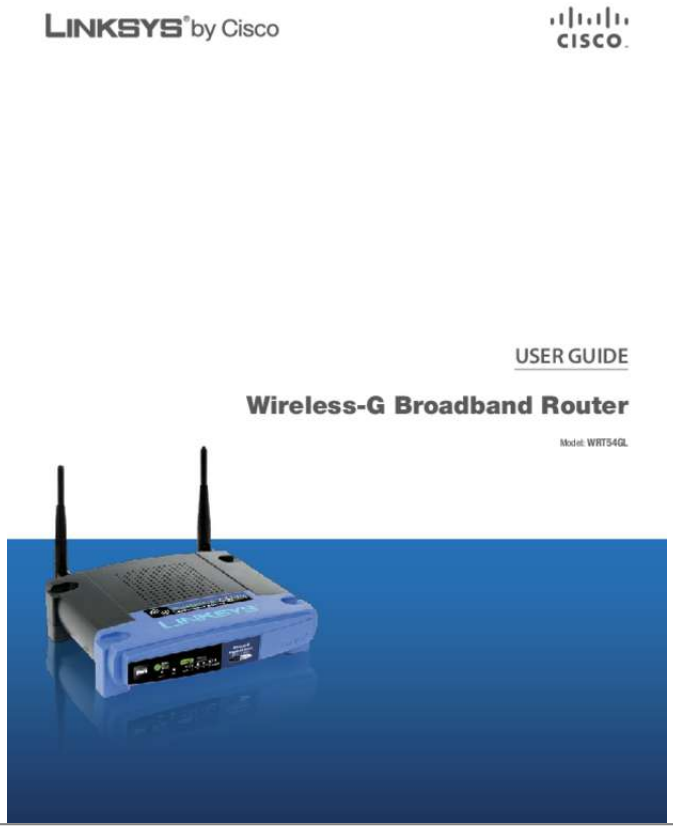

Manual abstract:

S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders. Wireless-G Broadband Router i Table of Contents Chapter 1: Product Overview 3 Front Panel . . . . .

. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . 3 Back Panel . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. 3 Chapter 2: Wireless Security Checklist 4 General Network Security Guidelines . . . .
. . . . . .

. . . . . .
. . . . .
. . . . 4 Additional Security Tips .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. 4 Chapter 3: Advanced Configuration 5 Setup > Basic Setup . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. 5 Setup > DDNS . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . . 8 Setup > MAC Address Clone . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . 9 Setup > Advanced Routing . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . 10 Wireless > Basic Wireless Settings . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . 10 Wireless > Wireless Security . . .

. . . . .
. . . . . .

. . . . . .
. . . . 27 Safety Notices .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. 27 Industry Canada Statement . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
27 Wireless-G Broadband Router i Table of Contents Avis d'Industrie Canada . . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. 28 Wireless Disclaimer . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . 28 Avis de non-responsabilité concernant les appareils sans fil . . . . .
. . . . .
. . . . .
. . . 28 User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) . . . . . .

. . . . . .
. . . . .
. . . . .
. . 29 Appendix E: Software License Agreement 33 Software in Linksys Products . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

33 Software Licenses . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . . .
. . . . .
33 Wireless-G Broadband Router ii Chapter 1 Product Overview Power (Green) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its selfdiagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit. DMZ (Green) The DMZ LED indicates when the DMZ function is being used. This LED will remain lit as long as DMZ is enabled. WLAN (Green) The WLAN LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network. 1, 2, 3, 4 (Green) 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. Internet (Green) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port. Chapter 1: Product Overview Thank you for choosing the Linksys Wireless-G Broadband Router. The Router lets you access the Internet via a wireless connection, broadcast at up to 54 Mbps, 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 SecureEasySetup (Orange/White) The Cisco logo is the Router's SecureEasySetup button. It lights up and will stay orange when the Router is powered on. The color orange indicates that the Router is not using the SecureEasySetup feature, while the color white indicates that the Router is using the SecureEasySetup feature. When the Router enters SecureEasySetup mode, the Cisco logo will turn white and start flashing.

After the Router has generated the SSID and WPA Personal key, the Cisco logo will stop flashing and stay white. To clear the SSID and WPA Personal key, press and hold down the Cisco logo for five seconds. The Cisco logo will flash slowly as the Router resets itself.

