LINKSYS®
A Division of Cisco Systems, Inc.

LINKSYS ONE READY COMMUNICATIONS SOLUTION

Release 2.0

Linksys Business Series Wireless-G Access Point With Power Over Ethernet User Guide

Model WAP2000

cisco

Specifications are subject to change without notice.

Contents

Chapter 1

Introduction

Welcome

Thank you for choosing the Wireless-G Access Point with Power Over Ethernet and Rangebooster. This Access Point will allow you to network wirelessly better than ever.

How does the Access Point do all of this? An access point allows for greater range and mobility within your wireless network while also allowing you to connect the wireless network to a wired environment. In fact, the Wireless-G Access Point with Power Over Ethernet and Rangebooster can support communications on up to four wireless networks, using Virtual Local Area Network (VLAN) technology.

The Wireless-G Access Point with Power Over Ethernet and Rangebooster also offers the convenience of Power over Ethernet (PoE) capability, so it can receive data and power over a single Ethernet network cable. You can even connect wired networks in two different buildings, by using two Access Points set to Wireless Bridge mode.

But what does all of this mean?

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

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called “wired”.

PCs equipped with wireless 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 both 802.11g and 802.11b standards and wired networks.

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

access point: a device that allows wireless-equipped computers and other devices to communicate with each other and with devices on a wired network. Also used to expand the range of a wireless network.

network: a series of computers or devices connected together.

lan (local area network): the computers and networking devices that make up your local network.

poe (power over ethernet): a technology enabling an Ethernet network cable to deliver both data and power.

ethernet: network protocol defined in IEEE 802.3 standard that specifies how data is placed on and retrieved from a common transmission medium.

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

802.11g: a wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

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

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Access Point.

- Chapter 1: Introduction
  This chapter describes the Wireless-G Access Point's applications and this User Guide.
- Chapter 2: Planning your Wireless Network
  This chapter describes the basics of wireless networking.
- Chapter 3: Getting to Know the Wireless-G Access Point
  This chapter describes the physical features of the Access Point.
- Chapter 4: Connecting the Wireless-G Access Point
  This chapter instructs you on how to connect your Access Point to your network and placement options.
- Chapter 5: Setting up the Wireless-G Access Point
  This chapter explains how to perform the most basic setting changes through the Web-based Utility.
- Chapter 6: Configuring the Wireless-G Access Point
  This chapter provides a reference for the available configuration through the Web-based Utility.
- Appendix A: Troubleshooting
  This appendix describes some frequently asked questions regarding installation and use of the Wireless-G Access Point with Power Over Ethernet and Rangebooster.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the Access Point's firmware.
- Appendix D: Windows Help.
  This appendix describes some of the ways Windows can help you with wireless networking.
- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.

Chapter 1

- Appendix F: Regulatory Information
  This appendix supplies the Access Point's regulatory information.
- AppendixG: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter

Chapter 2

Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one or more wireless adapters. Computers in a wireless network must be configured to share the same radio channel to talk to each other. Several PCs equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point.

***ad-hoc**: a group of wireless devices communicating directly with each other (peer-to-peer) 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.

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

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.

***hardware:** the physical aspect of computers, telecommunications, and other information technology devices.*

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), wireless channel, and wireless security settings.

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

This Access Point has 802.11F Inter-Access Point Protocol (IAPP) to complete the roaming process in seconds. If your wireless networks share the same IP subnet, this will not disrupt your data connection while moving around.

***ssid**: your wireless network's name*

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-G Access Point with Power Over Ethernet and Rangebooster has been designed for use with 802.11g and 802.11b products. The Access Point is compatible with 802.11g and 802.11b adapters, such as the notebook adapters for your laptop computers, PCI adapters for your desktop PCs, and USB adapters for all PCs when you want to enjoy wireless connectivity. These wireless products can also communicate with an 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.

Chapter 3

Connecting the Wireless-G 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. Refer to “Chapter 5: Setting Up the Wireless-G Access Point”.

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

Proceed to the following section, “Placement Options.”

Connect the Ethernet Cable

Placement Options

There are two ways to place the Wireless-G 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 mount it on a wall. The wall-mount options are explained in further detail below.

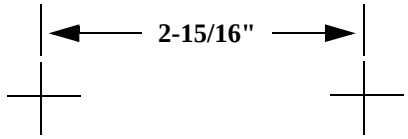
Now that the hardware installation is complete, proceed to “Chapter 5: Setting up the Wireless-G Access Point,” for directions on how to set up the Access Point.

Connect the Power

Wall-Mount Option

1. On the Access Point’s back panel are two crisscross 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.
5. Now that the hardware installation is complete, proceed to “Chapter 5: Setting up the Wireless-G Access Point,” for directions on how to set up the Access Point.



Mounting Dimensions

Chapter 4

Getting to Know the Wireless-G Access Point

The LEDs

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

Power	Green. The Power LED lights up when the Access Point is powered on.
PoE	Green. The PoE LED lights up when the Access Point is powered through Ethernet cable.
WLAN	Green. The WIRELESS LED lights up when the wireless module is active on the Access Point. If the Wireless LED is flashing, the Access Point is actively sending to or receiving data from a wireless device.
ETHERNET	Green. The ETHERNET LED 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 port are located on the back of the device.

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

IMPORTANT: Resetting the Access Point will erase all of your settings (including wireless security, IP address, and SSID) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Reset Button	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. **Note**: If you press the reset button for less than 10 seconds, the device will simply reboot without reseting to the factory default.
Ethernet	The Ethernet network port connects to Ethernet network devices, such as a switch or router that may or may not support Power over Ethernet (PoE).
Power	The Power port connects to the supplied power adapter.

Antennas and Positions

The Access Point's antennas are located on the back of the device. The Access Point can be placed on a desktop or wall-mounted. When placed on a desktop, the Access Point can be stacked with other Linksys Business Series products.

Antenna

The Access Point has two detachable 2dBi omni-directional antennas. Adjust the two antennas so that they form a 90 degree angle for best MIMO range performance.

Chapter 5

Setting Up the Wireless-G 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.

