LINKSYS®
A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G

Exterior Access Point

User Guide

WIRELESS

Model No. **WAP54GPE**

CISCO SYSTEMS

Copyright and Trademarks

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use this User Guide

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

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

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

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

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

word: *definition.*

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

Figure 0-1: Sample Figure Description

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

Table of Contents

List of Figures

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Exterior 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. In fact, the Wireless-G Exterior Access Point can support communications on up to eight wireless networks, using Virtual Local Area Network (VLAN) technology.

The Wireless-G Exterior Access Point also offers the convenience of Power over Ethernet (PoE) capability, so it can receive data and power over a single Ethernet network cable. And with the advantage of its weather-proof housing, you can mount the Access Point outside to extend your wireless networking range and mobility to the outdoors. You can even connect wired networks in two different buildings, by using two Access Points set to Wireless Bridge mode.

But what does all of this mean?

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

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

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wired Local Area Network. The Access Point bridges wireless networks of both 802.11g and 802.11b standards and wired networks.

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

access point*: a device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.*

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

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

poe *(power over ethernet): a technology enabling an Ethernet network cable to deliver both data and power.*

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

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

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

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

What's in this User Guide?

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

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

- Appendix G: Warranty Information
  This appendix supplies the Access Point's warranty information.

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

- Appendix I: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network.

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

Linksys wireless adapters also provide users access to a wired network when using an access point, such as the Wireless-G Exterior Access Point, or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

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

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled.

Roaming

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

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

Before 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.

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

Network Layout

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

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router with Power over Ethernet (PoE)—or a PoE injector, such as the Linksys WAPPOE or WAPPOE12.

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

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

The LEDs

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

Figure 3-1: Front Panel

(Power) Green. The power LED lights up when the Access Point is powered on.

(Wired) Green. The wired LED lights up when the Access Point is successfully connected to a device through the Ethernet network port. If the wired LED is flashing, the Access Point is actively sending to or receiving data from one of the devices over the Ethernet network port.

(Wireless) Green. The wireless LED lights up when the Access Point is successfully connected to a wireless device. If the wireless LED is flashing, the Access Point is actively sending to or receiving data from a wireless device.

The Ports

The Access Point's Ethernet network port is located on the bottom panel, while the antenna port is located on the top panel.

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

Ethernet

Figure 3-2: Ethernet Network Port

(Ethernet) The Ethernet network port connects to Ethernet network devices, such as a switch or router that supports Power over Ethernet (PoE).

Antenna

Figure 3-3: Antenna Port

(Antenna) The Access Point has a built-in, internal patch antenna. It also has a male N-type antenna port for an optional, high-gain external antenna.

The Reset Button and Ground

The Access Point's Reset button and ground are located on the back panel.

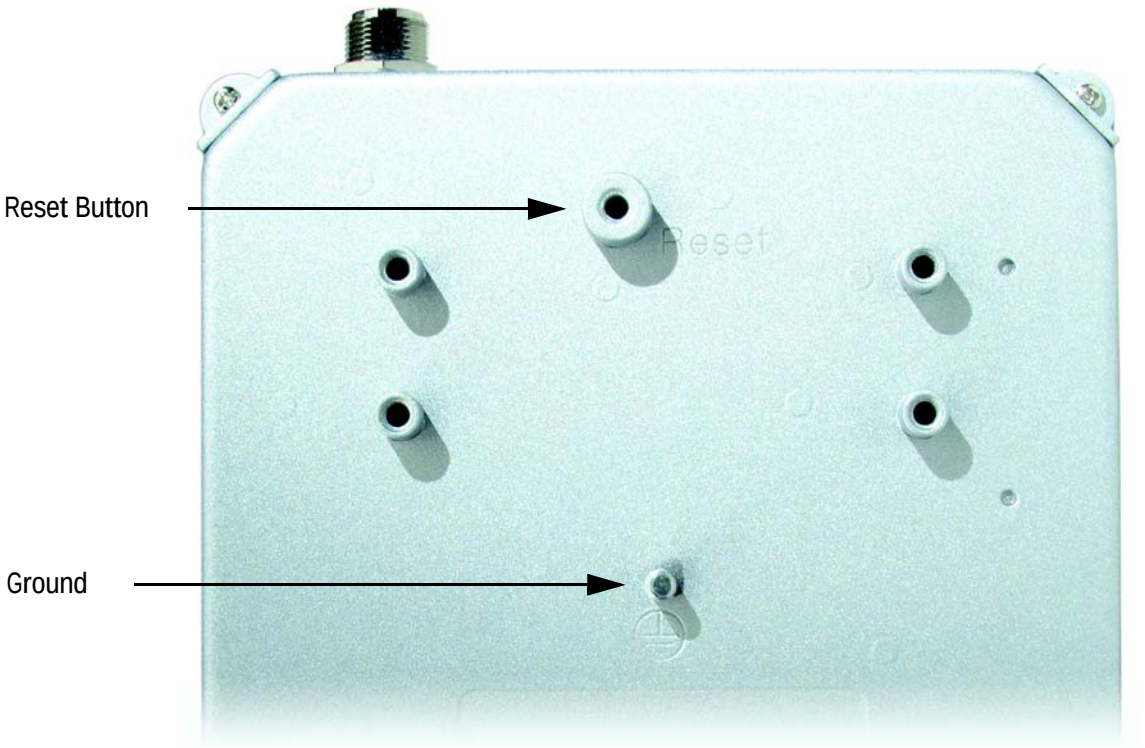

Figure 3-4: Reset Button

Reset Button

Reset 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 using the Access Point's Web-based Utility.

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

Ground

(Ground) Before you mount the Access Point, you must ground the Access Point as a precaution.

Chapter 4: Connecting the Wireless-G Exterior Access Point

Overview

This chapter explains how to mount and connect the Access Point.

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

Hardware Installation

1. Locate an optimum location for the Access Point.
2. Use the mounting plate as a template. On the wall you have chosen, mark the locations of the two wall-mount slots at the bottom of the mounting plate.
3. Attach two screws (not included) to the wall, so that the Access Point's wall-mount slots line up with the two screws.
4. Use four screws (included with the Access Point) to attach the mounting plate to the back panel of the Access Point.
5. Connect the included Category 5e Ethernet network cable to the Ethernet network port of the Access Point. Then screw the connector cap tightly onto the port, so the Access Point has a water-resistant seal.
6. If you want to connect the optional, high-gain external antenna, unscrew the cap protecting the Type-N antenna port. Then connect your antenna to this port.

Figure 4-1: Mark the Locations of the Two Wall-Mount Slots

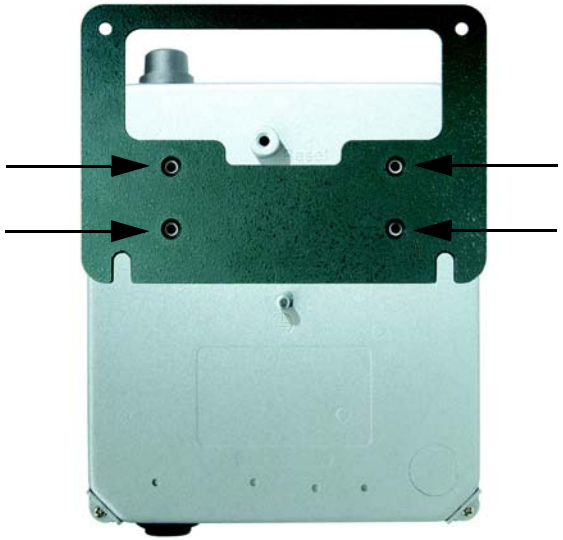

Figure 4-2: Attach the Mounting Plate

7. Make sure you properly ground the Access Point.

8. Maneuver the Access Point so the two screws on the wall are inserted into the Access Point's wall-mount slots. Then slide the Access Point down so the screws fit snugly in the slots.

