



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WRT54G3GV2-VF. You'll find the answers to all your questions on the LINKSYS WRT54G3GV2-VF in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual LINKSYS WRT54G3GV2-VF

User guide LINKSYS WRT54G3GV2-VF

Operating instructions LINKSYS WRT54G3GV2-VF

Instructions for use LINKSYS WRT54G3GV2-VF

Instruction manual LINKSYS WRT54G3GV2-VF

LINKSYS®
A Division of Cisco

USER GUIDE

**Wireless-G
Router for
3G/UMTS Broadband**



Model No: WRT54G3GV2-VF



[You're reading an excerpt. Click here to read official LINKSYS WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)
<http://yourpdfguides.com/dref/2361873>

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 Router for 3G/UMTS Broadband Table of Contents Chapter 1: Product Overview 4 Top Panel. . . .

.
.
.
.
.
.
.
.
.
. 4 Side Panel

.
.
.
.
.
.
.
. 4 Opposite Side Panel with Antenna. . . .

.
.
.
.
. 5 Front Panel.

.
.
.
.
.
. 5 Bottom Panel

.
.
.
.
. 5 Placement Positions .

.
.
.
.
.
. . . 6 Chapter 2: Wireless Security Checklist 7 General Network Security Guidelines . .

.
.
.
. 7 Additional Security Tips

.
.
.
. 7 Chapter 3: Advanced Configuration 8 Setup > Basic Setup . . .

.
.
.
.

.....
.....
.31 Administration > Factory Defaults
.....
.....

.....
.....
.31 Administration > Firmware Upgrade
.....

.....
.....
. . . .31 Status > HSDPA/3G/UMTS .
.....

.....
.....
.32 Status > Router .

.....
.....
.33 Status > Local Network
.....

.....
.....
.33 Status > Wireless Network . .

.....
.....
*.34 Appendix A: Troubleshooting Wireless-G Router for 3G/UMTS Broadband 35 Table of Contents Appendix B: Specifications Appendix C:
Warranty Information 37 38 Limited Warranty . .*

.....
.....
. . . .38 Exclusions and Limitations

.....
.....
. . .38 Obtaining Warranty Service
.....

.....
. .38 Technical Support . . .
.....

.....
.....
.....
.....39 Appendix D: Regulatory Information 40 FCC Statement . . .

.....
.....
.....
.....
.....
.....
.....
.....40 Industry Canada Statement .
.....
.....

.....
.....
.....
.....40 Avis d'Industrie Canada.

.....
.....
.....
.....
.....
.....
.....
.....40 Wireless Disclaimer

.....
.....
.....
.....41 Avis de non-responsabilité concernant les appareils sans fil .
.....

.....41 Safety Notices. . .
.....
.....
.....

.....
.....
.....
.....
.....
.....41 Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive) . 42 CE Marking . . .

.....
.....
.....
.....
.....
.....
.....
.....43 IDA Standards.

.....
.....
.....
.....
.....
.....
.....
.....43 Product Usage Restrictions
.....
.....
.....

...44 Technical Documents on www.linksys.com/international

.....

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

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

...45 Appendix E: Software License Agreement 49 Software in Linksys Products

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

...49 Software Licenses . .

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

...49 Appendix E: Contact Information 56 Vodafone Online Resource . .

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

...56 Vodafone Technical Support . .

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

.....
.....

.56 Wireless-G Router for 3G/UMTS Broadband Chapter1 Product Overview Side Panel Chapter 1: Product Overview Thank you for choosing the Linksys Wireless-G Router for 3G/UMTS Broadband. The Wireless-G Router for 3G/UMTS Broadband, lets you access the Internet through either your HSDPA/3G/UMTS or GPRS service (requires a Vodafone Mobile Connect HSDPA/3G/UMTS data card, available separately), or you can use a cable or DSL modem for broadband service. Plus, this access can be shared over the four switched ports or via the wireless broadcast at up to 54Mbps for Wireless-G or up to 11Mbps for Wireless-B. A variety of security features help to protect your data and your privacy while online. Security features include WPA2 (Wi-Fi Protected Access 2) security, a Stateful Packet Inspection (SPI) firewall, and NAT technology. Configuring the Router is easy using the Setup Wizard or through the provided browser-based utility. USB Port Reserved for future use. Power (Green) The Power LED lights up and stays on while the Router is powered on. Ethernet 1- (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. It flashes to indicate network activity over that port. Wireless (Green) The Wireless LED lights up when the wireless feature is enabled. It flashes when the Router is actively sending or receiving data over the wireless network. MODEM Top Panel If you have a Vodafone data card, use the PC Card slot.