*t**cp/ip:** a set of protocols PCs use to communicate over a network.*

IMPORTANT: Have you enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP

***browser:** an application that provides a way to look at and interact with all the information on the World Wide Web.*

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.

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

1. If you have a 48VDC Power Injector (e.g. Linksys WAPPOE), power up your Access Point first, then connect the Injector's cable to your PC. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address (192.168.1.245).

2. If you have a PoE switch (e.g. Linksys SRW224P), connect your Access Point and your PC to the same network. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address (192.168.1.245). Or if there is a DHCP server connected to the switch, configure it to assign the IP address in 192.168.1.0/24 subnet. Your PC will get an IP address in the subnet through the DHCP.

3. Although it is not recommended, you can connect your PC wirelessly to the Access Point when the DHCP server is connected on the LAN side. It is not recommended, because you can easily lose your connection through configuration changes.

Login Screen

Launch your web browser, such as Internet Explorer or Mozilla Firefox and enter the Access Point's default IP address, **192.168.1.245**, in the *Address* field. Press the **Enter** key.

Enter **admin** in the *User Name* field. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

After setting up the Access Point to use DHCP or manually configure a new IP address, move your Access Point to the desired network. You will have to use the new IP address the next time you access the Web-based Utility.

Navigating the Utility

The Web-based Utility consists of the following five main tabs: Setup, Wireless, Security Monitor, Administration, and Status. Additional screens (sub tabs) will be available from most of the main tabs.

The following briefly describes the main & sub tabs of the Utility.

Setup

Enter the Host Name, IP Address settings, and set the time on this screen.

- *Basic Setup.* Configure the host name and IP address settings for this Access Point.

- Time -Set the time on this Access Point.

Wireless

You will use the Wireless tabs to enter a variety of wireless settings for the Access Point.

- *Basic Wireless Settings*. Choose the wireless network mode (e.g. 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.
- *Advanced Wireless Settings*. Use this screen to configure the Access Point's more advanced wireless settings.
- *VLAN & QoS*. Use this screen to configure VLAN and QoS settings.

AP Mode

Use this screen to configure the Access Point mode. The three available modes are Access Point, Wireless Repeater, and Wireless Bridge.

Administration

You will use the Administration tabs to manage the Access Point.

- *Management*. This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings.
- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Default*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.
- *Reboot*. Use this screen to reboot the Access Point.
- *Config Management*. You can save the configuration file for the Access Point to your PC, as well as restore the backup configuration file to the Access Point.

snmp: *the standard network management protocol on the Internet.*

firmware: *the software image that runs on a CPU inside a networking device.*

Status

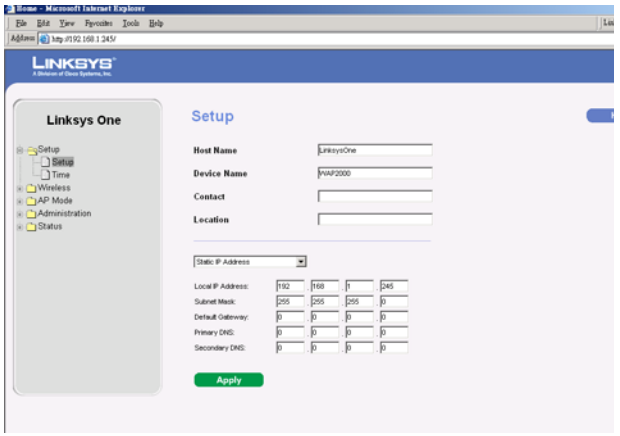
You will be able to view status information for your local network, wireless networks, and network performance.

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

Chapter 6

Configuring the Wireless-G 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. You also have the option to follow the instructions in “Setting Up the Wireless-G Access Point” on page 12 to perform the most basic settings without reading through this chapter.



The Setup - Basic Setup Tab

The first screen that appears is the *Setup* screen. This allows you to change the Access Point's general settings.

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 **WAP2000**.

Contact. This field is used for entering the contact information. You may enter the name for the Access Point’s owner or the person who administers this device.

Location. This field is used for entering the device’s location. You may enter the location, i.e. room or floor number of the building where the device locates.

Network Setup

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

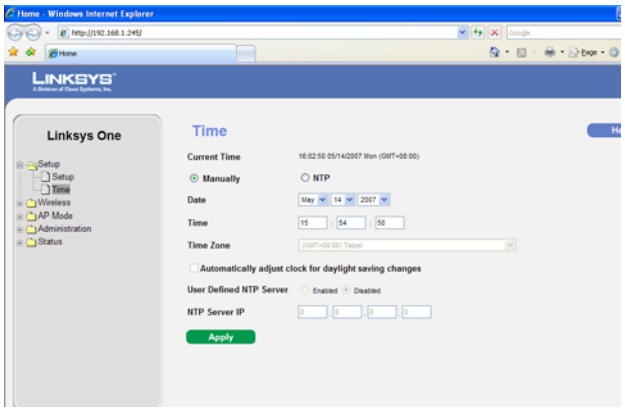
IP Settings

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

- **Local 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**.
- **Default Gateway**. Your ISP will provide you with the Default Gateway Address, which is the ISP server's IP address.
- **Primary DNS (Required)** and **Secondary DNS (Optional)**. Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

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

Change these settings as described here and click **Apply** to apply your changes, or cancel your changes by **not** applying your changes. Help information is available on the upper-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 option to set the date and time manually. The default is to set the time manually.

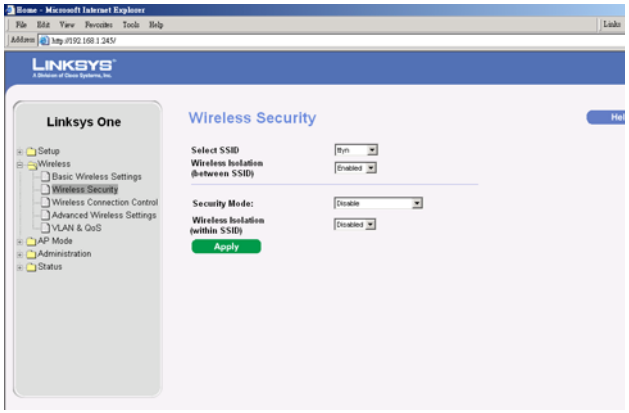
NTP. Select this option and time zone. The Access Point will contact the public time server to get the current time.

