Linksys by Cisco

Wireless-N Access Point with Power Over Ethernet

User Guide

Model: WAP4410N

BUSINESS SERIES

cisco

Table of Contents

Chapter 1: Getting Started 1
How to Use this Guide 1
Document Style Conventions 1
Finding Information in Your PDF Documents 2
Finding Text in a PDF 2
Finding Text in Multiple PDFs 2

Chapter 2: Introduction 3
Welcome 3

Chapter 3: Planning Your Wireless Network 4
Network Topology 4
Roaming 4
Network Layout 4
Example of a simple wireless network 5

Chapter 4: Getting to Know the Wireless-G Exterior Access Point 6
The LEDs 6
The Ports 7
Antennas and Positions 7

Chapter 5: Connecting the Wireless-N Access Point 9
Overview 9
Connection 9
Placement Options 9
Stand Option 10
Wall-Mount Option 11

Chapter 6: Setting Up the Wireless-N Access Point 12
Overview 12
Accessing the Utility 12
Navigating the Utility 13
Setup 13
Wireless 13
AP Mode 13
Administration 14
Status 14

Chapter 7: Configuring the Wireless-N Access Point 15
The Setup - Basic Setup Tab 15
Basic Setup 15
Network Setup 15
The Setup - Time Tab 17
Time 17
The Setup - Advanced Tab 18
HTTP Redirect Settings 18
The Wireless - Basic Wireless Settings Tab 19

Basic Settings 19
The Wireless - Wireless Security Tab 20
Wireless Security 20
The Wireless - Connection Control Tab 26
Connection Control 26
Local 26
Radius 27
The Wireless - Wi-Fi Protected Setup Tab 28
Wi-Fi Protected Setup 28
The Wireless - VLAN & QoS Tab 28
VLAN 29
QoS 29
The Wireless - Advanced Wireless Settings Tab 30
Advanced Wireless 30
Load Balancing 31
The AP Mode Tab 31
MAC Address 31
The Administration - Management Tab 32
Management 32
Web Access 33
SNMP 33
The Administration - Log Tab 34
Log 34
The Administration - Diagnostic Tab 35
Ping Test 35
The Administration - Factory Default Tab 35
Factory Default 35
The Administration - Firmware Upgrade Tab 35
Firmware Upgrade 35
The Administration - Reboot Tab 37
Reboot 37
The Administration - Config Management Tab 38
Config Management 38
The Status - Local Network Tab 39
Information 39
Local Network 39
The Status - Wireless Tab 40
Wireless Network 40
The Status - System Performance Tab 41
System Performance 41

Appendix A: Troubleshooting and Help 43
Frequently Asked Questions 43
Windows Help 48
TCP/IP 48
Shared Resources 48
Network Neighborhood/My Network Places 48

Appendix B: Wireless Security 49
Security Precautions 49
Security Threats Facing Wireless Networks 49

Appendix C: Upgrading Firmware 51

Appendix D: Glossary 52

Appendix E: Contact Information 56
US/Canada Contacts 56
EU Contacts 56

Appendix F: Warranty Information 57
LIMITED WARRANTY 57
Exclusions and Limitations 57
Obtaining Warranty Service 58
Technical Support 58

Appendix G: Regulatory Information 59
FCC Statement 59
FCC Caution 59
FCC Radiation Exposure Statement 59
Generic Discussion on RF Exposure 59
Explosive Environment, Medical and FAA Device Information 61
Safety Notices 61
Industry Canada (Canada) 61
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) 62

Appendix H: Software License Agreement 70
Software in Linksys Products: 70
Software Licenses: 70
Schedule 1 Linksys Software License Agreement 70
Schedule 2 72
Schedule 3 77

Appendix I: Specifications 80

Getting Started

How to Use this Guide

This User Guide has been designed to make understanding networking with the camera easier than ever. Look for the following items when reading this guide:

WARNING: This graphic means there is a Warning and is something that could damage your self, property, or the camera.

NOTE: This checkmark means there is a Note of interest and is something you should pay special attention to while using the camera.

CAUTION: This exclamation point means that caution should be used when performing a step or a serious error may occur.

Document Style Conventions

The following style conventions are used in this document.

- **Menus, Tabs, and Buttons:** Bold type is used to indicate the name of a button, menu, or tab in an application.

  Example: Click **Submit All Changes** to save your entries.

- **Screens, Page Areas, and Fields:** Italic type is used to indicate the name of screens, page areas, and fields.

  Example: Scroll down to the *PBX Parameters* area of the screen.

- **Data Input:** The `Courier` font is used to indicate characters that you should type into a field exactly as printed in this guide.

  Example: In the *Mailbox Subscribe Expires* field, type `30`.

  In this example, you would type the number 30 in the field.

- **Parameters:** Angle brackets and italic type indicate parameters that you must replace with the appropriate data.

  Example: Type `800@`*<IP address of device>*`:5090`

  In this example, you would type the characters 800@, followed by the IP address of your device, followed by a colon and the number 5090.

Finding Information in Your PDF Documents

The PDF Find/Search tool lets you find information quickly and easily online. You can:

- Search an individual PDF
- Search multiple PDFs at once (for example, all PDFs in a specific folder or disk drive)
- Perform advanced searches

Finding Text in a PDF

By default, the Find toolbar is open. If it has been closed, choose **Edit > Find**.

Use Find to search for text in an open PDF:

1. Enter your search terms in the *Find* box on the toolbar.
2. Optionally click the arrow next to the Find text box to refine your search (such as Whole words only).
3. Press **Enter**. Acrobat jumps to the first instance of the search term. Pressing **Enter** again continues to more instances of the term.

Finding Text in Multiple PDFs

The *Search* window lets you search for terms in multiple PDFs. The PDFs do not need to be open. Either:

- Choose **Edit** > **Search**

  or

- Click the arrow next to the *Find* box and choose Open Full Acrobat Search. The *Search* window appears.

In the *Search* window:

1. Enter the text you want to find.
2. Choose **All PDF Documents in**.
3. From the drop-down box, choose **Browse for Location**.
4. Choose the location you want to search, either on your computer or on a network, then click **OK**.
5. If you want to specify additional search criteria, click **Advanced Search Options**, and choose the options you want.
6. Click **Search.**

For more information about the Find and Search functions, see the Adobe Acrobat online help.

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 WPS (Wi-Fi Protected Setup) feature is also supported to help you simplify the setting up and configure security on a wireless network. The Wireless-N Access Point even 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 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.

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 adaptors 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.

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 settings.

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.

