireless-G		Wireless-G	
SSID	linksys-g	SSID	linksys-g
Channel	6-2.437GHz	Channel	6-2.437GHz
Security	Disabled	Security	Disabled

Exit Back Save

Wireless A+G Access Point Setup Wizard v2.0 Model No. WAP55AG

Figure 5-15: Confirm New Settings

Dual-Band Wireless A + G Access Point

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

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

**For more advanced configuration, you can go to
Chapter 6: Configuring the Dual-Band Wireless A + G Access Point.**



Figure 5-16: Congratulations

Chapter 6: Configuring the Dual-Band Wireless A + G Access Point

Overview

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

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:

- **Setup**
On the *Network Setup* screen, you can configure your basic network settings.
- **Wireless**
on the Basic Wireless screen, you can configure the wireless settings.
- **Administration**
Click the **Administration** 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.

Navigating the Utility

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

Setup

- *Network Setup*. You can configure the Access Point's network settings on this screen.



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.*

Wireless

- *Basic Wireless Settings.* The selections under this heading allow you to configure the Access Point's connection of your Wireless-A (802.11a) and Wireless-G (802.11g) networks.
- *Wireless Security.* The Wireless Security settings configure the security of your wireless network.
- *Wireless MAC Filter.* Wireless access can be filtered by using the MAC addresses of the wireless devices.
- *Advanced Wireless Settings.* These are advanced wireless settings. In most cases, these settings do not need to be changed.

Administration

- *Password.* The Password screen allows you to change the Access Point's password.
- *Log.* The Access Point can keep logs of wireless activity.
- *Factory Defaults.* This screen allows you to restore the Access Point's configuration to its factory default settings.
- *Firmware Upgrade.* This screen allows you to upgrade the Access Point's firmware. Do not upgrade the firmware unless you are experiencing problems with the Access Point or the new firmware has a feature you want to use.

Status

- *Local Network.* The Status tab displays the current status of the Access Point's local network.
- *Wireless.* The Wireless screen on the Status Tab displays the status of your Wireless-A and/or Wireless-G networks.

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, **192.168.1.246**, in the *Address* field. Press the **Enter** key. 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.

The Setup Tab

Network Setup

The *Network Setup* screen, the first screen, allows you to change the Access Point's general settings.

- **Device Name.** The Device Name is a unique name given to the Access Point to prevent confusion when using multiple Access Points.
- **Configuration Type.** Select **Automatic Configuration - DHCP** if your network has a router or DHCP server. Select **Static IP Address** if your network requires a static IP address.
- **IP Address.** This IP address must be unique to your network. (The default IP address is 192.168.1.246) Leave the default IP address, unless you know your network's IP address is different.
- **Subnet Mask.** The Access Point's Subnet Mask must be the same as your Ethernet network. Leave the default Subnet Mask, unless you know your network's subnet mask is different.
- **Default Gateway.** This IP address should be the IP address of the gateway device that allows for contact between the Internet and the local network. Leave the default Default Gateway blank, unless you know your network's default gateway.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.



NOTE: If you don't remember the Access Point's IP address, you can run the Setup Wizard to locate it.

The screenshot shows the 'Network Setup' page of the Linksys WAP55AG web utility. The 'Device Name' field contains 'WAP55AG'. The 'Configuration Type' dropdown is set to 'Automatic Configuration - DHCP'. The IP Address is 192.168.1.249, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.1.1. A 'More...' link is on the right. Buttons for 'Save Settings' and 'Cancel Changes' are at the bottom.

Figure 6-1: Automatic Configuration - DHCP

The screenshot shows the 'Network Setup' page with 'Configuration Type' set to 'Static IP'. The IP Address, Subnet Mask, and Default Gateway are each shown as a four-part numeric field. The 'More...' link and 'Save Settings'/'Cancel Changes' buttons are also visible.

Figure 6-2: Static IP Address

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

The Wireless Tab

The Wireless Tab - Basic Wireless Settings

The selections under this heading allow you to configure the Access Point's connection to your Wireless-A (802.11a) and Wireless-G (802.11g) networks.