9. Attach two screws (not included) at the top of the mounting plate so the Access Point is securely mounted.

10. Connect the other end of the Ethernet network cable to a switch, router, or other device that supports Power over Ethernet. The Access Point will then be connected to your wired network.

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

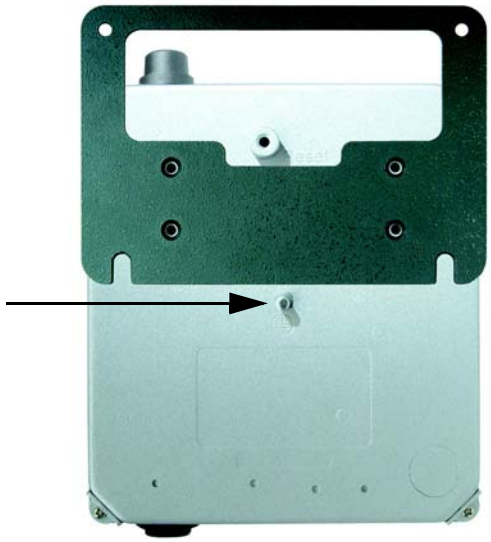

Figure 4-3: Ground the Access Point

Figure 4-4: Attach the Access Point to the Wall

Chapter 5: Setting Up the Wireless-G Exterior Access Point

Setup Wizard

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

1. Insert the Setup Wizard CD into your PC's CD-ROM drive. Your PC must be on your wired network to set up the Access Point.

2. The Setup Wizard's *Welcome* screen should appear on your monitor. If it does not, then click the **Start** button and select **Run**. In the field provided, enter **D:\setup.exe** (if "D" is the letter of your PC's CD-ROM drive).

   Click the **Setup** button to proceed with this Setup Wizard. Clicking the **User Guide** button opened this Guide. To exit this Setup Wizard, click the **Exit** button.

Figure 5-1: Setup Wizard's Welcome Screen

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

Figure 5-2: Connecting the Access Point

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

Figure 5-3: Select an Access Point

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

Figure 5-4: Login Screen

6. The *Configure Network Address Settings* screen will appear next. If your network router will automatically assign an IP address to the Access Point, then select **Automatically obtain an IP address (DHCP)**.

   If you want to assign a static or fixed IP address to the Access Point, then select **Set IP configuration manually**. Enter an IP Address, a 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 the subnet mask of your Ethernet network.
   - Gateway. This IP address should be the IP address of the gateway between the Internet and the local network. (If you do not have a gateway, then enter the IP address of your network router.)

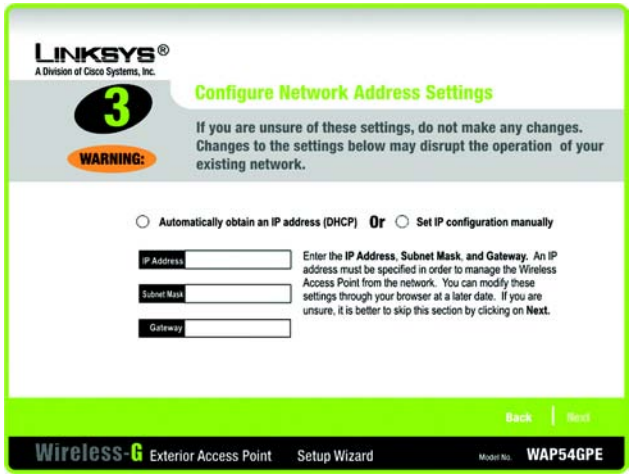

Figure 5-5: Configure Network Address Settings Screen

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.*

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.*

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

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

7. The *Wireless Settings* screen should now appear. The Access Point can connect to up to eight wireless networks at the same time. On this screen, you can configure up to three wireless networks and the Access Point's wireless mode. (If you want to configure additional networks, then use the Web-based Utility.)

   Select **Main SSID** and enter your primary SSID in the field provided. Then select the channel at which the network broadcasts its wireless signal.

   Select the wireless mode you want the Access Point to use for all of the wireless networks it supports.

   Select **SSID 2** and enter your second SSID in the field provided. Then select this network's channel setting.

   Select **SSID 3** and enter your third SSID in the field provided. Then select this network's channel setting.

   After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

   - SSID. The SSID is the unique name shared among all devices in a 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 devices 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 use the same channel in order to communicate.
   - Mode. Select **Mixed Mode** if you want both Wireless-G and Wireless-B computers allowed on the networks, but note that 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 networks. You can also disable wireless performance if you select **Disable**.

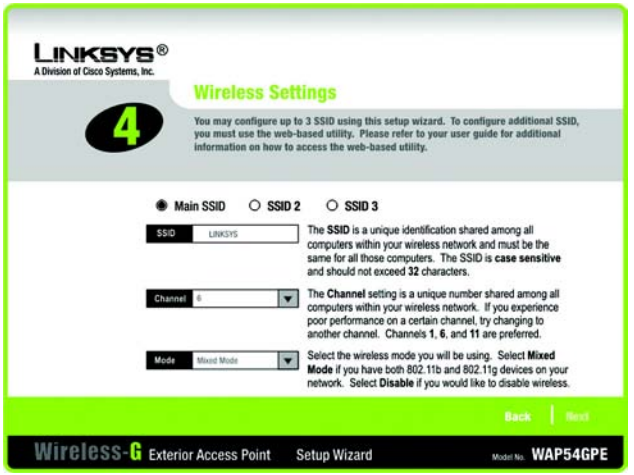

Figure 5-6: Wireless Settings Screen

8. The *Wireless Security Settings* screen will appear next. From this screen, you can set the level of security you desire for each of your three networks.

   First, select the wireless network you want to configure, **Main SSID**, **SSID 2**, or **SSID 3**.

   Then select from **WEP (64-Bit)**, **WEP (128-Bit)**, and **WPA-Personal**, and follow the appropriate instructions below. If you want to use WPA-Enterprise, then select **Disabled** from the *Security* drop-down menu. (You will have to use the Web-based Utility to set up WPA-Enterprise or RADIUS; for more information, refer to "Chapter 6: Configuring the Wireless-G Exterior Access Point.")

   After you have entered the settings for your three wireless networks, 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."

   - WEP (64-Bit) or WEP (128-Bit). Enter the Passphrase for your network. If want to manually enter the WEP key, then leave the *Passphrase* field blank and enter the WEP key in the *Key 1* field. 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.

     After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

Figure 5-7: Wireless Security Settings - WEP Screen

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

bit: *a binary digit.*

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.*

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

- WPA-Personal. With WPA-Personal, you will use TKIP or AES for encryption with dynamic keys. Then enter a Pre-Shared Key of 8-63 characters.

  After you have entered the settings for your three wireless networks, click the **Next** button to continue or **Back** to return to the previous page.

Figure 5-8: Wireless Security Settings - WPA-Personal Screen

tkip *(temporal key integrity protocol): a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.*

9. The *Wireless Power Management* screen will appear. You can adjust the power output of the Access Point to get the appropriate coverage for your wireless network. Select the setting appropriate for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**. Click the **Next** button to continue or **Back** to return to the previous page.

