



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for LINKSYS WRT300N. You'll find the answers to all your questions on the LINKSYS WRT300N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual LINKSYS WRT300N
User guide LINKSYS WRT300N
Operating instructions LINKSYS WRT300N
Instructions for use LINKSYS WRT300N
Instruction manual LINKSYS WRT300N



[You're reading an excerpt. Click here to read official LINKSYS WRT300N user guide](http://yourpdfguides.com/dref/326045)
<http://yourpdfguides.com/dref/326045>

Manual abstract:

and/or its affiliates in the U.S. and certain other countries. Copyright © 2006 Cisco Systems, Inc. All rights reserved. @@@@Look for the following items when reading this User Guide: This checkmark means there is a note of interest and is something you should pay special attention to while using the Wireless-N Broadband Router. This exclamation point means there is a caution or warning and is something that could damage your property or the Wireless-N Broadband Router. This question mark provides you with a reminder about something you might need to do while using the Wireless-N Broadband Router. In addition to these symbols, there are definitions for technical terms that are presented like this: word: definition. Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this: Figure 0-1: Sample Figure Description Figure numbers and descriptions can also be found in the "List of Figures" section in the "Table of Contents".

WRT300N-UG-60324NC JL Wireless-N Broadband Router Table of Contents Chapter 1: Introduction Welcome What's in this User Guide? 1 1 2 Chapter 2: Planning Your Wireless Network Network Topology Ad-Hoc versus Infrastructure Mode Network Layout 4 4 4 4 Chapter 3: Getting to Know the Wireless-N Broadband Router The Back Panel The Front Panel The Top Panel 6 6 7 7 Chapter 4: Connecting the Wireless-N Broadband Router Hardware Installation 8 8 Chapter 5: Configuring the Wireless-N Broadband Router Overview How to Access the Web-based Utility The Setup Tab - Basic Setup The Setup Tab - DDNS The Setup Tab - MAC Address Clone The Setup Tab - Advanced Routing The Wireless Tab - Basic Wireless Settings The Wireless Tab - Wireless Security The Wireless Tab - Wireless MAC Filter The Wireless Tab - Advanced Wireless Settings The Security Tab - Firewall The Security Tab - VPN Passthrough The Access Restrictions Tab - Internet Access Policy The Applications & Gaming Tab - Single Port Forwarding The Applications & Gaming Tab - Port Range Forwarding The Applications & Gaming Tab - Port Range Triggering The Applications & Gaming Tab - DMZ The Applications and Gaming Tab - QoS 9 9 11 11 17 19 20 22 23 26 27 29 30 31 33 34 35 36 37 Wireless-N Broadband Router The Administration Tab - Management The Administration Tab - Log The Administration Tab - Diagnostics The Administration Tab - Factory Defaults The Administration Tab - Firmware Upgrade The Status Tab - Router The Status Tab - Local Network The Status Tab - Wireless 40 42 43 44 45 46 47 48 Appendix A: Troubleshooting Common Problems and Solutions Frequently Asked Questions 49 49 57 Appendix B: Wireless Security Security Precautions Security Threats Facing Wireless Networks 63 63 63 Appendix C: Upgrading Firmware Appendix D: Windows Help Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter Windows 98SE or Me Instructions Windows 2000 or XP Instructions For the Router's Web-based Utility 66 67 68 68 69 69 Appendix F: Glossary Appendix G: Specifications Appendix H: Warranty Information Appendix I: Regulatory Information Appendix J: Contact Information 70 75 77 78 84 Wireless-N Broadband Router List of Figures Figure 3-1: The Router's Back Panel Figure 3-2: The Router's Front Panel Figure 3-3: The Router's Top Panel Figure 4-1: Connect the Modem Figure 4-2: Connect a PC Figure 4-3: Connect the Power Figure 5-1: Router Login Figure 5-2: Setup Tab - Basic Setup (Automatic Configuration - DHCP) Figure 5-3: Static IP Figure 5-4: PPPoE Figure 5-5: PPTP Figure 5-6: Telstra Cable Figure 5-7: L2TP Figure 5-8: DHCP Reservation Figure 5-9: Setup Tab - DDNS (DynDNS.org) Figure 5-10: Setup Tab - DDNS (TZO.com) Figure 5-11: Setup Tab - MAC Clone Figure 5-12: Setup Tab - Advanced Routing Figure 5-13: Routing Table Figure 5-14: Wireless Tab - Basic Wireless Settings Figure 5-15: Wireless Tab - Wireless Security (PSK-Personal) Figure 5-16: Wireless Security - PSK2-Personal Figure 5-17: Wireless Security - PSK-Enterprise Figure 5-18: Wireless Security - PSK2-Enterprise Figure 5-19: Wireless Security - RADIUS Figure 5-20: Wireless Security - WEP Figure 5-21: Wireless Tab - Wireless MAC Filter Figure 5-22: Wireless Client List Figure 5-23: Wireless Tab - Advanced Wireless Settings Figure 5-24: Security Tab - Firewall Figure 5-25: VPN Passthrough 6 7 7 8 8 8 11 11 12 12 13 13 14 16 17 18 19 20 21 22 23 23 24 24 25 25 26 26 27 29 30 Wireless-N Broadband Router Figure 5-26: Access Restrictions Tab - Internet Access Policy Figure 5-27: Summary Figure 5-28: List of PCs Figure 5-29: Applications & Gaming Tab - Single Port Forwarding Figure 5-30: Applications & Gaming Tab - Port Range Forwarding Figure 5-31: Applications & Gaming Tab - Port Range Triggering Figure 5-32: Applications & Gaming Tab - DMZ Figure 5-33: DHCP Client Table Figure 5-34: Applications & Gaming Tab - QoS (Applications) Figure 5-35: QoS - Applications (Add a New Application) Figure 5-36: QoS - Online Games Figure 5-37: QoS - MAC Address Figure 5-38: QoS - MAC Address Figure 5-39: QoS - Voice Device Figure 5-40: Administration Tab - Management Figure 5-41: Administration Tab - Log Figure 5-42: View Log Figure 5-43: Administration Tab - Diagnostics Figure 5-44: Ping Test Figure 5-45: Traceroute Test Figure 5-46: Administration Tab - Factory Defaults Figure 5-47: Administration Tab - Firmware Upgrade Figure 5-48: Status Tab - Router Figure 5-49: Status Tab - Local Network Figure 5-50: Status Tab - Local Network Figure 5-51: Status Tab - Wireless Figure C-1: Firmware Upgrade Figure E-1: IP Configuration Screen Figure E-2: MAC Address/Adapter Address Figure E-3: MAC Address/Physical Address Figure E-4: Wireless MAC Filter Figure E-5: MAC Address Cloning 31 31 32 33 34 35 36 37 38 38 38 38 39 40 42 42 43 43 43 44 45 46 47 47 48 66 68 68 68 69 69 Wireless-N Broadband Router Chapter 1: Introduction Welcome Thank you for choosing the Linksys Wireless-N Broadband Router. The Wireless-N Broadband Router will allow you to network wirelessly better than ever, sharing Internet access, files and fun, easily and securely and with a greater range of up to three times farther than standard Wireless-G. How does the Wireless-N Broadband Router do all of this? A router is a device that allows access to an Internet connection over a network.