Automatically adjust clock for daylight saving changes. Select this option if you are in using the Access Point in a location that observes daylight saving time.

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 **Apply** to apply your changes, or cancel your changes by **not** applying your changes. Help information is available on the upper-right-hand side of the screen.



The Wireless - Basic Wireless Settings Tab

Change the basic wireless network settings on this screen. The Access Point can connect to up to four wireless networks (SSIDs) at the same time, so this screen offers settings for up to four different SSIDs. Each SSID owns its own MAC address on this Access Point.

Basic Settings

Configure the Wireless Network basic attributes for the entire system and for each SSID.

Wireless Network Mode. Select one of the following modes. The default is **Mixed**.

Disable: To disable wireless connectivity completely. This might be useful during system maintenance.

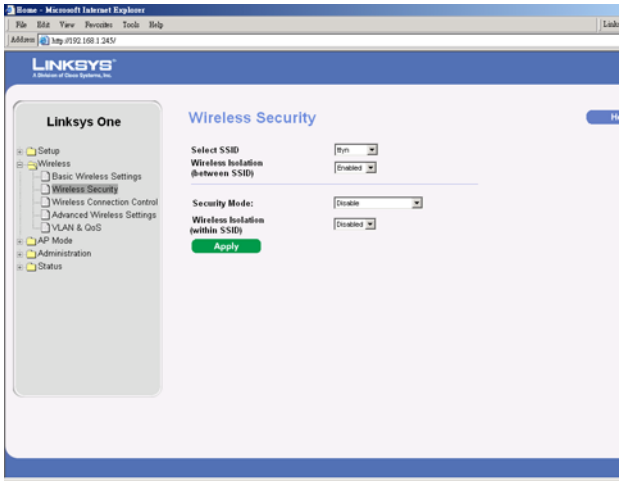
B-Only: All the wireless client devices can be connected to the Access Point at Wireless-B data rates with maximum speed at 11Mbps.

G-Only: 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.

Mixed: Both Wireless-B and Wireless-G client devices can be connected at their respective data rates. Wireless-G devices can be connected at Wireless-G data rates.

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.

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-g.



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 **Apply** to apply your changes, or cancel your changes by not applying them. Help information is available on the right side of the screen.

The Wireless - Wireless Security Tab

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

Wireless Security

Select SSID. Select any of the SSID names configured on the Basic Wireless Settings tab.

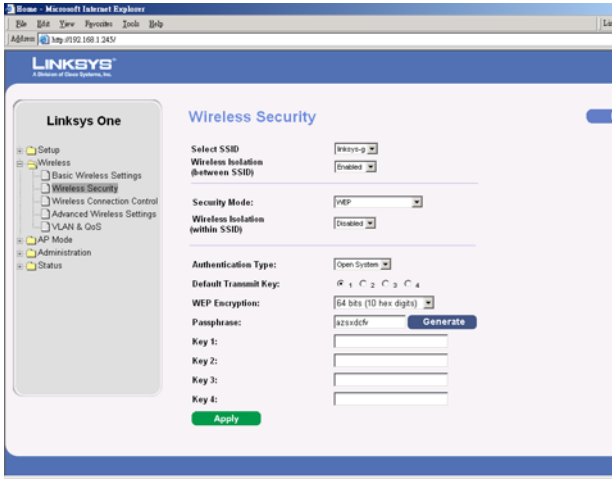
Wireless Isolation (between SSID). Wireless Isolation prevents eavesdropping in the network. When it is Enabled, wireless frames received on this Access Point will not be forwarded to other wireless networks (SSIDs). For example, if you have a wireless hotspot, you may want to keep the wireless network (SSID) isolated from your other wireless networks (SSIDs). This is a global option applying to all SSIDs. The default is Enabled.

The following options are specific for each SSID:

Security Mode. Select the wireless security mode you want to use, **WEP**, **WPA-Personal**, **WPA2-Personal**, **WPA2-Personal Mixed**, **WPA-Enterprise**, **WPA2-Enterprise, WPA2-Mixed**, or **RADIUS**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11i. WEP stands for Wired Equivalent Privacy, Enterprise modes use a 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.



Following section describes the detailed options for each Security Mode.

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.

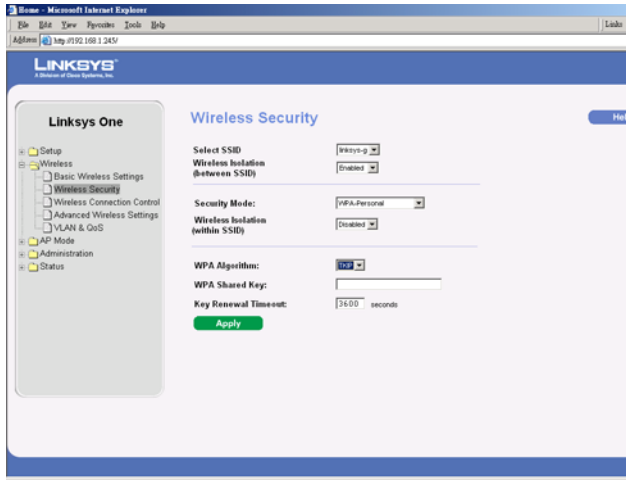
Default Transmit Key. Select the key to be used for data encryption.

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 available on the right side of the screen.



WPA-Personal (aka WPA-PSK)

WPA Algorithm. WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **TKIP** or **AES**. The default is **TKIP**.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

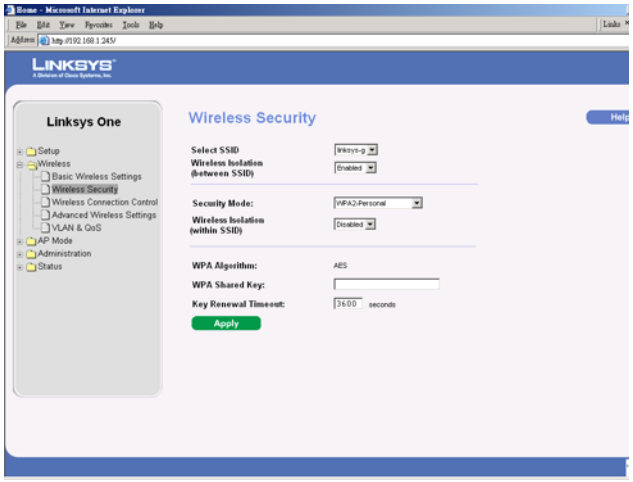
Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Personal

WPA Algorithm. WPA2 always uses AvES for data encryption.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.



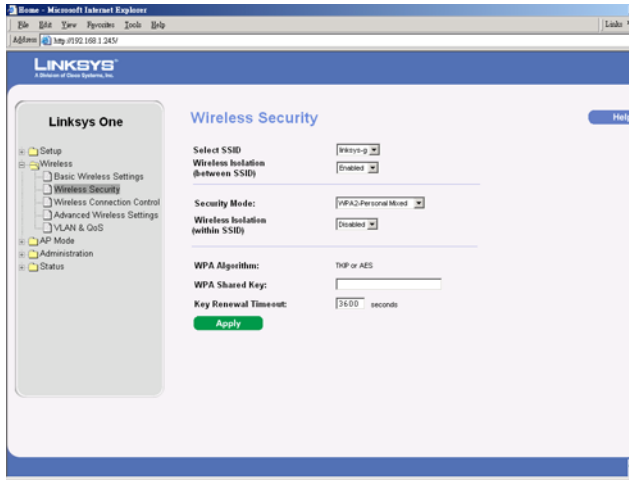
WPA2-Personal Mixed

This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The Access Point will automatically choose the encryption algorithm used by each client device.

WPA Algorithm. Mixed Mode automatically chooses TKIP or AES for data encryption.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.



WPA-Enterprise

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

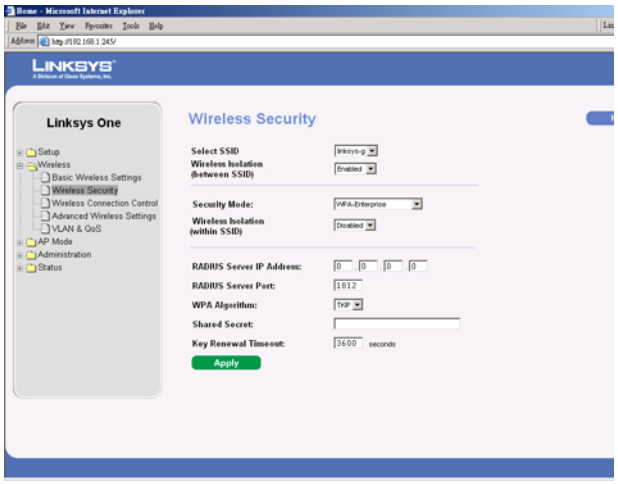
RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithm. WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **TKIP** or **AES**. The default is **TKIP**.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.



WPA2-Enterprise

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

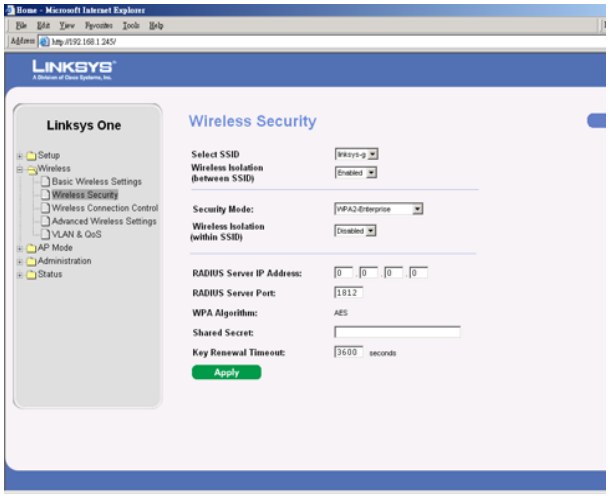
RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithm. WPA2 always uses AES for data encryption.

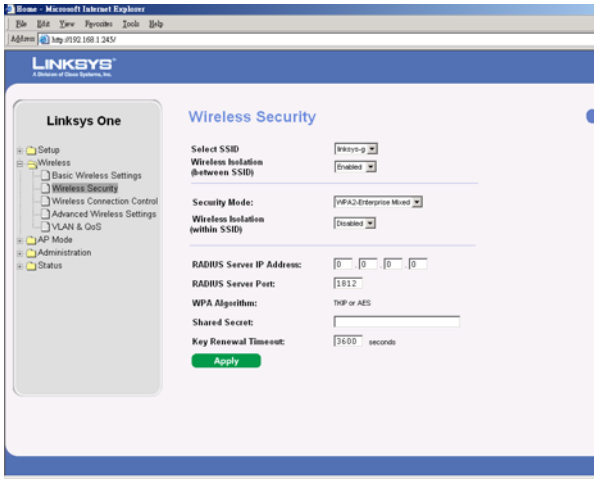
Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.



WPA2-Enterprise Mixed

This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The Access Point will automatically choose the encryption algorithm used by each client device.



RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

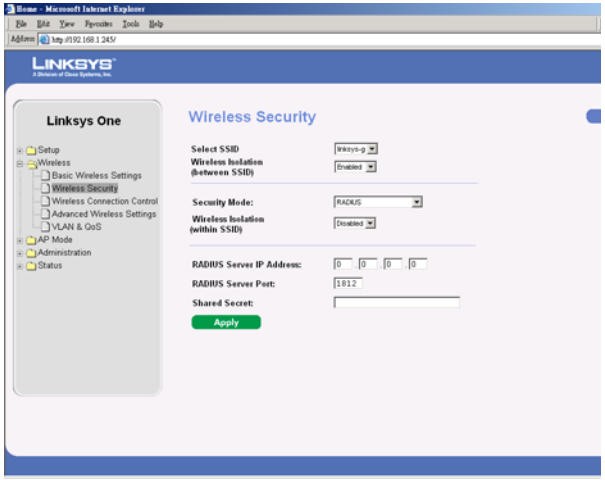
WPA Algorithm. Mixed Mode automatically chooses TKIP or AES for data encryption.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

RADIUS

This security mode is also known as Dynamic WEP with IEEE 802.1X. A RADIUS server is used for client authentication and WEP is used for data encryption. The WEP key is automatically generated by the RADIUS server. Manual WEP key is no longer supported to ensure compatibility with Microsoft's Windows implementation.



RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

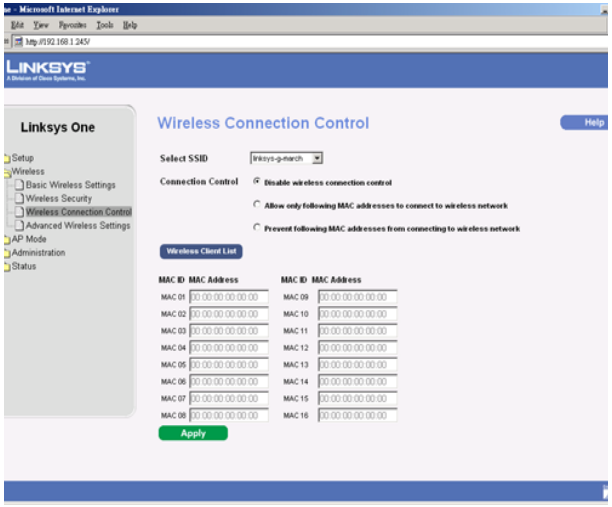
Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Disable

There is no option to be configured for this mode.

When you have finished making changes to the screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. Help information is available on the right side of the screen.

The Wireless - Wireless Connection Control Tab



This screen allows you to configure the Connection Control List to either permit or block specific wireless client devices connecting to (associating with) the Access Point.

Wireless Connection Control

Select SSID. Select the SSID of the wireless network that you want to use wireless connection control on.

Enabled/Disabled. Enable or disable wireless connection control. The default is **disabled**.

Connection Control

Allow only following MAC addresses to connect to wireless network. When this option is selected, only devices with a MAC address specified in the Connection Control List can connect to the Access Point.

Prevent following MAC addresses from connecting to wireless network. When this option is selected, devices with a MAC address specified in the Connection Control List will not be allowed to connect to the Access Point.

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.

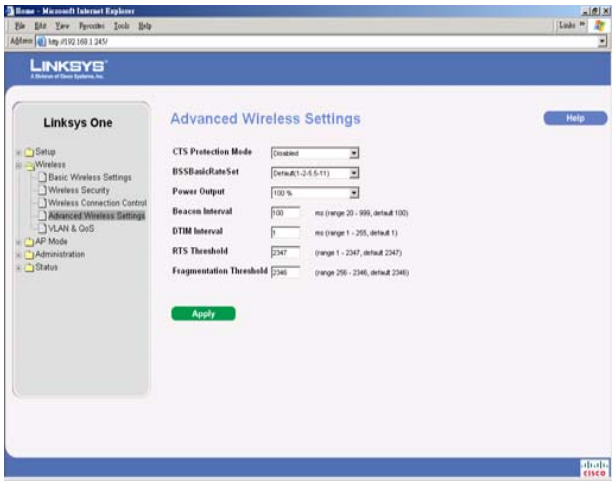
Connection Control List

MAC 01-16. Enter the MAC addresses of the wireless client devices you want to control.

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 available on the right side of the screen.

The Wireless - Advanced Wireless Settings Tab

This screen allows you to configure the advanced settings for the Access Point. Linksys recommends to let your Access Point automatically adjust the parameters for maximum data throughput.



Advanced Settings

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-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.

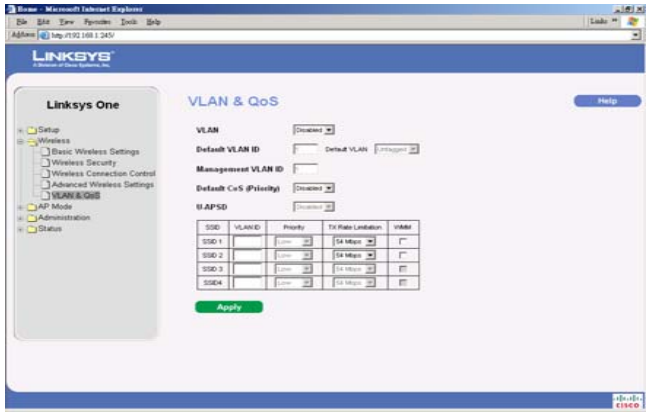
BSSBasicRateSet. This setting is a series of rates that are advertised to other wireless devices as defined in IEEE 802.11 specifications, so they know which data rates the Access Point can support. One of the rates is picked from the list for transmitting control frames, broadcast/multicast frames, or ACK frames. To support both 802.11b & 802.11g devices, use the Default (**Mixed** mode) setting so that frames can be decoded by all devices. To support 802.11g devices only, use the All (**G-only** mode) setting to achieve higher frame rates. For regular data frames, the transmission rate is configured through the Tx Rate Limiting on the Wireless - VLAN & QoS tab.

Power Output. The power output is set to its default setting which is 100%.

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. This specifies the maximum size a data packet can be before splitting and creating a new packet. It should remain at its default setting of 2346. A smaller setting means smaller packets, which will create more packets for each transmission. If you experience high packet error rates, you can decrease this value, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

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 available on the right side of the screen.

The Wireless - VLAN & QoS Tab

This screen allows you to configure the VLAN and QoS related settings for the Access Point.

VLAN

The following options are global VLAN settings for the Access Point.

VLAN. Select **Enabled** if you want to pass 802.1q VLAN tagged traffic between the wired LAN and wireless LAN. Your Access Point will map the VLAN tag (wired side) to different SSIDs (wireless side) according to your specified settings. Select **Disabled** and your Access Point will drop all tagged traffic coming in from the wired LAN. The default is **Disabled**.

Default VLAN ID. Enter the VLAN ID number, the default VLAN is 1.

VLAN Tag. Untagged is the default and should be used if the VLAN ID does not carry a tag. Otherwise, select the **Tagged** option.

