LINKSYS®
A Division of Cisco Systems, Inc.

# USER GUIDE

# Wireless-N Gigabit Router with Storage Link

Model No: **WRT350N**

# 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

LINKSYS® A Division of Cisco Systems, Inc.

CISCO

# Chapter 1: Product Overview

Thank you for choosing the Wireless-N Gigabit Router with Storage Link, which is four devices in one: a wireless access point, which lets you connect to a wireless network; a built-in 4-port full-duplex 10/100 switch to connect your wired-Ethernet devices together; a router function that lets your whole network share a high-speed cable or DSL Internet connection; and a Storage Link that easily lets you add gigabytes of storage space onto your network using USB 2.0 hard drives, or plug in a USB flash disk to access your portable data files. The built-in media server streams music, video, and photos from the attached storage device to any UPnP compatible media adapter. And you can get to your files from anywhere in the world through the Internet. You also get Wireless-N technology, which can highly increase your range and speed.

## Front Panel

POWER **Power** (Green) The Power LED lights up and will stay on while the Router is powered on.

ETHERNET **Ethernet** (Green) (Orange) The Ethernet LED lights up green when the Router is connected to a device through the Ethernet port. If the LED is flashing, the Router is sending or receiving data over that port. The Ethernet LED lights up orange when it is connected to Gigabit and green when it is connected to 10/100.

INTERNET **Internet** (Green) (Orange) The Internet LED lights up green when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port. The Ethernet LED lights up orange when it is connected to Gigabit and green when it is connected to 10/100.

USB **USB** (Green) The USB LED indicates when an external USB hard drive or USB flash disk is connected to the Router.

WIRELESS **Wireless** (Green) The Wireless LED lights up when there is a wireless connection. If the LED is flashing, the Router is sending or receiving data over the wireless network.

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

## Back Panel

**USB** The USB port connects your Router to a USB storage device.

**Internet** The Internet port is where you will connect your cable or DSL Internet connection.

**1, 2, 3, 4** These Ethernet ports (1, 2, 3, 4) connect the Router to PCs on your wired network and other Ethernet network devices.

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

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

# Table of Contents

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

## 3. Enable MAC address filtering

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

## 4. Enable encryption

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

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

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

## General Network Security Guidelines

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

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

## Additional Security Tips

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

**WEB:** For more information on wireless security, visit **www.linksys.com/security**

# Chapter 3: Advanced Configuration

After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. However, if you'd like to change its advanced settings, use the Router'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 Router.

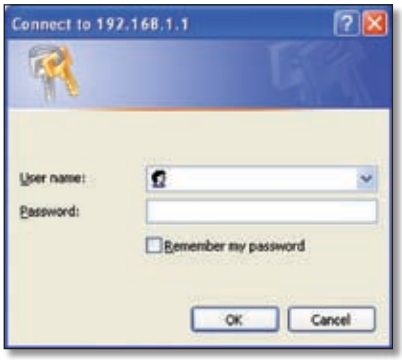
The web-based utility has these main tabs: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

**NOTE:** When first installing the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility.

## How to Access the Web-Based Utility

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

A password request screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. The first time you open the Web-based utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Click **OK** to continue.




Password Screen

## Setup > Basic Setup

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


Setup > Basic Setup

## Internet Setup

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

### Internet Connection Type

Select the type of Internet connection your ISP provides from the drop-down menu. The available types are:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

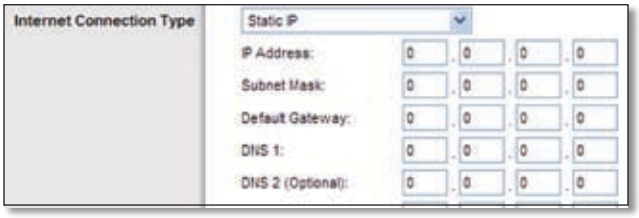
### Automatic Configuration - DHCP

By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. (This option usually applies to cable connections.)


Internet Connection Type > Automatic Configuration - DHCP

### Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.




Internet Connection Type > Static IP

**IP Address** This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

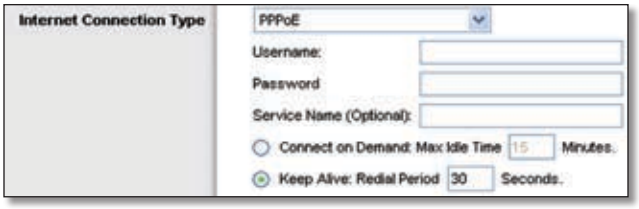
**Subnet Mask** This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

**Default Gateway** Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

**DNS** Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

### 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 > PPPoE

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

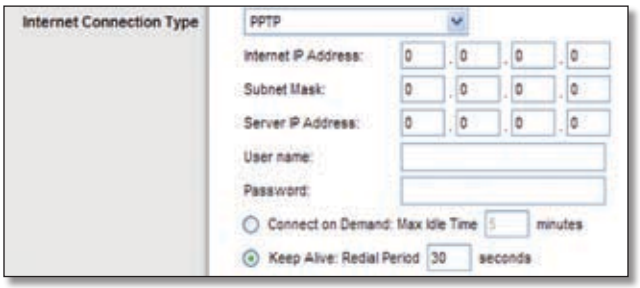
**Service Name (optional)** If provided by your ISP, enter the Service Name.

