



Wireless-N Business Notebook Adapter

USER GUIDE

BUSINESS SERIES

Model No. WPC4400N



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?	1
Chapter 2: Planning your Wireless Network	3
Network Topology	3
Roaming	3
Network Layout	4
Chapter 3: Getting to Know the Wireless-N Business Notebook Adapter	5
The LED Indicators	5
Chapter 4: Setting up and Connecting the Wireless-N Business Notebook Adapter	6
Starting the Setup	6
Connecting the Adapter	7
Setting up the Adapter	7
Chapter 5: Using the Wireless Network Monitor	17
Accessing the Wireless Network Monitor	17
Using the Wireless Network Monitors	17
Link Information	17
Profiles	20
Create a New Profile	21
Editing a Profile	30
Site Survey	37
Troubleshooting	38
Administration	38
Chapter 6: The Administrative Functions in the Wireless Network Monitor	41
Accessing the Wireless Network Monitor	41
Using the Administrative Functions in the Wireless Network Monitor	41
Classification	42
Security Monitor	46
Appendix A: Troubleshooting	50
Common Problems and Solutions	50
Frequently Asked Questions	51
Appendix B: Windows XP Wireless Zero Configuration	54

Windows XP Wireless Zero Configuration	54
Appendix C: Wireless Security	57
Security Precautions	57
Security Threats Facing Wireless Networks	57
Appendix D: Windows Help	60
Appendix E: Glossary	61
Appendix F: Specifications	66
Appendix G: Warranty Information	68
Appendix H: Regulatory Information	69
Appendix I: Contact Information	75

List of Figures

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

Figure 5-11: Creating Profiles - Manual Setup - Wireless Mode	24
Figure 5-12: Creating Profiles - Manual Setup - Wireless Security - WEP	25
Figure 5-13: Creating Profiles - Manual Setup - Wireless Security - WPA Personal	25
Figure 5-14: Creating Profiles - Manual Setup - Wireless Security - WPA2 Personal	26
Figure 5-15: Creating Profiles - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS	26
Figure 5-16: Creating Profiles - Manual Setup - Wireless Security - WPA Enterprise - PEAP	26
Figure 5-17: Creating Profiles - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS	27
Figure 5-18: Creating Profiles - Manual Setup - Wireless Security - WPA2 Enterprise - PEAP	27
Figure 5-19: Creating Profiles - Manual Setup - Wireless Security - RADIUS	28
Figure 5-20: Creating Profiles - Manual Setup - Wireless Security - LEAP	28
Figure 5-21: Creating Profiles - Manual Setup - Confirm New Settings	29
Figure 5-22: Creating Profiles - Manual Setup - Congratulations	29
Figure 5-23: Editing Profiles - Wireless Mode	30
Figure 5-24: Editing Profiles - Ad Hoc Mode	30
Figure 5-25: Editing Profiles - Wireless Security	31
Figure 5-26: Editing Profiles - Wireless Security - WEP	31
Figure 5-27: Editing Profiles - Wireless Security - WPA Personal	32
Figure 5-28: Editing Profiles - Wireless Security - WPA2 Personal	32
Figure 5-29: Editing Profiles - Wireless Security - WPA Enterprise - EAP-TLS	33
Figure 5-30: Editing Profiles - Wireless Security - WPA Enterprise - PEAP	33
Figure 5-31: Editing Profiles - Wireless Security - WPA2 Enterprise - EAP-TLS	34
Figure 5-32: Editing Profiles - Wireless Security - WPA2 Enterprise - PEAP	34
Figure 5-33: Editing Profiles - Wireless Security - RADIUS	35
Figure 5-34: Editing Profiles - Wireless Security - LEAP	35
Figure 5-35: Editing Profiles - Network Settings	36
Figure 5-36: Editing Profiles - Confirm New Settings	36
Figure 5-37: Editing Profiles - Congratulations	36
Figure 5-38: Site Survey	37
Figure 5-39: Troubleshooting	38
Figure 5-40: Administration	38
Figure 5-41: Administration - Login Access Point Account	39
Figure 5-42: Administration - Modify Access Point Account	39
Figure 5-43: Administration - Security Monitor Account	40
Figure 5-44: Administration - Email Alert	40