Wireless-A

- **Mode.** To enable Wireless-A (802.11a) networking, select **Enabled**. Otherwise, select **Disabled**.
- **Turbo Mode.** Using this mode enables high-speed connections but severely limits range. To function, Turbo Mode must be enabled on both the Access Point and wireless PCs. To increase the speed, select **Enabled**. (Keep in mind that the Access Point's range diminishes in Turbo Mode.) If you do not want to use Turbo Mode, select **Disabled**.
- **Network Name (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. All devices in your wireless network must broadcast on the same channel in order to communicate. If you want the Router to automatically scan for a clear channel, then select **Auto (DFS)**.
- **SSID Broadcast.** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Access Point. To broadcast the Access Point's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Access Point's SSID, then select **Disabled**.



Figure 6-3: Basic Wireless Settings

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.

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-G

- **Mode.** From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, **Mixed**. If you have only 802.11g devices, select **Wireless-G Only**. If you have only 802.11b devices, select **Wireless-B Only**. If you do not have any 802.11g and 802.11b devices in your network, select **Disabled**.
- **Network Name (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.
- **SSID Broadcast.** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Access Point. To broadcast the Access Point's SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Access Point's SSID, then select **Disabled**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Wireless Tab - Wireless Security

Wireless Security

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

WEP. WEP is a basic encryption method, which is not as secure as Pre-Shared Key. To use WEP, select a Default Transmit Key (choose which Key to use), and a level of WEP encryption, **40/ 64 bits, 128 bits, or 152 bits**. Then either generate a WEP key automatically using the Passphrase or enter the WEP key manually.

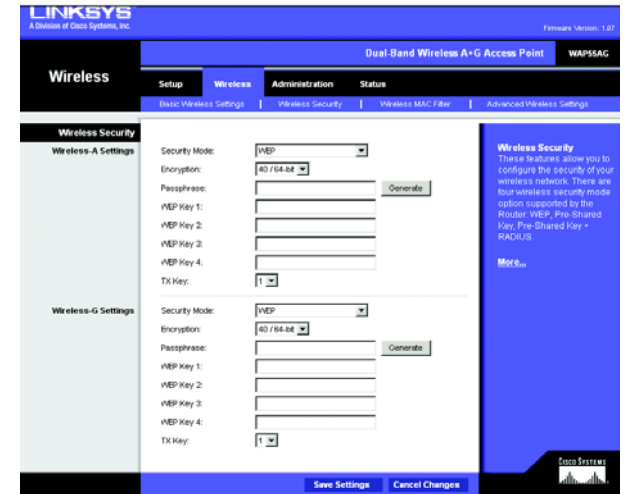


Figure 6-4: WEP

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

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

Pre-Shared Key. Pre-Shared Key gives you two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP or AES**. Enter a Pre-Shared Key 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.



Figure 6-5: Pre-Shared Key

Dual-Band Wireless A + G Access Point

Pre-Shared Key + RADIUS. This option features Pre-Shared Key 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 Pre-Shared Key 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.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**. For detailed instructions on configuring wireless security for the Access Point, turn to “Appendix B: Wireless Security.”

The screenshot displays the Linksys web interface for configuring a Dual-Band Wireless A+G Access Point. The 'Wireless' tab is selected, and the 'Wireless Security' sub-tab is active. The interface is divided into two main sections: 'Wireless-A Settings' and 'Wireless-G Settings'. Both sections have identical configuration options:

- Security Mode:** A dropdown menu set to 'Pre-Shared Key + RADIUS'.
- Encryption:** A dropdown menu set to 'TKIP'.
- RADIUS Server:** Four input fields for IP address, each containing a '0'.
- RADIUS Port:** An input field containing '1812'.
- Shared Key:** An empty text input field.
- Key Renewal:** An input field containing '3600' followed by the unit 'seconds'.

At the bottom of the page, there are two buttons: 'Save Settings' and 'Cancel Changes'. On the right side, there is a 'Wireless Security' help section with a 'More...' link. The top of the page shows the Linksys logo and the device name 'Dual-Band Wireless A+G Access Point'.