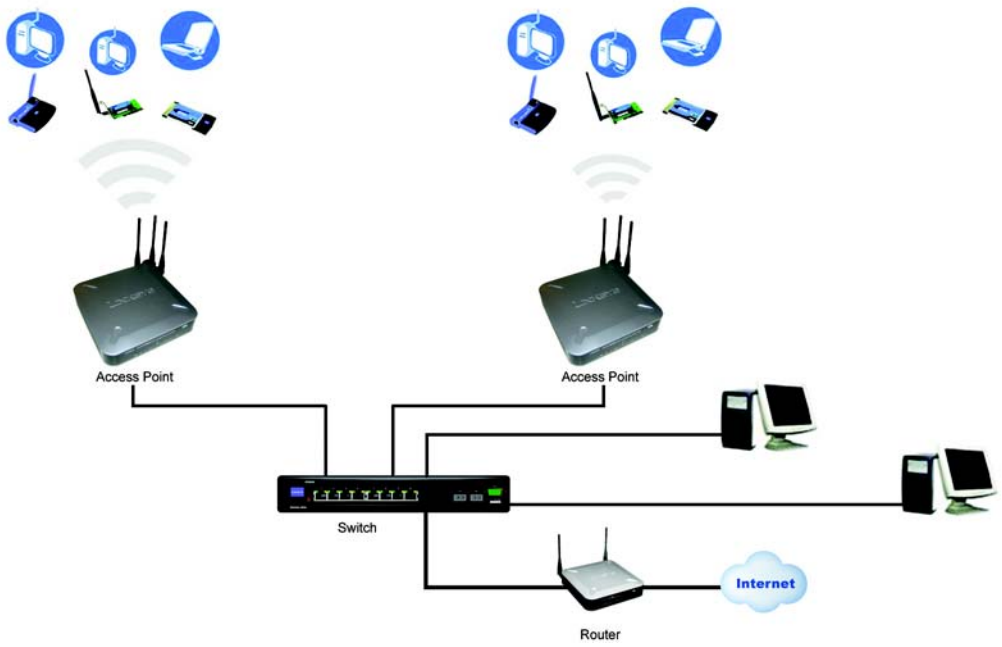
Network Layout

The Wireless-N Access Point has been designed for use with 802.11n, 802.11g and 802.11b products. The Access Point is compatible with 802.11n, 802.11g and 802.11b adapters, such as the notebook adapters for your laptop computers, PCI adapters for your desktop PCs, and USB adapters for all PCs when you want to enjoy wireless connectivity. These wireless products can also communicate with a 802.11n, 802.11g or 802.11b wireless print server (if available).

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router with Power over Ethernet (PoE)—or a PoE injector, such as the Linksys WAPPOE or WAPPOE12. Note that the 12 VDC on the WAPPOE12 is for the splitter output. Both PoE Injectors provide 48 VDC power output.

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.

Example of a simple wireless network



The above diagram shows a typical infrastructure wireless network setup. The wireless Access Points are connecting to a Linksys switch that provides power to the Access Points. Each Access Point can connect multiple wireless devices to the network. This network will provide connectivity among wireless network devices and PCs that have a wired connection to the switch.

The switch then can connect to a router that can connect to an ISP to reach global Internet.

Getting to Know the Wireless-G Exterior Access Point

This chapter provides you with information about the external characteristics of the Access Point.

The LEDs

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

Power—Green. Lights up when the Access Point is powered on.

PoE—Green. Lights up when the Access Point is powered through Ethernet cable.

WIRELESS—Green. Lights up when the Access Point is successfully connected to a wireless device. If the Wireless LED is flashing, the Access Point is actively sending to or receiving data from a wireless device.

ETHERNET—Green. Lights up when the Access Point is successfully connected to a device through the Ethernet network port. If the ETHERNET LED is flashing, the Access Point is actively sending to or receiving data from one of the devices over the Ethernet network port.

The Ports

The Access Point's ports are located on the back of the device.

Power—Connects to the supplied 12VDC power adapter.

Ethernet—Connects to Ethernet network devices, such as a switch or router that may or may not support Power over Ethernet (PoE).

Reset Button—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.

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 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.

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.

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."

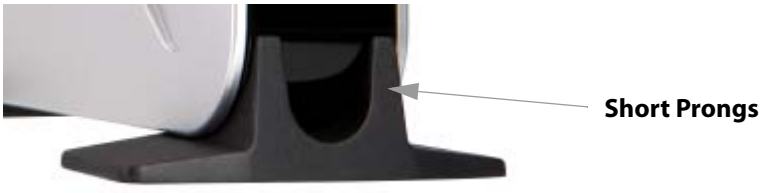
   If you are not using POE, then connect the included power adapter to the Access Point's Power port. Then plug the power adapter into an electrical outlet. The LEDs on the front panel will light up as soon as the Access Point powers on.

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.



3. Repeat this step with the other stand.

Wall-Mount Option

1. On the Access Point's back panel are two cris-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.

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 Web-based Utility. This chapter explains how to use the Utility to perform the most basic settings.

NOTE: Make sure you have Enabled TCP/IP on your PCs prior to proceeding. PCs communicate over the network with this protocol.

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.

Accessing the Utility

There are three ways to connect to your Access Point for the first time.

- 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).

- 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.

- 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.

1. 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.

2. 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.

3. 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

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.
- **Advanced**—Set the HTTP Redirect and 802.1x Supplicant settings for 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.
- **Wi-Fi Protected Setup**—Use this screen to simplify the process of setting up and configuring security on a wireless network.
- **VLAN & QoS**—Use this screen to configure the 802.1Q VLAN and the QoS (Quality of Service) settings.
- **Advanced Wireless Settings**—Use this screen to configure the Access Point's more advanced wireless settings (e.g. Load Balancing, Channel Bandwidth, etc.).

AP Mode

Use this screen to select the desired mode of Access Point. The default mode is Access Point.

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.
- **Diagnostic**—Use this to perform a *Ping*. The activities can be useful in solving network problems.
- **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.

Status

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

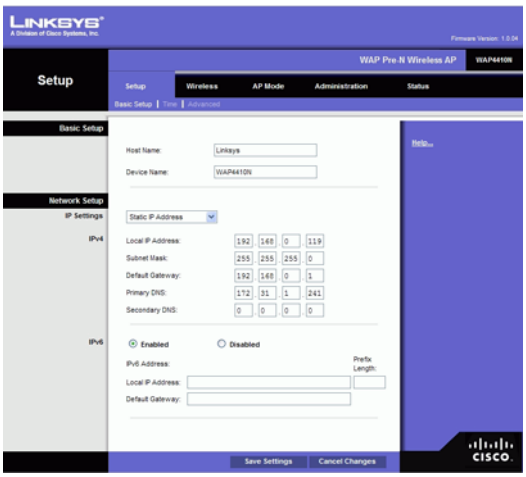
- **Local Network**—This screen displays system information, including software & hardware version, MAC address, and IP address on the LAN side of the Access Point.
- **Wireless**—This screen displays wireless network settings including SSID, network mode, priority setting, VLAN trunk, and wireless channel.
- **System Performance**—This screen displays the current traffic statistics of this Access Point for both Wireless and LAN ports.

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. This chapter provides detailed configuration instructions.

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 **WAP4410N**.

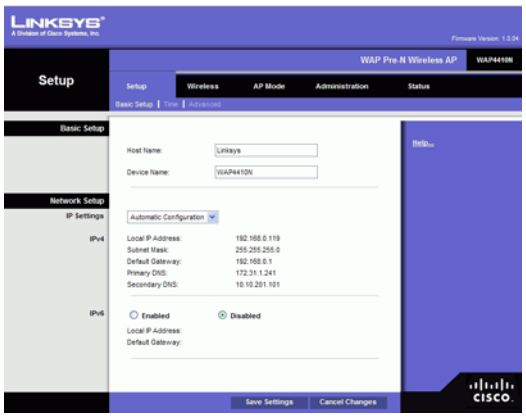
Network Setup

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

IP Settings (v4)

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**.
- **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** if you have a DHCP server enabled on the LAN that can assign an IP address to the Access Point.

