



# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WRT610N. You'll find the answers to all your questions on the LINKSYS WRT610N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual LINKSYS WRT610N  
User guide LINKSYS WRT610N  
Operating instructions LINKSYS WRT610N  
Instructions for use LINKSYS WRT610N  
Instruction manual LINKSYS WRT610N

LINKSYS® by Cisco



USER GUIDE

**Simultaneous Dual-N Band  
Wireless Router**

Model: WRT610N (EU)



[You're reading an excerpt. Click here to read official LINKSYS WRT610N user guide](http://yourpdfguides.com/dref/2361888)  
<http://yourpdfguides.com/dref/2361888>

**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. Simultaneous Dual-N Band Wireless Router i Table of Contents Chapter 1: Product Overview 3 Front Panel . . . .*

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

*3 Chapter 2: Wireless Security Checklist 5 General Network Security Guidelines . . . . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. . . 5 Additional Security Tips . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. . . . . 5 Chapter 3: Advanced Configuration 6 Setup > Basic Setup .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. . . 6 Setup > MAC Address Clone . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. .11 Setup > Advanced Routing . . . . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*.11 Wireless > Basic Wireless Settings . . . . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. . . . .12 Wireless > Wireless MAC Filter. . . . .*

. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
. . . . .  
*. . . .16 Wireless > Advanced Wireless Settings .*

.....  
.....  
*.17 Security > Firewall . . . .*  
.....

.....  
.....  
.....  
*.18 Security > VPN Passthrough . . . . .*  
.....  
.....  
.....

.....  
*18 Storage > Disk . . . . .*  
.....  
.....

.....  
.....  
.....  
*. . . . .19 Storage > Media Server. . .*  
.....  
.....  
.....

.....  
*. . . . .20 Storage > FTP Server .*  
.....  
.....  
.....

.....  
.....  
.....  
*. .21 Storage > Administration . . . . .*  
.....  
.....  
.....

*. .22 Access Restrictions > Internet Access . . . . .*  
.....  
.....  
.....

*. . . . .23 Applications and Gaming > Port Range Forwarding . . . . .*  
.....  
.....  
*. . . . .25 Applications & Gaming > Port Triggering . .*

.....  
.....  
.....  
*. . . . .25 Applications and Gaming > DMZ . .*  
.....  
.....  
.....

*. . .26 Applications and Gaming > QoS . . . . .*

	.....
	.....
	.....
.....	<i>26 Administration &gt; Management.</i>
	.....
	.....
	.....
	.....
	.....
	<i>29 Administration &gt; Log . . . .</i>
	.....
	.....
	.....
.....	<i>29 Administration &gt; Diagnostics .</i>
	.....
	.....
	.....
.....	<i>30 Administration &gt; Factory Defaults . . .</i>
	.....
	.....
	.....
	.....
	<i>30 Administration &gt; Firmware Upgrade . . .</i>
	.....
	.....
	.....
	<i>30 Status &gt; Router . . . . .</i>
	.....
	.....
	.....
	.....
	<i>31 Status &gt; Local Network . . . . .</i>
	.....
	.....
	.....
	.....
	<i>31 Status &gt; Wireless Network .</i>
	.....
	.....
	.....
.....	<i>32 Appendix A: Troubleshooting Appendix B: How to Install and Access USB Storage 33 34 Overview . . . . .</i>
	.....
	.....
	.....
	.....
	.....
	.....
	<i>34 How to Install the USB Storage . . . . .</i>



. . . . .47 CE Marking . . . . .

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

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

. . . . .47 National Restrictions . . . . .

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

. . . . .47 Product Usage Restrictions . . . . .

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

. . . . .  
. . . . .

.48 Technical Documents on [www.linksys.com/international](http://www.linksys.com/international) . . . . .

. . . . .

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

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

. . . . .49 Appendix F: Software License Agreement 53 Software in Linksys Products . . . . .

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

. . . . .  
. . . . .

.53 Software Licenses . . . . .

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

.53 Simultaneous Dual-N Band Wireless Router ii Chapter 1 Product Overview Wireless (Blue) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network. Internet (Green/Blue) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port. The LED lights up Green when it is connected to 10/100 port and Blue when it is connected to a gigabit port. USB (Blue) The USB LED lights up when a USB device is attached. If the LED is flashing, the data is being sent or received through this device. Power (Blue) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash.

When the diagnostic is complete, the LED will be solidly lit. Chapter 1: Product Overview Thank you for choosing the Dual-Band Wireless-N Gigabit Router with Storage Link. The Router lets you access the Internet via a wireless connection or through one of its four switched ports. With the built-in storage link, you can easily add gigabytes of storage space onto your network using USB 2.0 hard drives, or plug in a USB flash disk to access your portable data files. The built-in media server streams music, video and photos from the attached storage device to any UPnP-compatible media adapter. Configuring the Router is easy using the provided browser-based utility. Front Panel 1, 2, 3, 4 (Green/Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port.

The LED lights up Green when it is connected to 10/100 port and Blue when it is connected to a gigabit port. Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s). To use Wi-Fi Protected Setup, run the Linksys Easy Link Advisor (LELA) , or refer to the "Wireless > Basic Wireless Settings" section of "Chapter 3: Advanced Configuration". Wi-Fi Protected Setup (WPS) LED (Blue/ Amber) The LED flashes blue for two minutes during the WPS process and lights up blue when the WPS process is successful. The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again. The LED flashes when a Wi-Fi Protected Setup session is active.



[You're reading an excerpt. Click here to read official LINKSYS  
WRT610N user guide](http://yourpdfguides.com/dref/2361888)  
<http://yourpdfguides.com/dref/2361888>

The Router supports one session at a time. Wait until the LED is solidly lit, or off before starting the next Wi-Fi Protected Setup session.

**Simultaneous Dual-N Band Wireless Router Back Panel USB Port** For use with an external hard drive. Internet The Internet port is where you will connect your cable or DSL Internet connection. 1, 2, 3, 4 These Ethernet ports (1, 2, 3, 4) connect the Router to PCs on your wired network and other Ethernet network devices. Reset There are two ways to reset the Router's factory defaults. Either press and hold the Reset Button for approximately five seconds, or restore the defaults from Administration > Factory Defaults in the Router's web-based utility. Power The Power port is where you will connect the power adapter. 3 Chapter 1 Product Overview Follow these instructions: 1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.

2. Drill two holes into the wall. Make sure the holes are 175.56 mm (6.91 inches) apart.

3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed. 4. Maneuver the Router so the wall-mount slots line up with the two screws. 5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots. Horizontal Placement The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet. Wall-Mounting Placement The Router has two wall-mount slots on its bottom panel. The distance between the slots is 175.56 mm (6.91 inches). Two screws are needed to mount the Router. Suggested Mounting Hardware 2.

5-3.0 mm 4-5 mm true to scale. 1-1.5 mm Note: Mounting hardware illustrations are not NOTE: Linksys is not responsible for damages incurred by unsecure wall-mounting hardware. 175.56 mm Simultaneous Dual-N Band Wireless Router 4 Chapter 2 Wireless Security Checklist Chapter 2: Wireless Security Checklist Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure. 4.

Enable encryption Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication. A network encrypter to learn about the web-based utility. How to Access the Web-Based Utility To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, 192.168.

1.1 or <http://wrt610n.com> in the Address field. Then, press Enter. A password request screen will appear.

@@@ (You can set a new password on the Administration > Management screen.) Click OK to continue. Setup > Basic Setup Language Language To use a different language, select one from the drop-down menu. The language of the web-based utility will change five seconds after you select another language. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Internet Setup The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your Internet Service Provider (ISP). Internet Connection Type Select the type of Internet connection your ISP provides from the drop-down menu. The available types are: · Password Screen Automatic Configuration - DHCP Static IP PPPoE PPTP L2TP Telstra Cable · · · · Simultaneous Dual-N Band Wireless Router 6 Chapter 3 Advanced Configuration Service Name (optional) If provided by your ISP, enter the Service Name. Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time).

If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds. Automatic Configuration - DHCP By default, the Router's Internet Connection Type is set to Automatic Configuration - 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. Internet Connection Type > Static IP PPTP Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only. 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 enter 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 Gateway Address, which is the ISP server's IP address. DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address. 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 > PPTP If your ISP supports DHCP or you are connecting through a dynamic IP address, then select Obtain an IP Address Automatically.

If you are required to use a permanent IP address to connect to the Internet, then select Specify an IP Address. Then configure the following: 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).



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

[WRT610N user guide](#)

<http://yourpdfguides.com/dref/2361888>



Your ISP will provide you with the Subnet Mask. Internet Connection Type > PPPoE Default Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address. DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Server IP Address Your ISP will provide you with the Server IP Address. User Name and Password Enter the User Name and Password provided by your ISP.

Simultaneous Dual-N Band Wireless Router 7 Chapter 3 Advanced Configuration 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. User Name and Password Enter the User Name and Password provided by your ISP. Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again.

To use this option, select Connect on Demand. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection.

To use this option, select Keep Alive. In the Redial Period field, specify how often you want the Router to check the Internet connection. The default value is 30 seconds. Telstra Cable Telstra Cable is a service that applies to connections in Australia only. Internet Connection Type > Telstra Cable L2TP L2TP is a service that applies to connections in Israel only.

Server IP Address This is the IP address of the Telstra Cable. Your ISP will provide you with the IP Address you need to specify here. User Name and Password Enter the User Name and Password provided by your ISP. Optional Settings Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Internet Connection Type > L2TP 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. 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. Optional Settings 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, Static IP, or Telstra: 1500 PPPoE: 1492 PPTP or L2TP: 1460 8 Simultaneous Dual-N Band Wireless Router Chapter 3 Advanced Configuration Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address.

The default is 0 minutes, which means one day. Static DNS (1-3) The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here.

The Router will use these for quicker access to functioning DNS servers. WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank. DHCP Reservation Click DHCP Reservation if you want to assign a fixed local IP address to a MAC address. 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 Address This presents both the Router's IP Address, Subnet Mask, and URL Address as seen by your network. The default Router IP address is 192.168.

1.1 and URL address is http://WRT610N.com. 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. Network Address Server Settings (DHCP) DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select 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. DHCP Reservation You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>

Click the Select checkbox to reserve a client's IP address. Then click Add Clients.

If you want 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. Make sure the IP address is between the starting DHCP server's IP address and maximum number of DHCP users range. Enter its MAC Address in the To This MAC Address field. Click Add. 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. Simultaneous Dual-N Band Wireless Router 9 Chapter 3 Advanced Configuration Password Enter the Password for your DDNS account. Host Name The is the DDNS URL assigned by the DDNS service. WildCard Select Enabled to enable this feature or Disabled to disable it.

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 Update. Time Setting When you finish your changes, click Save Settings to save your changes.

Click Cancel Changes to cancel your changes. To view the most up-to-date information, click Refresh. To exit this screen, click Close. 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.)

) Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. TZO.com 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. Setup > DDNS > TZO 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. E-mail Address, TZO Password, and Domain Name Enter the settings of the account you set up with TZO. Internet IP Address The Router's Internet IP address is displayed here.

Because it is dynamic, it will change. Status The status of the DDNS service connection is displayed here. Update To manually trigger an update, click Update. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. DynDNS.

org Setup > DDNS > DynDNS User Name Enter the User Name for your DDNS account. Simultaneous Dual-N Band Wireless Router 10 Chapter 3 Advanced Configuration Setup > Advanced Routing This screen is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.

Setup > MAC Address Clone Every computer hardware device, including the network adapter of your computer has a unique code called a MAC address. Some Internet Service Providers (ISPs) require you to register this address with them in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.

Setup > MAC Address Clone Setup > Advanced Routing MAC Address Clone Enabled/Disabled To enable MAC Address cloning, select Enabled. User Defined Entry Enter the MAC Address registered with your ISP here. Clone Your PC's MAC Clicking this button will clone the MAC address of the computer you are using. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Advanced Routing NAT If this Router is hosting your network's connection to the Internet, select Enabled. When NAT is disabled, Dynamic Routing (RIP) will be available as an option. Dynamic Routing (RIP) 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. This feature is Disabled by default. Static Routing Select Route Entry number To set up a static route between the Router and another network, select a number from the drop-down list. (A static route is a predetermined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click Delete This Entry to delete a static route.) Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters. Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

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.

Simultaneous Dual-N Band Wireless Router 11 Chapter 3 Advanced Configuration Network Mode (5 GHz) From this drop-down menu, you can select the wireless standards running on your network.

If you have both Wireless-A and Wireless-N (5GHz) devices in your network, keep the default setting, Mixed. If you have only Wireless-A devices, select Wireless-A Only. If you have only Wireless-N (5GHz) devices, select Wireless-N Only. If you do not have any Wireless-A and Wireless-N (5GHz) devices in your network, select Disabled. Network Mode (2.

4 GHz) From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, keep the default setting, Mixed. If you have only Wireless-B devices, select Wireless-B Only. If you have only Wireless-G devices, select Wireless-G Only.

If you have only Wireless-N (2.4GHz) devices, select Wireless-N Only. If you do not have any Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, select Disabled. Wireless Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 keyboard characters. Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name. Radio Band (5 GHz) For best performance in a network using Wireless-A and Wireless-N (5GHz) devices, keep the default, Auto.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>

**Radio Band (2.4 GHz)** For best performance in a network using Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices, select Auto. The default is Standard - 20MHz Channel. **Wide Channel (5 GHz)** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (5GHz) channel. If you are not sure which channel to select, keep the default, Auto (DFS). **Wide Channel (2.4 GHz)** If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (2.4GHz) channel. If you are not sure which channel to select, keep the default, Auto.

**Standard Channel (5 GHz)** Select the channel for Wireless-A and Wireless-N (5GHz) networking. If you selected Wide 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (5GHz). If you are not sure which channel to select, keep the default, Auto (DFS). **Gateway** This is the IP address of the gateway device that allows for contact between the Router and the remote network or host. **Interface** This interface tells you whether the Destination IP Address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet).

Click **Show Routing Table** to view the Static Routes you have already set up. **Routing Table** 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. **Wireless > Basic Wireless Settings** **Wireless Configuration** **Wireless Configuration** Keep the default selection, **Wi-Fi Protected Setup** to configure your network using **Wi-Fi Protected Setup**. Select **Manual** to set up your wireless network your wireless network manually.

**Manual** If you set the **Wireless Configuration** to **Manual**, the **Basic Wireless Settings** screen displays the following fields. **Simultaneous Dual-N Band Wireless Router 12 Chapter 3 Advanced Configuration Method #1** Use this method if your client device has a **Wi-Fi Protected Setup** button. 1. Click or press the **Wi-Fi Protected Setup** button on the client device. 2. Click the **Wi-Fi Protected Setup** button on this screen. 3. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions. **Standard Channel (2.4 GHz)** Select the channel for Wireless-B, Wireless-G and Wireless-N (2.4GHz) networking. If you selected **Wide 40MHz Channel** for the **Radio Band** setting, then the **Standard Channel** will be a secondary channel for Wireless-N (2.4GHz). If you are not sure which channel to select, keep the default, Auto. **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. **Method #2** Use this method if your client device has a **Wi-Fi Protected Setup PIN** number.

1. Enter the PIN number from the client device in the field on this screen. 2. Click the **Register** button. 3.

After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions. **Wi-Fi Protected Setup** There are three methods available. Use the method that applies to the client device you are configuring. **Method #3** Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.) 2. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions. The **Wi-Fi Protected Setup Status**, **Network Name (SSID)**, **Security**, **Encryption**, and **Passphrase** are displayed at the bottom of the screen. **NOTE:** If you have client devices that do not support **Wi-Fi Protected Setup**, note the wireless settings, and then manually configure those client devices. **Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)** **NOTE:** **Wi-Fi Protected Setup** configures one client device at a time. Repeat the instructions for each client device that supports **Wi-Fi Protected Setup**.

**Simultaneous Dual-N Band Wireless Router 13 Chapter 3 Advanced Configuration 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.) **Wireless > Wireless Security** The **Wireless Security** settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: **WPA Personal**, **WPA Enterprise**, **WPA2 Personal**, **WPA2 Enterprise**, **RADIUS**, and **WEP**. (WPA stands for **Wi-Fi Protected Access**, which is a security standard stronger than WEP encryption. WEP stands for **Wired Equivalent Privacy**, while RADIUS stands for **Remote Authentication Dial-In User Service**.) These six are briefly discussed here. For detailed information on setting up wireless security networks, refer to "Chapter 2: Wireless Security." **Wireless Security Security Mode** Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

**WPA Personal** **NOTE:** If you are using WPA or WPA2, each device in your wireless network **MUST** use the same WPA or WPA2 method and shared key, or else the network will not function properly. **WPA Enterprise Encryption** WPA supports two encryption methods, **TKIP** and **AES**, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**. **RADIUS Server** Enter the IP Address of the RADIUS server.

**RADIUS Port** Enter the port number of the RADIUS server. The default value is 1812. **Shared 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** period is 3600 seconds.

**WPA2 Personal** **WPA Personal Encryption** WPA supports two encryption methods, **TKIP** and **AES**, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**. **Passphrase** Enter a passphrase of 8-63 characters. **Key Renewal** Enter a **Key Renewal** period, which instructs the Router how often it should change the encryption keys. The default **Key Renewal** period is 3600 seconds. **WPA2 Personal** **Simultaneous Dual-N Band Wireless Router**

**14 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.) **Encryption** WPA2 supports two encryption methods with dynamic encryption keys; **AES** or **WPA-TKIP/WPA2AES**. You must select **WPA-TKIP** or **WPA2-AES** to connect to the Router.

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



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>

**Key Renewal** Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is 3600 seconds. WPA2 Enterprise This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS WPA2 Enterprise Encryption WPA2 supports two encryption methods with dynamic encryption keys; AES or WPA-TKIP/WPA2AES. You must select WPA-TKIP or WPA2-AES to connect to the Router. 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 time out period is 3600 seconds. **IMPORTANT:** If you are using WEP encryption, always 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 value is 1812. **Shared Key** Enter the key shared between the Router and the server. **Encryption** Select a level of WEP encryption, 64 bits 10 hex digits or 128 bits 26 hex digits. The default is 64 bits 10 hex digits.

**Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click Generate. **Key 1-4** If you did not enter a Passphrase, enter the WEP key(s) manually. **Tx Key** Select a key from the drop-down menu. *Simultaneous Dual-N Band Wireless Router 15 Chapter 3 Advanced Configuration Wireless > Wireless MAC Filter* Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. WEP WEP is a basic encryption method that is not as secure as WPA. WEP Encryption Select a level of WEP encryption, 64 bits 10 hex digits or 128 bits 26 hex digits. The default is 64 bits 10 hex digits. **Passphrase** Enter a Passphrase to automatically generate WEP keys. Then click Generate.

**Key 1-4** If you did not enter a Passphrase, enter the WEP key(s) manually. **Tx Key** Select a key from the drop-down menu. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. *Wireless > Wireless MAC Filter* Wireless MAC Filter Access Restriction 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 PCs listed below from accessing the wireless network Select this to block wireless access by MAC Address. This option is selected by default. Permit PCs listed below to the wireless network Select this to allow wireless access by MAC Address. This option is not selected by default. **MAC Address Filter List** Click the Wireless Client List button to display the Wireless Client List.

It shows computers and other devices on the wireless network. Click the Save to MAC Address Filter List checkbox for any device you want to add to the MAC Address Filter List. Then click the Add button. To retrieve the most up-to-date information, click the Refresh button. To exit this screen and return to the Wireless MAC Filter screen, click the Close button.

*Simultaneous Dual-N Band Wireless Router 16 Chapter 3 Advanced Configuration Frame Burst* Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use the Frame Burst option, select Enabled. The default is Disabled. **Authentication Type** The default is set to Auto, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication.

With Shared Key authentication, the sender and recipient use a WEP key for authentication. **Basic Rate** The Basic Rate setting is not one, but a series of rates at which the Router can transmit. (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.) The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is Default, when the Router can transmit at all standard wireless rates.. **Transmission Rate** The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature.

**Auto-Fallback** will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto. **CTS Protection Mode** CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your wireless products not being able to transmit to the Router in an environment with heavy latency wireless traffic. This function boosts the Router's ability to catch all wireless transmissions but will severely decrease performance. The default value is Auto. **Beacon Interval** A beacon is a packet broadcast by the Router to synchronize the wireless network. Enter a value between 20 and 1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. The default value is 100. **DTIM Interval** This value, between 3 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 3. **Wireless Client List MAC XX** Enter the MAC addresses of the devices whose wireless access you want to control.

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 AP Isolation* This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select Enabled. AP Isolation is disabled by default. *Simultaneous Dual-N Band Wireless Router 17 Chapter 3 Advanced Configuration Filter Multicast* Multicasting allows for multiple transmissions to specific recipients at the same time.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>



If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. It is selected by default. Deselect this feature to disable it. Filter Internet NAT Redirection This feature is used to prevent a local computer from using a URL or Internet address to access the local server. Select Filter Internet NAT Redirection to filter Internet NAT redirection. It is not selected by default. Filter IDENT (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network.

It is selected by default. Deselect this feature to disable it. Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346. RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame.

After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Web Filters Filters Select to filter Proxy, Java, ActiveX, and Cookies. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Security > Firewall The Security > Firewall screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network. Security > 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 Security > Firewall Firewall SPI Firewall Protection To use firewall protection, keep the default selection, Enabled. To turn off firewall protection, select Disabled. IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer.

To allow IPSec tunnels to pass through the Router, keep the default, Enabled. PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enabled. L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. 18 Internet Filters 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. Simultaneous Dual-N Band Wireless Router Chapter 3 Advanced Configuration Storage > Disk An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

The Disk screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk. Shared Folder Screen Storage > Disk Shared Folder Screen Use this screen to add a Shared folder. Display Name Enter a display name that will appear in the Shared Folder table of the Disk screen. @@Location The location of the shared folder is displayed. @@@@Select a folder name to share. To see a sub-folder, click Enter into Folder. To return to the previous folder, click Return to Upper Folder. @@@@You can allow Read and Write or Read Only access. @@Click Close to exit the screen.

Disk Detail If a formatted disk is attached to the Router, you can view the Partition, File System, Capacity, and Free Space information for each partition of the disk. Click Create Share to create a shared folder. Safely Remove Disk Before physically disconnecting a disk from the Router, click Safely Remove first. This prevents the possible loss of data, if the disk is removed while data is transferring to or from the disk. If you click Create Share, the Shared Folder screen appears.

Simultaneous Dual-N Band Wireless Router 19 Chapter 3 Advanced Configuration Database This section lets you select content to add to the database of the Router's media server. Click Specify Folder to Scan to add a media folder to the Database table. If you click Specify Folder to Scan, the Media Folder screen appears. Shared Folder Each Display Name you created on the Shared Folder screen will be listed with its partition and shared folder, which you can edit or delete. Select Edit to edit an item or Delete to delete the item.

If you click the Edit, the Shared Folder screen appears. Refer to the "Shared Folder Screen" section above. Format Disk Select the disk you want to format, then click Format Disk to format the disk and create a new partition. If your hard drive is formatted with multiple partitions, it will delete them and create a single partition. Enter the name of the partition you want to format. Select Format to start the formatting or Cancel to cancel it before it begins. Media Folder Screen Use this screen to add a Media folder. Format Disk Storage > Media Server An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature. Media Folder Display Name Enter a display name that will appear in the Database table of the Media Server screen. @@Location The location of the shared folder is displayed.

@@@@@Select a folder name to share. To see a sub-folder, click Enter into Folder. To return to the previous folder, click Return to Upper Folder. @@Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. For more information, click Help. Storage > Media Server Setup Server Name The name of the router's media server is displayed here. It can be changed on the Storage > Administration screen. UPnP Media Server To use the Router's media server function, select Enabled. Otherwise, select Disabled. Simultaneous Dual-N Band Wireless Router 20 Chapter 3 Advanced Configuration Storage > FTP Server An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature. The FTP Server tab creates an FTP Server that can be accessed from the Internet or your local network.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>

*Storage > FTP Server Setup Server Name* The name of the Router's FTP server is displayed here. It can be changed on the *Storage > Administration* screen. *FTP Server Select Enabled* to set this Router as an FTP Server. Otherwise, select *Disabled* to turn the service off. An external USB hard drive or USB disk must be connected to the USB Port to use this service. *Internet Access Select Enabled* to allow access of the FTP Server from the Internet. Otherwise, select *Disabled* to only allow local network access. *FTP Port* Enter the FTP Port number to use. The default port is 21. *FTP Folder Screen Display Name* Enter a display name that will appear in the Access table of the FTP Server screen. @@Location The location of the shared folder is displayed. @@@@Select a folder name to share. To see a sub-folder, click *Enter into Folder*. To return to the previous folder, click *Return to Upper Folder*. @@@@You can allow *Read and Write* or *Read Only* access. To add more groups, go to the *Storage > Administration* screen. Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes. Click *Close* to close the screen. Each Display Name you created on the FTP Folder screen will be listed with its partition and folder, which you can edit or delete.

Select *Edit* to edit an item or *Delete* to delete the item. Access This section lets you add FTP folders that can be accessed through the FTP client. Click *Specify Folder to Access* to add a FTP folder to the Access table. If you click *Specify Folder to Access*, the FTP Folder screen appears. FTP Folder Screen Use this screen to add an FTP folder. *Simultaneous Dual-N Band Wireless Router 21 Chapter 3 Advanced Configuration User Management* The available users are listed in the User Management table. The two default users, Admin (read and write access) and Guest (read-only access) cannot be deleted. Click *Create New User* to create a new user. If you click *Create New User*, the User Account screen appears. Each user you created on the User Account screen will be listed with its group, which you can edit or delete.

Select *Edit* to edit a user or *Delete* to delete the user. If you click *Edit*, the User Account screen appears. Refer to the "User Account Screen" section. If you click *Edit*, the FTP Folder screen appears. Refer to the "FTP Folder Screen" section above.

Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes. For more information, click *Help*. *Storage > Administration The Administration* screen allows you to manage the users and groups of users that can access the shares. *User Account Storage > Administration User Account Screen* Users can be added, edited or deleted through the User Account screen: 1. Enter a user name for the user. 2. Enter the full name and description for the user. 3. Enter a password and enter it again in the *Confirm Password* field. 4. Select *Admin* or *Guest* from the *Group Member* dropdown menu. You can create a new group in the *Group Management* section. 5. Click *Save Settings* to save the new changes, or click *Cancel Changes* to cancel the changes. Click *Close* to close the screen.

*Information Server Name* Enter a name that will be used for the network storage FTP and Media server. Punctuation, spaces, and other special characters (e.g., \*/\ ) cannot be used in the name. *Workgroup Name* Enter the Workgroup Name of your Router in the local network. The (FTP and Media) Server LAN IP Address and the (FTP) Server Internet IP Address are displayed here. *Simultaneous Dual-N Band Wireless Router 22 Chapter 3 Advanced Configuration Access Restrictions > Internet Access The Access Restrictions > Internet Access* screen allows you to deny or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times. *Group Management* The groups are listed in the *Group Management* table. There are two default groups, Admin and Guest; these cannot be deleted. Click *Create New Group* to create a new group. If you click *Create New Group*, the Group Account screen appears. Each group you created on the Group Account screen will be listed with its access rights, which you can edit or delete. Select *Edit* to edit a user or *Delete* to delete the user. If you click *Edit*, the Group Account screen appears. Refer to the "Group Account Screen" section.

Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes. For more information, click *Help*. *Group Account Access Restrictions > Internet Access Group Account Screen* Groups can be added, edited or deleted: 1. Enter a name for the group. 2. Enter a description for the group. 3. Select *read and write* or *read only* access. 4. Click *Save Settings* to save the new changes, or click *Cancel Changes* to cancel the changes. Click *Close* to close the screen. *Internet Access Internet Access Policy* Internet 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*. *Deny or Allow* If you select *Deny*, the PC on the *Edit List* will be denied Internet Access by the dates and times selected. PCs not on the list will still have Internet access. If you select *Allow*, the PCs on the *Edit List* will have Internet access by the dates and times selected. The PCs not on the *Edit List* will be denied Internet access. If there is a conflict with a policy, the lower numbered policy will have priority over a higher numbered policy. To create an Internet Access Policy: 1. Select a number from the *Internet Access Policy* dropdown menu. 2. Enter a Policy Name in the field.

3. To enable this policy, select *Enabled*. *Simultaneous Dual-N Band Wireless Router 23 Chapter 3 Advanced Configuration* Click *Save Settings* to apply your changes, or click *Cancel Changes* to cancel your changes. 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*. *Applications and Gaming > Single Port Forwarding* The *Single Port Forwarding* screen allows you to customize port services for common applications. 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. *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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2361888)

[WRT610N user guide](http://yourpdfguides.com/dref/2361888)

<http://yourpdfguides.com/dref/2361888>

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.

Enter a URL address or Keyword for Website Blocking or select any Blocked Applications you wish to use. Using these features can slow down your Internet speed. 8. Click Save Settings to save the policy's settings, or click Cancel Changes to cancel the policy's settings. Applications and Gaming > Single Port Forwarding Single Port Forwarding To forward a port, enter the information on each line for the criteria required. Application Select a pre-configured application, or enter the name you wish to give the application. Each name can have up to 12 characters. External and Internal Port Enter the external and internal port numbers. Protocol Select the protocol used for this application, either TCP or UDP. IP Address For each application, enter the IP address of the computer that should receive the requests.

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. Blocked Applications You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting applications from the Applications List. To add an application, 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 an application, select it from the Application List. Change the application name, port range, or protocol setting. Then click Modify.

To delete an application, select it from the Application List. Then click Delete. Simultaneous Dual-N Band Wireless Router 24 Chapter 3 Advanced Configuration Applications & Gaming > Port Triggering The Applications & Gaming > Port Triggering screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules. Applications and Gaming > Port Range 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.) Applications and Gaming > Port Triggering Applications and Gaming > Port Range Forwarding Port Triggering Application Enter the application name of the trigger. Port Range Forwarding To forward a port, enter the information on each line for the criteria required. Application In this field, enter the name you wish to give the application.

Each name can be up to 12 characters. Start/End This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column. Protocol Select the protocol used for this application, either TCP or UDP, or Both. IP Address For each application, enter the IP Address of the PC running the specific application. 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. Triggered Range For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed. Start Port Enter the starting port number of the Triggered Range.

End Port Enter the ending port number of the Triggered Range. Forwarded Range For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed. Start Port Enter the starting port number of the Forwarded Range. End Port Enter the ending port number of the Forwarded Range.

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. Simultaneous Dual-N Band Wireless Router 25 Chapter 3 Advanced Configuration Applications and Gaming > QoS Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing. 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 Forward feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. Applications and Gaming > DMZ DMZ Any PC whose port is being forwarded should have its DHCP client function disabled and have a new static IP address assigned to it because its IP address may change when using the DHCP function. To allow PCs on the Internet to access a local PC, select Enabled. Then, select Any IP Address or manually enter a specific source IP address of the computer you want to allow access from the Internet. Then, enter your local PC's IP address or MAC address that you want to allow access to. This feature is disabled by default. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Applications and Gaming > QoS QoS (Quality of Service) Wireless Wireless WMM (Wi-Fi Multimedia) WMM is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, your wireless client devices in your network must support Wireless WMM. If you would like to disable this feature, select Disabled.

Otherwise, keep the default, Enabled. No Acknowledgement If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, select Enabled. Otherwise, keep the default, Disabled. Internet Access Priority In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels of priority; High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority. Enabled/Disabled To use the QoS policies you set, select Enabled.



[You're reading an excerpt. Click here to read official LINKSYS WRT610N user guide](http://yourpdfguides.com/dref/2361888)  
<http://yourpdfguides.com/dref/2361888>