AP Management VLAN. When the **VLAN** option is enabled, the value entered (VLAN ID) in this field defines the VLAN that can connect to the Access Point's web-based utility. The default setting is VLAN 1.

QoS

The following options are VLAN global settings for the Access Point.

Default CoS (Priority). Select **Enabled** if you want to assign a default CoS value to each SSID. This option is automatically enabled when the VLAN option is enabled. The default is **Disabled**.

U-APSD (Unscheduled Automatic Power Save Delivery). This option is only available when WMM is enabled on any of the SSIDs. Select **Enabled** if you want client devices with U-APSD capability to take advantage of the power save mode. The default is **Disabled**.

SSID Name. Displays the SSIDs defined under the Basic Wireless Settings tab. If an SSID has been disabled, the options cannot be configured.

VLAN ID. Select a number between 1 and 4094 to identify the VLAN. Multiple SSIDs can share the same VLAN value.

Priority. You can assign the default priority (802.1p COS bits) for packets coming in from each wireless network by selecting a number from the drop-down menu. The higher the number, the higher the priority will be. The default is 0.

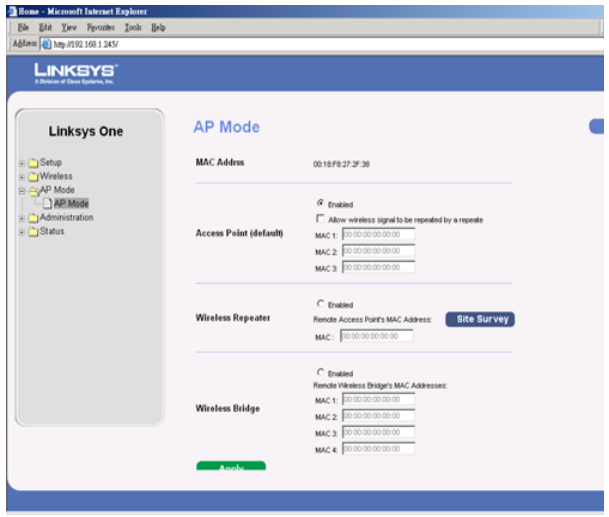
Tx Rate Limiting. You can limit the maximum data rate used in your network to save bandwidth and power consumption on client devices. The actual data rate is determined by the Auto-Fallback mechanism between your Access Point and a client device. The default is 54 Mbps for Mixed or G-Only wireless mode, 11 Mbps for B-Only mode.

WMM. Wi-Fi Multimedia is a QoS feature defined by the WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When this 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 the IP or layer 2 header). WMM provides the capability to prioritize wireless traffic in your environment. The default is Disabled (unchecked).

The AP Mode Tab

On this screen you can change the Access Point's mode of operation. In most cases, you can keep the default setting - **Access Point**. You may wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless repeater to extend the range of your wireless network. You may also wish to change the Access Point's mode of operation if you want to use the Access Point as a wireless bridge; for example, you can use two Access Points in Wireless Bridge mode to connect two wired networks that are in two different buildings.

AP Mode



The Access Point offers three modes of operation: Access Point, Wireless Repeater, and Wireless Bridge. For the Repeater and Bridge modes, make sure the SSID, channel, and security settings are the same for the 0ther wireless access points/devices.

MAC Address

The MAC address of the Access Point is displayed here.

Access Point. The Mode is set to Access Point by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary.

Allow wireless signal to be repeated by a repeater. Select this option if you want to use another wireless device to repeat the signal of this Access Point. You will need to enter the MAC address(es) of the repeating device(s). Up to 3 repeaters can be used.

Wireless Repeater. When set to Wireless Repeater mode, the Wireless Repeater is able to talk to up a remote access point within its range and retransmit its signal. Click **Site Survey** to select the access point that will have its signal repeated by this Access Point or enter the MAC address of the access point manually.

Wireless Bridge. This mode connects physically separated wired networks using multiple access points. Wireless clients will not be able to connect to the access point in this mode. This access point can operate in point-to-point and point-to-multipoint bridge mode. Like any wireless bridge, the WAP2000 lets you wirelessly connect two or more Ethernet LANs together. Enter the MAC address(es) of the access point(s) that will bridge to this access point.

The Administration - Management Tab

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

Management

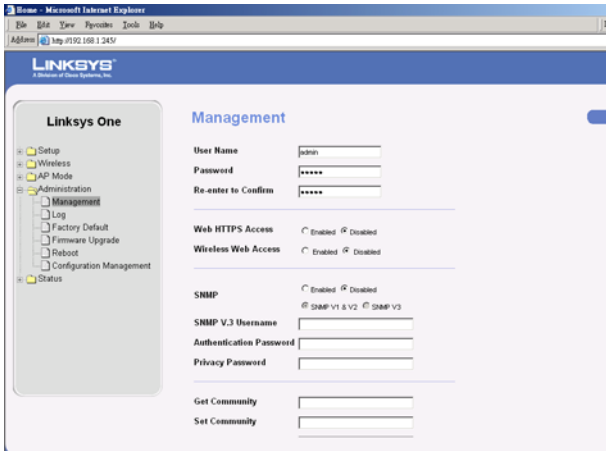
You should change the username/password that controls access to the Access Point's Web-based Utility to prevent unauthorized access.

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 **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**.

This Access Point supports SNMP version 1, 2, and 3. Select **SNMP V1 & V2** if you don't need the enhanced capability on V3 or your management software does not support V3. Otherwise, select **SNMP V3**.

Identification

User Name. SNMPv3 only. Create a administrator account to access and manage the SNMP MIB objects.

Authentication Password. SNMPv3 only. Enter the authentication password for administrator account (minimum length 8).

Privacy Passphrase. SNMPv3 only. Enter the passphrase for data encryption on administrator's management traffic.

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.

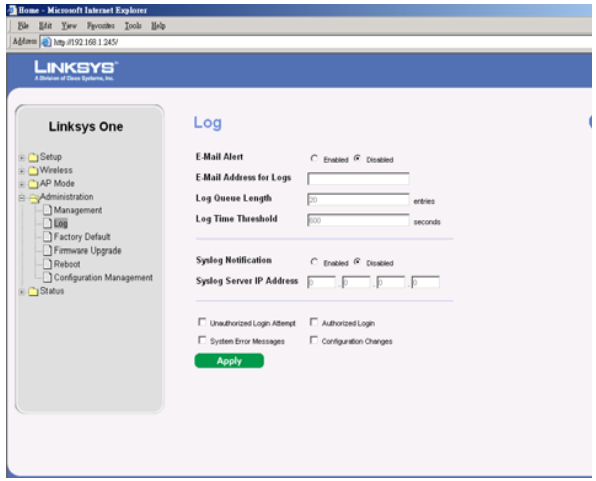
SNMP Trusted Host. You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.

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 available on the right side of the screen.

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**.

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.

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 available on the right side of the screen.

The Administration - Factory Default Tab

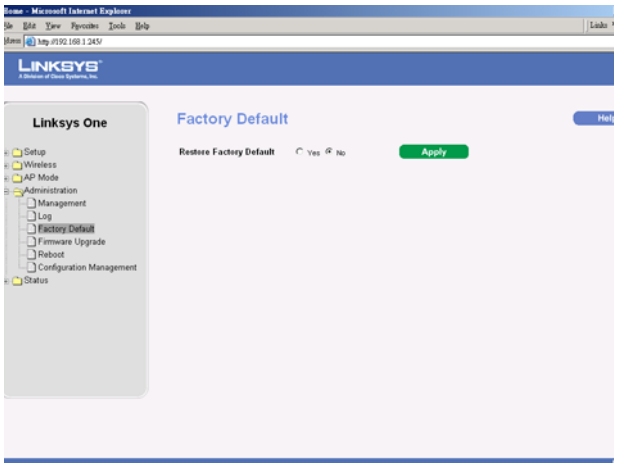
On this screen you can restore the Access Point's factory default settings.

Factory Default

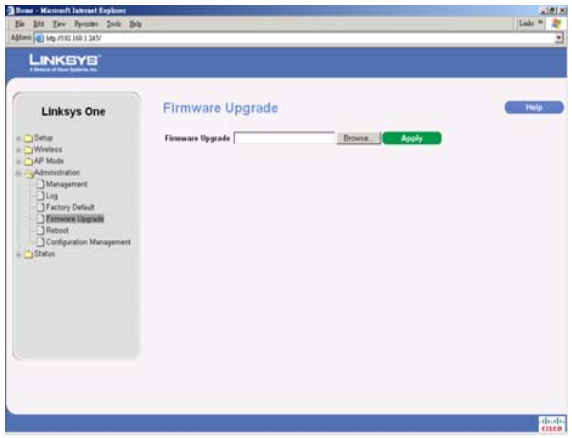
Note any custom settings before you restore the factory defaults. Once the Access Point is reset, you will have to re-enter all of your configuration settings.

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

Note: The Restore Factory Defaults will restore the device to its factory default which will erase all of your saved changes. It also means that the Ethernet interface will be set to use DHCP.



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:

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

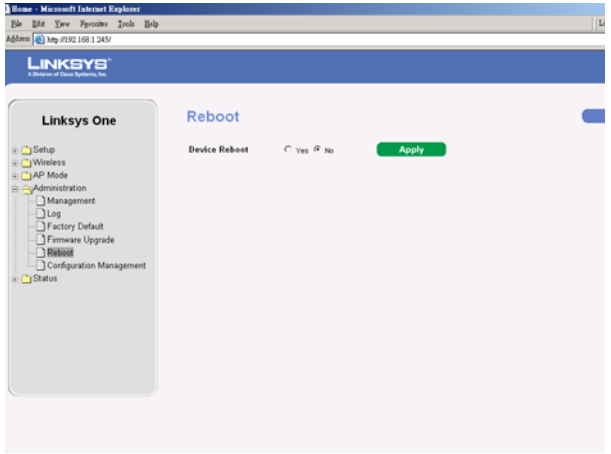
Extract the firmware upgrade file on your computer.

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.

Click the **Apply** button, and follow the on-screen instructions.

Help information is available on the upper-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.

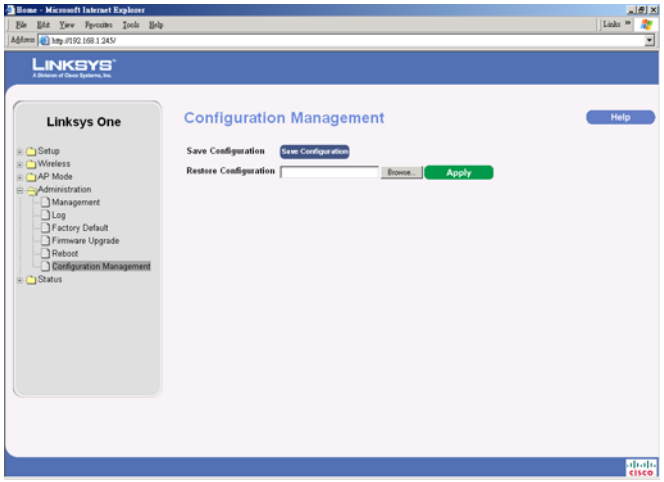
Device Reboot. To reboot the Access Point, click the **Yes** radio button.

Click **Apply** to apply your change and the Access Point will reboot itself, or cancel your change by not clicking **Apply**. Help information is available on the upper-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.

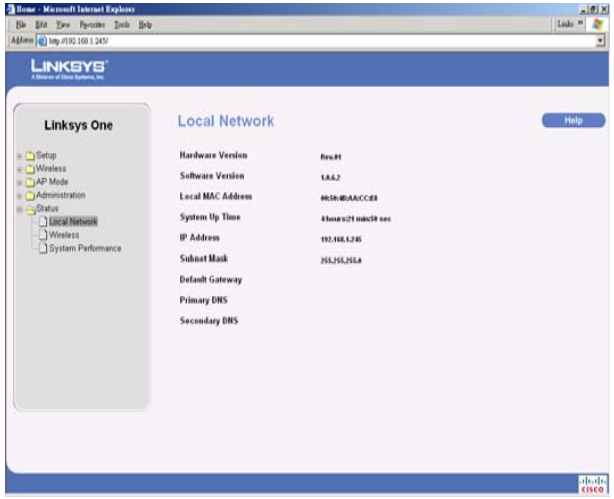
Save Configuration. To save a backup configuration file on a computer, click the **Save Configuration** button and follow the on-screen instructions.

