



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for NETGEAR WNR2200. You'll find the answers to all your questions on the NETGEAR WNR2200 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual NETGEAR WNR2200
User guide NETGEAR WNR2200
Operating instructions NETGEAR WNR2200
Instructions for use NETGEAR WNR2200
Instruction manual NETGEAR WNR2200

N300 Wireless Router with USB WNR2200 User Manual



NETGEAR

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134 USA

202-10667-01
September 2010
v1.0



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

Manual abstract:

inc. In the United States and/or other countries. microsoft , Windows , and Windows NT are registered trademarks and Windows Vista is a trademark of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders. Statement of Conditions In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein. Certificate of the Manufacturer/Importer It is hereby certified that the N300 Wireless Router with USB WNR2200 has been suppressed in accordance with the conditions set out in the BMPT-AmstbIVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions. Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Regulatory Compliance Information This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority. ii v1. 0, September 2010 NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards: EN300 328, EN301 893, EN301 489-17, EN60950 A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WNR2200 product package. , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. FCC Requirements for Operation in the United States FCC Information to User This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals FCC Guidelines for Human Exposure This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. , 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the model WNR2200 N300 Wireless Router with USB WNR2200 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: • • This device may not cause harmful interference, and This device must accept any interference received, including interference that may cause undesired operation. Federal Communication Commission Interference Statement This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods: • • • Reorient or relocate the receiving antenna. Increase the separation between the equipment and the receiver.

Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected. Consult the dealer or an experienced radio/TV technician for help. FCC Caution: Any changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This product will be used for indoor operations. This device meets all the other requirements specified in Part 15E, Section 15. 407 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. IMPORTANT NOTE: Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user. v v1. 0, September 2010 Industry Canada Statement This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body. The device and its antenna(s) must not be co-located or operated in conjunction with any other antenna or transmitter. This Class B digital apparatus complies with Canadian ICES-003. cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The Country Code Selection feature is disabled for products marketed in the United States and Canada. Caution: N300 Wireless Router with USB WNR2200 Tested to Comply with FCC Standards FOR HOME OR OFFICE USE Modifications made to the product, unless expressly approved by NETGEAR, Inc.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/3951726)

[WNR2200 user guide](http://yourpdfguides.com/dref/3951726)

<http://yourpdfguides.com/dref/3951726>

, could void the user's right to operate the equipment. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. 0, September 2010 ix N300 Wireless Router with USB WNR2200 User Manual Connecting to the USB Drive from a Remote Computer . 7-12 Connecting to the USB Drive with Microsoft Network Settings . 8-7 Testing the Path from Your Computer to a Remote Device . 0, September 2010 x N300 Wireless Router with USB WNR2200 User Manual About This Manual The user manual provides information for configuring the features of the NETGEAR® N300 Wireless Router with USB WNR2200 beyond initial configuration settings. Initial configuration instructions can be found in the NETGEAR Wireless Router Setup Manual. You should have basic to intermediate computer and Internet skills.

Conventions, Formats, and Scope The conventions, formats, and scope of this manual are described in the following paragraphs: • **Typographical conventions.** This manual uses the following typographical conventions: *Italic Bold Fixed Italic Emphasis*, books, CDs User input, IP addresses, GUI screen text Command prompt, CLI text, code URL links • **Formats.** This manual uses the following formats to highlight special messages: **Note:** This format is used to highlight information of importance or special interest. **Tip:** This format is used to highlight a procedure that will save time or resources. **Warning:** Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data. This manual is written for the WNR2200 router according to these specifications: Product Version Manual Publication Date N300 Wireless Router with USB WNR2200 September 2010 For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents. □ **Note:** Product updates are available on the NETGEAR, Inc. How to Print This Manual To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>. **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

revision History NETGEAR, Inc. Is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the WNR2200 router was introduced. 0, September 2010 N300 Wireless Router with USB WNR2200 User Manual Chapter 1 **Configuring Your Internet Connection** This chapter describes how to configure your WNR2200 router Internet connection. When you install your wireless router using the Resource CD as described in the NETGEAR Router Setup Manual, these settings are configured automatically for you. This chapter provides instructions on how to log in to the wireless router for further configuration. **Note:** NETGEAR recommends using the Smart Wizard™ on the Resource CD for initial configuration, as described in the NETGEAR Wireless Router Setup Manual. This chapter includes: • "Using the Setup Manual" • "Logging In to Your Wireless Router" on page 1-2 • "Selecting a Language for Your Screen Display" on page 1-4 • "Using the Setup Wizard" on page 1-6 • "Viewing or Manually Configuring Your ISP Settings" on page 1-6 Using the Setup Manual For first-time installation of your wireless router, refer to the NETGEAR Router Setup Manual. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the Resource CD to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network.

