



Wireless-G Business Notebook Adapter with RangeBooster

Model No. WPC200

USER GUIDE

BUSINESS SERIES

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 © 2006 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

This user guide has been designed to make understanding networking with the Notebook Adapter 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 Notebook Adapter.



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



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

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 Business Notebook Adapter	6
The LED Indicator	6
Chapter 4: Setting up and Connecting the Wireless-G Business Notebook Adapter	7
Starting the Setup	7
Connecting the Adapter	8
Setting up the Adapter	9
Chapter 5: Using the Wireless Network Monitor	19
Accessing the Wireless Network Monitor	19
Using the Wireless Network Monitors	19
Link Information	19
Profiles	22
Create a New Profile	23
Editing a Profile	32
Site Survey	41
Troubleshooting	42
Administration	42
Chapter 6: The Administrative Functions in the Wireless Network Monitor	45
Accessing the Wireless Network Monitor	45
Using the Administrative Functions in the Wireless Network Monitor	45
Classification	46
Security Monitor	49
Appendix A: Troubleshooting	61
Common Problems and Solutions	61
Frequently Asked Questions	62
Appendix B: Windows XP Wireless Zero Configuration	66

Windows XP Wireless Zero Configuration	66
Appendix C: Wireless Security	69
Security Precautions	69
Security Threats Facing Wireless Networks	69
Appendix D: Windows Help	72
Appendix E: Glossary	73
Appendix F: Specifications	78
Appendix G: Warranty Information	80
Appendix H: Regulatory Information	81
Appendix I: Contact Information	88

List of Figures

Figure 3-1: LEDs	6
Figure 4-1: Setup Wizard's Welcome Screen	7
Figure 4-2: Setup Wizard's License Agreement	7
Figure 4-3: Connecting the Adapter	8
Figure 4-4: Available Wireless Network	9
Figure 4-5: WEP	10
Figure 4-6: WPA - Personal	10
Figure 4-7: WPA2 - Personal	11
Figure 4-8: Confirm New Settings	11
Figure 4-9: Link Information	11
Figure 4-10: Creating a Profile	12
Figure 4-11: Network Settings - Wireless Mode	12
Figure 4-12: Ad-Hoc Mode Settings	13
Figure 4-13: Wireless Security - WEP	13
Figure 4-14: Wireless Security - WPA Personal	14
Figure 4-15: Wireless Security - WPA2 Personal	14
Figure 4-16: Wireless Security - WPA Enterprise-EAP-TLS	15
Figure 4-17: Wireless Security - WPA Enterprise-PEAP	15
Figure 4-18: Wireless Security - WPA2 Enterprise-EAP	16
Figure 4-19: Wireless Security - WPA2 Enterprise-PEAP	16
Figure 4-20: Wireless Security - RADIUS - EAP-TLS	17
Figure 4-21: Wireless Security - RADIUS - PEAP	17
Figure 4-22: Wireless Security - LEAP	18
Figure 4-23: Congratulations Screen	18
Figure 5-1: Wireless Network Monitor Icon	19
Figure 5-2: Link Information - Connection	19
Figure 5-3: Link Information - Wireless Network Status	20
Figure 5-4: Link Information - Wireless Network Statistics	21
Figure 5-5: Profiles	22
Figure 5-6: Import a Profile	22
Figure 5-7: Export a Profile	22
Figure 5-8: Creating a Profile - Available Wireless Network	23

Figure 5-9: Creating a Profile - WEP Key Needed	23
Figure 5-10: Creating a Profile - WPA-Personal	24
Figure 5-11: Creating a Profile - Congratulations	24
Figure 5-12: Creating a Profile - Manual Setup - Network Settings	25
Figure 5-13: Creating a Profile - Manual Setup - Wireless Mode	25
Figure 5-14: Creating a Profile - Manual Setup - Wireless Security - Disabled	26
Figure 5-15: Creating a Profile - Manual Setup - Wireless Security - WEP	26
Figure 5-16: Creating a Profile - Manual Setup - Wireless Security - WPA Personal	27
Figure 5-17: Creating a Profile - Manual Setup - Wireless Security - WPA2 Personal	27
Figure 5-18: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS	28
Figure 5-19: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - PEAP	28
Figure 5-20: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS	29
Figure 5-21: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - PEAP	29
Figure 5-22: Creating a Profile - Manual Setup - Wireless Security - RADIUS - EAP-TLS	30
Figure 5-23: Creating a Profile - Manual Setup - Wireless Security - RADIUS - PEAP	30
Figure 5-24: Creating a Profile - Manual Setup - Wireless Security - LEAP	31
Figure 5-25: Creating a Profile - Manual Setup - Confirm New Settings	31
Figure 5-26: Creating a Profile - Manual Setup - Congratulations	32
Figure 5-27: Editing a Profile	32
Figure 5-28: Editing a Profile - Wireless Mode	33
Figure 5-29: Editing a Profile - Ad Hoc Mode	33
Figure 5-30: Editing a Profile - Wireless Security	34
Figure 5-31: Editing a Profile - Wireless Security - WEP	34
Figure 5-32: Editing a Profile - Wireless Security - WPA Personal	35
Figure 5-33: Editing a Profile - Wireless Security -WPA2 Personal	35
Figure 5-34: Editing a Profile - Wireless Security - WPA Enterprise - EAP-TLS	36
Figure 5-35: Editing a Profile - Wireless Security - WPA Enterprise - PEAP	36
Figure 5-36: Editing a Profile - Wireless Security -WPA2 Enterprise - EAP-TLS	37
Figure 5-37: Editing a Profile - Wireless Security - WPA2 Enterprise - PEAP	37
Figure 5-38: Editing a Profile - Wireless Security - RADIUS - EAP-TLS	38
Figure 5-39: Editing a Profile - Wireless Security - RADIUS - PEAP	38
Figure 5-40: Editing a Profile - Wireless Security - LEAP	39
Figure 5-41: Editing a Profile - Network Settings	39
Figure 5-42: Editing a Profile - Confirm New Settings	40

Figure 5-43: Editing a Profile - Congratulations	40
Figure 5-44: Site Survey	41
Figure 5-45: Troubleshooting	42
Figure 5-46: Administration	42
Figure 5-47: Administration - Login Access Point Account	43
Figure 5-48: Administration - Modify Access Point Account	43
Figure 5-49: Administration - Security Monitor Account	44
Figure 6-1: Wireless Network Monitor Icon	45
Figure 6-2: Administration - Login Security Monitor Administration - Login Security Monitor Account	45
Figure 6-3: Classification	46
Figure 6-4: AP Classification	46
Figure 6-5: Client Classification	47
Figure 6-6: Trusted Mac Address	47
Figure 6-7: Allowed Vendor List Configuration	48
Figure 6-8: Allowed SSID Configuration	48
Figure 6-9: Allowed Channel Configuration	49
Figure 6-10: Security Monitor - Channel Usage	49
Figure 6-11: Security Monitor - AP Inventory	50
Figure 6-12: Security Monitor - Client Inventory	50
Figure 6-13: Security Monitor - Alerts Summary	51
Figure 6-14: Security Monitor - POP-UP Alert	51
Figure 6-15: Security Monitor - Alert List	52
Figure 6-16: Alert Details	52
Figure 6-17: Security Monitor - Alert Advice	53
Figure 6-18: Security Monitor - Windows Firewall Screen	60
Figure B-1: Wireless Network Monitor Icon	66
Figure B-2: Windows XP - Use Windows XP Wireless Configuration	66
Figure B-3: Windows XP Wireless Zero Configuration Icon	66
Figure B-4: Available Wireless Network	67
Figure B-5: No Wireless Security	67
Figure B-6: Network Connection - Wireless Security	68

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Business Notebook Adapter. Setting up your network and your Wireless-G Business Notebook Adapter is easier than ever.

The Wireless-G Notebook Adapter is the simple way to add or upgrade wireless connectivity in your computer. Just install it into your computer's Card slot and enjoy incredible high-speed wireless network access while not having to run cable wires.

RangeBooster technology increases your wireless network's range up to two times, and its throughput by up to 35%. Unlike ordinary wireless technologies that are confused by signal reflections, RangeBooster uses two smart receivers at each end to detect and decode reflected signals at distances where standard technologies give up. You'll find that "dead spots" in the wireless coverage area are reduced, too.

But what does all of this mean?

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.

Once you're connected, you can keep in touch with your e-mail, access the Internet, and share files and other resources such as printers and network storage with other computers on the network, wherever your work takes you, without cables.

The Advanced security features makes this solution ideal for your business. Advanced wireless security using Wi-Fi Protected Access™ (WPA2 Enterprise) with up to 256-bit encryption, and the new Wireless Security Monitoring functionality gives your business the visibility and protection it needs. When used with a Linksys WAP200, the Wireless Security Monitoring alerts you of possible wireless intruders and vulnerabilities in the wireless network deployment.

The included Setup Wizard walks you through configuring the Adapter to your wireless network settings, step by step. Use the instructions in this Guide to help you set up and connect the Adapter using the Setup Wizard. These instructions should be all you need to get the most out of the Adapter.

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

network: a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

802.11g: a wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

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

encryption: encoding data transmitted in a network

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Business Notebook Adapter.

- **Chapter 1: Introduction**
This chapter describes the Adapter's applications and this User Guide.
- **Chapter 2: Planning Your Wireless Network**
This chapter discusses a few of the basics about wireless networking.
- **Chapter 3: Getting to Know the Wireless-G Business Notebook Adapter**
This chapter describes the physical features of the Adapter.
- **Chapter 4: Setting up and Connecting the Wireless-G Business Notebook Adapter**
This chapter instructs you on how to install and configure the Adapter.
- **Chapter 5: Using the Wireless Network Monitor**
This chapter shows you how to use the Adapter's Wireless Network Monitor.
- **Chapter 6: Administration Functions in the Network Monitor**
This chapter shows you how to use the administration features of the Adapter's Wireless Network Monitor.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Adapter.
- **Appendix B: Windows XP Zero Configuration**
This appendix describes how to use the Windows XP Zero Configuration.
- **Appendix C: Wireless Security**
This appendix discusses security issues regarding wireless networking and measures you can take to help protect your wireless network.
- **Appendix D: Windows Help**
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix E: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix F: Specifications**
This appendix provides the Adapter's technical specifications.

Wireless-G Business Notebook Adapter with RangeBooster

- **Appendix G: Warranty Information**
This appendix supplies the Adapter's warranty information.
- **Appendix H: Regulatory Information**
This appendix supplies the Adapter's regulatory information.
- **Appendix I: Contact Information**
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning your Wireless Network

Network Topology

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

Linksys wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and can 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 can 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, if they both share the same channel and SSID.

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

topology: the physical layout of a network.

access point: a device that allows wireless-equipped computers and other devices to communicate with a wired network

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

Linksys wireless access points and wireless routers have been designed for use with 802.11a, 802.11b, and 802.11g products. With 802.11g products communicating with the 802.11b standard and some products incorporating both “a” and “g”, products using these standards can communicate with each other.

Access points and wireless routers are compatible with 802.11a, 802.11b and 802.11g adapters, such as the PC Cards for your laptop computers, PCI Cards for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity.

When you wish to connect your wired network with your wireless network, the network ports on the access points and wireless routers can be connected to Linksys switches or routers.

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

Chapter 3: Getting to Know the Wireless-G Business Notebook Adapter

The LED Indicator

The Notebook Adapter's LEDs display information about network activity.