Figure 6-6: Pre-Shared Key + Radius

The Wireless Tab - Wireless MAC Filter

Wireless network access can be filtered by using the MAC addresses of the wireless devices.

Access Restrictions

To filter wireless users by MAC Address, either permitting or blocking access, click **Enabled**. If you do not wish to filter users by MAC Address, select **Disabled**.

Prevent PCs listed below from accessing the wireless network. Clicking this radio button will block wireless access by MAC Address.

Permit PCs listed below to access the wireless network. Clicking this radio button will allow wireless access by MAC Address.

Wireless Client List

Wireless Client List. Click the **Wireless Client List** button to display a list of network users by MAC Address. From the *To Sort by* drop-down menu, you can sort the table by Client Name, Interface, IP Address, MAC Address, or Status. If you want to add any of the wireless clients to the Wireless MAC Filter List, then click the **Save to Wireless Client List** checkbox and then click the **Save Settings** button. Click the **Cancel Changes** button to cancel your changes. To view the most up-to-date information, click the **Refresh** button. To exit this screen, click the **Close** button.

List users, by MAC Address, whose wireless access you want to control.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

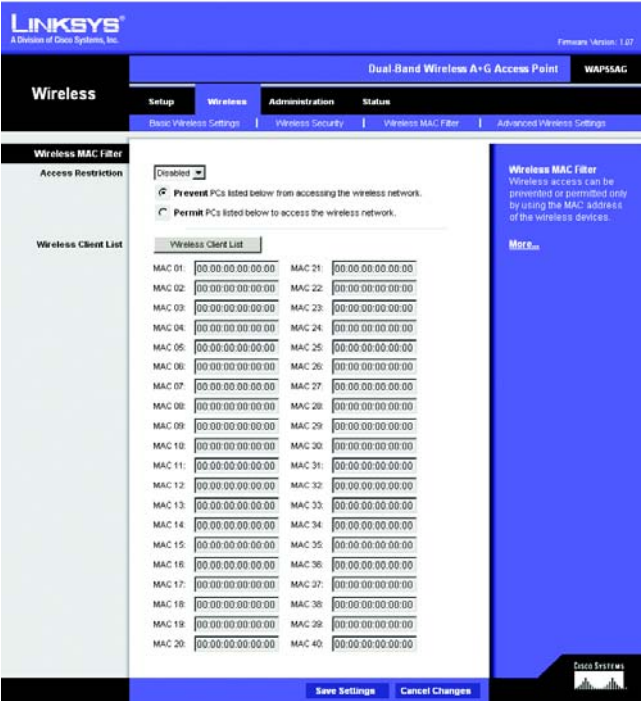


Figure 6-7: Wireless MAC Filter

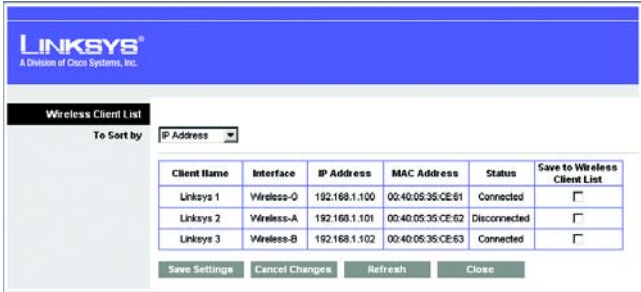


Figure 6-8: Wireless Client List

The Wireless Tab - Advanced Wireless Settings

This screen contains the advanced wireless settings. In most cases, these settings do not need to be changed.

Wireless-A Settings

Authentication Type. The default is set to **Open System (Default)** authentication, when the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Transmission Rate. 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 select **Auto (Default)** to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client. The default value is **Auto (Default)**.

Transmission Power. (Transmit Power Control (TPC)) The greater the transmission power used, the larger the area a wireless network covers. To minimize the likelihood of eavesdropping by unauthorized wireless users, do not use more transmission power than necessary to cover the range needed by your wireless network. Try using the Access Point at different levels of transmission power, and determine how much power is needed to reach the wireless client, such as a PC or access point, that is farthest from the Access Point. Then select the appropriate level, **Full (Default)**, **Half**, **Quarter**, **Eighth**, or **Min**, from the drop-down menu. The default is **Full (Default)**.