IP Settings (v6)

Enabled/Disabled. Enabled or Disabled IPv6 settings. The default is Disabled.

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

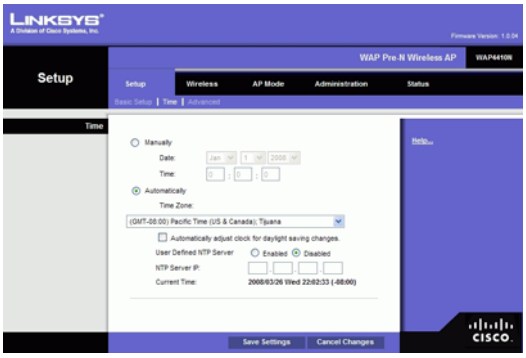
- **Local IP Address**—The IP address must be unique to your network.
- **Prefix Length**—Enter the Prefix length to match the IP address above.
- **Default Gateway**—Enter the IP Address of your Gateway or Router. Enter the value used by other devices on your LAN.

Select **Automatic Configuration** if you have an IPv6 RADVD device enabled on the LAN that can assign an IP address to the Access Point.

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

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.



Time

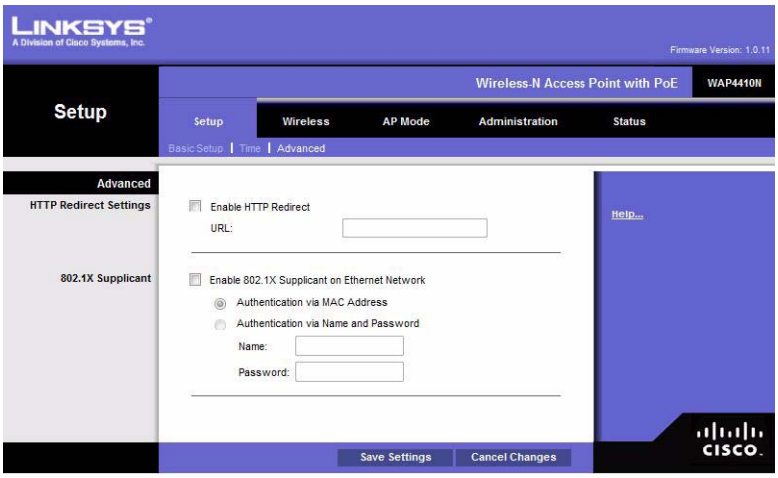
You can set the time either manually or automatically from a time server if the Access Point can access the public Internet.

- **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. If your location is currently using Daylight Saving, enable the **Automatically adjust clock for Daylight Saving changes** checkbox.
- **User Defined NTP Server**—Enable this option if you have set up local NTP server. Default is **Disabled**.
- **NTP Server IP**—Enter the IP address of user defined NTP Server.

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

The Setup - Advanced Tab

This allows you to configure the advanced Setup settings.



HTTP Redirect Settings

You can set the HTTP Redirect to make a web page available under many URLs.

- **Enable HTTP Redirect**—Enable this in order to make a redirect. Enter the desired URL in the following field
- 802.1x Supplicant
- **Enable 802.1x Supplicant on Ethernet Network**—Enable this if your network requires this AP to use 802.1x authentication in order to operate.
- **Authentication via MAC Address**—Select this if you want to Use MAC Address for Authentication.
- **Authentication via Name and Password**—Select this if you want to use name and password for Authentication. Enter the Name and Password in the following fields.

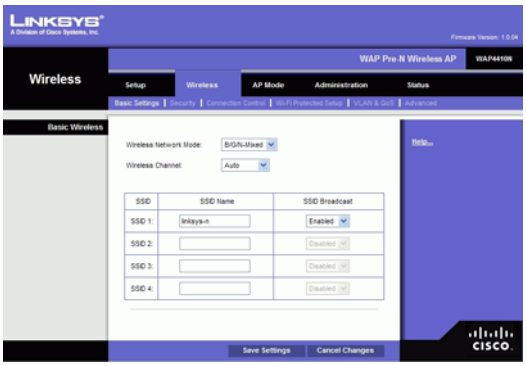
Change these settings as described and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen.

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.



- **Wireless Network Mode**—Select one of the following modes. The default is **B/G/N-Mixed**.
- **Disabled**—To disable wireless connectivity completely. This might be useful during system maintenance.
- **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.
- **B/G/N-Mixed**—All the wireless client devices can be connected at their respective data rates in this mixed mode.
- **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. 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 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 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

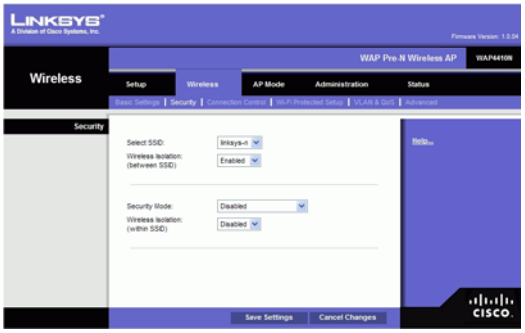
any keyboard character. Make sure this setting is the same for all devices in your wireless network. The default SSID name is **linksys-n**.

- **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.

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

The Wireless - Wireless Security Tab

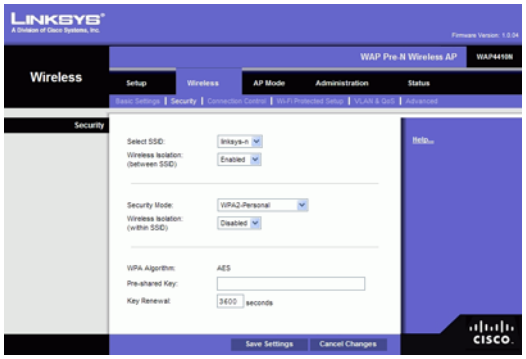
Change the Access Point's wireless security settings on this screen.



Wireless Security

- **Select SSID**—Select the desired SSID from the drop-down list.
- **Wireless Isolation (between SSID)**—When enabled, wireless clients using different SSIDs are isolated from each other.
- **Security Mode**—Select the wireless security mode you want to use, **WPA-Personal**, **WPA2-Personal**, **WPA2-Personal Mixed**, **WPA-Enterprise**, **WPA2-Enterprise, WPA2-Enterprise Mixed**, **Radius**, 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**.



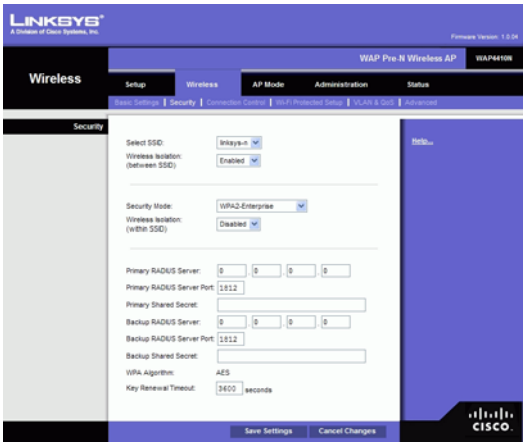
- **Wireless Isolation (within SSID)**—When disabled, wireless PCs that are associated to the same network name (SSID), can see and transfer files between each other. By enabling this feature, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. The default is Disabled.

The following section describes the detailed options for each Security Mode.

Disabled

There is no option to be configured for this mode.

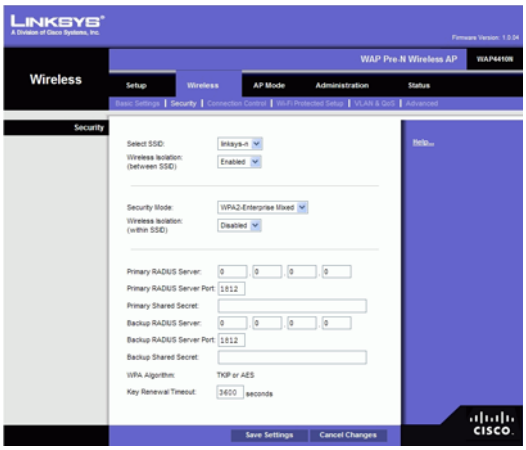
WPA-Personal (aka WPA-PSK)



- **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**.
- **Pre-Shared Key**—Enter a WPA Shared Key of 8-63 characters.
- **Key Renewal**— 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
- **WPA Algorithms**—WPA2 always uses AES for data encryption.

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

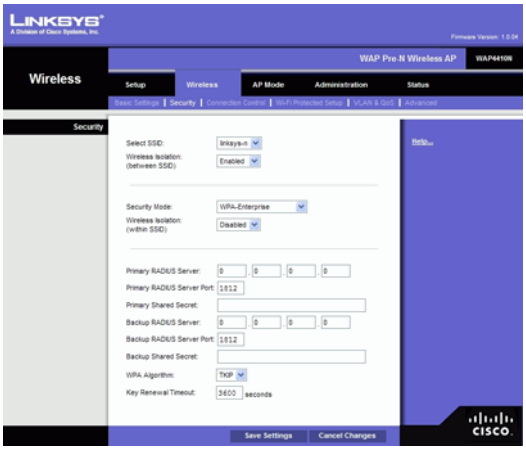
WPA2-Personal Mixed



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

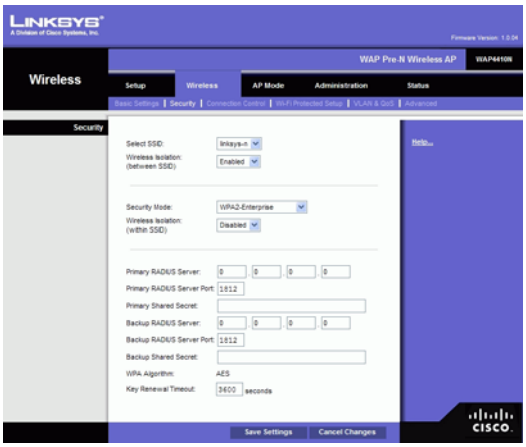
WPA-Enterprise



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.)

- **Primary/Backup RADIUS Server**—Enter the RADIUS server's IP address. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the Access Point and RADIUS server. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **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**.
- **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-Enterprise

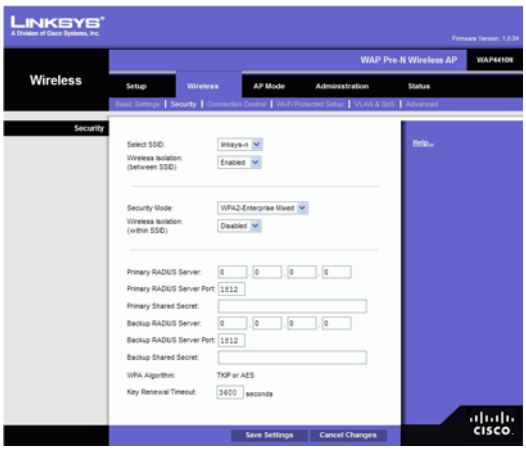


This option features WPA2 used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)

- **Primary/Backup RADIUS Server**—Enter the RADIUS server's IP address. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the Access Point and RADIUS server. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **WPA Algorithms**—WPA2 always uses AES for data encryption.

- **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.

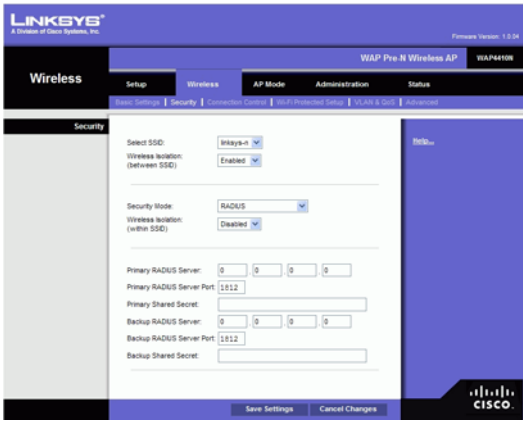
WPA2-Enterprise Mixed



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.

- **Primary/Backup RADIUS Server**—Enter the RADIUS server's IP address. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the Access Point and RADIUS server. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **WPA Algorithms**—Mixed Mode automatically chooses TKIP or AES for data encryption.
- **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.

Radius

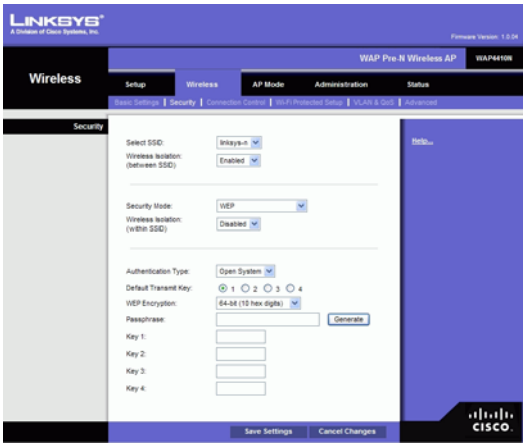


This option features a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)

- **Primary/Backup RADIUS Server**—Enter the RADIUS server's IP address. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup Shared Secret**.—Enter the Shared Secret key used by the Access Point and RADIUS server. The Backup Radius Server will be used only if the primary Radius Server is unavailable.

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.

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

The Wireless - Connection Control Tab

This screen allows you to configure the Wireless Connection Control to (associating with) the Access Point.

Connection Control

- **Select SSID**—Select the desired SSID from the list.
- **Local/Radius/Disabled**—Select the desired wireless connection control. The default is **disabled**.

Local

If you select **Local**, 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.

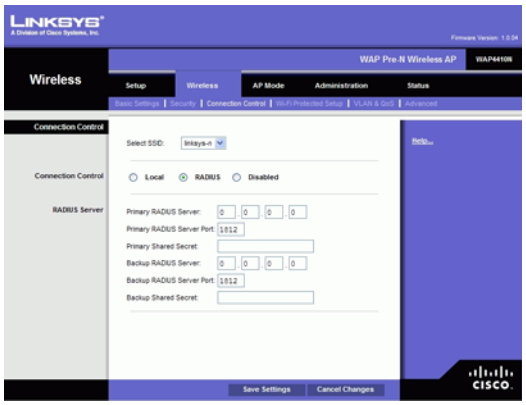
Wireless Client List

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.