**Connect on Demand: Max Idle Time** You can configure the Router 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 Router 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 Router will periodically check your Internet connection. If you are disconnected, then the Router 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 Router to check the Internet connection. The default Redial Period is **30** seconds.

### PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.




Internet Connection Type > PPTP

**Internet IP Address** This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

**Subnet Mask** This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

**Server IP Address** Your ISP will provide you with the Server IP[ Address.

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

**Connect on Demand: Max Idle Time** You can configure the Router 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 Router 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 Router will periodically check your Internet connection. If you are disconnected, then the Router 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 Router to check the Internet connection. The default value is **30** seconds.

### L2TP

L2TP is a service that applies to connections in Israel only.


Internet Connection Type > L2TP

**Internet IP Address** This is the IP address of the L2TP Server. Your ISP will provide you with the IP Address you need to specify here.

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

**Connect on Demand: Max Idle Time** You can configure the Router 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 Router 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 Router will periodically check your Internet connection. If you are disconnected, then the Router 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 Router to check the Internet connection. The default Redial Period is **30** seconds.

### Telstra Cable

Telstra Cable is a service that applies to connections in Australia only.

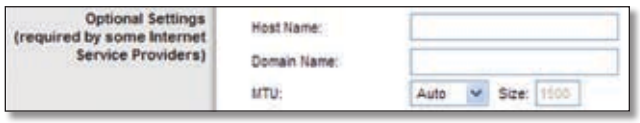

Internet Connection Type > Telstra Cable

**Internet IP Address** This is the IP address of the Telstra Cable. Your ISP will provide you with the IP Address you need to specify here.

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

### Optional Settings

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




Optional Settings

**Host Name/Domain Name** These fields allow you to supply a host and domain name for the Router. 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 Router select the best MTU for your Internet connection, keep the default setting, **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 size depends on the Internet Connection Type:

- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

## Network Setup

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

### Router Address

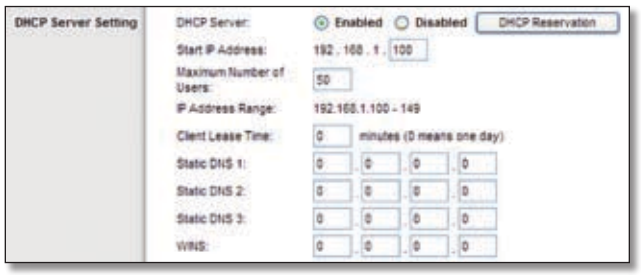
This presents both the Router's IP Address and Subnet Mask, and URL Address as seen by your network. The default Router IP address is 192.168.1.1 and URL address is http://WRT350N.com.


Router IP Address

### Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router 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

Router's DHCP server option, make sure there is no other DHCP server on your network.




Network Address Server Settings (DHCP)

**DHCP Server** DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disable** (no other DHCP features will be available).

**Starting IP Address** Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router'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 Starting IP Address is **192.168.1.100**.

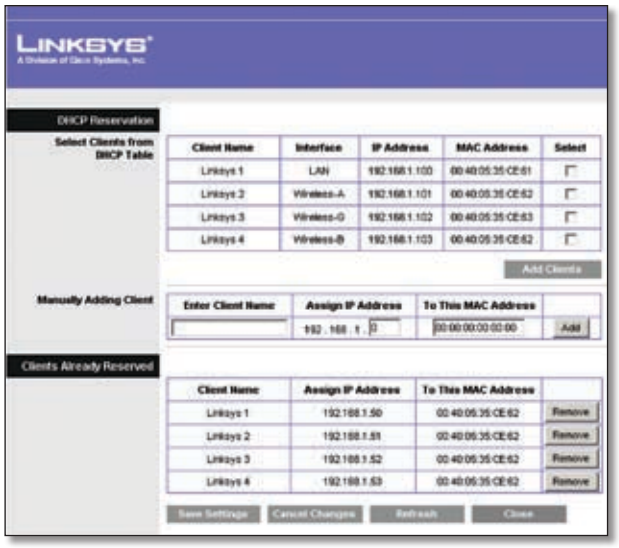
**Maximum Number of DHCP Users** Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

**Client Lease Time** The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user 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. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

**WINS** The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

**DHCP Reservation** Click **DHCP Reservation** if you want to assign a fixed local IP address to a MAC address.




DHCP Reservation

You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. Click the Select checkbox to reserve a client's IP address. Then click **Add Clients**.

If you want to manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Make sure the IP address is between the starting DHCP server's IP address and maximum number of DHCP users range. Enter its MAC Address in the *To This MAC Address* field. Click **Add**.

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**.

When you finish your changes, click **Save Settings** to save your changes. Click **Cancel Changes** to cancel your changes. To view the most up-to-date information, click **Refresh**. To exit this screen, click **Close**.

## Time Setting

Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.)


Time Setting

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

## Setup > DDNS

The Router 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 Router.

Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default setting, **Disable**.

### 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 > DDNS > DynDNS

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

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

**Host Name** The is the DDNS URL assigned by the DDNS service.

**WildCard** Select **Enabled** to enable this feature or **Disabled** to disable it.

**Internet IP Address** The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

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

**Update** To manually trigger an update, click **Update**.

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

#### TZO.com

Setup > DDNS > TZO

**E-mail Address, TZO Password, and Domain Name** Enter the settings of the account you set up with TZO.

**Internet IP Address** The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

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

**Update** To manually trigger an update, click **Update**.

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 Router with the MAC Address Clone feature.

Setup > MAC Address Clone

### MAC Address Clone

**Enable/Disable** To have the MAC Address cloned, select **Enable**.

**User Defined Entry** Enter the MAC Address registered with your ISP here.

**Clone Your PC's MAC** Clicking this button will clone the MAC address of the computer you are using.

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 Router'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** If this Router is hosting your network's connection to the Internet, select **Enable**. If another Router exists on your network, select **Disable.** When NAT is disabled, **Dynamic Routing (RIP)** will be available as an option.

#### Dynamic Routing

**RIP** This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is **Disabled** by default.

#### Static Routing

**Select Route Entry number** To set up a static route between the Router and another network, select a number from the drop-down list. (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. (Click **Delete This Entry** to delete a static route.)

**Enter Route Name** Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

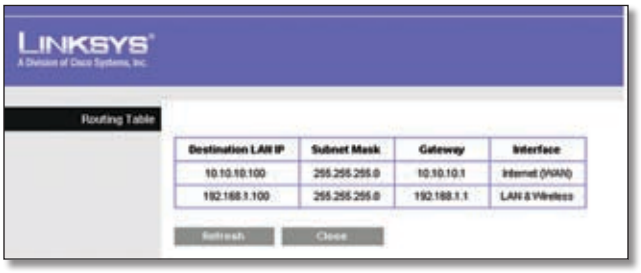
**Destination LAN IP** The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

**Subnet Mask** The Subnet Mask determines which portion of a Destination LAN 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 Router and the remote network or host.

**Interface** This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **WAN (Internet)**.

Click **Show Routing Table** to view the Static Routes you have already set up.




Routing Table

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

### Wireless Network

**Network Mode** If you have wireless devices in your network, keep the default setting, **Mixed**. If you do not have any wireless devices in your network, select **Disable**.

**Wireless Network Name (SSID)** The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.

**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**.

**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, keep the default, **Auto**.

**SSID Broadcast** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, **Enable**. If you do not want to broadcast the Router's SSID, then select **Disable**.

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

## Wireless > Wireless Security

The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security."

### Wireless Security

#### Security Mode

Select the mode you want to use: **PSK-Personal**, **PSK2-Personal**, **PSK-Enterprise**, **PSK2-Enterprise**, **RADIUS**, or **WEP**. PSK2 is a more advanced, more secure version of PSK.

Follow the instructions for the security method you want to use.

#### PSK-Personal


Security Mode > PSK-Personal

**Encryption.** Select the algorithm you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**Pre-shared Key.** Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

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

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

#### PSK2-Personal


Security Mode > PSK2-Personal

**Encryption.** Select the algorithm you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

**Pre-shared Key.** Enter the key shared by the Router and your other network devices. It must have 8-63 characters.

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

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

### PSK-Enterprise

Security Mode > PSK-Enterprise

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

**Encryption.** Select the algorithm(s) you want to use, **TKIP** or **AES**. (AES is a stronger encryption method than TKIP.)

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

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

**Shared Key.** Enter the key shared by the Router and RADIUS server.

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

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

### PSK2-Enterprise

Security Mode > PSK2-Enterprise

This option features PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

**Encryption.** Select the algorithm(s) you want to use, **AES** or **TKIP**. (AES is a stronger encryption method than TKIP.)

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

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

**Shared Key** Enter the key shared between the Router and the server.

**Key Renewal** Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

### RADIUS

Security Mode > RADIUS

**IMPORTANT:** If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

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

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

**RADIUS Port** Enter the port number of the RADIUS server. The default value is **1812**.

**Shared Key** Enter the key shared between the Router and the server.

**Encryption** Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**, which is stronger encryption than 40/64 bit encryption.

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

**Key 1-4** If you want to manually enter the WEP keys, then enter them in the Key 1-4 fields.Tx Key Select a key from the drop-down menu.

### WEP

Security Mode > WEP

WEP is a basic encryption method offering two levels of encryption; 128-bit is stronger than 40/64-bit encryption.

**Encryption.** Select the appropriate level of encryption, **40/64-bit (10 hex digits)** or **128-bit (26 hex digits)**.

**Passphrase.** To automatically generate keys, enter your passphrase. Then click the **Generate** button.

**Key 1-4.** If you want to manually enter the WEP keys, then enter them in the Key 1-4 fields.

**TX Key.** To indicate which WEP key to use, select a transmit key number.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

**NOTE:** If you have WEP enabled, and have trouble using Windows XP or Vista Zero Configuration, refer to Appendix A: Troubleshooting.

## 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

### Access Restriction

**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, keep the default setting, **Disabled**.

**Prevent** Select this to block wireless access by MAC Address. This button is selected by default.

**Permit** Select this to allow wireless access by MAC Address. This button is not selected by default.

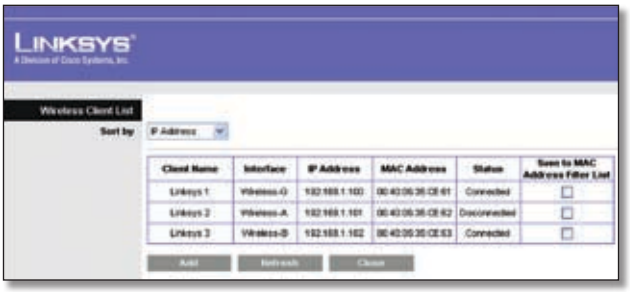
### MAC Address Filter List

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 **Save to MAC Address 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.

Then click the E**nable MAC Filter** checkbox for any device you want to add to the MAC Address Filter List. To update the information on this list, click the **Refresh** button. When you have finished making changes to the Wireless *Client MAC List* screen, click the **Update Filter List** button to save the changes. Click the **Close** button to return to the *Wireless MAC Filter* screen.

When you have finished making changes to the *MAC Address Filter List* screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes.

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




Wireless Client List

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click Help.

## Wireless > Advanced Wireless Settings

This *Wireless > Advanced Wireless Settings* screen is used to set up the Router'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 Router but not with each other. To use this function, select **Enable**. AP Isolation is on **Disable** by default.

**Frame Burst** Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To turn on the Frame Burst option, select **Enable**. The default is **Disable**.

**Authentication Type** The default is set to **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.

**Basic Rate** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.

**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 Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

**CTS Protection Mode** CTS (Clear-To-Send) Protection Mode's default setting is **Auto**. The Router 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 Router in an environment with heavy 802.11b traffic. This function boosts the Router's ability to catch all Wireless-N and Wireless-G transmissions but will severely decrease performance.

**Beacon Interval** The default value is **100**. Enter a value between 20 and 1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network.

**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 Router 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 value, 2346, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router 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. In most cases, keep its default value of **2346**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## Security > Firewall

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


Security > Firewall

### Firewall

**SPI Firewall Protection** A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select **Enabled** to use a firewall, or **Disabled** to disable it.

#### Internet Filters

**Filter 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.

**Filter Multicast** Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. This feature is selected by default. Select **Enabled** to filter multicasting, or **Disabled** to disable this feature.

**Filter Internet NAT Redirection** This feature uses port forwarding to block access to local servers from local networked computers. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. This feature is not selected by default.

**Filter IDENT (Port 113)** This feature keeps port 113 from being scanned by devices outside of your local network. This feature is selected by default. Deselect this feature to disable it.

### Web Filters

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

**Java** 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 **Enable** to enable Java filtering.

**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 **Enable** to enable ActiveX filtering.

**Cookies** A cookie is data stored on your computer and used by Internet sites when you interact with them. Select **Enable** to enable cookie filtering.

When you have finished making changes to this screen, click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to undo your changes. For more information, click **Help**.

## Security > VPN Passthrough

The *Security > VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router'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 Router, 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 Router, 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 Router, keep the default, **Enable**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## Storage > Disk

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

The Disk screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk.


Storage > Disk

### Disk Detail

If a blank disk is attached to the Router, the Disk, Make and Model, and Physical Size columns describe the disk.

**Claim.** For a blank disk, click the **Claim** button to create a partition that will be formatted as FAT32. On the *Claim Disk* screen, enter a name for the partition. Click the **Claim** button to save the new name, or click the **Clear** button to clear the *New Partition Name* field. Click the **Cancel** button to cancel the changes.

**Safely Remove.** Before physically disconnecting a disk from the Router, click the **Safely Remove** button first. This ensures that the disk is not removed while data is being transferred to or from the disk; otherwise, data may be lost.

If a formatted disk is attached to the Router, the Partition, File System, Total Space, and Free Space columns describe the partition(s) of the disk.

**Create Share.** Shares control access to the partition(s) of the disk. To create shares, click the **Create Share** button.

### Erase Disk

To erase a disk, click the check box next to the name of the disk and select the button

**Quick Erase** To quickly free up space on the disk, click the Quick Erase button to remove the table of contents from the disk. (This is less secure than the Full Erase option.)

**Full Erase** Click the Full Erase button to initiate complete removal of data from the disk. Once the removal is complete, the data cannot be recovered. The Full Erase option is recommended if the disk holds sensitive data.

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

## Storage > Share

Shares control access to the partition(s) of the disk attached to the Router. The *Share* screen describes the current shares. Using this screen, you can create new shares, modify share properties, or delete shares.


Storage > Share

## Share Management

### Shares

The Share Name, Partition, and Total Space columns describe the shares.

### Properties

**Modify** Click the **Modify** button to change the properties of a share. On the *Share Properties* screen, enter a different name for the share, and/or select a different partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

### Share Access

**Modify** Click the **Modify** button to change the access privileges of a share. On the *Share Access* screen, groups with no access are listed in the Other Group column, and groups with access are listed in the Group with Access column. To give a group read-only access, select the group, and click the **Read Only** button. To give a group read/write access, select the group, and click the **Read/Write** button. To strip a group of its current access privileges, select the group, and click the **Remove** button. Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the **Close** button to exit the *Share Access* screen.

**Delete** Click the **Delete** button to remove a share.

### Create Share

**Create New Share** Click the **Create New Share** button to create a new share. On the *Share Properties* screen, enter a name for the share, and select a partition from the *Resides in Partition* drop-down menu. Click the **Create Share** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

## Storage > Administration

The Administration screen allows you to manage the users and groups of users that can access the shares.


Storage > Administration.

## Basic

**Machine Name.** Enter a name for the Router. Punctuation and other special characters (e.g., * / | \) cannot be used in the name.

**Workgroup Name** Enter the Workgroup Name of your networked computers.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

## User Management

The users are listed in the User Management table. There are two default users, admin (read/write access) and guest (read-only access); these cannot be deleted.

### Properties

**Modify** Click the **Modify** button to change the properties of a user. On the *User Properties* screen, enter a different name for the user, change the password, and/or select a different group from the Group drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

**Delete** Click the **Delete** button to remove a user.

**Create New User** Click the **Create New User** button to create a new user. On the *User Properties* screen, enter a name for the user. Then enter a password and enter it again in the Re-enter to confirm field. Select a group from the Group drop-down menu. Click the **Create User** button to save the new properties, or click the **Clear** button to clear the changes. Click the **Cancel** button to cancel the changes.

## Group Management

The groups are listed in the Group Management table. There are two default groups, admin and guest; these cannot be deleted.


Storage > Group

### Properties

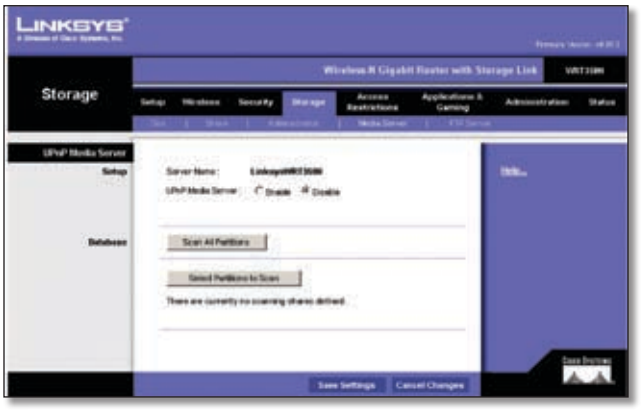
**Modify** Click the **Modify** button to change the user membership of a group. On the *Group Properties* screen, users who are not members are listed in the Other Users column, and users who are members are listed in the Users in Group column. To add a user to the group, select the user, and click the **Join Group** button. To remove a user from the group, select the user, and click the **Remove** button. Click the **Save Settings** button to save the changes, or click the **Cancel Changes** button to cancel the changes. Click the Close button to exit the Group Properties screen.

**Delete** Click the **Delete** button to remove a user.

**Create New Group** Click the **Create New Group** button to create a new group. On the *Group Properties* screen, enter a name for the group. Click the **Create Group** button to save the new name, or click the **Clear** button to clear the change. Click the **Cancel** button to cancel the change.

## Storage > Media Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.




Storage > Media Server

### Setup

**Server Name** The name of the router's media server is displayed here. It can be changed at Storage > Administration..

**UPnP Media Server** To use the Router's media server function, select **Enable**. Otherwise, select **Disable**.

## Database

Select content to add to the database of the Router's media server.

**Scan All Partitions** Click this button to scan all partitions of the USB hard disk for content.

**Select Partitions to Scan** Click this button to select specific partitions to scan for content.

The Partition and Folder columns describe the partitions of the USB hard disk.

**Scan** Click the **Scan** button to scan a specific partition for content. The *Partition List* screen will appear. Click the Select button to select a partition for scanning. Click the **Up List** button to move up one level in the file structure. Click the **Refresh** button to update the on-screen information. Click the **Close** button to exit the *Partition List* screen.


Storage > Partition List

**Delete** Click the **Delete** button to delete a specific partition from the Router's database.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes.

## Storage > FTP Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

The FTP Server tab creates an FTP Server that can be accessed from the Internet or your local network.


Storage> FTP Server

### Setup

**Server Name** The name of the router's FTP server is displayed here. It can be changed at Storage > Administration.

**FTP Server** Select **Enable** to set this Router as an FTP Server. Otherwise, select **Disable** to turn the service off. An external USB hard drive or USB disk must be connected to the USB Port to use this service.

**Internet Access** Select **Enable** to allow access of the FTP Server from the Internet. Otherwise, select **Disable** to only allow local network access.

**FTP Port** Enter the FTP Port number to use. The default port is 21.

### Share

Select the partition or folder to share in the FTP Server.

**All Partitions** Selects all partitions on the USB disk.

**Specify Folder** If you want to share a specific folder, click **Select Partition** and locate the folder.

### Access

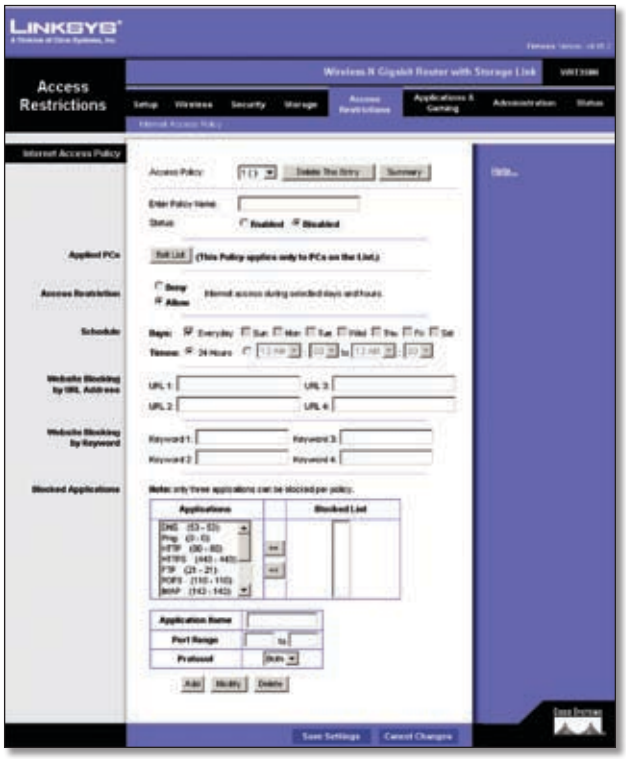
Click **FTP Share Access** to grant specific rights to groups. You can grant Read Only or Read/Write permissions.

**FTP Access** Select the group from the Other Group list and click either the **Read Only** or **Read/Write** button to move the group to the Group With Access column.

After you have made your changes, click the **Save Settings** button to apply your changes, or click the **Cancel Changes** button to cancel your changes. Click **Close** to exit this window.

## Access Restrictions > Internet Access

The *Access Restrictions > Internet Access* screen allows you to deny 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

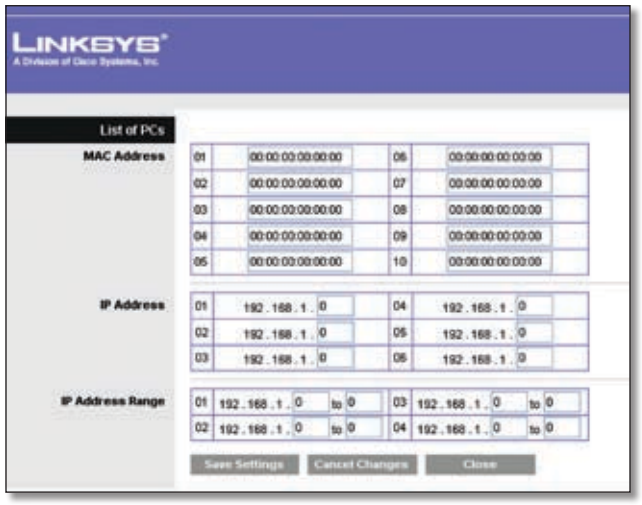
### Internet Access

**Internet Access Policy** Internet 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**.

**Deny or Allow** If you select **Deny**, the PC on the Edit List will be denied Internet Access by the dates and times selected. PCs not on the list will still have Internet access. If you select Allow, the PCs on the Edit List will have Internet access by the dates and times selected. The PCs not on the Edit List will not have Internet access. If there is a conflict with a policy, the lower numbered policy will have priority over a higher numbered policy.

### To create an Internet Access Policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. Enter a Policy Name in the field.
3. To enable this policy, select **Enable**.
4. Click the **Edit List** button to select which PCs will be affected by the policy. The *List of PCs* screen appears. You can select a PC 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 PCs. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.




List of PCs

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* 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. Enter a URL address or Keyword for Website Blocking or select any Blocked Applications you wish to use. Using these features can slow down your Internet speed.
8. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to cancel the policy's settings.

### Blocked Applications

You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting applications from the Applications List.

To add an application, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select its protocol from the *Protocol* drop-down menu. Then click **Add**.

To modify an application, select it from the *Application List*. Change the application name, port range, or protocol setting. Then click **Modify**.

To delete an application, select it from the *Application List*. Then click **Delete**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your 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** Select **pre-configure** or 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 **TCP** or **UDP**, or select **Both.,** .

**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. For more information, click **Help**.

## Applications and Gaming > Port Range Forwarding

The *Applications & Gaming* > *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.)


Applications and Gaming > Port Range Forwarding

### Port Range Forwarding

To forward a port, 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.

**Start/End** This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column.

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

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

**Enable** Select **Enable** to enable port forwarding for the relevant application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## Applications & Gaming > Port Range Triggering

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


Applications and Gaming > Port Triggering

### Port Range Triggering

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

**Triggered Range** For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

- **Start Port** Enter the starting port number of the Triggered Range.
- **End Port** Enter the ending port number of the Triggered Range.

**Forwarded Range** For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

- **Start Port** Enter the starting port number of the Forwarded Range.
- **End Port** Enter the ending port number of the Forwarded Range.

**Enable** Select **Enable** to enable port triggering for the applicable application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## 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 Forward 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

To use this feature, select **Enabled**. To disable DMZ hosting, select **Disabled**.

**Source IP Address** If you want any IP address to be the source, select **Any IP Address**. If you want to specify an IP address or range of IP addresses as the designated source, click the second radio button, and enter the IP address(es) in the fields provided.

**Destination** If you want to specify the DMZ host by IP address, select **IP Address** and complete the IP address in the field provided. If you want to specify the DMZ host by MAC address, select **MAC Address** and enter the MAC address in the field provided. To retrieve this information, click the **DHCP Client Table** button.

The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired Time (how much time is left for the current IP address). To select a DHCP client, click the **Select** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the DMZ screen, click the **Close** button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## 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

### QoS (Quality of Service)

#### Wireless

**Wireless WMM (Wi-Fi Multimedia)** WMM is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, your wireless client devices in your network must support Wireless WMM. If you would like to disable this feature, select **Disabled**. Otherwise, keep the default, **Enabled**.

**No Acknowledgement** If you want to disable the Router's Acknowledgement feature, so the Router 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 set, select **Enabled**. Otherwise, select **Disabled**.

### Category

There are five categories available. Select one of the following: **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 **Add** to save your changes. Your new entry will appear in the Summary list.

#### Add a New Application

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

### Online Games

**Games** Select the appropriate game. If you select **Add a New Game**, follow the Add a New Game instructions.

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

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

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

### Ethernet Port

**Ethernet** Select the Ethernet port that you want to use.

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

Click **Add** 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 **Add** 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.

When you finish making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. For more information, click **Help**.

## Administration > Management

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


Administration > Management

### Router Password

#### Router Access

To ensure the Router's security, you will be asked for your password when you access the Router's Web-based Utility. The default password is **admin**.

**Router Password** Enter a new Password for the Router.

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

#### Web Access

**Web Utility Access** HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS.** The default selection is **HTTP**.

**Web Utility Access via Wireless** If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, **Enable**, to enable wireless access to the Router's web-based utility, or select **Disable** to disable wireless access to the utility.

#### Remote Access

**Remote Management** To access the Router remotely from the Internet, select **Enable**.

**Web Utility Access** Select from HTTP or HTTPS communications protocols for remote access from the Internet.

**Remote Upgrade** Select **Enabled** to be able to upgrade the firmware remotely from the Internet.

**Allowed Remote IP Address** Select **Any IP Address** or manually enter an IP address to allow remote access to the Web-based Utility from the Internet.

**Remote Management Port** Enter the port number that will be open to outside access to access the Router's Web-based Utility. You will need to enter the Router's password when accessing the Router this way, as usual.

#### UPnP

**UPnP** Keep the default, **Enable** to enable the UPnP feature; otherwise, select **Disable**.

**Allow Users to Configure** To use Allow Users to Configure, select **Enabled**.

**Allow Users to Disable Internet Access** To use Allow Users to Disable Internet Access, click **Disabled**.

**Backup Configurations** To back up the Router's configuration file, click this button. Then, follow the on-screen instructions.

**Restore Configurations** To restore the Router's configuration file, click the **Browse** button to locate the file, and follow the on-screen instructions. After you select the file, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

## Administration > Log

The Router can keep logs of all traffic for your Internet connection.


Administration > Log

### Log

**Log** To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

When you wish to view the logs, click **View Log**.

Click **Save the Log** to save your log, click **Refresh** to refresh the screen, or click **Clear** to clear the screen.

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

## Administration > Diagnostics

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components.


Administration > Diagnostics

### Ping Test

**Ping** The Ping test checks the status of a connection. Enter the address of the PC whose connection you wish to test, the packet size (default is **32** bytes) and how many times you wish to test it. Then, click **Start to Ping**. The *Ping Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.


Administration > Ping Test

### Traceroute Test

**Traceroute** To test the performance of a connection, click **Traceroute** to open the *Traceroute Test* screen. Enter the address of the PC whose connection you wish to test and click **Traceroute**. The *Traceroute Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.


Administration > Traceroute Test

## Administration > Factory Defaults

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

**NOTE:** Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration settings.

### Factory Defaults

**Restore Factory Defaults** To reset the Router's settings to the default values, select **Restore Factory Defaults**. Any settings you have saved will be lost when the default settings are restored.


Administration > Factory Defaults

## Administration > Firmware Upgrade

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


Administration > Firmware Upgrade

Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file.

### Upgrade Firmware

**Please select a file to upgrade** Click **Browse** and select the extracted firmware upgrade file. Then click **Upgrade** and follow the on-screen instructions.

## Status > Router

The *Status* > *Router* screen displays the Router's current status.


Status > Router

### Router Information

**Firmware Version** This is the Router's current firmware.

**Current Time** This shows the time, as you set on the Setup tab.

**Internet MAC Address** This is the Router's MAC Address, as seen by your ISP.

**Host Name** If required by your ISP, this would have been entered on the Setup tab.

**Domain Name** If required by your ISP, this would have been entered on the Setup tab.

### Internet Connection

**Connection Type** This indicates the type of Internet connection you are using.

**Internet IP Address** The Router's Internet IP address is displayed here.

**Subnet Mask and Default Gateway** The Router's Subnet Mask and Default Gateway address are displayed here for DHCP and static IP connections.

**DNS1-3** Shown here are the DNS (Domain Name System) IP addresses currently used by the Router.

**MTU** Shown here is the MTU (Maximum Transmission Unit) setting for the Router.

**DHCP Lease Time** Displays how long the lease is for the IP address that your ISP automatically assigned you.

**IP Address Release** Available for a DHCP connection, click this button to release the current IP address of the device connected to the Router's Internet port.

**IP Address Renew** Available for a DHCP connection, click this button to replace the current IP address of the device connected to the Router's Internet port with a new IP address.

For PPoE, PPTP, L2TP, and Telstra Cable Internet Connection types, a connect and disconnect button will be available to establish a connection to your ISP.

Click the **Refresh** button to update the on-screen information. For more information, click **Help**.

## Status > Local Network

The Local Network screen displays information about the local network.

Status > Local Network

### Local Network

**Local MAC Address** The MAC Address of the Router's local interface is displayed here.

**Router IP Address** This shows the Router's IP address, as it appears on your local network.

**Subnet Mask.** The Router's Subnet Mask is shown here.

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

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

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

**DHCP Client Table** Click **DHCP Client Table** to view the DHCP Client Table. It lists computers and other devices that have been assigned IP addresses by the Router. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Expired 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**.

For more information, click **Help**.

## Status > Wireless Network

The Wireless screen displays the status information of your wireless network.

Status > Wireless Network

**MAC Address** The MAC Address of the Router's wireless interface is displayed here.

**Mode** Displayed here is the wireless mode (Mixed, Wireless-N Only, Wireless-G Only, Wireless-B Only or Disabled) used by the network.

**Net work Name (SSID)** Displayed here is the name of the wireless network or SSID.

**Radio Band** Displayed here is the Radio Band setting selected on the *Basic Wireless Settings* screen.

**Wide Channel** Displayed here is the Wide Channel setting selected on the *Basic Wireless Settings* screen.

**Standard Channel** Shown here is the Standard Channel setting selected on the *Basic Wireless Settings* screen.

**Security** Displayed here is the wireless security method used by the Router.

**SSID Broadcast** Displayed here is the status of the SSID Broadcast feature.

For more information, click **Help**.

# Appendix A: Troubleshooting

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

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

- Make sure that the Router 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 modem, Router, and computers. Then power on each device in the following order:
  1. Cable or DSL modem
  2. Router
  3. Computer
- Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the modem must be connected to the Internet port on the Router.

***The modem does not have an Ethernet port.***

The modem is a dial-up modem for traditional dial-up service. To use the Router, you need a cable/DSL modem and high-speed Internet connection.

***You cannot use the DSL service to connect manually to the Internet.***

After you have installed the Router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually.

***The DSL telephone line does not fit into the Router's Internet port.***

The Router does not replace your modem. You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer. Click **Setup** and follow the on-screen instructions.

***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**.

***The Router does not have a coaxial port for the cable connection.***

The Router does not replace your modem. You still need your cable modem in order to use the Router. Connect your cable connection to the cable modem, and then insert the setup CD into your computer. Click **Setup** and follow the on-screen instructions.

***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 Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router.

***You need to modify the settings on the Router.***

Open the web browser (for example, Internet Explorer or Firefox), and enter the Router's IP address in the address field (the default IP address is **192.168.1.1**). When prompted, enter the password to the Router (the default 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**

# Appendix B: Specifications

| | |
|---|---|
| Model | WRT350N |
| Standards | Draft 802.11n, 802.11g, 802.11b, 802.3, 802.3u |
| Ports | Power, Internet, Ethernet, USB |
| Button | Reset |
| LEDs | Power, Ethernet (1-4), Internet, USB, Wireless, Security |
| # of Antennas | 3 |
| Modulations | 802.11b: CCK, QPSK, BPSK<br>802.11g: OFDM<br>802.11a: OFDM<br>Wireless-N: BPSK, QPSK, 16-QAM, 64-QAM |
| RF Pwr (EIRP) in dBm | 17 dBm |
| Antenna Gain in dBi | 1.8 dBm |
| UPnP | Supported |
| Security Features | WEP, PSK, PSK2 |
| Security Key Bits | 128bit, 256bit |

## Environmental

| | |
|---|---|
| Dimensions | 7.40 x 1.57 x 6.93 in<br>(188 mm x 40 mm x 176 mm) |
| Unit Weight | 18.3 oz (0.52 kg) |
| Power | 12V, 1.5A |
| Certifications | FCC, CE, IC-03 |
| Operating Temp. | 0° C to 40° C (32° F to 104° F) |
| Storage Temp. | -20° C to 60° C (-4° F to 140° F) |
| Operating Humidity | 10% to 85%, Non-Condensing |
| Storage Humidity | 5% to 90% Non-Condensing |

# Appendix C: Warranty Information

## Limited Warranty

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

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

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

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

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

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

# Appendix D: Regulatory Information

## FCC Statement

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

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

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

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

## FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

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

The device for the band 5150-5250 MHz is only for indoor usage to reduce the potential for harmful interference to co-channel mobile satellite systems; the maximum antenna gain of 3.7 dBi permitted (for devices in the bands 5250-5350 MHz and 5470-5725 MHz) to comply with the e.i.r.p. limit; and the maximum antenna gain of 3.7 dBi permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

High-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

## Safety Notices

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

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

## Industry Canada Statement

This class B digital apparatus complies with Canada ICES-003 and RSS210 rules.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device. This device has been designed to operate with an antenna having a maximum gain of 3.7dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

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

### Industry Canada Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

## Avis d'Industrie Canada

Cet appareill numérique de classe B est conforme aux normes NMB003 et RSS210 d'Industrie Canada.

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

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

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

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

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

## Wireless Disclaimer

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

## Avis de non-responsabilité concernant les appareils sans fil

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

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

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

**English - Environmental Information for Customers in the European Union**

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

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

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

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

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

**Dansk (Danish) - Miljøinformation for kunder i EU**

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

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

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

**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.

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

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

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

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

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

**Malti (Maltese) - Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea**

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

**Magyar (Hungarian) - Környezetvédelmi információ az európai uniós vásárlók számára**

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

**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 şi/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 obişnuit. Este responsabilitatea dvs. să casați acest produs şi alte echipamente electrice şi electronice prin intermediul unităților de colectare special desemnate de guvern sau de autoritățile locale. Casarea şi reciclarea corecte vor ajuta la prevenirea potențialelor consecințe negative asupra sănătății mediului şi a oamenilor. Pentru mai multe informații detaliate cu privire la casarea acestui echipament vechi, contactați autoritățile locale, serviciul de salubrizare 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 insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

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