Figure 6-1: Wireless Network Monitor Icon	41
Figure 6-2: Administration - Login Security Monitor Account	41
Figure 6-3: Classification	42
Figure 6-4: AP Classification	42
Figure 6-5: Client Classification	43
Figure 6-6: Trusted Mac Address	43
Figure 6-7: Allowed SSID Configuration	44
Figure 6-8: Allowed AP Vendor list Configuration	44
Figure 6-9: Allowed Channel Configuration	45
Figure 6-10: Security Monitor - Channel Usage	46
Figure 6-11: Security Monitor - AP Inventory	46
Figure 6-12: Security Monitor - Client Inventory	47
Figure 6-13: Security Monitor - Alert List	47
Figure 6-14: Security Monitor - POP-UP Alert	48
Figure 6-15: Alert Information	48
Figure 6-16: Security Monitor - Advice	49
Figure B-1: Wireless Network Monitor Icon	54
Figure B-2: Windows XP - Use Windows XP Wireless Configuration	54
Figure B-3: Windows XP Wireless Zero Configuration Icon	54
Figure B-4: Available Wireless Network	55
Figure B-5: No Wireless Security	55
Figure B-6: Network Connection - Wireless Security	56

Chapter 1: Introduction

Welcome

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

How does the Adapter do this? Like all wireless products, the Adapter allows for greater range and mobility within your wireless network, whether it's using the Wireless-G (802.11g) or Wireless-B (802.11b) standard. But with Wireless-N (802.11n), it has even better range and speed.

But what does all of this mean?

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

PCs 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.

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.

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-N 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-N Business Notebook Adapter**
This chapter describes the physical features of the Adapter.
- **Chapter 4: Setting up and Connecting the Wireless-N Business Notebook Adapter**
This chapter instructs you on how to install and configure 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.

802.11n: a wireless networking standard that specifies a maximum data transfer rate of 540Mbps and offers a better operating distance than 802.11a or 802.11g.

bit: a binary digit.

encryption: encoding data transmitted in a network

- **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.
- **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. The wireless-N Business Notebook Adapter uses 802.11n, the latest wireless networking technology. It will be backward compatible with previous 802.11g and 802.11b equipment. Wireless products will also communicate with the wireless PrintServer.

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-N Business Notebook Adapter

The LED Indicators

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



Figure 3-1: Front Panel

Wireless *Blue.* The Power LED lights up when the Adapter's wireless networking is enabled.

Activity *Blue.* The Link LED lights up when the Adapter has an active connection.

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

Starting the Setup

The Wireless-N 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

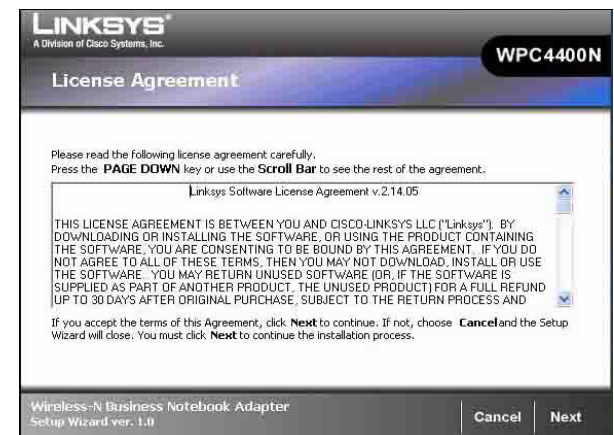


Figure 4-2: Setup Wizard's License Agreement

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**.

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.



Figure 4-3: Connecting the Adapter

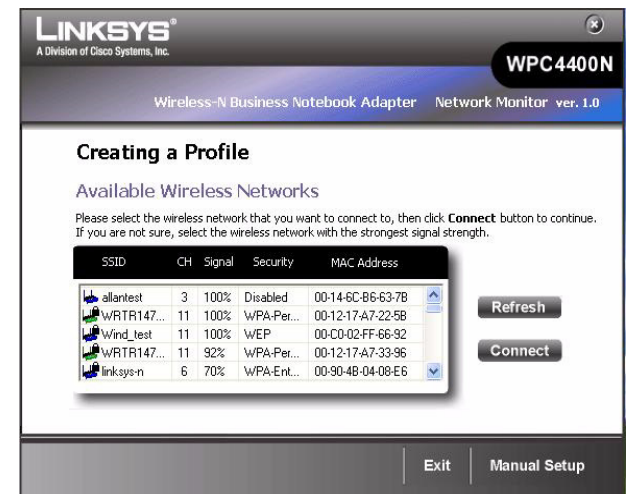


Figure 4-4: Available Wireless Network

2. **Wireless Security** If your network has WEP or WPA Personal wireless security enabled, then that security screen will appear. Continue to the screen for your wireless security.

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 10.

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.

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.

LINKSYS[®]
A Division of Cisco Systems, Inc.

WPC4400N

Wireless-N Business Notebook Adapter Network Monitor ver. 1.0

WEP Key Needed for Confirmation

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.

Security: WEP

WEP: 64-bit

Passphrase:

WEP Key 1:

Please select the method used by your existing wireless network.

To use WEP encryption, select 64-bit or 128-bit.

The Passphrase is case-sensitive and should be no more than 16 characters in length.

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".

Cancel Connect

Figure 4-5: WEP Key Needed for Connection

LINKSYS[®]
A Division of Cisco Systems, Inc.

WPC4400N

Wireless-N Business Notebook Adapter Network Monitor ver. 1.0

WPA-Personal Needed for Confirmation

This wireless network has WPA-Personal, also known as Pre-Shared Key, enabled. To connect to this network, select the encryption type. Enter the required passphrase in the appropriate field below. Then click the Connect button.

Passphrase:

Please enter a Passphrase that is 8 to 63 characters in length.

Cancel Connect

Figure 4-6: WPA - Personal Needed for Connection

3. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network. For more information about the Wireless Network Monitor, refer to *Chapter 5: Using the Wireless Network Monitor*.

Congratulations! The installation of the Wireless-N 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.

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.



Figure 4-7: 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 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.

The screenshot shows the 'Creating a Profile' screen in the Linksys WPC4400N Network Monitor. Under the 'Network Settings' section, the 'Obtain a network settings automatically (DHCP)' option is selected. Below this, there are input fields for IP Address, Subnet Mask, Default Gateway, DNS 1, and DNS 2. The 'Back' and 'Next' buttons are at the bottom right.

Figure 4-8: Creating a Profile

The screenshot shows the 'Creating a Profile' screen in the Linksys WPC4400N Network Monitor, specifically the 'Wireless Mode' section. The 'Infrastructure Mode' radio button is selected. Below it, there is a text input field for the SSID, which currently contains 'linksys'. A note states: 'The SSID (Service Set Identifier) is the wireless network name shared by all devices in a wireless network. Note: The SSID is case-sensitive.' The 'Back' and 'Next' buttons are at the bottom right.

Figure 4-9: Network Settings - Wireless Mode

4. 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.

5. 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.

The screenshot shows the 'Creating a Profile' window for the WPC4400N adapter. The title bar indicates 'WPC4400N' and 'Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' with a sub-heading 'Ad-Hoc Mode Settings'. A 'Channel' dropdown menu is set to '11'. To the right of the dropdown, it says 'Select the Channel used by all of the devices in your wireless network.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-10: Ad-Hoc Mode Settings

The screenshot shows the 'Creating a Profile' window for the WPC4400N adapter, specifically the 'Wireless Security - WEP' section. The title bar indicates 'WPC4400N' and 'Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' with a sub-heading 'Wireless Security - WEP'. The 'WEP' dropdown is set to '64-bit'. To the right, it says 'To use WEP encryption, select 64-bit or 128-bit.' Below this, there are fields for 'Passphrase' and 'WEP Key'. To the right of these fields, it says 'The Passphrase is case-sensitive and should be no more than 16 characters in length. 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".' Below these fields, there is a section for 'Advanced Users' with a 'TX Key' dropdown set to '1' and an 'Authentication' dropdown set to 'Open system'. To the right of these dropdowns, it says 'Select the transmit key for your network. (Default: 1)' and 'Select your network authentication type. (Default: Auto)'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-11: 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.

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.

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Personal'. The interface includes a header with the Linksys logo and 'WPC4400N'. Below the header, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main content area has a title 'Creating a Profile' and a subtitle 'Wireless Security - WPA Personal'. There are two input fields: 'Encryption' with a dropdown menu currently set to 'TKIP', and 'Passphrase' with a text input field. Both fields have placeholder text: 'Please select an encryption type used to protect your wireless data transmissions.' and 'Please enter a Passphrase that is 8 to 63 characters in length.' respectively. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-12: Wireless Security - WPA Personal

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Personal'. The interface is similar to Figure 4-12, with the Linksys logo and 'WPC4400N' in the header. The subtitle is 'Wireless Security - WPA2 Personal'. There is a single input field labeled 'Passphrase' with the placeholder text 'Please enter a Passphrase that is 8 to 63 characters in length.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-13: 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). 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 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The interface includes the Linksys logo and 'A Division of Cisco Systems, Inc.' at the top. The title bar indicates 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0' and 'WPC4400N'. The main content area has the following fields and instructions:

- Authentication:** EAP-TLS (selected). Instruction: Please select the authentication method that you use to access your network.
- Login Name:** (empty). Instruction: Enter the Login Name used for authentication.
- Server Name:** (empty). Instruction: Enter the Server Name used for authentication. (Optional)
- Certificate:** (empty). Instruction: Please select the certificate used for authentication.
- Encryption:** AES (selected). Instruction: Please select the encryption type used to protect the wireless data transmissions.