Frame Burst Mode. 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, **Enabled (Default)**.

Beacon Interval. The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to synchronize the wireless network.

DTIM Interval. This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

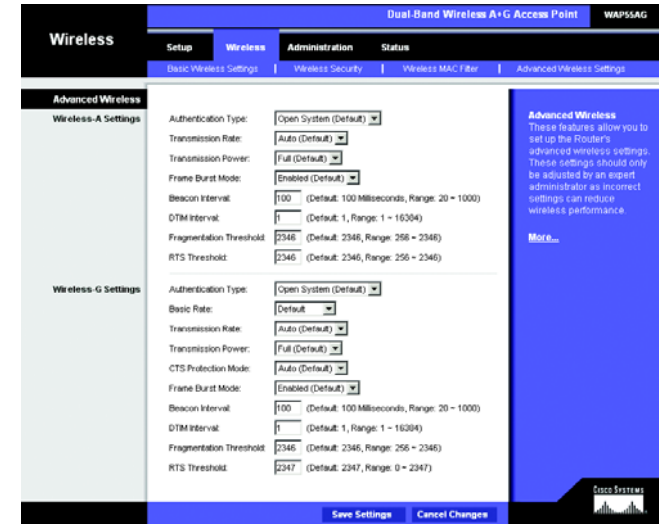


Figure 6-9: Advanced Wireless

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

packet: a unit of data sent over a network

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

fragmentation: breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, **2346**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Access Point sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2346**.

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

Wireless-G Settings

Authentication Type. The default is set to **Open System (Default)** authentication, when the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Basic Rate. The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Access Point can transmit. The Access Point will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Access Point will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Access Point can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Access Point can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Access Point's rate of data transmission, configure the Transmission Rate setting.

Transmission Rate. 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 select **Auto (Default)** to have the Access Point automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Access Point and a wireless client. The default value is **Auto (Default)**.

Transmission Power. (Transmit Power Control (TPC)) The greater the transmission power used, the larger the area a wireless network covers. To minimize the likelihood of eavesdropping by unauthorized wireless users, do not use more transmission power than necessary to cover the range needed by your wireless network. Try using the Access Point at different levels of transmission power, and determine how much power is needed to reach the wireless client, such as a PC or access point, that is farthest from the Access Point. Then select the appropriate level, **Full (Default)**, **Half**, **Quarter**, **Eighth**, or **Min**, from the drop-down menu. The default is **Full (Default)**.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode should be set to **Auto (Default)**. The Access Point will automatically use CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not 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. If you do not want to use CTS Protection Mode at all, select **Disabled**.

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

Frame Burst Mode. Enabling this option should 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, **Enabled**.

Beacon Interval. The default value is **100**. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to synchronize the wireless network.

DTIM Interval. This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Access Point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold. This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold. Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Access Point sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

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

packet: a unit of data sent over a network

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

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

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

The Administration Tab - Password

The Password screen allows you to change the Access Point's password and Backup & Restore settings.

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

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

The Administration Tab - Log

The Access Point can keep logs of wireless activity.

To disable the Log function, keep the default setting, **Disabled**. To monitor wireless activity, select **Enabled**.

Logviewer IP Address. For a permanent record of the Access Point's wireless activities, Logviewer software must be used. This software can be downloaded from the Linksys website, www.linksys.com. The Log viewer saves all wireless activities in a permanent file on your PC's hard drive. In the *Logviewer IP Address* field, enter the fixed IP address of the PC running the Log viewer software. The Access Point will now send updated logs to that PC.

View Log. When you wish to view the logs, click **View Log**.

Change these settings as described here and click the **Save Settings** button to apply your changes or **Cancel Changes** to cancel your changes. Help information is shown on the right-hand side of the screen. For additional information, click **More**.