If you have a Vodafone USB adapter, use one of the USB ports. NOTE: The Router supports a single mobile broadband device. Connect either a data card or a USB adapter--do not connect both at the same time. Modem Internet (Green) The Modem LED lights up and stays on when there is a connection made through the Modem port. It flashes to indicate network activity over the Modem port. 3G/UMTS Internet (Blue/Green) The 3G/UMTS LED flashes as the Router connects to the mobile network. When the LED stops flashing and stays on, then the connection is active. When the LED is blue, a 3G/UTMS/HSDPA connection has been established. When the LED is green, a GPRS connection has been established.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361873)

[WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)

<http://yourpdfguides.com/dref/2361873>

If the LED flashes quickly, the Router is not connected to the mobile network.

Before pressing the Mobile Connect/Disconnect button, make sure the mobile broadband data card or USB adapter is already installed. 3G/UMTS 3G/UMTS

USB Ports Insert the Vodafone Mobile Connect HSDPA/3G/UMTS data card (available separately) into this port if the Router will connect to a HSDPA/3G/UMTS or GPRS service. Mobile PC Card Slot If the Router will connect to a mobile broadband service, insert the mobile broadband data card (available separately) into this slot. After the data card is inserted, the eject button will pop up. To remove the data card, press the eject button.

Mobile Connect/Disconnect Button Press this button to connect to and disconnect from the mobile network. (You can also use the Basic Setup screen of the Router's web-based utility.) Wireless-G Router for 3G/UMTS Broadband Chapter1 Product Overview Bottom Panel To place the Router in a vertical position, rotate the stand 90 degrees. Opposite Side Panel with Antenna Modem The Modem port is where you will connect your cable or DSL modem. Ethernet 1, 2, 3, These Ethernet ports (1, 2, 3, 4) connect the Router to wired computers and other Ethernet network devices.

Security Bracket The security bracket labeled "Reset" clips onto the Router. It covers the Reset button and the security slot on the Router's top panel. You can remove the security bracket to access the Reset button. 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 the Administration > Factory Defaults screen of the Router's web-based utility. Power The Power port is where you will connect the power adapter. Front Panel Security Slot To protect the Router from theft, you can attach a lock to the Router using the security slot. Wireless-G Router for 3G/UMTS Broadband Chapter1 Product Overview Wall-Mounting Placement The Router has four wall-mount slots on its back panel. The distance between two adjacent slots is 68 mm (2.68 inches).

Two screws are needed to mount the Router. Suggested Mounting Hardware 2.5-3.0 mm Placement Positions There are three ways to physically install the Router. The first way is to place the Router horizontally on a surface. The second way is to stand the Router vertically on a surface. The third way is to mount the Router on a wall. Horizontal Placement The Router has four authorized 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. Wireless-G Router for 3G/UMTS Broadband WEB: For more information on wireless security, visit www.linksys.com/security Chapter3 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. How to Access the Web-Based Utility To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, 192.1.1.

1, in the Address field. Then, press Enter. A login screen will appear. (Non-Windows XP users will see a similar screen.) Enter admn (the default) in both the Username and Password fields. (You can set a new password on the Administration tab's Management screen.) Click OK to continue. Setup > Basic Setup 3G/UMTS Setup Configure the HSDPA/3G/UMTS and/or GPRS settings for the Router in this section. Mobile Connect This button enables you to connect to and disconnect from the HSDPA/3G/UMTS or GPRS network through the Web-based Utility (you can also connect and disconnect using the hardware button on the Router). It will also indicate the status of the Router's HSDPA/3G/UMTS or GPRS connection.

Service If you want the Router to connect to a HSDPA/ 3G/UMTS signal when available Select HSDPA/3G/UMTS Preferred (recommended) . If the HSDPA/3G/UMTS signal is not available, then Router will use a GPRS connection. If the Router is having problems maintaining a connection, you can select HSDPA/3G/UMTS Only or GPRS Only. Then the Router will be able to connect to only one type of signal. Mobile Network Bearer The name of the mobile network bearer the Router is using is displayed.

Login Screen Setup > Basic Setup The first screen that appears is the Basic Setup screen. This allows you to change the Router's general settings. Wireless-G Router for 3G/UMTS Broadband Chapter3 Advanced Configuration DNS 1-3 Your ISP will provide you with at least one DNS (Domain Name System) server IP address. Signal Strength This indicates the strength of the HSDPA/ 3G/UMTS or GPRS signal that the Router is receiving Internet Setup The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your ISP.

