



# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WAP4400N. You'll find the answers to all your questions on the LINKSYS WAP4400N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

**User manual LINKSYS WAP4400N**  
**User guide LINKSYS WAP4400N**  
**Operating instructions LINKSYS WAP4400N**  
**Instructions for use LINKSYS WAP4400N**  
**Instruction manual LINKSYS WAP4400N**

**LINKSYS®**  
A Division of Cisco Systems, Inc.



**Wireless-N Access Point  
with Power Over Ethernet**

Model No. WAP4400N



USER GUIDE

BUSINESS SERIES



[You're reading an excerpt. Click here to read official LINKSYS WAP4400N user guide](http://yourpdfguides.com/dref/344788)  
<http://yourpdfguides.com/dref/344788>

**Manual abstract:**

@@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. @@@@Wash hands after handling. How to Use this User Guide The user guide to the Wireless-G Exterior Access Point has been designed to make understanding networking with the Access Point easier than ever. Look for the following items when reading this User Guide: This checkmark means there is a note of interest and is something you should pay special attention to while using the Access Point. This exclamation point means there is a caution or warning and is something that could damage your property or the Access Point.

This question mark provides you with a reminder about something you might need to do while using the Access Point. In addition to these symbols, there are definitions for technical terms that are presented like this: word: definition. Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this: Figure 0-1: Sample Figure Description Figure numbers and descriptions can also be found in the "List of Figures" section.

WAP4400N-UG-60519NC BW Wireless-N Access Point with Power Over Ethernet Table of Contents Chapter 1: Introduction Welcome What's in this User Guide? 1 1 2 Chapter 2: Planning Your Wireless Network Network Topology Roaming Network Layout Example of a simple wireless network 4 4 4 4 5 Chapter 3: Getting to Know the Wireless-G Exterior Access Point The LEDs The Ports Antennas and Positions 7 7 8 9 Chapter 4: Connecting the Wireless-N Access Point Overview Connection Placement Options 11 11 11 12 Chapter 5: Setting Up the Wireless-N Access Point Overview Accessing the Utility Navigating the Utility 13 13 13 14 Chapter 6: Configuring the Wireless-N Access Point The Setup - Basic Setup Tab The Setup - Time Tab The Wireless - Basic Wireless Settings Tab The Wireless - Wireless Security Tab The Wireless - Wireless Connection Control Tab The Wireless - Advanced Wireless Settings Tab The Security Monitor Tab The Administration - Management Tab The Administration - Log Tab The Administration - Factory Default Tab The Administration - Firmware Upgrade Tab 16 16 17 18 20 24 25 27 28 30 32 32 Wireless-N Access Point with Power Over Ethernet The Administration - Reboot Tab The Administration - Config Management Tab The Status - Local Network Tab The Status - Wireless Tab The Status - System Performance Tab 33 34 35 36 37 Appendix A: Troubleshooting Frequently Asked Questions 39 39 Appendix B: Wireless Security Security Precautions Security Threats Facing Wireless Networks 44 44 44 Appendix C: Upgrading Firmware Appendix D: Windows Help Appendix E: Glossary Appendix F: Specifications Appendix G: Warranty Information Appendix H: Regulatory Information Appendix I: Contact Information 47 48 49 54 56 57 63 Wireless-N Access Point with Power Over Ethernet List of Figures Figure 2-1: Example of a Simple Wireless Network Figure 3-1: Front Panel Figure 3-2: Back View Figure 3-3: Stackable Position and its Antenna Setup Figure 3-4: Standalone Position and its Antenna Setup Figure 4-1: Connect the Ethernet Cable Figure 4-2: Connect the Power Figure 4-3: The Stand Option Figure 4-4: Stand Figure 4-5: Mounting Dimensions Figure 5-1: Login Screen Figure 6-1: Setup - Static IP Address Figure 6-2: Setup - Automatic Configuration - DHCP Figure 6-3: Setup - Time Figure 6-4: Wireless - Basic Wireless Settings Figure 6-5: Pop-up message on Auto Channel Selection Figure 6-6: Wireless - Wireless Security (Disabled) Figure 6-7: Wireless - Wireless Security (WPA-Personal) Figure 6-8: Wireless - Wireless Security (WPA2-Personal) Figure 6-9: Wireless - Wireless Security (WPA2-Personal Mixed) Figure 6-10: Wireless - Wireless Security (WPA-Enterprise) Figure 6-11: Wireless - Wireless Security (WPA2-Enterprise) Figure 6-12: Wireless - Wireless Security (WPA2 - Enterprise Mixed) Figure 6-13: Wireless Settings - WEP Figure 6-14: Wireless - Wireless Connection Control Figure 6-15: Select MAC Address from Wireless Client List Figure 6-16: Wireless - Advanced Wireless Figure 6-17: Security Monitor 5 7 8 9 10 11 11 12 12 12 14 16 17 17 18 18 20 20 21 21 22 22 23 23 24 24 25 27 Wireless-N Access Point with Power Over Ethernet Figure 6-18: Administration - Management Figure 6-19: The Administration - Log Figure 6-20: Administration - Factory Default Figure 6-21: Administration - Firmware Upgrade Figure 6-22: Administration - Reboot Figure 6-23: Administration - Config Management Figure 6-24: Status - Local Network Figure 6-25: Status - Wireless Figure 6-26: Status - System Performance Figure C-1: Firmware Upgrade 28 30 32 32 33 34 35 36 37 47 Wireless-N Access Point with Power Over Ethernet Chapter 1: Introduction Welcome Thank you for choosing the Wireless-N Access Point with Power Over Ethernet. This Access Point will allow you to network wirelessly better than ever.

