

LINKSYS®

A Division of Cisco Systems, Inc.



2.4GHz
802.11g **Wireless-G**



Access Point with
Power Over Ethernet

User Guide

Model No. **WAP54GP**

CISCO SYSTEMS



Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

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 Access Point with Power Over Ethernet 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

Chapter 1: Introduction	1
Welcome	1
What's in this User Guide?	2
Chapter 2: Planning Your Wireless Network	4
Network Topology	4
Roaming	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-G Access Point with Power Over Ethernet	6
The Front Panel	6
The Back Panel	7
Chapter 4: Connecting the Wireless-G Access Point with Power Over Ethernet	8
Overview	8
Connections for Setup	8
Placement Options	9
Chapter 5: Configuring the Wireless-G Access Point with Power Over Ethernet	10
Overview	10
Navigating the Utility	10
Accessing the Utility	12
The Setup Tab	12
The Wireless - Basic Wireless Settings Tab	14
The Wireless - Wireless Security Tab	16
The Wireless - Wireless Network Access Tab	20
The Wireless - Advanced Wireless Settings Tab	21
The AP Mode Tab	23
The Administration - Management Tab	26
The Administration - Log Tab	28
The Administration - Factory Default Tab	29
The Administration - Firmware Upgrade Tab	29
The Administration - Language Upgrade Tab	30
The Administration - Reboot Tab	30
The Administration - Config Management Tab	31
The Status - Local Network Tab	32

The Status - Wireless Tab	33
The Status - System Performance Tab	34
Appendix A: Troubleshooting	36
Frequently Asked Questions	36
Appendix B: Wireless Security	40
Security Precautions	40
Security Threats Facing Wireless Networks	40
Appendix C: Upgrading Firmware	43
Appendix D: Windows Help	44
Appendix E: Glossary	45
Appendix F: Specifications	52
Appendix G: Warranty Information	54
Appendix H: Regulatory Information	55
Appendix I: Contact Information	61

List of Figures

Figure 3-1: Front Panel	6
Figure 3-2: Back Panel	7
Figure 4-1: Connect the Ethernet Network Cable	8
Figure 4-2: Connect the Power	8
Figure 4-3: The Access Point's Stand Slots	9
Figure 4-4: The Access Point's Wall-Mount Slots	9
Figure 5-1: Login Screen	12
Figure 5-2: Setup - Automatic Configuration - DHCP Screen	12
Figure 5-3: Setup - Static IP Address Screen	13
Figure 5-4: Wireless - Basic Wireless Settings Screen	14
Figure 5-5: Wireless - Wireless Security (WPA-Personal) Screen	16
Figure 5-6: Wireless Security - WPA-Enterprise Screen	17
Figure 5-7: Wireless Security - RADIUS Screen	18
Figure 5-8: Wireless Security - WEP Screen	19
Figure 5-9: Wireless - Wireless Network Access Screen	20
Figure 5-10: Select MAC Address Screen	20
Figure 5-11: Wireless - Advanced Wireless Settings Screen	21
Figure 5-12: AP Mode Screen	23
Figure 5-13: Wireless Repeater Diagram	24
Figure 5-14: Site Survey Screen	24
Figure 5-15: Wireless Bridge Diagram	25
Figure 5-16: Administration - Management Screen	26
Figure 5-17: Administration - Log Screen	28
Figure 5-18: Administration - Factory Default Screen	29
Figure 5-19: Administration - Firmware Upgrade Screen	29
Figure 5-20: Administration - Language Upgrade Screen	30
Figure 5-21: Administration - Reboot Screen	30
Figure 5-22: Administration - Config Management Screen	31

Figure 5-23: Status - Local Network Screen	32
Figure 5-24: Status - Wireless Screen	33
Figure 5-25: Status - System Performance Screen	34
Figure C-1: Firmware Upgrade	43

Chapter 1: Introduction

Welcome

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

The Wireless-G Access Point with Power Over Ethernet also offers the convenience of Power over Ethernet (PoE) capability, so it can receive data and power over a single Ethernet network cable.

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 Access Point with Power Over Ethernet.

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

Wireless-G Access Point with Power Over Ethernet

- **Appendix I: Contact Information**

This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

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

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

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

Roaming

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

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

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

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

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

ssid: your wireless network's name

Network Layout

The Wireless-G Access Point with Power Over Ethernet 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. If you want to use Power Over Ethernet (POE), then connect the Access Point to any switch or router that complies with the POE standard (802.3af)—or you can use 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 Access Point with Power Over Ethernet

The Front Panel

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

- Power** Green. The **Power** LED lights up when the Access Point is powered on.
- Ethernet** Green. The **Ethernet** LED lights up when the Access Point is successfully connected to a device through the Ethernet network port. If the LED is flashing, the Access Point is actively sending to or receiving data from one of the devices over the Ethernet network port.
- Wireless-G** Green. The **Wireless-G** 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.



Figure 3-1: Front Panel

The Back Panel

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

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

Reset Button There are two ways to Reset the Access Point's factory defaults. Either press the **Reset** button, for approximately ten seconds, or 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.

Power Port The Power port connects to the Access Point's power adapter. (This port will not be used if you are using Power Over Ethernet.)

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



Figure 3-2: Back Panel

Chapter 4: Connecting the Wireless-G Access Point with Power Over Ethernet

Overview

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

Connections for Setup

1. Attach the Access Point's antenna.
2. Connect your Ethernet network cable to your network router or switch. Then connect the other end of the network cable to the Access Point's Ethernet port.
3. If you are using Power Over Ethernet (POE), proceed to the following section, "Placement Options."

If you are not using POE, then connect the included power adapter to the Access Point's Power port. Then plug the power adapter into an electrical outlet. The LEDs on the front panel will light up as soon as the Access Point's powers on.

