



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WRT54GC. You'll find the answers to all your questions on the LINKSYS WRT54GC in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual LINKSYS WRT54GC
User guide LINKSYS WRT54GC
Operating instructions LINKSYS WRT54GC
Instructions for use LINKSYS WRT54GC
Instruction manual LINKSYS WRT54GC

LINKSYS® by Cisco



USER GUIDE

**Compact Wireless-G
Broadband Router**

Model: WRT54GC (EU)



[You're reading an excerpt. Click here to read official LINKSYS WRT54GC user guide](http://yourpdfguides.com/dref/2353577)
<http://yourpdfguides.com/dref/2353577>

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. A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment. WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA. 1. Change the default wireless network name or SSID Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use linksys as the default wireless network name.

You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.



[You're reading an excerpt. Click here to read official LINKSYS](#)

[WRT54GC user guide](#)

<http://yourpdfguides.com/dref/2353577>

General Network Security Guidelines Wireless network security is useless if the underlying network is not secure. . . . Password protect all computers on the network and individually password protect sensitive files. Change passwords on a regular basis. Install anti-virus software and personal firewall software. Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge. 2. Change the default password For wireless products such as access points, routers, and gateways, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory.

The Linksys default password is admin. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess. Additional Security Tips . . . Keep wireless routers, access points, or gateways away from exterior walls and windows. Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).

Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary. . 3. Enable MAC address filtering Linksys routers and gateways give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device.

With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network. Compact Wireless-G Broadband Router WEB: For more information on wireless security, visit www.linksys.com/security 5 Chapter 3 Advanced Configuration Chapter 3: Advanced Configuration After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. However, if you'd like to change its advanced settings, use the Router's web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router. The web-based utility has these main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

NOTE: When first installing the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility. Setup > Basic Setup Internet Setup The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. Internet Connection Type > PPPoE User Name and Password Enter the User Name and Password provided by your ISP. 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. If your ISP charges you by the amount of time you are connected to the internet, you should use this option. 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, Compact Wireless-G Broadband Router 7 Chapter 3 Advanced Configuration Host Name/Domain Name These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, Auto. Size When Manual is selected in the MTU field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type: . DHCP or Static IP: 1500 . PPPoE: 1492 . PPTP: 1460 . L2TP: 1452 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. Default Gateway This is the IP address of the L2TP Server. Your ISP will provide you with the IP Address you need to specify here.

NOTE: If you are a L2TP client using DHCP, the IP Address must be left to 0.0.0.0, Gateway Address is required. 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. If your ISP charges you by the amount of time you are connected to the internet, you should use this option.

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.

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.



[You're reading an excerpt. Click here to read official LINKSYS](#)

[WRT54GC user guide](#)

<http://yourpdfguides.com/dref/2353577>

Router IP Address Network Address Server Settings (DHCP) The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network.

A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, make sure there is no other DHCP server on your network. Optional Settings Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Network Address Server Settings (DHCP) Optional Settings DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't 8 Compact Wireless-G Broadband Router Chapter 3 Advanced Configuration Before you can use this feature, you need to sign up for DDNS service at one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, Disabled. want a DHCP server, then select Disabled (no other DHCP features will be available).

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

Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50. Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day. 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. DDNS Service If your DDNS service is provided by DynDNS.org, then select DynDNS.org from the drop-down menu. If your DDNS service is provided by TZO, then select TZO.com.

The features available on the DDNS screen will vary, depending on which DDNS service provider you use. DynDNS.org 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.) Setup > DDNS > DynDNS User Name Enter the User Name for your DDNS account. Password Enter the Password for your DDNS account. Host Name The is the DDNS URL assigned by the DDNS service. Time Setting Status The status of the DDNS service connection is displayed here. Connect Click connection. Connect to establish the DDNS Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

Setup > DDNS The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router. Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dynDNS.org or www.TZO.com. If you do not want to use this feature, keep the default setting, Disabled. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

TZO.com 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. Compact Wireless-G Broadband Router Setup > DDNS > TZ O E-mail Address, TZ O Password, Domain Name Enter the settings of the account you set up with TZO. 9 Chapter 3 Advanced Configuration Status The status of the DDNS service connection is displayed here. Connect Click connection. Connect to establish the DDNS 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 > Advanced Routing (Gateway) Setup > Advanced Routing (Router) Setup > MAC Address Clone 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. Dynamic Routing (RIP) This option is displayed only if the Operating Mode is set to Router. This settings enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is Disabled by default. Route Entries To set up a static route between the Router and another network, select a number from the Static Routing 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 the Delete This Entry button to delete a static route.) Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters. MAC Address Clone Enabled/Disabled To have the MAC Address cloned, select Enabled.

MAC Address Enter the MAC Address registered with your ISP here. Clone My PC's MAC Clicking this button will clone the MAC address of the computer you are using. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Setup > Advanced Routing This screen is used to set up the Router's advanced routing functions. NAT routes the host Router's network connection to the Internet.

Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination. Compact Wireless-G Broadband Router 10 Chapter 3 Advanced Configuration the default setting, Mixed. If you have only 802.11g devices, select Wireless G-Only. If you have only 802.11b devices, select Wireless B-Only. If you do not have any 802.11g and 802.11b devices in your network, select Disabled.

Wireless Network Name (SSID) The SSID is the network name shared among all devices in a wireless network.



[You're reading an excerpt. Click here to read official LINKSYS WRT54GC user guide](http://yourpdfguides.com/dref/2353577)
<http://yourpdfguides.com/dref/2353577>

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 devices in your wireless network. For added security, you should change the default SSID (linksys) to a unique name. Wireless Channel Select the channel from the list provided to correspond with your network settings. All devices in your wireless network must be broadcast on the same channel in order to function correctly. 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, Enabled. If you do not want to broadcast the Router's SSID, then select Disabled.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route. Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion. 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).

Delete This Entry To delete a route, select its number from the drop-down menu, and click this button. Show Routing Table Click Show Routing Table to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click Refresh to update the information. Click Close to exit this screen.

Wireless > Wireless Security Routing Table Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Basic Wireless Settings The basic settings for wireless networking are set on this screen. 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. WPA2 is a more advanced, more secure version of WPA. WEP stands for Wired Equivalent Privacy, and RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security." Wireless Security Security Mode Basic Wireless Settings Select the security method for your wireless network.

If you do not want to use wireless security, keep the default, Disabled. Wireless Network The basic settings for wireless networking are set on this screen. 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 Compact Wireless-G Broadband Router 11 Chapter 3 Advanced Configuration WPA2 Personal WPA Personal Security Mode > WPA Personal Security Mode > WPA2 Personal Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, TKIP or AES. (AES is a stronger encryption method than TKIP.) Passphrase Enter the Passphrase (shared key) used by the Router and your other network devices. It must have 8-63 characters.

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

Passphrase Enter a WPA Passphrase (shared key) of 8-63 characters. Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Group Key Renewal period is 3600 seconds. WPA Enterprise This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

) 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 > WPA2 Enterprise Security Mode > WPA Enterprise Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, TKIP or AES. (AES is a stronger encryption method than TKIP.) RADIUS Server Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Enter the key shared between the Router and the server. Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys.

The default Key Renewal Timeout period is 3600 seconds. Compact Wireless-G Broadband Router Encryption 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 AES RADIUS Server Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Enter the key shared between the Router and the server. Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal Timeout period is 3600 seconds. 12 Chapter 3 Advanced Configuration 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 > WEP WEP Encryption Select a level of WEP encryption, 40/64bit (10 hex digits) or 108/128-bit (26 hex digits). The default is 40/64 bit (10 hex digits). Passphrase Enter a Passphrase to automatically generate WEP keys. Then click Generate.

WEP Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually. TX Key Select a Transmit Key (choose which Key to use). The default is 1. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Security Mode > RADIUS IMPORTANT: If you are using WEP encryption, always remember that each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

First, choose the Radius settings: RADIUS Server Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Key Select a level of WEP encryption, 64-bit (10 hex digits) or 128-bit (26 hex digits).



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2353577)

[WRT54GC user guide](http://yourpdfguides.com/dref/2353577)

<http://yourpdfguides.com/dref/2353577>

The default is 64 bit (10 hex digits). Then, choose the WEP settings: Encryption Select a level of WEP encryption, 40/64bit (10 hex digits) or 108/128-bit (26 hex digits). The default is 40/64 bit (10 hex digits). Passphrase Enter a Passphrase to automatically generate WEP keys. Then click Generate. WEP Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

TX Key Select a Transmit Key (choose which Key to use). The default is 1. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Wireless > Wireless MAC Filter Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. WEP WEP is a basic encryption method, which is not as secure as WPA. Compact Wireless-G Broadband Router 13 Chapter 3 Advanced Configuration Wireless > Wireless MAC Filter Wireless MAC Filter Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click Enabled. If you do not wish to filter users by MAC Address, keep the default setting, Disabled. Prevent Select this to block wireless access by MAC Address. This button is selected by default. Permit Select this to allow wireless access by MAC Address.