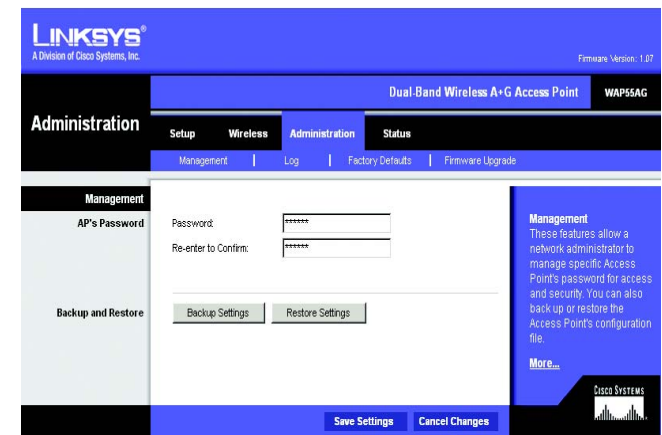


Figure 6-10: Password



Figure 6-11: Log

The Administration Tab - Factory Defaults

This screen allows you to restore the Access Point's configuration to its factory default settings.



Note: Do not restore the factory defaults unless you are having difficulties with the Access Point and have exhausted all other troubleshooting measures. Once the Access Point is reset, you will have to re-enter all of your configuration settings.

Factory Defaults

Restore Factory Defaults. Click this button to reset all configuration settings to their default values. Any settings you have saved will be lost when the default settings are restored.

Help information is shown on the right-hand side of the screen.



Figure 6-12: Factory Defaults

download: to receive a file transmitted over a network

firmware: the programming code that runs a networking device

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

The Administration Tab - Firmware Upgrade

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

Firmware Upgrade

Before upgrading the firmware, download the Access Point's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file.

Please select a file to upgrade. In the field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.

Start to Upgrade. After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Help information is shown on the right-hand side of the screen.



Figure 6-13: Firmware Upgrade

The Status Tab - Local Network

The *Status* tab displays the current status of the Access Point's local network.

AP's Information

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

Local Network

MAC Address. This is the Access Point's Ethernet MAC Address.

Configuration Type. This displays the Access Point's network configuration type.

AP's IP Address. This shows the Access Point's IP Address.

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

Default Gateway. This shows the Access Point's Default Gateway.

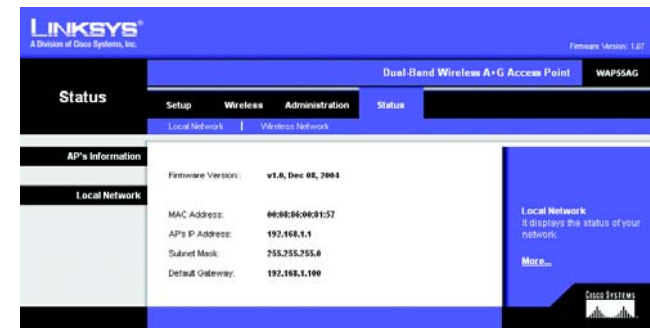


Figure 6-14: Status - Local Network

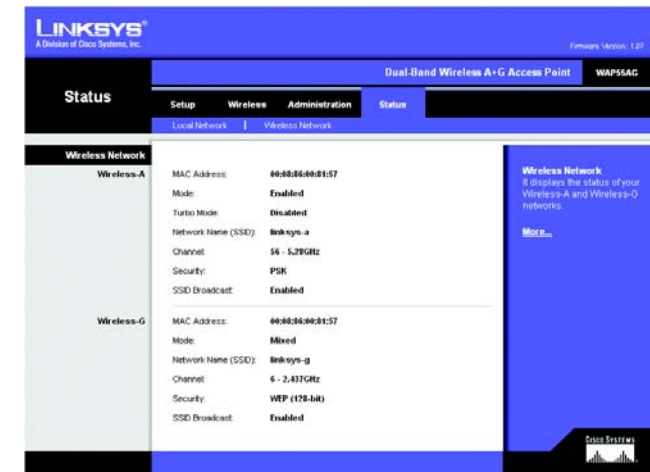


Figure 6-15: Status - Wireless Network

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

The Status Tab - Wireless

The *Wireless* screen on the Status Tab displays the status of your Wireless-A and/or Wireless-G networks.