The Cisco logo will turn orange to indicate a successful reset. NOTE: SecureEasySetup is a feature that makes it easy to set up your wireless network. If you have SecureEasySetup devices, run the Router's Setup Wizard CD-ROM and follow the onscreen instructions to use SecureEasySetup. Back Panel 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.

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. Power The Power port is where you will connect the power adapter. Wireless-G Broadband Router 3 Chapter 2 Wireless Security Checklist 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. 4. Enable encryption Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. Currently, devices that are Wi-Fi certified are required to support WPA2, but are not required to support WEP. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment. WEP is an older encryption standard and may be the only option available on some older devices that do not •• WRT54GL User Guide support WPA. 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 Wireless network security is useless if the underlying to 32 characters in length. Linksys wireless products network is not secure. use linksys as the default wireless network name. You should change the wireless network name to something •• Password protect all computers on the network and unique to distinguish your wireless network from other individually password protect sensitive files. wireless networks that may exist around you, but do not •• Change passwords on a regular basis. use personal nnecting through a dynamic IP address. (This option usually applies to cable connections.) Password Screen Setup > Basic Setup The first screen that appears is the Basic Setup screen. This allows you to change the Router's general settings. Internet Connection Type > Automatic Configuration - DHCP Wireless-G Broadband Router 5 Chapter 3 Advanced Configuration before your Internet connection terminates.

The default Max Idle Time is 5 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection.

The default Redial Period is 30 seconds. Static IP If you are required to use a permanent IP address to connect to the Internet, select Static IP. PPTP Internet Connection Type > 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. Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address. DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address. Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only. Internet Connection Type > PPTP PPPoE Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. Internet 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. Gateway Your ISP will provide you with the Gateway Address. User Name and Password Enter the User Name and Password provided by your ISP. Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection.

To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default value is 30 seconds. 6 Internet Connection Type > PPPoE User Name and Password Enter the User Name 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 Wireless-G Broadband Router Chapter 3 Advanced Configuration Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again.

To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds. L2TP L2TP is a service that applies to connections in Israel only. Internet Connection Type > L2TP User Name and Password Enter the User Name and Password provided by your ISP. L2TP Server This is the IP address of the L2TP Server.

Your ISP will provide you with the IP Address you need to specify here. Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds.

Optional Settings Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Optional Settings Router Name In this field, you can enter a name of up to 39 characters to represent the Router. Host Name/Domain Name These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification.

You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work. MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted.

To have the Router select the best MTU for your Internet connection, keep the default setting, Auto. Telstra Cable Telstra Cable is a service that applies to connections in Australia only. Internet Connection Type > Telstra Cable User Name and Password Enter the User Name and Password provided by your ISP. Heart Beat Server This is the IP address of the Heartbeat Server. Your ISP will provide you with the IP Address you need to specify here. Wireless-G Broadband Router 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: WRT54GL User Guide •• DHCP, Static IP, or Telstra: 1500 •• PPPoE: 1492 7 Chapter 3 Advanced Configuration 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. •• 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 Address Time Setting Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.) Network Address Server Settings (DHCP) The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network.

If you choose to enable the Router's DHCP server option, make sure there is no other DHCP server on your network. Time Setting Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Setup > DDNS The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

Network Address Server Settings (DHCP) DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select Disable (no other DHCP features will be available). Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.

168.1.253. The default Starting IP Address is 192.168.1.100. Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will Wireless-G Broadband Router Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.

dyndns.org or www.
TZO.com. If you do not want to use this feature, keep the default setting, Disable. DDNS DDNS Service If your DDNS service is provided by DynDNS.org, then select DynDNS.
org from the drop-down menu. If your DDNS service is provided by TZO, then select TZO.com. The features available on the DDNS screen will vary, depending on which DDNS service provider you use. 8 Chapter 3 Advanced Configuration TZO.com DynDNS.org Setup > DDNS > TZO Setup > DDNS > DynDNS E-mail Address, Password, and Domain Name Enter the settings of the account you set up with TZO. Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change. Status The status of the DDNS service connection is displayed here.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. System Select the DynDNS service you use: Dynamic, Static, or Custom. The default selection is Dynamic. User Name Enter the User Name for your DDNS account. Password Enter the Password for your DDNS account. Host Name The is the DDNS URL assigned by the DDNS service. 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, No. To enable the feature, select Yes.
If you are not sure which setting to select, keep the default, No. 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, Off. To enable wildcards, select On.
If you are not sure which setting to select, keep the default, Off. 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. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Setup > MAC Address Clone A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature. Setup > MAC Address Clone MAC Address Clone Enable/Disable To have the MAC Address cloned, select Enable. User Defined Entry Enter the MAC Address registered with your ISP here.

