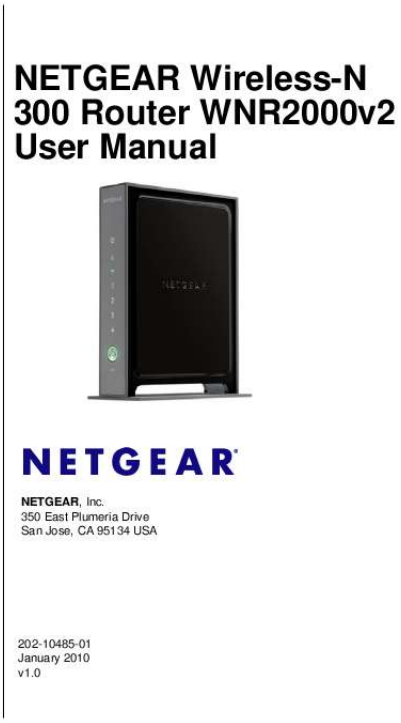

NETGEAR Wireless-N
300 Router WNR2000v2
User Manual

NETGEAR

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

202-10485-01
January 2010
v1.0

Manual abstract:

@@@@@@@@Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the Knowledge Base or the Documentation link under Web Support on the main menu to view support information. Trademarks NETGEAR and the NETGEAR logo are registered trademarks, and RangeMax and Smart Wizard are trademarks of NETGEAR. 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. @@@@Please refer to the notes in the operating instructions. @@Das vorschriftsmäßige Betreiben einiger Geräte (z. B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung. @@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, January 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 This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC: · · EN 60950-1: 2001 Safety of information technology equipment EN 300 328 V1.7. 1 (2006-10) Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive EN 301 489-17 V1.2.1 (2002-08) and EN 301 489-1 V1.4.1 (2002-08) Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment · This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries under the following conditions and/or with the following restrictions: · In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services. This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

· Cesky [Czech] Dansk [Danish] Deutsch [German] Eesti [Estonian] English Español [Spanish] [NETGEAR Inc.] tímto prohlasuje, ze tento [WNR2000] je ve shode se základními pozadavky a dalsími príslusnými ustanoveními smernice 1999/5/ES. Undertegnede [NETGEAR Inc.] erklærer herved, at følgende udstyr [WNR2000] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. Hiermit erklärt [NETGEAR Inc.], dass sich das Gerät [WNR2000] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. Käesolevaga kinnitab [NETGEAR Inc.] seadme [WNR2000] vastavust direktiivi 1999/5/ EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. Hereby, [NETGEAR Inc.], declares that this [WNR2000] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Por medio de la presente [NETGEAR Inc.] declara que el [WNR2000] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. iii v1.0, January 2010 E [Greek] Français [French] Italiano [Italian] Latviski [Latvian] Lietuvi [Lithuanian] Nederlands [Dutch] Malti [Maltese] Magyar [Hungarian] Polski [Polish] Português [Portuguese] Slovensko [Slovenian] Slovensky [Slovak] Suomi [Finnish] Svenska [Swedish] [NETGEAR Inc.] [WNR2000] 1999/5/.

Par la présente [NETGEAR Inc.] déclare que l'appareil [WNR2000] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Con la presente [NETGEAR Inc.] dichiara che questo [WNR2000] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. Ar so [NETGEAR Inc.

] deklar, ka [WNR2000] atbilst Direktvas 1999/5/EK btiskajm prasbm un citiem ar to saisttajiem noteikumiem. Siuo [NETGEAR Inc.] deklaruoja, kad sis [WNR2000] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. Hierbij verklaart [NETGEAR Inc.]. dat het toestel [WNR2000] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Hawnhekk, [NETGEAR Inc.], jiddikjara li dan [WNR2000] jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC. Alulírott, [NETGEAR Inc.] nyilatkozom, hogy a [WNR2000] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.

Niniejszym [NETGEAR Inc.] owiadcza, e [WNR2000] jest zgodny z zasadniczymi wymogami oraz pozostalymi stosownymi postanowieniami Dyrektywy 1999/5/EC. [NETGEAR Inc.] declara que este [WNR2000] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. [NETGEAR Inc.] izjavlja, da je ta [WNR2000] v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolocili direktive 1999/5/ES. [NETGEAR Inc.] týmto vyhlasuje, _e [WNR2000] spa základné po_iadavky a vsetky príslusné ustanovenia Smernice 1999/5/ES. [NETGEAR Inc.] vakuuttaa täten että [WNR2000] tyyppinen laite on direktiivin 1999/5/ EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. Härmed intygar [NETGEAR Inc.] att denna [WNR2000] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

iv v1.0, January 2010 FCC Requirements for Operation in the United States Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice: 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 in a residential installation.
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. However, there is no guarantee that interference will not occur in a particular installation. 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 measures: · · · · Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help. To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices). FCC Radiation Exposure Statement This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This device complies with Part 15 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. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. 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. FCC Declaration Of Conformity We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WNR2000v2 Wireless-N 300 Router Model WNR2000v2 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: v v1.0, January 2010 · · This device may not cause harmful interference, and This device must accept any interference received, including interference that may cause undesired operation. FCC Radio Frequency Interference Warnings & Instructions 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 in a residential installation.
This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interf.....

.....

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

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

.....
... A-1 General Specifications ..
.....
.....

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

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

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

.. A-3 Appendix B Related Documents Index Contents v1.0, January 2010 x About This Manual The user manual provides information for configuring the features of the NETGEAR® Wireless-N 300 Router Model WNR2000v2 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, 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. xi v1.0, January 2010 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Danger: This is a safety warning. Failure to take heed of this notice might result in personal injury or death. · Scope. This manual is written for the WNR2000v2 router according to these specifications: Product Version Manual Publication Date Wireless-N 300 Router Model WNR2000v2 January 2010 For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR website in Appendix B, "Related Documents." Note: Product updates are available on the NETGEAR, Inc. website at http://www.netgear.com/support.

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 WNR2000v2 router was introduced. Table 2-1. Publication Revision History Part Number 202-10485-01 Version Number 1. 0 Date January 2010 Description First publication. xii v1.0, January 2010 Chapter 1 Configuring Basic Connectivity This chapter describes the settings for your Internet connection and your wireless local area network (LAN) connection. When you perform the initial configuration of your wireless router using the Resource CD as described in the NETGEAR Wireless Router Setup Manual, these settings are specified automatically for you. This chapter provides further details about these connectivity settings, as well as instructions on how to log in to the router for further configuration. Note: NETGEAR recommends using the Smart WizardTM on the Resource CD for initial configuration, as described in the NETGEAR Wireless Router Setup Manual. This chapter includes the following sections: · "Using the Setup Manual" on page 1-1 · "Logging In To Your Wireless Router" on page 1-2 · "Selecting a Language for Your Screen Display" on page 1-5 · "Configuring Your Internet Connection Using the Smart Setup Wizard" on page 1-6 · "Viewing and Configuring Basic ISP Settings" on page 1-7 · "Setting Up and Testing Basic Wireless Connectivity" on page 1-11 Using the Setup Manual For first-time installation of your wireless router, refer to the NETGEAR Wireless 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 User Manual to configure additional features of your wireless router.

For installation instructions in a language other than English, refer to the language options on the Resource CD. 1-1 v1.0, January 2010 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Logging In To Your Wireless Router When the wireless router is connected to your network, you can access and configure the router using your browser. To access the router: 1. Connect to the wireless router by typing http://www.routerlogin.net in the address field of your browser, and then press Enter. A login window displays. Figure 1-1 Tip: You can connect to the wireless router by typing either of these URLs in the address field of your browser, and then pressing Enter: · · http://www.routerlogin.

net http://www.routerlogin.com If these URLs do not work, you must type the IP address of the router, for example, http://www.192.168.

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 Administrator Password" on page 2-21.

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 Basic Connectivity v1.0, January 2010 1-2 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual The Checking for Firmware Updates screen appears unless you previously cleared the Check for Updated Firmware Upon Log-in check box. Figure 1-2 If the router discovers a newer version of firmware, the message on the left displays when you log in. If no new firmware is available, the message on the right displays. Figure 1-3 To automatically update to the new firmware, click Yes to allow the router to download and install the new firmware file from NETGEAR. Warning: When uploading firmware to the WNR2000v2 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 firmware. When the upload is complete, your router automatically restarts. The update process typically takes about 1 minute.

Configuring Basic Connectivity v1.0, January 2010 1-3 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 3. In the main menu on the left, select Basic Settings under Setup. The Basic Settings screen displays showing the wireless router's home page and suggested default settings. Figure 1-4 Note: If the Check for New Version Upon Log-in check box is selected, the home page is the Router Upgrade screen. Otherwise, it is the Basic Settings screen. If the wireless router is connected to the Internet, you can select Knowledge Base or Documentation under Web Support in the main menu to view support information or the documentation for the wireless router. Configuring Basic Connectivity v1.0, January 2010 1-4 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual If you do not click Logout, the wireless router will wait for 5 minutes after no activity before it automatically logs you out. Selecting a Language for Your Screen Display Using the Select Language drop-down menu, located in the upper right corner of the Router Manager screen, you can display the router manager screens in any of languages shown in Figure 1-5: Figure 1-5 Configuring Basic Connectivity v1.

0, January 2010 1-5 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual The language is set to English by default.

The default language is always stored in memory. When you select a language other than the default, that language as well as English is stored in memory. The additional language stored is the most recently selected. For example, if you select Deutsch, German and English will be stored.

If you next select Chinese, Chinese and English will be stored. To specify a language to be used on your router manager screens, do the following: 1. Expand the list and select the language you want. 2. Click Apply.

The language you select is then downloaded and displayed in the language selection box, and your screen display will be in the selected language. Note: You can select from the entire list of supported languages only when the router is connected to the Internet. When the router is not connected to the Internet, you can select one of the stored languages only. Configuring Your Internet Connection Using the Smart Setup Wizard You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Smart Setup Wizard to determine your Internet Service Provider (ISP) configuration. The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. To use the Smart Setup Wizard to assist with configuration or to verify the Internet connection settings: 1. Select Setup Wizard from the top of the main menu. 2. Click Next to proceed. Enter your ISP settings, as needed.

3. At the end of the Setup Wizard, click Test to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 7, "Troubleshooting." Configuring Basic Connectivity v1.0, January 2010 1-6 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Viewing and Configuring Basic ISP Settings Settings related to your Internet service are specified in the Basic Settings screen. Select Basic Settings under Setup in the main menu. The content you see in the Basic Settings screen depends on whether your ISP requires that you log in with a user name and password for Internet access. · No login required by ISP. If no login is required by your ISP, the following settings appear in the Basic Settings screen. ISP does not require login Figure 1-6 Configuring Basic Connectivity v1.

0, January 2010 1-7 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Account Name (might also be called Host Name). The account name is provided to the ISP during a DHCP request from your router. In most cases, this setting is not required, but some ISPs require it for access to ISP services such as mail or news servers. Domain Name. The domain name is provided by your router to computers on your LAN when the computers request DHCP settings from your router.

In most cases, this settings is not required. Internet IP Address. Determines how your router obtains an IP address for Internet access. · If your ISP assigns an IP address dynamically (by DHCP), select Get Dynamically From ISP. · If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select Use Static IP Address.

Enter the IP address that your ISP assigned. Also, enter the subnet mask and the gateway IP address. The gateway is the ISP's router to which your router will connect. Domain Name Server (DNS) Address. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use These DNS Servers, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. Note: If you enter or change a DNS address, restart the computers on your network so that these settings take effect. Router MAC Address. This section determines the Ethernet MAC address that the router will use on the Internet port. Typically, you would leave Use Default Address selected.

However, some ISPs (especially cable modem providers) register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They then accept only traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" or "spoofing" its MAC address. To change the MAC address, select one of the following methods: · Select Use Computer MAC Address. The router will then 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. Select Use This MAC Address, and enter it here. · Configuring Basic Connectivity v1.0, January 2010 1-8 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual If a login is required by your ISP, the following settings appear in the Basic Settings screen: ISP does require login Figure 1-7 · Does Your Internet Connection Require A Login? If you usually must use a login program such as WinPOET to access the Internet, your Internet connection requires a login. After you select Yes, the Basic Settings screen displays.

Note: After you finish setting up your router, you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router will automatically log you in. Internet Service Provider. This drop-down list contains a few ISPs that need special protocols for connection. The list includes: · PPTP (Point to Point Tunneling Protocol), used primarily in Austrian DSL services Configuring Basic Connectivity v1.

0, January 2010 1-9 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual · Telstra Bigpond, an Australian residential cable modem service Note: The Telstra Bigpond setting is only for older cable modem service accounts still requiring a Bigpond login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cable modem accounts should select No for Does Your Internet Connection Require a Login. · Other, which selects PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide. Figure 1-8 Note: Not all ISPs are listed here. The ones on this list have special requirements. Login and Password. This is the user name and password provided by your ISP. This name and password are used to log in to the ISP server. Service Name. If your connection is capable of connecting to multiple Internet services, this setting specifies which service to use. · Connection Mode. This drop-down list selects when the router will connect to and disconnect from the Internet. Figure 1-9 Configuring Basic Connectivity v1.0, January 2010 1-10 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual The list includes: · · · 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 the user clicks Connect or Disconnect in the Router Status screen. Idle Timeout. Your Internet connection is logged out if there is no data transfer during the specified time interval. Domain Name Server (DNS) Address. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use These DNS Servers, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Note: If you enter or change a DNS address, restart the computers on your network so that these settings take effect. Setting Up and Testing Basic Wireless Connectivity Note: If you use a wireless computer to change wireless settings, you might be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings, or access the router from a wired computer to make any further changes. Follow these instructions to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

Configuring Basic Connectivity v1.0, January 2010 1-11 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 1. Select Wireless Settings under Setup in the main menu of the WNR2000v2 router. Figure 1-10 2. For the wireless network name (SSID), use the default name, or choose a suitable descriptive name.

In the Name (SSID) field, you can enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR. Note: The SSID is case-sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you specify in the WNR2000v2 router. If they do not match, you will not get a wireless connection to the WNR2000v2 router. 3. Select the region in which the wireless interface will operate. 4. Set the channel. The default channel is Auto.

This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information about the wireless channel frequencies, click the link to the online document "Wireless Networking Basics" in Appendix B. 5. Make sure that the mode is set to Up to 145Mbps. Configuring Basic Connectivity v1.0, January 2010 1-12 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 6. For Security Options, select None. 7.

Click Apply to save your changes. Note: If you are configuring the router from a wireless computer and you change the router's SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the router's new settings. 8. Select Wireless Settings under Advanced in the main menu of the WNR2000v2 router.

Figure 1-11 9. Make sure that the Enable Wireless Router Radio, Enable SSID Broadcast, and Enable WMM check boxes are selected. 10. Click Setup Access List. 11.

Make sure that the Turn Access Control On check box is not selected. 12. Configure and test your wireless computer for wireless connectivity. Program the wireless adapter of your computer to have the same SSID and channel that you specified in the router, and disable encryption. Check that your computer has a wireless link and can obtain an IP address by DHCP from the router. Configuring Basic Connectivity v1.0, January 2010 1-13 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router (for more information about security and these settings, see Chapter 2, "Safeguarding Your Network "). Configuring Basic Connectivity v1.0, January 2010 1-14 Chapter 2 Safeguarding Your Network The Wireless-N 300 Router Model WNR2000v2 provides highly effective security features, which are covered in detail in this chapter. This chapter includes the following sections: · "Choosing Appropriate Wireless Security" · "Recording Basic Wireless Settings Setup Information" on page 2-5 · "Changing Wireless Security Settings" on page 2-6 · "Viewing Advanced Wireless Settings" on page 2-12 · "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13 · "Restricting Wireless Access by MAC Address" on page 2-19 · "Changing the Administrator Password" on page 2-21 · "Backing Up Your Configuration" on page 2-22 · "Understanding Your Firewall" on page 2-23 · "Adding Guest Networks" on page 2-23 Choosing Appropriate Wireless Security Unlike wired networks, wireless networks allow anyone with a compatible adapter to receive your wireless data transmissions well beyond your walls.

Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. Indoors, computers can connect over 802.11g/n wireless networks at ranges of up to 300 feet. Such distances can allow for others outside your immediate area to access your network. Use the security features of your wireless equipment that are appropriate to your needs. The time it takes to establish a wireless connection can vary depending on both your security settings and router placement. 2-1 v1.0, January 2010 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Stronger security methods can entail a cost in terms of throughput, latency, battery consumption, and equipment compatibility. In choosing an appropriate security level, you can also consider the effort compared to the reward for a hacker to break into your network. As a minimum, however, NETGEAR recommends using WEP with Shared Key authentication.

Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public. WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK, and WPA2-PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer. Note: NETGEAR recommends that you change the administration password of your router. Default passwords are well known, and an intruder can use your administrator access to read or disable your security settings.

For information about how to change the administrator password, see "Changing the Administrator Password" on page 2-21. Wireless data security options Range: up to 300 foot radius 1) Open system: easy but no security WNR2000 2) MAC access list: no data security 3) WEP: security but some performance impact 4) WPA-PSK: strong security 5) WPA2-PSK: very strong security Note: Use these with other features that enhance security (Table 2-2 on page 2-4).

Figure 2-1 To configure the wireless network, you can: · Manually specify your SSID and your wireless security settings. The WNR2000v2 router provides two screens for configuring the wireless settings: Safeguarding Your Network v1.0, January 2010 2-2 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual · Wireless Settings.

You access these under Setup in the main menu (see "Viewing Basic Wireless Settings" on page 2-6). Advanced Wireless Settings. You access these under Advanced in the main menu (see "Viewing Advanced Wireless Settings" on page 2-12). Use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/ WPA2 security on both the router and the client device. If the clients in your network are WPS capable, you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security on both the router and the client device (see "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13). Basic security options are listed in order of increasing effectiveness in Table 2-1. Other features that affect security are listed in Table 2-2 on page 2-4. For more details on wireless security methods, click the link to the online document "Wireless Networking Basics" in Appendix B. Table 2-1. Wireless Security Options Security Type None.

Description No wireless security. Recommended only for troubleshooting wireless connectivity. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public. Wired Equivalent Privacy (WEP) data encryption provides moderate data security. WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools. For more information, see "Configuring WEP Wireless Security" on page 2-9. WEP. Wired Equivalent Privacy. Wi-Fi Protected Access with Pre-Shared Key (WPAPSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively WPA2-PSK (AES). Wi-Fi Protected Access version 2 blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters with Pre-Shared Key; WPA2-PSK standard and devices might not support them. encryption with the AES encryption type. For more information, see "Configuring WPA-PSK WPA-PSK (TKIP) + WPA2-PSK (AES). Mixed mode. and WPA2-PSK Wireless Security" on page 2-10.

WPA-PSK (TKIP). WPA-PSK standard encryption with TKIP encryption type. Safeguarding Your Network v1.0, January 2010 2-3 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Table 2-2. Other Features That Enhance Security Security Type Disable the wireless router radio.

Description If you disable the wireless router radio, wireless devices cannot communicate with the router at all. You might disable this when you are away or when other users of your network all use wired connections. For more information, see "Viewing Advanced Wireless Settings" on page 2-12. If you disable the broadcast of the SSID, only devices that know the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but your data is still fully exposed to an intruder using available wireless eavesdropping tools. For more information, see "Viewing Advanced Wireless Settings" on page 2-12. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WNR2000v2 router. MAC address filtering adds an obstacle against unwanted access to your network by the general public, but the data broadcast over the wireless link is fully exposed. This data includes your trusted MAC addresses, which can be read and impersonated by a hacker. For more information, see "Restricting Wireless Access by MAC Address" on page 2-19.

By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules. For more information, see "Understanding Your Firewall" on page 2-23. Wi-Fi Protected Setup provides easy setup by means of a push button. Older wireless adapters and devices might not support this. Check whether devices are WPS enabled. For more information, see "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13. Turn off the broadcast of the wireless network name SSID. Restrict access based on MAC address. Modify your firewall's rules.

Use the Push 'N' Connect feature (Wi-Fi Protected Setup). Safeguarding Your Network v1.0, January 2010 2-4 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Recording Basic Wireless Settings Setup Information Before and after customizing your wireless settings, print this section, and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network can provide this information. Otherwise, you must choose the settings for your wireless network.

Either way, record the settings for your wireless network in the spaces provided. · Wireless Network Name (SSID). _____ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID is casesensitive.

The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID. If WEP Authentication is used, circle one: Open System, Shared Key, or Auto. Note: If you select Shared Key, the other devices in the network will not connect unless they are also set to Shared Key and are configured with the correct key. WEP Encryption Key Size. Choose one: 64-bit or 128-bit. Again, the encryption key size must be the same for the wireless adapters and the wireless router. Data Encryption (WEP) Keys. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces provided.

· Passphrase Method. _____ These characters are case-sensitive. Enter a word or group of printable characters and click Generate. Not all wireless devices support the passphrase method. · Manual Method. These values are not case-sensitive. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 09, af, or AF). For 128-bit WEP, enter 26 hexadecimal digits. Key 1: _____ Key 2: _____ Key 3: _____ Key 4: _____ · If WPA-PSK or WPA2-PSK authentication is used: · Safeguarding Your Network v1.0, January 2010 2-5 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Passphrase.

_____ These characters are case-sensitive. Enter a word or group of printable characters.

When you use WPA-PSK, the other devices in the network will not connect unless they are also set to WPA-PSK and are configured with the correct passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are also set to WPA2-PSK and are configured with the correct passphrase. Use the procedures described in the following sections to specify the WNR2000v2 router.

Store this information in a safe place. Changing Wireless Security Settings This section describes the wireless settings that you can view and configure in the Wireless Settings screen, which you access under Setup in the main menu. Viewing Basic Wireless Settings To specify the wireless security settings of your router: 1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2. Safeguarding Your Network v1.

0, January 2010 2-6 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 2. Select Wireless Settings under Setup in the main menu. The Wireless Settings screen displays. Figure 2-2 The available settings in this screen are: · Name (SSID). The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. When more than one wireless network is active, different wireless network names provide a way to separate the traffic. For a wireless device to participate in a particular wireless network, it must be configured with the SSID for that network. The WNR2000v2 default SSID is NETGEAR. You can disable this broadcast as described in "Viewing Advanced Wireless Settings" on page 2-12.

Region. This field identifies the region where the WNR2000v2 router can be used. It might not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field. · Note: The region selection feature might not be available in all countries. Safeguarding Your Network v1.0, January 2010 2-7 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual · Channel. This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless network. The wireless router uses channel bonding technology to extend the bandwidth for data transmission. For more information about the wireless channel frequencies, see the online document that you can access from "Wireless Networking Basics" in Appendix B.

Mode. This field determines which data communications protocol is used. You can choose from: Up To 54 Mbps. Legacy mode, for compatibility with the slower 802.11b and 802.

11g wireless devices. Up To 145 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 802.11b and 802.

11g wireless devices. This is the default mode. Up To 300 Mbps. Performance mode, using channel expansion to achieve the 300 Mbps data rate. The WNR2000v2 router will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or 4) to achieve a 40 MHz frame-by-frame bandwidth. The WNR2000v2 router will detect channel usage and will disable frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients. Note: The maximum wireless signal rate is derived from the IEEE Standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

· · Security Options. The selection of wireless security options can significantly affect your network performance. The time it takes to establish a wireless connection can vary depending on both your security settings and router placement. WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK, and WPA2PSK encryption can consume more battery power on a notebook computer, and can cause significant performance degradation with a slow computer. Instructions for configuring the security options can be found in "Choosing Appropriate Wireless Security" on page 2-1. A full explanation of wireless security standards is available in the online document that you can access from "Wireless Networking Basics" in Appendix B. 3. Click Apply to save your settings. Safeguarding Your Network v1.

0, January 2010 2-8 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Configuring WEP Wireless Security WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools. WEP offers the following options: · Automatic. With the Automatic option, the router will try both Open System and Shared Key authentication. Normally this setting is suitable. If it fails, select Open System or Shared Key.

You can also refer to your wireless adapter's documentation to see what method to use. Open System. With Open System authentication and 64 or 128 bit WEP data encryption, the WNR2000v2 router does perform data encryption but does not perform any authentication. Anyone can join the network. This setting provides very little practical wireless security.

Shared Key. With Shared Key authentication, a wireless device must know the WEP key to join the network. Select the encryption strength (64 or 128 bit data encryption). Manually enter the key values, or enter a word or group of printable characters in the Passphrase field. Manually entered keys are not case-sensitive, but passphrase characters are case-sensitive. · · To configure WEP data encryption: Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired computer to make any further changes. Not all wireless adapter configuration utilities support passphrase key generation. 1. Select Wireless Settings under Setup in the main menu.

2. In the Security Options section, select WEP. The WEP options display. Safeguarding Your Network v1.0, January 2010 2-9 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual . Figure 2-3 3. Select the authentication type and encryption strength. 4. 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.

· Automatic. In the Passphrase field, enter a word or group of printable characters, and click Generate. The passphrase is case-sensitive. For example, NETGEAR is not the same as nETgear. The four key fields are automatically populated with key values.

Manual. Enter 10 hexadecimal digits (any combination of 09, af, or AF).

These entries are not case-sensitive. For example, AA is the same as aa. Select which of the four keys to activate.
· 5. Click Apply to save your settings. Configuring WPA-PSK and WPA2-PSK Wireless Security Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them. Check whether newer drivers are available from the manufacturer. Also, you might be able to use the Push 'N' Connect feature to configure this type of security if it is supported by your wireless clients. See "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13. Safeguarding Your Network v1.0, January 2010 2-10 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual WPAPre-Shared Key does perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption.

Both methods dynamically change the encryption keys making them nearly impossible to circumvent. Mixed mode allows clients using either WPA-PSK (TKIP) or WPA2-PSK (AES). This provides the most reliable security, and is easiest to implement, but it might not be compatible with older adapters. Note: Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (personal digital assistants) for WPA-PSK security, consult the documentation for the product you are using. To configure WPA-PSK, WPA2-PSK, or WPA-PSK+WPA2-PSK: 1. Select Wireless Settings under Setup in the main menu.
The Wireless Settings screen displays. 2. Select one of the WPA-PSK or WPA2-PSK options for the security type. The third option (WPA-PSK [TKIP] + WP2-PSK [AES]) is the most flexible, since it allows clients using either WPA-PSK or WPA2-PSK. 3.
In the Passphrase field, enter a word or group of 863 printable characters. The passphrase is case-sensitive. Figure 2-4 Safeguarding Your Network v1.0, January 2010 2-11 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 4. Click Apply to save your settings.
Viewing Advanced Wireless Settings This section describes the wireless settings that you can view and specify in the Advanced Wireless Settings screen, which you access under Advanced in the main menu. To configure the advanced wireless security settings of your router: 1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2. 2. Select Wireless Settings under Advanced in the main menu. The advanced Wireless Settings screen displays Figure 2-5 The available settings in this screen are: · Enable Wireless Router Radio. If you disable the wireless router radio, wireless devices cannot connect to the WNR2000v2 router. If you will not be using your wireless network for a period of time, you can clear this check box and disable all wireless connectivity. Enable SSID Broadcast. 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. 2-12 v1.0, January 2010 · Safeguarding Your Network NETGEAR Wireless-N 300 Router WNR2000v2 User Manual · Enable WMM. Clear this check box to disable WMM. WMM (Wireless Multimedia), a subset of the 802.11e standard, allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM. Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode. The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only.
Do not change these settings. WPS Settings. For information about these settings, see the section, "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13. Wireless Card Access List. For information about this list, see "Restricting Wireless Access by MAC Address" on page 2-19.
· · · . Using Push 'N' Connect (Wi-Fi Protected Setup) If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the router's network name (SSID) and security settings and, at the same time, connect a wireless client securely and easily to the router. Look for the symbol on your client device. WPS automatically configures the network name (SSID) and wireless security settings for the router (if the 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.
wi-fi.org). All other Wi-Ficertified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect. When you add wireless clients, whether or not they are WPS enabled, the added devices must share the same network name (SSID) and security passphrase. For more information, see "Connecting Additional Wireless Client Devices after WPS Setup" on page 2-18. Note: If you choose to use WPS, the only security methods supported are WPA-PSK and WPA2-PSK. WEP security is not supported by WPS. The WNR2000v2 router provides two methods for connecting to a wireless client that supports WPS, described in the following sections: Safeguarding Your Network v1.0, January 2010 2-13 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual · · "Push Button Configuration"" "Security PIN Entry" on page 2-15 Push Button Configuration There are two methods to enable a wireless client to join a network using a push button on the router: using the physical push button or using the software button in the Add WPS Client screen. Using the Physical Push Button 1.

Press the button on the WNR2000v2 router for over 5 seconds. For information about the WPS button light, see the NETGEAR Wireless Router Setup Manual. The green button light begins to blink in a regular pattern. While the light is blinking, you have 2 minutes to enable WPS on the client that you are trying to connect to the router. 2. On the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router. The WNR2000v2 router's green these conditions occurs: · · button light ceases blinking and remains on when one of The router and the client establish a wireless connection. The 2-minute window period expires for establishing a WPS connection.

If the connection is not established, no WPS security settings will be specified in the WNR2000v2 router. Using the Software Button in the Add WPS Client Screen 1.

Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2. 2. Select Add WPS Client in the main menu, and click Next. 3. Select the Push Button setup method.

Figure 2-6 Safeguarding Your Network v1.0, January 2010 2-14 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 4. Click the button in the Add WPS Client screen. The Connecting to New Wireless Client screen displays. Figure 2-7 The green button light on the WNR2000v2 router begins to blink in a regular pattern.

While the button light is blinking, you have 2 minutes to enable WPS on the device you are trying to connect to the router. 5. In the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router. The WNR2000v2 router's green these conditions occurs: · · button light ceases blinking and remains on when one of The router and the client establish a wireless connection. The 2-minute window period expires for establishing a WPS connection. If the connection is not established, no WPS security settings will be specified in the WNR2000v2 router. Security PIN Entry There are two ways to enable a wireless client to join a network using a PIN: using the router's security PIN or using the wireless client's security PIN. Using the Router's Security PIN 1. Obtain your router's security PIN from the rear panel of the router or from the Advanced Wireless Settings screen. 2.

On the wireless client, follow its specific networking instructions to enter the router's security PIN and to establish a wireless connection with the router. Using the Wireless Client's Security PIN 1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2. Safeguarding Your Network v1.0, January 2010 2-15 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 2. Select Add WPS Client in the main menu, and click Next. 3. Select the PIN Number setup method. Figure 2-8 4. On the wireless client, obtain its security PIN, or follow its specific networking instructions to generate a client security PIN.

5. In the Add WPS Client screen of the WNR2000v2 router, enter the client security PIN in the Enter Client's PIN field. 6. Click Next. The following screen displays, and the Smart Wizard initiates the wireless connection: Figure 2-9 Safeguarding Your Network v1.

0, January 2010 2-16 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Configuring the WPS Settings 1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2. 2. Select Wireless Settings under Advanced in the main menu. Figure 2-10 These options are available under WPS Settings: · · Router's PIN.

The PIN is displayed so that you can use it to configure the router through WPS (Wi-Fi Protected Setup). It is also displayed on the router's label. Disable Router's PIN. If the router's PIN is disabled, you cannot configure the router's wireless settings with WPS. However, if your settings are already configured, you can still add WPS-enabled wireless clients. The router might disable the PIN if it detects suspicious attempts to break into your wireless settings; this can happen if the check box is selected. You can enable the PIN by clearing the check box and clicking Apply. Keep Existing Wireless Settings. This check box is automatically selected after WPS is enabled to prevent unwanted settings changes, and is also selected if you have already specified wireless security settings or your SSID without using WPS. When this check box is not selected, adding a new wireless client using the push button or the Add WPS Client screen (see "Push Button Configuration" on page 2-14) changes the router's SSID and security passphrase.

You might need to clear it if you are using certain registrars, such as for a Windows Vista PC, to configure the router through WPS. · Safeguarding Your Network v1.0, January 2010 2-17 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual Connecting Additional Wireless Client Devices after WPS Setup You can add WPS-enabled and non-WPS-enabled client devices. Adding Additional WPS-Enabled Clients To add an additional wireless client device that is WPS enabled: Note: Your wireless settings do not change when you add an additional WPS-enabled client unless you have cleared the Keep Existing Wireless Settings check box (in the Wireless Settings screen). If you do clear the check box, a new SSID and a passphrase are generated, and all existing connected wireless clients are disassociated and disconnected from the router. 1. Follow the procedures in "Push Button Configuration" on page 2-14 or "Security PIN Entry" on page 2-15. 2. For information about how to view a list of all devices connected to your router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 6-7. Adding Additional Non-WPS-Enabled Clients If you are connecting a combination of WPS-enabled clients and clients that are not WPS enabled, you cannot use the WPS setup procedures to add clients that are not WPS enabled.

To connect both non-WPS-enabled and WPS-enabled clients to the WNR2000v2 router: 1. Configure the settings of the WNR2000v2 router (shown in the Wireless Settings screen) for WPA-PSK or WPA2-PSK security, and record that information. See "Configuring WPA-PSK and WPA2-PSK Wireless Security" on page 2-10. When you change security settings, all existing connected wireless clients that do not share those settings are disassociated and disconnected from the router. 2.

For the non-WPS-enabled devices that you wish to connect, open the networking utility, and follow the utility's instructions to enter security settings. 3. For the WPS-enabled devices that you wish to connect, follow the procedures in "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13. The WNR2000v2 router automatically preserves the settings you configured in step 1 so all clients share the same security settings (for more information, see "Configuring the WPS Settings" on page 2-17). Safeguarding Your Network v1.

0, January 2010 2-18 NETGEAR Wireless-N 300 Router WNR2000v2 User Manual 4. For information about how to view a list of all devices connected to your router (including wireless and Ethernet connected), see "Viewing a List of Attached Devices" on page 6-7. Restricting Wireless Access by MAC Address When a Wireless Card Access List is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computers list. The Wireless Card Access List displays a list of wireless computers that you allow to connect to the router based on their MAC addresses.