After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless router. For installation instructions in a language other than English, see the language options on the Resource CD. **configuring Your Internet Connection v1.** 0, September 2010 1-1 N300 Wireless Router with USB WNR2200 User Manual **Logging In to Your Wireless Router** You can log in to the wireless router to view or change its settings. **Note:** Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in "Preparing Your Network" in Appendix B. **Com,** or the router's LAN IP address (default is 192. 1) in the address field of your browser, and then press Enter. a login window displays: Figure 1-1 2. Enter admin for the router user name and your password (or the default, password).

For information about how to change the password, see "Changing the Built-In Password" on page 3-2. **Note:** The router user name and password are not the same as any other user name or password you might use to log in to your Internet connection. **configuring Your Internet Connection v1.** 0, September 2010 1-2 N300 Wireless Router with USB WNR2200 User Manual **The Checking for Firmware DNS address,** restart the computers on your network so that these settings take effect. 4. If no login is required, you can specify the MAC Address setting. If the NETGEAR website does not appear within one minute, see Chapter 8, "Troubleshooting". When your Internet connection is working, you do not need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your wireless router automatically logs you in. The fields that are displayed depend on whether or not your Internet connection requires a login.

ISP does not require login ISP does require login Figure 1-6 The following table explains the fields in the Basic Settings screen. These fields Account Name appear only if no (If required) login is required. Domain Name (If required) Description • Yes • No Enter the account name provided by your ISP. This might also be called the host name. Enter the domain name provided by your ISP.

internet Service Provider • PPTP (Point to Point Tunneling Protocol). This is used These fields primarily in Austrian DSL services. appear only if • Telstra Bigpond. This setting is only for older cable modem your ISP service accounts that still require a Bigpond Login utility. Those with Telstra DSL accounts and newer cable modem accounts should select No for Does Your Internet Connection Require A Login? • Other.

This is the default setting. It is for PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide. login Password Service Name Connection Mode The login name provided by your ISP. This is often an e-mail address. The password provided by your ISP.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

If your ISP provided a Service Name, enter it here. Specify when the router will connect to and disconnect from the Internet. • Always On. The router logs in to the Internet immediately after booting and never disconnects. • Dial on Demand.

The router logs in only when outgoing traffic is present and logs out after the idle time-out. • Manually Connect. The router logs in or logs out only when you click Connect or Disconnect in the Router Status screen. Idle Timeout (In minutes) If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless router keeps the Internet connection active after there is no Internet activity from the LAN. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • Use Static IP Address. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address.

The gateway is the ISP's wireless router to which your wireless router will connect. The DNS server is used to look up site addresses based on their names. • Get Automatically from ISP. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.

• Use These DNS Servers. If you know that your ISP does not automatically transmit DNS addresses to the wireless router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. The Ethernet MAC address that will be used by the wireless router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened.

They will then accept traffic only from the MAC address of that computer. This feature allows your wireless router to masquerade as that computer by "cloning" its MAC address. • Use Default Address. Use the default MAC address of the router (normally the LAN MAC address). • Use Computer MAC Address. The wireless router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • Use This MAC Address. Enter the MAC address that you want to use. Domain Name Server (DNS) Address This field appears only if no login is required.

router MAC Address Configuring Your Internet Connection v1. 0, September 2010 1-9 Chapter 2 Safeguarding Your Network For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the wireless router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security. Warning: Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network. This chapter includes: ••••• "Planning Your Wireless Network" "Manually Configuring Your Wireless Settings" on page 2-4 "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-12 "Connecting Additional Wireless Client Devices After WPS Setup" on page 2-17 "Restricting Access to Your Router" on page 2-19 Note: For information about restricting access to USB storage devices, see "Configuring USB Storage Advanced Settings" on page 7-7. Planning Your Wireless Network For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly. To configure the wireless network, you can either specify the wireless settings, or you can use WiFi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security. □ To manually configure the wireless settings, you must know the following: – SSID. The default SSID for the wireless router is NETGEAR.

To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports. see "Manually Configuring Your Wireless Settings" on page 2-4. □ Push 'N' Connect (WPS) automatically implements wireless security on the wireless router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the wireless router, clicking an onscreen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see <http://www.allthingswifi.com>). All other WiFi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect. To set up your wireless network using the WPS feature: – Use the WPS button on the side of the wireless router (there is also an onscreen WPS button), or enter the PIN of the wireless device. □ Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration. see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-12.

Wireless Placement and Range Guidelines The range of your wireless connection can vary significantly based on the physical placement of the wireless router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices. For best results, place your wireless router according to the following guidelines: ••••• Near the center of the area in which your PCs will operate. In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls). 0, September 2010 2-2 N300 Wireless Router with USB WNR2200 User Manual •• Put the router in a vertical position to provide the best side-to-side coverage. Put the router in a horizontal position to provide the best up-and-down coverage. If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11). The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish.

Also, WEP encryption can consume more battery power on a notebook computer. Such distances can allow for others outside your immediate area to access your network. Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WNR2200 router provides highly effective security features which are covered in detail in this chapter.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

Deploy the security features appropriate to your needs. There are several ways you can enhance the security of your wireless network: Wireless data security options Range: up to 300 foot radius 1) Open system: easy, but no security. 2) WEP: security, but some performance impact. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys.

The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise. • Safeguarding Your Network v1.0, September 2010 2-3 N300 Wireless Router with USB WNR2200 User Manual For more information about wireless technology, see the link to the online document in "Wireless Networking Basics" in Appendix B. Manually Configuring Your Wireless Settings You can view or manually configure the wireless settings for the wireless router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.

Note: If you use a wireless computer to change the wireless network name (SSID) or wireless security settings, you will be disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the wireless router. To view or manually configure the wireless settings: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin>.

Net with its default user name of admin, and default password of password, or using whatever password and LAN address you have chosen for the wireless router. Select Wireless Settings from the main menu to display the Wireless Settings screen: Figure 2-2 The settings for this screen are explained in Table 2-1 on page 2-6. 3. Select the region in which the wireless router will operate. 4. For initial configuration and test, leave the other settings unchanged. Configure and test your computers for wireless connectivity. Program the wireless adapter of your computers to have the same SSID and wireless security settings as your wireless router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless router. If there is interference, adjust the channel.

Select from the countries in the drop-down list. Note: In the US, the region is pre-selected as the United States. Enable SSID Broadcast The SSID of any wireless access adapter must match the SSID you configure in the wireless router. If they do not match, you will not get a wireless connection to the wireless router. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP. This is the wireless network name. Enter a 32-character (maximum) name in this field. this field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic.

Any device that you want to participate in a wireless network must use the SSID. The wireless channel fields determine the operating frequency used for the 11N or 11G wireless networks. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best. Legacy mode, using a maximum speed of up to 54 Mbps for b/g networks.

• Up to 150 Mbps. Neighbor friendly mode, for reduced interference with neighboring wireless networks. Provides two transmission streams with different data on the same channel at the same time, but also allows 802. This is the default value for the 2. Performance mode, using a maximum Wireless-N speed of up to 300 Mbps.

You can use this setting to establish wireless connectivity before implementing wireless security. This option is only available for "Up to 54 Mbps" wireless mode. For other wireless modes, this option is disabled. Use encryption keys and data encryption for data security. When you select this option, these additional areas appear on your screen: • Security Encryption (WEP). Select the Authentication Type (Automatic or Shared Key) and the Encryption Strength (64 bit or 128 bit). security Encryption (WEP) Key. Enter the Passphrase, select a key, and click Generate. • WPA-PSK [TKIP] (WiFi Protected Access Pre-Shared Key). This option is only available for "Up to 54 Mbps" wireless mode.

For other wireless modes, this option is disabled. Allow only computers configured with WPA to connect to the wireless router. When you select this option, this additional area appears on your screen: • Security Options (WPA-PSK). enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits. • WPA2-PSK [AES] (Wi-Fi Protected Access with 2 Pre-Shared Keys). Allow only computers configured with WPA2 to connect to the wireless router. When you select this option, this additional area appears on your screen: • Security Options (WPA2-PSK). enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits.

• WPA-PSK [TKIP] + WPA2-PSK [AES]. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router. When you select this option, this additional area appears on your screen: • Security Options (WPA-PSK + WPA2-PSK). enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits.

Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router. When you select this option, this additional area appears on your screen: Security Options (WPA/WPA2 Enterprise) • WPA Mode. Select the WPA Mode from the drop-down list (WPA [TKIP], WPA2 [AES], or WPA [TKIP + WPA2 [AES]]). rADIUS server IP Address. Enter the IP address of the RADIUS server.

rADIUS server Port. The RADIUS server port number is listed in this field. • Configuring WEP Wireless Security Note: WEP security is only available when you select Up to 54 Mbps on the Wireless Settings screen. Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes. to configure WEP data encryption: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin>. Net with its default user name of admin, and default password of password, or using whatever password and LAN address you have chosen for the wireless router. From the main menu, select Wireless Settings to display the Wireless Settings screen.

Set the Security Options by selecting the WEP radio button in the Security Options section: Figure 2-3 3.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

You can select an automatic authentication scheme, which may not run authentication, but still leaves the data transmissions encrypted. If you require strong security, use both the Shared Key and WEP encryption settings. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network: Safeguarding Your Network v1.0, September 2010 2-9 N300 Wireless Router with USB WNR2200 User Manual – Passphrase. To use a passphrase to generate the keys, enter a passphrase, and click Generate. This automatically creates the keys.

Wireless stations must use the passphrase or keys to access the wireless router. Note: Not all wireless adapters support passphrase key generation. – Key 1 – Key 4. These values are not case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Select which of the four keys will be the default.

Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected. Configuring WPA, WPA2, or WPA/WPA2 Wireless Security To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see “Using Push ‘N’ Connect (WPS) to Configure Your Wireless Network” on page 2-12. Both WPA and WPA2 provide strong data security.

WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later. NETGEAR recommends using WPA2 with AES, which provides the strongest security. WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings. Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. If this happens, reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes. Safeguarding Your Network v1.0, September 2010 2-10 N300 Wireless Router with USB WNR2200 User Manual To configure WPA or WPA2 in the wireless router: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin>.

Net with its default user name of admin and default password of password, or using whatever password and LAN address you have chosen for the wireless router. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice. Figure 2-4 4. The settings displayed on the screen depend on which security option you select. 5. For WPA-PSK or WPA2-PSK, enter the passphrase. 6. For WPA/WPA2 Enterprise, enter the settings for the Radius server. 1x, these settings are required for communication with the primary Radius server. The IP address of the Radius server.

Port number of the Radius server. This shared key is shared between the wireless access point and the Radius server during authentication. 0, September 2010 2-11 N300 Wireless Router with USB WNR2200 User Manual Using Push ‘N’ Connect (WPS) to Configure Your Wireless Network If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the wireless router’s SSID and security settings and, at the same time, connect the wireless client securely and easily to the wireless router. Look for the symbol on your client device (computers that will connect wirelessly to the wireless router are clients). WPS automatically configures the network name (SSID) and wireless security settings for the wireless router (if the wireless router is in its default state) and broadcasts these settings to the wireless client.

Note: NETGEAR’s Push ‘N’ Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see <http://www>. All other Wi-Fi certified and WPS-capable products should be compatible with NETGEAR products that implement Push ‘N’ Connect. Some considerations regarding WPS are: • WPS supports these types of wireless security: None, WPA-PSK, WPA2-PSK, and WEP (with the authentication type set to Automatic on the Wireless Settings screen). WEP security with shared key authentication is not supported by WPS. If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices.

This is the preferred method. For information about using the PIN method, see “Using PIN Entry to Add a WPS Client” on page 2-14. □ A WPS client can be added using the Push Button method or the PIN method. • Safeguarding Your Network v1.0, September 2010 2-12 N300 Wireless Router with USB WNR2200 User Manual Using a WPS Button to Add a WPS Client Any wireless computer or wireless adapter that will connect to the wireless router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart. To use the wireless router WPS button to add a WPS client: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin>. Net with its default user name of admin and default password of password, or using whatever LAN address and password you have set up.

2. On the wireless router main menu, select Add a WPS Client, and then click Next. The following screen displays: WPS button Figure 2-5 By default, the Push Button (recommended) radio button is selected. 3. Either press the WPS button on the side of the wireless router, or click the onscreen button. The wireless router tries to communicate with the client for 2 minutes. 4. Go to the client wireless computer, and run a WPS configuration utility. Go back to the wireless router screen to check for a message. Safeguarding Your Network v1.

0, September 2010 2-13 N300 Wireless Router with USB WNR2200 User Manual The wireless router WPS screen displays a message confirming that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security. The wireless router will keep these wireless settings unless you change them, or you clear the Keep Existing Wireless Settings check box in the WPS Settings screen. Figure 2-6 6. Note the new SSID and WPA/WPA2 password for the wireless network.

You can view these settings in the Wireless Settings screen. see “Manually Configuring Your Wireless Settings” on page 2-4. To access the Internet from any computer connected to your wireless router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

You should see the wireless router's Internet LED blink, indicating communication to the ISP. Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed, and no security will be implemented on the wireless router.

Using PIN Entry to Add a WPS Client Any wireless computer or wireless adapter that will connect to the wireless router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart. The first time you add a WPS client, make sure that the Keep Existing Wireless Settings check box on the WPS Settings screen is cleared. This is the default setting for the wireless router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later. safeguarding Your Network v1. 0, September 2010 2-14 N300 Wireless Router with USB WNR2200 User Manual To use a PIN to add a WPS client: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin.net> with its default user name of admin and default password of password, or using whatever LAN address and password you have set up.

2. On the wireless router main menu, select Add a WPS Client (computers that will connect wirelessly to the wireless router are clients), and then click Next. Take note of the client PIN. 5. From the wireless router Add WPS Client screen, enter the client PIN number, and then click Next. □ – The wireless router tries to communicate with the client for 4 minutes. The wireless router WPS screen displays a message confirming that the client was added to the wireless network. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See "Manually Configuring Your Wireless Settings" on page 2-4 To access the Internet from any computer connected to your wireless router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox.

You should see the wireless router's Internet LED blink, indicating communication to the ISP. Note: If no WPS-capable client devices are located during the 4-minute time frame, the SSID will not be changed and no security will be implemented on the wireless router. safeguarding Your Network v1. 0, September 2010 2-15 N300 Wireless Router with USB WNR2200 User Manual Configuring Advanced WPS Settings From the Advanced menu, select Advanced Wireless Settings to display the following screen: Figure 2-8 The WPS Settings area displays the wireless router PIN, and allows you to Disable Router's PIN and to Keep Existing Wireless Settings for the wireless network. By default, the Keep Existing Wireless Settings check box is unchecked.

This allows the wireless router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented or changes in wireless settings are applied, the wireless router automatically selects this check box so that your SSID and wireless security settings remain the same if you add WPS-enabled devices or if you manually add non WPS-capable devices later. Note: If you clear the Keep Existing Wireless Settings check box, all wireless settings and connections will be lost. safeguarding Your Network v1. 0, September 2010 2-16 N300 Wireless Router with USB WNR2200 User Manual Connecting Additional Wireless Client Devices After WPS Setup You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Adding More WPS Clients Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the Keep Existing Wireless Settings check box is selected in the Advanced Wireless screen (listed under the Advanced heading in the wireless router main menu). If you clear this check box, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the wireless router. To view a list of all devices connected to your wireless router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 4-9. Adding Both WPS and Non-WPS Clients For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see "Manually Configuring Your Wireless Settings" on page 2-4). to connect a combination of non-WPS enabled and WPS-Enabled clients to the wireless router: 1. Restore the wireless router to its factory default settings (press and hold the Reset button on the back of the router for 5 seconds). When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the wireless router. 2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see "Manually Configuring Your Wireless Settings" on page 2-4).

For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase). 4. For the WPS devices that you want to connect, follow the procedure "Using a WPS Button to Add a WPS Client" on page 2-13 or "Using PIN Entry to Add a WPS Client" on page 2-14. The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the wireless router. Note: To make sure that your new wireless settings remain in effect, verify that the Keep Existing Wireless Settings checkbox is selected in the WPS Settings screen. 5. To view a list of all devices connected to your wireless router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 4-9. safeguarding Your Network v1. 0, September 2010 2-18 N300 Wireless Router with USB WNR2200 User Manual Restricting Access to Your Router You can use the Advanced Wireless Settings screen to enable or disable the wireless router. From the main menu, select Advanced Wireless Settings to display the following screen: Figure 2-9 • Enable Wireless Router Radio.

You can completely turn off the wireless portion of the wireless router. For example, if you use your notebook computer to wirelessly connect to your wireless router, and you take a business trip, you can turn off the wireless portion of the wireless router while you are traveling. Other members of your household who use computers connected to the wireless router via Ethernet cables can still use the wireless router. To do this, clear the Enable Wireless Router Radio check box on the Advanced Wireless Settings screen, and then click Apply.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

(You can also turn the wireless portion of the router by pressing the Wireless button on the front of the router.

) The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings. For information about WPS settings, see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-12. restricting access by MAC address. You can use a Wireless Card Access List to restrict access.

see "Restricting Access by MAC Address" on page 3-2. Adding Guest Networks Adding a guest network allows visitors at your home to use the Internet without having to know your wireless security key. You can add a guest network to the wireless network. To add a guest network, do the following: 1. Select any of the following Wireless settings: – Enable Guest Network – When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile. safeguarding Your Network v1. 0, September 2010 2-20 N300 Wireless Router with USB WNR2200 User Manual – Enable SSID Broadcast – If selected, the Wireless Access Point broadcasts its name (SSID) to all Wireless Stations. Stations with no SSID can adopt the correct SSID for connections to this Access Point. Enable Wireless Isolation – If selected, the wireless client under this SSID can only access the Internet, and cannot access other wireless clients, even clients under the same SSID, Ethernet clients, or this device. Allow Guest to access MY Local Network – If selected, any user who connects to this SSID can access local networks associated with the router like users in the primary SSID.

The name is case-sensitive and can be up to 32 characters. The same name must be assigned to all wireless devices in your network. NETGEAR recommends that you change the name to a different value. 0, September 2010 2-21 Chapter 3 Protecting Your Network This chapter describes how to use the content filtering and reporting features of the N300 Wireless Router with USB WNR2200 to protect your network. You can find these features by selecting the items under Content Filtering in the wireless router main menu. This chapter includes the following sections: • "Protecting Access to Your Wireless Router" • "Restricting Access by MAC Address" on page 3-2 • "Blocking Access to Internet Sites" on page 3-4 • "Blocking Access to Internet Services" on page 3-6 • "Scheduling Blocking" on page 3-8 • "Viewing Logs of Web Access or Attempted Web Access" on page 3-10 • "Configuring E-mail Alert and Web Access Log Notifications" on page 3-9 • "Setting the Time" on page 3-11 Protecting Access to Your Wireless Router For security reasons, the wireless router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter admin for the wireless router user name and password for the wireless router password. You can use procedures in the following sections to change the wireless router password and the amount of time for the administrator's login time-out. Note: The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters. 3-1 v1. 0, September 2010 N300 Wireless Router with USB WNR2200 User Manual Changing the Built-In Password 1.

Log in to the wireless router at its default LAN address of <http://www.routerlogin.net> with its default user name of admin, default password of password, or using whatever password and LAN address you have chosen for the wireless router. 2. From the main menu, under the Maintenance heading, select Set Password to display the Set Password screen: 3.

To change the password, first enter the old password, and then enter the new password twice. Note: After changing the password, you must log in again to continue the configuration. If you have backed up the wireless router settings previously, you should do a new backup so that the saved settings file includes the new password. Restricting Access by MAC Address For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WNR2200 router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. to restrict access based on MAC addresses: 1. Log in to the wireless router at its default LAN address of <http://www.routerlogin.net> with its default user name of admin, and default password of password, or using whatever password and LAN address you have chosen for the wireless router.

Note: If you configure the router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the wireless router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes. From the Advanced menu, select Wireless Settings, and then click Set Up Access List to display the Wireless Card Access List screen. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses. figure 3-2 4. Adjust the list as needed for your network. You can add devices using either of the following methods: • If the computer is in the Available Wireless Cards table, select the radio button of that computer to capture its MAC address. protecting Your Network v1. 0, September 2010 3-3 N300 Wireless Router with USB WNR2200 User Manual • Use the Add button to enter the MAC address of the device to be added.

The MAC address can usually be found on the bottom of the wireless device. Note: If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding. 5. Click Add, and then click Apply to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the router.

Blocking Access to Internet Sites The WNR2200 router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. Keyword application examples: • If the keyword XXX is specified, the URL www.com is specified, only websites with other domain suffixes (such as . To block by schedule, be sure to specify a time period in the Schedule screen.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

For information about scheduling, see "Scheduling Blocking" on page 3-8. Block all access to Internet browsing during a scheduled period by entering a dot (.) as the keyword, and then set a schedule in the Schedule screen. 3. Add a keyword or domain by entering it in the keyword field and clicking Add Keyword.

The keyword or domain name then appears the Block sites containing these keywords or domain names list. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the Trusted IP Address fields. Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address. 5.

Click Apply to save all your settings in the Block Sites screen. Blocking Access to Internet Services The wireless router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request. Enable service blocking by selecting either Per Schedule or Always, and then click Apply. protecting Your Network v1.

0, September 2010 3-6 N300 Wireless Router with USB WNR2200 User Manual To block by schedule, be sure to specify a time period in the Schedule screen.

For information about scheduling, see "Scheduling Blocking" on page 3-8. From the Service Type list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select User Defined.

5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields. You can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network. Configuring a User-Defined Service To define a service, first you must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers.

□ Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching. protecting Your Network v1. 0, September 2010 3-7 N300 Wireless Router with USB WNR2200 User Manual • • Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select Both. Configure the schedule for blocking keywords and services. Select days on which you want to apply blocking by selecting the appropriate check boxes. Select Every Day to select the check boxes for all days.

Be sure to select your time zone in the E-mail screen as described in "Setting the Time" on page 3-11. Configuring E-mail Alert and Web Access Log Notifications To receive logs and alerts by e-mail, you must provide your e-mail account information. To receive e-mail logs and alerts from the router, select the Turn E-mail Notification On check box. Enter the name of your ISP's outgoing (SMTP) mail server (such as mail. You might be able to find this information in the configuration screen of your e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail. b. Enter the e-mail address to which logs and alerts are sent in the Send To This E-mail Address field. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by e-mail.

3. If your outgoing e-mail server requires authentication, select the My Mail Server requires authentication check box. a. Enter your user name for the outgoing e-mail server in the User Name field. b.

Enter your password for the outgoing e-mail server in the Password field. 4. You can specify that logs are automatically sent by e-mail with these options: • • Send alert immediately. Select this check box for immediate notification of attempted access to a blocked site or service. send Logs According to this Schedule. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full. -- Day. Specifies which day of the week to send the log. Specifies the time of day to send the log. relevant when the log is sent daily or weekly. If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents. So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Viewing Logs of Web Access or Attempted Web Access The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user. protecting Your Network v1. 0, September 2010 3-10 N300 Wireless Router with USB WNR2200 User Manual Select Logs under Content Filtering in the main menu. Log Entry Descriptions Field Description Date and time Source IP Target address Action The date and time the log entry was recorded. The IP address of the initiating device for this log entry. The name or IP address of the website or newsgroup visited or to which access was attempted. whether the access was blocked or allowed. To refresh the log screen, click the Refresh button.

To clear the log entries, click the Clear Log button. To e-mail the log immediately, click the Send Log button. Setting the Time The WNR2200 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. To localize the time for your log entries, you must specify your time zone: Protecting Your Network v1. 0, September 2010 3-11 N300 Wireless Router with USB WNR2200 User Manual • • Time Zone.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>

Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries. automatically Adjust for Daylight Savings Time. Select this check box if your region supports daylight savings time. When this check box is set, the router will adjust the time by adding one hour during the daylight savings time period.

When daylight savings time ends, be sure to un-check this check box. protecting Your Network v1. 0, September 2010 3-12 N300 Wireless Router with USB WNR2200 User Manual Chapter 4 Using Network Monitoring Tools This chapter describes features to help you manage your N300 Wireless Router with USB WNR2200. This chapter includes the following sections: • “Upgrading the Router Firmware” • “Viewing Wireless Router Status Information” on page 4-5 • “Viewing a List of Attached Devices” on page 4-9 • “Managing the Configuration File” on page 4-10 • “Enabling Remote Management Access” on page 4-12 • “Traffic Meter” on page 4-14 Upgrading the Router Firmware The routing software (also called firmware) of the WNR2200 router is stored in flash memory, and can be upgraded as NETGEAR releases new software. Your router can download and install the new software, or you can download upgrade files from the NETGEAR website and manually send the upgrade file to the router using your browser. Tip: To ensure that you are always using the latest router firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability. using Network Monitoring Tools v1. 0, September 2010 4-1 N300 Wireless Router with USB WNR2200 User Manual The Checking for Firmware Updates screen appears at login unless you clear the Check for Updated Firmware Upon Log-in check box. Figure 4-1 A screen is also provided for upgrading the router. From the main menu, under Maintenance, select Router Upgrade to display the Router Upgrade screen.

Figure 4-2 From this screen, you can check for new software versions by clicking the Check button. If a new version is found, you can download and install it in one step. To enable the Smart Wizard to automatically check for a new software version upon login, select the Check for New Version Upon Log-in check box. Alternatively, you can manually install an upgrade file stored on your computer. Tip: Before upgrading the router software, use the router Settings Backup screen to save your configuration settings. A router upgrade might cause the router settings to revert to the factory defaults. If this happens, after completing the upgrade, you can restore your settings from the backup. using Network Monitoring Tools v1. 0, September 2010 4-2 N300 Wireless Router with USB WNR2200 User Manual Upgrading Automatically to New Router Software If you have selected Check for New Version Upon Log-in, your router alerts you to the new software when you log in. Otherwise, you can click the Check button in the Router Upgrade screen to search for new software. If the router discovers a newer version of software, the message on the left displays when you log in. If no new firmware is available, the message on the right displays. Figure 4-3 To automatically upgrade to the new software, click Yes to allow the router to download and install the new software file from NETGEAR. Warning: When uploading software to the WNR2200 router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software.

When the upload is complete, your router automatically restarts. The upgrade process typically takes about three minutes. Read the new software release notes to determine whether you must reconfigure the router after upgrading. Upgrading Manually to New Router Software To manually select, download, and install new software to your router: 1. under Maintenance on the main menu , select Router Status.

Note the version number of your router firmware. 2. Go to the WNR2200 support page on the NETGEAR website at <http://www>. Check the most recent firmware version offered against the firmware version shown in the Router Status screen. If the version on the NETGEAR website is more recent, download the file to your computer. Click Browse, and locate the firmware image that you downloaded to your PC (the file ends in . Click Upload to send the firmware to the router. Warning: When uploading software to the WNR2200 router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the software. When the upload is complete, your router automatically restarts.

The upgrade process typically takes about three minutes. Read the new software release notes to determine whether you must reconfigure the router after upgrading. using Network Monitoring Tools v1. 0, September 2010 4-4 N300 Wireless Router with USB WNR2200 User Manual Viewing Wireless Router Status Information To view router status and usage information, from the main menu, under the Maintenance heading, select Router Status. 0, September 2010 4-5 N300 Wireless Router with USB WNR2200 User Manual You can use the Show Statistics and Connection Status buttons to view additional status information, as described in “Connection Status” on page 4-7 and “Statistics” on page 4-8. The version of the router firmware. It changes if you upgrade the router. The localized language of the GUI. the Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the router.

The IP address being used by the Internet (WAN) port of the router. 0, the router cannot connect to the Internet. • None. The router uses a fixed IP address on the WAN. • DHCP Client.

The router obtains an IP address dynamically from the ISP. IP Subnet Mask The IP subnet mask being used by the Internet (WAN) port of the router. For an explanation of subnet masks and subnet addressing, click the link to the online document “TCP/IP Networking Basics” in Appendix B. Domain Name Server LAN Port MAC Address IP Address DHCP The Domain Name Server addresses being used by the router. This is the unique physical address being used by the Ethernet (LAN) port of the router.

The IP address being used by the Ethernet (LAN) port of the router. Identifies whether the router’s built-in DHCP server is active for the LAN attached devices. IP Subnet Mask The IP subnet mask being used by the Ethernet (LAN) port of the router. Wireless Router Status Fields (continued) Field Wireless Settings Description Name (SSID): The 11N wireless network name (SSID) being used by the wireless port of the router. the default is NETGEAR. Region: The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.



[You're reading an excerpt. Click here to read official NETGEAR WNR2200 user guide](http://yourpdfguides.com/dref/3951726)
<http://yourpdfguides.com/dref/3951726>