N150 Wireless Router
WNR1000 User Manual

NETGEAR

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

202-10490-01
January 2009
v1.0

Manual abstract:

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 N150 Wireless Router WNR1000 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 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. 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. ii v1. 0, January 2009 Europe â 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: â¢ â¢ 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. 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 â¢ 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: â¢ 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.], declares that this [WNR1000] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. 0, January 2009 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: â¢ â¢ â¢ â¢ 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 N150 Wireless Router WNR1000 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: v v1.

0, January 2009 â□¢ â□¢ 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 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 methods: â□¢ â□¢ â□¢ â□¢ 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. N150 Wireless Router WNR1000 Tested to Comply with FCC Standards FOR HOME OR OFFICE USE Modifications made to the product, unless expressly approved by NETGEAR, Inc. , 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.

6-7 Checking for New Firmware in the Router Upgrade Screen . 7-9 Testing the Path from Your Computer to a Remote Device . 0, January 2009 Contents About This Manual The user manual provides information for configuring the features of the NETGEARÂ® N150 Wireless Router WNR1000 beyond initial configuration settings. Initial configuration instructions can be found in the NETGEAR N150 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: â□¢ 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 â□¢ 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 N150 Wireless Router according to these specifications: Product Version Manual Publication Date N150 Wireless Router WNR1000 January 2009 For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR website in Appendix B, â□□Related Documents. Â□□ Note: Product updates are available on the NETGEAR, Inc. How to Use This Manual The HTML version of this manual includes the following: â□¢ â□¢ Buttons, at a time. And , for browsing forward or backward through the manual one page A button that displays the table of contents and an button that displays an index. Double-click a link in the table of contents or index to navigate directly to where the topic is described in the manual.

Online knowledge base for the product â□¢ â□¢ Links to PDF versions of the full manual and individual chapters. How to Print This Manual To print this manual, you can choose one of the following options, according to your needs. â□¢ â□¢ Printing a page from HTML. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

printing from PDF. Your computer must have the free Adobe Acrobat Reader installed for you to view and print PDF files. The Acrobat Reader is available on the Adobe website at http://www. Use the PDF of This Chapter link at the top left of any page. N150 Wireless Router WNR1000 User Manual â□¢ Click the PDF of This Chapter link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window. Click the print icon in the upper left of your browser window. â□¢ â□□ Printing a PDF version of the complete manual. Use the Complete PDF Manual link at the top left of any page. Â□¢ â□¢ Click the Complete PDF Manual link at the top left of any page in the manual.

The PDF version of the complete manual opens in a browser window. Click the print icon in the upper left of your browser window. 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 anIf 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. If you do not click Logout, the wireless router will wait for 5 minutes after no activity before it automatically logs you out. 1-4 v1. 0, January 2009 Configuring Basic Connectivity N150 Wireless Router WNR1000 User Manual Configuring Your Internet Settings Using the Setup Wizard You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Setup Wizard to determine your Internet Service Provider (ISP) configuration. The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. To use the Setup Wizard to assist with configuration or to verify the Internet connection settings: 1.

Select Setup Wizard from the top of the main menu. 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, â□□Troubleshooting. Â□□ Viewing and Configuring Basic Internet 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. configuring Basic Connectivity v1. 0, January 2009 1-5 N150 Wireless Router WNR1000 User Manual Your Internet Connection Does Not Require a Login If no login is required by your ISP, the following settings appear in the Basic Settings screen.

no login required Figure 1-5 â□¢ â□¢ 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. Â□□ If your ISP assigns an IP address dynamically (by DHCP), select Get Dynamically From ISP. 1-6 v1. 0, January 2009 Configuring Basic Connectivity N150 Wireless Router WNR1000 User Manual â□□ â□¢ 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 ISPâ□□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 ISPâ□□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. â□¢ 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 â□□cloningâ□□ or â□□spoofingâ□□ its MAC address. To change the MAC address, select one of the following methods: â□□ 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.

0, January 2009 1-7 N150 Wireless Router WNR1000 User Manual Your Internet Connection Does Require a Login If a login is required by your ISP, the following settings appear in the Basic Settings screen: Login required Figure 1-6 â□¢ 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 ISPâ□□s login program on your computer to access the Internet. When you start an Internet application, your router will automatically log you in. This drop-down list contains a few ISPs that need special protocols for connection.

Not all ISPs are listed here. The ones on this list have special requirements. The list includes: Figure 1-7 â□□ â□□ PPTP (Point to Point Tunneling Protocol), used primarily in Austrian DSL services 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. Â□¢ Other, which selects PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide. 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. â□□ â□□ â□□ 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. the list includes: Figure 1-8 â□¢ Always On. The router logs in to the Internet immediately after booting and never disconnects. 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. â□¢ 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 ISPâ□□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 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. 1. Select Wireless Settings under Setup in the main menu of the WNR1000 router. As appropriate, select the region in which the wireless interface will operate. Note: In North America, you will not be able to change the region setting.

3. 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. Also, the SSID of any wireless access adapters must match the SSID you specify in the N150 Wireless Router. If they do not match, you will not get a wireless connection to the N150 Wireless Router. 4. For the remaining settings, accept the defaults . â□¢ The default channel is Auto. 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 â□□Wireless Networking Basicsâ□□ in Appendix B. the default mode of Up to 150Mbps. The options are: â□□ Up to 54 Mbps - Legacy Mode with maximum speed of up to 54 Mbps for b/g networks. Â□□ Up to 65 Mbps - Neighbor Friendly Mode - Default speed up to 65 Mbps which will not interfere with neighboring wireless networks. Note: If you are configuring the router from a wireless computer and you change the routerâ□□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 routerâ□□s new settings. Select Wireless Settings under Advanced in the main menu of the WNR1000 router. figure 1-10 7. Make sure that the Enable Wireless Router Radio, Enable SSID Broadcast, and Enable WMM check boxes are selected. Make sure that the Turn Access Control On check box is not selected.

10. 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. 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, â□□Safeguarding Your Network â□□).

1-12 v1. 0, January 2009 Configuring Basic Connectivity Chapter 2 Safeguarding Your Network The N150 Wireless Router WNR1000 provides highly effective security features, which are covered in detail in this chapter. This chapter includes the following sections: â□¢ â□□Choosing Appropriate Wireless Securityâ□□ â□¢ â□□Recording Basic Wireless Settings Setup Informationâ□□ on page 2-5 â□¢ â□□Changing Wireless Security Settingsâ□□ on page 2-6 â□¢ â□□Viewing Advanced Wireless Settingsâ□□ on page 2-11 â□¢ â□□Using Push 'N' Connect (Wi-Fi Protected Setup)â□□ on page 2-12 â□¢ â□□Restricting Wireless Access by MAC Addressâ□□ on page 2-18 â□¢ â□□Changing the Administrator Passwordâ□□ on page 2-20 â□¢ â□□Backing Up Your Configurationâ□□ on page 2-21 â□¢ â□□Understanding Your Firewallâ□□ on page 2-21 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 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. 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. 2-1 v1. 0, January 2009 N150 Wireless Router WNR1000 User Manual 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 â□□Changing the Administrator Passwordâ□□ on page 2-20. Wireless data security options Range: up to 300 foot radius 1) Open system: easy but no security 2) MAC access list: no data security WNR1000 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: â□¢ Manually specify your SSID and your wireless security settings. The N150 Wireless Router provides two screens for configuring the wireless settings: â□□ â□□ Wireless Settings. You access these under Setup in the main menu (see â□□Viewing Basic Wireless Settingsâ□□ on page 2-6). advanced Wireless Settings. You access these under Advanced in the main menu (see â□□Viewing Advanced Wireless Settingsâ□□ on page 2-11). 2-2 v1.

0, January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 User Manual â□¢ 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 â□□Using Push 'N' Connect (Wi-Fi Protected Setup)â□□ on page 2-12). 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 â□□Wireless Networking Basicsâ□□ in Appendix B.

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 â□□Configuring WEP Wireless Securityâ□□ on page 2-8. 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 with Pre-Shared Key; WPA2-PSK standard are relatively new standards, older wireless adapters encryption with the AES encryption type. and devices might not support them. For more information, see â□□Configuring WPA-PSK WPA-PSK (TKIP) + WPA2-PSK (AES). 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 â□□Viewing Advanced Wireless Settingsâ□□ on page 2-11. 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 â□□Viewing Advanced Wireless Settingsâ□□ on page 2-11. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the N150 Wireless 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 â□□Restricting Wireless Access by MAC Addressâ□□ on page 2-18. 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 firewallâ□□s rules. For more information, see â□□Understanding Your Firewallâ□□ on page 2-21. 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 â□□Using Push 'N' Connect (Wi-Fi Protected Setup)â□□ on page 2-12. Turn off the broadcast of the wireless network name SSID. 0, January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 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. 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 â□□wireless network nameâ□□ 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. 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. Enter a word or group of printable characters and click Generate. Not all wireless devices support the passphrase method. â□¢ Manual Method.

These values are not case-sensitive. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0â□□9, aâ□□f, or Aâ□□F). For 128-bit WEP, enter 26 hexadecimal digits. 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 N150 Wireless 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.

Figure 2-2 The available settings in this screen are: 2-6 v1. 0 , January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 User Manual â□¢ 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 WNR1000 default SSID is NETGEAR. You can disable this broadcast as described in â□□Viewing Advanced Wireless Settingsâ□□ on page 2-11. region. This field identifies the region where the N150 Wireless 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. 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 â□□Wireless Networking Basicsâ□□ in Appendix B. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. The Mode options are: â□□ â□□ â□□ Up to 54 Mbps - Legacy Mode with maximum speed of up to 54 Mbps for b/g networks. Up to 65 Mbps - Neighbor Friendly Mode - Will not interfere with neighboring wireless networks. up to 150 Mbps - Performance Mode - Maximum Nx speeds up to 150 Mbps. Using channel expansion to achieve the 150 Mbps data rate, the WNR1000 will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or â□□4) to achieve a 40 MHz frame-by-frame bandwidth.

The WNR1000 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. 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 â□□Choosing Appropriate Wireless Securityâ□□ on page 2-1. A full explanation of wireless security standards is available in the online document that you can access from â□□Wireless Networking Basicsâ□□ in Appendix B. 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: â□¢ Automatic. With the Automatic option, the router will try both Open System and Shared Key authentication.

You can also refer to your wireless adapterâ□□s documentation to see what method to use. open System. With Open System authentication and 64 or 128 bit WEP data encryption, the N150 Wireless 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.

Â□¢ â□¢ 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. 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. â□¢ 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. These entries are not case-sensitive. For example, AA is the same as aa. Select which of the four keys to activate. 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. Both methods dynamically change the encryption keys making them nearly impossible to circumvent.

This provides the most reliable security, and is easiest to implement, but it might not be compatible with older adapters. 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. 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 8â□□63 printable characters. 0, January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 User Manual 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.

The advanced Wireless Settings screen displays Figure 2-5 The available settings in this screen are: â□¢ Enable Wireless Router Radio. If you disable the wireless router radio, wireless devices cannot connect to the N150 Wireless 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. 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, â□□Using Push 'N' Connect (Wi-Fi Protected Setup)â□□ on page 2-12. wireless Card Access List. For information about this list, see â□□Restricting Wireless Access by MAC Addressâ□□ on page 2-18. â□¢ â□¢ â□¢ . 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 routerâ□□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: NETGEARâ□□s Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see http://www. 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 â□□Connecting Additional Wireless Client Devices after WPS Setupâ□□ on page 2-17. 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 N150 Wireless Router provides two methods for connecting to a wireless client that supports WPS, described in the following sections: 2-12 v1. 0, January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 User Manual â□¢ â□¢ â□□Push Button Configurationâ□□ â□□Security PIN Entryâ□□ on page 2-14 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 rear of the N150 Wireless Router for over 5 seconds. For information about the WPS light, see the NETGEAR N150 Wireless Router Setup Manual.

The green 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 N150 Wireless Routerâ□□s green these conditions occurs: â□¢ â□¢ 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 N150 Wireless Router.

Using the Software Button in the Add WPS Client Screen 1. Click the button in the Add WPS Client screen. the Connecting to New Wireless Client screen displays. Figure 2-7 The green light on the N150 Wireless 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 N150 Wireless Routerâ□□s green these conditions occurs: â□¢ â□¢ 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 N150 Wireless Router.

Security PIN Entry There are two ways to enable a wireless client to join a network using a PIN: using the routerâ□□s security PIN or using the wireless clientâ□□s security PIN. using the Routerâ□□s Security PIN 1. Obtain your routerâ□□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 routerâ□□s security PIN and to establish a wireless connection with the router.

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 N150 Wireless Router, enter the client security PIN in the Enter Clientâ□□s PIN field. The following screen displays, and the Smart Wizard initiates the wireless connection: Figure 2-9 Safeguarding Your Network v1. Figure 2-10 These options are available under WPS Settings: â□¢ â□¢ Routerâ□□s PIN. The PIN is displayed so that you can use it to configure the router through WPS (Wi-Fi Protected Setup). If the routerâ□□s PIN is disabled, you cannot configure the routerâ□□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 â□□Push Button Configurationâ□□ on page 2-13) changes the routerâ□□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. â□¢ 2-16 v1.

0, January 2009 Safeguarding Your Network N150 Wireless Router WNR1000 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. For information about how to view a list of all devices connected to your router (including wireless and Ethernet-connected), see â□□Viewing a List of Attached Devicesâ□□ on page 6-5. 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 N150 Wireless Router: 1. Configure the settings of the N150 Wireless Router (shown in the Wireless Settings screen) for WPA-PSK or WPA2-PSK security, and record that information. see â□□Configuring WPA-PSK and WPA2-PSK Wireless Securityâ□□ on page 2-9. 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 utilityâ□□s instructions to enter security settings. 3. For the WPS-enabled devices that you wish to connect, follow the procedures in â□□Using Push 'N' Connect (Wi-Fi Protected Setup)â□□ on page 2-12. The N150 Wireless Router automatically preserves the settings you configured in step 1 so all clients share the same security settings (for more information, see â□□Configuring the WPS Settingsâ□□ on page 2-16). For information about how to view a list of all devices connected to your router (including wireless and Ethernet connected), see â□□Viewing a List of Attached Devicesâ□□ on page 6-5.

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. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router. The MAC address is a network deviceâ□□s unique 12-character physical address, containing the hexadecimal characters 0â□□9, aâ□□f, or Aâ□□F only, and separated by colons (for example, 00:09:AB:CD:EF:01). It can usually be found on the bottom of the wireless card or network interface device.

If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer.

In WindowsXP, for example, typing the ipconfig/all command in an MSDOS command prompt window displays the MAC address as Physical Address. You might also find the MAC addresses in the routerâ□□s Attached Devices screen. In the Advanced Wireless Settings screen, click Setup Access List to display the Wireless Card Access List. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses. If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device. Tip: You can copy and paste the MAC addresses from the routerâ□□s Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices screen.

5. Click Add to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen. 6. Repeat step 3 through step 5 for each additional device you want to add to the list. Note: When configuring the router from a wireless computer whose MAC address is not in the Trusted PC list, if you select Turn Access Control On, you 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. 0, January 2009 2-19 N150 Wireless Router WNR1000 User Manual Now, only devices on this list can wirelessly connect to the N150 Wireless Router. Warning: MAC address filtering adds an obstacle against unwanted access to your network by the general public. However, because your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them.

Do not rely on MAC address filtering alone to secure your network. Changing the Administrator Password The default password for the routerâ□□s Web Configuration Manager is password. NETGEAR recommends that you change this password to a more secure password. Tip: Before changing the router password, back up your configuration settings with the default password of password. If you save the settings with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults, and log in using the default password of password.

This means you will have to re-enter all the router configuration settings. For information about how to back up your settings, see â□□Backing Up and Restoring the Configurationâ□□ on page 6-6. to change the administrator password: 1. On the main menu, under Maintenance, select Set Password to display the Set Password screen. To change the password, first enter the old password, then enter the new password twice.

Backing Up Your Configuration The configuration settings of the N150 Wireless Router are stored within the router in a configuration file. You can back up (save) this file and retrieve it later. NETGEAR recommends that you save your configuration file after you complete the configuration. If the router fails or becomes corrupted, or an administrator password is lost, you can easily re-create your configuration by restoring the configuration file. For instructions on saving and restoring your configuration file, see â□□Managing the Configuration Fileâ□□ on page 6-6. Tip: Before saving your configuration file, change the administrator password to the default, password. Then change it again after you have saved the configuration file. If you save the file with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults and log in using the default password of password. This means you will have to re-enter all the router configuration settings. Understanding Your Firewall Your N150 Wireless Router WNR1000 contains a true firewall to protect your network from attacks and intrusions.

A firewall is a device that protects one network from another while allowing communication between the two. Using a process called Stateful Packet Inspection, the firewall analyzes all inbound and outbound traffic to determine whether or not it will be allowed to pass through. 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 firewallâ□□s rules to achieve the following behavior: â□¢ Blocking sites. Block access from your network to certain Web locations based on Web addresses and Web address keywords. Block the use of certain Internet services by specific computers on your network. Block sites and services according to a daily schedule. this feature is described in â□□Scheduling Blockingâ□□ on page 3-5. Allow inbound access to your server. To allow inbound access to resources on your local network (for example, a Web server or remote desktop program), you can open the needed services by configuring port forwarding as described in â□□Allowing Inbound Connections to Your Networkâ□□ on page 5-1.

Allow certain games and applications to function correctly. Some games and applications need to allow additional inbound traffic in order to function. Port triggering can dynamically allow additional service connections, as described in â□□Configuring Port Triggeringâ□□ on page 5-9. Another feature to solve application conflicts with the firewall is Universal Plug and Play (UPnP), described in â□□Using Universal Plug and Playâ□□ on page 5-12. â□¢ 2-22 v1. 0, January 2009 Safeguarding Your Network Chapter 3 Restricting Access From Your Network This chapter describes how to use the content filtering and reporting features of the N150 Wireless Router WNR1000 to protect your network. This chapter includes the following sections: â□¢ â□□Content Filtering Overviewâ□□ â□¢ â□□Blocking Access to Internet Sitesâ□□ â□¢ â□□Blocking Access to Internet Servicesâ□□ on page 3-3 â□¢ â□□Scheduling Blockingâ□□ on page 3-5 â□¢ â□□Viewing Logs of Web Access or Attempted Web Accessâ□□ on page 3-6 â□¢ â□□Configuring E-mail Alert and Web Access Log Notificationsâ□□ on page 3-7 â□¢ â□□Setting the Time Zoneâ□□ on page 3-8 Content Filtering Overview The N150 Wireless Router WNR1000 provides you with Web content filtering options, plus browser activity reporting and instant alerts through e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses, and Web address keywords.

You can also block Internet access by applications and services, such as chat rooms or games. Blocking Access to Internet Sites The N150 Wireless 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: â□¢ â□¢ 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. For information about scheduling, see â□□Scheduling Blockingâ□□ on page 3-5. 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 computerâ□□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. 3-2 v1. 0, January 2009 Restricting Access From Your Network N150 Wireless Router WNR1000 User Manual Blocking Access to Internet Services The N150 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 playersâ□□ 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. To block by schedule, be sure to specify a time period in the Schedule screen.
For information about scheduling, see â□□Scheduling Blockingâ□□ on page 3-5. 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. 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, â□□Assigned Numbers. Â□□ 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. â□□ â□□ 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. 5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields. 0, January 2009 Restricting Access From Your Network N150 Wireless Router WNR1000 User Manual Blocking Services by IP Address Range In the Filter Services For area, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking The N150 Wireless Router allows you to specify when blocking is enforced. 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 â□□Setting the Time Zoneâ□□ on page 3-8. 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 128 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. Figure 3-5 Table 3-1 describes the log entries. table 3-1.
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. 0, January 2009 Restricting Access From Your Network N150 Wireless Router WNR1000 User Manual 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. 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. a. Enter the name of your ISPâ□□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. If your e-mail server requires authentication, select the My Mail Server requires authentication check box. a. Enter your user name for the e-mail server in the User Name field. b.

Enter your password for the e-mail server in the Password field. 4. You can specify that logs are automatically sent by e-mail with these options: â□¢ â□¢ 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. â□□ â□□ 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.