Wireless-A Network

MAC Address. This is the Access Point's Wireless-A network MAC address.

Mode. This displays the status of the Access Point's Wireless-A networking mode.

Turbo Mode. This displays the status of the Access Point's Wireless-A networking turbo mode.

Network Name (SSID). This displays the wireless network name or SSID of your Wireless-A network.

Channel. This displays the channel being used on your Wireless-A network.

Security. The encryption method being used on your Wireless-A network is displayed here.

SSID Broadcast. This displays the status of the Access Point's SSID Broadcast feature.

Wireless-G Network

MAC Address. This is the Access Point's Wireless-G network MAC address.

Mode. This displays the status of the Access Point's Wireless-G networking mode.

Network Name (SSID). This displays the wireless network name or SSID of your Wireless-G network.

Channel. This displays the channel being used on your Wireless-G network.

Security. The encryption method being used on your Wireless-G network is displayed here.

SSID Broadcast. This displays the status of the Access Point's SSID Broadcast feature.

Appendix A: Troubleshooting

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

Frequently Asked Questions

Can the Access Point act as my DHCP Server?

No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Can I run an application from a remote computer over the wireless network?

This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?

Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11 functions:

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

What is Ad-hoc?

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

What is Infrastructure?

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

What is Roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

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

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

Would the information be intercepted while transmitting on air?

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

Can Linksys Wireless products support file and printer sharing?

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

What is WEP?

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

What is a MAC Address?

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

How do I avoid interference?

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

How do I reset the Access Point?

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

How do I resolve issues with signal loss?

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

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, due to FCC regulations, more power may be transmitted, using 802.11a, on channels 52, 56, 60 and 64, than on the lower channels. Lastly, check the Advanced tab of the Web-Based Utility and make sure that FULL is selected in the Transmission Rate field.

Does the Access Point function as a firewall?

No. The Access Point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but I cannot see my network.

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

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

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

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

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

Appendix B: Wireless Security

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

Security Precautions

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

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

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

Security Threats Facing Wireless Networks

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

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



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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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



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

Dual-Band Wireless A + G Access Point

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

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

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

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

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

Appendix C: Upgrading Firmware

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

1. Before upgrading the firmware, download the Access Point's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file.
2. In the **Please select a file to upgrade** field provided, enter the name of the extracted firmware upgrade file, or click the **Browse** button to find this file.
3. After you have selected the appropriate file, click the **Start to Upgrade** button, and follow the on-screen instructions.



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.

Dual-Band Wireless A + G Access Point

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

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

Encryption - Encoding data transmitted in a network.

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

Firmware - The programming code that runs a networking device.

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

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

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

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

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

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

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

ISM band - Radio bandwidth utilized in wireless transmissions.

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

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

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

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

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

Packet - A unit of data sent over a network.

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

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

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

Router - A networking device that connects multiple networks together.

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

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

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

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

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

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

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

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

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

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

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

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

Dual-Band Wireless A + 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	IEEE 802.11a, IEEE802.11b, IEEE 802.11g, IEEE 802.3, IEEE 802.3u
Ports/Buttons	One 10/100 RJ-45 Port (Auto MDI/MDI-X) One Reset Button
Cabling Type	UTP CAT 5 or better
LEDs	Power, Ethernet, Wireless-A: WLAN, Wireless-G: WLAN
Security features	MAC address filtering, WEP Encryption
WEP key bits	64/128/152-bit
Power	External, 5V DC
Dimensions (L x W x H)	7.32" x 1.89" x 6.89" (186 mm x 48 mm x 175 mm)
Unit Weight	13.05 oz. (0.37 kg)
Certifications	FCC
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Warranty	3-Year Limited

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

Dual-Band Wireless A + G Access Point

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

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

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

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

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

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

Belgique:

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

France:

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

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

SAFETY NOTICES

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

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

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

Appendix I: Contact Information

Need to contact Linksys?

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

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

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

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

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

800-326-7114
support@linksys.com

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

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

949-823-3000