Proceed to the following section, "Placement Options."



Figure 4-1: Connect the Ethernet Network Cable



Figure 4-2: Connect the Power



NOTE: The Bridge features Power Over Ethernet (POE) support. POE technology allows a POE adapter (also known as a power injector, power hub, or inline power device) to supply data and power to an Ethernet device using a single Ethernet network cable. To use the Bridge's POE feature, follow the instructions for your specific POE device.

Placement Options

There are three ways to place the Access Point. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Access Point vertically on a surface. The third way is to mount it on a wall. The stand and wall-mount options are explained in further detail below.

Stand Option

1. Near the Access Point's bottom panel are two rubber feet and two rubber inserts. Remove them to expose the stand slots you want to use.
2. The Access Point includes four triangular stands. With its rubber pad facing the bottom, insert a stand into a slot, and push the stand upward until the stand snaps into place.

Repeat this step with the other stands.

Now that the hardware installation is complete, proceed to "Chapter 5: Configuring the Wireless-G Access Point with Power Over Ethernet," for directions on how to configure the Access Point.

Wall-Mount Option

1. On one of the Access Point's side panels are four rubber feet. Remove four adjacent feet to expose the wall-mount slots you want to use. The distance between two adjacent slots is 145 mm (5.7 inches).
2. Determine where you want to mount the Access Point.
3. Drill four holes into the wall. Make sure adjacent holes are 145 mm (5.7 inches) apart.
4. Insert a screw into each hole, and leave 5 mm (0.2 inches) of its head exposed.
5. Maneuver the Router so the wall-mount slots line up with the four screws.
6. Place the wall-mount slots over the screws and slide the Access Point down until the screws fit snugly into the wall-mount slots.

Now that the hardware installation is complete, proceed to "Chapter 5: Configuring the Wireless-G Access Point with Power Over Ethernet," for directions on how to configure the Access Point.



Figure 4-3: The Access Point's Stand Slots

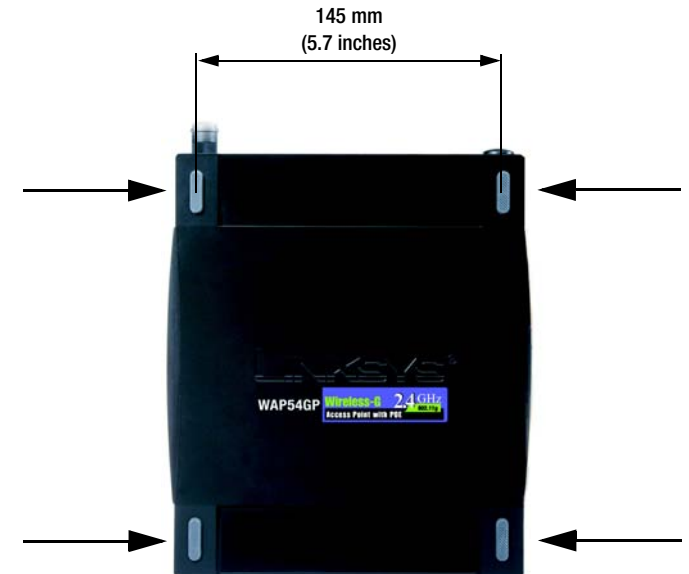


Figure 4-4: The Access Point's Wall-Mount Slots 9

Chapter 5: Configuring the Wireless-G Access Point with Power Over Ethernet

Overview

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.

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 settings for the Access Point and 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) settings, SSIDs, and other settings 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.



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.

Wireless-G Access Point with Power Over Ethernet

- *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.
- *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.
- *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.

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

firmware: the programming code that runs a networking device.

Status

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

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.

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 the Host and Device Names for the Access Point.

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

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

Network Setup

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

IP Settings

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



Figure 5-1: Login Screen

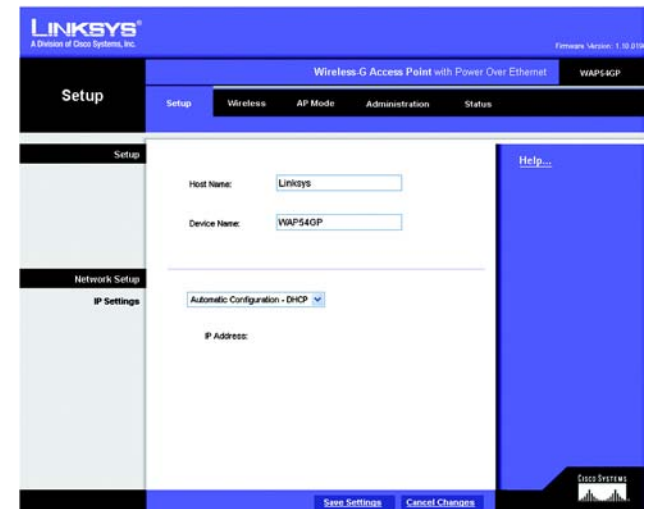


Figure 5-2: Setup - Automatic Configuration - DHCP Screen

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.
- **Default Gateway.** Enter the IP address of your network's gateway. The gateway is the device that enables communication between your computers and the Internet. In most cases, your router acts as your gateway.
- **Primary and Secondary DNS.** Enter the IP address of your Domain Name System (DNS) server. This information should be provided by your ISP. You should enter at least one DNS address.