At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-14: Wireless Security - WPA Enterprise-EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The interface includes the Linksys logo and 'A Division of Cisco Systems, Inc.' at the top. The title bar indicates 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0' and 'WPC4400N'. The main content area has the following fields and instructions:

- Authentication:** PEAP (selected). Instruction: Please select the authentication method that you use to access your network.
- Login Name:** (empty). Instruction: Enter the Login Name used for authentication.
- Password:** (empty). Instruction: Enter the Password used for authentication.
- Server Name:** (empty). Instruction: Enter the Server Name used for authentication. (Optional)
- Certificate:** Trust Any (selected). Instruction: Please select the certificate used for authentication.
- Inner Authn:** EAP-MSCHAPv2 (selected). Instruction: Please select the inner authentication method used inside the PEAP tunnel.
- Encryption:** AES (selected). Instruction: Please select the encryption type used to protect the wireless data transmissions.

At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-15: 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 interface includes the Linksys logo and 'WPC4400N' model number. The title bar indicates 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main content area has the following fields and options:

- Authentication:** EAP-TLS (selected). Description: Please select the authentication method that you use to access your network.
- Login Name:** (empty text field). Description: Enter the Login Name used for authentication.
- Server Name:** (empty text field). Description: Enter the Server Name used for authentication. (Optional)
- Certificate:** (empty dropdown menu). Description: Please select the certificate used for authentication.
- Encryption:** AES (selected). Description: 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 - WPA2 Enterprise-EAP

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The interface includes the Linksys logo and 'WPC4400N' model number. The title bar indicates 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main content area has the following fields and options:

- Authentication:** PEAP (selected). Description: Please select the authentication method that you use to access your network.
- Login Name:** (empty text field). Description: Enter the Login Name used for authentication.
- Password:** (empty text field). Description: Enter the Password used for authentication.
- Password Mode:** Static (selected). Description: Please select the password mode used for authentication.
- Server Name:** (empty text field). Description: Enter the Server Name used for authentication. (Optional)
- Certificate:** Trust Any (selected). Description: Please select the certificate used for authentication.
- Inner Authen.:** EAP-MSCHAPv2 (selected). Description: Please select the inner authentication method used inside the PEAP tunnel.
- Encryption:** AES (selected). Description: 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 - 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 Linksys WPC4400N Network Monitor interface. The title bar indicates 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main content area is titled 'Creating a Profile' and 'Wireless Security - RADIUS'. It features a form with the following 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 4-18: Wireless Security - RADIUS - EAP-TLS

The screenshot shows the Linksys WPC4400N Network Monitor interface. The title bar indicates 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main content area is titled 'Creating a Profile' and 'Wireless Security - RADIUS'. It features a form with the following fields: 'Authentication' (set to PEAP), 'Login Name', 'Password', 'Server Name', 'Certificate' (set to Trust Any), 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)', 'Please select the certificate used for authentication.', and 'Please select the inner authentication method used inside the PEAP tunnel.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-19: 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.

Figure 4-20: Wireless Security - LEAP



Figure 4-21: 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 Link Information Tab displays signal strength and link quality information about the current connection. It also provides tabs to click for additional connection information.

Signal Strength - The Signal Strength bar indicates signal strength with Red, Yellow, and Green colors to differentiate among low, medium and high strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection with Red, Yellow, and Green colors to differentiate among low, medium and high quality.

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



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.

Radio Band - This shows the radio band used on the wireless network.

SSID - Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN. This is the unique name of the wireless network which differentiates one wireless network to another.

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

Wide Channel - This displays the Wireless-N primary channel used with a 40 MHz radio band network.

Standard Channel - This displays the channel used by your wireless network.

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

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

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

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.

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.

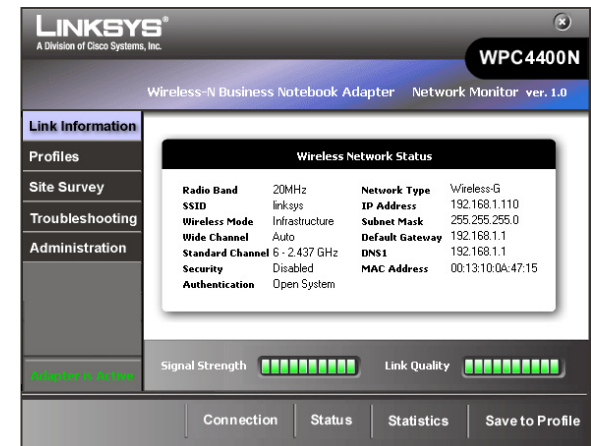


Figure 5-3: Link Information- Wireless Network Status

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 output at which the Adapter is transmitting. Transmit power is the amount of power used by a radio transceiver to send the signal out. It is generally measured in milliwatts, which you can convert to dBm. For a typical Wireless-N network, it is estimated to be at 10dBm in average. Here it states as auto to mean the network is transmitting at an average Wireless-N power output.

Up Time - This indicates the length of the most recent connection to a wireless network.

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.

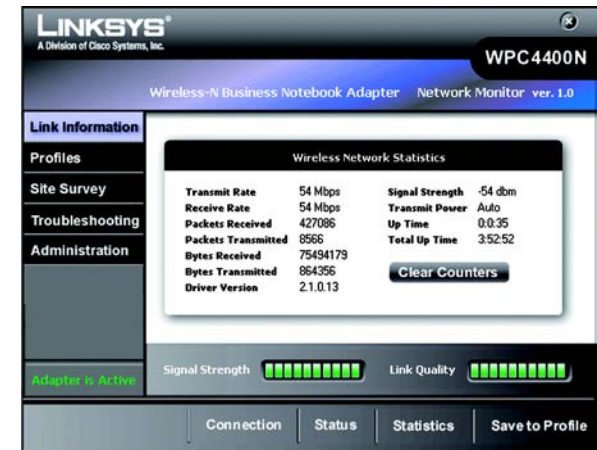


Figure 5-4: Link Information - Wireless Network Statistics

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.

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

Authentication - The authentication setting for the network is shown 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, “Editing 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 have to export them one at a time.

NOTE: Default profile cannot be deleted.



Figure 5-5: Profiles

Create a New Profile

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

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. 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 the wireless security WEP (Wired Equivalent Privacy), this screen will appear.

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.)



Figure 5-6: Creating Profiles - Available Wireless Network

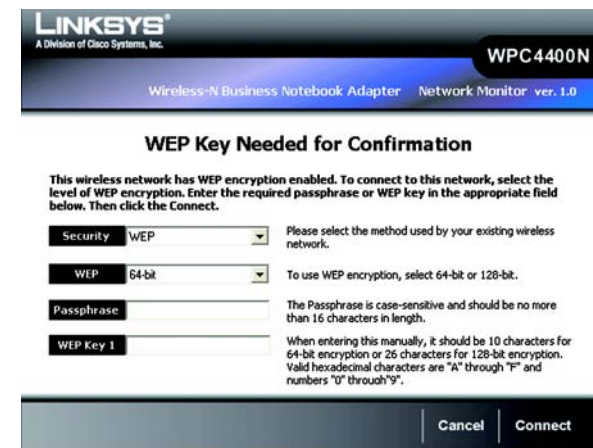


Figure 5-7: Creating Profiles - WEP Key Needed

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.

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.

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.

For connecting with other authentication method, please see the next section "Manual Setup" on page 23.

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.

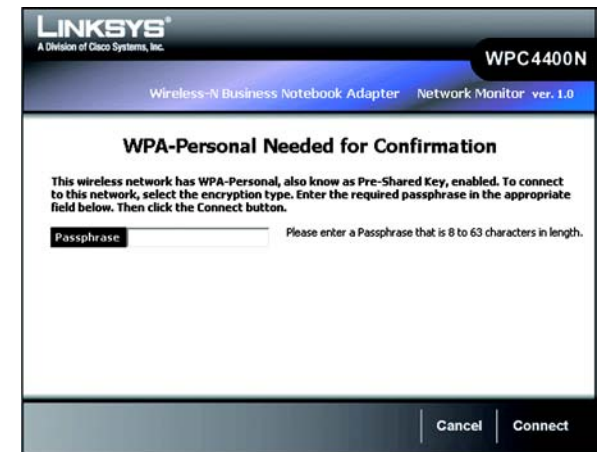


Figure 5-8: Creating Profiles - WPA-Personal Needed



Figure 5-9: Creating Profiles - 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 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 5-10: Creating Profiles - Manual Setup - Network Settings

- 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.

- 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.



Figure 5-11: Creating Profiles - Manual Setup - Wireless Mode

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.

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.

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.

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.

The screenshot shows the 'Creating a Profile' window for 'Wireless Security - WEP'. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC4400N'. Below that, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main title is 'Creating a Profile' and the subtitle is 'Wireless Security - WEP'. There are five main sections: 'WEP' with a dropdown set to '64-bit', 'Passphrase' with a text field, 'WEP Key' with a text field, 'TX Key' with a dropdown set to '1', and 'Authentication' with a dropdown set to 'Open system'. To the right of these fields are instructions: 'To use WEP encryption, select 64-bit or 128-bit.', 'The Passphrase is case-sensitive and should be no more than 16 characters in length.', '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".', 'Select the transmit key for your network. (Default: 1)', and 'Select your network authentication type. (Default: Auto)'. At the bottom right are 'Back' and 'Next' buttons.

Figure 5-12: Creating Profiles - Manual Setup - Wireless Security - WEP

The screenshot shows the 'Creating a Profile' window for 'Wireless Security - WPA Personal'. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WPC4400N'. Below that, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main title is 'Creating a Profile' and the subtitle is 'Wireless Security - WPA Personal'. There are two main sections: 'Encryption' with a dropdown set to 'TKIP' and 'Passphrase' with a text field. To the right of these fields are instructions: 'Please select an encryption type used to protect your wireless data transmissions.' and 'Please enter a Passphrase that is 8 to 63 characters in length.'. At the bottom right are 'Back' and 'Next' buttons.

Figure 5-13: Creating Profiles - Manual Setup - 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.

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). 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.



Figure 5-14: Creating Profiles - Manual Setup - Wireless Security - WPA2 Personal



Figure 5-15: Creating Profiles - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS



Figure 5-16: Creating Profiles - 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). 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 interface includes a header with the Linksys logo and 'WPC4400N'. Below the header, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main content area has a title 'Creating a Profile' and a subtitle 'Wireless Security - WPA2 Enterprise'. There are five fields with dropdown menus: 'Authentication' (set to EAP-TLS), 'Login Name' (empty), 'Server Name' (empty), 'Certificate' (empty), and 'Encryption' (set to AES). Each field has a corresponding instruction to its right. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-17: Creating Profiles - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The interface is similar to Figure 5-17 but with different settings. The 'Authentication' dropdown is set to PEAP. The 'Login Name' field is empty. The 'Password' field is empty, and the 'Password Mode' dropdown is set to Static. The 'Server Name' field is empty. The 'Certificate' dropdown is set to Trust Any. The 'Inner Authen.' dropdown is set to EAP-MSCHAPv2. The 'Encryption' dropdown is set to AES. Each field has a corresponding instruction to its right. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-18: Creating Profiles - 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). 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.

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username 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.

LINKSYS®
A Division of Cisco Systems, Inc.

WPC4400N

Wireless-N Business Notebook Adapter Network Monitor ver. 1.0

Creating a Profile

Wireless Security - RADIUS

Authentication: EAP-TLS Please select the authentication method that you use to access your network.

Login Name: Enter the Login Name used for authentication.

Server Name: Enter the Server Name used for authentication. (Optional)

Certificate: Please select the certificate used for authentication.

Back Next

Figure 5-19: Creating Profiles - Manual Setup - Wireless Security - RADIUS

LINKSYS®
A Division of Cisco Systems, Inc.

WPC4400N

Wireless-N Business Notebook Adapter Network Monitor ver. 1.0

Creating a Profile

Wireless Security - LEAP

Login Method: Manual Login Select the login method you want to use.

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 5-20: Creating Profiles - Manual Setup - Wireless Security - LEAP

- 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**.



Figure 5-21: Creating Profiles - Manual Setup - Confirm New Settings

- 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 5-22: Creating Profiles - Manual Setup - Congratulations

Editing a Profile

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. Following the steps below to complete the task:

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 Step3 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 5-23: Editing Profiles - Wireless Mode



Figure 5-24: Editing Profiles - Ad Hoc Mode

3. 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 5-25: Editing Profiles - Wireless Security



Figure 5-26: Editing Profiles - 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.

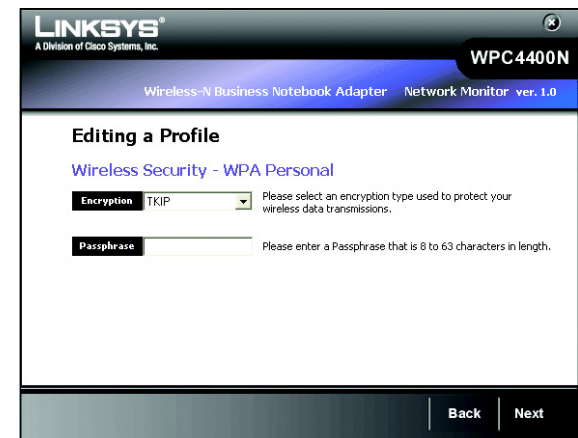


Figure 5-27: Editing Profiles - Wireless Security-WPA Personal

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.

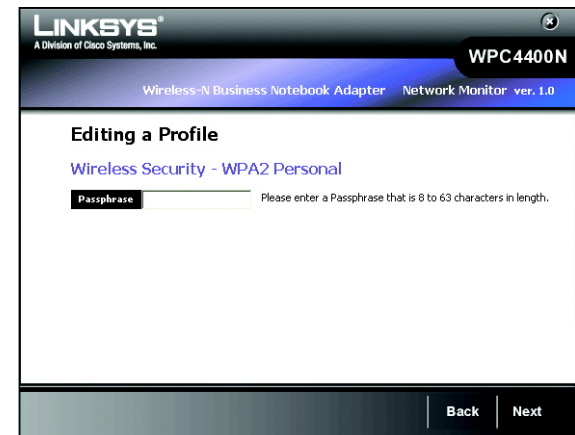


Figure 5-28: Editing Profiles - Wireless Security - WPA2 Personal

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 interface includes a header with the Linksys logo and 'WPC4400N'. Below the header, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main content area has a title 'Editing a Profile' and a subtitle 'Wireless Security - WPA Enterprise'. There are five form fields: 'Authentication' (set to EAP-TLS), 'Login Name' (empty), 'Server Name' (empty), 'Certificate' (empty), and 'Encryption' (set to 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 5-29: Editing Profiles - Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The interface includes a header with the Linksys logo and 'WPC4400N'. Below the header, it says 'Wireless-N Business Notebook Adapter Network Monitor ver. 1.0'. The main content area has a title 'Editing a Profile' and a subtitle 'Wireless Security - WPA2 Enterprise'. There are seven form fields: 'Authentication' (set to PEAP), 'Login Name' (empty), 'Password' (empty), 'Server Name' (empty), 'Certificate' (set to Trust Any), 'Inner Authen.' (set to EAP-MSCHAPv2), and 'Encryption' (set to 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 certificate used for authentication.', '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 5-30: Editing Profiles - 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 'LINKSYS' logo at the top left, 'A Division of Cisco Systems, Inc.' below it, and 'WPC4400N' at the top right. Below the header is 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main title is 'Editing a Profile' with a sub-title 'Wireless Security - WPA2 Enterprise'. The form has the following fields: 'Authentication' (EAP-TLS), 'Login Name' (empty), 'Server Name' (empty), 'Certificate' (empty), 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 are 'Back' and 'Next' buttons.

Figure 5-31: Editing Profiles - Wireless Security - WPA2 Enterprise - EAP-TLS

The screenshot shows the 'LINKSYS' logo at the top left, 'A Division of Cisco Systems, Inc.' below it, and 'WPC4400N' at the top right. Below the header is 'Wireless-N Business Notebook Adapter' and 'Network Monitor ver. 1.0'. The main title is 'Editing a Profile' with a sub-title 'Wireless Security - WPA2 Enterprise'. The form has the following fields: 'Authentication' (PEAP), 'Login Name' (empty), 'Password' (empty), 'Server Name' (empty), 'Certificate' (Trust Any), '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.', 'Please select the inner authentication method used inside the PEAP tunnel.', 'Enter the Server Name used for authentication. (Optional)', 'Please select the certificate used for authentication.', 'Please select the encryption type used to protect the wireless data transmissions.', and 'Please select the authentication method that you use to access your network.' At the bottom right are 'Back' and 'Next' buttons.

Figure 5-32: Editing Profiles - 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.

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username 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.

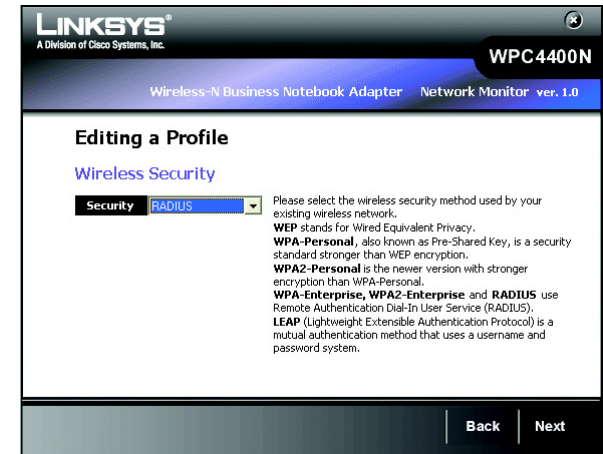


Figure 5-33: Editing Profiles - Wireless Security - RADIUS

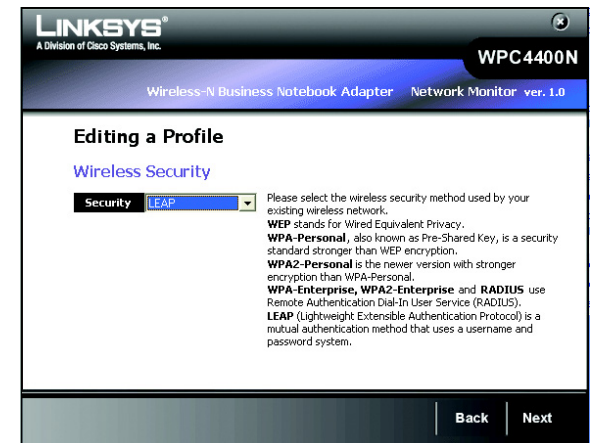


Figure 5-34: Editing Profiles - Wireless Security - LEAP

- 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.

- 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 5-35: Editing Profiles - Network Settings

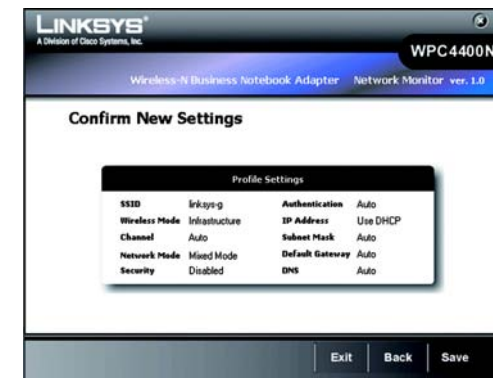


Figure 5-36: Editing Profiles - Confirm New Settings



Figure 5-37: Editing Profiles - 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.

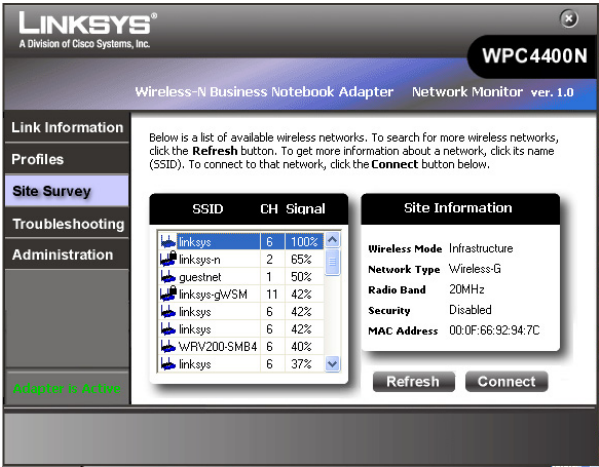


Figure 5-38: Site Survey

For more information about classification of the Access Points, please see section "AP Classification" of Chapter 6.

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-a, wireless-b,wireless-g or wireless-n 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.

Troubleshooting

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

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

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

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 station 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.

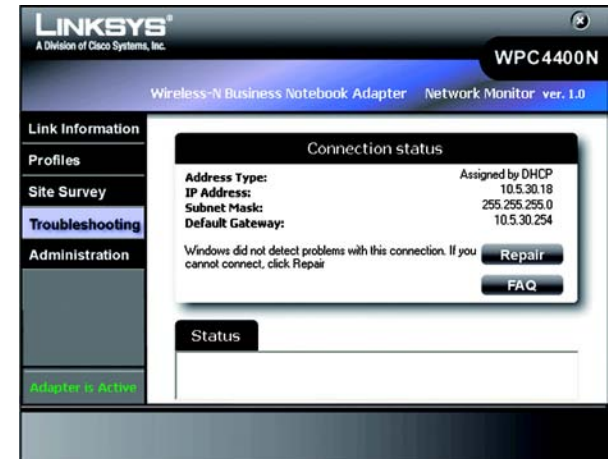


Figure 5-39: Troubleshooting

Administration

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

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

Enter the Security Monitor's account name and password and retype the password in the confirm field. Click **Next** to proceed with more administrative options.

Once you have logged in successfully, the Classification and Security Monitor Tab appears. Please see the next chapter "The Administrative Functions in the Wireless Network Monitor" on page 41 for more information.



Figure 5-40: Administration