With the Wireless-N Broadband Router, this access can be shared over the four switched ports or via the wireless broadcast. Use wireless security to secure your wireless network while the whole network is protected through a Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) technology. The Router also offers VPN passthrough and other features, which can be configured through the easy-to-use, browser-based utility. The incredible speed of Wireless-N makes it ideal for media-centric applications like streaming video and Voice over IP (VoIP) telephony, so your network can handle multiple data streams at the same time, with no degradation in performance.



**You're reading an excerpt. Click here to read official LINKSYS
WRT300N user guide
<http://yourpdfguides.com/dref/326045>**

But what does all of this mean? Networks are useful tools for sharing computer resources.

You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun. PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired". PCs equipped with wireless cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wireless Local Area Network. The Wireless-N Broadband Router bridges wireless and wired networks, allowing them to communicate with each other. Linksys recommends using the Setup Wizard on the Setup CD-ROM for first-time installation of the Router.

If you do not wish to run the Setup Wizard, then use the instructions in this Guide to help you connect the Router and configure it. These instructions should be all you need to get the most out of the Wireless-N Broadband Router. spi (stateful packet inspection) firewall: a technology that inspects incoming packets of information before allowing them to enter the network. firewall: Security measures that protect the resources of a local network from intruders. nat (network address translation): NAT technology translates IP addresses of a local area network to a different IP address for the Internet. lan (local area network): The computers and networking products that make up the network in your home or office. Chapter 1: Introduction Welcome 1 Wireless-N Broadband Router What's in this User Guide? This user guide covers the steps for setting up and using the Wireless-N Broadband Router. · Chapter 1: Introduction This chapter describes the Router's applications and this User Guide. · Chapter 2: Planning Your Wireless Network This chapter describes the basics of wireless networking. · Chapter 3: Getting to Know the Wireless-N Broadband Router This chapter describes the physical features of the Router. · Chapter 4: Connecting the Wireless-N Broadband Router This chapter instructs you on how to connect the Router to your network. · Chapter 5: Configuring the Wireless-N Broadband Router This chapter explains how to use the Web-based Utility to configure the settings on the Wireless-N Broadband Router. · Appendix A: Troubleshooting This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Wireless-N Broadband Router. · Appendix B: Wireless Security This appendix explains the risks of wireless networking and some solutions to reduce the risks. · Appendix C: Upgrading Firmware This appendix instructs you on how to upgrade the firmware on the Router should you need to do so. · Appendix D: Windows Help This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol. · Appendix E: Finding the MAC Address and IP Address for your Ethernet Adapter This appendix describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. · Appendix F: Glossary This appendix gives a brief glossary of terms frequently used in networking. Chapter 1: Introduction What's in this User Guide? 2 Wireless-N Broadband Router · Appendix G: Specifications This appendix provides the technical specifications for the Router. · Appendix H: Warranty Information This appendix supplies the warranty information for the Router. · Appendix I: Regulatory Information This appendix supplies the regulatory information regarding the Router. · Appendix J: Contact Information This appendix provides contact information for a variety of Linksys resources, including Technical Support. Chapter 1: Introduction What's in this User Guide? 3 Wireless-N Broadband Router Chapter 2: Planning Your Wireless Network Network Topology A wireless local area network (WLAN) is exactly like a regular local area network (LAN), except that each computer in the WLAN uses a wireless device to connect to the network. Computers in a WLAN share the same frequency channel and SSID, which is an identification name shared by the wireless devices belonging to the same wireless network. ssid (service set identifier): your wireless network's name. Ad-Hoc versus Infrastructure Mode Unlike wired networks, wireless networks have two different modes in which they may be set up: infrastructure and ad-hoc. An infrastructure configuration is a WLAN and wired LAN communicating to each other through an access point. An ad-hoc configuration is wireless-equipped computers communicating directly with each other. Choosing between these two modes depends on whether the Router is powered on. ETHERNET 1, 2, 3, 4 Green.

These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. The LED lights up when the Router is connected to a device through the corresponding port. If the LED is flashing, the Router is sending or receiving data over that port. INTERNET WIRELESS Green. The INTERNET LED lights up when there is a connection through the Internet port. Green. The WIRELESS LED lights up when there is a wireless connection. If the LED is flashing, the Router is sending or receiving data over the wireless network. Green. The SECURITY LED indicates when wireless security is enabled.

SECURITY The Top Panel The Router has a button reserved for a future function. Button Figure 3-3: The Router's Top Panel Chapter 3: Getting to Know the Wireless-N Broadband Router The Front Panel 7 Wireless-N Broadband Router Chapter 4: Connecting the Wireless-N Broadband Router Hardware Installation 1. Make sure that all of your hardware is powered off, including the broadband modem and PCs. 2. Connect your broadband modem's Ethernet cable to the Router's Internet port.

3. Connect one end of an Ethernet network cable to one of the numbered ports on the back of the Router. Connect the other end to an Ethernet port on a network device, e.g., a PC, print server, or switch.

Repeat this step to connect more PCs or other network devices to the Router. 4. Power on the broadband modem. 5. Connect the included power adapter to the Router's Power port, and then plug the power adapter into an electrical outlet. The Power LED on the front panel will light up when the adapter is connected properly. 6. Power on your PC(s). 7. Locate an optimum location for the Router.

The best place for the Router is usually at the center of your wireless network, with line of sight to all of your wireless devices. Proceed to "Chapter 5: Configuring the Wireless-N Broadband Router".



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>

Figure 4-2: Connect a PC Figure 4-1: Connect the Modem Figure 4-3: Connect the Power IMPORTANT: Make sure you use the power adapter that is supplied with the Router. Use of a different power adapter could damage the Router. Chapter 4: Connecting the Wireless-N Broadband Router Hardware Installation 8 Wireless-N Broadband Router Chapter 5: Configuring the Wireless-N Broadband Router Overview Linksys recommends using the Setup CD-ROM for first-time installation of the Router. If you do not wish to run the Setup Wizard on the Setup CD-ROM, then you can use the Web-based Utility to configure the Router. For advanced users, you may configure the Router's advanced settings through the Web-based Utility. This chapter will describe each web page on the Utility and each page's key functions. The Utility can be accessed via your web browser through use of a computer connected to the Router.

For a basic network setup, most users only have to use the following screens of the Utility: · Basic Setup.

On the Basic Setup screen, enter the Internet connection settings provided by your Internet Service Provider (ISP). If you do not have this information, you can call your ISP to request the settings. When you have the setup information, then you can configure the Router. · Management. Click the Administration tab and then the Management tab.

The Router's default password is admin. To secure the Router, change the Password from its default. · Wireless. On the Basic Wireless Settings screen, set the basic configuration for your wireless network. There are seven main tabs: Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status.

Additional tabs will be available after you click one of the main tabs. Setup · Basic Setup. Enter the Internet connection and network settings on this screen. · DDNS. Enable the Router's Dynamic Domain Name System (DDNS) feature on this screen. · MAC Address Clone. If you need to clone a MAC address onto the Router, use this screen. · Advanced Routing. Use this screen to alter dynamic and static routing configurations. Wireless · Basic Wireless Settings.

Enter the basic settings for your wireless network on this screen. · Wireless Security. Enable and configure the security settings for your wireless network. Chapter 5: Configuring the Wireless-N Broadband Router Overview 9 Wireless-N Broadband Router · Wireless MAC Filter. Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. · Advanced Wireless Settings. For advanced users, you can alter data transmission settings on this screen. Security · Firewall. You can enable or disable the Router's firewall, as well as various filters. · VPN Passthrough.

To enable or disable IPSec, L2TP, and/or PPTP Passthrough, use this screen. Access Restrictions Internet Access Policy. Create policies to control Internet access for your local network users. Applications & Gaming · Single Port Forwarding. This allows you to do port mapping and forwarding for a single service port.

· Port Range Forwarding. Set up public services or other specialized Internet applications on your network. · Port Range Triggering. Configure the Router to watch outgoing data for specific port numbers. · DMZ.

Click this tab to allow one local user to be exposed to the Internet for use of special-purpose services. · QoS. Quality of Service (QoS) ensures better service to high-priority types of network traffic. Administration · Management. On this screen, alter the Router's password, access privileges, and UPnP settings. You can also use this screen to back up and restore the Router's configuration file. · Log. If you want to view or save activity logs, click this tab. · Diagnostics. If you want to run a ping or traceroute test, then use this screen.

· Factory Defaults. If you want to restore the Router's factory defaults, then use this screen. · Firmware Upgrade. Click this tab if you want to upgrade the Router's firmware. Chapter 5: Configuring the Wireless-N Broadband Router Overview 10 Wireless-N Broadband Router Status · Router. This screen provides status information about the Router. · Local Network. This provides status information about the local network. · Wireless Network. This provides status information about the wireless network.

How to Access the Web-based Utility To access the Web-based Utility of the Router, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, 192.168.1.1, in the Address field. Press the Enter key.

A screen will appear asking you for your User name and Password. Leave the User Name field blank. Enter admin in the Password field. Then click the OK button. Make the necessary changes through the Utility.

When you have finished making changes to a screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. For information on a tab, click Help. Figure 5-1: Router Login The Setup Tab - Basic Setup The Basic Setup screen is the first screen you see when you access the Web-based Utility. Internet Setup The Internet Setup section configures the Router for your Internet connection type. This information can be obtained from your ISP. Internet Connection Type The Router supports six connection types: Automatic Configuration - DHCP, Static IP, PPPoE, PPTP, Telstra Cable, and L2TP. Each Basic Setup screen and available features will differ depending on what kind of connection type you select. Automatic Configuration - DHCP By default, the Router's Internet Connection Type is set to Automatic Configuration - DHCP, and it should be used only if your ISP supports DHCP or you are connecting through a dynamic IP address. Figure 5-2: Setup Tab - Basic Setup (Automatic Configuration - DHCP) NOTE: Some of these connection types may not be available in your area. 11 Chapter 5: Configuring the Wireless-N Broadband Router How to Access the Web-based Utility Wireless-N Broadband Router Static IP If you are required to use a permanent IP address, then select Static IP.

Internet IP Address. This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here. Subnet Mask. This is the Router's Subnet Mask, as seen by external 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 Default Gateway Address. DNS 1-3. Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Figure 5-3: Static IP PPPoE Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>

If you use a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable it. User Name and Password. Enter the User Name and Password provided by your ISP.

Service Name. If provided by your ISP, enter the Service Name. Connect on Demand and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects. Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds. Click the Save Settings button.

Then click the Status tab, and click the Connect button. **IMPORTANT:** For DSL users, if you need to enable PPPoE support, remember to remove any PPPoE applications that are installed on your PCs. pppoe: a type of broadband connection that provides authentication (username and password) in addition to data transport static ip address: a fixed address assigned to a computer or device connected to a network. subnet mask: an address code that determines the size of the network default gateway: a device that forwards Internet traffic from your local area network Figure 5-4: PPPoE Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Basic Setup 12 Wireless-N Broadband Router PPTP Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe and Israel only. Server IP Address. This is the IP address that the Router has, when seen from the Internet. Your ISP will provide you with the IP address you need to specify here. Subnet Mask. This is the Router's Subnet Mask, as seen by external 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 Default Gateway Address. User Name and Password. Enter the User Name and Password provided by your ISP. Connect on Demand and Max Idle Time.

You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds. Click the Save Settings button. Then click the Status tab, and click the Connect button. Figure 5-5: PPTP Telstra Cable Telstra Cable is a service used in Australia only. Check with your ISP for the necessary setup information.

Server IP Address. This is the IP address that the Router has, when seen from the Internet. 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. Click the Save Settings button. Then click the Status tab, and click the Connect button. Figure 5-6: Telstra Cable Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Basic Setup 13 Wireless-N Broadband Router L2TP Layer 2 Tunneling Protocol (L2TP) is a service that tunnels Point-to-Point Protocol (PPP) across the Internet. It is used mostly in European countries. Check with your ISP for the necessary setup information.

Server IP Address. This is the IP address that the Router has, when seen from the Internet. 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 and Max Idle Time. You can configure the Router to cut the Internet connection after it has been inactive for a specific 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 Connect on Demand, click the radio button. If you want your Internet connection to remain on at all times, enter 0 in the Max Idle Time field.

Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects. Keep Alive and Redial Period. This option keeps your Internet access connected indefinitely, even when it sits idle. If you select this option, the Router will periodically check your Internet connection. If the connection is down, then the Router will automatically re-establish the connection. To use this option, click the radio button next to Keep Alive. The default Redial Period is 30 seconds. Click the Save Settings button. Then click the Status tab, and click the Connect button. Figure 5-7: L2TP Optional Settings Some of these settings may be required by your ISP.

Verify with your ISP before making any changes. Host Name and Domain Name. Some 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. The MTU (Maximum Transmission Unit) setting specifies the largest packet size permitted for network transmission. To manually set a value, select Manual and enter the value desired in the Size field. You should leave this value in the 1200 to 1500 range. Most DSL users should use the value 1492.

The default is Auto, which allows the Router to select the best MTU for your Internet connection. packet: a unit of data sent over a network. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Basic Setup 14 Wireless-N Broadband Router Network Setup The Network Setup section allows you to change the Router's local network settings. Router IP The Router's Local IP Address and Subnet Mask are shown here.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>

In most cases, you should keep the defaults.

Local IP Address. The default value is 192.168.1.1.

Subnet Mask. The default value is 255.255.255.0. DHCP Server Setting The Router can be used as a Dynamic Host Configuration Protocol (DHCP) server for your network. A DHCP server automatically assigns an IP address to each computer on your network. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server. DHCP Server. DHCP is enabled by factory default.

If you already have a DHCP server on your network, set the Router's DHCP option to Disabled. If you disable DHCP, remember to assign a static IP address to the Router. Start IP Address. Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the Start IP Address must be 192.168.1.

2 or greater, but smaller than 192.168.1.254. The default Start IP Address is 192.

168.1.100. Maximum Number of Users (Optional). Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to.

This number cannot be greater than 253. The default is 50. Client Lease Time. The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, 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.

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) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank. dynamic ip address: a temporary IP address assigned by a DHCP server. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Basic Setup 15 Wireless-N Broadband Router DHCP Reservation. Click the DHCP Reservation button if you want to assign a fixed local IP address to a MAC address. You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address.

Click the Select checkbox to reserve a client's IP address. Then click the Add Clients button. 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. Enter its MAC Address in the To This MAC Address field.

Click the Add button. 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 the Remove button. When you have finished your changes, click the Save Settings button to save your changes. Click the Cancel Changes button to cancel your changes.

To view the most up-to-date information, click the Refresh button. To exit this screen, click the Close button. Time Setting Time Zone. Select the time zone in which your network functions. If you want the Router to automatically adjust the clock for daylight savings, then select the checkbox. @@For more information, click Help. Figure 5-8: DHCP Reservation NOTE: To test your settings, connect to the Internet now. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Basic Setup 16 Wireless-N Broadband Router The Setup Tab - 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 at one of two DDNS service providers, DynDNS.org or TZO.com. If you do not want to use this feature, keep the default setting, Disable. DDNS DDNS Service If your DDNS service is provided by DynDNS.org, then select DynDNS.org from the drop-down menu. If your DDNS service is provided by TZO, then select TZO.com. The features available on the DDNS screen will vary, depending on which DDNS service provider you use.

Figure 5-9: Setup Tab - DDNS (DynDNS.org) DynDNS.org Username, Password, and Host Name. Enter the settings of the account you set up with DynDNS.org.

System. Select the DynDNS service you use: Dynamic, Static, or Custom. 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 enable this feature, keep the default, Enabled. To disable the feature, select Disabled. If you are not sure which setting to select, keep the default, Enabled. 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 enable wildcards, keep the default, Enabled. To disable wildcards, select Disabled. If you are not sure which setting to select, keep the default, Enabled. Status. The status of the DDNS service connection is displayed here. Update. To manually trigger an update, click this button. ddns: allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.

g., www.xyz.com) and a dynamic IP address. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - DDNS 17 Wireless-N Broadband Router TZO.

com 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 this button. @@For more information, click Help. Figure 5-10: Setup Tab - DDNS (TZO.com) Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - DDNS 18 Wireless-N

Broadband Router The Setup Tab - MAC Address Clone A MAC address is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. 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. MAC Address Clone To use MAC address cloning, select Enabled.

Otherwise, keep the default, Disabled. MAC Address. Enter the MAC Address registered with your ISP. Figure 5-11: Setup Tab - MAC Clone Clone My PC's MAC. If you want to clone the MAC address of the PC you are currently using to configure the Router, then click this button.



[You're reading an excerpt. Click here to read official LINKSYS WRT300N user guide](#)

The Router will automatically detect your PC's MAC address, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone screen. @@For more information, click Help. mac address: the unique address that a manufacturer assigns to each networking device. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - MAC Address Clone 19 Wireless-N Broadband Router The Setup Tab - Advanced Routing The Advanced Routing screen allows you to configure the dynamic and static routing settings.

Advanced Routing NAT If this Router is hosting your network's connection to the Internet, select Enabled. If another Router exists on your network, select Disabled. When the NAT setting is disabled, dynamic routing will be enabled. Dynamic Routing 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.

To use dynamic routing, select Enabled. Otherwise, select Disabled. When the NAT setting is disabled, dynamic routing will be enabled. Figure 5-12: Setup Tab - Advanced Routing Static Routing A static route is a pre-determined pathway that network information must travel to reach a specific host or network.

Use this feature to set up a static route between the Router and another network (you can have up to 20 static routes).

To create a static route, alter the following settings: Route Entries. Select the number of the static route from the drop-down menu. Enter Route Name. Enter a name for the static route, using a maximum of 25 alphanumeric characters. Destination LAN IP. The Destination LAN IP Address is the address of the remote network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route. Subnet Mask. The Subnet Mask determines which portion of a Destination IP address is the network portion, and which portion is the host portion. Default Gateway.

This is the IP address of the gateway device that allows for contact between the Router and the remote network or host. Interface. Select LAN & Wireless or WAN (Internet), depending on the location of the final destination. Delete This Entry. To delete a route, select its number from the drop-down menu, and click this button. Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Advanced Routing 20 Wireless-N Broadband Router Show Routing Table. Click the Show Routing Table button to open a screen displaying how data is routed through your local network. For each route, the Destination LAN IP address, Subnet Mask, Gateway, and Interface are displayed. Click the Refresh button to update the information. Click the Close button to exit this screen.

@@For more information, click Help. Figure 5-13: Routing Table Chapter 5: Configuring the Wireless-N Broadband Router The Setup Tab - Advanced Routing 21 Wireless-N Broadband Router The Wireless Tab - Basic Wireless Settings The basic settings for wireless networking are set on this screen. Basic Wireless Settings Network Mode. If you have wireless devices in your network, keep the default setting, Mixed. If you do not have any wireless devices in your network, select Disable.

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. Radio Band. For best performance in a network using Wireless-N, Wireless-G and Wireless-B devices, keep the default, Wide - 40MHz Channel. For Wireless-G and Wireless-B networking only, select Standard - 20MHz Channel. 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. Standard Channel. Select the channel for Wireless-N, Wireless-G, and Wireless-B networking. If you selected Wide 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N.

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. @@For more information, click Help. Figure 5-14: Wireless Tab - Basic Wireless Settings NOTE: If you select Wide - 40MHz Channel for the Radio Band setting, then Wireless-N can use two channels: a primary one (Wide Channel) and a secondary one (Standard Channel). This will enhance Wireless-N performance. Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Basic Wireless Settings 22 Wireless-N Broadband Router The Wireless Tab - Wireless Security These settings configure the security of your wireless network. There are six wireless security modes supported by the Router: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2-Enterprise, RADIUS, and WEP.

(PSK stands for Pre-Shared Key, which is stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) For details on configuring wireless security for the Router, turn to "Appendix B: Wireless Security." If you do not want to use wireless security, select Disabled. Wireless Security Security Mode.

Select the mode you want to use: PSK-Personal, PSK2-Personal, PSK-Enterprise, PSK2Enterprise, RADIUS, or WEP. PSK2 is a more advanced, more secure version of PSK. Follow the instructions for the security method you want to use. Figure 5-15: Wireless Tab - Wireless Security (PSK-Personal) PSK-Personal Encryption. Select the algorithm you want to use, TKIP or AES.

(AES is a stronger encryption method than TKIP.) Pre-shared Key. Enter the key shared by the Router and your other network devices. It must have 8-63 characters. Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys. @@For more information, click Help. PSK2-Personal Encryption. Select the algorithm(s) you want to use, AES or TKIP or AES. (AES is a stronger encryption method than TKIP.

) Pre-shared Key. Enter the key shared by the Router and your other network devices. It must have 8-63 characters. Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>

@@For more information, click Help. Figure 5-16: Wireless Security - PSK2-Personal Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Wireless Security 23 Wireless-N Broadband Router PSK-Enterprise This option features PSK used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Encryption. Select the algorithm(s) you want to use, TKIP or AES. (AES is a stronger encryption method than TKIP.) RADIUS Server. Enter the IP address of your RADIUS server. RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server. Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys. @@For more information, click Help.

Figure 5-17: Wireless Security - PSK-Enterprise PSK2-Enterprise This option features PSK2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) Encryption. Select the algorithm(s) you want to use, AES or TKIP or AES. (AES is a stronger encryption method than TKIP.) RADIUS Server. Enter the IP address of your RADIUS server. RADIUS Port. Enter the port number of your RADIUS server. Shared Key.

Enter the key shared by the Router and RADIUS server. Key Renewal. Enter the Key Renewal period, which tells the Router how often it should change encryption keys. @@For more information, click Help. Figure 5-18: Wireless Security - PSK2-Enterprise Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Wireless Security 24 Wireless-N Broadband Router 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.) RADIUS Server. Enter the IP address of your RADIUS server. RADIUS Port. Enter the port number of your RADIUS server.

Shared Key. Enter the key shared by the Router and RADIUS server. Encryption. Select the appropriate level of encryption, 40/64-bit (10 hex digits) or 128-bit (26 hex digits), which is stronger encryption than 40/64 bit encryption. Passphrase.

To automatically generate keys, enter your passphrase. Then click the Generate button. Key 1-4. If you want to manually enter the WEP keys, then enter them in the Key 1-4 fields. TX Key.

To indicate which WEP key to use, select a transmit key number. @@For more information, click Help. Figure 5-19: Wireless Security - RADIUS WEP WEP is a basic encryption method offering two levels of encryption; 128-bit is stronger than 40/64-bit encryption. Encryption. Select the appropriate level of encryption, 40/64-bit (10 hex digits) or 128-bit (26 hex digits). Passphrase. To automatically generate keys, enter your passphrase. Then click the Generate button. Key 1-4. If you want to manually enter the WEP keys, then enter them in the Key 1-4 fields.

TX Key. To indicate which WEP key to use, select a transmit key number. @@For more information, click Help. Figure 5-20: Wireless Security - WEP Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Wireless Security 25 Wireless-N Broadband Router The Wireless Tab - Wireless MAC Filter Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius. 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, select Disabled. Access Restrictions Prevent. Click this button to block wireless access from the devices listed on this screen. Permit. Click this button to allow wireless access by the devices listed on this screen.

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. The list can be sorted by Client Name, Interface, IP Address, MAC Address, and Status. 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. Then click the Enable MAC Filter checkbox for any device you want to add to the MAC Address Filter List. To update the information on this list, click the Refresh button. When you have finished making changes to the Wireless Client MAC List screen, click the Update Filter List button to save the changes. Click the Close button to return to the Wireless MAC Filter screen. When you have finished making changes to the MAC Address Filter List screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. MAC 01-50. Enter the MAC addresses of the devices whose wireless access you want to block or allow. When you have finished making changes to the Wireless MAC Filter screen, click the Save Settings button to save the changes, or click the Cancel Changes button to undo your changes. For more information, click Help. Figure 5-21: Wireless Tab - Wireless MAC Filter Figure 5-22: Wireless Client List Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Wireless MAC Filter 26 Wireless-N Broadband Router The Wireless Tab - Advanced Wireless Settings This tab 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. 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, click Enabled. AP Isolation is disabled by default. Authentication Type. The default is set to Auto, which allows either Open System or Shared Key authentication to be used. Select Shared Key if you only want to use Shared Key authentication (the sender and recipient use a WEP key for authentication). Figure 5-23: Wireless Tab - Advanced Wireless Settings 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. 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.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>

Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default setting 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 setting is Auto. CTS Protection Mode. CTS (Clear-To-Send) Protection Mode's default setting is Auto. The Router will automatically use CTS 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 Wireless-N and Wireless-G transmissions but will severely decrease performance. Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Advanced Wireless Settings 27 Wireless-N Broadband Router Beacon Interval. Enter a value between 20-1000 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, 2346, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

In most cases, keep its default value of 2346. @@For more information, click Help. Chapter 5: Configuring the Wireless-N Broadband Router The Wireless Tab - Advanced Wireless Settings 28 Wireless-N Broadband Router The Security Tab - Firewall The Firewall screen offers a firewall and filters that block specific Internet data types. Firewall Firewall Protection. A firewall enhances network security and uses Stateful Packet Inspection (SPI) for more detailed review of data packets entering your network. Select Enabled to use a firewall, or Disabled to disable it. Internet Filter Filter Anonymous Internet Requests. When enabled, this feature keeps your network from being "pinged," or detected, by other Internet users. It also hides your network ports. Both make it more difficult for outside users to enter your network.

This filter is enabled by default. Select Disabled 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 Enabled to filter multicasting, or Disabled to disable this feature. Filter Internet NAT Redirection. This feature uses port forwarding to block access to local servers from local networked computers. Select Enabled to filter Internet NAT redirection, or Disabled to disable this feature. Filter IDENT (Port 113). This feature keeps port 113 from being scanned by devices outside of your local network. Select Enabled to filter port 113, or Disabled to disable this feature. Figure 5-24: Security Tab - Firewall Web Filter Proxy. Use of WAN proxy servers may compromise the Gateway's security. Denying Filter Proxy will disable access to any WAN proxy servers.

To enable proxy filtering, click the checkbox. Java. Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language. To enable Java filtering, click the checkbox.

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. To enable ActiveX filtering, click the checkbox. Cookies. A cookie is data stored on your computer and used by Internet sites when you interact with them. To enable cookie filtering, click the checkbox. @@For more information, click Help. Chapter 5: Configuring the Wireless-N Broadband Router The Security Tab - Firewall 29 Wireless-N Broadband Router The Security Tab - VPN Passthrough The VPN Passthrough screen allows you to allow VPN tunnels using IPSec, L2TP, or PPTP protocols to pass through the Router. VPN Passthrough IPSec Passthrough.

IPSec (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec Passthrough, click the Enabled button. To disable IPSec Passthrough, click the Disabled button. Figure 5-25: VPN Passthrough 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, click the Enabled button. To disable L2TP Passthrough, click the Disabled button. PPTP Passthrough. PPTP (Point-to-Point Tunneling Protocol) Passthrough allows the Point-to-Point (PPP) to be tunneled through an IP network. To allow PPTP Passthrough, click the Enabled button.

To disable PPTP Passthrough, click the Disabled button. @@For more information, click Help. vpn: a security measure to protect data as it leaves one network and goes to another over the Internet. ipsec: a VPN protocol used to implement secure exchange of packets at the IP layer. pptp: a VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network.

This protocol is also used as a type of broadband connection in Europe. Chapter 5: Configuring the Wireless-N Broadband Router The Security Tab - VPN Passthrough 30 Wireless-N Broadband Router The Access Restrictions Tab - Internet Access Policy The Internet Access Policy screen allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, websites, and inbound traffic during specific days and times.



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

[WRT300N user guide](#)

<http://yourpdfguides.com/dref/326045>

Internet Access Policy Access Policy. Access can be managed by a policy. Use the settings on this screen to establish an access policy (after the Save Settings button 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 the Delete This Policy button. To view all the policies, click the Summary button. On the Summary screen, the policies are listed with the following information: No., Policy Name, Access, Days, Time, and status (Enabled). To enable a policy, click the Enabled checkbox. To delete a policy, click its Delete button. Click the Save Settings button to save your changes, or click the Cancel Changes button to cancel your changes. To return to the Internet Access Policy screen, click the Close button. Status.

Policies are disabled by default. To enable a policy, select the policy number from the drop-down menu, and click the radio button beside Enabled. To create a policy: 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, click the radio button beside Enabled. 4. Click the Edit List button to select which PCs will be affected by the policy.

The List of PCs screen will appear. 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 the Save Settings button to apply your changes or Cancel Changes to cancel your changes. 5.

Click 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.

Figure 5-27: Summary Chapter 5: Configuring the Wireless-N Broadband Router The Access Restrictions Tab - Internet Access Policy Figure 5-26: Access Restrictions Tab - Internet Access Policy 31 Wireless-N Broadband Router 7. You can block websites with specific URL addresses. Enter each URL in a separate field next to Website Blocking by URL Address. 8. You can also block websites using specific keywords. Enter each keyword in a separate field next to Website Blocking by Keyword. 9. You can filter access to various services accessed over the Internet, such as FTP or telnet. (You can block up to three applications per policy.) From the Applications list, select the application you want to block.

Then click the >> button to move it to the Blocked List. To remove an application from the Blocked List, select it and click the << button. 10. If the application you want to block is not listed or you want to edit a service's settings, enter the application's name in the Application Name field. Enter its range in the Port Range fields. Select its protocol from the Protocol drop-down menu. Then click the Add button. To modify a service, select it from the Application list. Change its name, port range, and/or protocol setting. Then click the Modify button.

To delete a service, select it from the Application list. Then click the Delete button. 11. Click the Save Settings button to save the policy's settings. To cancel the policy's settings, click the Cancel Changes button.

For more information, click Help. Figure 5-28: List of PCs Chapter 5: Configuring the Wireless-N Broadband Router The Access Restrictions Tab - Internet Access Policy 32 Wireless-N Broadband Router The Applications & Gaming Tab - Single Port Forwarding When you click the Applications & Gaming tab, you will see the Single Port Forwarding screen. You can 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).

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. Click the Enabled checkbox to activate this entry. For additional applications, complete the following fields: Application Name. Enter the name of the application. 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 TCP or UDP, or select Both. To IP Address. Enter the IP address of the server that should receive the requests. To find the IP address, go to "Appendix E: Finding the MAC Address and IP Address for Your Ethernet Adapter." If you assigned a static IP address to the server, then you can click the DHCP Reservation button on the Basic Setup screen to look up its static IP address. Enabled. Click the Enabled checkbox to enable the applications you have defined.

This is disabled (unchecked) by default. @@For more information, click Help. tcp: a network protocol for transmitting data that requires acknowledgement from the recipient of data sent. udp: a network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent. Figure 5-29: Applications & Gaming Tab Single Port Forwarding Chapter 5: Configuring the Wireless-N Broadband Router The Applications & Gaming Tab - Single Port Forwarding 33 Wireless-N Broadband Router The Applications & Gaming Tab - Port Range Forwarding Port range forwarding sets up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications.

(Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers (use the DHCP Reservation feature on the Basic Setup screen). If you need to forward all ports to one PC, click the DMZ tab.

Port Range Forwarding To add an application, complete the following fields: Application Name. Enter the name of the application. Start ~ End Port. Enter the number or range of port(s) used by the server or Internet application. Check with the Internet application documentation for more information. Protocol. Select the protocol TCP or UDP, or select Both.



[You're reading an excerpt. Click here to read official LINKSYS](http://yourpdfguides.com/dref/326045)

[WRT300N user guide](http://yourpdfguides.com/dref/326045)

<http://yourpdfguides.com/dref/326045>