

# Wireless-N ADSL2+ Gateway



# About This Guide

---

## Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. 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.

<b>Chapter 1: Product Overview</b>	<b>4</b>
LEDs . . . . .	4
Back Panel . . . . .	4
<b>Chapter 2: Wireless Security Checklist</b>	<b>5</b>
General Network Security Guidelines . . . . .	5
Additional Security Tips . . . . .	5
<b>Chapter 3: Installation</b>	<b>6</b>
Connection . . . . .	6
Setup . . . . .	6
<b>Chapter 4: Advanced Configuration</b>	<b>7</b>
Setup > Basic Setup . . . . .	7
Setup > DDNS. . . . .	.11
Setup > MAC Address Clone. . . . .	.12
Setup > Advanced Routing . . . . .	.12
Wireless > Wireless Security . . . . .	.14
Wireless > Wireless Mac Filter . . . . .	.16
Wireless > Advanced Wireless Settings . . . . .	.17
Security > Firewall . . . . .	.18
Security > VPN Passthrough. . . . .	.18
Security > VPN . . . . .	.19
Access Restrictions > Internet Access Policy. . . . .	.21
Applications and Gaming > Single Port Forwarding. . . . .	.22
Applications and Gaming > Port Range Forwarding . . . . .	.23
Applications & Gaming > Port Range Triggering . . . . .	.23
Applications and Gaming > DMZ . . . . .	.24
Applications and Gaming > QoS . . . . .	.24
Administration > Management. . . . .	.26
Administration > Diagnostics . . . . .	.27
Administration > Backup & Restore . . . . .	.28
Administration > Factory Defaults . . . . .	.28
Administration > Firmware Upgrade . . . . .	.29
Status > Gateway. . . . .	.29
Status > Local Network. . . . .	.29
Status > Wireless . . . . .	.30
Status > DSL Connection. . . . .	.30
<b>Appendix A: Troubleshooting</b>	<b>32</b>
<b>Appendix B: Specifications</b>	<b>33</b>
<b>Appendix C: Warranty Information</b>	<b>34</b>
<b>Appendix D: Regulatory Information</b>	<b>35</b>

FCC Statement . . . . .	.35
Safety Notices. . . . .	.35
Industry Canada Statement . . . . .	.35
Avis d'Industrie Canada. . . . .	.35
Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive) . . . . .	.36
CE Marking . . . . .	.37
National Restrictions . . . . .	.37
Product Usage Restrictions . . . . .	.38
Technical Documents on <a href="http://www.linksys.com/international">www.linksys.com/international</a> . . . . .	.38
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) . . . . .	.39


# Chapter 1: Product Overview


Thank you for choosing the Linksys Wireless-N ADSL2+ Gateway. The Gateway lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the Gateway to share resources such as computers, printers and files. A variety of security features help to protect your data and your privacy while online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall and NAT technology. Configuring the Gateway is easy using the provided browser-based utility.


## LEDs




 **Power** (Green) The Power LED lights up and stays on while the Gateway is powered on.

 **Ethernet 1-4** (Green) These numbered LEDs, corresponding with the numbered ports on the Gateway's back panel, serve two purposes. If the LED is continuously lit, the Gateway is successfully connected to a device through that port. It flashes to indicate network activity over that port.

 **DSL** (Green) The DSL LED lights up whenever there is a successful DSL connection. The LED flashes while the Gateway is establishing the ADSL connection.


 **Internet** (Green) The Internet LED lights up and stays on when there is a connection made through the Internet port. It flashes to indicate network activity over the Internet port.


 **Wireless** (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Gateway is actively sending or receiving data over the network.


 **Security** (Green) The Security LED indicates when wireless security is enabled.


## Back Panel



 **DSL** The Internet port connects to the ADSL line.

 **Ethernet 1, 2, 3, 4** These Ethernet ports (1, 2, 3, 4) connect the Gateway to wired computers and other Ethernet network devices.

 **Reset** There are two ways to reset the Gateway's factory defaults. Either press and hold the Reset button for approximately five seconds, or restore the defaults from the *Administration > Factory Defaults* screen of the Gateway's web-based utility.

 **Power** The Power port is where you will connect the power adapter.

## Chapter 2: 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, routers, and gateways, 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 and gateways 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.

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.



**WEB:** For more information on wireless security, visit [www.linksys.com/security](http://www.linksys.com/security)

## Chapter 3: Installation

Linksys strongly recommends that you run the Setup CD-ROM. If you have problems running the Setup CD-ROM, use this chapter.

### Connection

1. Make sure that all the devices that you are working with are powered down, including your computer(s) and the Gateway. If you have a modem connected to your network, disconnect it. Your Gateway replaces your modem.
2. Connect one end of the provided phone cable to the wall jack with ADSL service.
3. Connect the other end of the phone cable to the DSL port on the back of the Gateway.



Connect the DSL



**NOTE:** To avoid interference, you may need to place a microfilter or splitter between the phone cable and wall jack. Contact your ISP to determine if one is required. (UK residents need to connect the microfilter to the wall phone jack with ADSL service and then connect one end of the provided phone cable to the RJ-11 port on it.)

If you use ISDN, then you do not need a microfilter.

4. Connect one end of the provided Ethernet cable to your computer's Ethernet adapter. Connect the other end of the Ethernet cable to one of the Ethernet ports on the back of the Gateway.



Connect the Computer

5. Repeat steps 1-4 for every computer or device that you want to connect to the Gateway via Ethernet.

If you connect more than four computers to the Gateway, you also need to connect a switch to the Gateway.



**NOTE:** If your computer's Ethernet adapter is not set up, refer to the Ethernet adapter's documentation for more information.

6. Connect the power adapter to the Gateway's power port and the electrical outlet.



Connect the Power

7. Power on the Gateway.
8. Power on the computer that you want to use to configure the Gateway.



**NOTE:** If you have more than one phone and you experience static on the line after installing the Gateway, then you need to install an additional microfilter for each phone or fax that you use.

**Connection is complete.**

**Continue to the "Setup" section.**

### Setup

For setup, configure the Gateway to access the Internet through your ADSL Internet Service Provider (ISP). Use the setup information provided by your ISP.

Continue to "Chapter 4: Advanced Configuration", and complete the following sections:

- Setup > Basic Setup
- Wireless > Basic Wireless Settings
- Wireless > Wireless Security

After completing the setup, to test it, enter **www.linksys.com/registration** in the web browser's Address field, and press **Enter**.

**Installation is complete.**



## Chapter 4: Advanced Configuration

After setting up the Gateway with the Setup Wizard (located on the CD-ROM), the Gateway will be ready for use. However, if you'd like to change its advanced settings, use the Gateway's web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Gateway.

The web-based utility has these main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.



**NOTE:** When first installing the Gateway, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter.



**NOTE:** For New Zealand residents, refer to the note under RFC 2364 PPPoA.

### How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Gateway's default IP address, **192.168.1.1**, in the *Address* field. Then, press **Enter**.

A login screen appears. Use the default user name and password, **admin**, unless you have changed them during the Setup Wizard. (You can set a new user name and password from the Administration tab's *Management* screen.) Click **OK** to continue.



Login Screen

### Setup > Basic Setup

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



Setup > Basic Setup

### Internet Setup

The Internet Setup section configures the Gateway to your Internet connection. Most of this information can be obtained through your ISP.

#### Internet Connection Type

Select the appropriate encapsulation method from the drop-down menu. Each *Basic Setup* screen and available features will differ depending on which encapsulation method you select. These are the available methods:

- RFC 2364 PPPoA
- RFC 2516 PPPoE
- RFC 1483 Routed
- IPoA
- RFC 1483 Bridged
- Bridge Mode Only



## VC Settings

Configure your Virtual Circuit (VC) settings in this section.

**Multiplexing** Select **LLC** or **VC**, depending on your ISP.

**QoS Type** Select from the drop-down menu: **CBR** (Continuous Bit Rate) to specify fixed bandwidth for voice or data traffic; **UBR** (Unspecific Bit Rate) for application that are not time-sensitive, such as e-mail; or **VBR** (Variable Bit Rate) for bursty traffic and bandwidth-sharing with other applications.

**PCR** For the Peak Cell Rate (PCR), divide the DSL line rate by 424 to get the maximum rate the sender can send cells. Enter the rate in the field (if required by your service provider).

**SCR** The Sustain Cell Rate (SCR) sets the average cell rate that can be transmitted. The SCR value is normally less than the PCR value. Enter the rate in the field (if required by your service provider).

**Autodetect** Select **Enable** to have the settings automatically entered, or select **Disable** to enter the values manually.

**Virtual Circuit** These fields consist of two items: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier). Enter the settings provided by your ISP.

**DSL Modulation** Select the appropriate mode: **MultiMode**, **T1.413**, **G.dmt**, **G.lite**, **ADSL2**, **ADSL2+**, **ADSL2 L**, **ADSL2 M**, or **ADSL2+ M**. Contact your ISP if you are not sure which mode to use.

Follow the instructions for your type of encapsulation.

## RFC 2364 PPPoA

Some DSL-based ISPs use PPPoA (Point-to-Point Protocol over ATM) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoA. If they do, you will have to enable PPPoA.

Internet Connection Type > RFC 2364 PPPoA

## PPPoA Settings

**User Name and Password** Enter the User Name and Password provided by your ISP.

**Connect on Demand: Max Idle Time** You can configure the Gateway to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

**Keep Alive: Redial Period** If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.



**NOTE:** For New Zealand, follow these instructions:

1. Select **RFC 2364 PPPoA** from the Encapsulation drop-down menu.
2. For the Virtual Circuit ID, enter **0** for the VPI and **100** for the VCI.
3. Select **VC** for Multiplexing.
4. Select **Multimode** from the DSL Modulation drop-down menu.
5. Obtain the User Name and Password details from your ISP.

## RFC 2516 PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

Internet Connection Type &gt; RFC 2516 PPPoE

### PPPoE Settings

**User Name and Password** Enter the User Name and Password provided by your ISP.

**Connect on Demand: Max Idle Time** You can configure the Gateway to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Gateway to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

**Keep Alive: Redial Period** If you select this option, the Gateway will periodically check your Internet connection. If you are disconnected, then the Gateway will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Gateway to check the Internet connection. The default Redial Period is **30** seconds.

### RFC 1483 Routed

If you are required to use RFC 1483 Routed, then select **RFC 1483 Routed**.

Internet Connection Type &gt; RFC 1483 Routed

### IP Settings

Your ISP provides these settings.

**Internet IP Address** Enter the Gateway's IP address, as seen from the Internet.

**Subnet Mask** Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP).

**Default Gateway** Enter the IP address of the ISP server.

**Primary (Required) and Secondary (Optional) DNS** Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required.

### IPoA

If you are required to use IPoA (IP over ATM), then select **IPoA**.

Internet Connection Type &gt; IPoA

### IP Settings

Your ISP provides these settings.

**Internet IP Address** Enter the Gateway's IP address, as seen from the Internet.

**Subnet Mask** Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP).

**Default Gateway** Enter the IP address of the ISP server.

**Primary (Required) and Secondary (Optional) DNS** Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required.

### RFC 1483 Bridged

If you are required to use RFC 1483 Bridged, then select **RFC 1483 Bridged**.

The screenshot shows the 'Internet Connection Type' configuration window. The 'VC Settings' section is active, showing 'Encapsulation' set to 'RFC 1483 Bridged'. Other settings include 'Multiplexing' (LLC selected), 'Qos Type' (UBR), 'Pcr Rate' and 'Scr Rate' (both 0 cps), 'Autodetect' (Disable selected), 'Virtual Circuit' (1), and 'DSL Modulation' (Multimode). The 'IP Settings' section is also visible, with 'Obtain an IP Address Automatically' selected.

Internet Connection Type &gt; RFC 1483 Bridged

### IP Settings

Select **Obtain an IP Address Automatically** if your ISP says you are connecting through a dynamic IP address.

If you are required to use a permanent (static) IP address to connect to the Internet, then select **Use the following IP Address**. Your ISP provides the settings needed for the following fields:

**Internet IP Address** Enter the Gateway's IP address, as seen from the Internet.

**Subnet Mask** Enter the Gateway's Subnet Mask, as seen from the Internet (including your ISP).

**Default Gateway** Enter the IP address of the ISP server.

**Primary (Required) and Secondary (Optional) DNS** Enter the DNS (Domain Name System) server IP address(es) provided by your ISP. At least one is required.

### Bridge Mode Only

If you are using your Gateway as a bridge, which makes the Gateway act like a stand-alone modem, select **Bridge Mode Only**. All NAT and routing settings are disabled in this mode.

The screenshot shows the 'Internet Connection Type' configuration window with 'Bridge Mode Only' selected. The 'VC Settings' section is active, showing 'Encapsulation' set to 'Bridge Mode Only'. Other settings include 'Multiplexing' (LLC selected), 'Qos Type' (UBR), 'Pcr Rate' and 'Scr Rate' (both 0 cps), 'Autodetect' (Disable selected), 'Virtual Circuit' (1), and 'DSL Modulation' (Multimode).

Internet Connection Type &gt; Bridge Mode Only

### Optional Settings

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.

Wireless-N ADSL2+ Gateway

The screenshot shows the 'Optional Settings' configuration window. It includes fields for 'Host Name', 'Domain Name', 'MTU' (set to 'Auto'), and 'Size' (set to '1500').

Optional Settings

**Host Name and Domain Name** These fields allow you to supply a host and domain name for the Gateway. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

**MTU** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select **Manual** if you want to manually enter the largest packet size that is transmitted. To have the Gateway select the best MTU for your Internet connection, keep the default, **Auto**.

**Size** When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default, MTU is configured automatically.

### Network Setup

The Network Setup section changes the settings on the network connected to the Gateway's Ethernet ports. Wireless setup is performed through the Wireless tab.

### Gateway IP

The values for the Gateway's Local IP Address and Subnet Mask are shown here. In most cases, keeping the default values will work.

The screenshot shows the 'Gateway IP' configuration window. The 'Local IP Address' is set to '192.168.1.1' and the 'Subnet Mask' is set to '255.255.255.0'.

Gateway IP

**Local IP Address** The default value is **192.168.1.1**.

**Subnet Mask** The default value is **255.255.255.0**.

### Network Address Server Settings (DHCP)

The settings allow you to configure the Gateway's Dynamic Host Configuration Protocol (DHCP) server function. The Gateway can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Gateway's DHCP server option, make sure there is no other DHCP server on your network.

Network Address Server Settings (DHCP)

**DHCP Server** A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, Linksys recommends that you keep the default, **Enable**. You can also use the Gateway in DHCP Relay mode. (This setting is not available for all encapsulation types.)

**DHCP Server** If you enable the DHCP Relay mode for the DHCP Server setting, enter the IP address for the DHCP relay server in the fields provided. (This setting is not available for all encapsulation types.)

**Starting IP Address** Enter a value for the DHCP server to start with when issuing IP addresses. Because the Gateway's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default is **192.168.1.100**.

**Maximum Number of DHCP Users** Enter the maximum number of users (network devices) that can obtain an IP address. The number will vary depending on the starting IP address entered and cannot be greater than 253. The default is **50**.

**Client Lease Time** The Client Lease Time is the amount of time a network device will be allowed connection to the Gateway with its current dynamic IP address. Enter the number of minutes that the device will be "leased" this dynamic IP address. After the time is up, the device will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

**Static DNS 1-3** The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. At least one DNS server IP address is provided by your ISP. You can enter up to three DNS server IP addresses here. The Gateway will use these for quicker access to functioning DNS servers.

**WINS** The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

## Time Settings

**Time Zone** Select the time zone in which your network functions.

**Automatically adjust clock for daylight saving changes** Select this option if you want the Gateway to automatically adjust for daylight saving time.

Time Settings and Language

## Language

**Language** To use a different language, select one from the drop down menu. The language of the web-based utility will change five seconds after you select another language.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Setup > DDNS

The Gateway offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Gateway.

Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, [www.dyndns.org](http://www.dyndns.org) or [www.TZO.com](http://www.TZO.com). If you do not want to use this feature, keep the default, **Disabled**.

## DDNS

### DDNS Service

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the *DDNS* screen will vary, depending on which DDNS service provider you use.

### DynDNS.org

Setup &gt; DDNS &gt; DynDNS

**User Name** Enter the User Name for your account.



**Password** Enter the Password for your account.

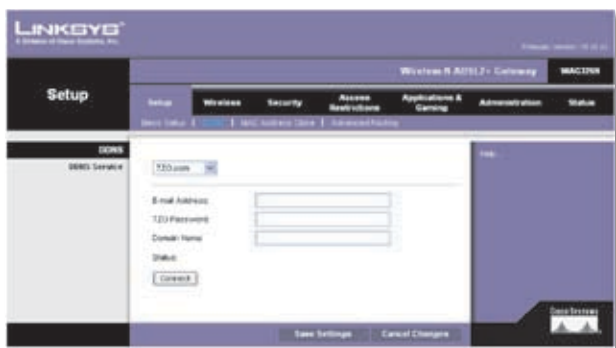
**Host Name** Enter the DDNS URL assigned by the service.

**Status** The status of the DDNS service connection is displayed.

**Connect** To manually trigger an update, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

TZO.com



Setup > DDNS > TZO

**E-mail Address** Enter the E-mail Address for your account.

**TZO Password** Enter the Password for your account.

**Domain Name** Enter the DDNS URL assigned by the service.

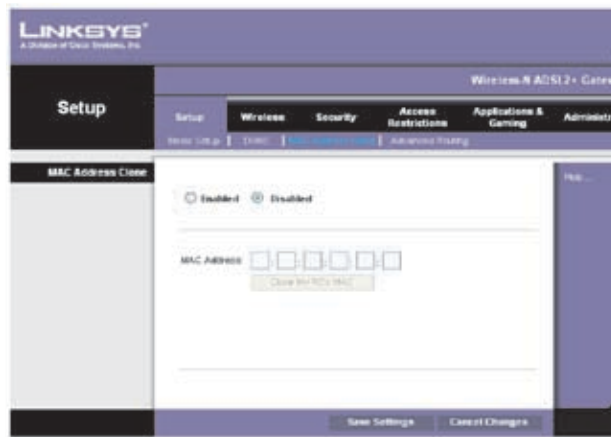
**Status** The status of the DDNS service connection is displayed here.

**Connect** To manually trigger an update, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Setup > MAC Address Clone

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Gateway with the MAC Address Clone feature.



Setup > MAC Address Clone

**Enable/Disable** To have the MAC Address cloned, click the radio button beside Enable.

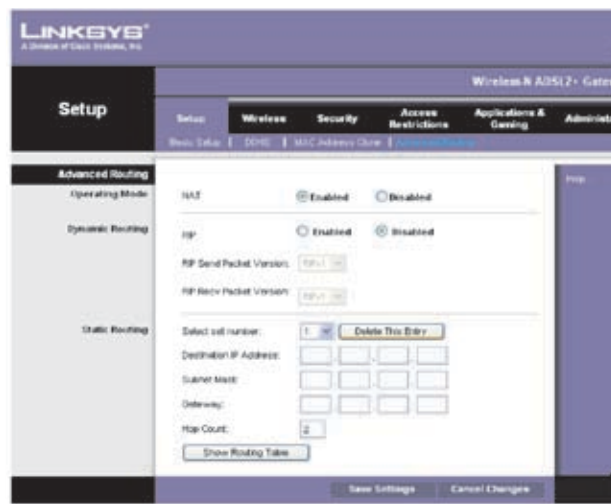
**MAC Address.** Enter the MAC Address registered with your ISP here.

**Clone My PC's MAC Address** Clicking this button will clone the MAC address.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Setup > Advanced Routing

This screen is used to set up the Gateway's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.



Setup > Advanced Routing

## Advanced Routing

### NAT

**Enabled/Disabled** If this Gateway is hosting your network's connection to the Internet, keep the default, **Enabled**. If another gateway or router exists on your network, select **Disabled**.

### Dynamic Routing

**RIP** This feature enables the Gateway to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Gateway determines the network packets' route based on the fewest number of hops between the source and the destination. Select **Enabled** to use the Dynamic Routing feature. Otherwise, keep the default, **Disabled**.

**RIP Version** Select the appropriate protocol version, **RIP1** or **RIP2**.

### Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.

**Select set number** To set up a static route between the Gateway and another network, select a number from the drop-down list. The Gateway supports up to 20 static route entries. Click **Delete This Entry** to delete a static route.

**Destination IP Address** The Destination IP Address is the IP address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0.

**Subnet Mask** The Subnet Mask determines which portion of a Destination IP Address is the network portion, and which portion is the host portion.

**Gateway** This is the IP address of the gateway device that allows for contact between the Gateway and the remote network or host.

**Hop Count** This is the number of hops to each node until the destination is reached (16 hops maximum). Enter the appropriate Hop Count.

Click **Show Routing Table** to view the static routes you have already set up.



Advanced Routing > Routing Table

### Routing Table

For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Wireless > Basic Wireless Settings

The basic settings for wireless networking are set on this screen.



Wireless > Basic Wireless Settings

This screen allows you to choose your wireless network mode and wireless security.

### Wireless Network

**Wireless Network Mode** Select the wireless standards running on your network. If you have Wireless-G and Wireless-B devices in your network, keep the default, **Mixed**. If you do not have any wireless devices, select **Disabled**.

**Wireless Network Name (SSID)** The network name is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Linksys recommends that you change the default, **linksys**, to a unique name of your choice.

**Radio Band** For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, **Wide - 40MHz Channel**. For Wireless-G and

Wireless-B networking only, select Standard - 20MHz Channel.



**NOTE:** If you select Wide - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel). This will enhance Wireless-N performance..

**Wide Channel** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu.

**Standard Channel** Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide - 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N. If you are not sure which channel to select, do not make any changes.

**Wireless SSID Broadcast** When wireless devices survey the local area for wireless networks to associate with, they will detect the wireless network name or SSID broadcast by the Gateway. If you want to broadcast the Gateway's SSID, keep the default, **Enable**. Otherwise, select **Disable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Wireless > Wireless Security

The *Wireless Security* screen configures the security of your wireless network(s). The following wireless security mode options are supported by the Gateway: WPA2-Personal, WPA Personal, WPA2-Enterprise, WPA Enterprise, RADIUS, and WEP. WPA (Wi-Fi Protected Access), is a security standard stronger than WEP (Wired Equivalent Privacy) encryption. WPA2 is a more advanced, more secure version of WPA. WPA-Enterprise, WPA2-Enterprise, and RADIUS use a RADIUS (Remote Authentication Dial-In User Service) server for authentication. For detailed instructions on configuring wireless security for the Gateway, refer to "Chapter 2: Wireless Security".

### Wireless Security

**Security Mode** Select the security method for your wireless network. Proceed to the appropriate instructions. If you do not want to use wireless security, keep the default, **Disabled**.



**NOTE:** If you are using wireless security, remember that each device in your wireless network **MUST** use the same security method and settings, or else the wireless devices cannot communicate.

### WPA2-Personal (Recommended)



Security Mode > WPA2-Personal

**Encryption** The method is **TKIP** or **AES**.

**Passphrase** Enter a Passphrase (also called a WPA shared key) of 8-63 characters.

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

**WPA-Personal (May affect wireless performance. WPA2 recommended)**



Security Mode > WPA-Personal

**Encryption** The method is **TKIP** or **AES**.

**Passphrase** Enter a Passphrase (also called a WPA shared key) of 8-63 characters.

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

### WPA2-Enterprise

WPA2-Enterprise features WPA2 used with a RADIUS server. (This method should only be used when the device is connected to a RADIUS server.)





Security Mode &gt; WPA2-Enterprise

**Encryption** The method is **TKIP** or **AES**.

**RADIUS Server** Enter the IP address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server.

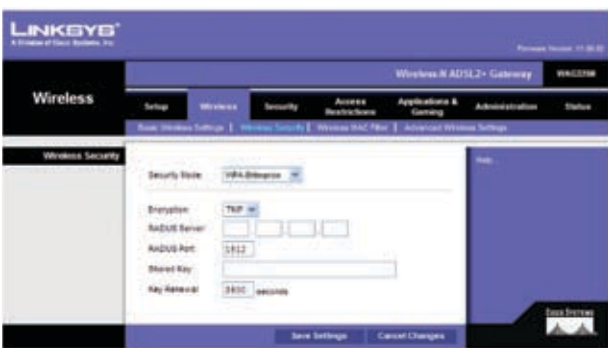
**Shared Key** Enter the key shared between the device and its RADIUS server.

**Key Renewal.** Enter the Key Renewal period, which tells the device how often it should change the dynamic encryption keys. WPA2-Enterprise.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

**WPA-Enterprise (May affect wireless performance. WPA2 recommended)**

WPA-Enterprise features WPA used with a RADIUS server. (This method should only be used when the device is connected to a RADIUS server.)



Security Mode &gt; WPA-Enterprise

**Encryption.** The method is **TKIP** or **AES**.

**RADIUS Server.** Enter the IP address of the RADIUS server.

**RADIUS Port.** Enter the port number of the RADIUS server.

**Shared Key** Enter the key shared between the device and its RADIUS server.

**Key Renewal** Enter the Key Renewal period, which tells the device how often it should change the dynamic encryption keys.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

**RADIUS (May affect wireless performance. WPA2 recommended)**

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the device.)



Security Mode &gt; RADIUS

**RADIUS Server** Enter the IP address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server.

**Shared Key** Enter the key shared between the device and its RADIUS server.

**Encryption.** Select the appropriate level of encryption, 40/64-bit (10 hex digits) or 104/128-bit (26 hex digits). A higher level of encryption is more secure.

**Passphrase** Instead of manually entering WEP keys, you can enter a Passphrase. It is case-sensitive and should not be longer than 32 alphanumeric characters. (This Passphrase function is compatible with Linksys wireless products only and cannot be used with Windows XP Zero Configuration. If you want to communicate with non-Linksys wireless products or Windows XP Zero Configuration, make a note of the WEP keys generated, and enter the appropriate one manually in the wireless computer or client.) If you want to use a Passphrase, then enter it in the Passphrase field and click the Generate button.

**Keys 1-4.** If you are not using a Passphrase, then manually enter a set of values. (Do not leave a key field blank, and do not enter all zeroes; they are not valid key values.) If you are using 40/64-bit WEP encryption, the key must be exactly 10 hexadecimal characters in length. If you are using 104/128-bit WEP encryption, the key must be exactly

26 hexadecimal characters in length. Valid hexadecimal characters are "0"-"9" and "A"-"F".

**TX Key.** To indicate which WEP key to use, select a default Transmit (TX) Key number.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

**WEP (May affect wireless performance. WPA2 recommended)**



Security Mode > WEP

**Encryption** Select a level of WEP encryption, **64-bit** or **128-bit**.

**Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.



**NOTE:** The WEP Passphrase is compatible with Linksys wireless products only. If you use non-Linksys products, manually enter the appropriate WEP key on those devices.

**WEP Key 1-4** If you did not enter a Passphrase, enter the WEP key(s) manually.

**TX Key** Select which TX (Transmit) Key to use. The default is **1**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

### Wireless > Wireless Mac Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.



Wireless > Wireless MAC Filter

### Wireless MAC Filter

To filter wireless users by MAC Address, either permitting or blocking access, click **Enabled**. If you do not wish to filter users by MAC Address, select **Disabled**.

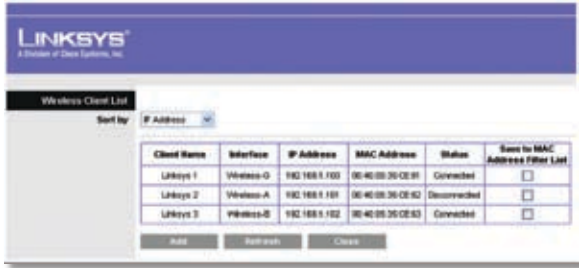
#### Access Restrictions

**Block.** Click this button to block wireless access from the devices listed on this screen.

**Permit.** Click this button to allow wireless access by the devices listed on this screen.

#### MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP address, MAC Address, and Status. Click the **Add to MAC Filter List** checkbox for any device you want to add to the MAC Address Filter List. Then click the **Add** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the Wireless MAC Filter screen, click the **Close** button.



**MAC 01-50** Enter the MAC addresses of the devices whose wireless access you want to block or allow

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Wireless > Advanced Wireless Settings

This *Advanced Wireless Settings* screen is used to set up the Gateway's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



Wireless > Advanced Wireless Settings

### Advanced Wireless

**AP Isolation.** This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Gateway but not with each other. To use this function, click Enabled. AP Isolation is disabled by default.

**Authentication Type** The default is **Auto**, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Select **Shared Key** to only use Shared Key authentication.

**Basic Rate** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the device

can transmit. The device will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The device will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the device can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are 1-2Mbps, for use with older wireless technology, and All, when the device can transmit at all wireless rates.

**Transmission Rate** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device and a wireless client. The default setting is Auto.

**N Transmission Rate** The rate of data transmission should be set depending on the speed of your Wireless-N networking. You can select from a range of transmission speeds, or you can select Auto to have the device automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the device and a wireless client. The default setting is Auto.

**CTS Protection Mode.** CTS (Clear-To-Send) Protection Mode's default setting is Disabled. Select **Auto** so the device will automatically use CTS Protection Mode when your Wireless-N and Wireless-G products are experiencing severe problems and are not able to transmit to the device in an environment with heavy 802.11b traffic. This function boosts the device's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance.

**Beacon Interval** Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Gateway to synchronize the wireless network(s). The default value is **100**.

**DTIM Interval** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Gateway has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

**Fragmentation Threshold** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor

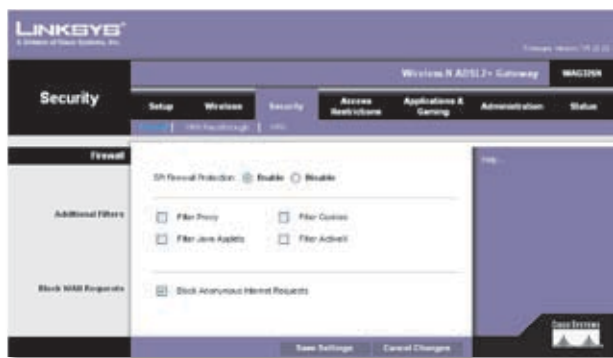
reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

**RTS Threshold** Should you encounter inconsistent data flow, only minor reduction of the default, **2346**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Gateway sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2346**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Security > Firewall

The *Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Gateway's local network.



Security > Firewall

## Firewall

**SPI Firewall Protection** To use firewall protection, keep the default selection, **Enable**. To turn off firewall protection, select **Disable**.

## Filters

**Filter Proxy** Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select **Filter Proxy** to enable proxy filtering. Deselect the feature to allow proxy access.

**Filter Java Applets** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. Select **Filter Java Applets** to enable Java filtering. Deselect the feature to allow Java usage.

**Filter Cookies** A cookie is data stored on your computer and used by Internet sites when you interact with them. Select **Filter Cookies** to filter cookies. Deselect the feature to allow cookie usage.

**Filter ActiveX** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select **Filter ActiveX** to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.

## Block WAN Requests

**Block Anonymous Internet Requests** This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Security > VPN Passthrough

The *VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Gateway's firewall.



Security > VPN Passthrough

## VPN Passthrough

**IPSec Passthrough** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Gateway, keep the default, **Enable**.

**PPTP Passthrough** Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Gateway, keep the default, **Enable**.

**L2TP Passthrough** Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Gateway, keep the default, **Enable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.



## Security > VPN



Security > VPN Tunnel

### Establishing a Tunnel

The Gateway creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure. To establish this tunnel, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. It is possible to create up to two simultaneous tunnels. To delete a tunnel, click the **Delete** button. To view a summary of that tunnel, click the **Summary** button.



VPN Summary

Then check the box next to **Enable** to enable the tunnel.

Once the tunnel is enabled, enter the name of the tunnel in the Tunnel Name field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

### Local Secure Group and Remote Secure Group

A Local Secure Group is a computer(s) on your network that can access the tunnel. A Remote Secure Group is a computer (s) on the remote end of the tunnel that can

access the tunnel. Under Local Secure Group, you may choose from Subnet and IP address. Under Remote Secure Group, you may choose from IP address, Subnet, and Any.

**Subnet** If you select Subnet (which is also the default), this will allow all computers on the local subnet to access the tunnel. When using the Subnet setting, the default values of 0 should remain in the last fields of the IP and Mask settings.

**IP Address** If you select IP Address, only the computer with the specific IP address that you enter will be able to access the tunnel.

**Any** If you select Any for the Remote Security Group, the local VPN Router will accept a request from any IP address. This setting should be chosen when the other endpoint is using DHCP or PPPoE on the Internet side.

### Remote Security Gateway

The Remote Security Gateway is the VPN device, such as a second VPN Router, on the remote end of the VPN tunnel. Under Remote Security Gateway, you have three options: IP address, FQDN, and Any. In this section, you can also set the levels and types of encryption and authentication.

**IP Address** If you select IP Address, enter the IP address of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP address correctly, or the connection cannot be made. Remember, this is NOT the IP address of the local VPN Router, but the IP address of the remote VPN Router or device with which you wish to communicate.

**FQDN (Fully Qualified Domain Name)** If you select FQDN, enter the FQDN of the VPN device at the other end of the tunnel. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. The FQDN is the host name and domain name for a specific computer on the Internet, for example, vpn.myvpnserver.com.

**Any** If you select Any for the Remote Security Gateway, the VPN device at the other end of the tunnel will accept a request from any IP address. The remote VPN device can be another VPN Router, a VPN Server, or a computer with VPN client software that supports IPSec. If the remote user has an unknown or dynamic IP address (such as a professional on the road or a telecommuter using DHCP or PPPoE), then Any should be selected.

**Encryption** Using encryption helps make your connection more secure. The encryption type used must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. You may choose not to encrypt by selecting Disable.

**Authentication** Authentication acts as another level of security. There are two types of authentication: MD5 and SHA (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to Disable authentication.

### Key Management

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a “key” to the encryption code. Under Key Management, you may choose automatic or manual key management.

#### Auto (IKE) Key Management

**Encryption** The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Notice that both sides must use the same method.

**Authentication** The Authentication method authenticates the Encapsulating Security Payload (ESP) packets. Select MD5 or SHA. Notice that both sides (VPN endpoints) must use the same method.

- MD5 - A one-way hashing algorithm that produces a 128-bit digest
- SHA - A one-way hashing algorithm that produces a 160-bit digest

**Perfect Forward Secrecy (PFS)** If PFS is enabled, IKE Phase 2 negotiation will generate new key material for IP traffic encryption and authentication. Note that both sides must have PFS enabled.

**Pre-Shared Key** IKE uses the Pre-Shared Key to authenticate the remote IKE peer. Both character and hexadecimal values are acceptable in this field, e.g., “My\_@123” or “0x4d795f40313233”. Note that both sides must use the same Pre-Shared Key.

**Key Lifetime** This field specifies the lifetime of the IKE generated key. If the time expires, a new key will be renegotiated automatically. The Key Lifetime may range from 300 to 100,000,000 seconds. The default lifetime is 3600 seconds.

#### Manual Key Management

**Encryption Algorithm** The Encryption method determines the length of the key used to encrypt/decrypt ESP packets. Notice that both sides must use the same method.

**Encryption Key** This field specifies a key used to encrypt and decrypt IP traffic. Both character and hexadecimal values are acceptable in this field. Note that both sides must use the same Encryption Key.

**Authentication Algorithm** The Authentication method authenticates the Encapsulating Security Payload (ESP)

packets. Select MD5 or SHA. Notice that both sides (VPN endpoints) must use the same method.

**MD5** A one-way hashing algorithm that produces a 128-bit digest

**SHA** A one-way hashing algorithm that produces a 160-bit digest

**Authentication Key** This field specifies a key used to authenticate IP traffic. Both character and hexadecimal values are acceptable in this field. Note that both sides must use the same Authentication Key.

**Inbound SPI/Outbound SPI** The Security Parameter Index (SPI) is carried in the ESP header. This enables the receiver to select the SA, under which a packet should be processed. The SPI is a 32-bit value. Both decimal and hexadecimal values are acceptable. e.g., “987654321” or “0x3ade68b1”. Each tunnel must have a unique Inbound SPI and Outbound SPI. No two tunnels share the same SPI. Note that the Inbound SPI must match the remote gateway’s Outbound SPI, and vice versa.

The Status field at the bottom of the screen will show when a tunnel is active.

To connect a VPN tunnel, click the **Connect** button. Click the **Disconnect** button to break a connection for the current VPN tunnel. The **View Log** button, when logging is enabled on the Log screen of the Administration tab, will show you VPN activity on a separate screen. The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used. For more advanced VPN options, click the **Advanced Settings** button to open the Advanced Settings screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Advanced VPN Tunnel Setup

Advanced VPN Tunnel Setup

From the Advanced Settings screen you can adjust the settings for specific VPN tunnels.

**Phase 1** Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.

**Operation Mode** There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device. If a user on one side of the tunnel is using a Unique Firewall Identifier, this should be entered under the User Name field.

**Encryption** 3DES is used to encrypt/decrypt ESP packets.

**Authentication** Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.

**Group.** There are two Diffie-Hellman Groups to choose from: 768-bit, 1024-bit, and 1536-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

**Key Lifetime** In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

## Phase 2

**Group** There are two Diffie-Hellman Groups to choose from: 768-bit, 1024-bit., and 1536-bit Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

**Key Lifetime** In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Access Restrictions > Internet Access Policy

The *Internet Access Policy* screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.



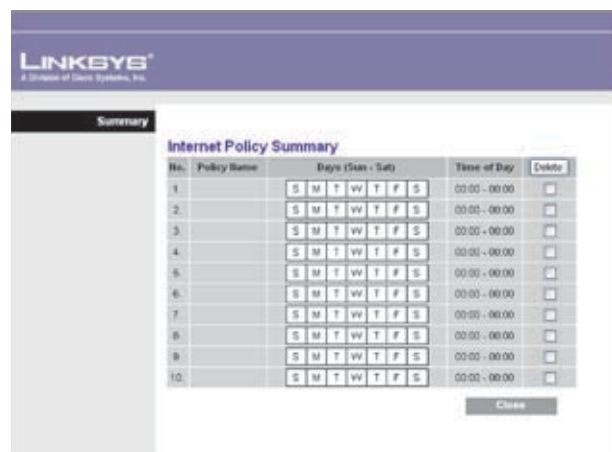
Access Restrictions > Internet Access Policy

## Internet Access Policy

**Internet Access Policy** Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click **Delete**. To view all the policies, click **Summary**.

### Summary

The policies are listed with the following information: No., Policy Name, Days, and Time of Day. To delete a policy, select **Delete**. To return to the *Internet Access Policy* screen, click **Close**.



Summary

**Status** Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select **Enable**.



To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time.

1. Select a number from the *Internet Access Policy* drop-down menu.
2. To enable this policy, select **Enable**.
3. Enter a Policy Name in the field provided.
4. Click **Edit List of PCs** to select which computers will be affected by the policy. The *Internet Access PC List* screen appears. You can select a computer by MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of computers. After making your changes, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Then click **Close**.

Internet Access PC List

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the computers you selected on the *Internet Access PC List* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. You can block websites with specific URL addresses. Enter each URL in a separate *Website Blocking by URL Address* field.
8. You can also block websites using specific keywords. Enter each keyword in a separate *Website Blocking by Keyword* field.

9. You can filter access to various services accessed over the Internet, such as FTP or telnet.

From the Blocked Services list, select the service you want to block. The port numbers and protocol for the selected service are automatically displayed.

10. If the service you want is not listed, select **User-Defined**. Enter its port numbers in the fields provided. Then select its protocol: **ICMP**, **TCP**, **UDP**, or **TCP & UDP** from the drop-down menu.
11. Click **Save Settings** to save the policy's settings. To cancel the policy's settings, click **Cancel Changes**.

## Applications and Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for common applications.

When users send these types of requests to your network via the Internet, the Gateway will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers.

Applications and Gaming > Single Port Forwarding

### Single Port Forwarding

To forward a port, enter the information on each line for the criteria required.

**Application** Enter the name you wish to give the application. Each name can be up to 12 characters.

**External and Internal Port** Enter the external and internal port numbers.

**Protocol** Select the protocol used for this application, either **TCP** or **UDP**.

**IP Address** For each application, enter the IP address of the computer that should receive the requests.

**Enabled** For each application, select **Enabled** to enable port forwarding.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Applications and Gaming > Port Range Forwarding

The *Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the Gateway will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers.

If you need to forward all ports to one computer, click the **DMZ** tab.



Applications and Gaming > Port Range Forwarding

### Port Range Forwarding

To forward a port range, enter the information on each line for the criteria required.

**Application** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

**Port Range Start and End** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.

**Protocol** Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

Wireless-N ADSL2+ Gateway

**IP Address** For each application, enter the IP address of the computer running the specific application.

**Enable** Select **Enable** to enable port forwarding for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Applications & Gaming > Port Range Triggering

The *Port Range Triggering* screen allows the Gateway to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Gateway, so that when the requested data returns through the Gateway, the data is pulled back to the proper computer by way of IP address and port mapping rules.



Applications and Gaming > Port Range Triggering

### Port Range Triggering

To trigger a port range, enter the information on each line for the criteria required.

**Application Name** Enter the application name of the trigger.

**Triggered Range Start Port and End Port** For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

**Forwarded Range Start Port and End Port** For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

**Enabled** Select **Enabled** to enable port triggering for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Applications and Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.



Applications and Gaming > DMZ

### DMZ

Any computer whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

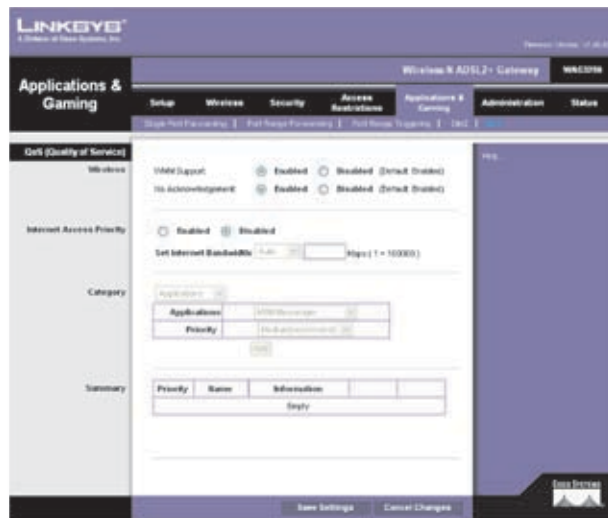
**DMZ Hosting** To disable DMZ hosting, keep the default, **Disable**. To expose one PC, select **Enable**. Then configure the following setting:

**DMZ Host IP Address** Enter the IP address of the computer.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Applications and Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.



Applications and Gaming > QoS

### Wireless

The Gateway features Wi-Fi Multimedia (WMM™) Support. The No Acknowledgement feature is available only when the WMM Support feature is enabled.

**WMM Support** Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. If you have other devices on your network that support WMM, keep the default, Enabled. Otherwise, select **Disabled**.

**No ACK** If you want to disable the Gateway's Acknowledgement feature, so the Gateway will not re-send data if an error occurs, then keep the default, Enabled. Otherwise, select **Disabled**.

### Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels priority: High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

**Enabled/Disabled** To use the QoS policies you have set, select **Enabled**. Otherwise, select **Disabled**.

### Category

The following categories are available: Applications, Online Games, MAC Address, Ethernet Port, or Voice Device. Proceed to the instructions for your selection.

## Applications

**Applications** Select the appropriate application. If you select Add a New Application, follow the Add a New Application instructions.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### Add a New Application

The dialog box shows the 'Applications' dropdown set to 'Online Game', 'Select a Game' dropdown set to 'Counter Strike', and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

Online Game

The dialog box shows the 'Applications' dropdown set to 'MSN Messenger' and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

MSN Messenger

The dialog box shows the 'Applications' dropdown set to 'YAHOO Messenger' and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

YAHOO Messenger

The dialog box shows the 'Applications' dropdown set to 'Skype' and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

Skype

The dialog box shows the 'Applications' dropdown set to 'Voice Device', 'Enter a Name' field empty, 'MAC Address' field with '00:00:00:00:00:00', and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

Voice Device

The dialog box shows the 'Applications' dropdown set to 'Add a New Application', 'Enter a Name' field with 'linksys', 'Category' dropdown set to 'Port Range', 'Port Range' field with '93' and '95', and 'Priority' dropdown set to 'Low'. An 'Add' button is at the bottom.

Add a New Application (Port Range)

The dialog box shows the 'Applications' dropdown set to 'Add a New Application', 'Enter a Name' field empty, 'Category' dropdown set to 'MAC Address', 'MAC Address' field with '00:00:00:00:00:00', and 'Priority' dropdown set to 'Medium'. An 'Add' button is at the bottom.

Add a New Application (MAC Address)

**Enter a Name** Enter any name to indicate the name of the entry.

**Port Range** Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

Select the protocol **TCP** or **UDP**, or select **Both**.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### Online Games

**Games** Select the appropriate game.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### MAC Address

**Enter a Name** Enter a name for your device.

**MAC Address** Enter the MAC address of your device.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### Ethernet Port

**Ethernet** Select the appropriate Ethernet port.

**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### Voice Device

**Enter a Name** Enter a name for your voice device.

**MAC Address** Enter the MAC address of your voice device.



**Priority** Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click the **Add** button to save your changes. Your new entry will appear in the Summary list.

### Summary

This lists the QoS entries you have created for your applications and devices.

**Priority** This displays the bandwidth priority of **High**, **Medium**, **Normal**, or **Low**.

**Name** This displays the application, device, or port name.

**Information** This displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

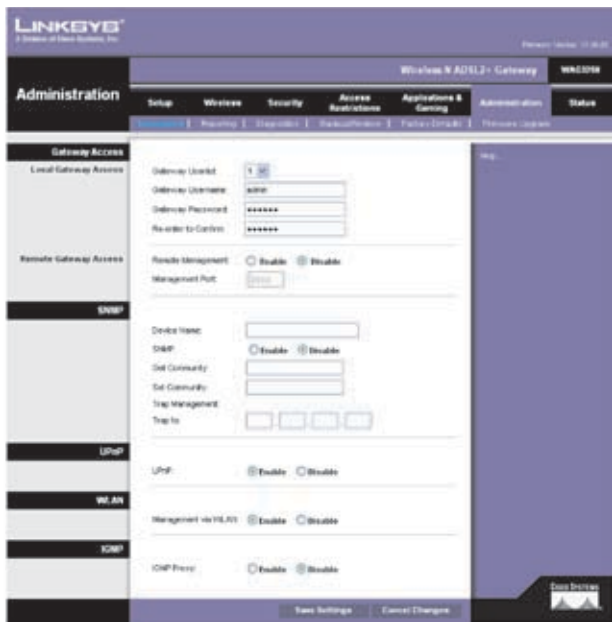
**Remove** Click this button to remove an entry.

**Edit** Click this button to make changes.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Administration > Management

The *Administration > Management* screen allows the network's administrator to manage specific Gateway functions for access and security.



Administration > Management

## Gateway Access

### Local Gateway Access

To ensure the Gateway's security, you will be asked for your User Name and password when you access the Gateway's web-based utility. The default User Name and password are **admin**.

**Gateway Userlist** Select the number of the user. The default is user **1**.

**Gateway User Name** Enter the default Gateway User Name, **admin**.

**Gateway Password** Linksys recommends that you change the default Gateway Password, **admin**, to one of your choice.

**Re-enter to Confirm** Enter the Gateway Password again to confirm.

For non-admin users, select a different user number, and then configure the Gateway User Name and Password settings.

### Remote Gateway Access

**Remote Management** To permit remote access of the Gateway, from outside the local network, select **Enable**. Otherwise, keep the default, **Disable**.

**Management Port** Enter the port number that will be open to outside access.



**NOTE:** When you are in a remote location and wish to manage the Gateway, enter **http://<Internet\_IP\_address>:port**. Enter the Gateway's specific Internet IP address in place of <Internet\_IP\_address>, and enter the Management Port number in place of the word port.

## SNMP

SNMP is a popular network monitoring and management protocol.

**Device Name** Enter the name of the Gateway.

**SNMP** To use SNMP, select **Enable**. Otherwise, select **Disable**.

**Get Community** Enter the password that allows read-only access to the Gateway's SNMP information.

**Set Community** Enter the password that allows read/write access to the Gateway's SNMP information.

**Trap Management: Trap to** Enter the IP address of the remote host computer that will receive the trap messages.

## UPnP

Universal Plug and Play (UPnP) allows Windows XP and Vista to automatically configure the Gateway for various Internet applications, such as gaming and videoconferencing.

**UPnP** If you want to use UPnP, keep the default, **Enable**. Otherwise, select **Disable**.

## WLAN

If you are using the Gateway in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Gateway's web-based utility.

**Management via WLAN** This feature allows the Gateway to be managed by a wireless computer on the local network when it logs into the Gateway's web-based utility. You will only be able to access the utility via a wired connection if you disable this feature. To allow wireless access to the utility, keep the default, **Enable**. Otherwise, select **Disable**.

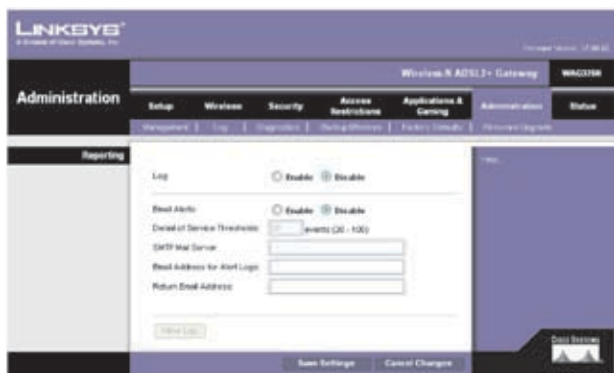
## IGMP

**IGMP Proxy** Internet Group Membership Protocol (IGMP) is a system to improve multicasting for wireless clients. This should be set to Enable if your clients support it; otherwise, select **Disable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Administration > Log

The Gateway can keep logs of traffic and events for your Internet connection.



Administration > Log

## Log

**Log** To disable the Log function, keep the default, **Disable**. To monitor traffic between the network and the Internet, select **Enable**. With logging enabled, you can choose to view temporary logs.

**E-Mail Alerts** To enable E-Mail Alerts, select **Enable**.

Wireless-N ADSL2+ Gateway

**Denial of Service Thresholds** Enter the number of Denial of Service attacks that will trigger an e-mail alert.

**SMTP Mail Server** Enter the IP address of the SMTP server.

**E-Mail Address for Alert Logs** Enter the e-mail address that will receive alert logs.

**Return E-Mail address** Enter the return address for the e-mail alerts. (This can be a dummy address.)

**View Log** To view the logs, click **View Log**.



View Log

## Log

**Type** Select from the following: **ALL**, **System Log**, **Access Log**, **Firewall Log**, or **VPN Log**.

Click **pageRefresh** to update the log. Click **Clear** to clear all the information that is displayed. Click **Previous Page** to view the previous page of information. Click **Next Page** to view the next page of information.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Administration > Diagnostics

The ping test allows you to check the connections of your network devices, including connection to the Internet.



Administration > Diagnostics

## Ping Test

### Ping Test Parameters

The ping test checks the status of a connection.

**Ping Target IP** Enter the IP address that you want to ping. This can be either a local (LAN) or Internet (WAN) IP address.

**Ping Size** Enter the packet size you want to use. The default is **60** bytes.

**Number of Pings** Enter how many times you want to ping. The default is **1**.

**Ping Interval** Enter the number of milliseconds between pings. The default is **1000** milliseconds.

**Ping Timeout** Enter the number of milliseconds before the ping test will time out. The default is **5000** milliseconds.

**Start Test** To run the test, click this button. The *Ping Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.



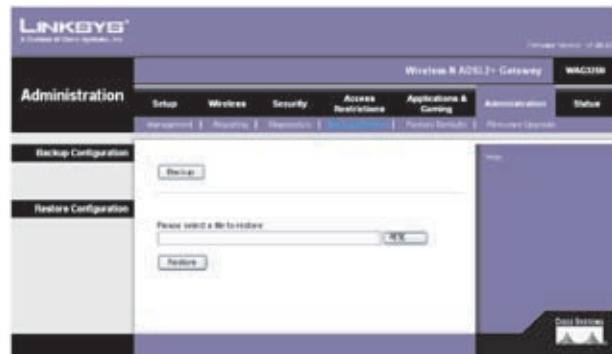
Diagnostics > Ping

**Ping Result** The results of the ping test are displayed.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

## Administration > Backup & Restore

The *Backup & Restore* screen allows you to back up or restore the Gateway's settings using a configuration file.



Administration > Backup & Restore

### Backup Configuration

**Backup** To save the Gateway's settings in a configuration file, click this button and follow the on-screen instructions.

### Restore Configuration

To use this option, you must have previously backed up its configuration settings.

**Please select a file to restore** Click the **Browse** button and select the Gateway's configuration file.

**Restore** To restore the Gateway's configuration settings, click this button and follow the on-screen instructions.

## Administration > Factory Defaults

The *Administration > Factory Defaults* screen allows you to restore the Gateway's configuration to its factory default settings.



Administration > Factory Defaults



**NOTE:** Restoring factory defaults deletes custom settings. Note your custom settings before restoring the factory defaults.

### Factory Defaults

**Restore Factory Defaults** To reset settings to the default values, click this button and follow the on-screen



instructions. Any custom Gateway settings you have saved will be lost when the default settings are restored.

## Administration > Firmware Upgrade

The *Firmware Upgrade* screen allows you to upgrade the Gateway's firmware. Do not upgrade the firmware unless you are experiencing problems with the Gateway or the new firmware has a feature you want to use.



Administration > Firmware Upgrade

## Firmware Upgrade

Before upgrading the firmware, download the Gateway's firmware upgrade file from the Linksys website, [www.linksys.com/international](http://www.linksys.com/international). Then extract the file.

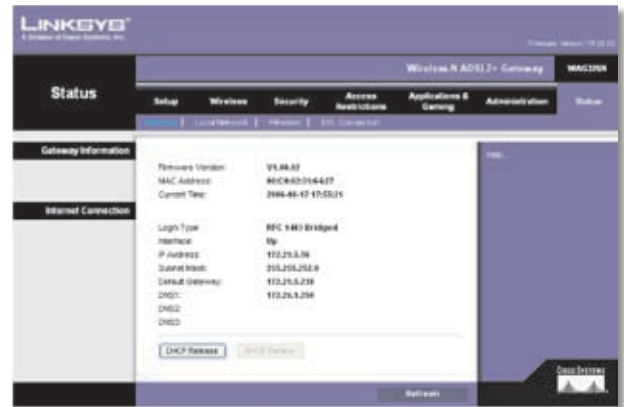
**Please Select a File to Upgrade** Click **Browse** and select the extracted firmware upgrade file.

**Start to Upgrade** After you have selected the appropriate file, click this button, and follow the on-screen instructions.

**Language** To use a different language, select one from the drop down menu. The language of the web-based utility will change five seconds after you select another language.

## Status > Gateway

The *Gateway* screen displays information about the Gateway and its current settings.



Status > Gateway

## Gateway Information

**Firmware Version** The version number of the Gateway's current firmware is displayed.

**MAC Address** The Gateway's MAC address, as seen by your ISP, is displayed.

**Current Time** The time set on the Gateway is displayed.

## Internet Connection

This section shows the current network information stored in the Gateway. The information varies depending on the Internet connection type selected on the *Basic Setup* screen.

Click **Refresh** to update the on-screen information.

## Status > Local Network

The *Local Network* screen displays information about the local, wired network.



Status > Local Network

## Local Network

**MAC Address** The MAC address of the Gateway's local, wired interface is displayed.

**IP Address** The Gateway's IP address, as it appears on your local network, is displayed.

**Subnet Mask** The Subnet Mask of the Gateway is displayed.

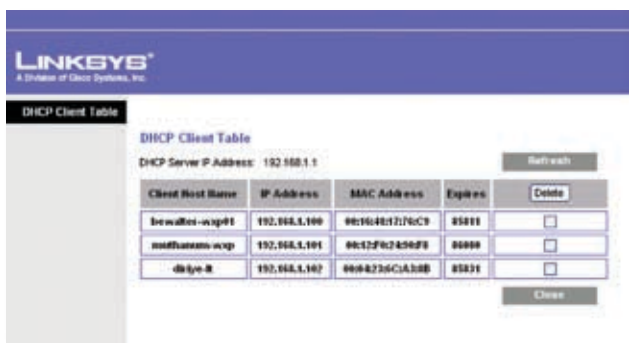
## DHCP Server

**DHCP Server** The status of the Gateway's DHCP server function is displayed.

**Start IP Address** For the range of IP addresses used by devices on your local network, the starting IP address is displayed.

**End IP Address** For the range of IP addresses used by devices on your local network, the ending IP address is displayed.

**DHCP Client Table** Click this button to view a list of devices that are using the Gateway as a DHCP server.



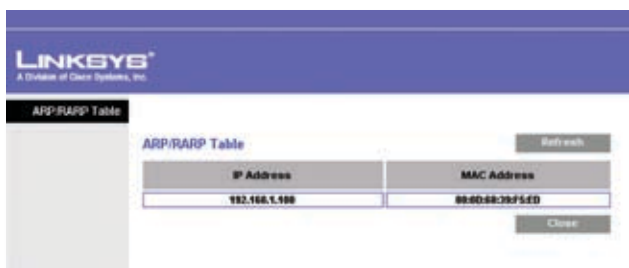
Client Host Name	IP Address	MAC Address	Expires	Delete
bevalles-wg01	192.168.1.100	0816481276C9	5500	<input type="checkbox"/>
madhams-wg01	192.168.1.101	0812767250F9	5500	<input type="checkbox"/>
dhcpe-R	192.168.1.102	0008236C1A5B	5500	<input type="checkbox"/>

DHCP Client Table

## DHCP Client Table

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Gateway. The list displays Client Host Name, IP Address, MAC Address, and Expires time (how much time is left for the current IP address). To remove a DHCP client, click **Delete**. To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the *Local Network* screen, click **Close**.

**ARP/RARP Table** Click this button to view the current IP and MAC addresses for the local network clients of the Gateway.



IP Address	MAC Address
192.168.1.100	08008236F5E0

ARP/RARP Table

## ARP/RARP Table

An ARP request is a request sent by the Gateway asking local network devices with IP addresses for their MAC addresses, so the Gateway can map IP addresses to MAC addresses. RARP is the reverse of ARP. (This data is stored in temporary memory and changes periodically.) To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the *Local Network* screen, click **Close**.

## Status > Wireless

The *Wireless* screen displays information about your wireless network.



MAC Address:	
Mode:	Mixed
Network Name (SSID):	Linksys
Radio Band:	Wide - 80MHz Channel
Wide Channel:	1
Standard Channel:	11 2.417GHz
Security:	Enabled
SSID Broadcast:	Enabled

Status > Wireless

## Wireless

**MAC Address** The wireless MAC address of the Gateway's local, wireless interface is displayed.

**Mode** The wireless network mode of the Gateway is displayed.

**Network Name (SSID)** The wireless network name, which is also called the SSID, is displayed.

### Radio Band

**Wide Channel** The wide channel of the wireless network is displayed.

**Standard Channel** The standard channel of the wireless network is displayed.

**Security Method** The wireless security method is displayed.

**SSID Broadcast** The status of SSID Broadcast is displayed.

## Status > DSL Connection

The *DSL* screen displays information about your DSL connection.



Status &gt; DSL Connection

## DSL Connection

**Status** The status of the DSL connection is displayed.

**Downstream Rate** The download speed of traffic from the Internet to the Gateway is displayed.

**Upstream Rate** The upload speed of traffic from the Gateway to the Internet is displayed. For ADSL connection, the Upstream Rate is typically 25% of the Downstream Rate.



**NOTE:** The Downstream and Upstream Rates are affected by distance from and configuration of the DSL central office.

## PVC Connection

**Encapsulation** The Encapsulation setting selected on the *Basic Setup* screen is displayed.

**Multiplexing** The Multiplexing setting selected on the *Basic Setup* screen is displayed.

**QoS** The QoS method selected on the *Basic Setup* screen is displayed.

**PCR** The PCR value entered on the *Basic Setup* screen is displayed.

**SCR** The SCR value entered on the *Basic Setup* screen is displayed.

**Autodetect** The Autodetect setting selected on the *Basic Setup* screen is displayed.

**VPI** The VPI value entered on the *Basic Setup* screen is displayed.

**VCI** The VCI value entered on the *Basic Setup* screen is displayed.

**Enable** The number of Permanent Virtual Circuits (PVC) is displayed.

**PVC Status** The status of the PVC is displayed.

## Appendix A: Troubleshooting

---

### ***Your computer cannot connect to the Internet.***

Follow the instructions until your computer can connect to the Internet:

- Make sure that the Gateway is powered on. The Power LED should be green and not flashing.
- If the Power LED is flashing, then power off all of your network devices, including the Gateway and computers. Then power on each device in the following order:
  1. Gateway
  2. Computer
- Check the LEDs on the front panel of the Gateway. Make sure the Power, DSL, and at least one of the numbered LEDs are lit. If they are not, then check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Gateway, and the Line port of the Gateway must be connected to the ADSL line.

***When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions.***

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Select **Tools > Internet Options**.
2. Click the **Connections** tab.
3. Select **Never dial a connection**.
4. Click **OK**.

***You are using a static IP address and cannot connect.***

Refer to Windows Help and change your Internet Protocol (TCP/IP) Properties to Obtain an IP address automatically.

***The computer cannot connect wirelessly to the network.***

Make sure the wireless network name or SSID is the same on both the computer and the Gateway. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Gateway.

***You need to modify the basic settings on the Gateway.***

Run the Setup Wizard on the Setup CD-ROM.

***You need to modify the advanced settings on the Gateway.***

Open the web browser (for example, Internet Explorer or Firefox), and enter the Gateway's IP address in the address field (the default IP address is **192.168.1.1**). When prompted, complete the *User name* and *Password* fields (the default user name and password is **admin**). Click the appropriate tab to change the settings



---

**WEB:** If your questions are not addressed here, refer to the Linksys website, [www.linksys.com/international](http://www.linksys.com/international)

---

## Appendix B: Specifications

---

Model Number	WAG325N
Standards	Draft 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3u, IEEE 802.3, g.992.1 (g.dmt), g.992.2 (g.lite), g.992.3, g.992.5, T1.413i2, U-R2 for Annex B
Ports	Power, DSL, Ethernet (1-4)
Button	Reset
Cabling Type	RJ-45, RJ-11 for Annex A
LEDs	Power, Ethernet (1-4), DSL, Internet, Wireless, Security
Antennas	3 non-detachable
Transmit Power	17 dBm
Antenna Gain	2 dBi
Security Features	Password-Protected Configuration for Web Access PAP and CHAP Authentication Denial of Service (DoS) Prevention URL Filtering, and Keyword, Java, ActiveX, Proxy, Cookie Blocking ToD Filter (Blocks Access by Time) VPN Passthrough for IPSec, PPTP, and L2TP Protocols 128, 64 Bits WEP with Passphrase WEP Key Generation, WPA, WPA2 SSID Broadcast Disable Access Restriction by MAC and IP Addresses
WEP Key Bits	64, 128, 256

### Environmental

Dimensions	188 x 40 x 176 mm
Weight	527 g
Power	12VDC, 1A
Certification	CE, FCC, IC-03, Wi-Fi, A-tick, Telepermit
Operating Temp.	0 to 40°C
Storage Temp.	-20 to 70°C
Operating Humidity	10 to 85% Noncondensing
Storage Humidity	5 to 90% Noncondensing

## Appendix C: Warranty Information

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.

**This Warranty is valid and may be processed only in the country of purchase.**

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



## Appendix D: Regulatory Information

### FCC Statement

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 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 20 cm between the radiator and your body.

### 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.

### 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.

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 20 cm 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.

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.



## Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2,4-GHz and 5-GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ftigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]:	Acest echipament este în conformitate cu cerințele esențiale și cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

For all products, the Declaration of Conformity (DofC) is available through one or more of these options:

- A pdf file is included on the product's CD.
- A print copy is included with the product.
- A pdf file is available on the product's webpage. Visit [www.linksys.com/international](http://www.linksys.com/international) and select your country or region. Then select your product.

If you need any other technical documentation, see the "Technical Documents on [www.linksys.com/international](http://www.linksys.com/international)" section, as shown later in this appendix.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328 and/or EN 301 893 as applicable
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950 and either EN 50385 or EN 50371

Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) are required for operation in the 5 GHz band.

DFS: The equipment meets the DFS requirements as defined in ETSI EN 301 893. This feature is required by the regulations to avoid interference with Radio Location Services (radars).

TPC: For operation in the 5 GHz band, the maximum power level is 3 dB or more below the applicable limit. As such, TPC is not required.

## CE Marking

For the Linksys Wireless-N, -G, -B, and/or -A products, the following CE mark, notified body number (where applicable), and class 2 identifier are added to the equipment.

CE 0560 !

or

CE 0678 !

or

CE 0336 !

or

CE !

Check the CE label on the product to find out which notified body was involved during the assessment.

## National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

*Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:*

*Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesi menzionati di seguito:*

*Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Richtlinie 1999/5/CE folgen) mit Ausnahme der folgenden aufgeführten Staaten:*

In the majority of the EU and other European countries, the 2,4- and 5-GHz bands have been made available for the use of wireless local area networks (LANs). The table labeled "Overview of Regulatory Requirements for Wireless LANs" provides an overview of the regulatory requirements applicable for the 2,4- and 5-GHz bands.

Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. Linksys recommends that you check with the local authorities for the latest status of their national regulations for both the 2,4- and 5-GHz wireless LANs.

**Overview of Regulatory Requirements for Wireless LANs**

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor ONLY	Indoor & Outdoor
2400-2483.5	100		X
5150-5350 <sup>†</sup>	200	X	
5470-5725 <sup>†</sup>	1000		X

<sup>†</sup>Dynamic Frequency Selection and Transmit Power Control are required in the frequency ranges of 5250-5350 MHz and 5470-5725 MHz.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "Overview of Regulatory Requirements for Wireless LANs":

### Denmark

In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage.

*I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.*

## France

For 2,4 GHz, the product should not be used outdoors in the band 2454 - 2483,5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band when used indoors. Check <http://www.arcep.fr/> for more details.

*Pour la bande 2,4 GHz, l'équipement ne doit pas être utilisé en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations en intérieur dans d'autres parties de la bande 2,4GHz. Consultez <http://www.arcep.fr/> pour de plus amples détails.*

Applicable Power Levels in France

Location	Frequency Range (MHz)	Power (EIRP)
Indoor (No restrictions)	2400-2483.5	100 mW (20 dBm)
Outdoor	2400-2454 2454-2483.5	100 mW (20 dBm) 10 mW (10 dBm)

## Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this 2,4-GHz wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization". Please check <http://www.comunicazioni.it/it/> for more details.

*Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN a 2,4 GHz richiede una "Autorizzazione Generale". Consultare <http://www.comunicazioni.it/it/> per maggiori dettagli.*

## Latvia

The outdoor usage of the 2,4 GHz band requires an authorization from the Electronic Communications Office. Please check <http://www.esd.lv> for more details.

*2,4 GHz frekveču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: <http://www.esd.lv>.*

### Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.
2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

## Product Usage Restrictions

This product is designed for indoor usage only. Outdoor usage is not recommended, unless otherwise noted.

### 2,4 GHz Restrictions

This product is designed for use with the standard, integral or dedicated (external) antenna(s) that is/are shipped together with the equipment. However, some applications may require the antenna(s), if removable, to be separated from the product and installed remotely from the device by using extension cables. For these applications, Linksys offers an R-SMA extension cable (AC9SMA) and an R-TNC extension cable (AC9TNC). Both of these cables are 9 meters long and have a cable loss (attenuation) of 5 dB. To compensate for the attenuation, Linksys also offers higher gain antennas, the HGA7S (with R-SMA connector) and HGA7T (with R-TNC connector). These antennas have a gain of 7 dBi and may only be used with either the R-SMA or R-TNC extension cable.

Combinations of extension cables and antennas resulting in a radiated power level exceeding 100 mW EIRP are illegal.

### Third-Party Software or Firmware

The use of software or firmware not supported/provided by Linksys may result that the equipment is no longer compliant with the regulatory requirements.

## Technical Documents on [www.linksys.com/international](http://www.linksys.com/international)

Follow these steps to access technical documents:

1. Enter <http://www.linksys.com/international> in your web browser.
2. Select the country or region in which you live.
3. Click the **Products** tab.
4. Select the appropriate product category.
5. Select the product sub-category, if necessary.
6. Select the product.
7. Select the type of documentation you want from the More Information section. The document will open in PDF format if you have Adobe Acrobat installed on your computer.




**NOTE:** If you have questions regarding the compliance of this product or you cannot find the information you need, please contact your local sales office or visit [www.linksys.com/international](http://www.linksys.com/international)

## 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/EC 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. Вашата отговорност е 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 Hausaltmüll 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 Liidus asuvatele klientidele**

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


### **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/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο , στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινотικά 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 mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.




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

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir  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 Kliġenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fi h is-simbolu  fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart municipali 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-fanot 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 hulladékészállítás rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken 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 afvalverwerkingsdienst, 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 gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

### 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, avfallshanteringen eller butiken där du köpte produkten.



**WEB:** For additional information, please visit [www.linksys.com/international](http://www.linksys.com/international)