

LINKSYS®

A Division of Cisco Systems, Inc.



USER GUIDE

BUSINESS SERIES

Wireless-G Access Point with Power Over Ethernet

LINKSYS **one** Ready

Model: WAP2000


CISCO

About This Guide

Icon Descriptions

While reading through the User Guide you may encounter various icons designed to call attention to a specific item. Below is a description of these icons:



NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.



WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Open Source

This product may contain material licensed to you under the GNU General Public License or other open-source software licenses. Upon request, open-source software source code is available at cost from Linksys for at least three years from the product purchase date.



WEB: For detailed license terms and additional information visit: www.linksys.com/gpl

Chapter 1: Introduction	1
Chapter 2: Planning Your Wireless Network	2
Network Topology	2
Roaming	2
Network Layout.	2
Example of a Simple Wireless Network	2
Chapter 3: Product Overview	3
Front Panel.	3
Back Panel	3
Side Panels.	3
Chapter 4: Installation	4
Placement	4
Wall-Mount	4
Connecting the Access Point	5
Chapter 5: Advanced Configuration	6
Accessing the Web-Based Utility	6
Web-Based Utility	6
Setup > Setup.	6
Setup > Time	7
Wireless > Basic Wireless Settings	7
Wireless > Wireless Security	8
Wireless > Wireless Connection Control	12
Wireless > Advanced Wireless Settings	12
Wireless > VLAN & QoS	13
AP Mode	14
Administration > Management.	14
Administration > Log	15
Administration > Factory Default.	16
Administration > Firmware Upgrade	16
Administration > Reboot	16
Administration > Configuration Management	17
Status > Local Network	17
Status > Wireless	18
Status > System Performance	18
Appendix A: Troubleshooting	20
Appendix B: Wireless Security Checklist	23
General Network Security Guidelines	23
Additional Security Tips	23

Appendix C: Glossary	24
Appendix D: Specifications	28
Appendix E: Warranty Information	29
Appendix F: Regulatory Information	30
FCC Statement30
FCC Radiation Exposure Statement30
Safety Notices.30
Industry Canada Statement30
Industry Canada Radiation Exposure Statement:.30
Avis d'Industrie Canada.31
Avis d'Industrie Canada concernant l'exposition aux radiofréquences :.31
Wireless Disclaimer31
Avis de non-responsabilité concernant les appareils sans fil31
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)32
Appendix G: Contact Information	36

Chapter 1: Introduction

Thank you for choosing the Wireless-G Access Point with Power Over Ethernet.

The Wireless-G Access Point with Power Over Ethernet is ideal for small businesses that want to expand their existing wired networks or create new wireless networks for the workforce or guests. The Access Point features RangeBooster technology that is compatible with standard 802.11g but with a range up to two times further and throughput up to 35% faster. Unlike ordinary wireless technologies that are hampered by wireless signals that reflect off walls, ceilings, and other objects, RangeBooster uses these multiple signals with two smart receivers at each end (router or access point and client adapter) to boost range and throughput speeds. As a result, a RangeBooster solution reduces or eliminates wireless signal dead spots in offices and other buildings so users can connect to the network in more areas. The Access Point comes with two 3 dBi antennas for increased power, also helping to extend the range of the Access Point.

Advanced security features like Wi-Fi Protected Access™ (WPA2 Enterprise), make this solution ideal for business. Integrated Quality of Service (QoS) features provide consistent voice and video quality on both the wired and wireless networks, enabling your workforce to communicate or view video content without disruptions and delay.

The Wireless-G Access Point with Power Over Ethernet can be powered from its included AC adapter or from a Power over Ethernet (PoE) Switch via Ethernet cabling, enabling mounting in ceilings or high on walls where power outlets may not be available.

Additional features like Multiple BSSIDs, Wireless Roaming, Auto-Channel Selection, and Load Balancing give your business added flexibility to keep employees and guests connected. The Access Point also features dual firmware images so it remains functional if a firmware upgrade process is disrupted.

The Wireless-G Access Point with Power Over Ethernet is Linksys One Ready. That means it includes the necessary firmware for seamless integration into a Linksys One data or data/voice network. Once connected, a Linksys One Service Router will discover the Access Point, automatically configure it and make it available to other users on the network. Linksys One technology is automatic and self-configuring.

Chapter 2: Planning Your Wireless Network

Network Topology

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

Linksys wireless adapters also provide access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired 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 doubled (depending on antenna characteristics).

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 security and SSID.

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



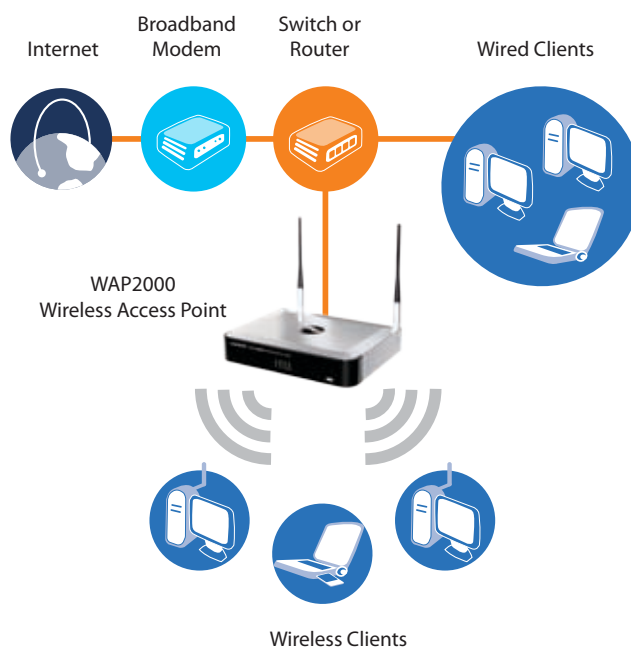
NOTE: Spanning Tree Protocol should be disabled on the switches connecting to the APs to allow roaming to work without disruption.

Network Layout

The Access Point has been designed for use with 802.11g and 802.11b products, such as the Notebook Adapters for your laptop computers, PCI Adapters for your desktop PCs, and USB Adapters for either a laptop or desktop. These wireless products can also communicate with a 802.11g or 802.11b Wireless Print Server.

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router.

Example of a Simple Wireless Network



Example of Simple Wireless Network

The above diagram shows a typical infrastructure wireless network setup. The Wireless Access Point connects to a Linksys switch that provides power to the Access Point. The 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 for Internet access.


Chapter 3: Product Overview


Front Panel


The front panel is where the Access Point's LEDs are located. The LEDs display information about network activity and connectivity.




Front Panel

 **Power** (Green) The Power LED lights up when the Access Point is powered on.

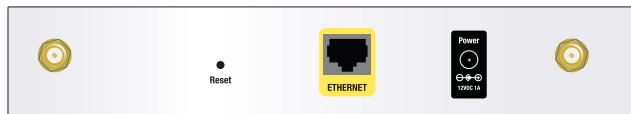
 **PoE** (Green) The PoE LED lights up when the Access Point is powered through Ethernet cable.

 **Wireless** (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 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.

Back Panel

The back panel is where the power, Ethernet, and antennas are connected to the Access Point.



Back Panel

 **Antenna Ports** The Access Point has two antenna ports for connecting detachable 3 dBi omnidirectional antennas. Adjust the two antennas so that they form a 90 degree angle for best MIMO range performance.

- **Reset** There are two ways to reset the Access Point's factory defaults. Either press the **Reset** button for more than ten seconds, or restore the defaults using the Access Point's web-based utility. If you press the reset button for less than ten seconds, the Access Point will simply reboot.

If you power on the Access Point while holding down the reset button, the Access Point will be configured with a default static IP address of **192.168.1.245**, see "Chapter 5: Advanced Configuration" for details.



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



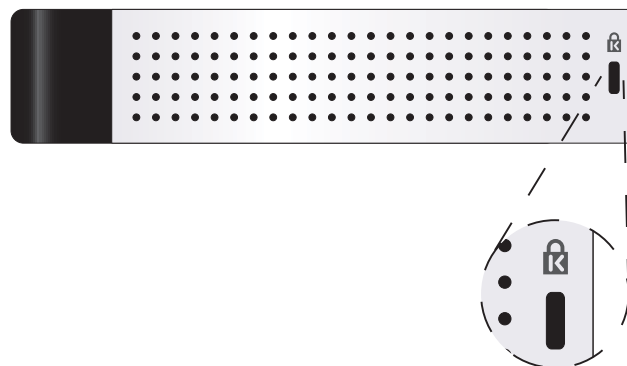
Ethernet The Ethernet network port connects to Ethernet network devices, such as a switch or router. The Access Point can be powered using Power over Ethernet.



Power The Power port connects to the supplied power adapter. Use this option if your switch or router doesn't support Power over Ethernet.

Side Panels

Security slots are located on both side panels of the Access Point.



Side Panel



Security Slots The security slots can be utilized to attach a lock to the Access Point.

Chapter 4: Installation

Placement

The Access Point can be placed horizontally on a flat surface such as a desktop so it sits on its four rubber feet or it can be mounted on a wall.





Desktop Placement

Wall-Mount

The unit has two sets of wall-mount slots so that it can be mounted either vertically or horizontally.

You will need 2 suitable screws to mount the Access Point.

Suggested Mounting Hardware

		2.5-3 mm
4-5 mm	1-2 mm	

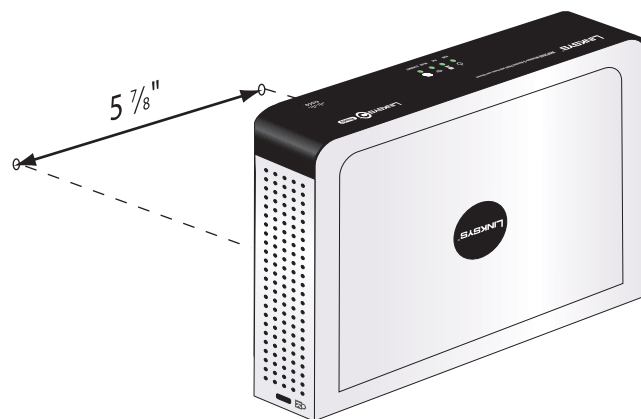


NOTE: Linksys is not responsible for damages incurred by insecure wall-mounting hardware.

1. Determine where you want to mount the Access Point. Ensure that the wall you use is smooth, flat, dry and sturdy and make sure the location is within reach of the power outlet.
2. Drill two holes into the wall for either vertical or horizontal placement.



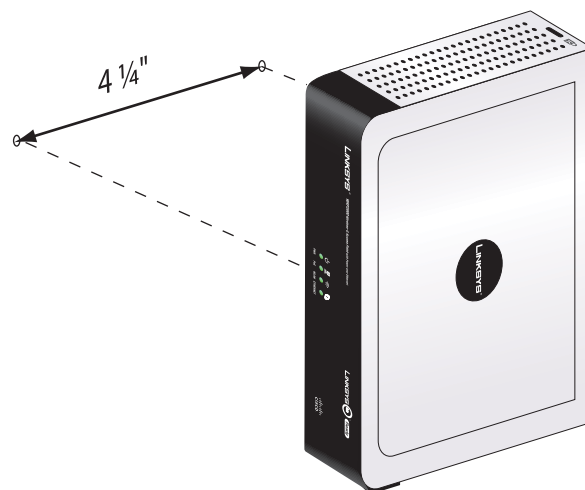
NOTE: The printed Quick Installation Guide that accompanies the Access Point includes templates that can be used for spacing between holes.



Horizontal Mounting



NOTE: The Access Point should be oriented as shown above for horizontal mounting.



Vertical Mounting

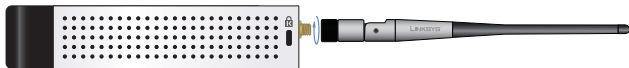


NOTE: The Access Point should be oriented as shown above for vertical mounting.

3. Insert a screw into each hole, and leave 3 mm of its head exposed.
4. Maneuver the Access Point so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Access Point down until the screws fit snugly into the wall-mount slots.