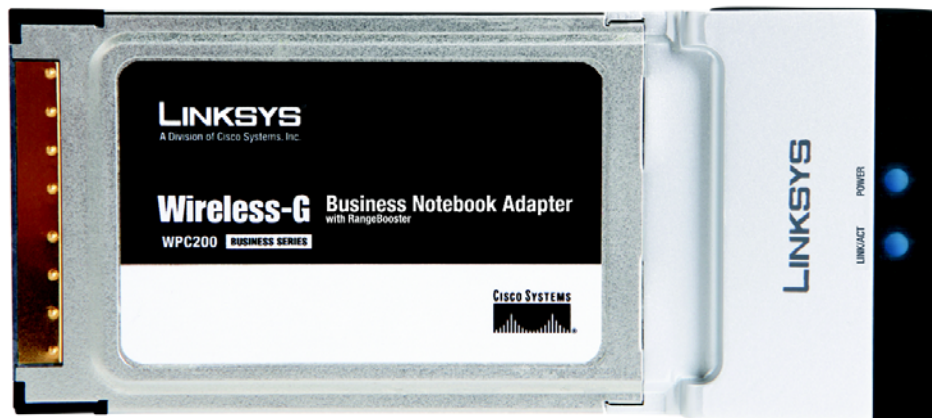


Figure 3-1: LEDs

- Power** *Blue.* The Wireless LED lights up when the Adapter is powered on.
- Link/Act** *Blue.* The Link/Act LED lights up when the Adapter has an active connection.

Chapter 4: Setting up and Connecting the Wireless-G Business Notebook Adapter

Starting the Setup

The Wireless-G Business Notebook Adapter Setup Wizard will guide you through the installation procedure. The Setup Wizard will install the driver and Wireless Network Monitor, as well as connect and configure the Adapter.



IMPORTANT: Do not connect the Adapter until you are instructed to do so or the setup will not work correctly.

Insert the **Setup Wizard CD-ROM** into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if “D” is the letter of your CD-ROM drive).

On the *Welcome* screen, you have the following choices:

Click Here to Start- Click the **Click Here to Start** button to begin the software installation process.

User Guide - Click the **User Guide** button to open the PDF file of this User Guide.

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

1. To install the Adapter, click the **Click Here to Start** button on the *Welcome* screen.
2. After reading the License Agreement, click the **Next** button if you agree and want to continue the installation, or click the **Cancel** button to end the installation.
3. Windows will begin copying the files onto your PC.



Figure 4-1: Setup Wizard's Welcome Screen



Figure 4-2: Setup Wizard's License Agreement

Connecting the Adapter

1. Locate an available CardBus slot on your notebook PC.
2. With the connector pin end facing the CardBus slot and the label facing up, slide the Adapter into the CardBus slot until it locks in place.
3. Windows will begin copying the driver files to your computer. If Windows asks you for the original Windows CD-ROM, insert the CD-ROM, and direct Windows to its correct location (e.g., D:\).
4. Then, click **Next**. It may take a minute for the next screen to appear.
5. Windows 98 and Windows Me users may need to restart their PCs again when prompted to do so. The Power LED should light up when the Adapter is installed correctly.



Figure 4-3: Connecting the Adapter

Setting up the Adapter

The next screen to appear will be the *Available Wireless Network* screen.

This screen provides two options for setting up the Adapter.

- **Available Wireless Network. (For most users.)** Use this option if you already have a network set up. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for Advanced Users only.

The setup for each option is described, step by step, under the appropriate heading on the following pages.

Click **Exit** to close the Setup Wizard, if you wish to set up the Adapter later.

Available Wireless Network

The available networks are listed in the table on the center of the screen by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If you do not see your network listed, you can click the **Refresh** button to bring the list up again.) If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If you have wireless security enabled on your network, continue to step 2. Only *One* of these security screens will be shown. If you don't have wireless security enabled, continue to step 3.

2. Wireless Security

If your network has WEP, WPA-Personal, or WPA2-Personal wireless security enabled, then that security screen will appear. Continue to the screen for your wireless security.



Figure 4-4: Available Wireless Network

WEP

If your network has the wireless security WEP (Wired Equivalent Privacy), RADIUS or LEAP enabled, this screen will appear. For connecting with RADIUS or LEAP, click **Connect**, then continue to the next section “Manual Setup” on page 12.

Security - Select **WEP**.

WEP - Select **64-bit** or **128-bit**.

Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Then click **Connect** and proceed to Step 3.

WPA-Personal

If your network has the wireless security WPA-Personal (Wi-Fi Protected Access) enabled, this screen will appear.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.

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

encryption: encoding data transmitted in a network.

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.

The screenshot shows the 'WEP Key Needed for Confirmation' screen. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC200'. Below that, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main heading is 'WEP Key Needed for Confirmation'. The text below reads: 'This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then click the Connect button.' There are three input fields: 'Security' (a dropdown menu set to 'WEP'), 'WEP' (a dropdown menu set to '64-bit'), and 'Passphrase' (a text input field). Below these is a 'WEP Key 1' input field. To the right of the 'Security' dropdown, there is a note: 'Please select the method used by your existing wireless network.' To the right of the 'WEP' dropdown, there is a note: 'To use WEP encryption, select 64-bit or 128-bit.' To the right of the 'Passphrase' field, there is a note: 'The Passphrase is case-sensitive and should be no more than 16 characters in length.' To the right of the 'WEP Key 1' field, there is a note: 'When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".' At the bottom right, there are 'Cancel' and 'Connect' buttons.

Figure 4-5: WEP

The screenshot shows the 'WPA-Personal Configuration' screen. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC200'. Below that, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main heading is 'WPA-Personal Configuration'. The text below reads: 'This wireless network has WPA-Personal, also known as Pre-Shared Key, enabled. Enter the required passphrase in the field below. Then click the Connect button.' There is one input field labeled 'Passphrase'. To the right of this field, there is a note: 'Please enter a Passphrase that is 8 to 63 characters in length.' At the bottom right, there are 'Cancel' and 'Connect' buttons.

Figure 4-6: WPA - Personal

WPA2-Personal

If your network has the wireless security WPA2-Personal enabled, this screen will appear.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.



Figure 4-7: WPA2 - Personal

3. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.

4. After the software has been successfully installed, the *Link Information* screen will appear.

For more information about the Wireless Network Monitor, refer to *Chapter 5: Using the Wireless Network Monitor*.



Figure 4-8: Confirm New Settings

Congratulations! The installation of the Wireless-G Business Notebook Adapter is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, proceed to *Chapter 5: Using the Wireless Network Monitor*.



Figure 4-9: Link Information

Manual Setup

If your network is not listed with the available networks, you can use Manual Setup.

1. Click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.
2. The *Network Settings* screen from the Wireless Network Monitor will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

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

3. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

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

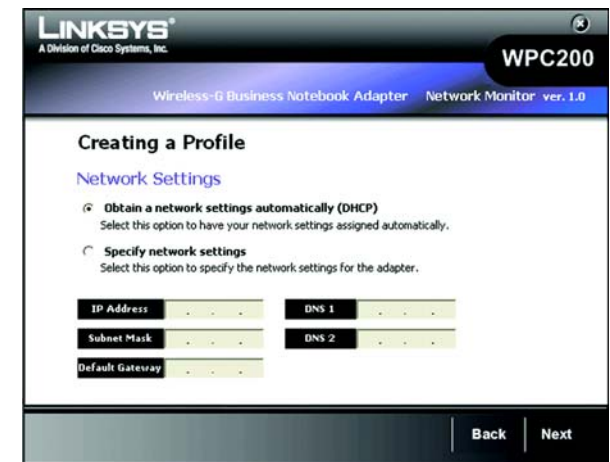


Figure 4-10: Creating a Profile



Figure 4-11: Network Settings - Wireless Mode

- If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.

- If your wireless network does not have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 6.

If your wireless network has wireless security, select the method of security used: **WEP**, **WPA/WPA2-Personal**, **WPA/WPA2-Enterprise**, **RADIUS**, or **LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP - Select **64-bit** or **128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.



Figure 4-12: Ad-Hoc Mode Settings

encryption: encoding data transmitted in a network.

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



Figure 4-13: Wireless Security - WEP

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

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

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

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

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

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

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.

wpa2 offers a stronger encryption than wpa by using the AES (Advanced Encryption Standard) which is a block cipher with block sizes of 128, 192 or 256 bits.

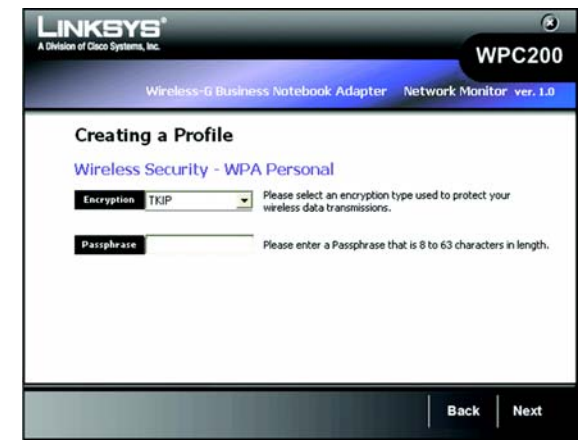


Figure 4-14: Wireless Security - WPA Personal



Figure 4-15: Wireless Security - WPA2 Personal

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method can be used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS


If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

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



The screenshot shows the 'LINKSYS' logo at the top left, 'WPC200' at the top right, and 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0' in the header. The main content area is titled 'Creating a Profile' and 'Wireless Security - WPA Enterprise'. It features a form with the following fields: 'Authentication' (EAP-TLS), 'Login Name', 'Server Name', 'Certificate', and 'Encryption' (AES). Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Server Name used for authentication. (Optional)', 'Please select the certificate used for authentication.', and 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-16: Wireless Security - WPA Enterprise-EAP-TLS



The screenshot shows the 'LINKSYS' logo at the top left, 'WPC200' at the top right, and 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0' in the header. The main content area is titled 'Creating a Profile' and 'Wireless Security - WPA Enterprise'. It features a form with the following fields: 'Authentication' (PEAP), 'Login Name', 'Password', 'Server Name', 'Inner Authen.' (EAP-MSCHAPv2), and 'Encryption' (AES). Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Password used for authentication.', 'Enter the Server Name used for authentication. (Optional)', 'Please select the inner authentication method used inside the PEAP tunnel.', and 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-17: Wireless Security - WPA Enterprise-PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, Trust Any. Then select the authentication method used inside the PEAP tunnel.

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

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. The 'Login Name' field is empty. The 'Server Name' field is empty. The 'Certificate' dropdown is set to 'Trust Any'. The 'Encryption' dropdown is set to 'AES'. The 'Back' and 'Next' buttons are visible at the bottom right.

Figure 4-18: Wireless Security - WPA2 Enterprise-EAP

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. The 'Login Name' field is empty. The 'Password' field is empty. The 'Server Name' field is empty. The 'Inner Authen:' dropdown is set to 'EAP-MSCHAPv2'. The 'Encryption' dropdown is set to 'AES'. The 'Back' and 'Next' buttons are visible at the bottom right.

Figure 4-19: Wireless Security - WPA2 Enterprise-PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel.

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

The screenshot shows the 'Creating a Profile' page for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'EAP-TLS'. Below it are fields for 'Login Name', 'Server Name', and 'Certificate'. The 'Certificate' dropdown is also visible. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-20: Wireless Security - RADIUS - EAP-TLS

The screenshot shows the 'Creating a Profile' page for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'PEAP'. Below it are fields for 'Login Name', 'Password', 'Server Name', and 'Inner Authen.'. The 'Inner Authen.' dropdown is set to 'EAPMSCHAPV2'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-21: Wireless Security - RADIUS - PEAP

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a user name and password based system.

Login method - Select the login method your network is using, **Manual Login** or **Windows Login**.

If you select manual login, enter the username and password in the username and password field accordingly. Enter the password again in the confirm field.

6. The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings and return to the *Link Information* screen. Click **Return to Profile screen** to return to the Creating a Profile screen.