This button is not selected by default. MAC 01 - MAC 40 Enter the MAC address for each wireless client to be filtered. Wireless Client List Click this to open the Wireless Client List screen. This screen lists network users by MAC Address, to whom you wish to provide or block access. For easy reference, click Wireless Client List to display a list of network users by MAC Address.

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. 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 Auto, 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. 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 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. DTIM Interval This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346. RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, 2346, is recommended.

If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2346. 14 Wireless Client List 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 This setting cannot be changed. 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 Compact Wireless-G Broadband Router Chapter 3 Advanced Configuration 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.

Beacon Interval The default value is 100. Enter a value between 20 and 1,000 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. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Security > Firewall Firewall SPI Firewall Protection To use firewall protection, keep the default selection, Enabled. To turn off firewall protection, select Disabled. 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. Web Filters Select any web filters that you want to use. Proxy If local users have access to WAN proxy servers, they may be able to circumvent the Router's content filters and access Internet sites blocked by the Router. Proxy filtering will block access to any WAN proxy servers.



You're reading an excerpt. [Click here to read official LINKSYS](http://yourpdfguides.com/dref/2353577)

[WRT54GC user guide](http://yourpdfguides.com/dref/2353577)

<http://yourpdfguides.com/dref/2353577>

To enable proxy filtering, click the box in front of this option. · Java Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java applet filtering, click the box in front of this option. · ActiveX ActiveX is a programming language for websites.

If you deny ActiveX, you run the risk of not having access to Internet sites created using this Compact Wireless-G Broadband Router 15 Chapter 3 Advanced Configuration 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. programming language. To enable ActiveX filtering, click the box in front of this option. · Cookies A cookie is data stored on your PC and used by Internet sites when you interact with them. To enable cookie filtering, click the box in front of this option.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Security > VPN Passthrough The Security > VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall. Security > VPN Passthrough VPN Passthrough IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default, Enabled. L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled. PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enabled. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. 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.) Internet Policy Summary Status Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select Enabled. Compact Wireless-G Broadband Router 16 Chapter 3 Advanced Configuration To create an Internet Access policy: 1. Select a number from the Internet Access Policy dropdown menu. 2. To enable this policy, select Enabled. 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. Port Services 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. 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 Save Settings to save the changes.

If you want to cancel your changes, click Cancel Changes. To close the Port Services screen and return to the Access Restrictions screen, click Close. Website Blocking by URL Address List of PCs 5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen. 6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. Then enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours. 7. 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. 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 and Gaming > Port Range Forwarding The Applications & Gaming > Port Range Forwarding screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) Blocked Services You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting services from the dropdown menus next to Blocked Services. (You can block up to 2 services per policy.

) 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 or Modify. Compact Wireless-G Broadband Router 17 Chapter 3 Advanced Configuration Applications and Gaming > Port Range Triggering Applications and Gaming > Port Range Forwarding Port Range Forwarding To forward a port, enter the information on each line for the criteria required. Application Name In this field, enter the name you wish to give the application. Each name can be up to 12 characters. Start ~ End Port 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. To IP Address For each application, enter the IP Address of the PC running the specific application. Enabled Select Enabled to enable port forwarding for the relevant application.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Port Range Triggering Application Name Enter the application name of the trigger.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2353577)

[WRT54GC user guide](http://yourpdfguides.com/dref/2353577)

<http://yourpdfguides.com/dref/2353577>

Triggered Range For each application, list the triggered port number start and end range. Check with the Internet application documentation for the port number(s) needed. **Forwarded Range** For each application, list the forwarded port number start and end range. Check with the Internet application documentation for the port number(s) needed. **Enabled Select** Enabled to enable port triggering for the applicable application. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. **Applications and Gaming > DMZ** The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC.

The **Port Range 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 & Gaming > Port Range Triggering** The **Applications & Gaming > Port Range Triggering** screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. **Applications and Gaming > DMZ Compact Wireless-G Broadband Router 18 Chapter 3 Advanced Configuration Administration > Management** The **Administration > Management** screen allows the network's administrator to manage specific Router functions for access and security. 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 **Enabled**. 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. **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 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, **Enabled**, to enable wireless access to the Router's web-based utility, or select **Disabled** to disable wireless access to the utility. **Remote Router Access Remote Management** To access the Router remotely, from outside the network, select **Enabled**. **Remote Upgrade** Select **Enabled** to be able to upgrade the firmware remotely from the Internet. **Allow Remote IP Address:** Select **Any IP Address** or manually enter an Internet IP address to allow remote access to the web-based utility from the Internet. **Remote Management Port** Enter the port number that will be open to outside access. You will need to enter the Router's password when accessing the Router this way, as usual. **Compact Wireless-G Broadband Router 19 Chapter 3 Advanced Configuration Administration > Diagnostics** The diagnostic tests (**Ping** and **Traceroute**) allow you to check the connections of your network components.

UPnP UPnP Keep the default, **Enabled** to enable the UPnP feature; otherwise, select **Disabled**. **Allow Users to Configure** To use the **Allow Users to Configure UPnP** options from the Windows operating system, select **Enabled**. **Allow Users to Disable Internet Access** To allow users to disable options from the Windows operating system, click **Enabled**. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. **Backup and Restore** Click **Backup Settings** or **Restore Settings**, then enter the file location, or click **Browse** to find the settings file you want to backup or restore. **Administration > Diagnostics Ping Test Ping Test** The Ping test checks the status of your Internet connection. To **IP or URL Address** Enter the IP address or URL that you want to ping. **Packet Size** Enter the size, (up to 32 bytes) of the packet to test. **Times to Ping** Select the number of times you wish to test the connection, the minimum is 5. Then, click **Ping**.

A new screen will show the test results. **Administration > Log** The Router can keep logs of all traffic for your Internet connection. **Traceroute Test Administration > Log Log Log** To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**. To view a log, click **View Log**.

A new window will appear and you can select the type you want to view: **Incoming Log**, **Outgoing Log**, **Security Log** or **DHCP Client Log**. On this screen you can click **Refresh** to see up-to-date information, **Clear Log** to delete the log or **Close** to exit the screen. When you return to the Log screen, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. **Traceroute Test** To test the performance of a connection, click **Traceroute** to open the **Traceroute Test** screen. This test shows how many hops a packet from your computer takes to reach the Internet, and how long each hop takes.

Compact Wireless-G Broadband Router 20 Chapter 3 Advanced Configuration Status > Router The **Status > Router** screen displays the Router's current status. **Administration > Factory Defaults** The **Administration > Factory Defaults** screen allows you to restore the Router's configuration to its factory default settings. **Factory Defaults Restore Factory Defaults** To reset the Router's settings to the default values, click **Restore Factory Defaults**. A new screen will appear. Click **OK** to confirm that you want to reset to the factory defaults. Any settings you have saved will be lost when the default settings are restored. **Status > Router Administration > Factory Defaults Router Information Firmware Version** This is the Router's current firmware. **Current Time** This shows the time, as you set on the **Setup** tab. **MAC Address** This is the Router's MAC Address, as seen by your ISP. **Router Name** This is the specific name for the Router, which you set on the **Setup** tab.

Host Name If required by your ISP, this would have been entered on the **Setup** tab. **Domain Name** If required by your ISP, this would have been entered on the **Setup** tab. **Administration > Upgrade Firmware** The **Administration > Upgrade Firmware** screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use. **Internet Administration > Upgrade Firmware Configuration Type** This section shows the current network information stored in the Router.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2353577)

[WRT54GC user guide](http://yourpdfguides.com/dref/2353577)

<http://yourpdfguides.com/dref/2353577>

The information varies depending on the Internet connection type selected on the Setup > Basic Setup screen. Example: IP Release or IP Renew buttons appear if you are using DHCP for your connection. Disconnect and Connect buttons appear if you are using PPPoE, PPTP or L2TP. Click Refresh to update the on-screen information. Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file. Firmware Upgrade Please Select a language Select your language from the drop-down menu. The choices are English

(default), French, German, Italian, Spanish, Portuguese, Dutch.

Please Select a File to Upgrade Click Browse and select the extracted firmware upgrade file. Then click Upgrade and follow the on-screen instructions. Compact Wireless-G Broadband Router 21 Chapter 3 Advanced Configuration Status > Wireless The Status > Wireless screen displays the status of your wireless network. Status > Local Network The Status > Local Network screen displays the status of your network. Status > Wireless Status > Local Network Wireless MAC Address This is the Router's MAC Address, as seen on your local, wireless network.