Connection Control List

- **MAC 01-20**—Enter the MAC addresses of the wireless client devices you want to control.

Radius

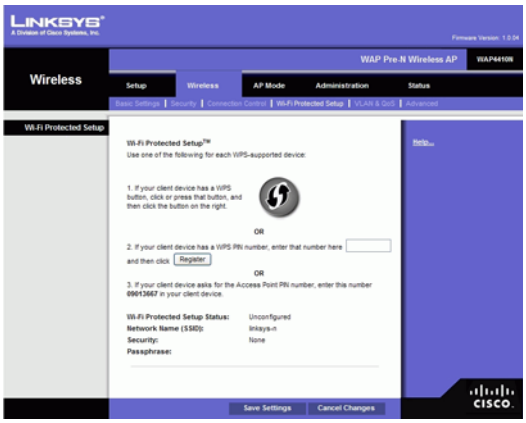


- **Primary/Backup RADIUS Server**—Enter the RADIUS server's IP address. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The Backup Radius Server will be used only if the primary Radius Server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the Access Point and RADIUS server. The Backup Radius Server will be used only if the primary Radius Server is unavailable.

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

The Wireless - Wi-Fi Protected Setup Tab

This screen allows you to configure the WPS settings for the Access Point. WPS (Wi-Fi Protected Setup) was designed to help standardize and simplify ways of setting up and configuring security on a wireless network by typing a PIN (numeric code) or pushing a button (Push-Button Configuration, or PBC).



Wi-Fi Protected Setup

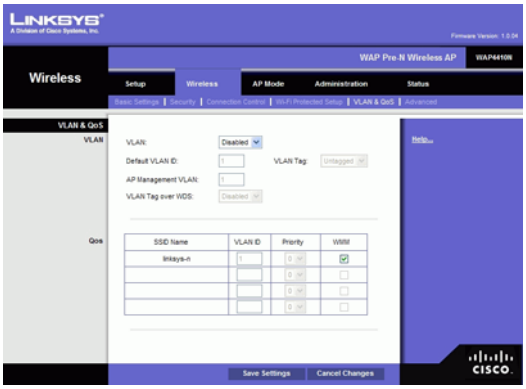
- **Option 1**—This method can be used only if the client device has the WPS push button. Press the WPS button of the client device and then click the button on the right.
- **Option 2**—The user has to give the PIN number which is founded in the utility of the client device. Enter the number and click **Register** button.
- **Option 3**—Enter the PIN number shown on the label at the bottom of the Access Point into the utility of client device.

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

The Wireless - VLAN & QoS Tab

This screen allows you to configure the Qos and VLAN settings for the Access Point. The QoS (Quality of Service) feature allows you specify priorities for different traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic. The

802.1Q VLAN feature is allowing traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your LAN.



VLAN

- **Enabled/Disabled VLAN**—You can enabled this feature only if the hubs/switches on your LAN support the VLAN standard.
- **Default VLAN ID**—Enter the default VLAN ID.
- **VLAN Tag**—Select **Tagged** to determine the associated VLAN from the VLAN tag. The default is **Untagged**.
- **AP Management VLAN**—Define the VLAN ID used for management.
- **VLAN Tag over WDS**—Select Disabled or Enabled as required.

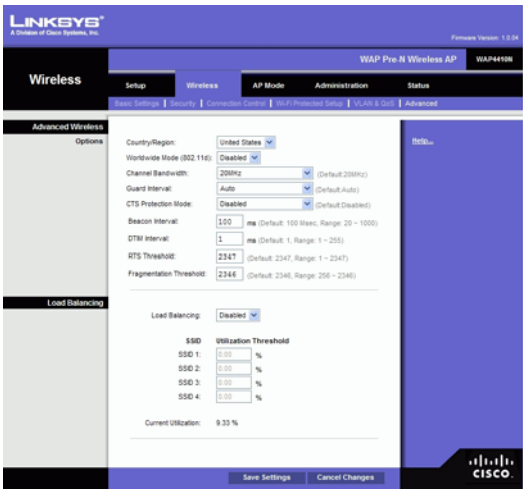
QoS

- **VLAN ID**—Enter the desired value for the VLAN.
- **Priority**—Select the desired priority from the list.
- **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 in Enabled.

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

The Wireless - Advanced Wireless Settings Tab

This screen allows you to configure the advanced and load balancing 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.

- **Country/Region**—Choose the country for your location from the drop-down list.
- **Worldwide Mode (802.11d)**—Enable this setting if you wish to use this mode, and your Wireless stations support this mode.
- **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 **20MHz**.
- **Guard Interval**—You can select the guard interval manually for Wireless-N connections. The three options are **Auto**, **Short (400ns)** and **Long (800ns)**. 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.
- **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 power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions. The default is **1** ms.

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

- **Fragmentation Threshold**—Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value.

Load Balancing

- **Load Balancing**—If Enabled, this feature can spread work between two or more devices to get optimal resource utilization, throughput, or response time.

- **Utilization Threshold**—Enter the desired utilization value for the SSID.

- **Current Utilization**—This displays the current value of the utilization.

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

The AP Mode Tab

On this screen you can configure the AP mode settings for the Wireless Access Point. There are five options for you to choose from.

MAC Address

Access Point

You can select this option to let the device operate as a normal Access Point.

- **Allow Wireless Signal to be repeated by a repeater**—If selected, the device will act as a repeater for another Access Point. Provide the MAC addresses of the other APs in the fields.

Wireless WDS Repeater

This option will let APs communicate with each other and with wireless stations.

- **Remote Access Point's MAC Address**—You can either enter the MAC address directly, or, if the other AP is on-line, you can click the *Site Survey* button and select from a list of available APs.

Wireless WDS Bridge

This option will let WDS APs communicate only with each other and don't allow wireless clients or Stations to access them

- **Remote Wireless Bridge's MAC Address**—Enter the MAC addresses of the other APs in the fields.

Wireless Client/Repeater

This option will let the Wireless Access Point to operate as a Client or Repeater Access Point, sending all traffic received to another Access Point.

- **Allow wireless stations to associate**—Enable or Disable the function.
- **Remote Access Point**—Enter the MAC address and SSID of the desired Access Point or click the Site Survey button to choose the Access Point from the available networks.

Wireless Monitor

When it is enabled, the Access Point can detect unauthorized (Rouge) Access Points on your LAN

- **No Security**—If checked, then any AP operating with security disabled is considered to be a Rogue AP.
- **Not in Legal AP List**—If checked, then any AP not listed in the Legal AP List is considered to be a Rogue AP. If checked, you must maintain the Legal AP List
- **Define Legal AP**—Click this button to open a sub-screen where you can modify the Legal AP List. This list must contain all known APs, so must be kept up to date.

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

The Administration - Management Tab

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

Management

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

Local AP Password

- **User Name**—Modify the administrator user name. The default is **admin**.
- **AP Password**—Modify the administrator password for the Access Point's Web-based Utility. The default is **admin**.
- **Re-enter to confirm**—To confirm the new password, enter it again in this field.

Web Access

To increase the security on accessing the Web-based Utility, you can enable HTTPS. Once enabled, users need to use *https://* when accessing the Web-based Utility.

- **Web HTTPS Access**—The default is **Disabled**.
- **Wireless Web Access**—Allow or deny wireless clients to access Web based Utility. The default is **Enabled**.

Remote Console

To exchange data over a secure channel between two computers, you can enable Secure Shell (SSH).

- **Secure Shell (SSH)**—The default is **Disabled**.

SNMP

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

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

Identification

- **Contact**—Enter the name of the contact person, such as a network administrator, for the Access Point.
- **Device Name**—Enter the name you wish to give to the Access Point.
- **Location**—Enter the location of the Access Point.
- **Get Community**—Enter the password that allows read-only access to the Access Point's SNMP information. The default is **public**.
- **Set Community**—Enter the password that allows read/write access to the Access Point's SNMP information. The default is **private**.
- **SNMP Trap-Community**—Enter the password required by the remote host computer that will receive trap messages or notices sent by the Access Point.
- **SNMP Trusted Host**—You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.
- **SNMP Trap-Destination**—Enter the IP address of the remote host computer that will receive the trap messages.

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

The Administration - Log Tab

On this screen you can configure the log settings and alerts of particular events.

Log

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

Email Alert

- **E-Mail Alert**—If you want the Access Point to send e-mail alerts in the event of certain attacks, select **Enabled**. The default is **Disabled**.\
- **SMTP Server**—Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use.
- **E-Mail Address for Logs**—Enter the e-mail address that will receive logs.
- **Log Queue Length**—You can designate the length of the log that will be e-mailed to you. The default is **20** entries.
- **Log Time Threshold**—You can designate how often the log will be emailed to you. The default is **600** seconds (10 minutes).

Syslog Notification

Syslog is a standard protocol used to capture information about network activity. The Access Point supports this protocol and sends its activity logs to an external server. To enable Syslog, select **Enabled**. The default is **Disabled**.

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

Log

Select the events that you want the Access Point to keep a log.

- **Unauthorized Login Attempt**—If you want to receive alert logs about any unauthorized login attempts, click the checkbox.
- **Authorized Login**—If you want to log authorized logins, click the checkbox.
- **System Error Messages**—If you want to log system error messages, click the checkbox.
- **Configuration Changes**—If you want to log any configuration changes, click the checkbox.
- **View Log**—If you want to see the logs, click the button.

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

The Administration - Diagnostic Tab

On this screen you can use the Wireless Access Point to perform a Ping. The activity can be useful in solving network problems.

Ping Test

- **IP or URL Address**—Enter the IP address you wish to ping. The IP address can be on your LAN, or on the Internet. Note that if the address is on the Internet, and no connection currently exists, you could get a Timeout error. In that case, wait a few seconds and try again.
- **Packet Size**—Enter the size of the packet.
- **Times to Ping**—Select the desired time from the list.
- **Start to Ping**—Click this button to start the ping procedure.

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

The Administration - Factory Default Tab

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

Factory Default

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

- **Restore Factory Defaults**—To restore the Access Point's factory default settings, click the **Yes** radio button. Then, click **Save Settings**. Your Access Point will reboot and come back up with the factory default settings in a few seconds.

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

The Administration - Firmware Upgrade Tab

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

Firmware Upgrade

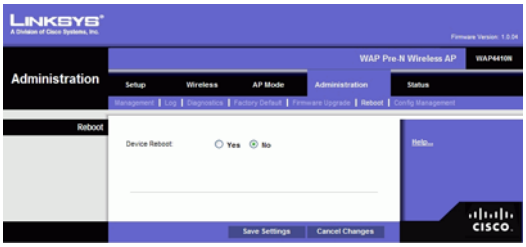
Before you upgrade the Access Point's firmware, note all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings. To upgrade the Access Point's firmware:

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

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

The Administration - Reboot Tab

On this screen you can reboot the Access Point.



Reboot

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

- **Device Reboot**—To reboot the Access Point, click the **Yes** radio button.

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.

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

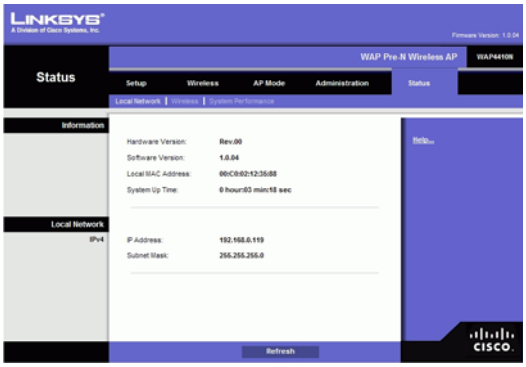
Use this screen to upload or download configuration files for the Access Point.

- **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.

The Status - Local Network Tab

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



Information

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

Local Network

- **IP Address**—This shows the Access Point's IP Address, as it appears on your local network.
- **Subnet Mask**—This shows the Access Point's Subnet Mask.

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

The Status - Wireless Tab

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

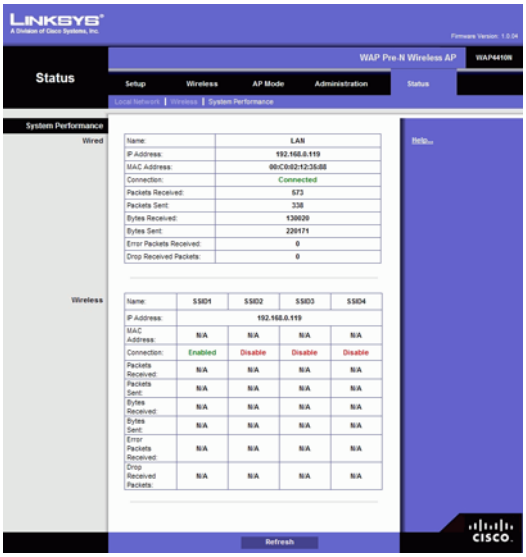
Wireless Network

- **Mode**—The Access Point's wireless network mode is displayed here.
- **Channel**—The Access Point's Channel setting for the SSID is shown here.
- **SSID 1~4 MAC Address**—The MAC Address of the Access Point's wireless interface is displayed here.
- **SSID 1~4**—The Access Point's SSID is displayed here.
- **VLAN Trunk**—The Access Point's VLAN Trunk status is displayed here.
- **Priority Setting**—The current priority setting is displayed here.
- **SSID 1~4 Security Mode**—The security mode of the SSID is displayed here.
- **SSID 1~4 Priority**—The priority status of the SSID is displayed here.

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

The Status - System Performance Tab

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



System Performance

Wired

- **Name**—This indicates that the statistics are for the wired network, the LAN.
- **IP Address**—The Access Point's local IP address is displayed here.
- **MAC Address**—This shows the MAC Address of the Access Point's wired interface.
- **Connection**—This shows the status of the Access Point's connection for the wired network.
- **Packets Received**—This shows the number of packets received.
- **Packets Sent**—This shows the number of packets sent.
- **Bytes Received**—This shows the number of bytes received.
- **Bytes Sent**—This shows the number of bytes sent.
- **Error Packets Received**—This shows the number of error packets received.
- **Drop Received Packets**—This shows the number of packets being dropped after they were received.

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.
- **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.

Troubleshooting and Help

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*.

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.

Can the Access Point work with a Centrio client?

Yes. However, a Centrio client only supports 20 MHz channels so the maximum throughput with this client will be 130 Mbps. A WPC300N is recommended instead.

What is the IEEE 802.11b standard?

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11g standard?

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

What 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:

- 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 IPv6 features are supported?

The device supports the following IPv6 functions:

- Path MTU discovery (RFC1981)
- Internet Protocol v6 -IPv6 (RFC2460)
- IPv6 Neighbor Discovery (ND) (RFC2461)
- IPv6 Stateless Address autoconfiguration (RFC2462)
- ICMPv6: Internet Control Message Protocol v6 ICMPv6 (RFC2643)
- IPv6 Address architecture (RFC3513)
- Default address selection (RFC3484)
- Transmission of IPv6 Packets over Ethernet Networks (RFC 2464)
- IPv6 Node - (RFC4294)

- Dual IPv4/IPv6 stack - simultaneous access from IPv4 and IPv6 client at the same time.

The device supports the following IPv6 Applications:

- WEB/SSL
- SNTP
- PING6
- TRACE Route

What is Ad-hoc?

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

What is Infrastructure?

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

What is roaming?

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

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

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

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in

particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

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

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

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

Would the information be intercepted while transmitting on air?

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

Can Linksys wireless products support file and printer sharing?

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

What is WEP?

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

What is a MAC Address?

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

How do I avoid interference?

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

How do I reset the Access Point?

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

How do I resolve issues with signal loss?

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

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

Does the Access Point function as a firewall?

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

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

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

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

No more than 63, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.

How do I configure multiple WAP4410N Access Points with the same configuration?

1. Configure one Access Point and then save the configuration file through its web page.
2. Using a text editor, change the command "`secret_shown=1`" to "`secret_shown=0`" in the configuration file, and then save the file.
3. Restore the file to the Access Point through its web page and save the configuration, naming it `AP_Config.cfg`.

   At this point, all keys and passwords are shown in clear text.
4. Restore the `AP_config.cfg` file on other Access Point's through their web pages one by one.

Windows Help

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

TCP/IP

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

Shared Resources

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

Network Neighborhood/My Network Places

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

Wireless Security

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

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

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

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

Security Threats Facing Wireless Networks

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

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

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

- Disable Broadcast
- Make it unique
- Change it often

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

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

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

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

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

There are several ways that WEP can be maximized:

- Use the highest level of encryption possible
- Use "Shared Key" authentication
- Change your WEP key regularly

WPA/WPA2 Personal. Wi-Fi Protected Access (WPA) This method offers two encryption methods, TKIP and AES, with dynamic encryption keys.

WPA /WPA2 Enterprise. This option requires that your LAN has a RADIUS server for authentication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level.

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

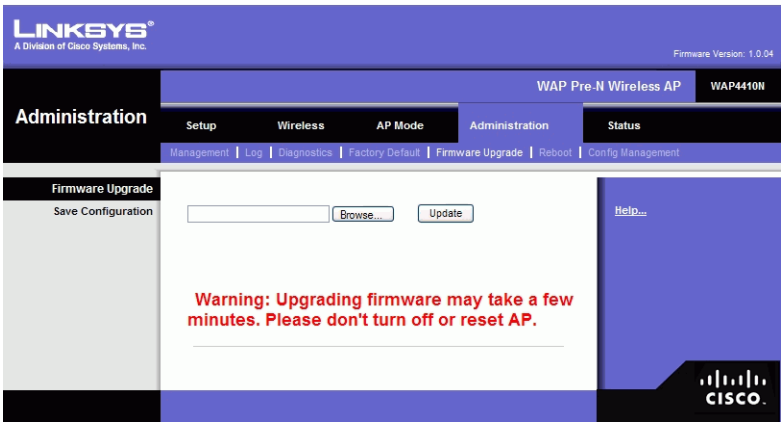
These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

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

Upgrading Firmware

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

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com*.



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

Glossary

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

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

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

AES (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

Byte - A unit of data that is eight bits long

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

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

DDNS (Dynamic Domain Name System) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

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

DHCP (Dynamic Host Configuration Protocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

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

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

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

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

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

Encryption - Encoding data transmitted in a network.

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

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

Firmware - The programming code that runs a networking device.

FTP (File Transfer Protocol) - A protocol used to transfer files over a TCP/IP network.

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

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

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

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

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

IP (Internet Protocol) - A protocol used to send data over a network.

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

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

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

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

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

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

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

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

Packet - A unit of data sent over a network.

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

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

POP3 (Post Office Protocol 3) - A standard mail server commonly used on the Internet.

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

PoE (Power over Ethernet) - A technology enabling an Ethernet network cable to deliver both data and power.

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

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

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

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

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

Router - A networking device that connects multiple networks together.

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

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

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

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

SSID (Service Set IDentifier) - Your wireless network's name.

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

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

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

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

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

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

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

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

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

TKIP (Temporal Key Integrity Protocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

Upload - To transmit a file over a network.

UPnP - Universal Plug and Play is a series of protocols to allow devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

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

WAN (Wide Area Network)- The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting network data transmitted on a wireless network for greater security.

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

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

Contact Information

Need to contact Linksys?

For additional information or troubleshooting help, refer to the User Guide on the CD-ROM. Additional support is also available by phone or online.

US/Canada Contacts

- 24-Hour Technical Support: 866-606-1866
- RMA (Return Merchandise Authorization): http://www.linksys.com/warranty
- Website: http://www.linksys.com
- FTP Site: ftp://ftp.linksys.com
- Support: http://www.linksys.com/support
- Sales Information: 800-546-5797 (800-LINKSYS)

EU Contacts

- Website: http://www.linksys.com/international
- Product Registration: http://www.linksys.com/registration

Warranty Information

LIMITED WARRANTY

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified for this product at www.linksys.com/warranty. The internet URL address and the web pages referred to herein may be updated by Linksys from time to time; the version in effect at the date of purchase shall apply.

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non.Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED AS IS WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

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

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

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact the Value Added Reseller (VAR) from whom you purchased the product or Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at: www.linksys.com/support. This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623

Regulatory Information

FCC Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Caution

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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

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

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.

Generic Discussion on RF Exposure

The Cisco products are designed to comply with the following national and international standards on Human Exposure to Radio Frequencies.

US 47 Code of Federal Regulations Part 2 Subpart J

American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1 (92)

International Commission on Non Ionizing Radiation Protection (ICNIRP) 98

Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz

Australia Radiation Protection Standard

To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco approved antennas and accessories.

US

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on evaluation per ANI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on evaluation per RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

EU

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

Australia

This system has been evaluated for RF exposure for Humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

ANSI C 95.1 (99)

This system has been evaluated for RF exposure for Humans in reference to the ANSI (American National Standards Institute) limits as referenced in C 95.1 (99). The minimum separation distance from the antenna to the user is 7.9 inches (20cm).