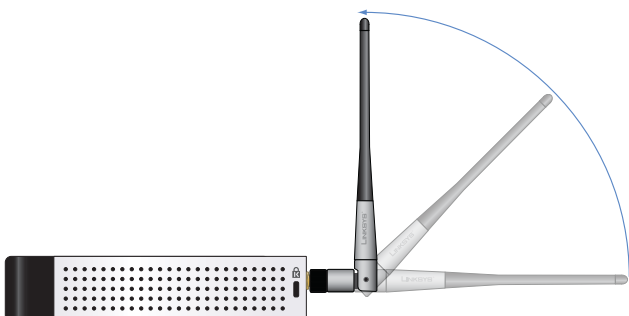
Connecting the Access Point

1. Connect the antennas to the antenna connectors on the Access Point.



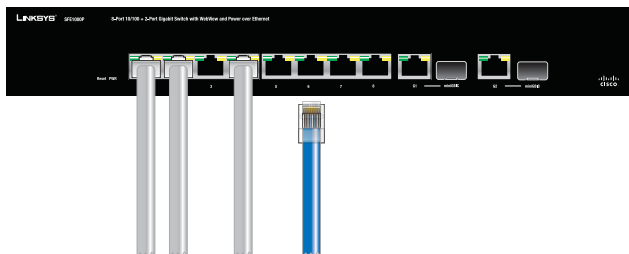
Connect the Antennas

2. Adjust the two antennas so that they form a 90 degree angle for best performance.



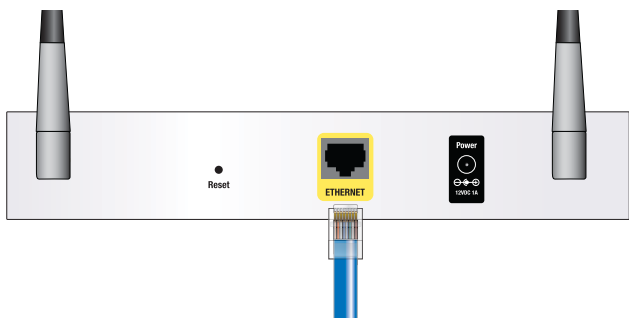
Adjust the Antennas

3. Connect your Ethernet network cable to your network router or switch.



Connect the Ethernet cable to the Router or Switch

4. Connect the other end of the network cable to the Access Point's Ethernet port.

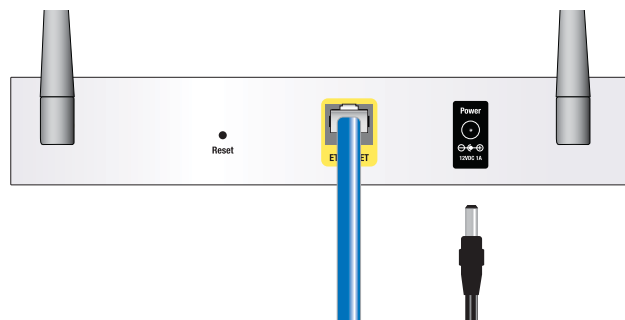


Connect the Ethernet cable to the Access Point



NOTE: If your router or switch provides Power over Ethernet, then step 5 is not necessary.

5. If you are not using PoE (Power over Ethernet), 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.



Connect the Power

Installation is complete. For advanced configuration information, proceed to the next chapter.

Chapter 5: Advanced Configuration

The Access Point has DHCP enabled by default and should receive an IP address automatically from the DHCP server on your network.

If your network doesn't have a DHCP server, a static IP address (**192.168.1.245**) can be assigned to the Access Point by performing the following steps:

1. Disconnect the power to the unit.
2. Using a straightened paper clip or similar object to hold down the reset button on the back panel of the Access Point.
3. Keep the reset button held down and reconnect the power to the unit. The reset button should be held until the WLAN LED lights up.

Accessing the Web-Based Utility

1. Open your web browser and enter the IP address of your Access Point into the *Address* field and press the **Enter** key. The *Password* screen will appear.



Address Field

2. The first time you open the web-based utility, enter **admin** (the default user name) in the *User name* field and enter it again in the *Password* field. Click the **OK** button. You can change the Access Point's password later from the *Administration > Management* screen.



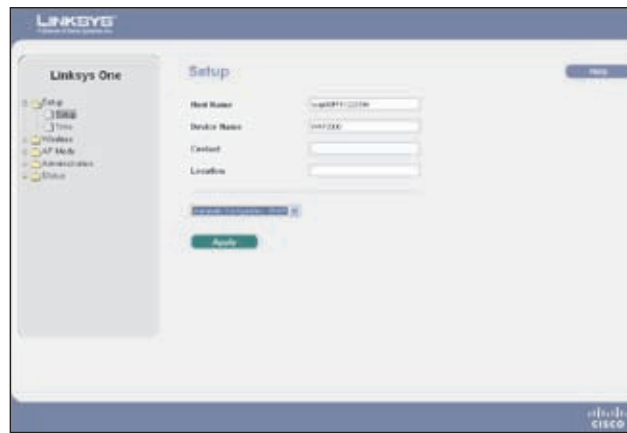
Login Screen

Web-Based Utility

The first screen that appears is the *Setup* screen. This allows you to change the Access Point's general settings. There are options on the left side of the screen: Setup, Wireless, AP Mode, Administration, and Status. Each option contains screens that will help you configure and manage the Access Point.

Setup > Setup

This screen is used to enter names for the Access Point and configure the IP settings.



Setup > Basic Setup

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.

Contact Use this field to specify the contact string for your SNMP agent.

Location Use this field to specify the location string for your SNMP agent.

Automatic Configuration - DHCP Selected by default, this option is used if you have a DHCP server enabled on the LAN and want it to assign an IP address to the Access Point.

Static IP Address This option is used to assign a static or fixed IP address to the Access Point.



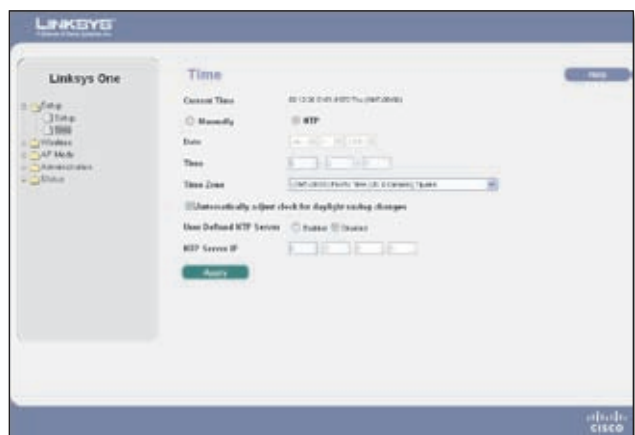
Setup > Basic Setup with Static IP

- **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 the LAN that your Access Point is connected to. The default is **255.255.255.0**.
- **Default Gateway** Enter the default gateway address, typically this is the IP address of your router.
- **Primary DNS (Required) and Secondary DNS (Optional)** Your ISP will provide you with at least one DNS (Domain Name System) Server IP address.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Setup > Time

This screen 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.



Setup > Time

You can set the time either manually or use the NTP option to automatically set the time from a time server if the Access Point can access the public Internet. **NTP** is the default setting.

Current Time Displays the current time setting.

Manually Select this option to set the date and time manually.

- **Date** When the time is manually configured, this field is used to select the current date from the pull-down menus.
- **Time** When the time is manually configured, this field is used to enter the time. The time is entered in a 24 hour format (hour : minutes : seconds).

NTP Select this option if you want the Access Point to contact a public time server to get the current time.

- **Time Zone** When NTP is enabled, the appropriate time zone must be selected.
- **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.

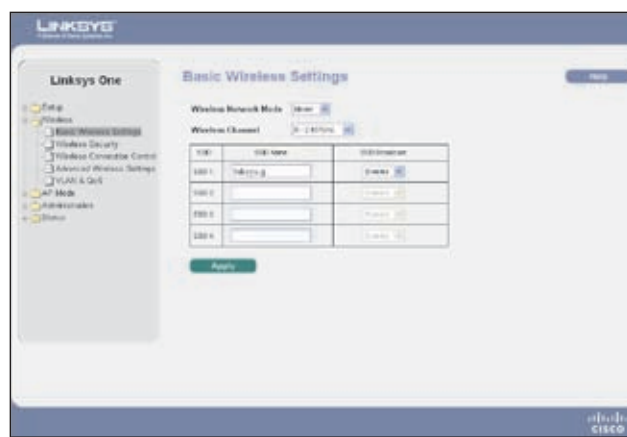
User Defined NTP Server Enable this option if you have set up a local NTP server. Default is **Disabled**.

NTP Server IP Enter the IP address of user defined NTP Server.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Wireless > Basic Wireless Settings

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.



Wireless > Basic Wireless Settings

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

- **Disable** This option disables wireless connectivity completely. This is useful during system maintenance.

- **B-Only** This option is used when all wireless client devices connect to the Access Point at Wireless-B data rates (maximum speed of 11 Mbps).
- **G-Only** This option is used when all wireless client devices connect to the Access Point at Wireless-G data rates (maximum speed of 54 Mbps). Wireless-B clients cannot be connected in this mode.
- **Mixed** This option allows both Wireless-B and Wireless-G client devices to connect to the Access Point at their respective data rates. Wireless-G devices can be connected at Wireless-G data rates.

Wireless Channel Select the appropriate channel to communicate between the 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 the **Apply** 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. 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** to make network configuration easier.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Wireless > Wireless Security

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



Wireless > Wireless Security

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

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. The detailed options are described on the following pages:

- **WEP**
- **WPA-Personal**
- **WPA2-Personal**
- **WPA2-Personal Mixed**
- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA2-Enterprise Mixed**
- **RADIUS**



NOTE: 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.

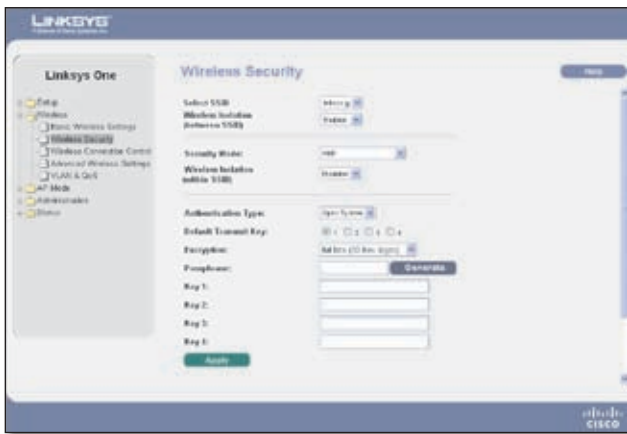
To disable wireless security completely, select **Disabled**. The default is **Disabled**.

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.

WEP

This security mode is defined in the original IEEE 802.11 specification. This mode is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.



Wireless > Wireless Security > WEP

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. The default is **1**.

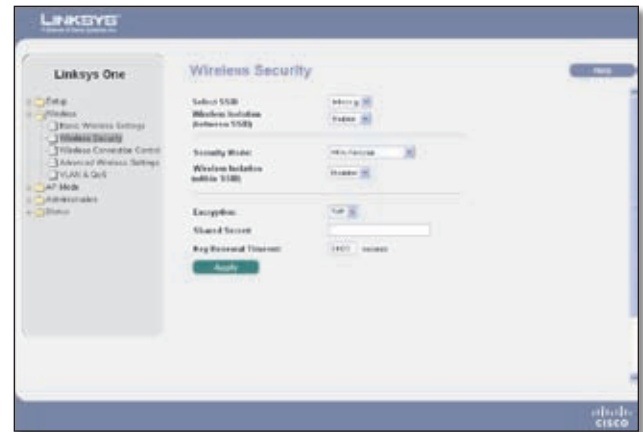
Encryption Select a level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). The default setting is **64 bits**.

Passphrase If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the **Generate** button. 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 **Apply** to save your changes. Help information is available on the right side of the screen.

WPA-Personal (aka WPA-PSK)



Wireless > Wireless Security > WPA-Personal

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

Shared Secret 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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

WPA2-Personal



Wireless > Wireless Security > WPA2-Personal

Encryption WPA2 always uses AES for data encryption.

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

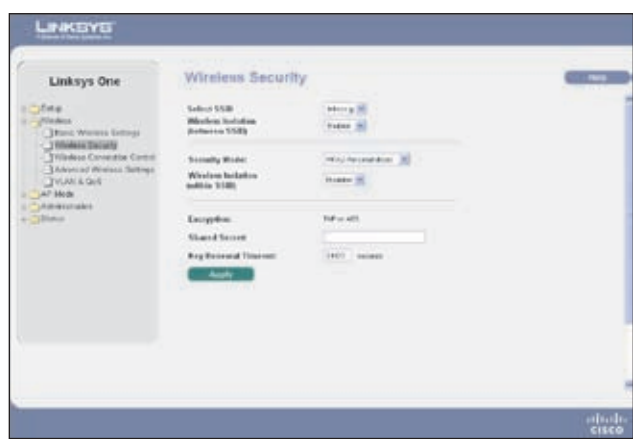
Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Access Point how often it

should change the encryption keys. The default is **3600** seconds.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

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.



Wireless > Wireless Security > WPA2=Personal Mixed

Encryption Mixed Mode automatically chooses TKIP or AES for data encryption.

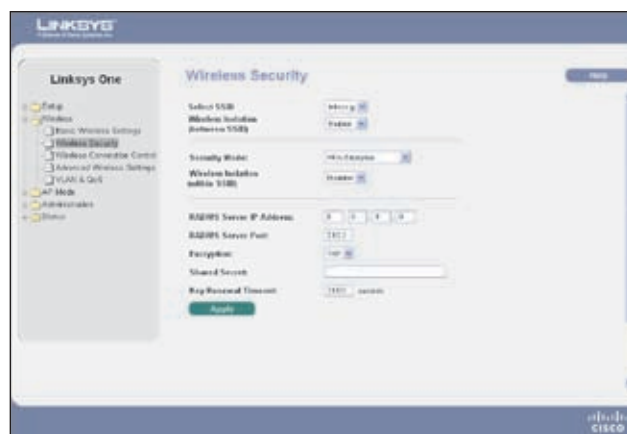
Shared Secret Enter a WPA Shared Key of 8-63 characters.

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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

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.)



Wireless > Wireless Security > WPA-Enterprise

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**.

Encryption 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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

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.)



Wireless > Wireless Security > WPA2-Enterprise

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**.

Encryption 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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

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.



Wireless > Wireless Security > WPA2-Enterprise Mixed

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.

Encryption 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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

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.



Wireless > Wireless Security > RADIUS

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.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

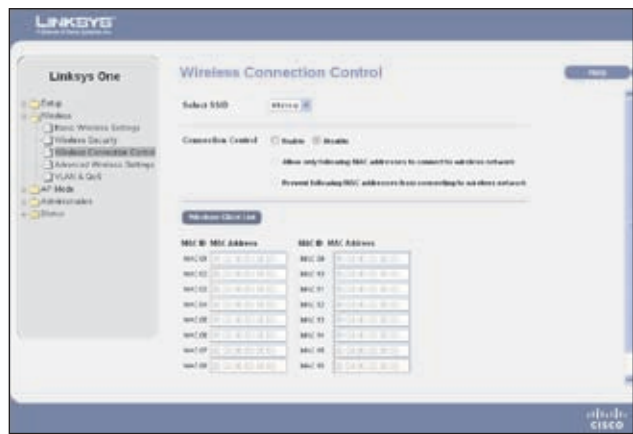
Disable

There are no options to be configured for this mode.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Wireless > Wireless Connection Control

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 > Wireless Connection Control

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

Connection Control Enable or disable wireless connection control. The default is set to **Disable**. When connection control is enabled, the following options are available:

- **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.



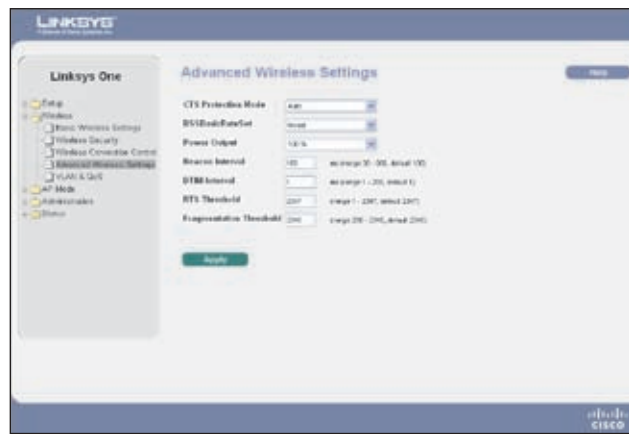
Wireless Client List

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 **Apply** to save your changes. Help information is available on the right side of the screen.

Wireless > Advanced Wireless Settings

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



Wireless > Advanced Wireless 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. **Auto** allows the Access Point to use this feature as needed, when Wireless-G products are not able to transmit to the Access Point in an environment with heavy 802.11b traffic. This option is **Disabled** by default.

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**) setting so that frames can be decoded by all devices. To support 802.11g devices only, use the All (G-only) 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 You can adjust the output power of the Access Point to get the appropriate coverage for your wireless network. Select the level you need for your environment. If you are not sure of which setting to choose, then keep the default setting, **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**.

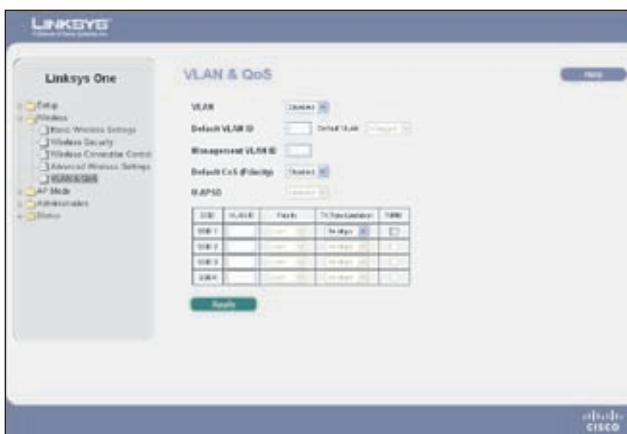
RTS Threshold This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.

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 **Apply** to save your changes. Help information is available on the right side of the screen.

Wireless > VLAN & QoS

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



Wireless > VLAN & QoS

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 default VLAN ID number (1 - 4094), the default value is **1**. The default VLAN number should match with your Switch's settings. For example, the SRW2024 has Trunk port mode which set default VLAN (PVID) to 1 untagged, while General port mode can set PVID to any VLAN either tagged or untagged.

Default VLAN Set the tagging option for the default VLAN ID. This has to match your Switch's settings. The default is **untagged**.

Management VLAN ID When the VLAN option is enabled, the value entered (VLAN ID) in this field defines the VLAN that connects to the Access Point. The default value is **1**. The VLAN should be accessible from the wired side in order to use web-based utility. To access the web-based utility from wireless side, the SSID needs to map to the same VLAN ID. Remember to enable wireless web access on the *Administration > Management* tab.

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 on the *Basic Wireless Settings* screen. If an SSID has been disabled, the options cannot be configured.

VLAN ID Select a VLAN ID (1 - 4094) for the SSID where you want to map the traffic to on the wired side. The wireless traffic will not carry VLAN information. Multiple SSIDs can map to the same VLAN on the wired side.

Priority You can assign the default priority (802.1p CoS bits) for packets coming in from each wireless network by selecting a value from the drop-down menu. The default is **Low**.

Tx Rate Limitation 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**.

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).

AP Mode

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.



The AP Mode Tab

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 other 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 communicate with 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.

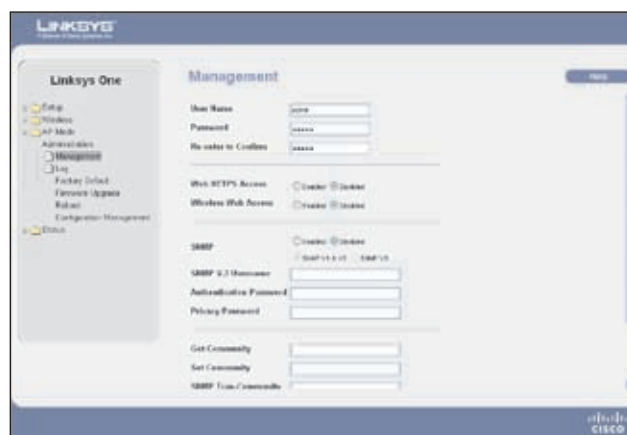


AP Mode > Wireless Repeater > Site Survey

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. Enter the MAC address(es) of the access point(s) that will bridge to this access point.

Administration > Management

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



Administration > Management

You should change the User Name/Password that controls access to the Access Point's web-based utility.

User Name Modify the administrator user name. The default is **admin**.

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.

To increase the security on accessing web-based utility. You can enable HTTPS. Once enabled, users need to use https:// when accessing the web-based utility.

Web HTTPS Access Use secured HTTP session to access web-based utility. 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**.

SNMP V.3 Username Create a SNMP V3 administrator to access and manage MIB objects.

Authentication Password Enter the authentication password for the SNMP V3 administrator. The minimum password length is 8 characters.

Privacy Password Enter the privacy password for the SNMP V3 administrator. The minimum password length is 8 characters.

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.

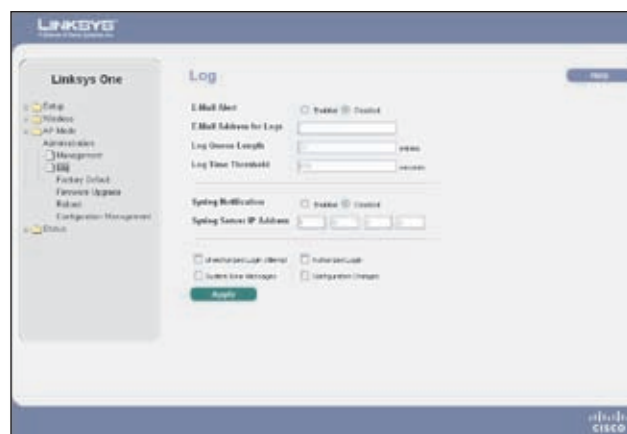
SNMP Trusted Host You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is set to 0.0.0.0, then access is permitted from any IP address.

SNMP Trap-Destination Enter the IP address of the remote host computer that will receive the trap messages. To prevent sending traps to any host in your LAN, enter 0.0.0.0 as the trap destination.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Administration > Log

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



Administration > Log

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 e-mailed 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 check box.

Authorized Login If you want to log authorized logins, click the check box.

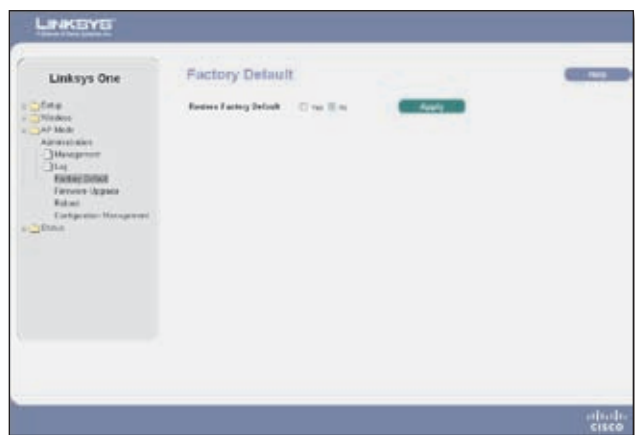
System Error Messages If you want to log system error messages, click the check box.

Configuration Changes If you want to log any configuration changes, click the check box.

Change these settings as described here and click **Apply** to save your changes. Help information is available on the right side of the screen.

Administration > Factory Default

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



Administration > Factory Default

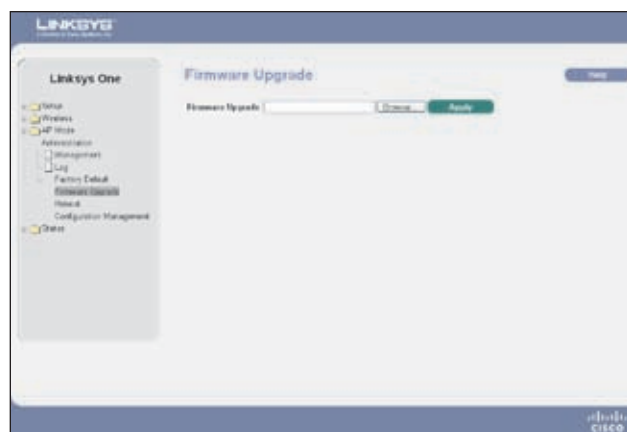
Note any custom settings before you restore the factory defaults. Once the Access Point is reset, you will have to re-enter all of your configuration settings.

Restore Factory Defaults To restore the Access Point's factory default settings, follow the steps below:

1. Click the **Yes** option.
2. Click the **Apply** button.
3. Click **OK** to confirm that you want to restore the factory default settings. Your Access Point will reboot and come back up with the factory default settings in a few seconds.

Administration > Firmware Upgrade

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.



Administration > Firmware Upgrade

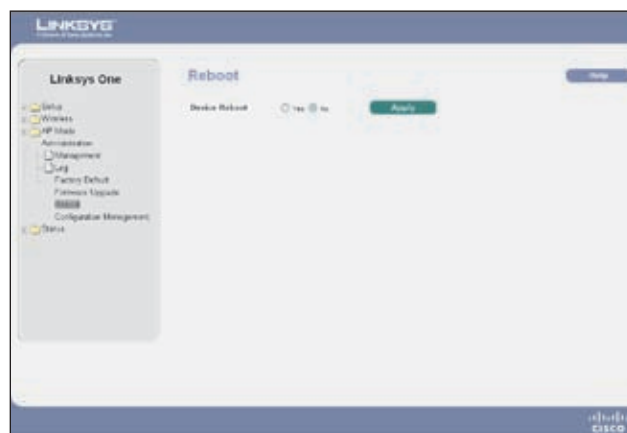
To upgrade the Access Point's firmware:

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

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

Administration > Reboot

On this screen you can reboot the Access Point.



Administration > Reboot

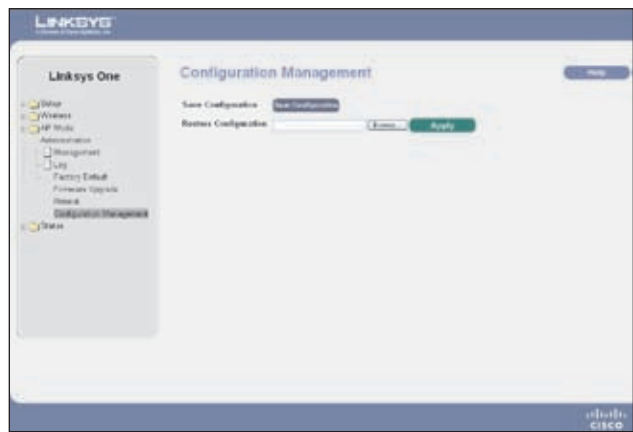
This feature is useful when you need to remotely reboot the Access Point.

Device Reboot To reboot the Access Point, click the **Yes** option. Click **Apply** and the Access Point will reboot itself.

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

Administration > Configuration Management

On this screen you can save a configuration file of the Access Point's current settings or restore a configuration file of previously saved settings.



Administration > Configuration Management

Save Configuration To save a backup configuration file, click the **Save Configuration** button and save the file to the desired location.

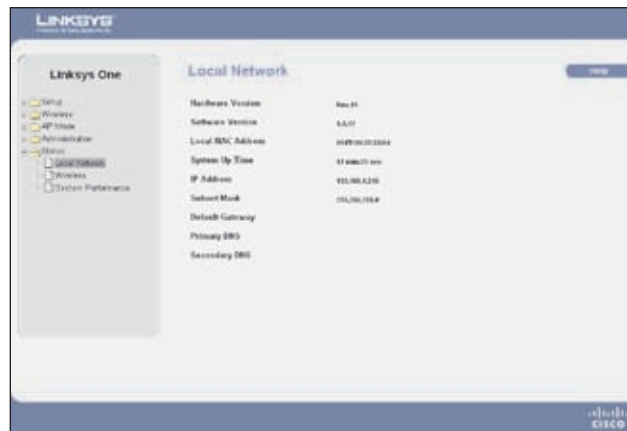
Restore Configuration To upload a configuration file to the Access Point, follow the steps below:

1. Type the filename and path of the configuration file in the field provided or click the **Browse** button to locate the file.
2. Click the **Apply** button.

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

Status > Local Network

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



Status > Local Network

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.

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.

Default Gateway This displays the Access Point's default gateway information.

Primary DNS This displays the Access Point's primary DNS information.

Secondary DNS This displays the Access Point's secondary DNS information.

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

Status > Wireless

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



Status > Wireless

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

Mode The Access Point's wireless network mode 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.

SSID 1-4 Security Mode Displays the security mode utilized for the appropriate SSID.

SSID 1-4 Priority Displays the priority of the SSID.

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

Status > System Performance

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



Status > 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.

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

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Exterior Access Point with Power Over Ethernet. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at www.linksys.com.

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 2.4 GHz.

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 2.4 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 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 65, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.



WEB: If your questions are not addressed here, refer to the Linksys website, **www.linksys.com**

Appendix B: Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.



1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.



2. Change the default password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.



3. Enable MAC address filtering

Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.



4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP.

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 of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

Appendix C: Glossary

This glossary contains some basic networking terms you may come across when using this product.



WEB: For additional terms, please visit the glossary at www.linksys.com/glossary

Access Mode Specifies the method by which user access is granted to the system.

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.

Access Profiles Allows network managers to define profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by the following criteria:

- Ingress interfaces
- Source IP address and/or Source IP subnets.

ACE Filters in Access Control Lists (ACL) that determine which network traffic is forwarded. An ACE is based on the following criteria:

- Protocol
- Protocol ID
- Source Port
- Destination Port
- Wildcard Mask
- Source IP Address
- Destination IP Address

ACL (Access Control List) Access Control Lists are used to grant, deny, or limit access devices, features, or applications.

Auto-negotiation Allows 10/100 Mbps or 10/100/1000 Mbps Ethernet ports to automatically establish the optimal duplex mode, flow control, and speed.

Back Pressure A mechanism used with Half Duplex mode that enables a port not to receive a message.

Bandwidth The transmission capacity of a given device or network.

Bandwidth Assignments Indicates the amount of bandwidth assigned to a specific application, user, and/or interface.

Baud Indicates the number of signaling elements transmitted each second.

Best Effort Indicates that traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.

Bit A binary digit.

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

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

Bridge A device that connect two networks. Bridges are hardware specific, however they are protocol independent. Bridges operate at Layer 1 and Layer 2 levels.

Broadcast Domain Devices sets that receive broadcast frames originating from any device within a designated set. Routers bind Broadcast domains, because routers do not forward broadcast frames.

Broadcast Storm An excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.

Burst A packet transmission at faster than normal rates. Bursts are limited in time and only occur under specific conditions.

Burst Size Indicates the burst size transmitted at a faster than normal rate.

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.

CBS (Committed Burst Size) Indicates the maximum number of data bits transmitted within a specific time interval.

CIR (Committed Information Rate) The data rate is averaged over a minimum time increment.

Class Maps An aspect of Quality of Service system that is comprised of an IP ACL and/or a MAC ACL. Class maps are configured to match packet criteria, and are matched to packets in a first-fit fashion.

Combo Ports A single logical port with two physical connections, including an RJ-45 connection and a SFP connection.

Communities Specifies a group of users which retain the same system access rights.

CoS (Class of Service) The 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.

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.

DHCP Clients An Internet host using DHCP to obtain configuration parameters, such as a network address.

DHCP Server An Internet host that returns configuration parameters to DHCP clients.

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.

DSCP (DiffServ Code Point) Provides a method of tagging IP packets with QoS priority information.

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

EIGRP (Enhanced Interior Gateway Routing Protocol) Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.

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.

Firmware The programming code that runs a networking device.

Flow Control Enables lower speed devices to communicate with higher speed devices. This is implemented by the higher speed device refraining from sending packets.

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.

GARP (General Attributes Registration Protocol) Registers client stations into a multicast domain.

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

GBIC (GigaBit Interface Converter) A hardware module used to attach network devices to fiber-based transmission systems. GBIC converts the serial electrical signals to serial optical signals and vice versa.

GVRP (GARP VLAN Registration Protocol) Registers client stations into a VLANs.

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.

HTTPS (HyperText Transport Protocol Secure) An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

ICMP (Internet Control Message Protocol) Allows the gateway or destination host to communicate with the source host. For example, to report a processing error.

IGMP (Internet Group Management Protocol) Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.

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.

Jumbo Frames Enable transporting identical data in fewer frames. Jumbo Frames reduce overhead, lower processing time, and ensure fewer interrupts.

LAG (Link Aggregated Group) Aggregates ports or VLANs into a single virtual port or VLAN.

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.

Mask A filter that includes or excludes certain values, for example parts of an IP address.

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

MD5 (Message Digest 5) An algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication and authenticates the origin of the communication.

MDI (Media Dependent Interface) A cable used for end stations.

MDIX (Media Dependent Interface with Crossover) A cable used for hubs and switches.

MIB (Management Information Base) MIBs contain information describing specific aspects of network components.

Multicast Transmits copies of a single packet to multiple ports.

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

NMS (Network Management System) An interface that provides a method of managing a system.

OID (Object Identifier) Used by SNMP to identify managed objects. In the SNMP Manager/Agent network management paradigm, each managed object must have an OID to identify it.

Packet A unit of data sent over a network.

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

Policing Determines if traffic levels are within a specified profile. Policing manages the maximum traffic rate used to send or receive packets on an interface.

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

Port Mirroring Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

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

QoS (Quality of Service) Provides policies that contain sets of filters (rules). QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.

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.

RMON (Remote Monitoring) Provides network information to be collected from a single workstation.

Router A networking device that connects multiple networks together.

RSTP (Rapid Spanning Tree Protocol) Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.

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.

SSH Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.

SSL (Secure Socket Layer) Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

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

STP (Spanning Tree Protocol) Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.

Subnet (Sub-network) Subnets are portions of a network that share a common address component. In TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

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

Switch Filters and forwards packets between LAN segments. Switches support any packet protocol type.

TACACS+ (Terminal Access Controller Access Control System Plus) Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

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.

Trunking Link Aggregation. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).

TX Rate Transmission Rate.

UDP (User Data Protocol) Communication protocol that transmits packets but does not guarantee their delivery.

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

Upload To transmit a file over a network.

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

VLAN (Virtual Local Area Networks) Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.

WAN (Wide Area Network) Networks that cover a large geographical area.

Wildcard Mask Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

For example, if the destination IP address is 149.36.184.198 and the wildcard mask is 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.

Appendix D: Specifications

Specifications

Model	WAP2000
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power over Ethernet), 802.1p (QoS priority), 802.1Q (VLAN), 802.1X (Security Authentication), 802.11i - Ready (Security WPA2), 802.11e - Ready (Wireless QoS), 802.11F (Wireless Roaming)
Ports	10BASE-T/100 BASE-TX Ethernet, 12 VDC Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, PoE, Wireless, Ethernet
Operating System	Linux

Setup/Config

WebUI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
-------	---

Management

SNMP Version	SNMP Version 1, 2c, 3
Event Logging	E-mail Notification Remote Syslog
Web F/W Upgrade	Firmware Upgradable Through Web-Browser
Diags: Flash, etc.	Flash, RAM, LAN, WLAN
DHCP	DHCP Client

Operating Modes

Access Point	Access Point Mode, point-to-point Bridge Mode, point-to-multipoint Bridge Mode, Repeater Mode
--------------	---

Wireless

Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 11g/OFDM
Channels	Operating Channels: 11 North America, 13 Most of Europe (ETSI and Japan)

# of Internal Ant.	None
# of External Ant.	2 (Omnidirectional) 3 dBi SMA detachable
Transmit Power	Transmit Power (Adjustable) @ Normal Temp Range: 11b - 18 dBm; 11g - 16 dBm
Antenna Gain	3 dBi
Receiver Sensitivity	11.g: 54Mbps@ -72dBm, 11.b: 11Mbps@ -85dBm

Security

WEP/WPA/WPA2	WEP 64bit/128 bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT
Access Control	Wireless Connection Control: MAC-Based
SSID Broadcast	SSID Broadcast Enable/Disable
802.1X	IEEE 802.1X support
Wireless Client Isolation	Wireless Client devices can be isolated from each other either within an SSID or between two SSIDs

Quality of Service

QoS	4 Queues WMM Wireless priority
General	Wireless roaming based on IAPP Load Balancing Auto-channel selection

Environmental

Dimensions	8.66" x 6.69" x 1.50" (220 x 170 x 38 mm)
Weight	1.69 lb (0.765 kg)
Power	12V 1A DC input and IEEE802.3af Compliant PoE Max Power Draw: 3.48W
Certification	FCC, ICES-003, CE
Operating Temp.	14 to 131°F (-10 to 55°C)
Storage Temp.	-22 to 158°F (-30 to 70°C)
Operating Humidity	10 to 90%, Noncondensing
Storage Humidity	5 to 95%, Noncondensing

Appendix E: Warranty Information

Limited Warranty

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

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

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

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

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

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

Appendix F: Regulatory Information

FCC Statement

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.

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

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

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 and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

Safety Notices

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.



WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Industry Canada Statement

This device complies with Industry Canada ICES-003 and RSS210 rules.

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 2dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

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

Avis d'Industrie Canada

Cet appareil est conforme aux normes NMB003 et RSS210 d'Industrie Canada.

L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes :

1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif. Le dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximum de 2 dBi. Les règlements d'Industrie Canada interdisent strictement l'utilisation d'antennes dont le gain est supérieur à cette limite. L'impédance requise de l'antenne est de 50 ohms.
Afin de réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon à ce que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

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

Ce matériel est conforme aux limites établies par IC en matière d'exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d'au moins 20 cm entre l'antenne et le corps de l'utilisateur.

L'émetteur ne doit pas être placé près d'une autre antenne ou d'un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Avis de non-responsabilité concernant les appareils sans fil


Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable.

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


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




English - Environmental Information for Customers in the European Union

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


Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ  върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.


Čeština (Czech) - Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

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


Dansk (Danish) - Miljøinformation for kunder i EU

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


Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union

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


Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidu asuvatele klientidele

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


Español (Spanish) - Información medioambiental para clientes de la Unión Europea

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


Ελληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

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


Français (French) - Informations environnementales pour les clients de l'Union européenne

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


Italiano (Italian) - Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

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


Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

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


Lietuvškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir  kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), 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 għex 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' għbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ għin 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.


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 rendszertől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőrendszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.


Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

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


Norsk (Norwegian) - Miljøinformasjon for kunder i EU

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


Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

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


Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo  no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das 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.


Română (Romanian) - Informații de mediu pentru clienții din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol  pe produs și/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obișnuit. Este responsabilitatea dvs. să cașiți acest produs și alte echipamente electrice și electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea și reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului și a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubritate sau magazinul de la care ați achiziționat produsul.


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 gospodinjstskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille

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

Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol  på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda samlingsplatser 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, avfallshantering eller butiken där du köpte produkten.



WEB: For additional information, please visit www.linksys.com

Appendix G: Contact Information

Linksys Contact Information	
Website	http://www.linksys.com
E-Mail	support@linksys.com
FTP Site	ftp.linksys.com
Advice Line	800-546-5797 (LINKSYS)
Support	800-326-7114
RMA (Return Merchandise Authorization)	949-823-3000
Fax	949-823-3002



NOTE: Details on warranty and RMA issues can be found in the Warranty and Regulatory Information section of this Guide.