Clone Your PC's MAC Clicking this button will clone the MAC address of the computer you are using. Wireless-G Broadband Router 9 Chapter 3 Advanced Configuration exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is Disabled by default. From the drop-down menu, you can also select LAN & Wireless, which performs dynamic routing over your Ethernet and wireless networks. You can also select WAN (Internet), which performs dynamic routing with data coming from the Internet. Selecting Both enables dynamic routing for both networks, as well as data from the Internet. 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. Static Routing Select set number To set up a static route between the Router and another network, select a number from the drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route.
(Click Delete This Entry to delete a static route.) Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters. Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route. Setup > Advanced Routing (Gateway) 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. Default 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. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Basic Wireless Settings Setup > Advanced Routing (Router) Advanced Routing Operating Mode Select the mode in which this Router will function. If this Router is hosting your network's connection to the Internet, select Gateway. If another Router exists on your network, select Router. When Router is chosen, Dynamic Routing will be available as an option. The basic settings for wireless networking are set on this screen. Dynamic Routing RIP This feature enables the Router to automatically adjust to physical changes in the network's layout and Wireless-G Broadband Router 10 Chapter 3 Advanced Configuration Wireless > Wireless Security The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP.

(WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security." Wireless > Basic Wireless Settings Wireless Network Wireless Network Mode From this drop-down menu, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices in your network, keep the default setting, Mixed. If you have only 802.11g devices, select G-Only.
If you have only 802.11b devices, select B-Only. If you do not have any 802.11g and 802.11b devices in your network, select Disable.
Wireless Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network.

It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID (linksys) to a unique name.
Wireless Channel Select the appropriate channel from the list provided to correspond with your network settings. All devices in your wireless network must use the same channel in order to communicate. Wireless SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, Enable. If you do not want to broadcast the Router's SSID, then select Disable. SecureEasySetup If you did not utilize this network connection feature during the Setup Wizard, you may use it here by clicking the green logo. When you are prompted to start the push button setup, click OK. Reset Security Use this button to reset the security settings on your network. You will need to run SecureEasySetup again on each device on your network to re-associate it with your network. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

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. Security Mode > WPA Personal WPA Algorithm WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, TKIP or AES. The default is TKIP. WPA Shared Key Enter a WPA Shared Key of 8-63 characters. Group Key Renewal Enter a Group 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.) 11 Wireless-G Broadband Router Chapter 3 Advanced Configuration 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.) Security Mode > WPA Enterprise WPA Algorithm 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 Address Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Enter the key shared between the Router and the server.
Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is 3600 seconds. Security Mode > WPA2 Enterprise WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES, or TKIP + AES. The default selection is TKIP + AES RADIUS Server Address Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Enter the key shared between the Router and the server. Key Renewal Timeout Enter a Key Renewal Timeout period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is 3600 seconds.

WPA2 Personal 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.) Security Mode > WPA2 Personal WPA Algorithm WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES, or TKIP + AES. The default selection is TKIP + AES. WPA Shared Key Enter a WPA Shared Key of 8-63 characters. Group Key Renewal Enter a Group Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Group Key Renewal period is 3600 seconds. Security Mode > RADIUS Wireless-G Broadband Router 12 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. 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.
RADIUS Server Address Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Enter the key shared between the Router and the server. Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is 1. WEP Encryption Select a level of WEP encryption, 64 bits 10 hex digits or 128 bits 26 hex digits. The default is 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. Wireless > Wireless MAC Filter Wireless MAC Filter Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click Enable. If you do not wish to filter users by MAC Address, keep the default setting, Disable. Prevent Select this to block wireless access by MAC Address. This button is selected by default. Permit Only Select this to allow wireless access by MAC Address. This button is not selected by default. Edit MAC Filter List Click this to open the MAC Address Filter List screen. On this screen, you can list users, by MAC Address, to whom you wish to provide or block access. For easy reference, click Wireless Client MAC List to display a list of network users by MAC Address.