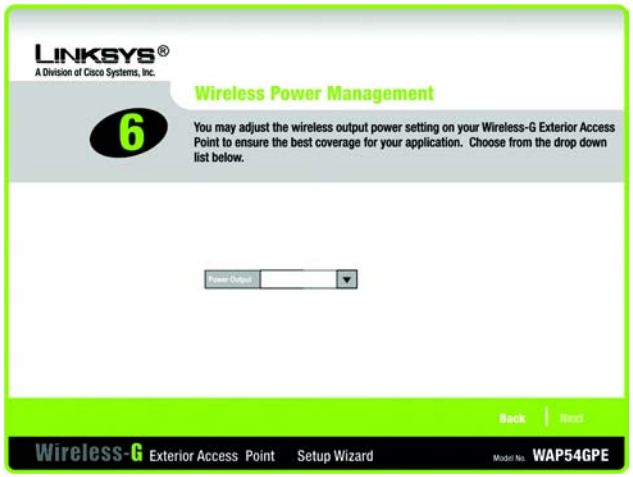

Figure 5-9: Wireless Power Management Screen

10. On the *Confirmation* screen, make sure your new settings are correct. To save your new settings, click the **Yes** button. If you do not want to save your changes, then click the **No** button.

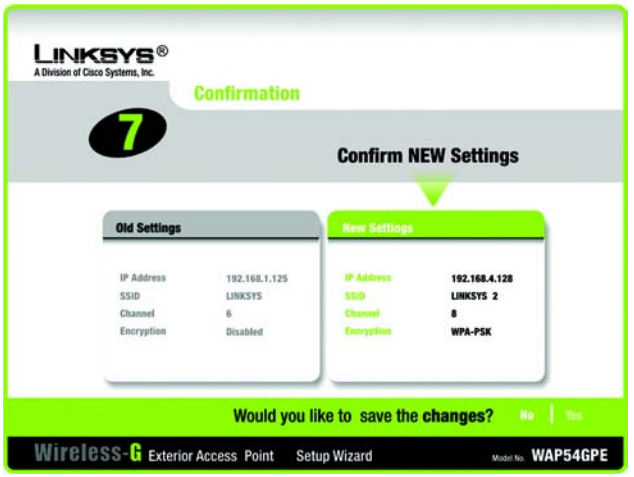

Figure 5-10: Confirmation Screen

11. 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 **Online Registration** button to register the Access Point, or click the **Exit** button to exit the Setup Wizard.

    For more advanced configuration, you can go to "Chapter 6: Configuring the Wireless-G Exterior Access Point."

Figure 5-11: Congratulations Screen

Chapter 6: Configuring the Wireless-G Exterior Access Point

Overview

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

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

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

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

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

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

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

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

Navigating the Utility

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

Setup

Enter the Host Name and settings for your Internet connection on this screen.

Wireless

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

- *Basic Wireless Settings*. Enter the network mode, Virtual Local Area Network (VLAN) priority, SSIDs, and transmit rates on this screen.
- *Wireless Security*. Use this screen to configure the Access Point's security settings.

- *Wireless Network Access*. From this screen, you can permit or block access to your wireless network.
- *Advanced Wireless Settings*. Use this screen to configure the Access Point's more advanced wireless settings.

AP Mode

Use this screen to configure how the Access Point will work with other access points in your network.

Administration

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

- *Management*. This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings.

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

- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Default*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.

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

- *Language Upgrade*. On this screen, change the language of the Access Point's Web-based Utility.
- *Reboot*. Use this screen to reboot the Access Point.
- *Config Management*. You can back up the configuration file for the Access Point, as well as save the backup configuration file to the Access Point.

Status

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

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

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. Enter **admin** in the *User Name* field. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

Figure 6-1: Login Screen

The Setup Tab

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

Setup

Enter a name for the Access Point.

Host 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.

Network Setup

The selections under this heading allow you to configure the Access Point's IP setting(s).

AP IP Type

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

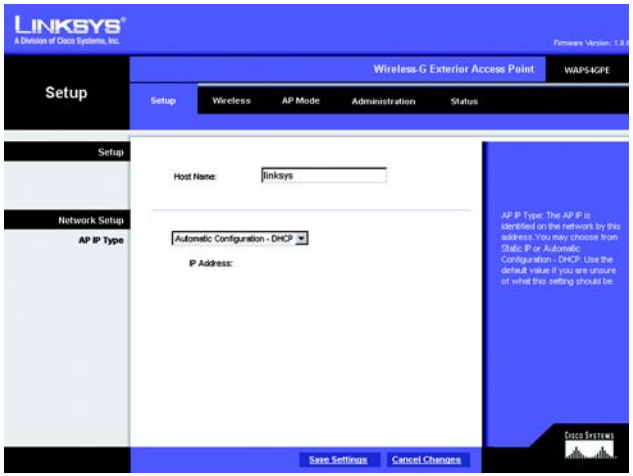

Figure 6-2: Setup - Automatic Configuration - DHCP Screen

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

- **IP Address**. The IP address must be unique to your network. We suggest you use the default IP address of **192.168.1.245**.
- **Subnet Mask**. The Subnet Mask must be the same as that set on your Ethernet network.

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

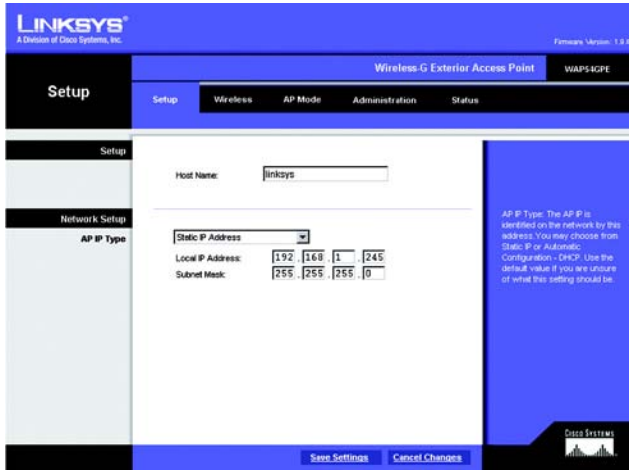

Figure 6-3: Setup - Static IP Address Screen

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

The Wireless - Basic Wireless Settings Tab

Change the wireless network settings on this screen. The Access Point can connect to up to eight wireless networks at the same time, so this screen offers settings for up to eight different SSIDs.

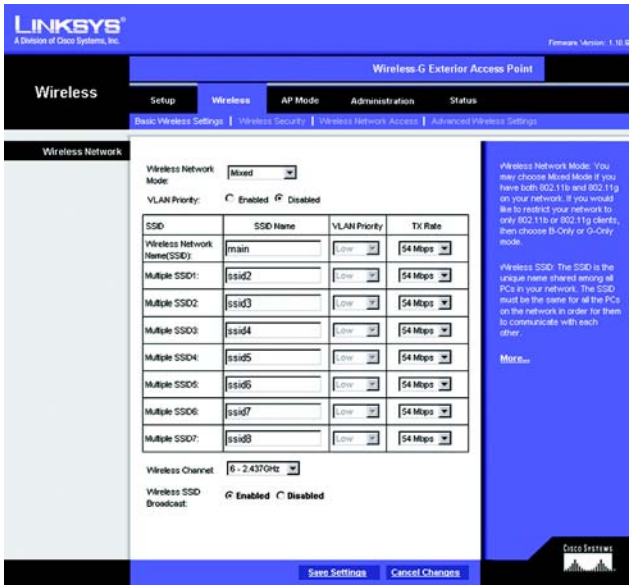

Figure 6-4: Wireless - Basic Wireless Settings Screen

Wireless Network

Configure the Access Point using the available settings. You can enter and save more than one configuration for the Access Point. (In other words, the Access Point can support up to eight VLANs.)