Mode As selected from the Wireless > Basic Wireless Settings screen, this displays the wireless mode (Mixed, GOnly, or Disabled) used by the network. SSID As entered on the Wireless > Basic Wireless Settings screen, this displays the wireless network name or SSID. Channel As entered on the Wireless > Basic Wireless Settings screen, this displays whether SSID Broadcast is enabled or disabled. Local Network MAC Address This is the Router's MAC Address, as seen on your local, Ethernet network. IP Address This shows the Router's IP Address, as it appears on your local, Ethernet network. Subnet Mask This shows the current subnet mask being configured for your local network. DHCP Server If you are using the Router as a DHCP server, that will be displayed here. 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 Client Table To see assigned IP Addresses, MAC Addresses, Interface or Client Names on the DHCP server, click DHCP Client Table. A new screen will appear. Choose the option to view from the drop down list. Click Refresh to see an up-to-date list or Close to exit the screen. DHCP Client Table Compact 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, and then insert the setup CD into your computer. Click Setup and follow the on-screen instructions. The computer cannot connect wirelessly to the network. Make sure the wireless network name or SSID is the same on both the computer and the Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router. You need to modify the settings on the Router. Open the web browser (for example, Internet Explorer or Firefox), and enter the Router's IP address in the address field (the default IP address is 192.168.1.1). When prompted, enter the password to the Router (the default is admin). Click the appropriate tab to change the settings. 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. 2. 3. Cable or DSL modem Router Computer · Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the modem must be connected to the Internet port on the Router. The modem does not have an Ethernet port. The modem is a dial-up modem for traditional dial-up service.

To use the Router, you need a cable/DSL modem and high-speed Internet connection. You cannot use the DSL service to connect manually to the Internet. After you have installed the Router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually. The DSL telephone line does not fit into the Router's Internet port. The Router does not replace your modem.

You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer.

Click Setup and follow the on-screen instructions. WEB: If your questions are not addressed here, refer to the Linksys website, www.linksys.com Compact Wireless-G Broadband Router 23 Appendix B Specifications Appendix B: Specifications Model Standards Channels Ports WRT54GC v3 IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b 11 Channels (US, Canada) 13 Channels (most of Europe) Internet: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Port Reset CAT5 Power, DMZ, WLAN, LAN (1-4), Internet 802.11g: Typical 13 dBm (± 1.5) 802.11b: Typical 16.5 dBm (± 2) UPnP able/cert Security Features Wireless Security Able Stateful Packet Inspection (SPI) Firewall, Internet Policy Wi-Fi Protected AccessTM2 (WPA2), WEP, Wireless MAC Filtering 98 x 98 x 25 mm 140 g External, 5V DC, 1A FCC, IC-03, CE, Wi-Fi (802.11b, 802.

11g) 0 to 40°C -20 to 70°C 5 to 90%, Noncondensing Button Cabling Type LEDs RF Power Output Environmental Dimensions Weight Power Certifications Operating Temp. Storage Temp. Storage Humidity Operating Humidity 10 to 85%, Noncondensing Specifications are subject to change without notice.

Compact Wireless-G Broadband Router 24 Appendix C Warranty Information network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or 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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2353577)

[WRT54GC user guide](http://yourpdfguides.com/dref/2353577)

<http://yourpdfguides.com/dref/2353577>

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 Warranty Linksys warrants that this Linksys hardware product will be substantially free of defects in materials and workmanship arising under normal use during the Warranty Period, which begins on the date of purchase by the original enduser purchaser and lasts for the period specified below: · · Two (2) years 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. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and/or parts that are replaced become the property of Linksys. This limited warranty shall apply in addition to any statutory or other rights which you may have under a contract of sale.

Exclusions and Limitations This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with nonLinksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee. ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED "AS IS" WITHOUT ANY WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, service, software or any equipment, system or Compact Wireless-G Broadband Router Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to www.linksys.com/support where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at www.linksys.com.

Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number 25 Appendix C Warranty Information and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

Technical Support This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at www.linksys.com/support General This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you. If any portion of this limited warranty is found to be void or unenforceable, its remaining provisions shall remain in full force and effect.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623. For more information, please contact us www.linksys.com Select your country, and then select SUPPORT/TECHNICAL For product returns: Select your Country and then select CUSTOMER SUPPORT Compact Wireless-G Broadband Router 26 Appendix D Regulatory Information Wireless Disclaimer The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions. Appendix D: Regulatory Information FCC Statement This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules.



[You're reading an excerpt. Click here to read official LINKSYS WRT54GC user guide](http://yourpdfguides.com/dref/2353577)
<http://yourpdfguides.com/dref/2353577>