WEP WEP is a basic encryption method, which is not as secure as WPA. Security Mode > WEP Default Transmit Key Select a Default Transmit Key (choose which Key to use). The default is 1. WEP Encryption Select a level of WEP encryption, 64 bits 10 hex digits or 128 bits 26 hex digits. The default is 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. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless-G Broadband Router MAC Address Filter List Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.
13 Chapter 3 Advanced Configuration to transmit to the Router in an environment with heavy 802.

11b traffic. This function boosts the Router's ability to catch all Wireless-G transmissions but will severely decrease performance. Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To turn on the Frame Burst option, select Enable.

The default is Disable. Beacon Interval The default value is 100. 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.

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. 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 On. AP Isolation is turned Off by default. SecureEasySetup This feature allows you to enable or disable the SecureEasySetup feature.

Select Disabled to disable the feature and turn off the button's light. The feature is Enabled by default. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Advanced Wireless Settings This Wireless > Advanced Wireless Settings screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Wireless > Advanced Wireless Settings Advanced Wireless Authentication Type The default is set to Auto, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication. Basic Rate The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used.

The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the Router can transmit at all standard wireless rates (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 value is Auto.

CTS Protection Mode CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able Wireless-G Broadband Router 14 Chapter 3 Advanced Configuration Security > VPN Passthrough The Security > VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall. Security > Firewall The Security > Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network. Security > Firewall Security > VPN Passthrough Firewall Firewall Protection To use firewall protection, keep the default selection, Enable. To turn off firewall protection, select Disable. VPN Passthrough IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default, Enable. PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enable. L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enable.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Block WAN Requests Block Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests. Filter Multicast Multicasting allows for multiple transmissions to specific recipients at the same time.

If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. This feature is selected by default. Deselect this feature to disable it. Filter Internet NAT Redirection This feature uses port forwarding to block access to local servers from local networked computers. Select Filter Internet NAT Redirection to filter Internet NAT redirection.

This feature is not selected by default. Filter IDENT (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network.

This feature is selected by default. Deselect this feature to disable it. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless-G Broadband Router 15 Chapter 3 Advanced Configuration 2. To enable this policy, select Enable. 3. Enter a Policy Name in the field provided. 4.

Click Edit List of PCs to select which PCs will be affected by the policy. The List of PCs screen appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click Save Settings to apply your changes or Cancel Changes to cancel your changes. Then click Close. Access Restrictions > Internet Access The Access Restrictions > 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. List of PCs 5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen. Access Restrictions > Internet Access Internet Access Internet Access Policy Access can be managed by a policy.
Use the settings on this screen to establish an access policy (after Save Settings is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click Delete. To view all the policies, click Summary. (Policies can be deleted from the Summary screen by selecting the policy or policies and clicking Delete.
To return to the Internet Access tab, click Close.) 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. Select any Blocked Services or Website Blocking you wish to use. 8. Click Save Settings to save the policy's settings, or click Cancel Changes to cancel the policy's settings. Blocked Services You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the drop-down menus next to Blocked Services. (You can block up to 20 services.) Then enter the range of ports you want to filter. If the service you want to block is not listed or you want to edit a service's settings, then click Add/Edit Service. Then the Port Services screen will appear. Internet Policy Summary Status Policies are disabled by default.