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 **Apply** button.

Help information is available on the right 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 period 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 available on the right side of the screen.

Default Gateway. This shows the default gateway that has been set in the Setup Tab.

Primary DNS/Secondary DNS. This shows the primary/secondary DNS that has been set in the Setup Tab.

The Status - Wireless Tab

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

Wireless Network

MAC Address. The MAC Address of the Access Point's wireless interface is displayed here.

Mode. The Access Point's wireless network mode which could be B, G, mixed or disabled. is displayed here.

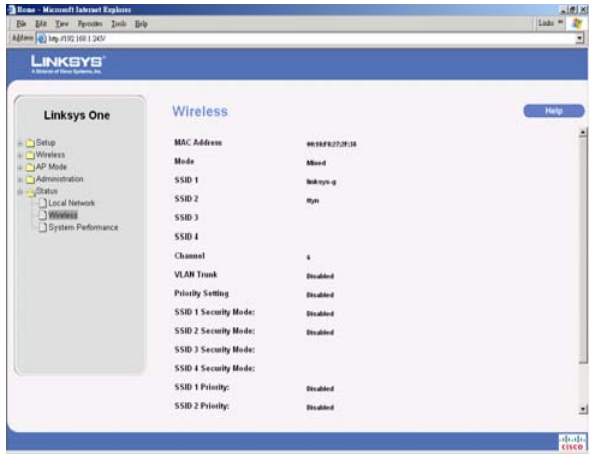
SSID 1-4. The Access Point's SSIDs that have been configured are displayed here.

Channel. The Access Point's Channel setting for the SSID is shown here.

VLAN Trunk. The VLAN Trunk Status is displayed here.

Priority Setting. The priority setting status is displayed here.

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

A Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Access Point with Power Over Ethernet. Read the 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.

What is the IEEE 802.11b standard?

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

What is the IEEE 802.11g standard?

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

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11 functions:

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

What is Ad-hoc?

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

What is Infrastructure?

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

What is roaming?

Roaming is the ability of a portable computer 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.

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.

B Wireless Security

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

Security Precautions

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

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.
8. To ensure network security, steps one through five should be followed, at least.

Security Threats Facing Wireless Networks

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

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your

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.

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:

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

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

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

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

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

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

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Change your WEP key regularly

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

WPA. Wi-Fi Protected Access (WPA) is the replacement standard for WEP in Wi-Fi security. Two modes are available: Personal, and Enterprise. Both give you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. Enterprise utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

WPA Personal. If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the AP or other device how often it should change the encryption keys.

WPA Enterprise. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the AP or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

WPA2. Wi-Fi Protected Access 2 (WPA2) is the latest security standard in Wi-Fi security. Two modes are available: Personal and Enterprise. WPA2 always uses AES (Advanced Encryption System) for stronger data encryption.

WPA2 Personal. If you do not have a RADIUS server, enter a password in the Pre-Shared key field of 8-63 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the AP or other device how often it should change the encryption keys.

WPA2 Enterprise. WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the AP or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

WPA2 Mixed. WPA2 Mixed modes provide users an upgrade path from WPA to WPA2. You can have client devices running both WPA and WPA2 and the Access Point will automatically select the security method used by the client.

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.

C

Upgrading Firmware

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

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


C

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.


D

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 (**A**dvanced **E**ncryption **S**tandard) - A security method that uses symmetric 128-bit block data encryption.

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

Bit - A binary digit.

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

Broadband - An always-on, fast Internet connection.

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

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

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

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

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - 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 (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - 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 (**D**e**m**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) - 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 (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

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

EAP (**E**xtensible **A**uthentication **P**rotocol) - 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 (**F**ile **T**ransfer **P**rotocol) - 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 (**H**yper**T**ext **T**ransport **P**rotocol) - 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 (**I**nternet **P**rotocol) - 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 (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

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

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

NAT (**N**etwork **A**ddress **T**ranslation) - 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 (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

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

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - 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 (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**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 (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (**S**ervice **S**et **ID**entifier) - 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 (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - 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 (**T**rivial **F**ile **T**ransfer **P**rotocol) - 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 (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

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

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix

E

Regulatory Information

Federal Communication Commission Interference 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.

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.

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 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.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS-210 of the Industry Canada 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.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

- Ce périphérique ne doit pas causer d'interférence et.
- Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with IC 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.

This device has been designed to operate with an antenna having a maximum gain of 3 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

G

Linksys Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at: http://www.linksys.com/international

If you experience problems with any Linksys product, you can e-mail us at:

In Europe	E-mail Address
Austria	support.at@linksys.com
Belgium	support.be@linksys.com
Czech Republic	support.cz@linksys.com
Denmark	support.dk@linksys.com
Finland	support.fi@linksys.com
France	support.fr@linksys.com
Germany	support.de@linksys.com
Greece	support.gr@linksys.com (English only)
Hungary	support.hu@linksys.com
Ireland	support.ie@linksys.com
Italy	support.it@linksys.com
Netherlands	support.nl@linksys.com
Norway	support.no@linksys.com
Poland	support.pl@linksys.com
Portugal	support.pt@linksys.com

In Europe	E-mail Address
Russia	support.ru@linksys.com
Spain	support.es@linksys.com
Sweden	support.se@linksys.com
Switzerland	support.ch@linksys.com
United Kingdom	support.uk@linksys.com

Outside of Europe	E-mail Address
Asia Pacific	asiasupport@linksys.com (English only)
Latin America	support.portuguese@linksys.com or support.spanish@linksys.com
Middle East & Africa	support.mea@linksys.com (English only)
South Africa	support.ze@linksys.com (English only)
UAE	support.ae@linksys.com (English only)
U.S. and Canada	support@linksys.com

Software Release Number 1.8.0