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

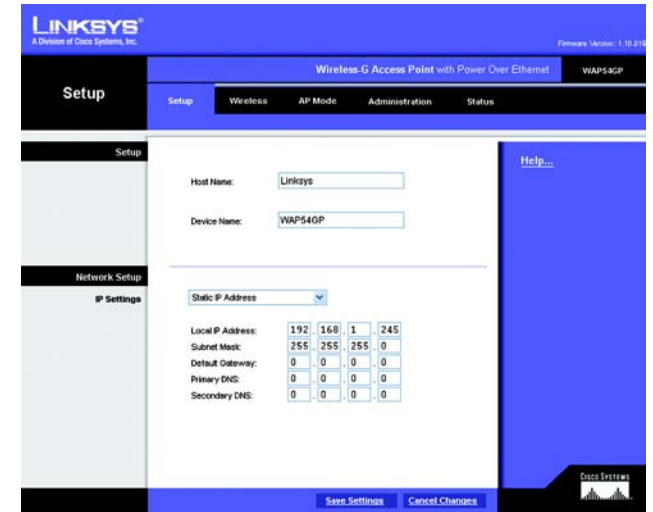


Figure 5-3: Setup - Static IP Address Screen

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.

Wireless Network

Configure the Access Point using the available settings. You can enter and save more than one configuration for the Access Point because the Access Point can work with a primary wireless network and up to seven Virtual Local Area Networks (VLANs). The Access Point can support a maximum of 32 wireless client devices.



NOTE: To use the Access Point's VLAN features, you must have a managed switch.

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 Trunk. Select **Enabled** if you want to use the Access Point's VLAN features.

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.

Main SSID. Enter settings for the Access Point's primary wireless network.

Virtual SSID1-7. You can enter settings for up to seven virtual wireless networks.

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 each wireless network.

VLAN ID. Enter the ID number you want to assign to this VLAN. Make sure at least one of these matches the Access Point VLAN ID entered on this screen.

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

TX Rate Limitation. 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-

SSID	SSID Name	VLAN ID	Priority	TX Rate Limitation
Main SSID:	linksys-g	2	Lower	54 Mbps
Virtual SSID1:		2	Lower	54 Mbps
Virtual SSID2:		2	Lower	54 Mbps
Virtual SSID3:		2	Lower	54 Mbps
Virtual SSID4:		2	Lower	54 Mbps
Virtual SSID5:		2	Lower	54 Mbps
Virtual SSID6:		2	Lower	54 Mbps
Virtual SSID7:		2	Lower	54 Mbps

Figure 5-4: Wireless - Basic Wireless Settings Screen

Fallback feature. Auto-Fallback will automatically negotiate the best possible connection speed between the Access Point and a wireless device.

Access Point VLAN ID. Enter the VLAN ID of the Access Point. Make sure this matches at least one of the VLAN IDs listed in the aforementioned table.



NOTE: You must use the Access Point VLAN ID for one of your wireless networks in order to maintain access to the Access Point's Web-based Utility.

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

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



NOTE: Only the main SSID of the Access Point can be broadcast. The Access Point cannot broadcast any of its Virtual SSIDs.

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

The Wireless - 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. For detailed instructions on configuring wireless security for the Access Point, turn to "Appendix B: Wireless Security." To disable such security, select **Disable**.

WPA-Personal

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

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.

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

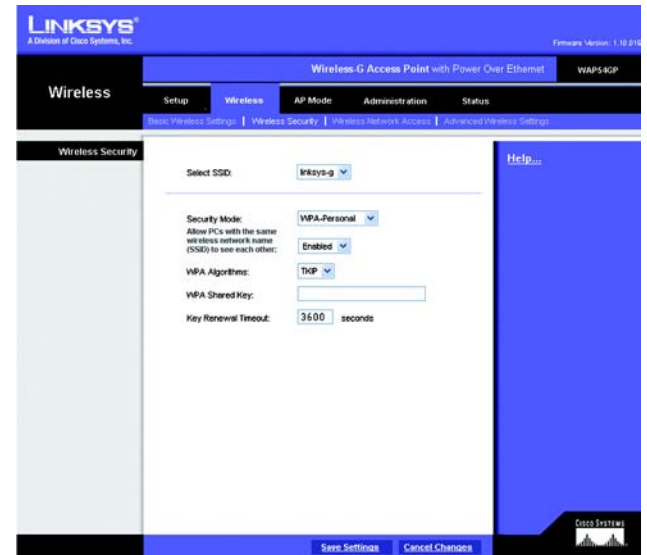


Figure 5-5: Wireless - Wireless Security (WPA-Personal) Screen

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.)

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

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**.

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.