Congratulations! Your manual setup through the Wireless Network Monitor is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, proceed to Chapter 5: Using the Wireless Network Monitor.



The screenshot shows the Linksys WPC200 Wireless-G Business Notebook Adapter Network Monitor interface. The page title is "Creating a Profile" and the sub-section is "Wireless Security - LEAP". There are three input fields: "User Name" with the instruction "Enter the Login Name used for authentication.", "Password" with "Enter the Password used for authentication.", and "Confirm" with "Re-enter the Password again.". At the bottom right, there are "Back" and "Next" buttons.

Figure 4-22: Wireless Security - LEAP



Figure 4-23: Congratulations Screen

Chapter 5: Using the Wireless Network Monitor

Use the Wireless Network Monitor to check the link information, set up profiles of your wireless settings, search for available wireless networks, troubleshoot your wireless connections, or administer the accounts that hold privileges to access the Security Monitor.

Accessing the Wireless Network Monitor

After installing the Adapter, the Wireless Network Monitor icon will appear in the system tray of your computer. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.



Figure 5-1: Wireless Network Monitor Icon

Using the Wireless Network Monitors

The opening screen of the Wireless Network Monitor is the **Link Information** screen. From this screen, you can find out how strong the current wireless signal is and how good the connection's quality is. You can also perform configuration changes or create connection profiles by clicking the **Profiles** tab. To view the available wireless networks, click the **Site Survey** tab. To troubleshoot the current connections or view the FAQ pages, click the **Troubleshooting** tab. To perform the administrative tasks of the account information or specify email alert addresses, click the **Administration** tab.

Link Information

The *Connection* screen of the Link Information tab displays signal strength and link quality information of the current connection. It also provides tabs to click for additional connection information.

Signal Strength - The Signal Strength bar indicates signal strength from low to high; low is red, medium is yellow and high is green.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection from low to high; low is red, medium is yellow and high is green.

Click the **Status** or **Statistics** tabs to view additional information about the wireless network connection.

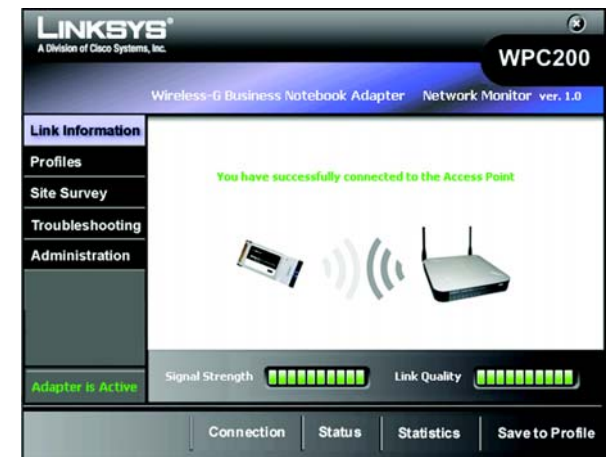


Figure 5-2: Link Information - Connection

Status

Click the **Status** tab to view the *Wireless Network Status* screen. The *Status* screen provides information on your current network settings.

Status- This shows the status of the connection.

SSID - Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN. This is the unique name used to identify a network.

Wireless Mode - The mode of the wireless network currently in use is displayed here.

Transfer Rate - This shows the speed at which your wireless network transmits.

Channel - This displays the channel used by your network.

Security - The status of the wireless security feature is displayed here.

Authentication - This is your wireless network's authentication method.

IP Address - The IP Address of the Adapter is displayed here.

Subnet Mask - The Subnet Mask of the Adapter is shown here.

Default Gateway - The Default Gateway address of the Adapter is displayed here.

DNS - This is the DNS (Domain Name Service) address of the Adapter.

DHCP - This shows the status of the DHCP server.

MAC Address- The MAC address of the wireless network's access point or wireless router is shown here.

Click the **Statistics** tab to view the *Wireless Network Statistics* screen. Click the **Connection** button to return to the initial *Link Information* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile.



Figure 5-3: Link Information - Wireless Network Status

Statistics

The *Statistics* screen provides statistics on your current network settings.

Transmit Rate - This is the data transfer rate of the current connection. (In Auto mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)

Receive Rate - This is the rate at which data is received.

Packets Received - This shows the packets received by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Packets Transmitted - This shows the packets transmitted from the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Bytes Received - This shows the bytes received by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Bytes Transmitted - This shows the bytes transmitted by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Driver Version - This shows the version of the Adapter's driver.

Signal Strength - This is the intensity of the wireless signal received by the Adapter.

Transmit Power - This is the power at which the Adapter transmits.

Total Up Time - This indicates the cumulative total of the Adapter's connection time.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Connection** button to return to the initial *Link Information* screen. Click the **Status** button to go to the *Wireless Network Status* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile. Click the **Clear Counters** button to reset the statistics counter.

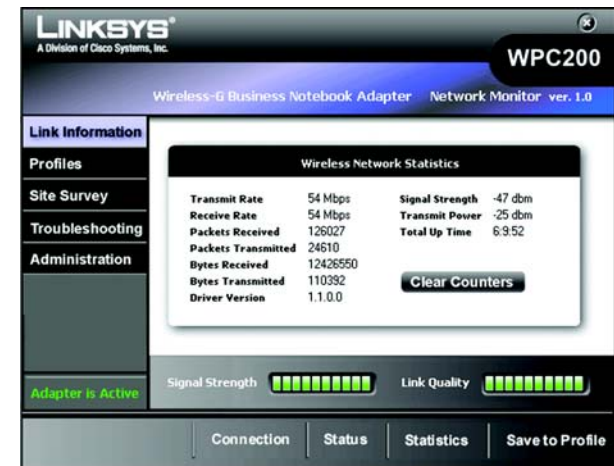


Figure 5-4: Link Information - Wireless Network Statistics

Profiles

The *Profiles* screen lets you save different configuration profiles for different network setups. The table on the left displays a list of available profiles with their profile names and SSIDs.

Profile - The name of the profile is displayed here.

SSID - The SSID or unique name of the wireless network is displayed here.

Profile Information

For each profile selected, the following are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Transfer Rate - The data transfer rate of the current connection is shown here.

Channel - This is the channel to which the wireless network devices are set.

Authentication - The authentication setting for the network is shown here.

Encryption - The status of the wireless security feature is displayed here.

Connect - To connect to a wireless network using a specific profile, select the profile, and click **Connect**.

New - Click the **New** button to create a new profile. See the next section, “Create a New Profile,” for detailed instructions.

Edit - Select the profile you want to change, and then click the **Edit** button. See the section, “Edit a New Profile,” for detailed instructions.

Import - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file, and click the **Open** button.

Export - Select the profile you want to save in a different location, and click the **Export** button. Direct Windows to the appropriate folder, and click the **Save** button.

Delete - Select the profile you want to delete, and then click the **Delete** button.



NOTE: If you want to export more than one profile, you must export them one at a time.

NOTE: The default profile cannot be deleted.

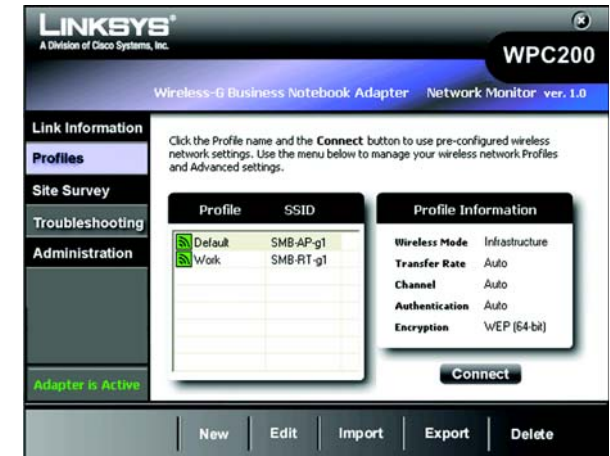


Figure 5-5: Profiles



Figure 5-6: Import a Profile

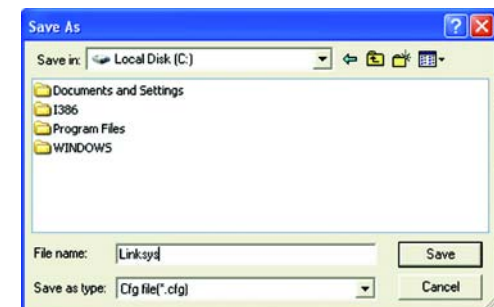


Figure 5-7: Export a Profile

Create a New Profile

When you click the **New** button on the *Profiles* screen, you will need to enter a name for your new profile and click **OK**, then the *Available Wireless Network* screen appears.

This screen provides two options for setting up the Adapter.

- **Available Wireless Network. (For most users.)** Use this option if you already have a network set up. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for advanced users only.

The setup for each option is described under the appropriate heading on the following pages.

Click **Exit** to return to the *Profiles* screen.

Available Wireless Network

The available networks are listed by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If your network is not listed, you can click the **Refresh** button to bring the list up again.)

If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If you have wireless security enabled on your network, continue to step 2. One of these security screens will be shown. If you don't have wireless security enabled, continue to step 3.
2. If your network has WEP, WPA Personal, or WPA2 Personal wireless security enabled, then that security screen will appear. Continue to the screen for your wireless security.
 - WEP (Wired Equivalent Privacy)

If your network has the wireless security WEP (Wired Equivalent Privacy), this screen will appear. You must enter the same security settings used on your network.

Select **64-bit** or **128-bit** WEP encryption, then enter a passphrase or WEP key.



Figure 5-8: Creating a Profile - Available Wireless Network

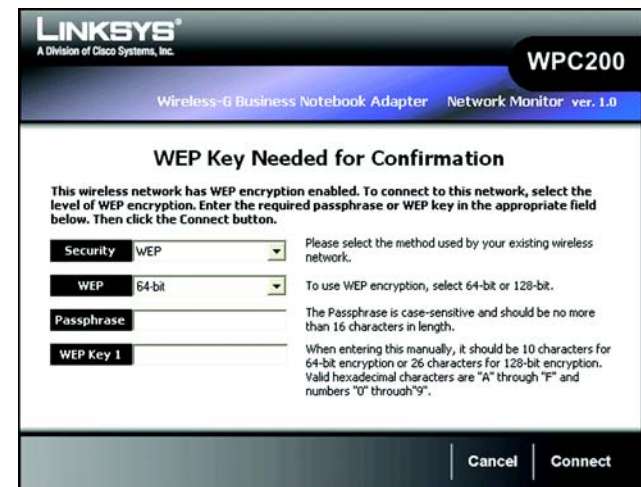


Figure 5-9: Creating a Profile - WEP Key Needed

Passphrase - Enter a passphrase in the *Passphrase* field, to automatically generate a WEP key. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Then click **Connect** and proceed to Step 3.

- **WPA Personal**

If your network has the wireless security WPA Personal (Wi-Fi Protected Access) enabled, this screen will appear. You must enter the same security settings used on your network.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.

- **WPA2 Personal**

If your network has the wireless security WPA2 Personal enabled, this screen will appear. You must enter the same security settings used on your network.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.

3. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network, implement the new settings, and return to the *Link Information* screen.

Congratulations! The profile has been successfully configured.



Figure 5-10: Creating a Profile - WPA-Personal



Figure 5-11: Creating a Profile - Congratulations

Manual Setup

If your network is not listed with the available networks, you can use Manual Setup.

1. Click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.
2. The *Network Settings* screen will appear. If your network has a router or other DHCP server, select **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, select **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

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

3. The *Wireless Mode* screen shows a choice of two wireless modes. Select **Infrastructure Mode** if you want to connect to a wireless router or access point. Select **Ad-Hoc Mode**, if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

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

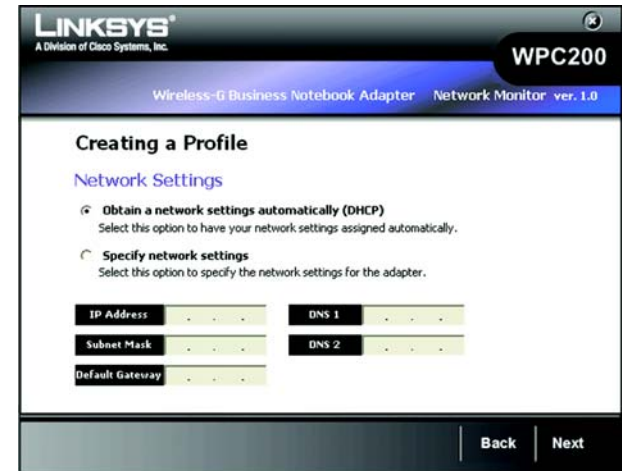


Figure 5-12: Creating a Profile - Manual Setup - Network Settings



Figure 5-13: Creating a Profile - Manual Setup - Wireless Mode

- If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.

- If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 6.

If your wireless network has wireless security, select the method of security used: **WEP, WPA/WPA2 Personal, WPA/WPA2 Enterprise, RADIUS or LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit or 128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

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

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

wpa2 offers a stronger encryption than **wpa** by using the **AES (Advanced Encryption Standard)** which is a block cipher with block sizes of 128, 192 or 256 bits.

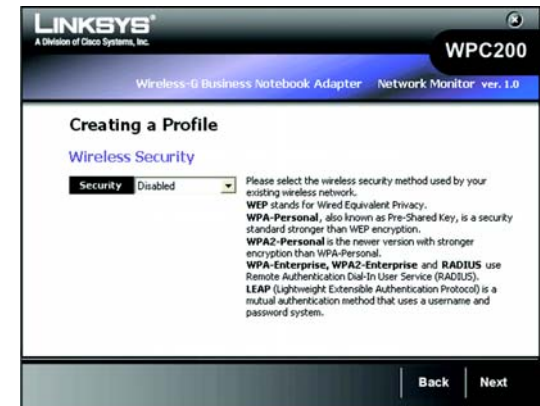


Figure 5-14: Creating a Profile - Manual Setup - Wireless Security - Disabled



Figure 5-15: Creating a Profile - Manual Setup - Wireless Security - WEP

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

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

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

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

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

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



Figure 5-16: Creating a Profile - Manual Setup - Wireless Security - WPA Personal



Figure 5-17: Creating a Profile - Manual Setup - Wireless Security - WPA2 Personal

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method is used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

The screenshot shows the 'Creating a Profile' screen for WPA Enterprise with EAP-TLS authentication. The interface includes the following fields and options:

- Authentication:** EAP-TLS (selected)
- Login Name:** (empty text field)
- Server Name:** (empty text field)
- Certificate:** (empty dropdown menu)
- Encryption:** AES (selected)

Instructions for each field are provided to the right of the input fields. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-18: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for WPA Enterprise with PEAP authentication. The interface includes the following fields and options:

- Authentication:** PEAP (selected)
- Login Name:** (empty text field)
- Password:** (empty text field)
- Server Name:** (empty text field)
- Inner Authen.:** EAP-MSCHAPv2 (selected)
- Encryption:** AES (selected)

Instructions for each field are provided to the right of the input fields. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-19: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

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

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. Below it are fields for 'Login Name', 'Server Name', 'Certificate', and 'Encryption' (set to 'AES'). Each field has a corresponding instruction. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-20: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. Below it are fields for 'Login Name', 'Password', 'Server Name', 'Inner Authn.' (set to 'EAP-MSCHAPv2'), and 'Encryption' (set to 'AES'). Each field has a corresponding instruction. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-21: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

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

The screenshot shows the WPC200 Network Monitor interface. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC200'. Below that, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' and the sub-heading is 'Wireless Security - RADIUS'. There are four fields: 'Authentication' (EAP-TLS), 'Login Name', 'Server Name', and 'Certificate'. Each field has a description: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Server Name used for authentication. (Optional)', and 'Please select the certificate used for authentication.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-22: Creating a Profile - Manual Setup - Wireless Security - RADIUS - EAP-TLS

The screenshot shows the WPC200 Network Monitor interface. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC200'. Below that, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' and the sub-heading is 'Wireless Security - RADIUS'. There are five fields: 'Authentication' (PEAP), 'Login Name', 'Password', 'Server Name', and 'Inner Authen.'. Each field has a description: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Password used for authentication.', 'Enter the Server Name used for authentication. (Optional)', and 'Please select the inner authentication method used inside the PEAP tunnel.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-23: Creating a Profile - Manual Setup - Wireless Security - RADIUS - PEAP

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username and password based system.

Enter the username and password in their fields. Enter the password again in the Confirm field.

6. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.

LINKSYS
A Division of Cisco Systems, Inc. WPC200

Wireless-G Business Notebook Adapter Network Monitor ver. 1.0

Creating a Profile

Wireless Security - LEAP

User Name Enter the Login Name used for authentication.

Password Enter the Password used for authentication.

Confirm Re-enter the Password again.

Back Next

Figure 5-24: Creating a Profile - Manual Setup - Wireless Security - LEAP

LINKSYS
A Division of Cisco Systems, Inc. WPC200

Wireless-G Business Notebook Adapter Network Monitor ver. 1.0

Confirm New Settings

Profile Settings			
SSID	linksys-g	Encryption	None
Wireless Mode	Infrastructure	IP Address	Use DHCP
Channel	Auto	Subnet Mask	Auto
Network Mode	Auto	Default Gateway	Auto
Authentication	Open System	DNS	Auto

Exit Back Save

Figure 5-25: Creating a Profile - Manual Setup - Confirm New Settings

7. The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings immediately and return to the *Link Information* screen. Click **Return to Profile Screen** to keep the current settings active and return to the *Profiles* screen.

Congratulations! The profile has been successfully configured.

Editing a Profile

On the Profiles screen, select the profile that you would like to edit in the profile list and click on **Edit** button. The next screen would be the Wireless Mode. Follow the steps below to complete the task.



Figure 5-26: Creating a Profile - Manual Setup - Congratulations

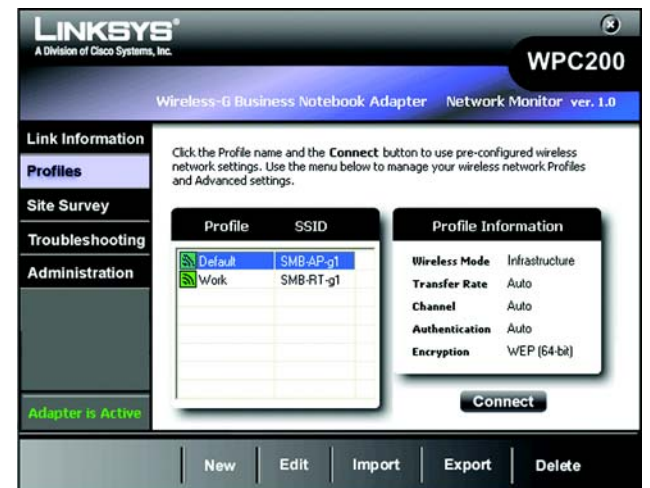


Figure 5-27: Editing a Profile

1. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

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

2. If you chose **Infrastructure Mode**, go to Step 3 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.



Figure 5-28: Editing a Profile - Wireless Mode



Figure 5-29: Editing a Profile - Ad Hoc Mode

- If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 4.

If your wireless network has wireless security, select the method of security used: **WEP, WPA/WPA2 Personal, WPA/WPA2 Enterprise, RADIUS or LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit or 128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

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

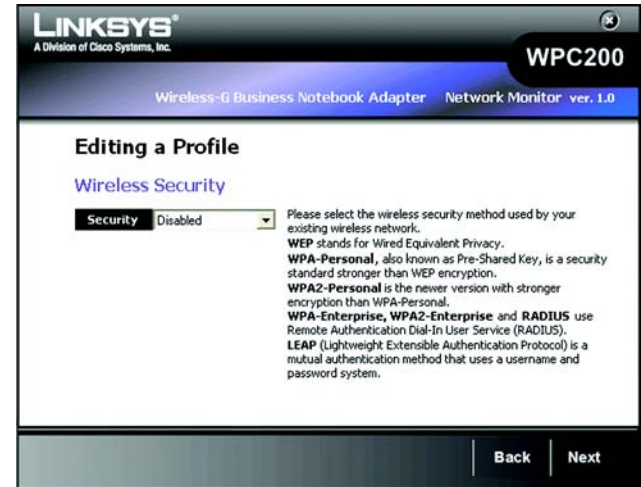


Figure 5-30: Editing a Profile - Wireless Security

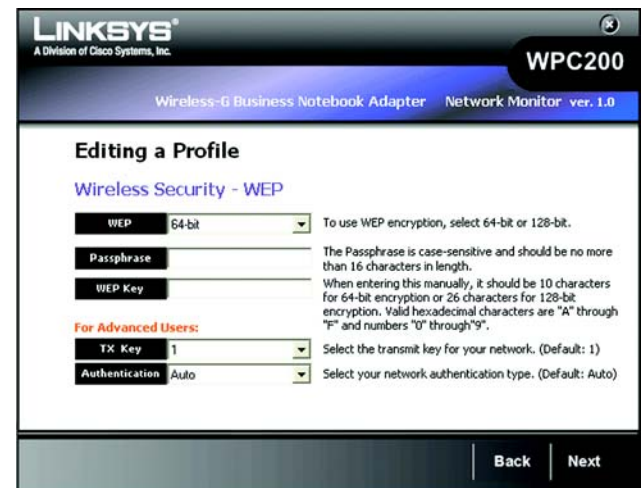


Figure 5-31: Editing a Profile - Wireless Security - WEP

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

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

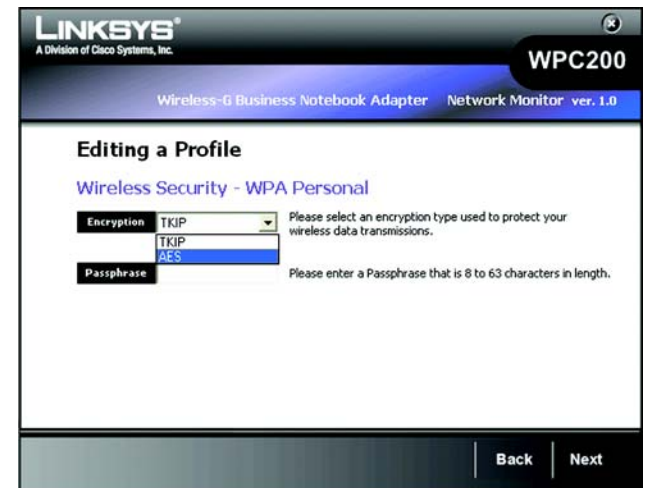


Figure 5-32: Editing a Profile - Wireless Security - WPA Personal

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

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



Figure 5-33: Editing a Profile - Wireless Security -WPA2 Personal

WPA Enterprise

WPA/WPA2 Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method is used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

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

The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. The 'Encryption' dropdown is set to 'AES'. The 'Login Name' and 'Server Name' fields are empty. The 'Certificate' dropdown is also empty. The interface includes 'Back' and 'Next' buttons at the bottom.

Figure 5-34: Editing a Profile - Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. The 'Encryption' dropdown is set to 'AES'. The 'Login Name' and 'Password' fields are empty. The 'Server Name' field is empty. The 'Inner Authen.' dropdown is set to 'EAP-MSCHAPv2'. The interface includes 'Back' and 'Next' buttons at the bottom.