An access point allows for greater range and mobility within your wireless network while also allowing you to connect the wireless network to a wired environment. The Wireless-N Access Point also offers the convenience of Power over Ethernet (PoE) capability (in addition to regular 12VDC power adaptor), so it can receive data and power over a single Ethernet network cable. This Access Point supports the latest 802.11n draft Specification by IEEE early 2006. It also support 802.

11g and 802.11b clients in a mixed environment. This Access Point currently can support an 11n data rate up to 300 Mbps. Besides the higher data rate, 802.11n technology also promises longer coverage by using multiple antennas to transmit and receive data streams in different directions. Users are encouraged to update their firmware through [www.linksys.com](http://www.linksys.com) when 802.11n specification is finalized by IEEE to ensure compatibility with all the wireless-N devices. Networks are useful tools for sharing computer resources.

You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun. PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless client cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. The Access Point bridges wireless networks of 802.11n, 802.

11g and 802.11b standards and wired networks. Use the instructions in this Guide to help you connect the Access Point, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Access Point.



**[You're reading an excerpt. Click here to read official LINKSYS WAP4400N user guide](http://yourpdfguides.com/dref/344788)**  
<http://yourpdfguides.com/dref/344788>

*access point: a device that allows wireless-equipped computers and other devices to communicate with each other and with devices on a wired network. Also used to expand the range of a wireless network. network: a series of computers or devices connected together. lan (local area network): the computers and networking devices that make up your local network. poe (power over ethernet): a technology enabling an Ethernet network cable to deliver both data and power. ethernet: network protocol defined in IEEE 802.*

*3 standard that specifies how data is placed on and retrieved from a common transmission medium. adapter: a device that adds network functionality to your PC. 802.11n: wireless networking draft standard that specifies a maximum data rate up to 600Mbps (300Mbps supported by this device), an operating frequency of 2.4GHz, and backward compatibility with 802.11b/g devices. 802.11g: a wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

*802.11b: a wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz. Chapter 1: Introduction Welcome 1 Wireless-N Access Point with Power Over Ethernet What's in this User Guide? This user guide covers the steps for setting up and using the Wireless-N Access Point. · Chapter 1: Introduction This chapter describes the Wireless-N Access Point's applications and this User Guide. · Chapter 2: Planning your Wireless Network This chapter describes the basics of wireless networking. · Chapter 3: Getting to Know the Wireless-N Access Point This chapter describes the physical features of the Access Point. · Chapter 4: Connecting the Wireless-N Access Point This chapter instructs you on how to connect your Access Point to your network and placement options. · Chapter 5: Setting up the Wireless-N Access Point This chapter explains how to perform the most basic setting changes through the Web-based Utility. · Chapter 6: Configuring the Wireless-G Exterior Access Point This chapter provides a reference for the available configuration through the Web-based Utility.*

*· Appendix A: Troubleshooting This appendix describes some frequently asked questions regarding installation and use of the Wireless-G Exterior Access Point. · Appendix B: Wireless Security This appendix explains the risks of wireless networking and some solutions to reduce the risks. · Appendix C: Upgrading Firmware This appendix instructs you on how to upgrade the Access Point's firmware. · Appendix D: Windows Help. This appendix describes some of the ways Windows can help you with wireless networking.*

*· Appendix E: Glossary This appendix gives a brief glossary of terms frequently used in networking. · Appendix F: Specifications This appendix provides the Access Point's technical specifications. Chapter 1: Introduction What's in this User Guide? 2 Wireless-N Access Point with Power Over Ethernet · Appendix G: Warranty Information This appendix supplies the Access Point's warranty information. · Appendix H: Regulatory Information This appendix supplies the Access Point's regulatory information. · Appendix I: Contact Information This appendix provides contact information for a variety of Linksys resources, including Technical Support.*

*Chapter 1: Introduction What's in this User Guide? 3 Wireless-N Access Point with Power Over Ethernet Chapter 2: Planning Your Wireless Network Network Topology A wireless network is a group of computers, each equipped with one or more wireless adapters. Computers in a wireless network must be configured to share the same radio channel to talk to each other. Several PCs equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point. Linksys also provides products to allow wireless adapters to access wired network through a bridge such as the wireless 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 or wireless network via the access point or wireless router. An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an Access Point is able to forward data within a network, the effective transmission range in an infrastructure network may be more than doubled since Access Point can transmit signal at higher power to the wireless space. 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 Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same wireless network (SSID) and wireless security. The Ethernet network port connects to Ethernet network devices, such as a switch or router that may or may not support Power over Ethernet (PoE). There are two ways to reset the Access Point to the factory default configuration. Either press the Reset button, for approximately ten seconds, or restore the defaults using the Access Point's Web-based Utility. IMPORTANT: Resetting the Access Point will erase all of your settings (including wireless security, IP address, and SSID) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings. Reset Button Antennas and Positions The Access Point's port are located on the back of the device. The Access Point can be placed in three different positions. It can be either stackable, standalone, or wall-mount.*

*Antenna The Access Point has three non-detachable 2dBi omni-directional antennas. The three antennas have a base that can rotate 90 degrees when in the standing position. The three antennas will all be used to support 2X3 MIMO diversity in wireless-N mode. Figure 3-3: Stackable Position and its Antenna Setup Chapter 3: Getting to Know the Wireless-G Exterior Access Point Antennas and Positions 9 Wireless-N Access Point with Power Over Ethernet Figure 3-4: Standalone Position and its Antenna Setup Chapter 3: Getting to Know the Wireless-G Exterior Access Point Antennas and Positions 10 Wireless-N Access Point with Power Over Ethernet Chapter 4: Connecting the Wireless-N Access Point Overview This chapter explains how to place and connect the Access Point. Depending on your application, you might want to set up the device first before mounting the device.*



[You're reading an excerpt. Click here to read official LINKSYS WAP4400N user guide](http://yourpdfguides.com/dref/344788)  
<http://yourpdfguides.com/dref/344788>

Refer to "Chapter 5: Setting Up the Wireless-N Access Point". hardware: the physical aspect of computers, telecommunications, and other information technology devices. Connection 1. Connect your Ethernet network cable to your network router or switch. Then connect the other end of the network cable to the Access Point's Ethernet port.

2. If you are using Power Over Ethernet (POE), proceed to the following section, "Placement Options." If you are not using POE, then connect the included power adapter to the Access Point's Power port. Then plug the power adapter into an electrical outlet. The LEDs on the front panel will light up as soon as the Access Point powers on. Proceed to the following section, "Placement Options." Figure 4-1: Connect the Ethernet Cable Figure 4-2: Connect the Power Chapter 4: Connecting the Wireless-N Access Point Overview 11 Wireless-N Access Point with Power Over Ethernet Placement Options There are three ways to place the Wireless-N Access Point. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Access Point vertically on a surface. The third way is to mount it on a wall.

The stand and wall-mount options are explained in further detail below. Stand Option 1. Locate the Access Point's left side panel. 2. The Access Point includes two stands. With the two large prongs facing outward, insert the short prongs into the little slots in the Access Point, and push the stand upward until it snaps into place. Repeat this step with the other stand. Now that the hardware installation is complete, proceed to "Chapter 5: Setting up the Wireless-N Access Point," for directions on how to set up the Access Point." Figure 4-3: The Stand Option Large Prongs Wall-Mount Option 1. On the Access Point's back panel are two criss-cross wall-mount slots.

2. Determine where you want to mount the Access Point, and install two screws that are 2-15/16" apart. 3. Line up the Access Point so that the wall-mount slots line up with the two screws. 4.

Place the wall-mount slots over the screws and slide the Access Point down until the screws fit snugly into the wall-mount slots. Now that the hardware installation is complete, proceed to "Chapter 5: Setting up the Wireless-N Access Point," for directions on how to set up the Access Point." Figure 4-5: Mounting Dimensions Chapter 4: Connecting the Wireless-N Access Point Placement Options Figure 4-4: Stand 2-15/16" 12 Wireless-N Access Point with Power Over Ethernet Chapter 5: Setting Up the Wireless-N Access Point Overview The Access Point has been designed to be functional right out of the box with the default settings. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the Webbased Utility. This chapter explains how to use the Utility to perform the most basic settings.

The Utility can be accessed via web browsers, such as Microsoft Internet Explorer or Mozilla Firefox through the use of a computer that is networked with the Access Point. For a basic network setup, most users only have to use the following screens of the Utility: · Setup On the Setup screen, enter your basic network settings (IP address) here. · Management Click the Administration tab and then select the Management screen. The Access Point's default password is admin. To secure the Access Point, change the AP Password from its default. Most users will also customize their wireless settings: · Wireless On the Wireless screen, change default SSID under the Basic Wireless Settings Tab. Select the level of security under the Wireless Security Tab and complete the options for the selected security mode. HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP. tcp/ip: a set of protocols PCs use to communicate over a network.

browser: an application that provides a way to look at and interact with all the information on the World Wide Web. Accessing the Utility There are three ways to connect to your Access Point for the first time. 1. If you have a 48VDC Power Injector (e.g. Linksys WAPPOE), power up your Access Point first, then connect the Injector's cable to your PC. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address (192.168.1.245).

2. If you have a PoE switch (e.g. Linksys SRW224P), connect your Access Point and your PC to the same network. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address (192.

168.1.245). Or if there is a DHCP server connected to the switch, configure it to assign the IP address in 192.168.

1.0/24 subnet. Your PC will get an IP address in the subnet through the DHCP. Chapter 5: Setting Up the Wireless-N Access Point Overview 13 Wireless-N Access Point with Power Over Ethernet 3. Although it is not recommended, you can connect your PC wirelessly to the Access Point when the DHCP server is connected on the LAN side. It is not recommended, because you can easily lose your connection through configuration changes. Launch your web browser, such as Internet Explorer or Mozilla Firefox and enter the Access Point's default IP address, 192.168.1.245, in the Address field.

Press the Enter key. Enter admin in the User Name field. The first time you open the Web-based Utility, use the default password, admin. (You can set a new password from the Administration - Management tab.) Then click the OK button. After setting up the Access Point to use DHCP or manually configure a new IP address, move your Access Point to the desired network. You will have to use the new IP address the next time you access the Web-based Utility.

Navigating the Utility Figure 5-1: Login Screen The Web-based Utility consists of the following five main tabs: Setup, Wireless, Security Monitor, Administration, and Status. Additional screens (sub tabs) will be available from most of the main tabs. The following briefly describes the main & sub tabs of the Utility.

Setup Enter the Host Name, IP Address settings, and set the time on this screen. · Basic Setup. Configure the host name and IP address settings for this Access Point. · Time. Set the time on this Access Point.

Wireless You will use the Wireless tabs to enter a variety of wireless settings for the Access Point. · Basic Wireless Settings. Choose the wireless network mode (e.g. B/G/N-Mixed), SSID, and radio channel on this screen.

· Wireless Security. Use this screen to configure the Access Point's security settings. · Wireless Connection Control. Use this screen to control the wireless connections from client devices to this Access Point. Chapter 5: Setting Up the Wireless-N Access Point Navigating the Utility 14 Wireless-N Access Point with Power Over Ethernet · Advanced Wireless Settings.



[You're reading an excerpt. Click here to read official LINKSYS WAP4400N user guide](http://yourpdfguides.com/dref/344788)  
<http://yourpdfguides.com/dref/344788>

Use this screen to configure the Access Point's more advanced wireless settings (e.g. Tx Rate Limiting, Channel Bandwidth, etc.). Security Monitor Use this screen to configure the Access Point's security monitor capabilities.

You will be able to monitor your wireless network through a client utility on administrator's PC. This feature works with WPC4400N and future Linksys client devices. Administration You will use the Administration tabs to manage the Access Point. Management. This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings. Log. Configure the Log settings for the Access Point on this screen. Factory Default. Use this screen to reset the Access Point to its factory default settings. Firmware Upgrade.

Upgrade the Access Point's firmware on this screen. Reboot. Use this screen to reboot the Access Point. Config Management. You can save the configuration file for the Access Point to your PC, as well as restore the backup configuration file to the Access Point. snmp: the standard network management protocol on the Internet. firmware: the software image that runs on a CPU inside a networking device. Status You will be able to view status information for your local network, wireless networks, and network performance. Local Network. This screen displays system information, including software & hardware version, MAC address, and IP address on the LAN side of the Access Point. Wireless. This screen displays wireless network settings including SSID, network mode, and wireless channel. System Performance. This screen displays the current traffic statistics of this Access Point for both Wireless and LAN ports. Chapter 5: Setting Up the Wireless-N Access Point Navigating the Utility 15 Wireless-N Access Point with Power Over Ethernet Chapter 6: Configuring the Wireless-N Access Point This chapter is a detailed reference guide for the Web-based Utility. You do not need the Utility to start using your Access Point. The Access Point has been designed to be functional right out of the box with the default settings. Besides, you can follow the instructions in "Setting Up the Wireless-N Access Point" on page 13 to perform the most basic settings without reading through this chapter. The Setup - Basic Setup Tab The first screen that appears is the Setup screen. This allows you to change the Access Point's general settings.

Basic Setup Enter names for the Access Point. The host name can be used to access the Web Utility through the network if DNS has been set up. The device name is for the benefit of identifying your Access Point after you log in. Host Name. This is the host name assigned to the Access Point. This host name will be published to your DNS server if the Access Point is configured to acquire the IP address through DHCP. In that case, Linksys recommends to follow the company policy on the host name assignment. The default name is Linksys. Device Name. You may assign any device name to the Access Point. This name is only used by the Access Point administrator for identification purposes. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. The default name is WAP4400N. Network Setup The selections under this heading allow you to configure the Access Point's IP address setting(s). IP Settings Select Static IP Address (default) if you want to assign a static or fixed IP address to the Access Point.

Then complete the following: IP Address. The IP address must be unique to your network. The default IP address is 192.168.1.245. Figure 6-1: Setup - Static IP Address Chapter 6: Configuring the Wireless-N Access Point The Setup - Basic Setup Tab 16 Wireless-N Access Point with Power Over Ethernet Subnet Mask. The Subnet Mask must be the same as that set on the LAN that your Access Point is connected to. The default is 255.255.255.0. Select Automatic Configuration - DHCP if you have a DHCP server enabled on the LAN that can assign an IP address to the Access Point. @@Help information is displayed on the right-hand side of the screen. The Setup - Time Tab This allows you to change the Access Point's time settings.

The correct time setting can help the administrator to search the system log to identify problems. Figure 6-2: Setup - Automatic Configuration - DHCP Time You can set the time either manually or automatically from a time server if the Access Point can access the public Internet. Manually. Select this radio button to set the date and time manually. The default is to set the time manually. Automatically. Select this option and time zone. The Access Point will contact the public time server to get the current time. User Defined NTP Server. Enable this option if you have set up local NTP server.

Default is Disabled. Figure 6-3: Setup - Time NTP Server IP. Enter the IP address of user defined NTP Server. @@Help information is displayed on the right-hand side of the screen. Chapter 6: Configuring the Wireless-N Access Point The Setup - Time Tab 17 Wireless-N Access Point with Power Over Ethernet The Wireless - Basic Wireless Settings Tab Change the basic wireless network settings on this screen.

Basic Settings Configure the Wireless Network basic attributes for this Access Point. SSID Name. The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.

The default SSID name is linksys-n. Wireless Network Mode. Select one of the following modes. The default is B/G/N-Mixed. B-Only: All the wireless client devices can be connected to the Access Point at Wireless-B data rates with maximum speed at 11Mbps. G-Only: Both Wireless-N and Wireless-G client devices can be connected at Wireless-G data rates with maximum speed at 54Mbps. Wireless-B clients cannot be connected in this mode. N-Only: Only Wireless-N client devices can be connected at Wireless-N data rates with maximum speed at 300Mbps. B/G-Mixed: Both Wireless-B and Wireless-G client devices can be connected at their respective data rates. Wireless-N devices can be connected at Wireless-G data rates.

G/N-Mixed: Both Wireless-G and Wireless-N client devices can be connected at their respective data rates. Wireless-B clients cannot be connected in this mode. B/G/N-Mixed: All the wireless client devices can be connected at their respective data rates in this mixed mode. Disabled: To disable wireless connectivity completely. This might be useful during system maintenance. Figure 6-4: Wireless - Basic Wireless Settings Wireless Channel. Select the appropriate channel to be used among your Access Point and your client devices. The default is channel 6. You can also select Auto so that your Access Point will select the channel with the lowest amount of wireless interference while the system is powering up.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/344788)

[WAP4400N user guide](http://yourpdfguides.com/dref/344788)

<http://yourpdfguides.com/dref/344788>

Auto channel selection will start when you click Save Settings button, it will take several seconds to scan through all the channels to find the best Figure 6-5: Pop-up message on Auto Channel Selection Chapter 6: Configuring the Wireless-N Access Point The Wireless - Basic Wireless Settings Tab 18 Wireless-N Access Point with Power Over Ethernet channel.

For the Wireless-N 40MHz channel option (see Wireless - Advanced Wireless Settings Tab), the Access Point will automatically select the adjacent 20MHz channel to combine them into a wider channel. SSID Broadcast. This option allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this enabled, someone could easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network.

Click Enabled to broadcast the SSID to all wireless devices in range. Click Disabled to increase network security and prevent the SSID from being seen on networked PCs. The default is Enabled in order to help users configure their network before use. @ @Help information is displayed on the right-hand side of the screen, and click More for additional details. Chapter 6: Configuring the Wireless-N Access Point The Wireless - Basic Wireless Settings Tab 19 Wireless-N Access Point with Power Over Ethernet The Wireless - Wireless Security Tab Change the Access Point's wireless security settings on this screen.

Wireless Security Security Mode. Select the wireless security mode you want to use, WPA-Personal, WPA2-Personal, WPA2Personal Mixed, WPA-Enterprise, WPA2-Enterprise, WPA2-Enterprise Mixed, or WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11e. WEP stands for Wired Equivalent Privacy, Enterprise refers to using RADIUS server for authentication, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings. For detailed instructions on configuring wireless security for the Access Point, refer to "Appendix B: Wireless Security." To disable wireless security completely, select Disabled. The default is Disabled. Wireless Isolation (within SSID).

When disabled, wireless PCs that are associated to the same network name (SSID), can see and transfer files between each other. By enabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. The default is Disabled. Figure 6-6: Wireless - Wireless Security (Disabled) Following section describes the detailed options for each Security Mode. Disabled There is no option to be configured for this mode. WPA-Personal (aka WPA-PSK) WPA Algorithms. WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is TKIP.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters. Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds.

Figure 6-7: Wireless - Wireless Security (WPA-Personal) Chapter 6: Configuring the Wireless-N Access Point The Wireless - Wireless Security Tab 20 Wireless-N Access Point with Power Over Ethernet WPA2-Personal WPA Algorithms. WPA2 always uses AES for data encryption. WPA Shared Key. Enter a WPA Shared Key of 8-63 characters. Key Renewal Timeout.

Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds. WPA2-Personal Mixed This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The Access Point will automatically choose the encryption algorithm used by each client device. WPA Algorithms. Mixed Mode automatically chooses TKIP or AES for data encryption. WPA Shared Key. Enter a WPA Shared Key of 8-63 characters. Key Renewal Timeout.

Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds. Figure 6-8: Wireless - Wireless Security (WPA2Personal) Figure 6-9: Wireless - Wireless Security (WPA2-Personal Mixed) Chapter 6: Configuring the Wireless-N Access Point The Wireless - Wireless Security Tab 21 Wireless-N Access Point with Power Over Ethernet WPA-Enterprise This option features WPA used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.) RADIUS Server IP Address. Enter the RADIUS server's IP address. RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812. WPA Algorithms.

WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, TKIP or AES. The default is TKIP. Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds. Figure 6-10: Wireless - Wireless Security (WPAEnterprise) WPA2-Enterprise This option features WPA2 used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.

) RADIUS Server IP Address. Enter the RADIUS server's IP address. RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812. WPA Algorithms. WPA2 always uses AES for data encryption. Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server. Key Renewal Timeout.

Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is 3600 seconds. Figure 6-11: Wireless - Wireless Security (WPA2Enterprise) Chapter 6: Configuring the Wireless-N Access Point The Wireless - Wireless Security Tab 22 Wireless-N Access Point with Power Over Ethernet WPA2-Enterprise Mixed This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The Access Point will automatically choose the encryption algorithm used by each client device. RADIUS Server IP Address. Enter the RADIUS server's IP address. RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithms. Mixed Mode automatically chooses TKIP or AES for data encryption. Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server. Key Renewal Timeout.

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



[You're reading an excerpt. Click here to read official LINKSYS](#)

[WAP4400N user guide](#)

<http://yourpdfguides.com/dref/344788>

The default is 3600 seconds. Figure 6-12: Wireless - Wireless Security (WPA2 Enterprise Mixed) WEP This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection.

Users are urged to migrate to WPA or WPA2. Authentication Type. Choose the 802.11 authentication type as either Open System or Shared Key. The default is Open System. Default Transmit Key. Select the key to be used for data encryption. WEP Encryption. Select a level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). Passphrase.

If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the Generate key. Those auto-generated keys are not as strong as manual WEP keys. Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption. Figure 6-13: Wireless Settings - WEP @@Help information is displayed on the right-hand side of the screen, and click More for additional details. Chapter 6: Configuring the Wireless-N Access Point The Wireless - Wireless Security Tab 23 Wireless-N Access Point with Power Over Ethernet The Wireless - Wireless Connection Control Tab This screen allows you to configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the Access Point. Wireless Connection Control Enabled/Disabled. Enable or disable wireless connection control. The default is disabled. Connection Control There are two ways to control the connection (association) of wireless client devices. You can either prevent specific devices from connecting to the Access Point, or you can allow only specific client devices to connect to the Access Point. The client devices are specified by their MAC addresses. The default is to allow only specific client devices.

Wireless Client List Instead of manually entering the MAC addresses of each client, the Access Point provides a convenient way to select a specific client device from the client association table. Click this button and a window appears to let you select a MAC address from the table. The selected MAC address will be entered into the Connection Control List. Figure 6-14: Wireless - Wireless Connection Control Connection Control List MAC 01-20. Enter the MAC addresses of the wireless client devices you want to control.

@@Help information is displayed on the right-hand side of the screen. Figure 6-15: Select MAC Address from Wireless Client List Chapter 6: Configuring the Wireless-N Access Point The Wireless - Wireless Connection Control Tab 24 Wireless-N Access Point with Power Over Ethernet The Wireless - Advanced Wireless Settings Tab This screen allows you to configure the advanced settings for the Access Point. The Wireless-N adopts several new parameters to adjust the channel bandwidth, and guard intervals to improve the data rate dynamically. Linksys recommends to let your Access Point automatically adjust the parameters for maximum data throughput. Advanced Wireless You can change the following advanced parameters (some only for Wireless-N) for this Access Point. Wireless-N data rates are classified into 16 MCS numbers (0-15). MCS stands for Modulation and Coding Scheme. For the same MCS number, the data rate changes according to the Channel Bandwidth and Guard Interval settings. You can see the change through the drop-down menu of Tx Rate Limiting (11n clients). Channel Bandwidth.

You can select the channel bandwidth manually for Wireless-N connections. When it is set to 20MHz, only the 20MHz channel is used. When it is set to 40MHz, Wireless-N connections will use 40MHz channel but Wireless-B and Wireless-G will still use 20MHz channel. The default is Auto. Guard Interval. You can select the guard interval manually for Wireless-N connections. The two options are Short (400ns) and Long (800ns). The default is Auto. Tx Rate Limiting (11b clients). This option provides rate limiting on Wireless-B connections.

Wireless-B clients can be limited to data rate specified by IEEE 802.11b. The default is Auto. Tx Rate Limiting (11g clients). This option provides rate limiting on Wireless-G connections.

Wireless-G clients can be limited to data rates specified by IEEE 802.11g and 802.11b. The default is Auto. Tx Rate Limiting (11n clients).

This option provides rate limiting on Wireless-N connections. Wireless-N clients can be limited to data rates specified by draft IEEE 802.11n, IEEE 802.11g, and 802.11b. The data rate associated with each MCS number (0-15) changes according to your selection on Channel Bandwidth and Guard Interval. The default is Auto. CTS Protection Mode. CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all wireless transmissions, but will severely decrease performance. Keep the default setting, Auto, so the Access Point can use this feature as needed, when the Wireless-N/G products are not able to transmit to the Access Point in an environment with heavy 802.

11b traffic. Select Disabled if you want to permanently disable this feature. WMM. Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment.

The default is Enabled. Select Chapter 6: Configuring the Wireless-N Access Point The Wireless - Advanced Wireless Settings Tab Figure 6-16: Wireless - Advanced Wireless 25 Wireless-N Access Point with Power Over Ethernet High Performance (N-Only) if you want to achieve highest throughput on 11n connections. Note that 11b and 11g clients performance will be affected by setting to this mode. IOT Mode. Interoperability Mode.

Enabling this mode will help this AP to communicate with Linksys retail client cards (e.g. WPC300N) at 11n rates. This mode is a temporary measure to cope with implementation differences on 802.11n draft specification.

This option will be removed eventually when IEEE802.11n is finalized. The default is disabled. Beacon Interval. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless networks service area, the Access Point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM). The default is 100 ms. DTIM Interval. This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM).

Lower settings result in more efficient networking, while preventing your PC from dropping into powersaving sleep mode.



[You're reading an excerpt. Click here to read official LINKSYS](#)

[WAP4400N user guide](#)

<http://yourpdfguides.com/dref/344788>



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

*To reboot the Access Point, click the Yes radio button. Click Save Settings to apply your change and the Access Point will reboot itself, or click Cancel Changes to cancel your change. Help information is displayed on the right-hand side of the screen. Figure 6-22: Administration - Reboot Chapter 6: Configuring the Wireless-N Access Point The Administration - Reboot Tab 33 Wireless-N Access Point with Power Over Ethernet The Administration - Config Management Tab On this screen you can create a backup configuration file or save a configuration file to the Access Point. Config Management Use this screen to upload or download configuration files for the Access Point. Save Configuration. To save a backup configuration file on a computer, click the Save Configuration to File button and follow the on-screen instructions. Restore Configuration. To upload a configuration file to the Access Point, enter the location of the configuration file in the field provided, or click the Browse button to find the file. Then click the Load button.*

*Help information is displayed on the right-hand side of the screen. Figure 6-23: Administration - Config Management Chapter 6: Configuring the Wireless-N Access Point The Administration - Config Management Tab 34 Wireless-N Access Point with Power Over Ethernet The Status - Local Network Tab The Local Network screen displays the Access Point's current status information for the local network. Information Hardware Version. This is the version of the Access Point's current hardware. Software Version.*

*This is the version of the Access Point's current software. Local MAC Address. The MAC address of the Access Point's Local Area Network (LAN) interface is displayed here. System Up Time. This is the length of time the Access Point has been running.*

*Figure 6-24: Status - Local Network Local Network IP Address. This shows the Access Point's IP Address, as it appears on your local network. Subnet Mask. This shows the Access Point's Subnet Mask. To update the status information, click the Refresh button. Help information is displayed on the right-hand side of the screen. Chapter 6: Configuring the Wireless-N Access Point The Status - Local Network Tab 35 Wireless-N Access Point with Power Over Ethernet The Status - Wireless Tab The Wireless screen displays the Access Point's current status information for the wireless network(s). Wireless Network MAC Address. The MAC Address of the Access Point's wireless interface is displayed here. SSID.*

*The Access Point's SSID is displayed here. Mode. The Access Point's wireless network mode is displayed here. Channel. The Access Point's Channel setting for the SSID is shown here. Figure 6-25: Status - Wireless To update the status information, click the Refresh button. Help information is displayed on the right-hand side of the screen. Chapter 6: Configuring the Wireless-N Access Point The Status - Wireless Tab 36 Wireless-N Access Point with Power Over Ethernet The Status - System Performance Tab The System Performance screen displays the Access Point's status information for its current settings and data transmissions. System Performance Wired Name. This indicates that the statistics are for the wired network, the LAN.*

*IP Address. The Access Point's local IP address is displayed here. MAC Address. This shows the MAC Address of the Access Point's wired interface. Connection.*

*This shows the status of the Access Point's connection for the wired network. Packets Received. This shows the number of packets received. Packets Sent. This shows the number of packets sent.*

*Bytes Received. This shows the number of bytes received. Bytes Sent. This shows the number of bytes sent. Error Packets Received. This shows the number of error packets received. Drop Received Packets. This shows the number of packets being dropped after they were received. Figure 6-26: Status - System Performance Wireless Name. This indicates the wireless network/SSID to which the statistics refer.*

*IP Address. The Access Point's local IP address is displayed here. MAC Address. This shows the MAC Address of the Access Point's wireless interface. Connection. This shows the status of the Access Point's wireless networks. Packets Received. This shows the number of packets received for each wireless network. Packets Sent. This shows the number of packets sent for each wireless network.*

*Chapter 6: Configuring the Wireless-N Access Point The Status - System Performance Tab 37 Wireless-N Access Point with Power Over Ethernet Bytes Received. This shows the number of bytes received for each wireless network. Bytes Sent. This shows the number of bytes sent for each wireless network. Error Packets Received.*

*This shows the number of error packets received for each wireless network. Drop Received Packets. This shows the number of packets being dropped after they were received. To update the status information, click the Refresh button. Help information is displayed on the right-hand side of the screen.*

*Chapter 6: Configuring the Wireless-N Access Point The Status - System Performance Tab 38 Wireless-N Access Point with Power Over Ethernet Appendix A: Troubleshooting This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-N Access Point with Power Over Ethernet. Read the descriptions below to help solve your problems. If you can't find an answer here, check the Linksys website at [www.linksys.com](http://www.linksys.com). Frequently Asked Questions Can the Access Point act as my DHCP Server? No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities. Can I run an application from a remote computer over the wireless network? This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network. Can I play multiplayer games with other users of the wireless network? Yes, as long as the game supports multiple players over a LAN (local area network).*

*Refer to the game's documentation for more information. What is the IEEE 802.11b standard? It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz. What is the IEEE 802.11g standard? It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.*



**[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/344788)**

**[WAP4400N user guide](http://yourpdfguides.com/dref/344788)**

**<http://yourpdfguides.com/dref/344788>**

4GHz. What is the IEEE 802.11n draft standard? It is one of the IEEE standards for wireless networks that is being finalized. The 802.

11n standard will allow wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11n standard. The 802.11n standard states a maximum data transfer rate of 600Mbps and an operating frequency of either 2.4GHz or 5 GHz. What IEEE 802.11b features are supported? The product supports the following IEEE 802.11 functions: Appendix A: Troubleshooting Frequently Asked Questions 39 Wireless-N

Access Point with Power Over Ethernet · CSMA/CA plus Acknowledge protocol · Multi-Channel Roaming · Automatic Rate Selection · RTS/CTS feature · Fragmentation · Power Management What IEEE 802.11g features are supported? The product supports the following IEEE 802.11g functions: · CSMA/CA plus Acknowledge protocol · OFDM protocol · Multi-Channel Roaming · Automatic Rate Selection · RTS/CTS feature · Fragmentation · Power Management

What is Ad-hoc? An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN.

An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation. What is Infrastructure? An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers. What is roaming? Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the workstation must make sure that it is set to the same channel number as the Access Point of the dedicated coverage area. To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and Access Point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links Access Points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system.

First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each Access Point and the distance of each Access Point to the wired backbone. Based on that information, the node next selects the right Access Point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone. Appendix A: Troubleshooting Frequently Asked Questions 40 Wireless-N Access Point with Power Over Ethernet As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original Access Point or whether it should seek a new one. When a node no longer receives acknowledgment from its original Access Point, it undertakes a new search.

Upon finding a new Access Point, it then re-registers, and the communication process continues. What is the ISM band? The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe. What is Spread Spectrum? Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). What is DSSS? What is FHSS? And what are their differences? Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. Would the information be intercepted while transmitting on air? WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers a variety of wireless security methods to enhance security and access control. Users can set it up depending upon their needs. Can Linksys wireless products support file and printer sharing? Linksys wireless products perform the same function as LAN products.

Therefore, Linksys wireless products can work with NetWare, Windows NT/2000, or other LAN operating systems to support printer or file sharing. Appendix A: Troubleshooting Frequently Asked Questions 41 Wireless-N Access Point with Power Over Ethernet What is WEP? WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard. What is a MAC Address? The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent.

Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network. How do I avoid interference? Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, make sure to operate each one on a different channel (frequency).



[You're reading an excerpt. Click here to read official LINKSYS WAP4400N user guide](http://yourpdfguides.com/dref/344788)  
<http://yourpdfguides.com/dref/344788>