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

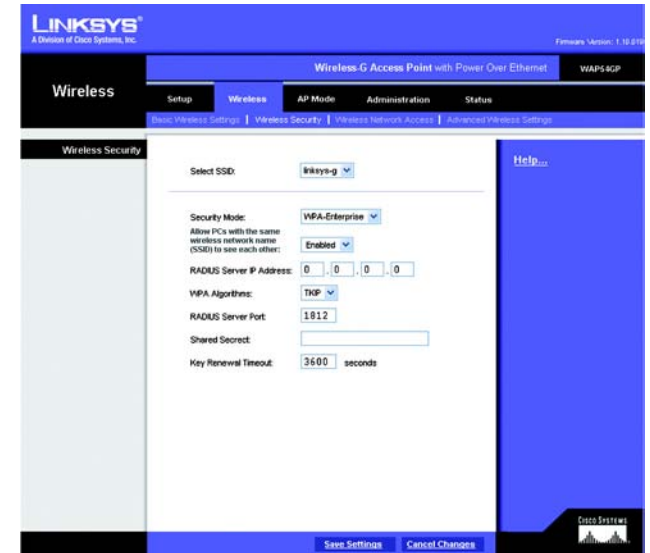


Figure 5-6: Wireless Security - WPA-Enterprise Screen

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

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

RADIUS

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

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

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

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

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

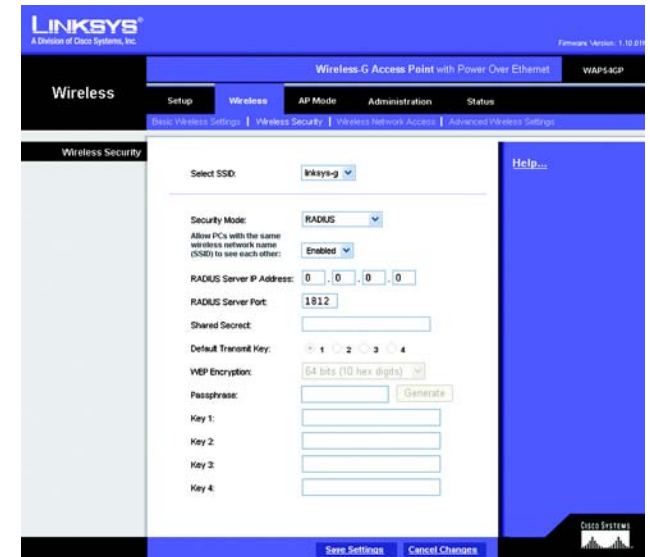


Figure 5-7: Wireless Security - RADIUS Screen

WEP

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

Allow PCs with the same wireless network name (SSID) to see each other. When enabled, devices in the same wireless network will be able to access each other, so they can transfer files through the network. To deny access, select **Disabled**. Otherwise, keep the default, **Enabled**.

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

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

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

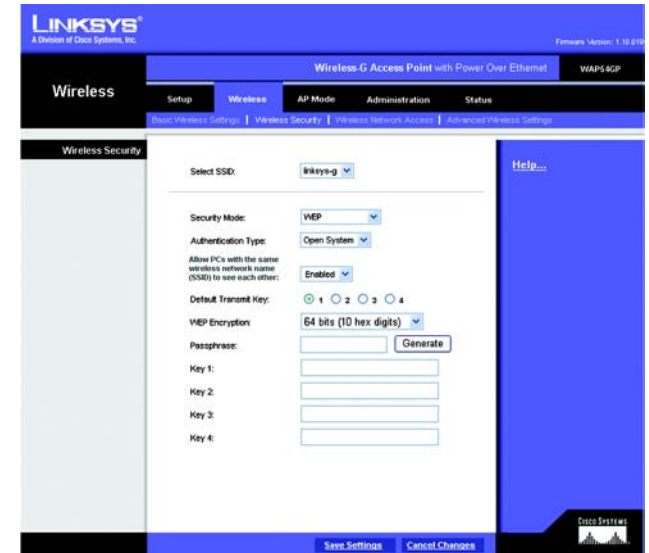


Figure 5-8: Wireless Security - WEP Screen

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.

Select MAC Address from Networked Computers. If you want to select a MAC address from a list, click this button. The MAC addresses for your computers will be automatically displayed. Click the checkboxes of the MAC addresses you want to add to your access list. Change these settings as described here and click **Apply** to apply your changes. Click **Refresh** to retrieve the latest MAC addresses. Click **Close** to close this screen and return to the *Wireless Network Access* screen.

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

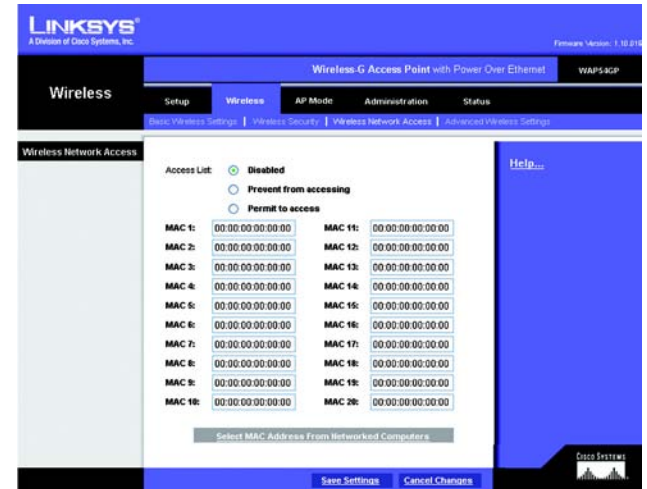


Figure 5-9: Wireless - Wireless Network Access Screen

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

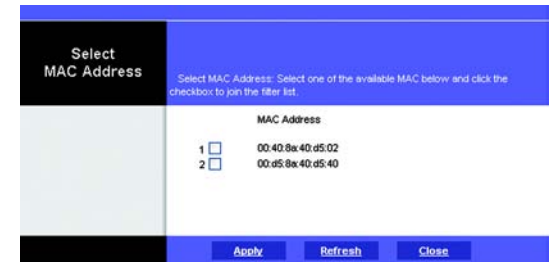


Figure 5-10: Select MAC Address Screen

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. The CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance. 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. When this feature is enabled, PCs using different SSIDs cannot see each other, so the different wireless networks are kept separate from each other. In most cases, including wireless hotspots, keep the default, **Enabled**. If you want PCs from different wireless networks to communicate, select **Disabled**.

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 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.

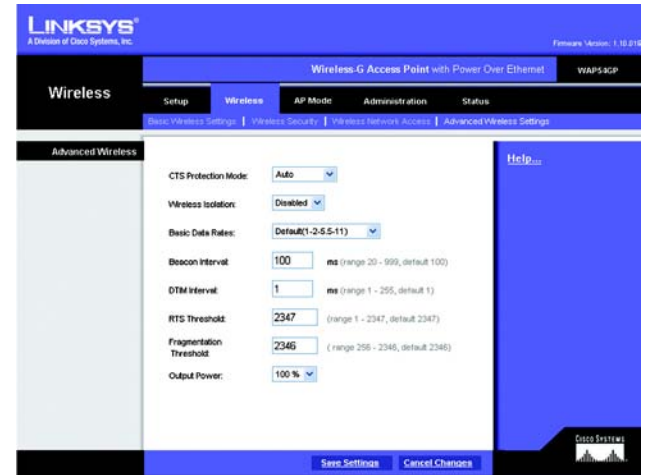


Figure 5-11: Wireless - Advanced Wireless Settings Screen

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

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

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 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. Click **Help** for more information.

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 Wireless Repeater and Wireless Bridge modes, the remote access point must be a second Linksys Wireless-G Access Point with Power Over Ethernet (model number: WAP54GP) or a Linksys Wireless-G Exterior Access Point with Power Over Ethernet (model number: WAP54GPE). 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*. Enter the MAC addresses of the repeaters in the *MAC 1-3* fields. Repeaters can be another access point or the Wireless-G Range Expander (model number: WRE54G).

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

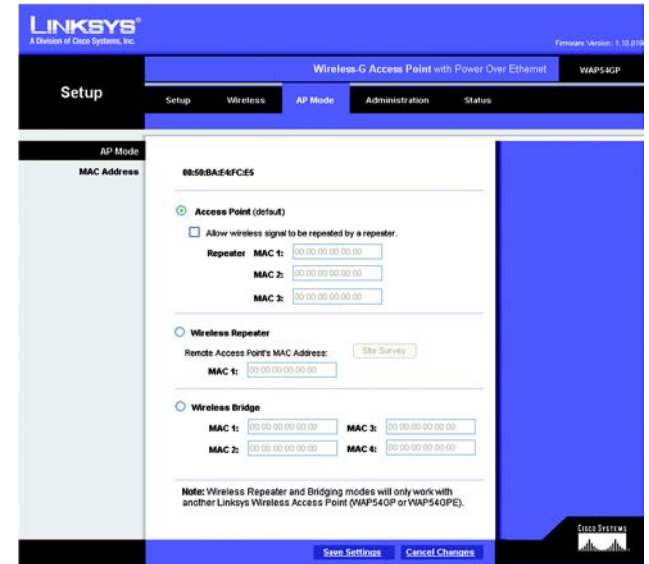


Figure 5-12: AP Mode Screen

Wireless Repeater. When set to Wireless Repeater mode, the Wireless Repeater is able to talk to up a remote access point within its range and retransmit its signal. This feature only works with the Linksys Wireless-G Exterior Access Point with Power Over Ethernet (model number: WAG54GPE) or another Wireless-G Access Point with Power Over Ethernet (model number: WAP54GP).



Figure 5-13: Wireless Repeater Diagram

To configure a Wireless Repeater environment, select **Wireless Repeater** and enter the MAC address of the remote access point in the *MAC 1* field. If you do not know the access point's MAC address, click the **Site Survey** button. Select the access point 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 search for access points again.

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



Figure 5-14: Site Survey Screen

Wireless Bridge. This mode connects two physically separated wired networks using two access points (use additional access points to connect more wired networks). This feature only works with the Linksys Wireless-G Exterior Access Point with Power Over Ethernet (model number: WAG54GPE) or another Wireless-G Access Point with Power Over Ethernet (model number: WAP54GP).



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 5-15: Wireless Bridge Diagram

To configure a Wireless Bridge environment, select **Wireless Bridge**, and enter the MAC addresses of the wireless bridges/access points in the *MAC 1-4* fields. You will also need to set the remote wireless bridges/access points to Wireless Bridge mode.

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

The Administration - Management Tab

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

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.

Web Access

Web HTTPS Access. HTTPS (HyperText Transport Protocol Secure) uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. To secure remote access of the Access Point's Web-based Utility, select **Enabled**. Otherwise, select **Disabled**.

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**.

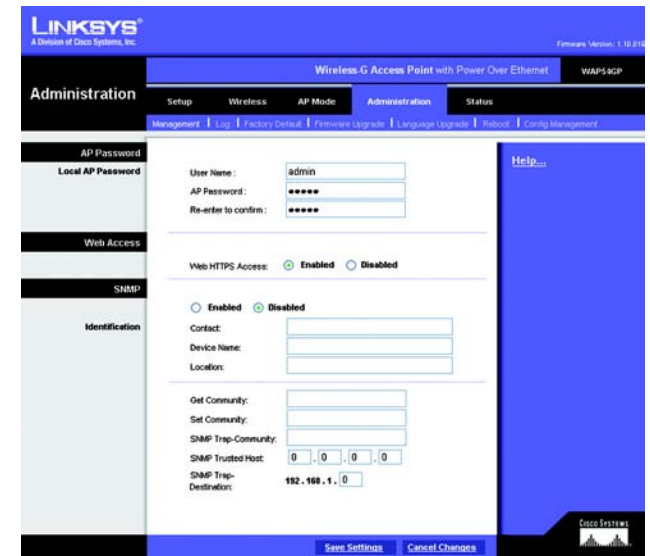


Figure 5-16: Administration - Management Screen

Wireless-G Access Point with Power Over Ethernet

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. Click **Help** for more information.

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 receive e-mail alerts when certain events occur, select **Enabled**. Otherwise, select **Disabled**.

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

Notification Queue Length

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

Log Time Threshold. Designate how often the log will be e-mailed. The default is **600** seconds (10 minutes).

Syslog Notification

Syslog is a 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**. Otherwise, select **Disabled**.

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 information about all data transmissions.

Log

Unauthorized Login Attempt. To receive alert logs about any unauthorized login attempts, click the checkbox.

System Error Messages. If you want to log system error messages, 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. Click **Help** for more information.

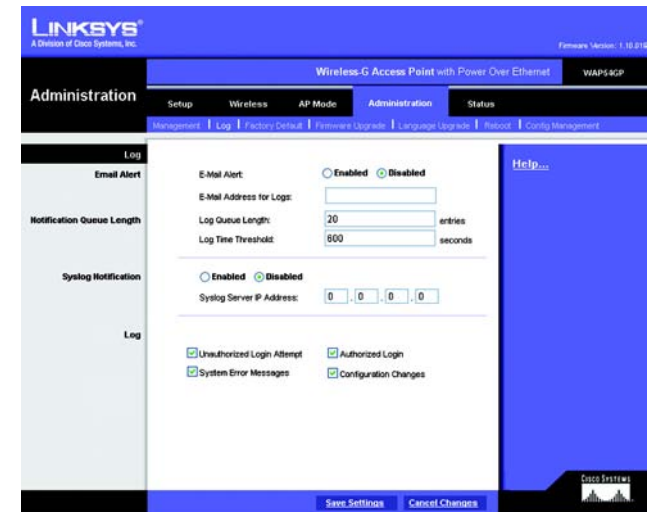


Figure 5-17: Administration - Log Screen

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.

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

The Administration - 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.

Click **Help** for more information.

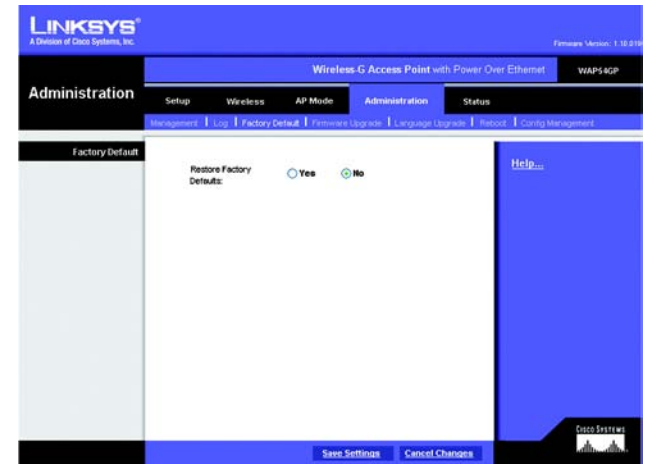


Figure 5-18: Administration - Factory Default Screen

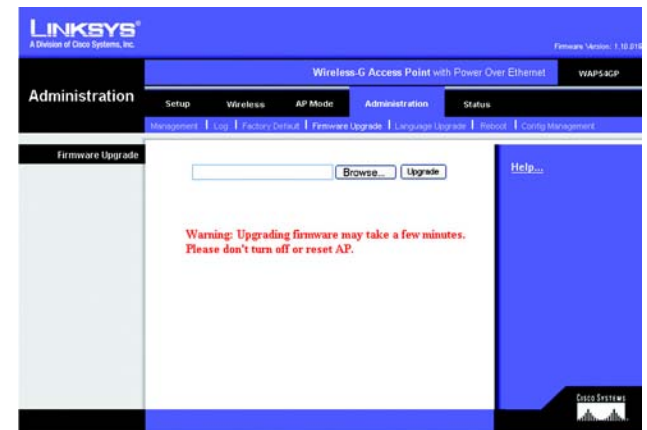


Figure 5-19: Administration - Firmware Upgrade Screen

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.

Click **Help** for more information.

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.

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

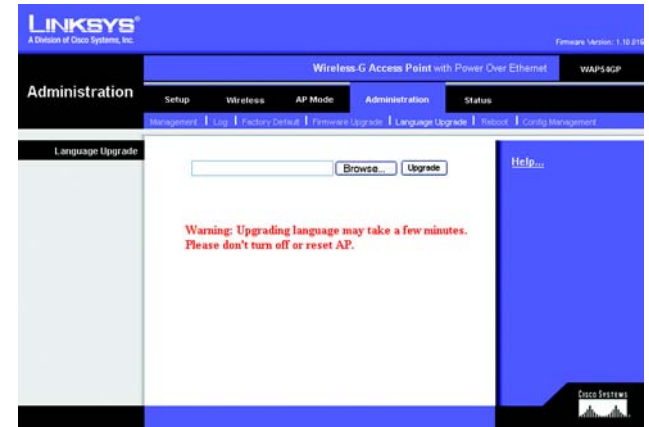


Figure 5-20: Administration - Language Upgrade Screen



NOTE: Not all languages are available. Check the Linksys website for available language upgrade files.

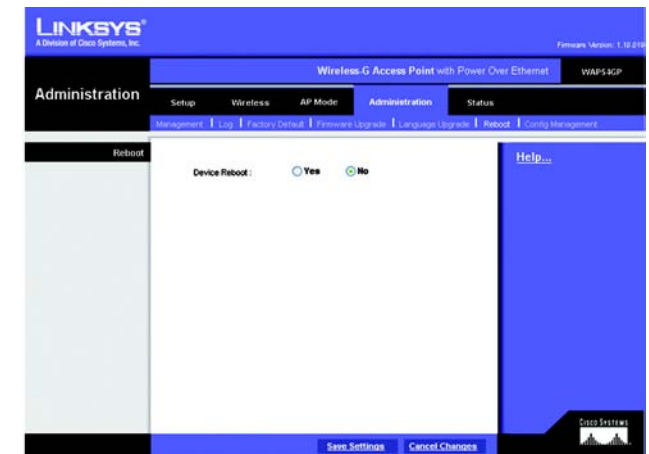


Figure 5-21: Administration - Reboot Screen

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** button.

Click **Help** for more information.

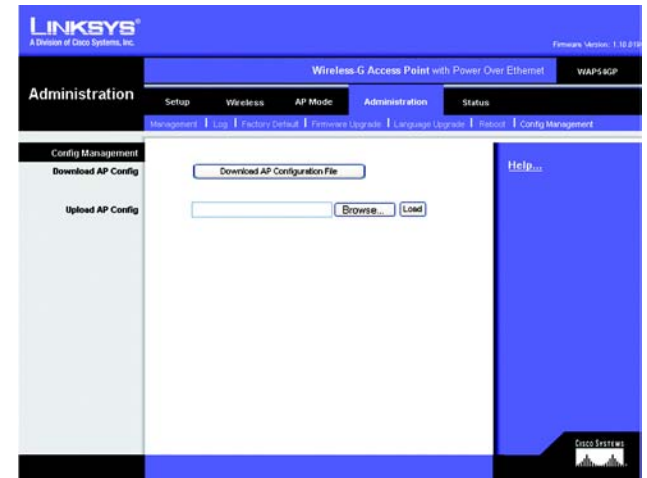


Figure 5-22: Administration - Config Management Screen

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.

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

Primary and Secondary DNS. DNS addresses used by the Access Point are displayed here.

To update the status information, click the **Refresh** button. Click **Help** for more information.

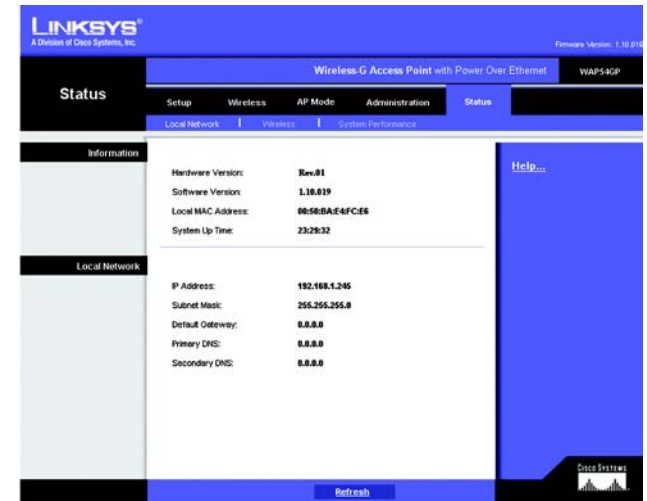


Figure 5-23: Status - Local Network Screen

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 main SSID is displayed here.

Virtual SSID1-7. The Access Point's virtual SSIDs are displayed here.

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

VLAN Trunk. The status of the Access Point's VLAN feature is shown here.

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

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

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

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

Virtual SSID1-7 Priority. The VLAN Priority settings for the virtual SSIDs are displayed here.

To update the status information, click the **Refresh** button. Click **Help** for more information.

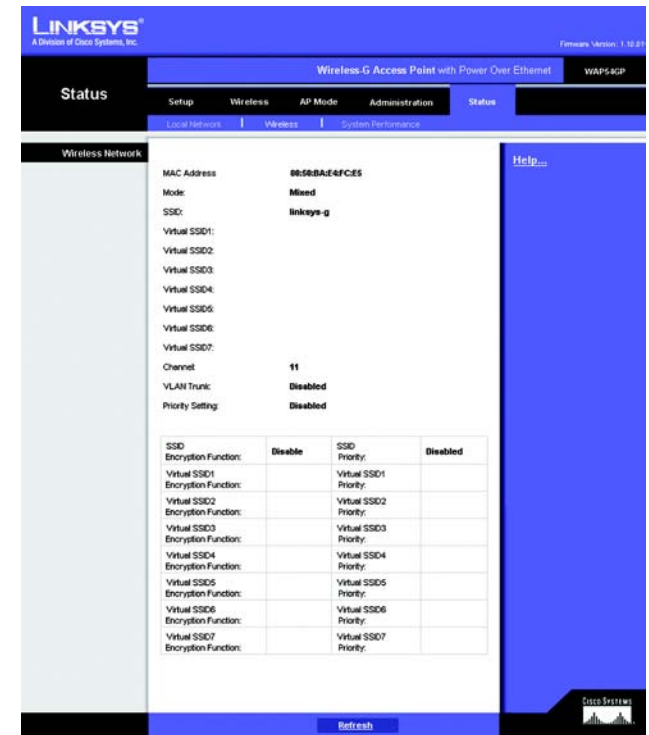


Figure 5-24: Status - Wireless Screen

The Status - System Performance Tab

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

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.

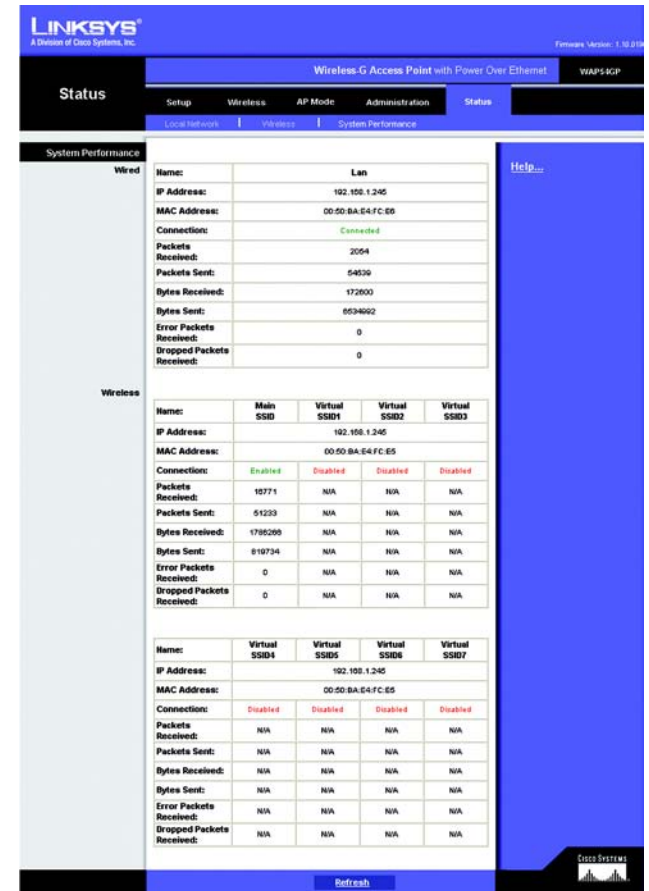


Figure 5-25: Status - System Performance Screen

Wireless-G Access Point with Power Over Ethernet

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. Click **Help** for more information.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Access Point with Power Over Ethernet. 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 to communicate continuously while its user is moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the user must make sure that the computer is set to the same channel number as the Access Point of the dedicated coverage area.

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

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

What is the ISM band?

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

What is Spread Spectrum?

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

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

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

Would the information be intercepted while transmitting on air?

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

Can Linksys wireless products support file and printer sharing?

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

What is WEP?

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

What is a MAC Address?

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

How do I avoid interference?

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

How do I reset the Access Point?

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

How do I resolve issues with signal loss?

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

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

Does the Access Point function as a firewall?

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

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

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

What is the maximum number of users the Access Point can handle?

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

Appendix B: Wireless Security

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

Security Precautions

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

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

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

Security Threats Facing Wireless Networks

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

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



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

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

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

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

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

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

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

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

There are several ways that WEP can be maximized:

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

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



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

Wireless-G Access Point with Power Over Ethernet

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.

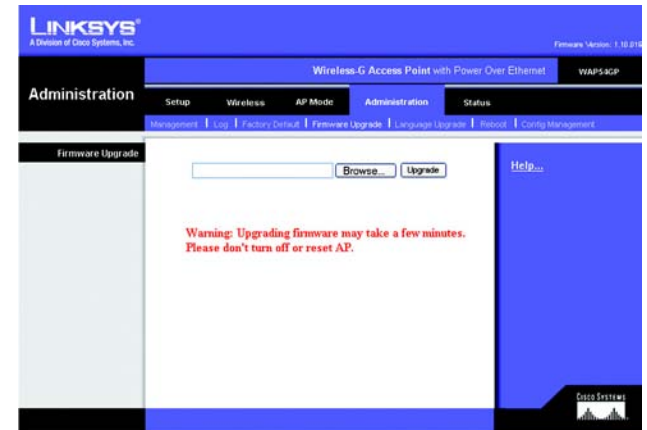


Figure C-1: Firmware Upgrade

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

802.11b - 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 (Advanced Encryption Standard) - 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

Wireless-G Access Point with Power Over Ethernet

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

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

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

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 (Dynamic Domain Name System) - 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 (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.

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

DNS (Domain Name Server) - 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 (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

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

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

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

Wireless-G Access Point with Power Over Ethernet

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - 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 (File Transfer Protocol) - 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 (HyperText Transport Protocol) - 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 (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.

Wireless-G Access Point with Power Over Ethernet

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

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

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

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

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

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

Mbps (MegaBits Per Second) - 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 (Network Address Translation) - 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 (Network News Transfer Protocol) - 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 (Orthogonal Frequency Division Multiplexing) - 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 (Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

Wireless-G Access Point with Power Over Ethernet

Ping (Packet Internet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 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 over Ethernet (PoE) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - 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 (Remote Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.

RJ-45 (Registered Jack-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 (Request To Send) - A networking method of coordinating large packets through the RTS Threshold setting.

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

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

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

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

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

SPI (Stateful Packet Inspection) 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 (Service Set Identifier) - Your wireless network's name.

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

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

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

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

TFTP (Trivial File Transfer Protocol) - 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 (Temporal Key Integrity Protocol) - 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 (User Datagram Protocol) - 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 (Uniform Resource Locator) - The address of a file located on the Internet.

Wireless-G Access Point with Power Over Ethernet

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network)- The Internet.

WEP (Wired Equivalent Privacy) - 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 (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

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

Appendix F: Specifications

Model	WAP54GP
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af
Ports	Ethernet, Antenna, Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, Ethernet, Wireless-G
Transmit Power	802.11g: 14dBm @ Normal Temp; 802.11b: 18dBm Normal Temp
Security Features	WEP, WPA, RADIUS
WEP Key Bits	64, 128
Dimensions (W x H x D)	1.26" x 7.83" x 6.89" (32 mm x 199 mm x 175 mm)
Unit Weight	1.01 lbs. (0.46 kg)
Power	12V 1A, IEEE802.3af Compliant PoE
Certifications	FCC, CE
Operating Temp.	-4° ~ 140° F (-20° ~ 60° C)
Storage Temp.	-4° ~ 140° F (-20° ~ 60° C)

Wireless-G Access Point with Power Over Ethernet

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 and your body.

Industry Canada (Canada)

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

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

Wireless-G Access Point with Power Over Ethernet

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

Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

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

Wireless-G Access Point with Power Over Ethernet

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

NOTE: The full Declaration of Conformity can be found either on the CD or a separate document included with this product.

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

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

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

CE Marking

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

CE 0560 ⓘ or CE 0678 ⓘ or CE ⓘ

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

National Restrictions

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

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

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

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

Belgium

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

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

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

France

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

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

Table 1: Applicable Power Levels in France

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

Wireless-G Access Point with Power Over Ethernet

Italy

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

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

Product Usage Restrictions

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

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

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

Power Output of Your Device

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

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

Wireless Adapters

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

Wireless-G Access Point with Power Over Ethernet

Windows XP

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

Windows 2000

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

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

Wireless Access Points, Routers, or Other Wireless Products

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

Technical Documents on www.linksys.com/international

Follow these steps to access technical documents:

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

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

Appendix I: Contact Information

Need to contact Linksys?

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

<http://www.linksys.com> or
[ftp.linksys.com](ftp://ftp.linksys.com)

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

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

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

800-326-7114
support@linksys.com

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

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

949-823-3000