To enable a policy, select the policy number from the drop-down menu, and select Enable. To create an Internet Access policy: 1. Select a number from the Internet Access Policy dropdown menu. Wireless-G Broadband Router Port Services 16 Chapter 3 Advanced Configuration Port Range Forward To forward a port, enter the information on each line for the criteria required. Application In this field, enter the name you wish to give the application. Each name can be up to 12 characters. Start/End This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column. Protocol Select the protocol used for this application, either TCP or UDP, or Both. IP Address For each application, enter the IP Address of the PC running the specific application.
Enable Select Enable to enable port forwarding for the relevant application. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. To add a service, enter the service's name in the Service Name field. Select its protocol from the Protocol dropdown menu, and enter its range in the Port Range fields. Then click Add.
To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click Modify. To delete a service, select it from the list on the right. Then click Delete.
When you are finished making changes on the Port Services screen, click Apply to save the changes. If you want to cancel your changes, click Cancel. To close the Port Services screen and return to the Access Restrictions screen, click Close. Website Blocking by URL Address If you want to block websites with specific URL addresses, enter each URL in a separate field next to Website Blocking by URL Address. Website Blocking by Keyword If you want to block websites using specific keywords, enter each keyword in a separate field next to Website Blocking by Keyword. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Applications & Gaming > Port Triggering The Applications & Gaming > Port Triggering screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. Applications and Gaming > Port Range Forward The Applications & Gaming > Port Range Forward screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming.

Some Internet applications may not require any forwarding.) Applications and Gaming > Port Triggering Port Triggering Application Enter the application name of the trigger. Triggered Range For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. Applications and Gaming > Port Range Forward Wireless-G Broadband Router 17 Chapter 3 Advanced Configuration Applications and Gaming > QoS Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing. There are three types of QoS available: Device Priority, Ethernet Port Priority, and Application Priority. Start Port Enter the starting port number of the Triggered Range. End Port Enter the ending port number of the Triggered Range. Forwarded Range For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.
Start Port Enter the starting port number of the Forwarded Range. End Port Enter the ending port number of the Forwarded Range. Enable Select Enable to enable port triggering for the applicable application. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wired QoS Enable/Disable To enable QoS, select Enable.
Otherwise, select Disable. QoS is disabled by default.

Upstream Bandwidth Select Auto or Manual from the drop-down menu. Manual allows you to specify the maximum outgoing bandwidth that applications can utilize. Applications and Gaming > DMZ The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing.

DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forward feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. Applications and Gaming > DMZ DMZ 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. To expose one PC, select Enable. Then, enter the computer's IP address in the DMZ Host IP Address field. This feature is disabled by default. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Applications and Gaming > QoS Device Priority Enter the name of your network device in the Device name field, enter its MAC Address, and then select its priority from the drop-down menu. Ethernet Port Priority Ethernet Port Priority QoS allows you to prioritize performance for the Router's four ports, LAN Ports 1-4. For each port, select the priority and flow control setting.

Wireless-G Broadband Router 18 Chapter 3 Advanced Configuration Priority Select High or Low in the Priority column. The Router's four ports have been assigned low priority by default. Flow Control If you want the Router to control the transmission of data between network devices, select Enabled. To disable this feature, select Disabled. Ethernet Port Priority QoS does not require support from your ISP because the prioritized ports LAN ports 1-4 are in your network. This feature is enabled by default. Application Priority Application Priority QoS manages information as it is transmitted and received. Depending on the settings of the QoS screen, this feature will assign information a high or low priority for the applications that you specify. Optimize Gaming Applications Select this to automatically allow common game application ports to have a higher priority. These games include, but are not limited to: Counter-Strike, Half-Life, Age of Empires, Everquest, Quake2/Quake3, and Diablo II.

The default setting is unselected. Application Name Enter the name you wish to give the application in the Application Name field. Priority Select High or Low to assign priority to the application. The default selection is Low. Specific Port # Enter the port number for the application.

Administration > Management Router Password Local Router Access Router Password Enter a new Password for the Router. Re-enter to confirm Enter the Password again to confirm. Web Access Access Server HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select HTTP or HTTPS.

The default selection is HTTP. Wireless Access Web If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, Enable, to enable wireless access to the Router's web-based utility, or select Disable to disable wireless access to the utility. Wireless QoS WMM Support Wi-Fi Multimedia (WMM), formerly known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance certified feature, based on the IEEE 802.11e standard. This feature provides QoS to wireless networks. It is especially suitable for voice, music and video applications; for example, Voice over IP (VoIP), video streaming, and interactive gaming. If you have other devices on your wireless network that support WMM, select Enabled. Otherwise, keep the default, Disabled.

