

How do I get mIRC to work with the Router?

Under the Port Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

Can the Router act as my DHCP server?

Yes. The Router has DHCP server software built-in.

Can I run an application from a remote computer over the wireless network?

This will depend on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

What is the IEEE 802.11a standard?

It is one of the IEEE standards for wireless networks. The 802.11a standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11a standard. The 802.11a standard states a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

What is the IEEE 802.11b standard?

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

What is the IEEE 802.11g standard?

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

What IEEE 802.11a features are supported?

The product supports the following IEEE 802.11a functions:

- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation

What IEEE 802.11b features are supported?

The product supports the following IEEE 802.11b functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is ad-hoc mode?

When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured to communicate directly with each other. The ad-hoc wireless network will not communicate with any wired network.

What is infrastructure mode?

When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

What is roaming?

Roaming is the ability of a portable computer to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the user must make sure that the workstation uses the same channel number as the access point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next

selects the right access point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

What is ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all

Dual-Band Wireless A+G Broadband Router

practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs onto the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I reset the Router?

Press the Reset button on the back panel for about five seconds. This will reset the Router to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between the Router and a wireless PC will create signal loss. Lead glass, metal, concrete floors, water and walls will inhibit the signal and reduce range. Start with the Router and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel.

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

Appendix B: Wireless Security

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

Security Precautions

The following is a complete list of security precautions to take (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

For information on implementing these security features, refer to “Chapter 5: Configuring the Dual-Band Wireless A+G Broadband Router.”

Security Threats Facing Wireless Networks

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

Change the administrator’s password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator’s password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator’s password regularly.



Note: Some of these security features are available only through the network router or access point. Refer to the router or access point’s documentation for more information.

SSID. There are several things to keep in mind about the SSID:

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

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

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

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

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

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

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.



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

Dual-Band Wireless A+G Broadband Router

WPA Pre-Shared Key. If you do not have a RADIUS server, Select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

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

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Upgrading Firmware

The Broadband Router's firmware is upgraded through the Web-based Utility's Administration tab. 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 will lose all of 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.

To upgrade the Router's firmware, follow these instructions:

1. Download the firmware from Linksys's website at www.linksys.com. Then extract the firmware file.
2. Click **Firmware Upgrade** from the Web-Utility's Administration tab, and the *Upgrade Firmware* screen will appear.
3. Enter the location of the extracted firmware file or click the **Browse** button to find the file.
4. Then click the **Start to Upgrade** button and follow the on-screen instructions.

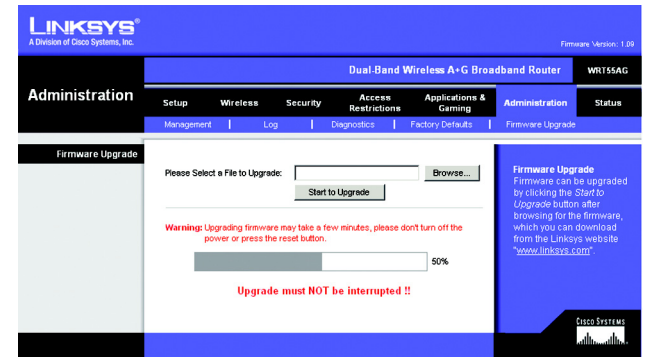


Figure C-1: Administration Tab - Firmware Upgrade

Appendix D: Windows Help

Almost all Linksys wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with the Broadband Router, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98SE or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter `winipcfg`. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a Category 5 Ethernet network cable.
3. Write down the Adapter Address as shown on your computer screen. This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.

The MAC address/Adapter Address is what you will use for MAC address cloning or MAC filtering.

The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

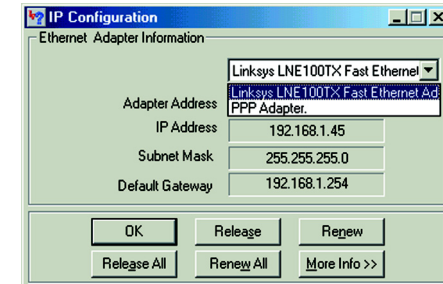


Figure E-1: IP Configuration Screen

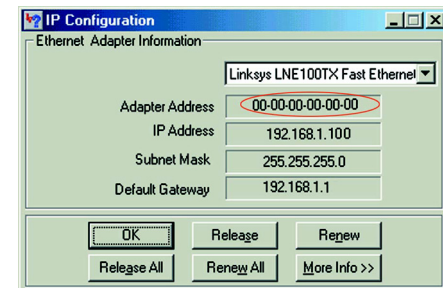


Figure E-2: MAC Address/Adapter Address



Note: The MAC address is also called the Adapter Address.

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter `cmd`. Press the **Enter** key or click the **OK** button.
2. At the command prompt, enter `ipconfig /all`. Then press the **Enter** key.

Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter
Windows 98SE or Me Instructions

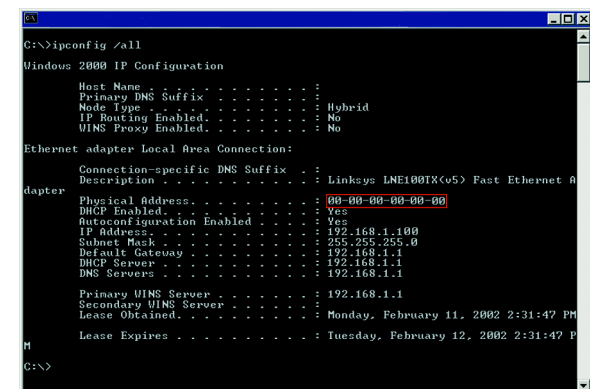


Figure E-3: MAC Address/Physical Address

- Write down the Physical Address as shown on your computer screen (Figure E-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.



Note: The MAC address is also called the Physical Address.

The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

For the Router's Web-based Utility

For MAC filtering, enter the 12-digit MAC address.

For MAC address cloning, enter the 12-digit MAC address in the *MAC Address* fields provided, two digits per field.

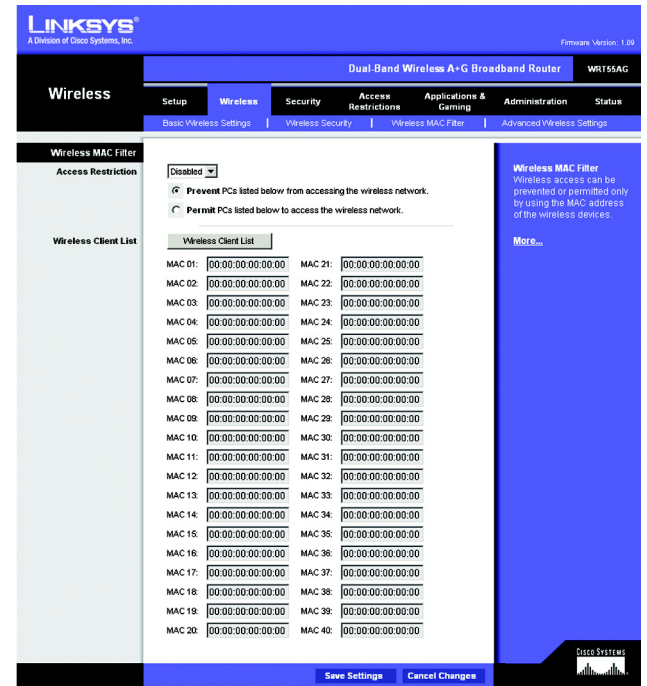


Figure E-4: Wireless MAC Filter List

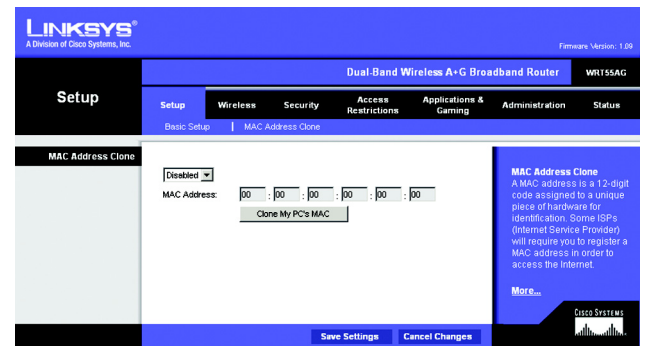


Figure E-5: MAC Address Clone

Appendix F: Glossary

802.11a - A wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

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

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

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (Advanced Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

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

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

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

Bridge - A device that connects different networks.

Broadband - An always-on, fast Internet connection.

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

Dual-Band Wireless A+G Broadband Router

Buffer - A shared or assigned memory area that is used to support and coordinate different computing and networking activities so one isn't held up by the other.

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

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

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data collisions.

CTS (Clear To Send) - A signal sent by a wireless device, signifying that it is ready to receive data.

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

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

Dual-Band Wireless A+G Broadband Router

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

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

EAP (Extensible Authentication Protocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

EAP-PEAP (Extensible Authentication Protocol-Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) - A mutual authentication method that uses digital certificates.

Encryption - Encoding data transmitted in a network.

Ethernet - A networking protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

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

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

Dual-Band Wireless A+G Broadband Router

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

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

LEAP (Lightweight Extensible Authentication Protocol) - A mutual authentication method that uses a username and password system.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

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

mIRC - An Internet Relay Chat program that runs under Windows.

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

NNTP (Network News Transfer Protocol) - The protocol used to connect to Usenet groups on the Internet.

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - Frequency transmission that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel to prevent information from being lost in transit.

Packet - A unit of data sent over a network.

Dual-Band Wireless A+G Broadband Router

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

PEAP (Protected Extensible Authentication Protocol) - A mutual authentication method that uses a combination of digital certificates and another system, such as passwords.

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

POP3 (Post Office Protocol 3) - A standard mail server commonly used on the Internet.

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

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

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RADIUS (Remote Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (Request To Send) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Dual-Band Wireless A+G Broadband Router

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

SPI (Stateful Packet Inspection) Firewall - A technology that inspects incoming packets of information before allowing them to enter the network.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set Identifier) - Your wireless network's name.

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

Static Routing - Forwarding data in a network via a fixed path.

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

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (Transmission Control Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (Trivial File Transfer Protocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (Temporal Key Integrity Protocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

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

Dual-Band Wireless A+G Broadband Router

Upload - To transmit a file over a network.

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

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network)- The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Me utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (Wi-Fi Protected Access) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix G: Specifications

Model	WRT55G
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11a, IEEE 802.11g, IEEE 802.11b
Ports	Internet: One 10/100 RJ-45 Port for Cable/DSL Modem LAN: Four 10/100 RJ-45 Switched Ports One Power Port
Button	One Reset Button
Cabling Type	UTP CAT 5 Ethernet Cable or Better
LEDs	Power, DMZ, Internet, Ethernet (1, 2, 3, 4) Wireless-A: WLAN, Wireless-G: WLAN
Dimensions (W x H x D)	7.32" x 1.89" x 6.89" (186 mm x 48 mm x 175 mm)
Unit Weight	0.88 lbs. (0.4 kg)
Power	External, 5V DC, 2.5A
Certifications	FCC
Operating Temp.	0° C to 40° C (32° F to 104° F)
Storage Temp.	-20° C to 70° C (-4° F to 158° F)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Warranty	3-Year Limited

Appendix H: Warranty Information

LIMITED WARRANTY

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

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

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

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

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

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

Appendix I: Regulatory Information

FCC STATEMENT

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

Reorient or relocate the receiving antenna

Increase the separation between the equipment or devices

Connect the equipment to an outlet other than the receiver's

Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

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

Linksys declares that WRT55AG ver. 2 (FCC ID: Q87-WRT55AGV2) is limited in CH1~CH11 for 2.4GHz by specified firmware controlled in U.S.A..

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003, RSS210.

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

The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys declares that this product conforms to the specifications listed below, following the provisions of the European R&TTE directive 1999/5/EC:

EN 301 489-1, 301 489-17 General EMC requirements for Radio equipment.

EN 609 50 Safety

Appendix I: Regulatory Information

•This device complies with Part 15 of the FCC Rules. □
Operation is subject to the following two conditions: (1) This □
device may not cause harmful interference, and (2) this □
device must accept any interference received, including □
interference that may cause undesired operation.□
•FCC Caution: Any changes or modifications not expressly □
approved by the party responsible for compliance could void □
the user's authority to operate this equipment.□

•If this device is going to be operated in 5.15 ~ 5.25GHz □
frequency range, then it is restricted in indoor environment only.
•This transmitter must not be co-located or operating in □
conjunction with any other antenna or transmitter.□

IC Statement□

1.Operation is subject to the following two conditions:□
1) this device may not cause interference and□
2) this device must accept any interference, including interference that □
may cause undesired operation of the device.□
To reduce potential radio interference to other users, the antenna type □
and its gain should be so chosen that the EIRP is not more than required □
for successful communication.□
To prevent radio interference to the licensed service (i.e. co-channel □
Mobile Satellite systems) this device is intended to be operated indoors □
and away from windows to provide maximum shielding. Equipment (or its □
transmit antenna) that is installed outdoors is subject to licensing.□
Because high power radars are allocated as primary users (meaning □
they have priority) in 5250-5350 MHz, these radars could cause □
interference and/or damage to license exempt LAN devices.□

Dual-Band Wireless A+G Broadband Router

EN 300-328-1, EN 300-328-2 Technical requirements for Radio equipment.

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local Authority for procedure to follow.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC.

For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys vakuuttaa täten että dieses produkt tyypinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys déclare que le produit est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC.

Belgique:

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France:

2.4 GHz Bande : les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complètement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le département. L'utilisation en extérieur est soumise à autorisation préalable et très restreinte.

Vous pouvez contacter l'Autorité de Régulation des Télécommunications (<http://www.art-telecom.fr>) pour de plus amples renseignements.

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.

Appendix J: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:

<http://www.linksys.com> or
[ftp.linksys.com](ftp://ftp.linksys.com)

Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:
Or fax your request in to:

800-546-5797 (LINKSYS)
949-823-3002

If you experience problems with any Linksys product, you can call us at:
Don't wish to call? You can e-mail us at:

800-326-7114
support@linksys.com

If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at:
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)

949-823-3000