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.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys</td>
<td><a href="http://www.linksys.com">www.linksys.com</a></td>
</tr>
<tr>
<td>Linksys International</td>
<td><a href="http://www.linksys.com/international">www.linksys.com/international</a></td>
</tr>
<tr>
<td>Glossary</td>
<td><a href="http://www.linksys.com/glossary">www.linksys.com/glossary</a></td>
</tr>
<tr>
<td>Network Security</td>
<td><a href="http://www.linksys.com/security">www.linksys.com/security</a></td>
</tr>
</tbody>
</table>

Copyright and Trademarks

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2007 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.
# Table of Contents

Chapter 1: Product Overview  
Front Panel .................................................. 3  
Back Panel .................................................. 3  

Chapter 2: Wireless Security Checklist  
General Network Security Guidelines ....................... 4  
Additional Security Tips ..................................... 4  

Chapter 3: Advanced Configuration  
Setup > Basic Setup ........................................... 5  
Setup > DDNS .................................................... 9  
Setup > MAC Address Clone ................................ 10  
Setup > Advanced Routing ................................... 10  
Wireless > Basic Wireless Settings ......................... 11  
Wireless > Wireless Security ................................ 12  
Wireless > Wireless MAC Filter ............................ 13  
Wireless > Advanced Wireless Settings ................... 15  
Security > Firewall ......................................... 16  
Security > VPN Passthrough ................................ 17  
Access Restrictions > Internet Access ...................... 17  
Applications and Gaming > Single Port Forwarding ... 19  
Applications and Gaming > Port Range Forwarding .... 19  
Applications & Gaming > Port Range Triggering ....... 20  
Applications and Gaming > DMZ .......................... 20  
Applications and Gaming > QoS .......................... 21  
Administration > Management ............................ 23  
Administration > Log ........................................ 24  
Administration > Diagnostics .............................. 24  
Administration > Factory Defaults ......................... 25  
Administration > Firmware Upgrade ...................... 25  
Status > Router ............................................. 26  
Status > Local Network ..................................... 26  
Status > Wireless Network ................................. 27  

Appendix A: Troubleshooting .................................. 28  
Appendix B: Specifications .................................... 29  
Appendix C: Warranty Information ........................... 30  
Appendix D: Regulatory Information ......................... 31  
      FCC Statement ........................................... 31  
      FCC Radiation Exposure Statement .................. 31  
      Safety Notices .......................................... 31  
      Industry Canada Statement ............................ 31  
      Avis d’Industrie Canada ................................ 32
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Disclaimer</td>
<td>32</td>
</tr>
<tr>
<td>Avis de non-responsabilité concernant les appareils sans fil</td>
<td>32</td>
</tr>
</tbody>
</table>
Chapter 1: Product Overview

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

Front Panel

1, 2, 3, 4 (Blue) These numbered LEDs, corresponding with the numbered ports on the Router’s back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.

Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

To use Wi-Fi Protected Setup, run the Setup Wizard, or refer to the “Wireless > Basic Wireless Settings” section of “Chapter 3: Advanced Configuration”.

Wi-Fi Protected Setup LED (Blue/Amber) It lights up blue when wireless security is enabled. The LED flashes blue for two minutes during Wi-Fi Protected Setup.

The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

The LED flashes amber when a Wi-Fi Protected Setup session is active, and a second session begins. The Router supports one session at a time. Wait until the LED is off before starting the next Wi-Fi Protected Setup session.

Back Panel

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.
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.

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, 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 login 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.

Setup > Basic Setup

The first screen that appears is the Basic Setup screen. This allows you to change the Router’s general settings.
Chapter 3

Advanced Configuration

Static IP

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

Internet 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 IP address of the ISP server.

DNS 1-3 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.

Username and Password Enter the Username and Password provided by your ISP.

Service Name 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 15 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.

If your ISP supports DHCP or you are connecting through a dynamic IP address, then select Obtain an IP Address Automatically. If you are required to use a permanent IP address to connect to the Internet, then select Specify an IP Address. Then configure the following:

- **Specify an 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.
- **Default Gateway** Your ISP will provide you with the IP address of the ISP server.
- **DNS 1-3** Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

**PPTP Server IP Address** Your ISP will provide you with the IP address of the PPTP server.

**Username and Password** Enter the Username 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 **15** 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.

**Telstra Cable**

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

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

**Username and Password** Enter the Username 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 **15** 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.

**Optional Settings**

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

**Host Name and 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 IP**

This presents both the Router’s IP Address and Subnet Mask as seen by your network.

| Router IP | IP Address: 192.168.1.1 | Subnet Mask: 255.255.255.0 |

**DHCP Server Setting**

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.

**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 **Disabled** (no other DHCP features will be available).

**DHCP Reservation** Click this button 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.

- **Select Clients from DHCP Table** Click the Select check box to reserve a client’s IP address. Then click **Add Clients**.
- **Manually Adding Client** 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. Enter its MAC address in the **To This MAC Address** field. Then click **Add**.

**Clients Already Reserved**

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**.

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

**Start 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 Start 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 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**.

**IP Address Range** Displayed here is the range of available IP addresses.
Chapter 3

Advanced Configuration

**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.

**Time Setting**

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

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, **Disabled**.

**DDNS**

**DDNS Service**

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

**DynDNS.org**

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

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

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

**System** Select the DynDNS service you use: **Dynamic**, **Static**, or **Custom**. The default selection is **Dynamic**.

**Mail Exchange (Optional)** Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

**Backup MX** This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, **Disabled**. To enable the feature, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

**Wildcard** This setting enables or disables wildcards for your host. For example, if your DDNS address is myplace.dyndns.org and you enable wildcards, then x.myplace.dyndns.org will work as well (x is the wildcard). To disable wildcards, keep the default, **Disabled**. To enable wildcards, select **Enabled**. If you are not sure which setting to select, keep the default, **Disabled**.

**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 this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.
Chapter 3

Advanced Configuration

TZO.com

Setup > DDNS > TZO

**E-mail Address, TZO Key, 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 this button. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > MAC Address Clone

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

MAC Address Clone

**Enabled/Disabled** To have the MAC Address cloned, select **Enabled**.

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

Clone My PC’s MAC Click this button to 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.

**Advanced Routing**

**NAT**

**Enabled/Disabled** If this Router is hosting your network’s connection to the Internet, keep the default, **Enabled**. If another router exists on your network, select **Disabled**. When the NAT setting is disabled, dynamic routing will be enabled.

**Dynamic Routing (RIP)**

**Enabled/Disabled** 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. When the NAT setting is enabled, the Dynamic Routing feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select **Enabled** to use the Dynamic Routing feature.

**Static Routing**

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.
Route Entries  To set up a static route between the Router and another network, select a number from the drop-down list. 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**

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

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

**Basic Wireless Settings**

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

There are two ways to configure the Router’s wireless network(s), manual and Wi-Fi Protected Setup.

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup.

**Wireless Configuration**  To manually configure your wireless network, select **Manual**. Proceed to the “Basic Wireless Settings” section. To use Wi-Fi Protected Setup, select **Wi-Fi Protected Setup**. Proceed to the “Wi-Fi Protected Setup” section.

**Network Mode**  From this drop-down menu, you can select the wireless standards running on your network. If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, keep the default setting, **Mixed**. If you have only Wireless-G and Wireless-B devices in your network, select **BG-Mixed**. If you have only Wireless-N devices, select **Wireless-N Only**. If you have only Wireless-G devices, select **Wireless-G Only**. If you have only Wireless-B devices, select **Wireless-B Only**. If you do not have any wireless devices in your network, select **Disabled**.

**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 (**Linksys**) 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**. If you are not sure which radio band to select, keep the default, **Auto**.

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

**Wide Channel**  If you selected **Wide - 40MHz Channel** for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu. If you are not sure which channel to select, keep the default, **Auto**.
Standard Channel  If you selected Wide - 40MHz Channel or Standard - 20MHz Channel for the Radio Band setting, then this setting will be available. 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.

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, Enabled. If you do not want to broadcast the Router’s SSID, then select Disabled.

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

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.

**Method #1**

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the Wi-Fi Protected Setup button on the client device.
2. Click the Wi-Fi Protected Setup button on this screen.
3. After the client device has been configured, click OK. Then refer back to your client device or its documentation for further instructions.

**Method #2**

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number in the field on this screen.
2. Click Register.
3. After the client device has been configured, click OK. Then refer back to your client device or its documentation for further instructions.

**Method #3**

Use this method if your client device asks for the Router’s PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click OK. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.

**NOTE:** If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

The Wireless Security screen configures 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 security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

**WPA Personal**

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

**Encryption** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

**Passphrase** Enter a Passphrase of 8-63 characters.

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

**WPA2 Personal**

**Encryption** WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP** or **AES**.

**Passphrase** Enter a Passphrase of 8-63 characters.

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

**WPA Enterprise**

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

**Encryption** WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

**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 Secret** 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. The default Key Renewal period is **3600** seconds.

**WPA2 Enterprise**

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)
Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP or AES. The default is TKIP or AES.

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 Secret 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. The default Key Renewal period is 3600 seconds.

RADIUS

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.)

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.

Encryption Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). The default is 40/64 bits (10 hex digits).

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

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

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

WEP

WEP is a basic encryption method, which is not as secure as WPA.
Chapter 3

Advanced Configuration

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 Client List

This screen shows computers and other devices on the wireless network. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status. Select Save to MAC Address Filter List for any device you want to add to the MAC Address Filter List. Then click Add.

To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the Wireless MAC Filter screen, click Close.

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

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

Wireless > Advanced Wireless Settings

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

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 **Enabled**. AP Isolation is disabled by default.

**Frame Burst** Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, **Enabled**. Otherwise, select **Disabled**.

**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. Select **Shared Key** to only use Shared Key authentication.

**Basic Rate** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the 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 (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps). Other options are **1-2Mbps**, for use with older wireless technology, and **All**, when the Router can transmit at all 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 is **Auto**.

**N Transmission Rate** The rate of data transmission should be set depending on the speed of your Wireless-N networking. You can select from a range of transmission speeds, or you can select **Auto** to have the 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 is **Auto**.

**CTS Protection Mode** The Router will automatically use CTS (Clear-To-Send) 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. The default is **Auto**.

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

**DTIM Interval** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the 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, **2347**, 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. The RTS Threshold value should remain at its default value of **2347**.

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

**Security > Firewall**

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

SPI Firewall Protection To use firewall protection, keep the default selection, Enabled. To turn off firewall protection, select Disabled.

Internet Filter

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. Select this feature to filter multicasting. This feature is not selected by default.

Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It 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 Filter

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

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 this feature to enable Java filtering. Deselect the feature to allow Java usage.

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 this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage.

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

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

Security > VPN Passthrough

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

VP N 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, Enabled.

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, Enabled.

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, Enabled.

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

Access Restrictions > Internet Access

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

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

Summary
The policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, select Enabled. To delete a policy, click Delete. Click Save Settings to save your changes, or click Cancel Changes to cancel your changes. To return to the Internet Access Policy screen, click Close.

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

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

1. Select a number from the Access Policy drop-down menu.
2. Enter a Policy Name in the field provided.
3. To enable this policy, select Enabled.
4. Click Edit List 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 click Cancel Changes to cancel your changes. Then click Close.
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. You can block websites with specific URL addresses. Enter each URL in a separate URL field.
8. You can also block websites using specific keywords. Enter each keyword in a separate Keyword field.
9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.)

From the Applications list, select the application you want to block. Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button.

10. If the application you want to block is not listed or you want to edit a service’s settings, 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 a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click Modify.

To delete a service, select it from the Application list. Then click Delete.

11. Click Save Settings to save the policy’s settings. To cancel the policy’s settings, click Cancel Changes.

**Applications and Gaming > Single Port Forwarding**

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

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen).

**Single Port Forwarding**

Common applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select Enabled to activate this entry.

For additional applications, complete the following fields:

- **Application Name**: Enter the name you wish to give the application. Each name can be up to 12 characters.
- **External Port**: Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.
- **Internal Port**: Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.
- **Protocol**: Select the protocol used for this application, either TCP or UDP, or Both.
- **To IP Address**: For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address.
- **Enabled**: For each application, select Enabled to enable port forwarding.

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

**Applications and Gaming > Port Range Forwarding**

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

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen).

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

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

- **Application Name** In this field, enter the name you wish to give the application. Each name can be up to 12 characters.
- **Start-End Port** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information.
- **Protocol** Select the protocol used for this application, either TCP or UDP, or Both.
- **To IP Address** For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click DHCP Reservation on the Basic Setup screen to look up its static IP address.
- **Enabled** Select Enabled to enable port forwarding for the applications you have defined.

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

**Applications & Gaming > Port Range Triggering**

The Port Range Triggering screen allows the 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.

**Port Range Triggering**

- **Application Name** Enter the application name of the trigger.
- **Triggered Range** For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed.
- **Forwarded Range** For each application, enter the starting and ending port numbers of the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.
- **Enabled** Select Enabled to enable port triggering for the applications you have defined.

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

**Applications and Gaming > DMZ**

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

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

**Enabled/Disabled** To disable DMZ hosting, select **Disabled**. To expose one PC, select **Enabled**. Then configure the following settings:

**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, select and complete the IP address range fields.

**Destination** If you want to specify the DMZ host by IP address, select **IP Address** and enter 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 **DHCP Client Table**.

DHCP Client Table

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 **Select**. To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the DMZ screen, click **Close**.

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

Applications and Gaming > QoS

**Quality of Service (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.

**Wireless**

You can configure the support and No Acknowledgement settings in this section.

**WMM Support** If you have other devices that support Wi-Fi Multimedia (WMM) on your network, keep the default, **Enabled**. Otherwise, select **Disabled**.

**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 select **Enabled**. Otherwise, keep the default, **Disabled**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels of 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. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

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

There are four 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 (Recommend), 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.

Priority Select the appropriate priority: High, Medium (Recommend), 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 (Recommend), Normal, or Low.

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

Ethernet Port

Ethernet Select the appropriate Ethernet port.

Priority Select the appropriate priority: High, Medium (Recommend), 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 (Recommend), 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 column displays the bandwidth priority of High, Medium, Normal, or Low.
Name This column displays the application, device, or port name.
Information This column displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.
Remove Click this button to remove an entry.
Edit Click this button to make changes.
Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

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

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. HTTP is the default.

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 utility via a wired connection if you disable the setting. Keep the default, Enabled, to allow wireless access to the utility, or select Disabled to block wireless access to the utility.

Remote Access
Remote Management To permit remote access of the Router, from outside the local network, select Enabled. Otherwise, keep the default, Disabled.

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. HTTP is the default.

Remote Upgrade If you want to be able to upgrade the Router remotely, from outside the local network, select Enabled. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, Disabled.

Allowed Remote IP Address If you want to be able to access the Router from any external IP address, select Any IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided.

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

NOTE: When you are in a remote location and wish to manage the Router, enter http://<Internet_IP_address>:port or https://<Internet_IP_address>:port, depending on whether you use HTTP or HTTPS. Enter the Router’s specific Internet IP address in place of <Internet_IP_address>, and enter the Remote Management Port number in place of the word port.

UPnP
Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.
UPnP If you want to use UPnP, keep the default setting, Enabled. Otherwise, select Disabled.

Allow Users to Configure Keep the default, Enabled, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select Disabled.

Allow Users to Disable Internet Access Select Enabled, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting, Disabled.

Backup and Restore

Backup Configurations To back up the Router’s configuration settings, click this button and follow the on-screen instructions.

Restore Configurations To restore the Router’s configuration settings, click this button and follow the on-screen instructions. (You must have previously backed up the Router’s configuration settings.)

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

Administration > Log

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

Log

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

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

Ping Test
The Ping test checks the status of a connection.

**IP or URL Address** Enter the address of the PC whose connection you wish to test.

**Packet Size** Enter the packet size you want to use. The default is 32 bytes.

**Times to Ping** Enter many times you wish to test it.

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

Traceroute Test
The Traceroute test tests the performance of a connection.

**IP or URL Address** Enter the address of the PC whose connection you wish to test.

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

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 All Settings** To reset the Router’s settings to the default values, click this button and then follow the on-screen instructions. Any settings you have saved will be lost when the default settings are restored.

Administration > Firmware Upgrade

The Firmware Upgrade screen allows you to upgrade the 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.

**NOTE:** The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.
Firmware Upgrade


Please select a file to upgrade the firmware Click Browse and select the extracted firmware upgrade file.

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

Status > Router

The Router screen displays information about the Router and its current settings.

Router Information

Firmware Version This is the version number of the Router’s current firmware.

Current Time This shows the time set on the Router.

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

Host Name If required by your ISP, this was entered on the Basic Setup screen.

Domain Name If required by your ISP, this was entered on the Basic Setup screen.

Internet Connection

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

Click Refresh to update the on-screen information.

Status > Local Network

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

Local Network

Local MAC Address The MAC address of the Router’s local, wired interface is displayed here.

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

Subnet Mask This shows the Subnet Mask of the Router.

DHCP Server

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 starting 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 Clients Table Click this button to view a list of PCs that are using the Router as a DHCP server.
DHCP Client Table

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 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.

Status > Wireless Network

The Wireless Network screen displays information about your wireless network.

Wireless Network

MAC Address The MAC address of the Router’s local, wireless interface is displayed here.

Mode Displayed here is the wireless mode used by the network.

Network Name (SSID) Displayed here is the name of the wireless network, which is also called the SSID.

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

Wide Channel Shown 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.
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
<td>WRT160N</td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td>Draft 802.11n, 802.11g, 802.11b, 802.3, 802.3u</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td>Power, Internet, and Ethernet</td>
</tr>
<tr>
<td><strong>Buttons</strong></td>
<td>Reset, Wi-Fi Protected Setup</td>
</tr>
<tr>
<td><strong>LEDs</strong></td>
<td>Ethernet (1-4), Wi-Fi Protected Setup, Wireless, Internet, Power</td>
</tr>
<tr>
<td><strong>Cabling Type</strong></td>
<td>CAT 5e</td>
</tr>
<tr>
<td><strong>RF Pwr (EIRP) in dBm</strong></td>
<td>17 dBm</td>
</tr>
<tr>
<td><strong>Antenna Gain in dBi</strong></td>
<td>1.5 dBi</td>
</tr>
<tr>
<td><strong>UPnP able/cert</strong></td>
<td>Able</td>
</tr>
<tr>
<td><strong>Security Features</strong></td>
<td>WEP, WPA, WPA2</td>
</tr>
<tr>
<td><strong>Security Key Bits</strong></td>
<td>128-Bit, 256-Bit</td>
</tr>
</tbody>
</table>

### Environmental

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dimensions</strong></td>
<td>7.95” x 6.3” x 1.34” (202 x 160 x 34 mm)</td>
</tr>
<tr>
<td><strong>Weight</strong></td>
<td>13.40 oz (0.38 kg)</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>12V, 1A</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td>FCC, CE, IC-03, Wi-Fi</td>
</tr>
<tr>
<td><strong>Operating Temp.</strong></td>
<td>0 to 40°C (32 to 104°F)</td>
</tr>
<tr>
<td><strong>Storage Temp.</strong></td>
<td>-20 to 60°C (-4 to 140°F)</td>
</tr>
<tr>
<td><strong>Operating Humidity</strong></td>
<td>10 to 85% Noncondensing</td>
</tr>
<tr>
<td><strong>Storage Humidity</strong></td>
<td>5 to 90% Noncondensing</td>
</tr>
</tbody>
</table>
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 the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion 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.

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 Canadian ICES-003 and RSS210.

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

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Avis d'Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du 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 isotope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

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.

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.

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:

![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.

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

Европейска директива 2002/96/ЕС изисква уредите, носещи този символ ☑️ върху изделието и/или опаковката му, да не се изхвърлят с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Вашата 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 вреди за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обрнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

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

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

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

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

Europos direktyva 2002/96/EC numato, kad įrankos, kurio ir sailingas pakuočė yra pažymėta šiuo simboliu (įvėrskite simbolį), negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia atskirtai nuo bendro buitinio atliekų srauto. Jūs privalote užtikrinti, kad ši iki elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemos. Tinkamai šalintų ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie šį įrankį ir jų šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduočiavus, kuriose įsigijote šį gaminį.

Malti (Maltese) - Informazzjoni Ambjentali ghal Klijenti fl-Unjoni Ewropea


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 alsóbb címke Ő megjelenik, tilos a többi szelektálási tanács megfelelő hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékszállítási hulladékkal együtt kidobni. A megfelelő hulladékfeldolgozás segít a környezet és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgáltattal, 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 �DataService 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.

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

Dyrekczywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem ╌ znajdujący 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 domowymi. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w sposób odrębny wskazany przez władze lokalne. Pozbywanie się sprzętu we właściwy sposób oraz 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.

Wireless-N Broadband Router
Appendix D

Regulatory Information

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 eletrónico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem corretas 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


Slovenčina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej unii

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 odvodené od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenie prostredníctvom špecializovaných zbieriek zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie fúdi. Ak máte záujem o podrobnéjsie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaobľučujúce 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 odvriči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbiralnišča, 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


Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen


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