No Acknowledgement This feature prevents the Router from re-sending data if an error occurs. To use this feature, select Enabled. Otherwise, keep the default setting, Disabled. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Remote Router Access Remote Management To access the Router remotely, from outside the network, select Enable. Management Port Enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual. Use https To require the use of HTTPS for remote access, select this feature. Administration > Management The Administration > Management screen allows the network's administrator to manage specific Router functions for access and security. UPnP UPnP Keep the default, Enable to enable the UPnP feature; otherwise, select Disable.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless-G Broadband Router 19 Chapter 3 Advanced Configuration Administration > Log The Router can keep logs of all traffic for your Internet connection. The Ping Test Administration > Log Traceroute Test Traceroute To test the performance of a connection, click Traceroute to open the Traceroute Test screen. Enter the address of the PC whose connection you wish to test and click Traceroute. The Traceroute Test screen will show if the test was successful.

To stop the test, click Stop. Click Clear Log to clear the screen. Click Close to return to the Diagnostics screen. Log Log To disable the Log function, keep the default setting, Disable. To monitor traffic between the network and the Internet, select Enable.

When you wish to view the logs, click Incoming Log or Outgoing Log, depending on which you wish to view. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Administration > Diagnostics The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components. The Traceroute Test Administration > Factory Defaults The Administration > Factory Defaults screen allows you to restore the Router's configuration to its factory default settings. Administration > Diagnostics Factory Defaults Restore Factory Defaults To reset the Router's settings to the default values, select Yes, and then click Save Settings. Any settings you have saved will be lost when the default settings are restored. Ping Test Ping The Ping test checks the status of a connection. Click Ping to open the Ping Test screen. @@Then, click Ping. The Ping Test screen will show if the test was successful.

To stop the test, click Stop. Click Clear Log to clear the screen. @@@@linksys.

com. @@@@Current Time This shows the time, as you set on the Setup tab.
@@Start IP Address For the range of IP Addresses used by devices on your local, Ethernet network, the beginning of that range is shown here. End IP Address For the range of IP Addresses used by devices on your local, Ethernet network, the end of that range is shown here. DHCP Clients Table Clicking this button will open a screen to show you which PCs are utilizing the Router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a Delete box and clicking the Delete button. DHCP Clients Table Click Refresh to update the on-screen information.
Wireless-G Broadband Router 22 Appendix A Troubleshooting 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, insert the setup CD into your computer, and then 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 WRT54GL User Guide 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, leave the User name field blank and enter the password to the Router (the default is admin). Click the appropriate tab to change the settings. 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, insert the setup CD into your computer, and then follow the on-screen instructions. WEB: If your questions are not addressed here, refer to the Linksys website, www.linksys.com. Wireless-G Broadband Router 23 Appendix B Specifications Appendix B: Specifications Model Standards Channels Ports Button Cabling Type LEDs RF Power Output UPnP able/cert Security Features Wireless Security WRT54GL IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b 11 Channels (US, Canada) 13 Channels (Europe, Japan) Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port Reset, SecureEasySetup CAT5 Power, DMZ, WLAN, LAN (1-4), Internet, SecureEasySetup 18 dBm Able Stateful Packet Inspection (SPI) Firewall, Internet Policy Wi-Fi Protected Access™2 (WPA2), WEP, Wireless MAC Filtering 7.

32" x 1.89" x 6.06" (186 x 48 x 154 mm) 13.8 oz (391 g) External, 12V DC, 0.5A FCC, ICES-003, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM 32 to 104ºF (0 to 40ºC) -4 to 158ºF (-20 to 70ºC) 5 to 90%, Noncondensing Environmental Dimensions Weight Power Certifications Operating Temp. Storage Temp. Storage Humidity Operating Humidity 10 to 85%, Noncondensing Wireless-G Broadband Router 24 Appendix C Warranty Information service offerings. This limited warranty shall not apply to such third party software or service offerings.
This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require. TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY 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, BUT NOT LIMITED TO, 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 limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.
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 limited warranty 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. Appendix C: Warranty Information Limited Warran WRT54GL User Guide ty Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified below: •• One (1) year for new product •• Ninety (90) days for refurbished product This limited warranty is non-transferable and extends only to the original end-user purchaser.
Your exclusive remedy and Linksys' entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates.