



# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WRT320N. You'll find the answers to all your questions on the LINKSYS WRT320N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual LINKSYS WRT320N  
User guide LINKSYS WRT320N  
Operating instructions LINKSYS WRT320N  
Instructions for use LINKSYS WRT320N  
Instruction manual LINKSYS WRT320N

LINKSYS® by Cisco



USER GUIDE

**Dual-Band Wireless-N  
Gigabit Router**

Model: WRT320N



[You're reading an excerpt. Click here to read official LINKSYS WRT320N user guide](http://yourpdfguides.com/dref/2315731)  
<http://yourpdfguides.com/dref/2315731>

**Manual abstract:**

S. and certain other countries. Copyright © 2009 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders. Dual-Band Wireless-N Gigabit Router i Table of Contents Chapter 1: Product Overview 4 Front Panel. . . .

.....  
.....

.....  
.....

..... 4 Back Panel .....

.....  
.....

.....  
.....

.....  
.....

4 Placement Positions .....

.....  
.....

.....  
.....

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

.....  
.....

.....  
.....

.. 6 Additional Security Tips .....

.....  
.....

.....  
.....

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

.....  
.....

.....  
.....

.....  
.....

..... 7 Setup > DDNS. . .

.....  
.....

.....  
.....

.....  
.....

11 Setup > MAC Address Clone. ....

.....  
.....

.....  
.....

....12 Setup > Advanced Routing .....

.....  
.....

.....  
.....



.....  
...22 Administration > Management . .

.....

.....

.....

.....

.....24 Administration > Log . . . . .

.....

.....

.....

.....

.....25 Administration > Diagnostics . .

.....

.....

.....

.....

.....

.26 Administration > Factory Defaults . . . .

.....

.....

.....

.....

.26 Administration > Firmware Upgrade . . . . .

.....

.....

.....

...27 Status > Router . . . . .

.....

.....

.....

.....

.....

.27 Status > Local Network . . . .

.....

.....

.....

.....

.....

...27 Status > Wireless Network . . . . .

.....

.....

.....

.....

...28 Appendix A: Troubleshooting Appendix B: Specifications Appendix C: Warranty Information 29 30 31 Limited Warranty . . . . .

.....

.....

.....

.....

.....

...31 Exclusions and Limitations.

.....

.....

.....

.....

.....31 Obtaining Warranty Service .

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

.....31 Technical Support ..

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

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

.. @@.....

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

.....33 FCC Radiation Exposure Statement ..

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

.....  
..33 Safety Notices...  
.....

.....  
.....

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

33 Industry Canada Statement .....

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

.....33 Avis d'Industrie Canada.

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

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

.34 Wireless Disclaimer .....

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

.... @@.....

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

@ @.....

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

.. @@..

.....

.....  
.....  
.....  
.....39 Software Licenses.....

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

.....

39 Dual-Band Wireless-N Gigabit Router iii 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 (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. 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 Linksys Dual-band Wireless-N Gigabit Router. The Router lets you access the Internet via a wireless connection or through one of its four switched ports. You can also use the Router to share resources, such as computers.

A variety of security features help to protect your data and your privacy while online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall and NAT technology. Configuring the Router is easy using the provided browser-based utility. Front Panel Back Panel 1, 2, 3, 4 (Green/Blue)

These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. The LED is solidly lit when the Router is connected to a device through that port. It flashes to indicate network activity. Green indicates Gigabit speeds, and blue indicates 10/100 speeds. 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 Setup Wizard, or refer to the "Wireless > Basic Wireless Settings" section of "Chapter 3: Advanced Configuration". Wi-Fi Protected Setup LED (Blue/Amber) It lights up blue when wireless security is enabled.

The LED flashes blue for two minutes during Wi-Fi Protected Setup. 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 amber when a Wi-Fi Protected

Setup session is active, and a second session begins. The Router supports one session at a time. Wait until the LED is off before starting the next Wi-Fi

Protected Setup session. Dual-Band Wireless-N Gigabit Router Internet This Gigabit port is where you will connect your cable or DSL Internet connection. 1,

2, 3, 4 These Gigabit ports (1, 2, 3, 4) connect the Router to computers and other Ethernet network devices on your wired network. 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. Placement Positions There are two ways to physically install the Router.

The first way is to place the Router horizontally on a surface. The second way is to mount the Router on a wall.

Horizontal Placement The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet. 4 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.



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

[WRT320N user guide](#)

<http://yourpdfguides.com/dref/2315731>

2. Drill two holes into the wall. Make sure the holes are 152 mm (6 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. Wall-Mounting Placement The Router has two wall-mount slots on its bottom panel. The distance between the slots is 152 mm (6 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 insecure wall-mounting hardware. 152 mm Print this page at 100% size.

Cut along the dotted line, and place on the wall to drill precise spacing. Wall Mounting Template Dual-Band Wireless-N Gigabit Router 5 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 encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA. 1. Change the default wireless network name or SSID Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use linksys as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks. For example, you could use your name or address. 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.) 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. Internet Connection Type > Automatic Configuration - DHCP Dual-Band Wireless-N Gigabit Router 7 Chapter 3 Advanced Configuration before your Internet connection terminates.

The default Max Idle Time is 15 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection. The default Redial Period is 30 seconds. Static IP If you are required to use a permanent IP address to connect, you need to specify here. Username and Password Enter the Username 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 15 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. 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.

Username and Password Enter the Username 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 15 minutes. Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period field, you specify how often you want the Router to check the Internet connection.

The default Redial Period is 30 seconds. Optional Settings Some of these settings may be required by your ISP. Verify with your ISP before making any changes. Optional Settings Host Name and 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 Dual-Band Wireless-N Gigabit Router 9 Chapter 3 Advanced Configuration DHCP Reservation You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. 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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2315731)

[WRT320N user guide](http://yourpdfguides.com/dref/2315731)

<http://yourpdfguides.com/dref/2315731>

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 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. DHCP Reservation Router IP This presents both the Router's IP Address and Subnet Mask as seen by your network. . 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. . Router IP DHCP Server Setting 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. 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 192.168.1.1, the Start 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 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.

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 10 DHCP Server Setting 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). DHCP Reservation Click this button if you want to assign a fixed local IP address to a MAC address. Dual-Band Wireless-N Gigabit Router Chapter 3 Advanced Configuration DynDNS.org 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. 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.) Setup > DDNS > DynDNS Username Enter the Username for your DDNS account.

Password Enter the Password for your DDNS account. Host Name The is the DDNS URL assigned by the DDNS service. Time Setting System Select the DynDNS service you use: Dynamic, Static, or Custom. The default selection is Dynamic. Mail Exchange (Optional) Enter the address of your mail exchange server, so e-mails to your DynDNS address go to your mail server.

Backup MX This feature allows the mail exchange server to be a backup. To disable this feature, keep the default, Disabled. To enable the feature, select Enabled. If you are not sure which setting to select, keep the default, Disabled. Wildcard This setting enables or disables wildcards for your host.

For example, if your DDNS address is myplace.dyndns.org and you enable wildcards, then x.myplace.dyndns.org will work as well (x is the wildcard). To disable wildcards, keep the default, 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 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. 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. 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.

Dual-Band Wireless-N Gigabit Router 11 Chapter 3 Advanced Configuration Clone My PC's MAC Click this button to 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. TZO.com 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 > 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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/2315731)

[WRT320N user guide](http://yourpdfguides.com/dref/2315731)

<http://yourpdfguides.com/dref/2315731>



Setup > MAC Address Clone A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs will require you to register a MAC address in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature. Setup > Advanced Routing 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. 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. Dual-Band Wireless-N Gigabit Router 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. 12 Chapter 3 Advanced Configuration Wi-Fi Protected Setup. Proceed to the "Wi-Fi Protected Setup" section.

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. 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. 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. Basic Wireless Settings Wireless > Basic Wireless Settings (Manual Setup) Wireless Band This is used to select the 2.4 GHz or 5.

0 GHz band. Network Mode From this drop-down menu, you can select the wireless standards running on your network. If you have Wireless-N, Wireless-G, and Wireless-B devices in your network, keep the default setting, Mixed. If you have only Wireless-G and Wireless-B devices in your network, select BG-Mixed. If you have only Wireless-N devices, select Wireless-N Only. If you have only Wireless-G devices, select Wireless-G Only. If you have only Wireless-B devices, select Wireless-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. Channel Width Select Auto if you want the Router to automatically determine the proper channel width (20 MHz or 40 MHz) to use, or select 20 MHz only (default) if you want the Router to operate in Wireless-B and Wireless-G mode only. For best performance, Auto is recommended.

Wide Channel If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N channel. Select any channel from the drop-down menu. If you are not sure which channel to select, keep the default, Auto. Channel Select a channel from 1 to 11, or Auto (default). 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 13 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. Wireless > Basic Wireless Settings The basic settings for wireless networking are set on this screen. There are two ways to configure the Router's wireless network(s), manual and Wi-Fi Protected Setup. Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup. Configuration View To manually configure your wireless network, select Manual. Proceed to the "Basic Wireless Settings" section.

To use Wi-Fi Protected Setup, select Dual-Band Wireless-N Gigabit Router Chapter 3 Advanced Configuration 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 OK. 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. 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. Wi-Fi Protected Setup There are three methods available. Use the method that applies to the client device you are configuring. 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, 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.



[You're reading an excerpt. Click here to read official LINKSYS WRT320N user guide](http://yourpdfguides.com/dref/2315731)  
<http://yourpdfguides.com/dref/2315731>

For detailed instructions on configuring wireless security for the Router, refer to "Chapter 2: Wireless Security.

"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. 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. 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 OK. Then refer back to your client device or its documentation for further instructions. WPA Personal NOTE: If you are using WPA, always remember that each device in your wireless network MUST use the same WPA method and shared key, or else the network will not function properly. Method #2 Use this method if your client device has a Wi-Fi Protected Setup PIN number. 1. Enter the PIN number in the field on this screen. 2. Click Register. 3. After the client device has been configured, click OK.

Then refer back to your client device or its documentation for further instructions. Dual-Band Wireless-N Gigabit Router 14 Chapter 3 Advanced Configuration Security Mode > WPA Personal 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 Group Key Renewal period is 3600 seconds. Security Mode > WPA Enterprise 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 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 Key Renewal period is 3600 seconds.

WPA2 Personal WPA2 Enterprise This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Security Mode > WPA2 Personal Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP or AES. The default is TKIP or AES. 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 Group Key Renewal period is 3600 seconds. WPA Enterprise This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.

) Security Mode > WPA2 Enterprise Encryption WPA2 supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP or AES. The default is TKIP or AES. RADIUS Server Enter the IP Address of the RADIUS server. RADIUS Port Enter the port number of the RADIUS server. The default value is 1812. Shared Secret Enter the key shared between the Router and the server. Dual-Band Wireless-N Gigabit Router 15 Chapter 3 Advanced Configuration 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. RADIUS This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Security Mode > WEP Encryption Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). The default is 40/64 bits (10 hex digits). 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 manually. Security Mode > RADIUS Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. 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 value is 1812. Shared Secret Enter the key shared between the Router and the server. Encryption Select a level of WEP encryption, 40/64 bits (10 hex digits) or 104/128 bits (26 hex digits). The default is 40/64 bits (10 hex digits). 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 manually. 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. Wireless > Wireless MAC Filter Dual-Band Wireless-N Gigabit Router 16 Chapter 3 Advanced Configuration Wireless MAC Filter Enabled/Disabled To filter wireless users by MAC Address, either permitting or blocking access, select Enabled.

If you do not wish to filter users by MAC Address, keep the default setting, Disabled. Access Restriction Prevent Select this to block wireless access by MAC Address. This option is selected by default. Permit Select this to allow wireless access by MAC Address. This option is not selected by default. MAC Address Filter List Wireless Client List Click this to open the Wireless Client List screen. 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.

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. Wireless Client List 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 Filter List 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 01-50 Enter the MAC addresses of the devices whose wireless access you want to block or allow.

Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Authentication Type The default is set to Auto, which allows either Open System or Shared Key authentication to be used.



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

[WRT320N user guide](#)

<http://yourpdfguides.com/dref/2315731>

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. 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 setting is Default, when the Router can transmit at all standard wireless rates (1-2Mbps, 5.5Mbps, 11Mbps, 18Mbps, and 24Mbps).

Other options are 1-2Mbps, for use with older wireless technology, and All, when the Router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting. Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible 17 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. Dual-Band Wireless-N Gigabit Router Chapter 3 Advanced Configuration 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. connection speed between the Router and a wireless client. The default is Auto.

N Transmission Rate The rate of data transmission should be set depending on the speed of your Wireless-N networking. 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 value 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 value is 1. Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance.

Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346. RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Dual-Band Wireless-N Gigabit Router Security > Firewall Firewall SPI Firewall Protection To use firewall protection, keep the default selection, 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.

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. 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 18 Chapter 3 Advanced Configuration 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 > VPN Passthrough The VPN Passthrough screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.



[You're reading an excerpt. Click here to read official LINKSYS  
WRT320N user guide  
http://yourpdfguides.com/dref/2315731](http://yourpdfguides.com/dref/2315731)

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.

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. 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. 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. 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. Dual-Band Wireless-N Gigabit Router Summary 19 Chapter 3 Advanced Configuration 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. 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 Edit List 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 click 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 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). List of PCs 5. Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen. 6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select Everyday. Then enter a range of hours and minutes during which the policy will be in effect, or select 24 Hours. 7. You can block websites with specific URL addresses.

Enter each URL in a separate URL field. 8. You can also block websites using specific keywords. Enter each keyword in a separate 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.

Dual-Band Wireless-N Gigabit Router 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. 20 Chapter 3 Advanced Configuration 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. 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. 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. 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.



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

[WRT320N user guide](#)

<http://yourpdfguides.com/dref/2315731>

(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 Application Name Enter the application name of the trigger. 21 Dual-Band Wireless-N Gigabit Router Chapter 3 Advanced Configuration address in the field provided. To retrieve this information, click DHCP Client Table. 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. Check with the Internet application documentation for the port number(s) needed.

Enabled Select Enabled to enable port triggering for the applications you have defined. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. DMZ > DHCP Client Table Applications and Gaming > DMZ The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding 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. DHCP Client Table The DHCP Client Table lists computers and other devices that have been assigned IP addresses by the Router. @@To select a DHCP client, click Select. To retrieve the most up-to-date information, click Refresh. To exit this screen and return to the DMZ screen, click Close. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes.

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 DMZ Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

Enabled/Disabled To disable DMZ hosting, select Disabled. To expose one PC, select Enabled. Then configure the following settings: Source IP Address If you want any IP address to be the source, select Any IP Address.

If you want to specify an IP address or range of IP addresses as the designated source, select and complete the IP address range fields. Destination If you want to specify the DMZ host by IP address, select IP Address and enter the IP address in the field provided. If you want to specify the DMZ host by MAC address, select MAC Address and enter the MAC Dual-Band Wireless-N Gigabit Router Applications and Gaming > QoS QoS (Quality of Service) Wireless You can configure the support and No Acknowledgement settings in this section. 22 Chapter 3 Advanced Configuration can range from 1 to 65535. Check your application's documentation for details on the service ports used.

Select the protocol TCP or UDP, or select Both. Priority Select the appropriate priority: High, Medium (Recommend), Normal, or Low. Click Add to save your changes. Your new entry will appear in the Summary list. WMM Support If you have other devices that support WiFi Multimedia (WMM) on your network, keep the default, Enabled. Otherwise, select Disabled. No Acknowledgement If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, then 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 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 have set, keep the default, Enabled. Otherwise, select Disabled. Online Games QoS > Online Games Games Select the appropriate game. Priority Select the appropriate priority: High, Medium (Recommend), Normal, or Low. Click Add to save your changes. Your new entry will appear in the Summary list. Category There are four categories available.

Select one of the following: Applications, Online Games, MAC Address, Ethernet Port, or Voice Device. Proceed to the instructions for your selection. MAC Address Applications Applications Select the appropriate application. If you select Add a New Application, follow the Add a New Application instructions. Priority Select the appropriate priority: High, Medium, Normal, or Low.

Click Add to save your changes. Your new entry will appear in the Summary list. Add a New Application QoS > MAC Address Enter a Name Enter a name for your device. MAC Address Enter the MAC address of your device. Priority Select the appropriate priority: High, Medium (Recommend), Normal, or Low. Click Add to save your changes. Your new entry will appear in the Summary list. Ethernet Port QoS > Add a New Application Enter a Name Enter any name to indicate the name of the entry. Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 10001250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers Dual-Band Wireless-N Gigabit Router QoS > Ethernet Port Ethernet Select the appropriate Ethernet port. Priority Select the appropriate priority: High, Medium (Recommend), Normal, or Low. Click Add to save your changes.

Your new entry will appear in the Summary list.



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

[WRT320N user guide](#)

<http://yourpdfguides.com/dref/2315731>

23 Chapter 3 Advanced Configuration Voice Device QoS > Voice Device Enter a Name Enter a name for your voice device. MAC Address Enter the MAC address of your voice device. Priority Select the appropriate priority: (Recommend), Medium, Normal, or Low. High Click Add to save your changes. Your new entry will appear in the Summary list. Summary This lists the QoS entries you have created for your applications and devices. Priority This column displays the bandwidth priority of High, Medium, Normal, or Low. Name This column displays the application, device, or port name. Information This column displays the port range or MAC address entered for your entry.

If a pre-configured application or game was selected, there will be no valid entry shown in this section. Remove Click this button to remove an entry. Edit Click this button to make changes. Click Save Settings to apply your changes, or click Cancel Changes to cancel your changes. Administration > Management

Management Router Access To ensure the Router's security, you will be asked for your password when you access the Router's web-based utility. The default is admin. Router Password Enter a new password for the Router. Re-enter to confirm Enter the password again to confirm. Web Access Web Utility Access HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security.

Select HTTP or HTTPS. HTTP is the default. Web Utility Access via Wireless If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the utility via a wired connection if you disable the setting. Keep the default, Enabled, to allow wireless access to the utility, or select Disabled to block wireless access to the utility. Administration > Management The Administration > Management screen allows the network's administrator to manage specific Router functions for access and security.

Remote Access Remote Management To permit remote access of the Router, from outside the local network, select Enabled. Otherwise, keep the default, Disabled. Web Utility Access HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security.

Select HTTP or HTTPS. HTTP is the default. Dual-Band Wireless-N Gigabit Router 24 Chapter 3 Advanced Configuration Administration > Log The Router can keep logs of all traffic for your Internet connection. Remote Upgrade If you want to be able to upgrade the Router remotely, from outside the local network, select Enabled. (You must have the Remote Management feature enabled as well.) Otherwise, keep the default, Disabled. Allowed Remote IP Address If you want to be able to access the Router from any external IP address, select Any IP Address. If you want to specify an external IP address or range of IP addresses, then select the second option and complete the fields provided. Remote Management Port Enter the port number that will be open to outside access. NOTE: When you are in a remote location and wish to manage the Router, enter http://<Internet\_IP\_address>:port or https://<Internet\_IP\_address>:port, depending on whether you use HTTP or HTTPS.

Enter the Router's specific Internet IP address in place of <Internet\_IP\_address>, and enter the Remote Management Port number in place of the word port. Administration > Log Log Log To disable the Log function, select Disabled. To monitor traffic between the network and the Internet, keep the default, Enabled. With logging enabled, you can choose to view temporary logs. View Log To view the logs, click View Log.

UPnP Universal Plug and Play (UPnP) allows Windows Me and XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. UPnP If you want to use UPnP, keep the default setting, Enabled. Otherwise, select Disabled. Allow Users to Configure Keep the default, Enabled, if you want to be able to make manual changes to the Router while using the UPnP feature. Otherwise, select Disabled.

Allow Users to Disable Internet Access Select Enabled, if you want to be able to prohibit any and all Internet connections. Otherwise, keep the default setting, Disabled. Administration > Log > View Log Log · · Type Select Incoming Log, Outgoing Log, Security Log, or DHCP Client Log. <Type> Log The Incoming Log will display a temporary log of the source IP addresses and destination port numbers for the incoming Internet traffic. The Outgoing Log will display a temporary log of the local IP addresses, destination URLs/IP addresses, and service/port numbers for the outgoing Internet traffic. The Security log will display the login information for the web-based utility. The DHCP Client Log will display the LAN DHCP server status information. Click Save the Log to save this information to a file on your PC's hard drive. Click Refresh to update the log. Click Clear to clear all the information that is displayed.

Backup and Restore Backup Configurations To back up the Router's configuration settings, click this button and follow the onscreen instructions. Restore Configurations To restore the Router's configuration settings, click this button and follow the onscreen instructions. (You must have previously backed up the Router's configuration settings.) 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. Dual-Band Wireless-N Gigabit Router 25 Chapter 3 Advanced Configuration Traceroute Test The Traceroute test tests the performance of a connection. IP or URL Address Enter the address of the PC whose connection you wish to test. Start to Traceroute To run the test, click this button. The Traceroute Test screen will show if the test was successful. Click Close to return to the Diagnostics screen.

Administration > Diagnostics The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network devices, including connection to the Internet. This screen also allows you to reset the router. Administration > Diagnostics Reboot Reboot Click Reboot to reset the router. Diagnostics > Traceroute Diagnostics Ping Test The Ping test checks the status of a connection. IP or URL Address Enter the address of the PC whose connection you wish to test.

Packet Size Enter the packet size you want to use. The default is 32 bytes. Times to Ping Enter many times you wish to test it. Start to Ping To run the test, click this button. The Ping Test screen will show if the test was successful.



[You're reading an excerpt. Click here to read official LINKSYS  
WRT320N user guide  
http://yourpdfguides.com/dref/2315731](http://yourpdfguides.com/dref/2315731)