PPPoE Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE. Internet Connection Type Select the type of Internet connection your ISP provides from the drop-down menu. These are the available types: · · · · · Automatic Configuration - DHCP Static IP PPPoE PPTP L2TP Telstra Cable Internet Connection Type > PPPoE Username and Password Enter the Username and Password provided by your ISP.



[You're reading an excerpt. Click here to read official LINKSYS WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)
<http://yourpdfguides.com/dref/2361873>

Service Name If provided by your ISP, enter the Service Name. *Connect on Demand: Max Idle Tme* 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 1 minutes. *Keep Alive: Redal Perod* 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, specify how often you want the Router to check the Internet connection. The default *Redial Period* is 30 seconds. *Automatic Configuration - DHCP* By default, the Router's Internet Connection Type is set to *Automatic Configuraton - DHCP*, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. (This option usually applies to cable connections.) *Internet Connection Type > Automatic Configuration - DHCP Static IP* If you are required to use a permanent IP address to connect to the Internet, select *Static IP*. *PPTP Internet Connection Type > Static IP Point-to-Point Tunneling Protocol (PPTP)* is a service that applies to connections in Europe only.

Internet IP Address This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here. *Subnet Mask* This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask. *Default Gateway* Your ISP will provide you with the IP address of the ISP server.

Internet Connection Type > PPTP Wreless-G Router for 3G/UMTS Broadband 9 Chapter3 Advanced Configuration before your Internet connection terminates. The default *Max Idle Time* is 1 minutes. *Keep Alive: Redal Perod* 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, specify how often you want the Router to check the Internet connection. The default *Redial Period* is 30 seconds. *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. *Default Gateway* Your ISP will provide you with the IP address of the ISP server. *Username and Password* Enter the Username and Password provided by your ISP. *Connect on Demand: Max Idle Tme* 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 1 minutes. *Keep Alive: Redal Perod* 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, specify how often you want the Router to check the Internet connection. The default *Redial Period* is 30 seconds. *Telstra Cable Telstra Cable* is a service that applies to connections in Australia only. If your ISP uses *HeartBeat Signal (HBS)*, then select *Telstra*.

Internet Connection Type > Telstra Cable Server IP Address This is the IP address of the Server. Your ISP will provide you with the IP Address you need to specify here. *Username and Password* Enter the Username and Password provided by your ISP. *Connect on Demand: Max Idle Tme* 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 minutes *Keep Alive: Redal Perod* 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 Username and Password* Enter the Username and Password provided by your ISP. *Server IP Address* This is the IP address of the L2TP Server. Your ISP will provide you with the IP address you need to specify here. *Connect on Demand: Max Idle Tme* 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 *Wreless-G Router for 3G/UMTS Broadband 10 Chapter3 Advanced Configuration from the Modem port or mobile network* to the client, depending on how the Router is currently connected.

NOTE: If the upstream DNS servers change between connections, the clients may become unable to resolve addresses because they have valid DHCP leases that use the old server values. *Mode 3 - Manual configuraton* Select this option if you want to set arbitrary DNS/WINS values for the clients to use. These values are not validated by the Router. *Optional Settings* Some of these settings may be required by your ISP. Verify with your ISP before making any changes. *Optional Settings Host Name and Doman 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're reading an excerpt. Click here to read official LINKSYS
WRT54G3GV2-VF user guide
http://yourpdfguides.com/dref/2361873](http://yourpdfguides.com/dref/2361873)

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, 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 Server Settings 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. DHCP, Static IP, or Telstra: 100 PPPoE: 192 PPTP or L2TP: 10 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. Network Address Server Settings (DHCP) Router IP This presents both the Router's IP Address and Subnet Mask as seen by your network. DHCP Server DHCP is enabled by default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select Disabled (no other DHCP features will be available). DHCP Reservation Click this button if you want to assign a fixed local IP address to a MAC address. Router IP DHCP Reservation You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. DHCP Server Settings This setting determines how the clients (network devices) use DNS/WINS. Mode 1 - Fixed configuration (Default) Select this option if you want the Router to advertise itself as the DNS server to use and handle upstream changes automatically. Mode 2 - Network Supplied Select this option if you want the Router to pass through the DNS server values (learned Wireless-G Router for 3G/UMTS Broadband 11 Chapter3 Advanced Configuration Server Setting. 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 0-1 These settings are available if you selected Mode 3 - Manual configuration for the DHCP Server Setting. 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. You can enter up to two WINS server IP addresses here. Otherwise, leave these fields blank.

DHCP Reservation Time Setting Time Zone Select the time zone in which your network functions from this drop-down menu.

(You can even automatically adjust for daylight saving time.) · Select Clients from DHCP Table Click the Select check box to reserve a client's IP address. Then click Add Clients. Manually Adding Client To manually assign an IP address, enter the client's name in the Enter Client Name field. Enter the IP address you want it to have in the Assign IP Address field.

Enter its MAC address in the To This MAC Address field. Then click Add. · Time Setting Clients Already Reserved A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click Remove. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

To view the most up-to-date information, click Refresh. To exit this screen, click Close. Start IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.100, the Start IP Address must be 192.168.1.101 or greater, but smaller than 192.

168.1.253. The default is 192.1.1.100. Maximum Number of Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 0.

IP Address Range Displayed here is the range of available IP addresses. Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

Static DNS 1-3 These settings are available if you selected Mode 3 - Manual configuration for the DHCP Wireless-G Router for 3G/UMTS Broadband Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. 12 Chapter3 Advanced Configuration Time field, enter the number of minutes you want to have elapsed before your mobile network connection terminates. The default Max Idle Time is 0 minutes. Keep Alive: Redial Period If you select this option, you can specify how often the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically reestablish your connection.

To use this option, select Keep Alive. 0 Setup > Mobile Network Configure mobile network settings and view status information for your mobile broadband service and device (data card or USB adapter). Some of these settings will be automatically configured by the Router and, in most cases, should not be changed unless you are instructed to do so. Reset data card To reset the data card after a number of failed attempts, select this option. The default number of failed connection attempts is . Link Check You can have the Keep Alive Server link checked through LCP (Link Control Protocol) or ICMP (Internet Control Message Protocol). The server will be pinged in the number of seconds specified. The default is 30 seconds. After the number of tries specified with no response, (default is 3), the LCP or ICMP will attempt to re-establish the connection. For ICMP you can also choose to automatically reboot your connection if a specified number of seconds have passed since the last reply.

The default is 300. You can also enter up to two server IP addresses to use. 0 Disconnect field If you want to disconnect the Router from the HSDPA/3G/UMTS or GPRS network if no data has been sent or received from the Vodafone network for a specific period of time, then enter the number of minutes you want to specify in the field provided.



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

[WRT54G3GV2-VF user guide](#)

<http://yourpdfguides.com/dref/2361873>

The default is 0. PAP or CHAP Authentication Setup > Mobile Network Select the authentication type used by your service provider: PAP or CHAP. If you do not know which type to use, select Auto. Mobile Network Settings Auto Connect If this feature is enabled, the Router will automatically connect to the default HSDPA/3G/UMTS or GPRS network when it powers on. The default is Disabled. You can use the Mobile Connect/Disconnect button on the Router to connect and disconnect from the mobile network. Connect on Demand: Max Idle Tme You can configure the Router to cut the mobile network connection after it has been inactive for a specified period of time (Max Idle Time).

If your mobile network 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 Wreless-G Router for 3G/UMTS Broadband APN Configuration Configure how the Router will selects its Access Point Name (APN) or network. APN Selecton Mode If you want the Router to select a suitable APN based on the current SIM card, select Auto. If you want to override the automatic selection, select Manual.

Then select a suitable APN from the Home Network drop-down menu. If you want to specify values that may not be in the standard configuration (such as a corporate APN), select Custom Values. Then complete the APN Name, Username, Password, DNS Supplied by Network, and DNS 1-2 fields as needed. If you selected Custom Values, complete the following: APN Name The APN (Access Point Name) Name is automatically entered by the Router. Do not change this 13 Chapter3 Advanced Configuration IMSI IMSI (International Mobile Subscriber Identity) is a fixed identification number and is read automatically from the Vodafone card.

Click Refresh to update the on-screen information. Click Save Setngs to apply your changes, or click Cancel Changes to cancel your changes. setting unless told to do so by either Vodafone or LInksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter its name here. Username The Username is automatically entered by the Router. Do not change this setting unless told to do so by either Vodafone or LInksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter the new Username here. Password The Password is automatically entered by the Router. Do not change this setting unless told to do so by either Vodafone or LInksys technical support, or the IT manager of your company. If you have access to a private APN, you can enter the new Password here.

DNS Suppled by Network If the network automatically supplies the DNS address(es), click Enable (default). If you need to specify the DNS address(es), remove the checkmark, and enter the DNS address(es) in the DNS 1-2 fields. DNS 1-2 Enter the DNS address(es) you want the Router to use. PIN Code If required, enter the PIN code of your SIM card. The code will be stored here for future reference by the Router, and you will not have to re-enter this unless you change SIM cards. 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, Disabled. DDNS DDNS Service If your DDNS service is provided by DynDNS.org, then select DynDNS.org from the drop-down menu. If your DDNS service is provided by TZO, then select TZO.com. The features available on the DDNS screen will vary, depending on which DDNS service provider you use.

Mobile Network Status Moble Network Bearer The name of the mobile network bearer the Router is using is displayed. @@To select a different network, click the Select Network button and follow the on-screen instructions. Signal Strength The strength of the HSDPA/3G/UMTS or GPRS signal that the Router is receiving is displayed. Connecton Tme The length of time the Router has been connected to the HSDPA/3G/UMTS or GPRS network since your last connection is displayed. Current Session Usage The amount of data that has been sent to and received from the HSDPA/3G/UMTS or GPRS network since your last connection is displayed. DynDNS.org 3G/UMTS Card Status Card Model The model number of your Vodafone card is displayed. Card Revson The revision number of your Vodafone card is displayed. Card Frmware The firmware version of your Vodafone card is displayed. Setup > DDNS > DynDNS Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account. Host Name This is the DDNS URL assigned by the DDNS service. System Select the DynDNS service you use: Dynamic, Statc, or Custom. The default is Dynamic. 1 Wreless-G Router for 3G/UMTS Broadband Chapter3 Advanced Configuration 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. Mal Exchange (Optonal) Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server. Backup MX This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, Disabled.

To enable the feature, select Enabled. If you are not sure which setting to select, keep the default, Disabled. Wldcard This setting enables or disables wildcards for your host. For example, if your DDNS address is myplace.dyndns.

org and you enable wildcards, then x.myplace.dyndns.org will work as well (x is the wildcard). To disable wildcards, keep the default, Disabled.

To enable wildcards, select Enabled. If you are not sure which setting to select, keep the default, Disabled. Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change. Status The status of the DDNS service connection is displayed here. Update To manually trigger an update, click this button. Click Save Setngs to apply your changes, or click Cancel Changes to cancel your changes. Setup > MAC Address Clone MAC Address Clone Enabled/Disabled To have the MAC Address cloned, select Enabled. MAC Address Enter the MAC Address registered with your ISP here. Clone My PC's MAC Click this button to clone the MAC address of the computer you are using.

Click Save Setngs to apply your changes, or click Cancel Changes to cancel your changes. TZO.com Setup > Advanced Routing This screen is used to set up the Router's advanced functions.



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

[WRT54G3GV2-VF user guide](#)

<http://yourpdfguides.com/dref/2361873>

Operating Mode allows you to select the type(s) of advanced functions you use. *Dynamic Routing* automatically adjusts how packets travel on your network. *Static Routing* sets up a fixed route to another network destination. *Setup > DDNS > TZO E-mail Address, TZO Key, and Domain Name* Enter the settings of the account you set up with TZO. *Internet IP Address* The Router's Internet IP address is displayed here. Because it is dynamic, it will change. *Status* The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click this button. Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes. *Setup > Advanced Routing Wireless-G Router for 3G/UMTS Broadband 1 Chapter3 Advanced Configuration Advanced Routing NAT Enabled/Disabled* If this Router is hosting your network's connection to the Internet, keep the default, *Enabled*. If another router exists on your network, select *Disabled*. When the NAT setting is disabled, dynamic routing will be enabled.

Dynamic Routing (RIP) Enabled/Disabled This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. When the NAT setting is enabled, the *Dynamic Routing* feature is automatically disabled. When the NAT setting is disabled, this feature is available. Select *Enabled* to use the *Dynamic Routing* feature.

Advanced Routing > Routing Table Routing Table For each route, the *Destination LAN IP address, Subnet Mask, Gateway, and Interface* are displayed. Click *Refresh* to update the information. Click *Close* to exit this screen. Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes.

Static Routing A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route. *Route Entries* To set up a static route between the Router and another network, select a number from the dropdown list. Click *Delete This Entry* to delete a static route. *Route Name* Enter a name for the Route here, using a maximum of 25 alphanumeric characters. *Destination LAN IP* The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion. *Gateway* This is the IP address of the gateway device that allows for contact between the Router and the remote network or host. *Interface* This interface tells you whether the Destination IP address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet). Click *Show Routing Table* to view the static routes you have already set up. *Wireless > Basic Wireless Settings* The basic settings for wireless networking are set on this screen. *Wireless > Basic Wireless Settings Basic Wireless Settings Network Mode* From this drop-down menu, you can select the wireless standards running on your network. If you have *Wireless-G* and *Wireless-B* devices in your network, keep the default, *Mixed*. If you have only *Wireless-G* devices, select *G-Only*. If you have only *Wireless-B* devices, select *B-Only*. If you do not have any wireless devices in your network, select *Disabled*.

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

Standard Channel Select the channel you want to use for wireless networking. *Wireless-G Router for 3G/UMTS Broadband 1 Chapter3 Advanced Configuration Key Renewal* Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is 300 seconds. *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, *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. *WPA2 Personal Wireless > Wireless Security* The *Wireless Security* screen configures the security of your wireless network. There are six wireless security mode options supported by the Router: *WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, RADIUS, and WEP*. (WPA stands for *Wi-Fi Protected Access*, which is a security method 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." *Security Mode > WPA2 Personal 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*.

Encrypton WPA2 supports two encryption methods, *TKIP* and *AES*, with dynamic encryption keys. Select the type of algorithm, *AES* or *TKIP*. The default is *AES* or *TKIP*. *Passphrase* Enter a Passphrase of 8-63 characters. *Key Renewal* Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is 300 seconds. *WPA Personal NOTE:* If you are using WPA, always remember that each device in your wireless network **MUST** use the same WPA method and passphrase, or else the network will not function properly. *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.) *Security Mode > WPA Enterprise Security Mode > WPA Personal Encrypton* WPA supports two encryption methods, *TKIP* and *AES*, with dynamic encryption keys. Select the type of algorithm, *TKIP* or *AES*. The default is *TKIP*. *Passphrase* Enter a Passphrase of 8-63 characters. *Encrypton WPA* supports two encryption methods, *TKIP* and *AES*, with dynamic encryption keys. Select the type of algorithm, *TKIP* or *AES*.

The default is *TKIP*. *RADIUS Server* Enter the IP address of the RADIUS server. *RADIUS Port* Enter the port number of the RADIUS server. The default is 112. *Wireless-G Router for 3G/UMTS Broadband 1 Chapter3 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.) *Shared Secret* Enter the key shared between the Router and the server.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361873)

[WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)

<http://yourpdfguides.com/dref/2361873>

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is 300 seconds. **WPA2 Enterprise** This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) **Security Mode > RADIUS Security Mode > WPA2 Enterprise** Encrypton WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or AES or TKIP. The default is AES or TKIP. **RADIUS Server** Enter the IP address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default is 112. **Shared Secret** Enter the key shared between the Router and the server. **Key Renewal** Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is 300 seconds. **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** Enter the IP address of the RADIUS server. **RADIUS Port** Enter the port number of the RADIUS server. The default is 112. **Shared Secret** Enter the key shared between the Router and the server.

Encrypton Select a level of WEP encryption, 0/ bts (10 hex dgts) or 10/12 bts (2 hex dgts). The default is 0/ bts (10 hex dgts). **Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**. **Key 1-** If you did not enter a Passphrase, enter the WEP key(s) manually. **TX Key** Select which TX (Transmit) Key to use. The default is 1. **Wireless-G Router for 3G/UMTS Broadband 1 Chapter3 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. **WEP** WEP is a basic encryption method, which is not as secure as WPA. **Security Mode > WEP Encrypton** Select a level of WEP encryption, 0/ bts (10 hex dgts) or 10/12 bts (2 hex dgts).

The default is 0/ bts (10 hex dgts). **Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click **Generate**. **Key 1-** If you did not enter a Passphrase, enter the WEP key(s) manually. **TX Key** Select which TX (Transmit) Key to use. The default is 1. Click **Save Settngs** to apply your changes, or click **Cancel Changes** to cancel your changes. **Wireless > Wireless MAC Filter Wireless MAC Filter Enabled/Disabled** To filter wireless users by MAC Address, either permitting or blocking access, select **Enabled**. To not filter users by MAC Address, keep the default, **Disabled**. **Access Restriction** Prevent Select this to block wireless access by MAC Address.

This button is selected by default. **Permt** Select this to allow wireless access by MAC Address. This button is not selected by default. **MAC Address Filter List** **Wireless Clent Lst** Click this to open the Wireless Client List screen. **Wireless Client List** **Wireless-G Router for 3G/UMTS Broadband 19 Chapter3 Advanced Configuration** use a WEP key for authentication. Select **Shared Key** to only use Shared Key authentication. **Basic Rate** The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default 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. **Transmsson Rate** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the **Auto-Fallback** feature. **Auto-Fallback** will negotiate the best possible connection speed between the Router and a wireless client. The default is **Auto**. **CTS Protection Mode** The Router will automatically use **CTS (Clear-To-Send) Protection Mode** when your **Wireless-N** and **Wireless-G** products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy 802.11b traffic.

This function boosts the Router's ability to catch all **WirelessN** and **Wireless-G** transmissions but will severely decrease performance. The default is **Auto**. **Beacon Interval** Enter a value between 1 and 65,535 milliseconds. The **Beacon Interval** value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default is 100. **DTIM Interval** This value, between 1 and 255, indicates the interval of the **Delivery Traffic Indication Message (DTIM)**. A **DTIM** field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next **DTIM** with a **DTIM Interval** value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

The default is 1. **Fragmentaton 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 of 23. **20 Wireless Client List** This screen shows computers and other devices on the wireless network. The list can be sorted by **Client Name**, **Interface**, **IP Address**, **MAC Address**, and **Status**. Select **Save to MAC Address Flter Lst** for any device you want to add to the **MAC Address Filter List**. Then click **Add**.

To retrieve the most up-to-date information, click **Refresh**. To exit this screen and return to the **Wireless MAC Filter** screen, click **Close**. **MAC 01-0** Enter the MAC addresses of the devices whose wireless access you want to block or allow. Click **Save Settngs** to apply your changes, or click **Cancel Changes** to cancel your changes. **Wireless > Advanced Wireless Settings** This **Advanced Wireless Settings** screen is used to set up the Router's advanced wireless functions.

These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance. **Wireless > Advanced Wireless Settings** **Advanced Wireless AP Isolation** This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361873)

[WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)

<http://yourpdfguides.com/dref/2361873>

To use this function, select Enabled. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use this option, keep the default, Enabled. Otherwise, select Disabled. **Authentication Type** The default is set to Auto, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient Wireless-G Router for 3G/UMTS Broadband Chapter3 Advanced Configuration 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. **RTS Threshold** Should you encounter inconsistent data flow, only minor reduction of the default value, 23, 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 23. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. **Web Filter Proxy** Use of WAN proxy servers may compromise the Gateway's security. Denying Proxy will disable access to any WAN proxy servers. Select this feature to enable proxy filtering. Deselect the feature to allow proxy access. **Java** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.

Select this feature to enable Java filtering. Deselect the feature to allow Java usage. **ActiveX** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language. Select this feature to enable ActiveX filtering. Deselect the feature to allow ActiveX usage. **Cookies** A cookie is data stored on your computer and used by Internet sites when you interact with them. Select this feature to filter cookies. Deselect the feature to allow cookie usage. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

Security > Firewall The Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network. **Security > VPN Passthrough** **Security > Firewall** The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall. **Firewall SPI Firewall Protection** To use firewall protection, keep the default, Enabled. To turn off firewall protection, select Disabled. **Internet Filter Filter Anonymous Internet Requests** This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests. **Filter Multicast** Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. Select this feature to filter multicasting.

This feature is not selected by default. **Filter Internet NAT Redirection** This feature uses port forwarding to block access to local servers from local networked computers. Select this feature to filter Internet NAT redirection. It is not selected by default. **Wireless-G Router for 3G/UMTS Broadband 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. **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. **21 Chapter3 Advanced Configuration Security > L2TP Mobile** The L2TP Mobile screen allows you to enable L2TP Mobile server information to pass through the Router's firewall. **L2TP Passthrough** **Layer 2 Tunneling Protocol** is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. **Security > PPTP Mobile** The PPTP Mobile screen allows you to enable PPTP Mobile server information to pass through the Router's firewall.

Security > L2TP Mobile Logn Status To log in to L2TP Mobile, click Connect. **Username** Enter your L2TP Mobile username in the field. **Password** Enter your L2TP Mobile password in the field. **L2TP Server** Enter the name of the L2TP server. **Security > PPTP Mobile Logn Status** To log in to PPTP Mobile, click Connect. **Username** Enter your PPTP Mobile username in the field. **Password** Enter your PPTP Mobile password in the field. **PPTP Server** Enter the name of the PPTP server. **Auto Connect** Select Enable to automatically connect to the server. **Keep Alive: Redal Perod** If you select this option, you can specify how often the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically reestablish your connection. To use this option, select Keep Alive. **Auto Connect** Select Enable to automatically connect to the server. **Keep Alive: Redal Perod** If you select this option, you can specify how often the Router will periodically check your mobile network connection. If you are disconnected, then the Router will automatically reestablish your connection. To use this option, select Keep Alive. **Wireless-G Router for 3G/UMTS Broadband 22 Chapter3 Advanced Configuration Access Restrictions > Internet Access** The Internet Access screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.

Summary Status Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and select Enabled. To create a policy, follow steps 1-11. Repeat these steps to create additional policies, one at a time. 1. Select a number from the Access Policy drop-down menu. 2. Enter a Policy Name in the field provided. 3. To enable this policy, select Enabled. 4. Click Edt Lst 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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361873)

[WRT54G3GV2- VF user guide](http://yourpdfguides.com/dref/2361873)

<http://yourpdfguides.com/dref/2361873>

After making your changes, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Then click **Close**. **Access Restrictions > Internet Access Internet Access Policy Access Policy Access** can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the dropdown menu will display that policy's settings.

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

Wireless-G Router for 3G/UMTS Broadband 23 Chapter3 Advanced Configuration Applications and Gaming > Single Port Forwarding The Single Port Forwarding screen allows you to customize port services for common applications on this screen. When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the **DHCP Reservation** feature on the **Basic Setup** screen). 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 **2 Hours**. 7. You can block websites with specific URL addresses. Enter each URL in a separate **Website Blocking by URL Address** field.

8. You can also block websites using specific keywords. Enter each keyword in a separate **Website Blocking by Keyword** field. 9. You can filter access to various services accessed over the Internet, such as **FTP** or **telnet**.

(You can block up to three applications per policy.) From the **Applications** list, select the application you want to block. Then click the **>>** button to move it to the **Blocked List**. To remove an application from the **Blocked List**, select it and click the **<<** button. 10.

If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the **Application Name** field. Enter its range in the **Port Range** fields. Select its protocol from the **Protocol** drop-down menu. Then click **Add**. To modify a service, select it from the **Application** list.

Change its name, port range, and/or protocol setting. Then click **Modify**. To delete a service, select it from the **Application** list. Then click **Delete**. 11.

Click **Save Settings** to save the policy's settings. To cancel the policy's settings, click **Cancel Changes**. **Applications and Gaming > Single Port Forwarding Single Port Forwarding Common** applications are available for the first five entries. Select the appropriate application. Then enter the IP address of the server that should receive these requests. Select **Enabled** to activate this entry. For additional applications, complete the following fields: **Application Name** Enter the name you wish to give the application. Each name can be up to 12 characters. **External Port** Enter the external port number used by the server or Internet application. Check with the Internet application documentation for more information.

Internal Port Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information. **Protocol** Select the protocol used for this application, either **TCP** or **UDP**, or **Both**. **To IP Address** For each application, enter the IP address of the PC that should receive the requests. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the **Basic Setup** screen to look up its static IP address.

Wireless-G Router for 3G/UMTS Broadband 2 Chapter3 Advanced Configuration To IP Address For each application, enter the IP address of the PC running the specific application. If you assigned a static IP address to the PC, then you can click **DHCP Reservation** on the **Basic Setup** screen to look up its static IP address. **Enabled** Select **Enabled** to enable port forwarding for the applications you have defined. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. **Enabled** For each application, select **Enabled** to enable port forwarding.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. **Applications and Gaming > Port Range Forwarding The Port Range Forwarding** screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the **DHCP Reservation** feature on the **Basic Setup** screen). If you need to forward all ports to one computer, click the **DMZ** tab. **Applications & Gaming > Port Range Triggering The Port Range Triggering** screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. **Applications and Gaming > Port Range Triggering 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** Enter the number or range of port(s) used by the server or Internet applications. Check with the Internet application documentation for more information. **Protocol** Select the protocol used for this application, either **TCP** or **UDP**, or **Both**. **Wireless-G Router for 3G/UMTS Broadband Application Name** Enter the application name of the trigger. **Triggered Range** For each application, enter the starting and ending port numbers of the triggered port number range. Check with the Internet application documentation for the port number(s) needed. **Forwarded Range** For each application, enter the starting and ending port numbers of the forwarded port number range.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361873)

[WRT54G3GV2-VF user guide](http://yourpdfguides.com/dref/2361873)

<http://yourpdfguides.com/dref/2361873>