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. You can also disable wireless performance if you select **Disabled**.

VLAN Priority. Select **Enabled** if you want to use the Access Point's capability to assign VLAN priorities. Select **Disabled** if you want to disable the Access Point's capability to assign VLAN priorities.

SSID. You can enter settings for up to eight wireless networks, one primary (the first one listed) and seven alternative ones.

SSID Name. The SSID is the unique name shared among all devices in a 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 devices in your wireless network.

VLAN Priority. You can assign VLAN priority to each wireless network, **Low**, **Medium**, or **High**.

TX Rate. The default setting is **54 Mbps**. 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, **54 Mbps**, to have the Access Point enable the Auto-Fallback feature. Auto-Fallback will automatically negotiate the best possible connection speed between the Access Point and a wireless device.

Wireless Channel. Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to function correctly.

Wireless SSID Broadcast. This feature allows the primary 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 **Enabled** to broadcast the primary SSID to all wireless devices in range. Click **Disabled** to increase network security and prevent the primary SSID from being seen on networked PCs.

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

The Wireless - Wireless Security Tab

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

Wireless Security

Enter the security settings for each SSID of the Access Point.

Select SSID. Select the SSID whose security settings you want to configure.

Security Mode. Select the security method you want to use, **WPA-Personal**, **WPA-Enterprise**, **RADIUS**, or **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.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings. For detailed instructions on configuring wireless security for the Access Point, turn to "Appendix B: Wireless Security." To disable such security, select **Disable**.

Authentication Type. If you select WPA-Personal or WPA-Enterprise, then select **WPA**.

If you select RADIUS or WEP, or if you disable wireless security, select the authentication method you want the Access Point to use, **Shared Key** or **Open Key**. 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 devices on your network must use the same authentication type.

SSID Interoperability. When enabled, the devices of the designated wireless network will have access to the other wireless networks configured on the Access Point. If you want devices of the designated wireless network to have access to other wireless networks, select **Enabled**. Otherwise, select **Disabled**.

WPA-Personal

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

WPA Shared Key. Enter a WPA Shared Key of 8-32 characters.

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

Figure 6-5: Wireless - Wireless Security (WPA Pre-Shared Key) Screen

encryption: *encoding data transmitted in a network.*

WPA-Enterprise

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

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

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

WPA Shared Key. Enter a WPA Shared Key of 8-32 characters.

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

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

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

Figure 6-6: Wireless Security - WPA RADIUS Screen

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

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

RADIUS

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

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

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

Default Transmit Key. Select a Default Transmit Key (choose which Key to use).

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

Passphrase. If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the **Generate** key.

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

WEP

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

Passphrase. If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the **Generate** key.

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

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

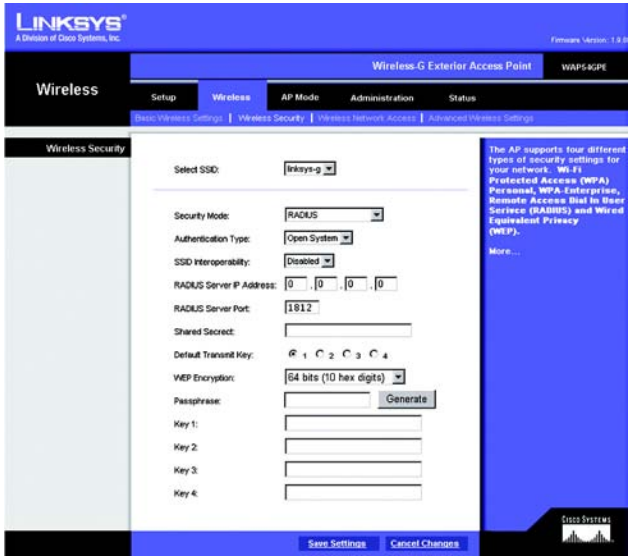

Figure 6-7: Wireless Security - RADIUS Screen

Figure 6-8: Wireless Settings - WEP Screen

The Wireless - Wireless Network Access Tab

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

Wireless Network Access

You can allow or block access for the MAC addresses you have entered.

Access List. To permit access, click **Permit to access**. To deny access, click **Prevent from accessing**. If you do not wish to filter users by MAC address, select **Disabled**.

MAC 1-20. Enter the MAC addresses of the computers whose access you want to control.

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

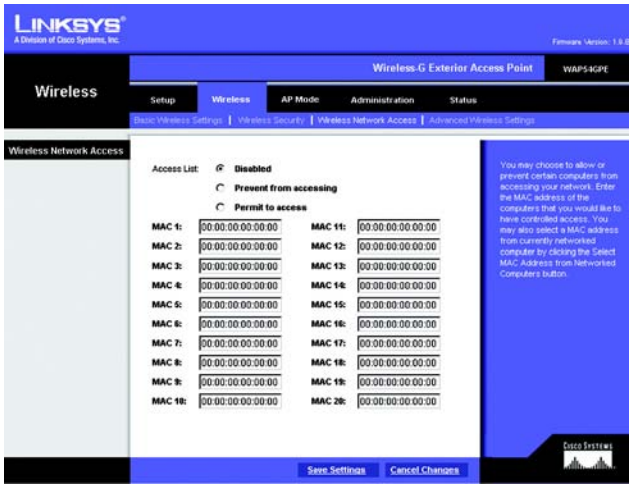

Figure 6-9: Wireless - Wireless Network Access Screen

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

The Wireless - Advanced Wireless Settings Tab

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

Advanced Wireless

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

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance. Keep the default setting, **Auto**, so the Access Point can use this feature as needed, when the Wireless-G products are not able to transmit to the Access Point in an environment with heavy 802.11b traffic. Select **Enabled** if you want to permanently enable this feature, or select **Disabled** if you want to permanently disable this feature.

Wireless Isolation. In most cases, keep the default, **Disabled**. Select **Enabled** if you do not want your wired and wireless networks to communicate; for example, if you have a wireless hotspot, you may want to keep the wireless network isolated from your wired network.

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

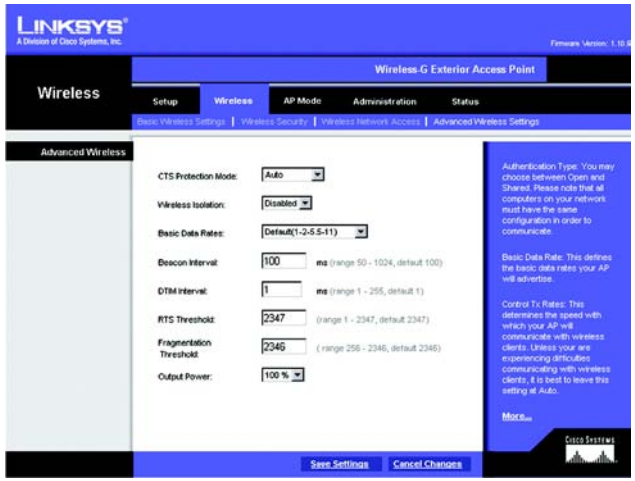

Figure 6-10: Wireless - Advanced Wireless Settings Screen

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

advertised. The Basic Data Rates are not the rates transmitted; the rates transmitted can be configured through the TX Rate setting on the Wireless - Basic Wireless Settings tab.

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

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

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

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

Output Power. You can adjust the output power of the Access Point to get the appropriate coverage for your wireless network. Select the level you need for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**.

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

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

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

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

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

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

The AP Mode Tab

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

IMPORTANT: For all modes of operation EXCEPT Access Point, the remote access point must be a second Linksys Wireless Access Point (for Wireless Repeater mode, a Wireless-G Broadband Router is also compatible). The Access Point will not communicate with any other kind of remote access point.

AP Mode

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

MAC Address

The MAC address of the Access Point is displayed here.

Access Point. The Mode is set to **Access Point** by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary. If you want to let the Access Point's signal be repeated, then click the checkbox next to *Allow wireless signal to be repeated by a repeater*. For example, you can use the Access Point with the Linksys Wireless-G Range Expander (model number: WRE54G).

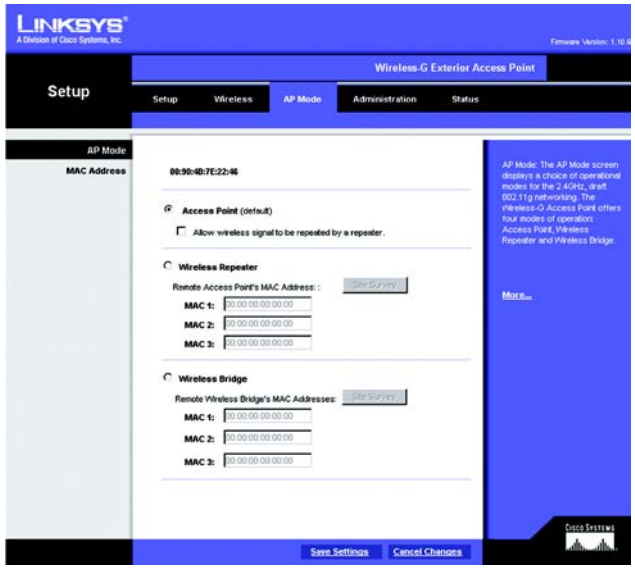

Figure 6-11: AP Mode Screen

Wireless Repeater. When set to Wireless Repeater mode, the Wireless Repeater is able to talk to up to three remote access points within its range and retransmit its signal. (This feature only works with the Linksys Wireless-G Exterior Access Point (model number: WAG54GPE), Wireless-G Access Point (model number: WAP54G), and Wireless-G Broadband Router (model number: WRT54G).

Figure 6-12: Wireless Repeater Diagram

To configure a Wireless Repeater environment, click **Wireless Repeater** and enter the local MAC addresses of the remote access points in the *MAC 1-3* fields. If you do not know an access point's MAC address, click the **Site Survey** button. Select the access points you want to use and click the **Apply** button. Then click the **Close** button to return to the *AP Mode* screen. If you do not see the access point you want, click the **Refresh** button to run another site survey.

Figure 6-13: Site Survey Screen

Wireless Bridge. This mode connects two physically separated wired networks with two access points. If you are trying to create a wireless connection between two wired networks, select **Wireless Bridge**. and enter the local MAC addresses of the wireless bridges/access points in the *MAC 1-3* fields. If you do not know a wireless bridge/access points's MAC address, click the **Site Survey** button. Select the wireless bridges/access points you want to use and click the **Apply** button. Then click the **Close** button to return to the *AP Mode* screen. If you do not see the wireless bridge/access point you want, click the **Refresh** button to run another site survey. The remote wireless bridges/access points also need to be set to Wireless Bridge mode.

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 6-14: Wireless Bridge Diagram

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

The Administration - Management Tab

On this screen you can configure the password and SNMP settings.

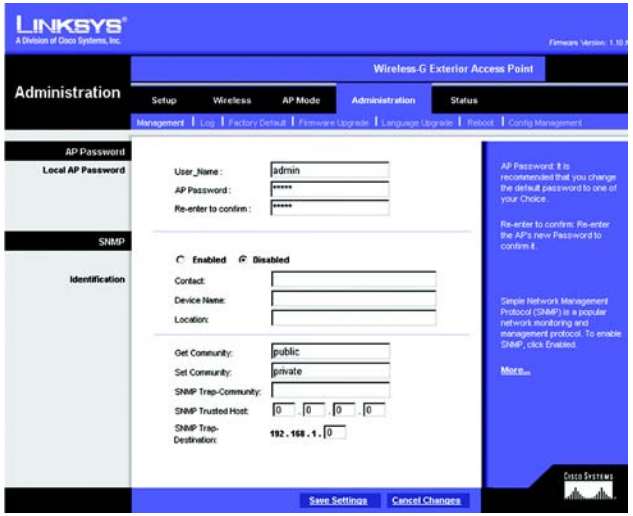

Figure 6-15: Administration - Management Screen

AP Password

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

Local AP Password

User Name. Create a User Name and enter it in the field provided.

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

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

SNMP

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

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

Identification

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

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

Location. Enter the location of the Access Point.

Get Community. Enter the password that allows read-only access to the Access Point's SNMP information. The default is **public**.

Set Community. Enter the password that allows read/write access to the Access Point's SNMP information. The default is **private**.

SNMP Trap-Community. Enter the password required by the remote host computer that will receive trap messages or notices sent by the Access Point.

SNMP Trusted Host. You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.

SNMP Trap-Destination. Enter the IP address of the remote host computer that will receive the trap messages.

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

The Administration - Log Tab

On this screen you can configure the log settings, as well as options for e-mail alerts of particular events.

Log

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

Email Alert

E-Mail Alert. To enable the Access Point to send e-mail alerts in the event of certain attacks (see the "Alert Log" section below), select **Enabled**. If you do not want to have e-mail alerts, select **Disabled**.

E-Mail Address for General Logs. Enter the e-mail address that will receive general logs.

E-Mail Address for Alert Logs. Enter the e-mail address that will receive alert logs.

Return E-Mail address. Your mail server may require a return e-mail address. If so, enter that address here. If you are not sure about what address to enter, enter the same e-mail address you entered above for the *E-Mail Address for Alert Logs* field.

E-Mail Server IP Address. Enter the IP address or full mail server name (e.g., mail.domain.com) of your mail server.s

Syslog Notification

Syslog is a standard protocol used to capture information about network activity. The Access Point supports this protocol and send its activity logs to an external server. To enable Syslog, select **Enabled**. If you do not want to use Syslog, select **Disabled**.

Device Name. Enter a name for the Access Point.

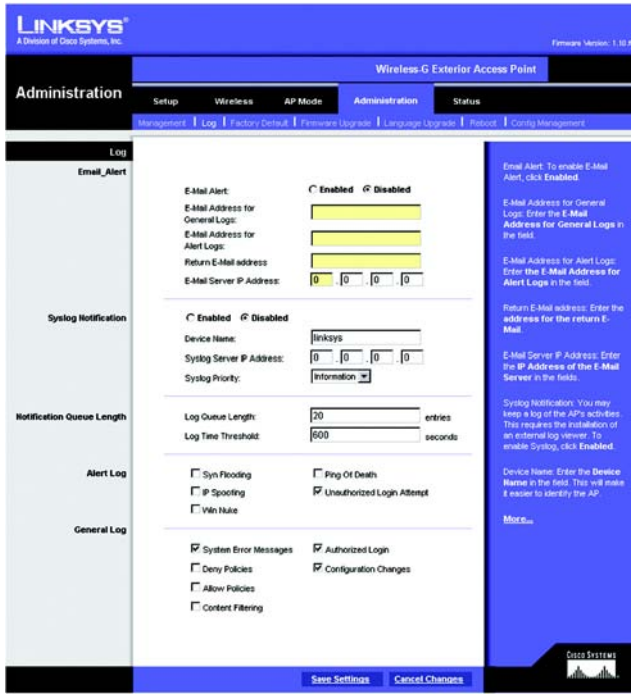

Figure 6-16: The Administration - Log Screen

Syslog Server IP Address. Enter the IP address of the Syslog server. In addition to the standard event log, the Access Point can send a detailed log to an external Syslog server. The Access Point's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP server, and number of bytes transferred.

Syslog Priority. Select the appropriate priority from the drop-down menu. The default is **Information**.

Notification Queue Length

Log Queue Length. You can designate the length of the log that will be e-mailed to you. The default is **20** entries.

Log Time Threshold. You can designate how often the log will be e-mailed to you. The default is **600** seconds (10 minutes).

Alert Log

Syn Flooding. If you want to receive alert logs about any Syn Flooding events, click the checkbox.

IP Spoofing. If you want to receive alert logs about any IP Spoofing events, click the checkbox.

Win Nuke. If you want to receive alert logs about any Win Nuke events, click the checkbox.

Ping of Death. If you want to receive alert logs about any Ping of Death attacks, click the checkbox.

Unauthorized Login Attempt. If you want to receive alert logs about any unauthorized login attempts, click the checkbox.

General Log

System Error Messages. If you want to log system error messages, click the checkbox.

Deny Policies. If you want to log any denial of access policies, click the checkbox.

Allow Policies. If you want to log any permission of access policies, click the checkbox.

Content Filtering. If you want to log any content filtering activities, click the checkbox.

Authorized Login. If you want to log authorized logins, click the checkbox.

Configuration Changes. If you want to log any configuration changes, click the checkbox.

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

The Administration - Factory Default Tab

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

Factory Default

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

Restore Factory Defaults. To restore the Access Point's factory default settings, click the **Yes** radio button. Otherwise, click the **No** radio button.

Click **Save Settings** to apply your change, or click **Cancel Changes** to cancel your change. Help information is displayed on the right-hand side of the screen.

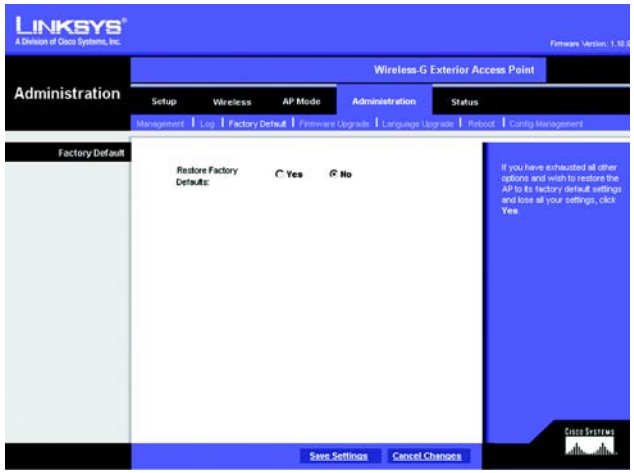

Figure 6-17: Administration - Factory Default Screen

The Administration - Firmware Upgrade Tab

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

Firmware Upgrade

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

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com*.
2. Extract the firmware upgrade file on your computer.
3. On the *Firmware Upgrade* screen, enter the location of the firmware upgrade file in the field provided, or click the **Browse** button to find the file.
4. Click the **Upgrade** button, and follow the on-screen instructions.

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

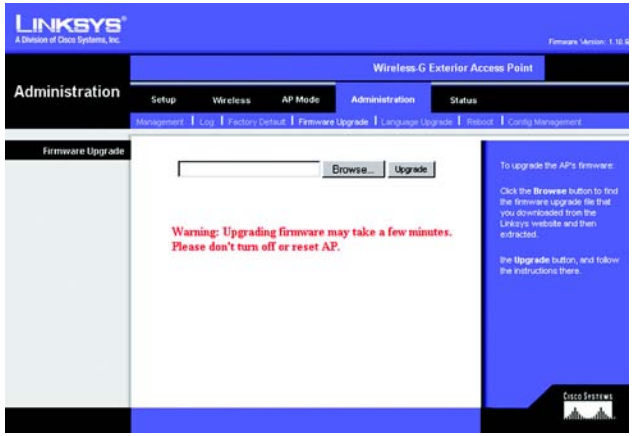

Figure 6-18: Administration - Firmware Upgrade Screen

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

The Administration - Language Upgrade Tab

On this screen you can do a language upgrade to change the language used by the Access Point's Web-based Utility.

Language Upgrade

If you do want to change the language currently used by the Web-based Utility, then you can download a language upgrade file and update the Access Point.

To change the Access Point's language:

1. Download the language upgrade file from the Linksys website, *www.linksys.com*.
2. Extract the language upgrade file on your computer.
3. On the *Language Upgrade* screen, enter the location of the language upgrade file in the field provided, or click the **Browse** button to find the file.
4. Click the **Upgrade** button, and follow the on-screen instructions.

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

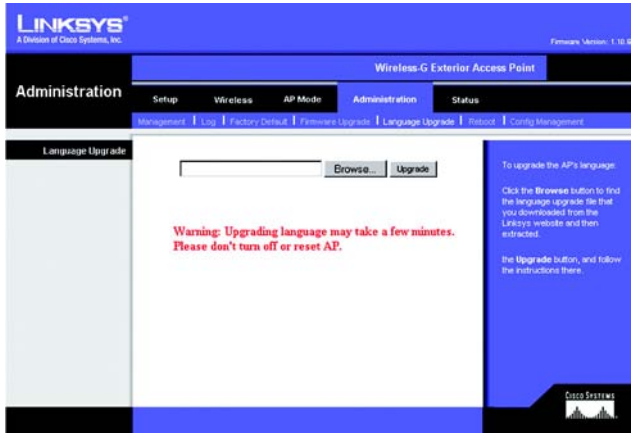

Figure 6-19: Administration - Language Upgrade Screen

The Administration - Reboot Tab

On this screen you can reboot the Access Point.

Reboot

This feature is useful when you need to remotely reboot the Access Point.

Device Reboot. To reboot the Access Point, click the **Yes** radio button. Otherwise, click the **No** radio button.

Click **Save Settings** to apply your change, or click **Cancel Changes** to cancel your change. Help information is displayed on the right-hand side of the screen.

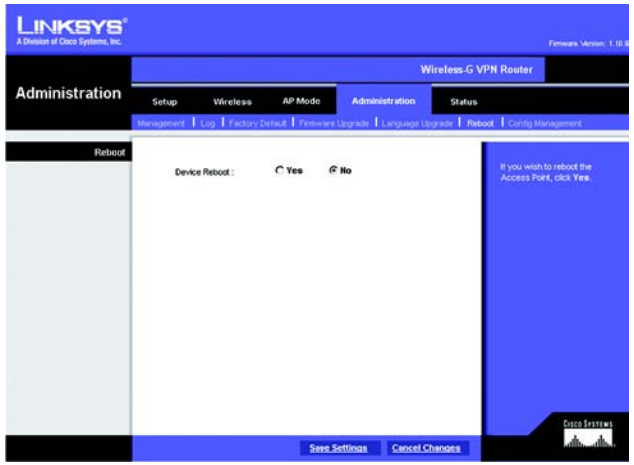

Figure 6-20: Administration - Reboot Screen

The Administration - Config Management Tab

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

Config Management

Use this screen to upload or download configuration files for the Access Point.

Download AP Config. To save a backup configuration file on a computer, click the **Download AP Configuration File** button and follow the on-screen instructions.

Upload AP Config. To upload a configuration file to the Access Point, enter the location of the configuration file in the field provided, or click the **Browse** button to find the file. Then click the **Load** radio button.

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

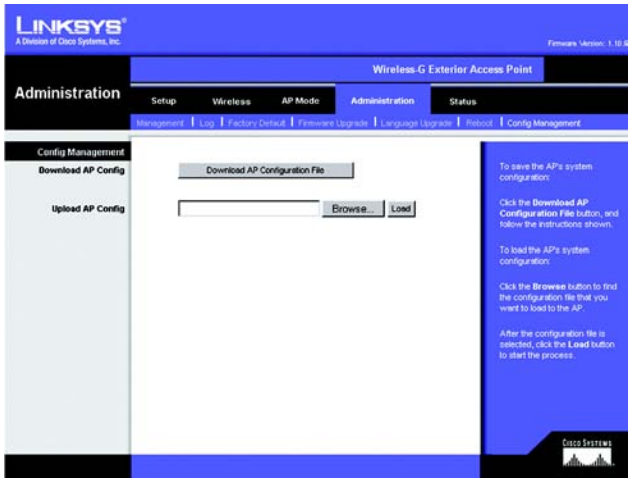

Figure 6-21: Administration - Config Management Screen

The Status - Local Network Tab

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

Information

Hardware Version. This is the version of the Access Point's current hardware.

Software Version. This is the version of the Access Point's current software.

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

System Up Time. This is the length of time the Access Point has been running.

Local Network

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

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

To update the status information, click the **Refresh** button. Help information is displayed on the right-hand side of the screen.

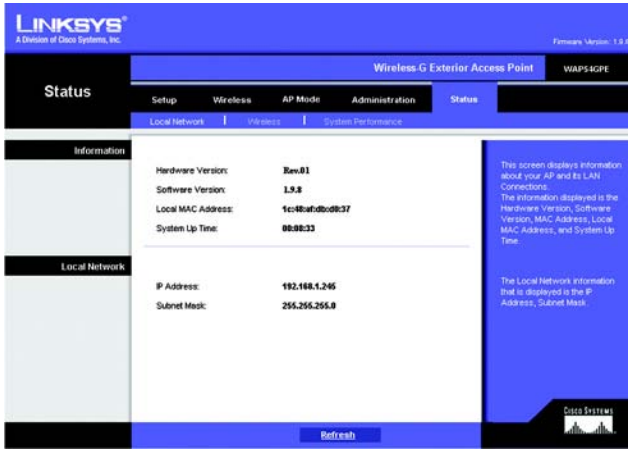

Figure 6-22: Status - Local Network Screen

The Status - Wireless Tab

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

Wireless Network

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

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

SSID. The Access Point's primary SSID is displayed here.

Multiple SSID1-7. The Access Point's alternative SSIDs are displayed here.

Channel. The Access Point's Channel setting for the primary SSID is shown here.

VLAN Priority Setting. The VLAN Priority Setting for the primary SSID is shown here.

SSID Encryption Function. The wireless security setting for the primary SSID is displayed here.

SSID VLAN Priority. The VLAN Priority setting for the primary SSID is displayed here.

Multiple SSID1-7 Encryption Function. The wireless security settings for the alternative SSIDs are displayed here.

Multiple SSID1-7 VLAN Priority. The VLAN Priority settings for the alternative SSIDs are displayed here.

To update the status information, click the **Refresh** button. Help information is displayed on the right-hand side of the screen.

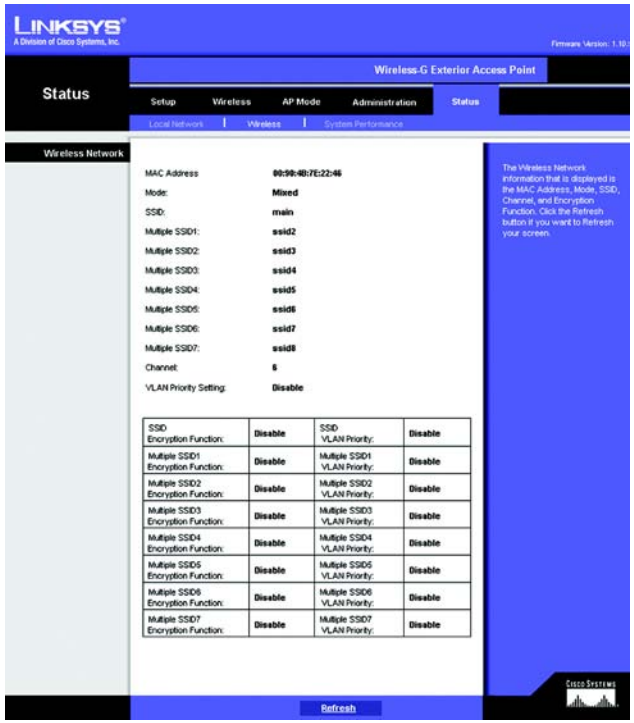

Figure 6-23: Status - Wireless Screen

The Status - System Performance Tab

The *System Performance* screen displays the Access Point's status information for its current settings and data transmissions.

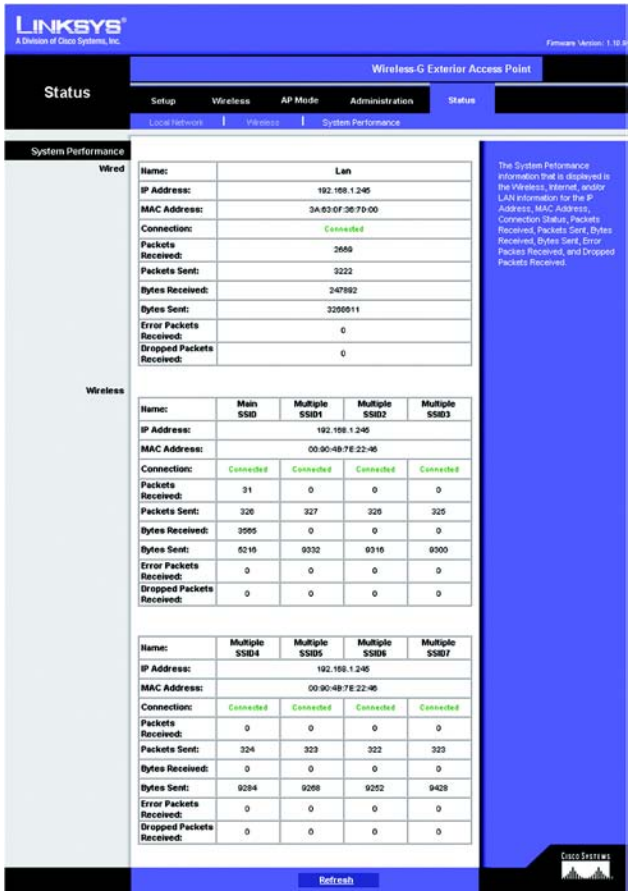

Figure 6-24: Status - System Performance Screen

System Performance

Wired

Name. This indicates that the statistics are for the wired network, the LAN.

IP Address. The Access Point's local IP address is displayed here.

MAC Address. This shows the MAC Address of the Access Point's wired interface.

Connection. This shows the status of the Access Point's connection for the wired network.

Packets Received. This shows the number of packets received.

Packets Sent. This shows the number of packets sent.

Bytes Received. This shows the number of bytes received.

Bytes Sent. This shows the number of bytes sent.

Error Packets Received. This shows the number of error packets received.

Dropped Packets Received. This shows the number of dropped packets received.

Wireless

Name. This indicates which wireless network/SSID to which the statistics refer.

IP Address. The Access Point's local IP address is displayed here.

MAC Address. This shows the MAC Address of the Access Point's wireless interface.

Connection. This shows the status of the Access Point's connection for each wireless network.

Packets Received. This shows the number of packets received for each wireless network.

Packets Sent. This shows the number of packets sent for each wireless network.

Bytes Received. This shows the number of bytes received for each wireless network.

Bytes Sent. This shows the number of bytes sent for each wireless network.

Error Packets Received. This shows the number of error packets received for each wireless network.

Dropped Packets Received. This shows the number of dropped packets received for each wireless network.

To update the status information, click the **Refresh** button. Help information is displayed on the right-hand side of the screen.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Exterior 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 is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

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

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

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

What IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

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

What is Ad-hoc?

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

What is Infrastructure?

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

What is roaming?

Roaming is the ability of a portable computer 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 set to the same channel number as the Access Point of the dedicated coverage area.

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

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

What is the ISM band?

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

What is Spread Spectrum?

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

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

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

Would the information be intercepted while transmitting on air?

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

Can Linksys wireless products support file and printer sharing?

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

What is WEP?

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

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

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

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

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

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

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

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

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

Appendix B: Wireless Security

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

Security Precautions

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

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

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

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

Security Threats Facing Wireless Networks

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

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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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.

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

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

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

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

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

Appendix C: Upgrading Firmware

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

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

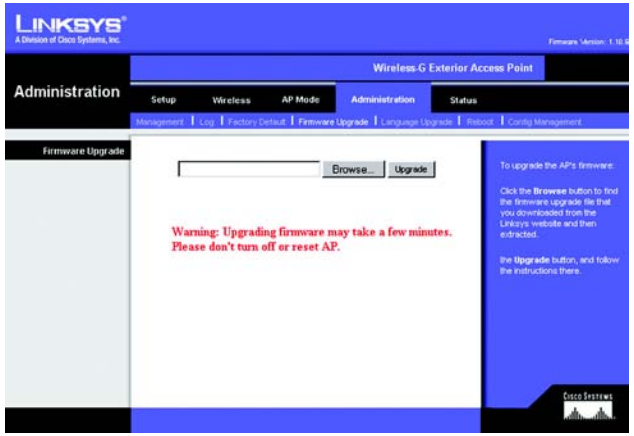

Figure C-1: Firmware Upgrade

Appendix D: Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Appendix E: Glossary

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

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

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

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

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

AES (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

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

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision **A**voidance) - A method of data transfer that is used to prevent data collisions.

CTS (**C**lear **T**o **S**end) - A signal sent by a wireless device, signifying that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

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

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**De**militarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

DSSS (**D**irect-**S**equence **S**pread-**S**pectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (**D**elivery **T**raffic **I**ndication **M**essage) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (**E**xtensible **A**uthentication **P**rotocol-**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (**E**xtensible **A**uthentication **P**rotocol-**T**ransport **L**ayer **S**ecurity) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

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

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

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

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

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

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

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

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

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

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

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

LEAP (**L**ightweight **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a username and password system.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) - The protocol used to connect to Usenet groups on the Internet.

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

OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

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

PEAP (**P**rotected **E**xtensible **A**uthentication **P**rotocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

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

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

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

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

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

Router - A networking device that connects multiple networks together.

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

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

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

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

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

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

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

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

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

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

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

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

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

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

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

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

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

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

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

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

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

Upload - To transmit a file over a network.

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

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

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

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

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

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

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

Appendix F: Specifications

Model	WAP54GPE
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3u, IEEE802.3af
Ports	Ethernet, Antenna
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, LAN, Wireless
Transmit Power	15+/-1dBm
Security Features	WEP, WPA, RADIUS
WEP Key Bits	64, 128
Dimensions (W x H x D)	6.42" x 8.07" x 2.17" (163 mm x 205 mm x 55 mm)
Unit Weight	2.5 lbs. (1.14 kg)
Power	IEEE802.3af Compliant PoE
Certifications	FCC, **ICES-003**
Operating Temp.	-20ºC to 60ºC (-4ºF to 140ºF)
Storage Temp.	-20ºC to 60ºC (-4ºF to 140ºF)

Operating Humidity	5% to 95%, Non-Condensing
Storage Humidity	5% to 95%, 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 & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

INDUSTRY CANADA (CANADA)

Operation is subject to the following two conditions: 1) This device may not cause interference and 2) This device must accept any interference, including interference that may cause undesired operation of the device.
This device has been designed to operate with an antenna having a maximum gain of 9 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that this product conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

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

EN 609 50 Safety

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Règlement d'Industry Canada
Les conditions de fonctionnement sont sujettes à deux conditions:
1)•Ce périphérique ne doit pas causer d'interférence et.
2)•Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

•IMPORTANT NOTE:
•Radiation Exposure Statement:
•This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

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

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

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

Linksys vakuuttaa täten että dieses produkt tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys déclare que le produit est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

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

France:

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

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

SAFETY NOTICES

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

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

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

Appendix I: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at: Or fax your request in to:	800-546-5797 (LINKSYS) 949-823-3002
If you experience problems with any Linksys product, you can call us at: Don't wish to call? You can e-mail us at:	800-326-7114 support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000

About This Book

This manual supplements the Antenna Installation Guides for the WAP54GPE.
The Antenna Installation Guides explain how to install and set up an outdoor antenna with the WAP54GPE hardware devices.
This guide does not explain how to erect antenna masts, nor how to install a safety grounding system. These prerequisites must be in place before installing the directional antenna.

WHO SHOULD USE THIS MANUAL

The installation of outdoor wireless links requires technical expertise. At the very least, you should be able to:

- Install and configure the network components, such as the WAP54GPE hardware.
- Understand, or have a working knowledge of, installation procedures for network operating systems using Microsoft Windows.
- Mount the outdoor antenna and surge arrestor. Antenna installation must be provided by professional installers.

WARNING!

The outdoor antennas to be used with these products are intended for mounting on an antenna tower, on a roof, or on the side of a building. Installation is not to be attempted by someone not trained or experienced in this type of work. The antenna must be installed by a suitably trained professional installation technician or by a qualified antenna installation service. The site prerequisites must be checked by a person familiar with the national electrical code and with other regulations governing this type of installation.

Local radio regulations or legislation may impose restrictions on the use of specific combinations of:

- Low-loss antenna cables and outdoor antennas
- Radio channels selected at the radios that are connected to specific outdoor antennas

Note: A basic rule for selecting a combination of cables and antennas is that no combination is allowed unless explicitly approved in the *WAP54GPE Antenna Installation Guide* for your WAP54GPE model. Therefore, always use *WAP54GPE Recommended Antennas* in combination with “Chapter 2. Determining Range and Clearance” of the appropriate *Antenna Installation Guide* to select the correct type of antenna equipment and to inform your antenna installer and LAN administrator about the impact of regulatory constraints on their job or activities.

Professional installation instruction

1. Installation personal
   This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location
   The product shall be installed at a location where the radiating antenna can be kept 20 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna,
   Use only the antennas which have been approved by Linksys. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC limit and is prohibited.

4. Installation procedure
   Please refer to user's manual for the detail.

5. Warning
   Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in US Rule CFR 47 part 15 section 15.247 & 15.407. The violation of the rule could lead to serious federal penalty.

Maximum compliance conducted power setting for antenna: Outdoor Omni Antenna with 9dBi gain

802.11b DSSS MODULATION

CHANNEL	CHANNEL FREQUENCY (MHz)	PEAK POWER OUTPUT (dBm)
1	2412	15.04
6	2437	15.09
11	2462	10.01

802.11g OFDM MODULATION

CHANNEL	CHANNEL FREQUENCY (MHz)	PEAK POWER OUTPUT (dBm)
1	2412	15.56
6	2437	16.52
11	2462	10.04