Figure 5-35: Editing a Profile - Wireless Security - WPA Enterprise - PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, Trust Any. Then select the authentication method used inside the PEAP tunnel.

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

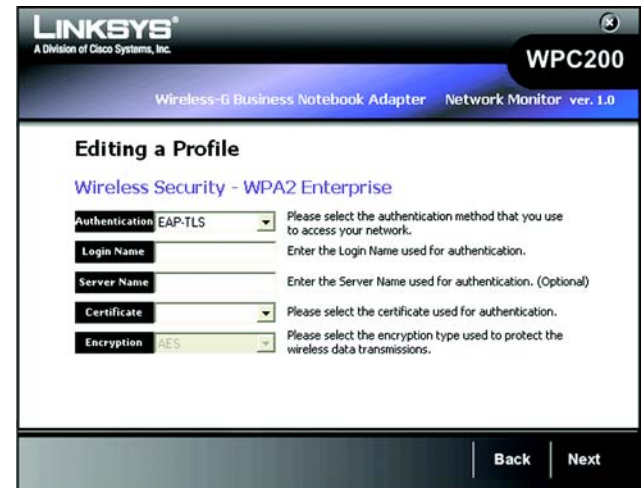


Figure 5-36: Editing a Profile - Wireless Security -WPA2 Enterprise - EAP-TLS

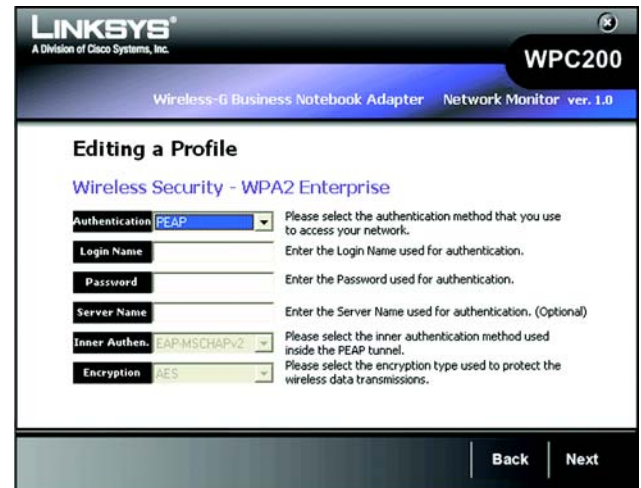


Figure 5-37: Editing a Profile - Wireless Security - WPA2 Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

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

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

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

The screenshot shows the Linksys WPC200 Network Monitor interface. The title bar includes the Linksys logo, 'A Division of Cisco Systems, Inc.', and 'WPC200'. Below the title bar, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main content area is titled 'Editing a Profile' and 'Wireless Security - RADIUS'. There are four fields: 'Authentication' (set to EAP-TLS), 'Login Name', 'Server Name', and 'Certificate'. Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Server Name used for authentication. (Optional)', and 'Please select the certificate used for authentication.'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-38: Editing a Profile - Wireless Security - RADIUS - EAP-TLS

The screenshot shows the Linksys WPC200 Network Monitor interface. The title bar includes the Linksys logo, 'A Division of Cisco Systems, Inc.', and 'WPC200'. Below the title bar, it says 'Wireless-G Business Notebook Adapter Network Monitor ver. 1.0'. The main content area is titled 'Editing a Profile' and 'Wireless Security - RADIUS'. There are five fields: 'Authentication' (set to PEAP), 'Login Name', 'Password', 'Server Name', and 'Inner Authen.' (set to EAP-MSCHAPv2). Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Password used for authentication.', 'Enter the Server Name used for authentication. (Optional)', and 'Please select the inner authentication method used inside the PEAP tunnel.'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-39: Editing a Profile - Wireless Security - RADIUS - PEAP

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username and password based system.

Enter the username and password in the username and password field accordingly. Enter the password again in the *Confirm* field.



Figure 5-40: Editing a Profile - Wireless Security - LEAP

4. The *Network Settings* screen from the Wireless Network Monitor will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

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



Figure 5-41: Editing a Profile - Network Settings

- The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.

- The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings immediately and return to the *Link Information* screen. Click **Return to Profile Screen** to keep the current settings active and return to the *Profiles* screen.

Congratulations! The profile has been successfully configured.



Figure 5-42: Editing a Profile - Confirm New Settings



Figure 5-43: Editing a Profile - Congratulations

Site Survey

The *Site Survey* screen displays a list of available networks in the table on the left. The table shows each network's SSID, Channel, and the quality of the wireless signal the Adapter is receiving. You may click **SSID**, **CH** (Channel), or **Signal**, to sort by that field.

SSID - The SSID or unique name of the wireless network is displayed here.

CH - This is the channel that the network uses.

Signal - This is the percentage of signal strength, from 0 to 100%.



The Access Points in the Site Survey list will be represented with different icons that will indicate Access Points in various states of classification. For instance, trusted Access Points are green, untrusted Access Points are red, and unclassified Access Points are blue. And if there is a lock next to it, it indicates the Access Point has a security method enabled.

For more information about classification of the Access Points, refer to “AP Classification” section of “Chapter 6: The Administrative Functions in the Wireless Network Monitor.”

Site Information

For each network selected, the following settings for each SSID are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Network Type - The type of your network connection in either wireless-b or wireless-g is displayed here.

Security - The status of the wireless security feature is displayed here.

MAC Address- The MAC address of the wireless network's access point is displayed here.

Refresh - Click the **Refresh** button to perform a new search for wireless devices.

Connect - Click the **Connect** button to connect to a selected network.



Figure 5-44: Site Survey

Troubleshooting

The *Troubleshooting* screen lets you troubleshoot your wireless connection.

Address Type - This shows the addressing method of your client.

IP Address - This shows the current IP Address of your client.

Subnet Mask - This shows the subnet mask of your IP addressing.

Default Gateway - This shows the default gateway of your IP addressing.

You may click **Repair** to troubleshoot your connection to the wireless network. Repair will disconnect your client from the network and then reconnect, in order to re-establish an IP address. You may also click **FAQ** to view the FAQ pages from the Linksys website.

Administration

The *Administration* screen lets you administer your Security Monitor account and classification functions, and modify your Access Point's username and password in Account Management. Select on a button to log in to either the Security Monitor account or Account Management as the Access Point's administrator.

Log in to the Security Monitor account to access the classification and Security Monitor functions:

Enter the Security Monitor's account name and password in the *username* and *password* fields, then retype the password in the *confirm* field. Click Next to continue to the administrative options.

After a successful login, the Classification and Security Monitor tab appears. Only the login screens are provided in this section. To use the Administration tab, continue to Chapter 6: The Administrative Functions in the Wireless Network Monitor.



Figure 5-45: Troubleshooting



Figure 5-46: Administration

Log in as the Access Point's administrator:

Enter the Access Point's administrative account and password and retype the password in the confirm field (default account name is *admin* and password is *admin*). Click **Next** to continue to the administrative options.

Access Point Account

This screen appears when you click the Access Point button on the Security Monitor Account screen. This will let you modify your Access Point's username and password.



Figure 5-47: Administration - Login Access Point Account



Figure 5-48: Administration - Modify Access Point Account

Security Monitor Account

The *Security Monitor Account* screen provides you with the function to create and modify your Security Monitor account. The Security Monitor account gives access to the administrative functions of the Wireless Network Monitor.

Enter the administrator's **username** and **password** and retype the password in the confirm field. Click **Next** to proceed with more administrative options.



The username and password for the Security Monitor administrator account do not need to be the same as the Access Point's administrator account.

You can select an account from the drop-down menu to create or modify the username and password. There are a total of five accounts available. Click **Save** to save your existing changes.

Figure 5-49: Administration - Security Monitor Account

Chapter 6: The Administrative Functions in the Wireless Network Monitor

When used with the WAP200 Access Point, you can use the administration functions in the Wireless Network Monitor to classify your wireless networks into different groups and monitor the activities and resources within your networks. The following functions under *Classification* and *Security Monitor* screens are only enabled after an administrator or privileged user enters a valid username and password.

Accessing the Wireless Network Monitor

After installing the Adapter, the Wireless Network Monitor icon will appear in the system tray of your computer. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.

Using the Administrative Functions in the Wireless Network Monitor

The *Administration* tab will give you access to the administrative tasks of the account information and other functions, such as classification and monitoring of your wireless networks. The *Classification* and *Security Monitor* functions will be provided after logging in to the Security Monitor account on the Administration screen. To configure trusted and untrusted wireless networks, click the **Classification** tab. To view the summarized report of the monitored wireless activities and alert messages, click the **Security Monitor**.



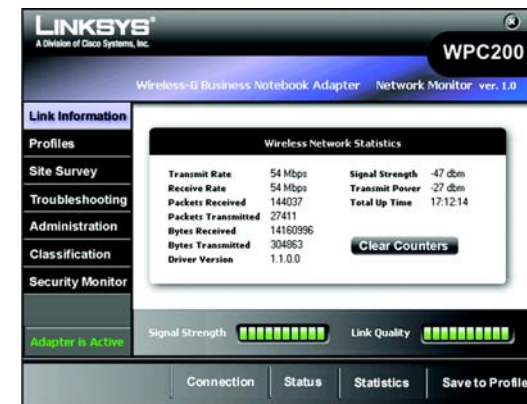
NOTE: You must associate with a WAP200 Access Point to be able to log in to the Security Monitor.
NOTE: You will need to log in with a valid Security Monitor account to view the screens in this chapter.



Figure 6-1: Wireless Network Monitor Icon



Figure 6-2: Administration - Login Security Monitor



Administration - Login Security Monitor Account

Classification

The *Classification* tab displays a summary of classified devices. The Classification Summary table shows the number of access points and clients classified as trusted and untrusted by MAC addresses in your networks. It also shows the number of allowed vendors, SSIDs, and channels.

You may uncheck the **Receive classification rules** to disable a client from receiving the network's current classification rules. The default condition is checked, so each client always receives classification rules in synchronization with other clients in the network. You may also click the **Synchronize** button to send out the classification rules to other users within your monitored wireless networks.

Click **Next** to configure your trusted networks.



NOTE: Classification rules: access points and clients can be classified as trusted or untrusted, and access points can be additionally classified by MAC address, SSID, vendor, or channel.

AP Classification

The *AP Classification* screen lets you classify the existing access points as trusted or untrusted. A Trusted device is one that has been identified by the system administrator to be known and legitimate. An untrusted device is one that is known and not legitimate. This device could be a malicious device or simply a neighborhood device not part of the network. Remaining devices that have not been classified are considered unclassified or unknown.

The *Unclassified Access Points* table lists the available unclassified wireless access points with their SSIDs, channels and MAC Addresses. The top right table lists the *Trusted Access Points*. The lower right table lists the *Untrusted Access Points*.

You may select any items from the *Unclassified Access Points* table and click the arrow to classify your selections into *Trusted Access Points* or *Untrusted Access Points*. You may also select any items from the *Trusted Access Points* or *Untrusted Access Points* and click the arrow to de-classify your selections into the *Unclassified Access Points* table.

You may select **Warning when connecting to untrusted AP**, if you want to be warned when connecting to an untrusted AP, or select **Restrict connection to untrusted AP** to disallow connection to an untrusted AP.

Click **Refresh** to refresh the list, **Clear** to clear selected items on the list, or click **Back** to go to the previous screen.

Click **AP Classification**, **Client Classification**, or **Advanced Settings** to go to that screen.

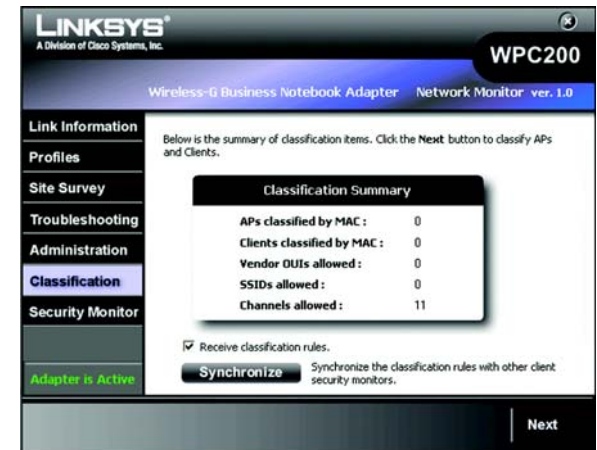


Figure 6-3: Classification

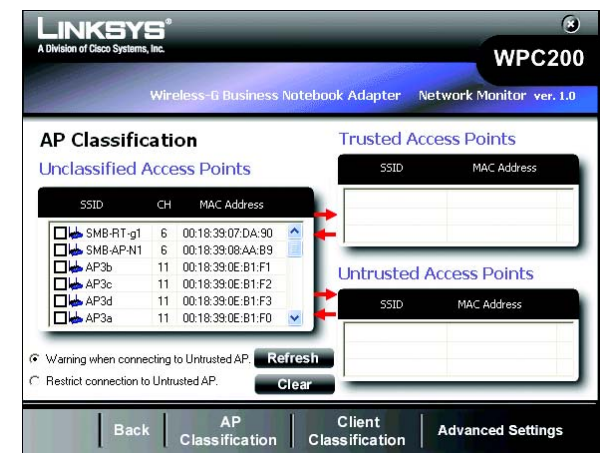


Figure 6-4: AP Classification

Client Classification

The *Client Classification* Screen lets you classify the existing wireless clients into trusted networks and untrusted networks. New client information is received from Linksys Business Series access points. New clients start off as **Unclassified** until the System Administrator classifies them. A **Trusted Client** is one that has been identified by the System Administrator to be known and legitimate. An **Untrusted Client** is one that is known and not legitimate; this client could be a malicious client or simply a neighborhood client not part of the network. Remaining clients that have not been classified can be considered as unclassified or unknown.

The left table lists the available unclassified clients with their associated Access Point's SSID. The top right table lists the clients that have been classified as **Trusted**. The lower right table lists the clients that have been classified as **Untrusted**.

You may select any items from the *Unclassified Clients* table and click the arrow to classify your selections into **Trusted Clients** or **Untrusted Clients**. You may also select any items from the **Trusted Clients** or **Untrusted Clients** and click the arrow to de-classify your selections into the *Unclassified Clients* table.

You may click **Refresh** to refresh the list, **Clear** to clear selected items on the list, or **Back** to go to the previous screen.

You may click **AP Classification**, **Client Classification**, or **Advanced Settings** to go to that screen.

Advanced Settings

Click **Advanced Settings** to classify your wireless networks by **Mac (Address)**, **Vendor**, **SSID** or **Channel**. Click the **MAC** tab to configure the trusted MAC addresses, **Vendor** to configure the trusted AP vendor list, **SSID** to configure the trusted SSID list, **Channel** to configure the trusted channel, or **Back** to go to the previous screen.

Trusted MAC Addresses

Clicking the **MAC** button displays the *Trusted MAC Addresses* screen, which provides information and function for configuring the existing wireless networks as trusted networks with MAC Access control of the access points and the clients. The Trusted AP's MAC Addresses that you enter on this screen will also appear on the *AP Classification* screen as a trusted access point.

The tables list the entry of MAC addresses of your trusted and allowed wireless access points and clients.

Enter the 12-digit hexadecimal numbers in the field and click **Add** to add the entry. To delete an entry, select it, then click **Delete**.

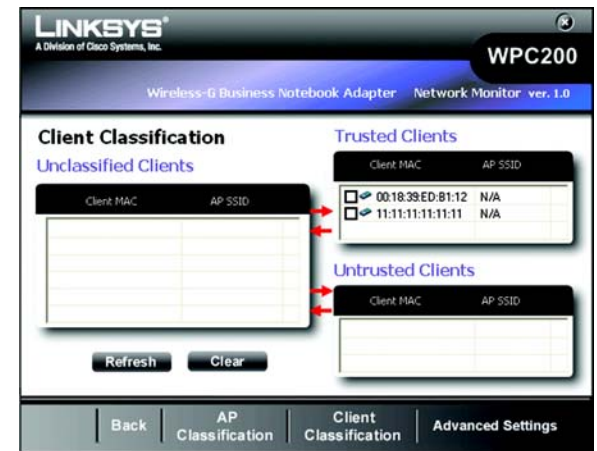


Figure 6-5: Client Classification



Figure 6-6: Trusted Mac Address

Allowed Vendor List Configuration

The Allowed Vendor List Configuration table lists the OUI (Organization Unique Identification) and vendor name of your trusted and allowed AP Vendor OUIs. A OUI is the three-octet (first 6 digits) used to generate LAN MAC Addresses for hardware manufacturers. To delete an item, select it, and click **delete**. The latest vendor OUI lists are available at <http://standards.ieee.org/regauth/oui/index.shtml>.

Vendor Name - This is the name of your desired vendor. Select a vendor's name from the drop-down list and click **Add** to add the vendor.

Vendor OUI - If the vendor OUI is not listed, you may enter the company's OUI and click **Add** to enter your vendor's OUI in the list.

APs from vendors not on the allowed vendor list will be automatically classified as untrusted. A blank list indicates that all vendor OUIs are allowed for AP classification.



Figure 6-7: Allowed Vendor List Configuration

Allowed SSID Configuration

The Allowed SSID Configuration table shows the SSIDs of the allowed APs on your network. APs from SSIDs not on this list will be automatically classified as untrusted. A blank list indicates that all SSIDs are allowed for classification.

SSID - This is the unique name of the wireless network. (a unique identification, up to 32 characters, attached to the header of packets sent over a WLAN)

You may enter the **SSID** of a trusted and allowed wireless network in the field and click **Add** to add it into your list. You may select an item and click **Delete** to delete it from the list.



Figure 6-8: Allowed SSID Configuration

Allowed Channel Configuration

The *Allowed Channel Configuration* screen shows the channels that are allowed to be used in your wireless networks. You may select individual channels or click **Check All** to check all of the channels. Unclassified access points on unchecked channels will be automatically classified as untrusted.

Security Monitor



IMPORTANT: You must use a WAP200 Access Point with your Notebook Adapter to use the Security Monitor.

The Security Monitor helps to make your network more secure. It monitors the airspace through the WAP200 Access Point and Notebook Adapter for security related issues like vulnerabilities in the network configuration, which allows you to act quickly to solve issues and secure your network. The Monitor runs on the client PC, which allows the administrator to perform initial setup of security profiles and classification of the wireless network devices and later view assorted security alerts.

The *Security Monitor* tab displays the statistics of your wireless network and alerts you of network activity by Channel Usage, AP Inventory, Client Inventory, or Alerts.

Click **Channel Usage**, **AP Inventory** to view the statistics of the distribution on your AP's classifications, **Client Inventory** to view the distribution of the client's classifications on your wireless networks, or **Alert** to monitor that function.

Channel Usage

The *Channel Usage* screen provides statistics of the distribution on your channel's usages. The histogram shows the number of access points in each channel, so unclassified access points can be detected. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.



Figure 6-9: Allowed Channel Configuration

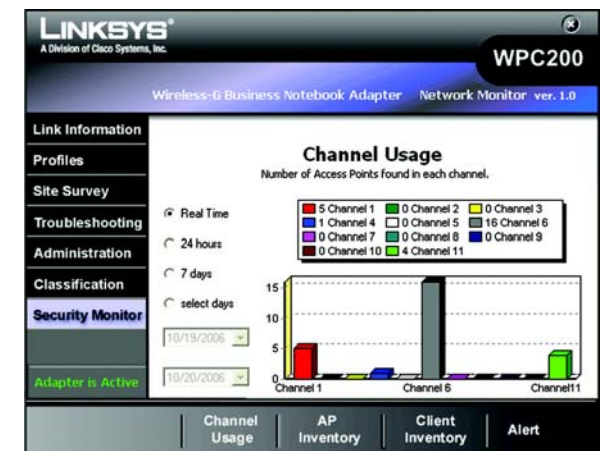


Figure 6-10: Security Monitor - Channel Usage

AP Inventory

The *AP Inventory* screen provides statistics of the distribution grouped by your AP's classification of your wireless networks. The pie chart shows the percentage of each classification type, so you can easily view the number of trusted, untrusted, and unknown APs in the airspace. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.

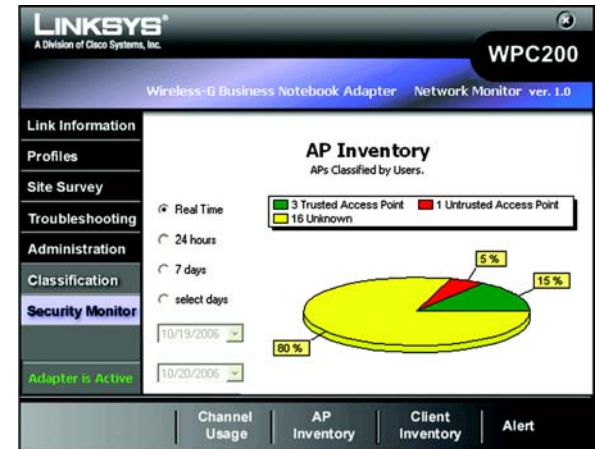


Figure 6-11: Security Monitor - AP Inventory

Client Inventory

The *Client Inventory* screen provides statistics of trusted, untrusted, and unknown clients. The pie chart shows the percentage of each wireless client's classification, so you can easily view the number of trusted, untrusted, and unknown clients in the airspace. Select the specified period of time you want for the data calculations. You may select **Real Time** for current data, **24 hours** for data within the last 24 hours, **7 days** for data within the last 7 days or **select days** for a range of days.



Figure 6-12: Security Monitor - Client Inventory

Alert

Overview

Both the WAP200 Access Point and client Notebook Adapter monitor the state of your wireless network and report on security related issues, ranging from on-going attacks down to vulnerabilities in the network configuration.

The Access Point does most of the security monitoring work while the client Notebook Adapter can detect new and rogue access points. The management software runs on the client PC, which allows the system administrator to perform initial setup of security profiles and classification of the wireless network devices.

When a client Notebook Adapter detects an unknown access point, it will notify its associated Access Point. The Access Points synchronize security alerts with each other and send the alert to the administrator.

Once the administrator is alerted with the security alarm, the administrator or one of the five authorized users can log in to the Security Monitor to retrieve the Alert Log from the Access Point.

There are four categories of policy violation rules listed under *Alert Type*: Intrusion Alarms: unauthorized connection or hacking attack taking place on the network, Denial of Service Alarms: denial of service attack detected on the network, Vulnerability Alarms: potential threat to the security of the network, and Others. Each represents a different kind of threat to the wireless network, ranging from poor performance to unauthorized users connected to the network. A violation will be listed under *Amount*. You can click Retrieve Alert log to view the *Alert List*. When *Detail* is clicked, the *Details* screen appears with more detailed information of the event, then you can click *Advice* to view the suggested advice for the event.

Alerts Summary

The *Alerts Summary* screen lists the alert types, amount of alerts, and available details.

Detail - Click the **Detail** button to view more detailed information for each event.

Receive AP Alert- Select this to receive alert logs from access points.

Retrieve Alert log - Click this button to view an alert log.

Enable Pop-up - Select this to allow this client to receive a pop-up warning message when any alert is detected.

Click **Back** to go to the previous screen.



Figure 6-13: Security Monitor - Alerts Summary

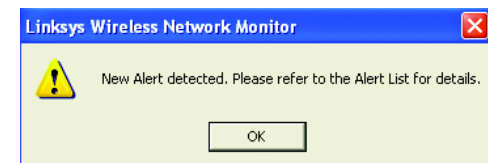


Figure 6-14: Security Monitor - POP-UP Alert



NOTE: You will be alerted when an Access Point is detected, if you enable pop-up.

Alert List

The *Alert List* screen shows the list of the alert activities within your monitored wireless networks.

SSID - This shows the SSID (network name) of your wireless network.

MAC - This shows the MAC Address of the wireless client or access point that was detected.

Alert Description - This shows brief descriptions of the alert activities. The alert system will alert you when new access points or wireless clients are detected, or if other policy violations or attacks are detected.

Date/Time - This indicates the date/time that an alert activity happened.

Delete - Select an item, then click this button to delete the item.

Click **Back** to go to the previous screen or **Exit** to go to the main menu.

Alert Details

The *Details* screen shows the detailed message of each alert event.

Alert - This indicates the description of the event.

MAC Address - This shows the MAC Address of the wireless client or Access Point that performed the action.

Date/Time - This shows the Date/Time of the alert.

Description - This shows the detailed description of the event.

You may click the **Advice** button to view the advice message, **Back** to go back to the previous screen, or **Exit** to go back to the main menu.

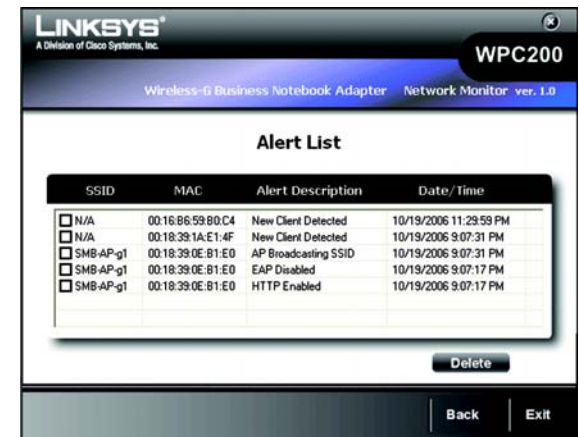


Figure 6-15: Security Monitor - Alert List



Figure 6-16: Alert Details

Advice

The *Advice* screen gives advice, when applicable, on what can be done for each alert event. You may need to adjust your wireless network settings according to the advice to better protect your networks.



Figure 6-17: Security Monitor - Alert Advice

The following table is a summary of the various alert descriptions and **advice**.

Table 1: Alerts

Item	Alert	Description	Advice
1	Rogue Client Detected	A Rogue Client is detected. For details, press the Advice button.	<p>Description: Rogue Client is detected doing one or more illegal actions, e.g., causing Message Integrity Check (MIC) errors, sending disassociation frames, sending deauthentication frames, and sending association frames with incorrect encryption.</p> <p>MIC error generation: The MIC function prevents attacks on encrypted packets. During an attack, an intruder intercepts an encrypted (WPA - Personal) message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. This action will cause a MIC error. If an attacker causes two MIC errors within 60 seconds, it will be considered a Rogue Client.</p> <p>Disassociation attacking: Occurs when a wireless station transmits a disassociation request to an AP which it is not associated with.</p> <p>De-authentication attacking: Occurs when a wireless station transmits a de-authentication request to an AP which it is not associated with.</p> <p>Authentication failure: Occurs when the AP receives an association request with different encryption from a wireless client.</p> <p>Action:</p> <ol style="list-style-type: none"> 1. Contact the network administrator and send the administrator the Rogue Client computer information. 2. Change MAC access control list on the AP and further block the Rogue Client's activities.

Table 1: Alerts

Item	Alert	Description	Advice
2	AP SSID Changed	SSID on the AP has changed. For details, press the Advice button.	<p>Description: AP's SSID was changed by an unknown source. This may be caused by a possible intruder if the AP's SSID was not changed by the administrator. Original SSID: Modified SSID:</p> <p>Action: 1. Contact the network administrator. 2. If an intruder is suspected, change administrator's password on the AP.</p>
3	AP Channel Changed	AP's Channel has Changed. For details, press the Advice button.	<p>Description: AP's Channel was changed by an unknown source. It could possibly be done by an intruder if it was not changed by the administrator or via auto channel selection. Original Channel: Modified Channel:</p> <p>Action: 1. Contact the network administrator and send the administrator the Login Information/history. 2. If an intruder is suspected, change the administrator's password on the AP.</p>
4	Spoofed MAC Address	The AP's MAC Address has been spoofed by a wireless client. For details, press the Advice button.	<p>Description: AP's MAC address has been spoofed by a wireless client. Client sends a frame with a MAC address which is the same as the AP's MAC address. By processing these packets, the AP may be subjected to heavy loading.</p> <p>Action: No actions required. The AP will automatically drop these frames.</p>

Table 1: Alerts

Item	Alert	Description	Advice
5	Client is Sending Spurious Traffic	Client not associated with AP is sending traffic. For details, press the Advice button.	<p>Description: Client not associated with AP is sending traffic. Probable rogue client. The Client might be trying to make the network busy and causing heavy loading to the AP.</p> <p>Action: 1. Contact network administrator. 2. Add the Client MAC address to MAC Access Control List on AP Web Page.</p>
6	Adhoc SSID is the same as the AP's	A wireless client using Adhoc structure has the same SSID as the AP's SSID. For details, press the Advice button.	<p>Description: A wireless client using Adhoc structure has the same SSID as the AP's SSID. Illegitimate AP could use the same SSID to fool other wireless clients that it is a legitimate AP.</p> <p>Action: 1. Contact network administrator. 2. Try to physically locate the wireless client computers.</p>
7	Duration Attack	Abnormally large duration for packets sent by client. For details, press the Advice button.	<p>Description: Packets with abnormally large duration sent by a client may prevent other clients from sending packets to the AP. Client computer information:</p> <p>Action: 1. Try to physically locate the wireless client computer. 2. Add the Client's MAC address to MAC Access Control List on the AP.</p>

Table 1: Alerts

Item	Alert	Description	Advice
8	Association Table Full	Possibly a Denial of Service Attack. For details, press the Advice button.	<p>Description: A New client association request is refused due to a lack of memory. It could be an overloaded AP from being associated with too many legitimate clients or it could be a possible Denial of Service attack that will prevent legitimate clients from associating with the AP.</p> <p>Action: 1. AP will stop allowing more client association with the AP. 2. Check the AP's client's list to see if any wireless client is illegitimate.</p>
9	AP Is Not Using Encryption	AP does not have any encryption method enabled. For details, press the Advice button.	<p>Description: AP does not have any authentication method enabled, so it is vulnerable to network attacks or sniffing.</p> <p>Action: 1. Contact the network administrator. 2. In order to make the wireless network more secure, set up the AP with a stronger authentication method, e.g., WPA or WPA2.</p>
10	AP Broadcasting SSID	AP has SSID Broadcasting enabled. For details, press the Advice button.	<p>Description: AP has SSID Broadcasting enabled, so any wireless station can obtain its SSID.</p> <p>Action: In order to avoid being attacked by rogue clients, turn off SSID broadcasting on the AP.</p>
11	Default SSID in Use	AP is using the default SSID. For details, press the Advice button.	<p>Description: AP is using the default SSID. Default SSIDs are easy to identify, so a hacker can effortlessly connect to the AP.</p> <p>Action: In order to keep the connection secure, change the AP SSID to a non-default SSID.</p>

Table 1: Alerts

Item	Alert	Description	Advice
12	Duplicate SSID in Use	Unclassified AP has the same SSID as a trusted AP. For details, press the Advice button.	<p>Description: An unclassified AP has same SSID as the trusted AP.</p> <p>Action: 1. Contact the network administrator and inform the administrator about the untrusted AP's SSID and MAC address. 2. Check if the untrusted AP is legitimate. 3. Unclassified AP needs to be classified and the classification table needs to be updated.</p>
13	New Access Point Detected	New AP is detected. For details, press the Advice button.	<p>Description: New AP is detected. The new Access Point needs to be classified and the classification table needs to be updated.</p> <p>Action: 1. Contact the network administrator and inform the administrator about the new Access Point's SSID and MAC address. 2. Unclassified AP needs to be classified and the classification table needs to be updated.</p>
14	Adhoc Network Operating	Clients are operating in Adhoc mode. For details, press the Advice button.	<p>Description: Clients are operating in Adhoc mode, so network security could be compromised.</p> <p>Action: 1. Contact the network administrator and inform the administrator of the client's SSID and MAC address. 2. Try to physically locate the wireless client's computers.</p>

Table 1: Alerts

Item	Alert	Description	Advice
15	New Client Detected	New client is detected. For details, press the Advice button.	<p>Description: New wireless client computer is detected.</p> <p>Action: 1. Contact the network administrator and inform the administrator about the new client computer's SSID and MAC address. 2. The new Client needs to be classified and the classification table needs to be updated.</p>
16	Low Speed Connection	Connection is at low speed. For details, press the Advice button.	<p>Description: Data packets are being transferred at a very slow rate. Possible cause may be a poor signal reception due to some interference or the client is too far away from the AP.</p> <p>Action: 1. Check the environment and find possible causes for wireless signal interference, e.g., a microwave oven or a cordless telephone. 2. Check the MAC association table on the AP for any illegitimate wireless clients.</p>
17	Rogue AP Detected	Rogue AP is detected. For details, press the Advice button.	<p>Description: A Rogue AP is detected doing an illegal action. The AP is using the same SSID and encryption as the Trusted AP and is trying to crack the client computer's encryption key. During the decryption process, the AP has a 4-way handshake and if compromised, the client computer will detect a MIC error, indicating a Rogue AP.</p> <p>Action: 1. Contact network administrator. 2. Try to physically locate the Access Point.</p>

Windows Firewall

Windows XP users may see a Windows Firewall screen when using the security monitor.



IMPORTANT: DO NOT select **Don't allow exceptions** or the security monitor will not work correctly.

Select **On (recommended)** to use the firewall. Do not select the *Don't allow exceptions* or the Adapter's security monitor will not work properly. Then, click **OK**.

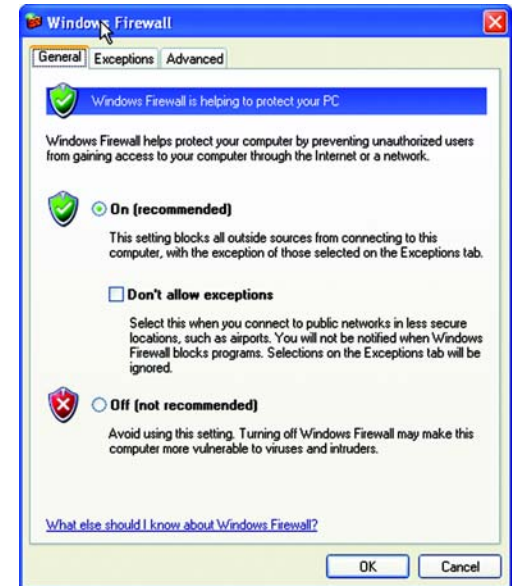


Figure 6-18: Security Monitor - Windows Firewall Screen

Appendix A: Troubleshooting

This appendix consists of two parts: “Common Problems and Solutions” and “Frequently Asked Questions.” This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Business Notebook Adapter. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

Common Problems and Solutions

1. *The Wireless-G Business Notebook Adapter does not work properly.*

- Reinsert the Wireless-G Business Notebook Adapter into your PC's CardBus slot.
- Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find the Wireless-G Notebook Adapter with RangeBooster if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of the Wireless-G Notebook Adapter with RangeBooster. If there is a yellow question mark, please check the following:
- Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.)
- Make sure that you have inserted the right adapter and installed the proper driver.

If the Wireless-G Business Notebook Adapter does not function after attempting the above steps, remove the adapter and do the following:

- Uninstall the driver software from your PC.
- Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2. *I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.*

- Make sure that the PC to which the Wireless-G Business Notebook Adapter is associated is powered on.
- Make sure that your Wireless-G Business Notebook Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

Frequently Asked Questions

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.

How will the Wireless networking technology help with my business?

Keeping your business connected to the internet and managing networking in your office without wires give you the freedom to create a dynamic office environment that changes and grows as your business needs. The Linksys Wireless-G Business Notebook Adapter will not only let you communicate sensitive data in a wireless setting, but also give you the security and management options within your monitored networks. We designed our wireless products to be simple to set up with the advances of the latest data encryption methods and Security Monitor functions.

How long does it take for intrusions and policy violation events to appear in the alert lists?

Periodic polling is used to report alerts, so the AP and wireless client won't over-burdened. It may take up to five minutes for the alert to appear in the alert lists.

Can non-administrative users have pop-up alerts appear on their screens?

Yes, if the administrator enables *receive pop-up alerts* on the users' wireless network monitors.

Can users turn off the pop-up alerts?

Pop-up alerts are disabled by default and are enabled by the administrator on other stations to aid him in monitoring the airspace. Only someone with administrative rights or a designate of the administrator can turn off the pop-up alerts.

What if user a user turns off the Linksys wireless network monitor utility and only uses the Windows Zero Config to connect to the wireless network?

The user will not be able to enjoy the benefits of the Linksys utility, including participation in classification and security monitoring, which helps the administrator to detect intrusions and policy violations and improve the state of the network. For example, if not using the wireless network monitor utility, the user might compromise the network by inadvertently associating to an Untrusted AP.

My new AP is automatically classified as untrusted when I try to classify using the "Vendor OUI" filter. Why does this happen?

It is possible that the device is new and the Vendor OUI of the AP was not available when we released our software. In this case, visit the website: <http://standards.ieee.org/regauth/oui/index.shtml> and add it into the *Allowed Vendor List*. The Vendor OUI is the three octet (the first 6 digits) of the MAC address.

What is the 802.11b standard?

It is one of the 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 802.11b features are supported?

The product supports the following 802.11b 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 mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. This type of network will not communicate with any wired network.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?

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

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

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

What is ISM band?

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

What is Spread Spectrum?

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

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

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if

Wireless-G Business Notebook Adapter with RangeBooster

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.

What is WEP?

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

What is WPA?

WPA is Wi-Fi Protected Access, a wireless security protocol that can be used in conjunction with a RADIUS server.

What is RADIUS?

RADIUS is Remote Authentication Dial-In User Service, which uses an authentication server to control network access.

Appendix B: Windows XP Wireless Zero Configuration

Windows XP Wireless Zero Configuration

If your computer is running Windows XP, then this choice will be available. If you want to use Windows XP Wireless Zero Configuration to control the Adapter, instead of using the Wireless Network Monitor, then right-click on the Wireless Network Monitor and select **Use Windows XP Wireless Configuration**.

If you want to switch back to the Wireless Network Monitor, right-click the **Wireless Network Monitor** icon, and select **Use Linksys Wireless Network Monitor**.



Figure B-1: Wireless Network Monitor Icon

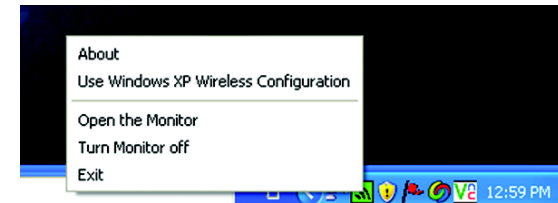


Figure B-2: Windows XP - Use Windows XP Wireless Configuration

1. After installing the Adapter, the Windows XP Wireless Zero Configuration icon will appear in your computer's system tray. Double-click the icon.



NOTE: For more information about Wireless Zero Configuration, refer to Windows Help.



Figure B-3: Windows XP Wireless Zero Configuration Icon

Wireless-G Business Notebook Adapter with RangeBooster

- The screen that appears will show any available wireless network. Select the network you want. Click the **Connect** button.

If your network does not have wireless security enabled, go to step 3.

If your network does have wireless security enabled, go to step 4.



NOTE: Steps 2 and 3 are the instructions and screenshots for Windows XP with Service Pack 2 installed.

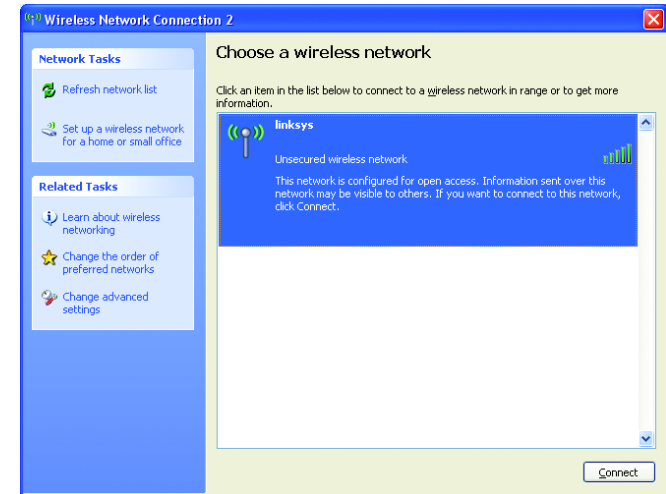


Figure B-4: Available Wireless Network

- If your network does not have wireless security enabled, click the **Connect Anyway** button to connect the Adapter to your network.



Figure B-5: No Wireless Security

4. If your network uses wireless security WEP, enter the WEP Key used into the *Network Key* and *Confirm network key* fields. If your network uses wireless security WPA Personal, enter the Passphrase used into the *Network Key* and *Confirm network key* fields. Click the **Connect** button.



Figure B-6: Network Connection - Wireless Security

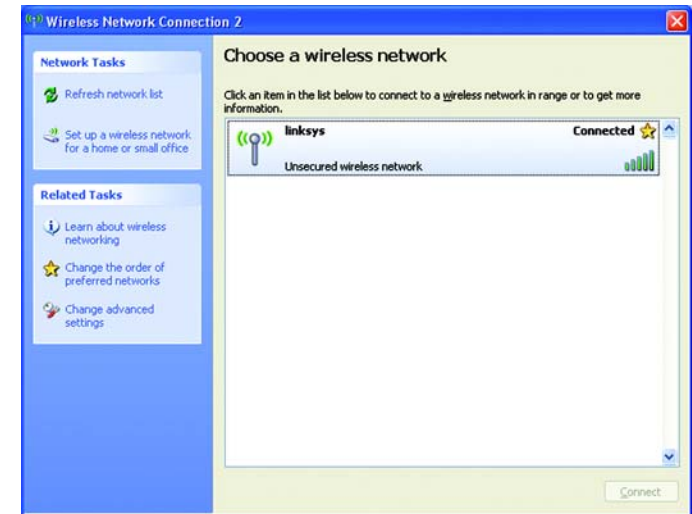


NOTE: Windows XP Wireless Zero Configuration does not support the use of a passphrase. Enter the exact WEP key used by your access point.

5. Your wireless network will appear as Connected when your connection is active.

For more information about wireless networking on a Windows XP computer, click the **Start** button, select **Help**, and choose **Support**. Enter the keyword wireless in the field provided, and press the **Enter** key.

The installation of the Windows XP Wireless Configuration is complete.



Appendix C: 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 (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/WPA2 if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

Security Threats Facing Wireless Networks

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

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

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



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.

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. Three modes are available: WPA-Personal, WPA Enterprise, and Radius. WPA-Personal 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. WPA Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication.



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 Business Notebook Adapter with RangeBooster

WPA-Personal. If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, and enter a password in the Passphrase field of 8-63 characters.

WPA Enterprise. 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.) WPA Enterprise offers two encryption methods, TKIP and AES, with dynamic encryption keys.

WPA2. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

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.)

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 D: Windows Help

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

TCP/IP

Before a computer can communicate with an access point or wireless router, 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

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at <http://www.linksys.com/glossary>.

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.

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.

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

Bit - A binary digit.

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

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.

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

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

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

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.

Wireless-G Business Notebook Adapter with RangeBooster

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.

DOS (Denial of Service) - A network security term which defines a type of attack designed to prevent legitimate users from using wireless service by flooding with useless/malicious traffic.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

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

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

Encryption - Encoding data transmitted in a network.

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

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.

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.

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.

Intrusion attack - A type of internet attacks in which an attacker tries to gain or access the information transmitted through the networks.

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.

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.

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

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

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

Mbps (MegaBits Per Second) - One million bits per second; a unit of measurement for data transmission.

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.

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.

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.

QoS (Quality of Service) - A mechanism which gives priorities to certain types of traffic to ensure the throughput; for example, the streaming multimedia.

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.

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.

SPI (Stateful Packet Inspection) Firewall - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (Service Set Identifier) -It consists of 32 alphanumeric characters to identify a group of wireless network devices uniquely.

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.

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.

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.

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

Standards	IEEE802.11g, IEEE802.11b, 802.1x (Security Authentication), (802.1i)
Channels	802.11b/802.11g 11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
LEDs	Power, Link/Act
Protocols	802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps); 802.11g: OFDM
Peak Gain of the Antenna	PIFA: -4 dBi (average), -1 dBi (peak)
Transmitted Power	802.11b: 19~20dBm 802.11g: 17~18dBm
Receive Sensitivity	11Mbps @ -88dBm, PER <= 8% 54Mbps @ -77dBm, PER <=10%
Security Features	WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise with RADIUS
WEP key bit lengths	64 Bit and 128 Bit
Security Monitor address)	Intrusion Alarms (e.g., Rogue Client Detected, Spoofed MAC Vulnerability Alarms (e.g., AP is not using encryption, AP is broadcasting SSID)
Dimensions	2.13" x 0.59" x 4.88" (54 mm x 15 mm x 124 mm)

Wireless-G Business Notebook Adapter with RangeBooster

Unit Weight	1.76 oz (0.05 kg)
Certifications	FCC, CE,IC, Wi-Fi (802.11b/g)
Operating Temp.	32°F to 149°F (0°C to 65°C)
Storage Temp.	-4°F to 185°F (-20°C to 85°C)
Operating Humidity	10 to 85%, Non-Condensing
Storage Humidity	5 to 90%, Non-Condensing

Appendix G: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix H: Regulatory Information

FCC Statement

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

This equipment has been SAR-evaluated for use in notebooks with side slot configuration.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Notices

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

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

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

Industry Canada Statement

Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

Declaration d'Industrie Canada

Le fonctionnement est soumis aux conditions suivantes:

- Ce peripherique ne doit pas causer d'interferences
- Ce peripherique doit accepter doit accepter toutes les interferences recues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

Industry Canada Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for uncontrolled environments. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Avis d'Industrie Canada concernant l'exposition aux radiofréquences :

Ce matériel est conforme aux limites établies par IC en matière d'exposition aux radiofréquences dans un environnement non contrôlé. L'émetteur ne doit pas être placé près d'une autre antenne ou d'un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:

English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.



Dansk/Danish

Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ελληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķīrotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskās un elektroniskās ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdurbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jstax jintrema ma' skart municiġpali li ma għiex iſseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir iehor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riciklagg jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-hanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai unió vásárlók számára

A 2002/96/EC számú európai unió irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszeren keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácnosti. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjstvih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

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

800-326-7114
support@linksys.com

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

949-823-3000