ICNIRP Limits

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to the user is 20cm (7.9 inches).

Explosive Environment, Medical and FAA Device Information

Use on Board Aircraft

The use of wireless on board aircraft is restricted by certain regulations and airline policy. Unless otherwise instructed by the airlines wireless devices should be turned off while on board aircraft.

Interference to Implanted Medical Devices

A minimum separation distance of 6 inches (15cm) is recommended between portable devices and implanted pacemakers to avoid possible interference. Please consult your physician or medical device maker for further details.

Medical Device use

Cisco products unless otherwise specified are not registered or listed as a FDA medical device. Therefore specific use in some unique medical applications may require additional approvals. Please contact your Cisco sales person for further details

Safety Notices

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

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

Industry Canada (Canada)

Operation is subject to the following two conditions:

1. This device may not cause interference and

2. This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 3.3 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

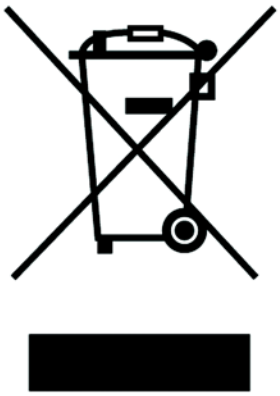
This device complies with Canadian ICES-003 and RSS210 rules.

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

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

WARNING: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

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



English

Environmental Information for Customers in the European Union

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

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

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

Dansk/Danish

Miljøinformation for kunder i EU

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

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

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

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

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

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

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

Français/French

Informations environnementales pour les clients de l'Union européenne

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

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

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

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

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

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

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

Italiano/Italian

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

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

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

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

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

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

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

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

Norsk/Norwegian

Miljøinformasjon for kunder i EU

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

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

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

Português/Portuguese

Informação ambiental para clientes da União Europeia

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

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

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

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

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

Español/Spanish

Información medioambiental para clientes de la Unión Europea

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

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

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

For more information, visit www.linksys.com.

Software License Agreement

Software in Linksys Products:

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pt. Ltd. or Cisco-Linksys K.K. ("Linksys") contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at www.linksys.com/gpl or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from www.linksys.com/gpl. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: www.linksys.com/gpl/ or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Software Licenses:

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: www.linksys.com and www.linksys.com/gpl/ respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

Schedule 1 Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("LINKSYS") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

"Software" includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/ or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

Software Upgrades etc. If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at http://www.linksys.com/gpl. If You would like a copy of the GPL or other open source code in this

Software on a CD, Linksys will mail to You a CD with such code for $9.99 plus the cost of shipping, upon request.

Term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

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

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

END OF SCHEDULE 1

Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at http://www.gnu.org/copyleft/gpl.html

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE

STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at http://www.openssl.org/source/license.html

---

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*
==========
===

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

END OF SCHEDULE 3

Specifications

WAP4410N Specifications

Model	WAP4410N
Standards	Draft IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power Over Ethernet), 802.1x (Security Authentication), 802.11i Security WPA/WPA2, WMM
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP Cat 5e or higher
LEDs	Power, Ethernet, Wireless, POE
Operating System	Linux
Web UI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
SNMP Version	Version 1, 2c, 3
Event Logging	Email logging, Remote Syslog
Web F/W Upgrade	Firmware Upgradeable Through Web-Browser
Diagnostics, Flash, etc	Flash, RAM, LAN, WLAN
DHCP	DHCP Client
HTTP Redirect	Redirects initial user access to an external Web Server to display company logo or network usage policy
IPv6 Host	Support for management and control of Access Point over IPv6. Supports RFC2460 (IPv6 protocol) and RFC4294 (IPv6 Node Requirements)
Multiple BSSID	Supports up to 4 BSSIDs allowing creating of multiple virtual Access Points
VLANs	Supports 802.1q - up to 4 VLANs
SSID to VLAN mapping	Supports mapping of SSIDs to VLANs to securely separate workgroups across wireless and wired domains
802.1x Supplicant	Supports 802.1x Supplicant on the Ethernet port to allow the AP to authenticate itself to the network
Spanning Tree	Supports 802.1d Spanning Tree protocol to prevent loops when using WDS links as redundant links in a distribution system

WAP4410N Specifications

Operating Modes	Access Point Mode, point-to-point Bridge Mode, point-to-multipoint Bridge Mode, Repeater Mode, Wireless Client Mode
Load Balancing	This capability allows the bandwidth control with user defined CPU usage ratio
Auto-channel selection	On boot up, the AP selects the least congested channel
802.11d	With 802.11d Regulatory Domain support, the AP provides radio channel settings for client devices facilitating easy client access as they move across regulatory domains
WEP/WPA/WPA2	WEP 64bit/128bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT
Access Control	Wireless Connection Control: MAC-Based
SSID Broadcast	SSID Broadcast Enable/Disable
Client Isolation	Supports wireless client isolation between SSIDs
802.1x	Wireless clients can be authenticated through IEEE 802.1x
802.1x Supplicant	Supports 802.1x Supplicant on the Ethernet port to allow the AP to authenticate itself to the network
Radius Server	Up to 2 Radius Servers can be configured for redundancy purposes
WPS	Supports WPS (WiFi Protected Setup) which is a WIFI Alliance specification for simple and secure setup of a wireless network
Rogue AP Detection	New Access Points detected, which have not been categorized as known, are logged as a Rogue AP. This allows the administrator to control unapproved devices in the network.
QoS	4 queues, 802.1p VLAN priority, WMM Wireless priority, Mapping of 802.1p priority to WMM priority to maintain end-to-end QoS
Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 11g/OFDM, 11n/OFDM
Channels	Operating Channels: 11 North America, 13 Most of Europe (ETSI and Japan)
Internal Antenna	None
External Antennas	3 (Omni-Directional)

WAP4410N Specifications

Transmit Power	Transmit Power at Normal Temp Range for FCC: 11b - 16 dBm@1TX, 19 dBm@2TX, 20.5dbm@3TX; 11g - 13 dBm@1TX, 16 dBm@2TX, 17.5dbm@3TX; 11n - 17 dBm@1TX@MCS0~5/8~13, 13 dBm@1TX@MCS6/14, 11 dBm@1TX@MCS7/15, 20 dBm@2TX@MCS0~5/8~13, 16 dBm@2TX@MCS6/14, 14 dBm@2TX@MCS7/15, 21.5 dBm@3TX@MCS0~5/8~13, 17.5 dBm@3TX@MCS6/14, 15.5 dBm@3TX@MCS7/15 Transmit Power at Normal Temp Range for ETSI: 11b/g/n - 13 dBm@1TX, 16 dBm@2TX, 17.5dbm@3TX;
Antenna Gain in dBi	2
Receiver Sensitivity	11.n: 300Mbps@ -69dBm, 11.g: 54Mbps@ -73dBm, 11.b: 11Mbps@ -88dBm
Device Dimensions	6.69X6.69X1.60 inches (170X170X40.7mm) 0.86 lbs. (0.39 kg)
Power	12V 1A DC input, and IEEE802.3af Compliant PoE. Maximum power draw is 10.1 Watts.
Certification	CC, CE, IC
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4 to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing