Manual abstract:

@@@@@Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders. Statement of Conditions To improve 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. Revision History Publication Part Number 202-10614-01 Version v1.0 Publish Date July 2010 Comments 2\ Table of Contents Chapter 1 Configuring Your Internet Connection Logging In to Your Wireless Router. . . . .

. . . . .

. . . . .

. . . . . .

. . . . . Selecting a Language for Your Screen Display . . . .

. . . . .

. . . . .

. . . . . Using the Setup Wizard . .

. . . . . .

. . . . .

. . . . .

. . . . . .

. . . . . Viewing or Manually Configuring Your ISP Settings . .

. . . . .

. . . . .

. . . . . 7 8 9 9 Chapter 2 Wireless Configuration Planning Your Wireless Network . . . .

. . . . . .

. . . . .

. . . . .

. . . . . Wireless Placement and Range Guidelines . .

. . . . . .

. . . . .

. . . . Wireless Security Options .

. . . . . .

. . . . . .

. . . . .

. . . . .

. . . . Manually Configuring Your Wireless Settings . . . . . .

. . . . . .

. . . . .

. Configuring WEP . . . .

. . . . . .

. . . . . .

. . . . .

. . . . .

. . . . . Configuring WPA, WPA2, or WPA + WPA2 . .

. . . . . .

. . . . .

. . . . Using Push 'N' Connect (WPS) to Configure Your Wireless Network .

. . . WPS Button . . . . . .

. . . . . .

. . . . .

. . . . .

. . . . . .

. . . . . WPS PIN Entry .

. . . . .

. . . . .

. . . . . .

. . . . . .

This chapter includes: · · · · Logging In to Your Wireless Router on page 7 Selecting a Language for Your Screen Display on page 8 Using the Setup Wizard on page 9 Viewing or Manually Configuring Your ISP Settings on page 9 Chapter 1: Configuring Your Internet Connection | 6 Wireless-N 150 Router WNR612v2 User Manual Logging In to Your Wireless Router You can log in to the wireless router to view or change its settings, and to access the Knowledge Base and documentation. To log in to the wireless router: 1.

If you have not set up wireless connections yet, connect your computer to the wireless router with an Ethernet cable. 2. In the address field of your Internet browser, enter http://www.routerlogin.com. or http://www.routerlogin.net. To connect, you can also enter the router's IP address, http://192.168. 1.1. The wireless 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. 3. Enter admin for the user name and your password (or the default, password).

For information about how to change the password, see Changing the Administrator Password on page 27. 4. The screen that displays when you log in depends on whether the wireless router has already been set up. · Firmware Upgrade Assistant: If you log in after the wireless router has been configured, this screen displays. See Upgrading the Firmware on page 44for details.

· Router Status screen: The wireless router Internet connection is not configured, or the wireless router has been reset to its factory default settings. See Viewing Wireless Router Status Information on page 47. Basic Settings screen: If there is no new firmware and your Internet connection is configured, the Basic Settings screen displays. See Viewing or Manually Configuring Your ISP Settings on page 9. · If you do not click Logout, the wireless router will wait for 5 minutes after no activity before it automatically logs you out. Chapter 1: Configuring Your Internet Connection | 7 Wireless-N 150 Router WNR612v2 User Manual Selecting a Language for Your Screen Display Using the Select Language drop-down list, located in the upper right corner of the Router Manager screen, you can change the language. The language is set to English by default. The default language is always stored in memory. When you select another language, it is stored in memory in addition to English. The additional language stored is the most recently selected.

For exampassigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's wireless router to which your wireless router will connect. Domain Name Server (DNS) Address The DNS server is used to look up site addresses based on their names. · Get Automatically from ISP. Your ISP uses DHCP to assign your DNS server address automatically. · Use These DNS Servers. If you know your ISP does not automatically transmit DNS addresses to the wireless router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. 10 | Chapter 1: Configuring Your Internet Connection Wireless-N 150 Router WNR612v2 User Manual Table 1.

Basic Settings Screen Fields (Continued) Settings This field appears only if your ISP does not require a login. Router MAC Address Description Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address. · Use Default MAC Address. This is the usual setting.

· Use Computer MAC address. If your ISP requires MAC authentication, you can use this setting to disguise the wireless router's MAC address with the computer's own MAC address. · Use This MAC Address. If your ISP requires MAC authentication, you can manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX.

Chapter 1: Configuring Your Internet Connection | 11 2. Wireless Configuration 2 This chapter describes how to configure your wireless connection. This chapter includes: · · · · · · Planning Your Wireless Network on page 13 Manually Configuring Your Wireless Settings on page 14 Using Push 'N' Connect (WPS) to Configure Your Wireless Network on page 18 Wireless Guest Networks on page 21 Advanced Wireless Settings on page 22 Restricting Wireless Access by MAC Address on page 24 For a wireless connection, the SSID, also called the wireless network name, and the wireless security settings must be the same for the wireless router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security. Note: Computers can connect wirelessly at a range of several hundred feet. If you do not use wireless security, this can allow others outside your immediate area to access your network. Chapter 2: Wireless Configuration | 12 Wireless-N 150 Router WNR612v2 User Manual Planning Your Wireless Network For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly. To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security. · To manually configure the wireless settings, you must know the following: SSID. The default SSID for the wireless router is NETGEAR.

The wireless mode (80.211n, 802.11g, or 802.11b) that each wireless adapter supports. Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports. See Manually Configuring Your Wireless Settings on page 14. · Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the wireless router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS. See Using Push 'N' Connect (WPS) to Configure Your Wireless Network on page 18.

Wireless Placement and Range Guidelines The range of your wireless connection can vary significantly based on the physical placement of the wireless router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices. For best results, place your wireless router according to the following guidelines: · · · · · · Near the center of the area in which your PCs will operate. In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls). Away from sources of interference, such as PCs, microwave ovens, and 2.

4 GHz cordless phones. Away from large metal surfaces. Put the antenna in a vertical position to provide the best side-to-side coverage.

Put the antenna in a horizontal position to provide the best up-and-down coverage. If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference.

The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11). The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer. Chapter 2: Wireless Configuration | 13 Wireless-N 150 Router WNR612v2 User Manual Wireless Security Options Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network. Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Wireless-N 150 Router WNR612v2 provides highly effective security features, which are covered in detail in this chapter.

Deploy the security features appropriate to your needs. There are several ways you can enhance the security of your wireless network: · Turn off the broadcast of the wireless network name (SSID). If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. WEP. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK. WPA-PSK (TKIP), WPA2-PSK (AES). Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys.

The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise. · · For more information about wireless technology, click the link to the online document in Wireless Networking Basics in Appendix B. Manually Configuring Your Wireless Settings Note: If you use a wireless computer to change the wireless network name (SSID) or wireless security, you will be disconnected when you click Apply. To avoid this problem, connect your computer to the router with an Ethernet cable while you are making changes. To view or manually configure the wireless settings: 1. Log in to the wireless router as described in Logging In to Your Wireless Router on page 7. 14 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual 2. Select Wireless Settings from the main menu: The settings for this screen are explained in Table 2. 3. Select the region in which the wireless router will operate.

4. For initial configuration and test, leave the other settings unchanged. 5. To save your changes, click Apply. 6. Configure and test your computers for wireless connectivity. Set up your wireless computers with the same SSID and wireless security settings as your wireless router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless router. If there is interference, adjust the channel. Table 2.

Wireless Settings Settings Region Wireless Network Enable SSID Broadcast Enable Wireless Isolation Name (SSID) Description The location where the wireless router is used. If this check box is selected, the SSID is broadcast in the selected channel. If this check box is selected, computers will not be able to connect wirelessly to the wireless router. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. When there is more than one wireless network, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID. Chapter 2: Wireless Configuration | 15 Wireless-N 150 Router WNR612v2 User Manual Table 2. Wireless Settings (Continued) Settings Wireless Network (Continued) Channel Description The wireless channel: 1 through 13.

This setting applies to any guest networks you set up. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to try different channels to see which is best. The number of available channels varies by region and depends on the selected mode. Mode The mode can be set only for the primary wireless LAN (NETGEAR).

· Up to 150 Mbps (default setting): Allows wireless stations that support speeds up to 150 Mbps. The router transmits two streams with different data concurrently on the same channel. This mode restricts channel bandwidth to minimize interference with the transmissions of other wireless networks. Up to 65 Mbps: Neighbor Friendly Mode - Will not interfere with neighboring wireless networks. Up to 54 Mbps: Allows wireless stations that support speeds up to 54 Mbps.

· · Security Options None You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See Configuring WEP on page 16. Allow only computers configured with WPA to connect to the wireless router. See the following section, Configuring WEP on page 16. Allow only computers configured with WPA2 to connect to the wireless router. See Configuring WPA, WPA2, or WPA + WPA2 on page 18. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router.

See Configuring WPA, WPA2, or WPA + WPA2 on page 18. WEP WPA-PSK (TKIP) WPA2-PSK (AES) WPA-PSK (TKIP) + WPA2-PSK (AES) Configuring WEP WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools. Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes. To configure WEP data encryption: 1. Log in to the wireless router as described in Logging In to Your Wireless Router on page 7. 16 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual 2. From the main menu, select Wireless Settings to display the Wireless Settings screen. 3. In the Security Options section, select the WEP radio button: 4. Select the Authentication Type: Automatic, or Shared Key. The default is Automatic. Note: The authentication is separate from the data encryption. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted.

Security is stronger if you use both the Shared Key and WEP encryption settings.
5. Select the Encryption Strength setting: · WEP 64-bit encryption. Enter 10 hexadecimal digits (any combination of 09, af, or AF). · WEP 128-bit encryption. Enter 26 hexadecimal digits (any combination of 09, af, or AF).
6. Enter the encryption keys. 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: · Passphrase. To use a passphrase to generate the keys, enter a passphrase, and click Generate. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the wireless router. Note: Not all wireless adapters support passphrase key generation. · Key 1Key4. These values are not case-sensitive.

You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 09, af, or AF). 7. Select which of the four keys will be the default. Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected. 8. Click Apply to save your settings.
Chapter 2: Wireless Configuration | 17 Wireless-N 150 Router WNR612v2 User Manual Configuring WPA, WPA2, or WPA + WPA2 Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later, WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings. Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. If this happens, reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes.
To configure WPA or WPA2 in the wireless router: 1. Log in to the wireless router as described in Logging In to Your Wireless Router on page 7. 2. Select Wireless Settings from the main menu. 3.
On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice. 4. The settings displayed on the screen depend on which security option you select. 5. For WPA-PSK or WPA2-PSK, enter the passphrase. 6. To save your settings, click Apply. Using Push 'N' Connect (WPS) to Configure Your Wireless Network For you to use Push 'N' Connect, your wireless computers or devices must support Wi-Fi WPS symbol on it. WPS Protected Setup (WPS). Compatible equipment usually has the can configure the network name (SSID) and set up WPA/WPA2 wireless security for the wireless router and the wireless computer or device at the same time.

Some considerations regarding WPS are: · NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect. If your wireless network will include a combination of WPS-capable devices and non-WPS-capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS-capable devices. · 18 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual You can connect to the network using WPS either with a push button or a PIN. · · Push Button. This is the preferred method. See the following section, WPS Button. Entering a PIN. See WPS PIN Entry on page 20. WPS Button Any wireless computer or wireless adapter that will connect to the wireless router wirelessly is a client.
The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart. To use the wireless router WPS button to add a WPS client: 1. Log in to the wireless router as described in Logging In to Your Wireless Router on page 7. 2. On the wireless router main menu, select Add a WPS Client, and then click Next.
By default, the Push Button (recommended) radio button is selected. 3. Either click the onscreen button or press the WPS button on the front of the wireless router. The wireless router tries to communicate with the client (the computer that wants to join the network) for 2 minutes. 4.
Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button. 5. Go back to the wireless router screen to check for a message. The wireless router WPS screen displays a message confirming that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security. The wireless router keeps these wireless settings unless you change them, or you clear the Keep Existing Wireless Settings check box in the WPS Settings screen. 6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen.

See Manually Configuring Your Wireless Settings on page 14. To access the Internet from any computer connected to your wireless router, launch an Internet browser such as Mozilla Firefox. You should see the wireless router's Internet LED blink, indicating communication to the ISP. WPS button Chapter 2: Wireless Configuration | 19 Wireless-N 150 Router WNR612v2 User Manual Note: If no WPS-capable client devices connect during the 2-minute time frame, the wireless settings do not change on the wireless router. WPS PIN Entry Any wireless computer or device that will connect to the wireless router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart. The first time you add a WPS client, make sure that the Keep Existing Wireless Settings check box on the WPS Settings screen is cleared. This is the default setting for the wireless router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless router automatically selects this check box so that your SSID and wireless security settings stay the same if other WPS devices are added later. To use a PIN to add a WPS client: 1.
Log in to the wireless router as described in Logging In to Your Wireless Router on page 7. 2. On the wireless router main menu, select Add a WPS Client (computers that will connect wirelessly to the wireless router are clients), and then click Next. The Add WPS Client screen displays: 3. Select the PIN Number radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN.

Take note of the client PIN.

5. From the wireless router Add WPS Client screen, enter the client PIN number, and click Next. · The wireless router tries to communicate with the client for 4 minutes. · The wireless router WPS screen confirms that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security. If the client is not added during the 2-minute time frame, the router wireless settings remain unchanged. · 6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See Manually Configuring Your Wireless Settings on page 14.

To access the Internet from any computer connected to your wireless router, launch an Internet browser. You should see the wireless router's Internet LED blink, indicating communication to the ISP. 20 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual Adding Wireless Computers That Do Not Support WPS If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. For information about how to view the wireless settings for the router, see Manually Configuring Your Wireless Settings on page 14. Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the wireless settings so that they are easier for you to remember. If you do that, then you will need to set up the WPS-compatible computers again. Changing wireless settings for the network: Note: Making these changes will cause all wireless computers to be disconnected from network. You will then have to set them up with the new wireless settings. 1.

Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings. 2. Log in to the router and select Wireless Settings (see Manually Configuring Your Wireless Settings on page 14). 3.

Make the following changes: · Change the wireless network name (SSID) to a meaningful name. · · On the WPA/PSK + WPA2/PSK screen, select a passphrase. Make sure that the Keep Wireless Settings check box is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS. 4. Click Apply so that your changes take effect.

Write down your settings. All wireless clients are disassociated and disconnected from the wireless router. 5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 3 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase). 6. For the WPS devices that you want to connect, follow the procedure in WPS Button on page 19 or WPS PIN Entry on page 20. The settings that you configured in Step 3 are broadcast to the WPS devices so that they can connect to the wireless router. Wireless Guest Networks A wireless guest network allows you to provide guests access to your wireless network without prior authorization of each individual guest. You can configure wireless guest networks and specify the security options for each wireless guest network. Chapter 2: Wireless Configuration | 21 Wireless-N 150 Router WNR612v2 User Manual To configure a wireless guest network: 1.

In the main menu, under Setup, select Wireless Settings. 2. Select any of the following Wireless settings: · Enable Guest Network When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile. · Enable SSID Broadcast If selected, the Wireless Access Point broadcasts its name (SSID) to all Wireless Stations. Stations can adopt the correct SSID for connections to this Access Point. Allow Guest to access MY Local Network If selected any user who connects to this SSID can access local networks associated with the router like users in the primary SSID. · 3. Give the wireless network a name. The name is case-sensitive and can be up to 32 characters. The same name must be assigned to all wireless devices in your network.

NETGEAR recommends that you change the name to a different value. 4. Select a Security option from the list. 5. Click Apply to save your selections. 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: 1. Log in to the router as described in Logging In to Your Wireless Router on page 7. 22 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual 2. Select Wireless Settings under Advanced in the main menu.

The advanced Wireless Settings screen displays: The available settings in this screen are: · Enable Wireless Router Radio. If you disable the wireless router radio, wireless devices cannot connect to the 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. Fragmentation Length, CTS/RTS Threshold, and Preamble Mode. The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings. Transmit Power Control. There are four different settings for transmit power control: 100% (the default), 75%, 50%, and 25%. WPS Settings. For information about these settings, see Using Push 'N' Connect (WPS) to Configure Your Wireless Network on page 18.

Wireless Card Access List. For information about this list, see Restricting Wireless Access by MAC Address on page 24. · · · · . Advanced WPS Settings On the Advanced Wireless Setting screen, these WPS Settings are available: · · 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 Chapter 2: Wireless Configuration | 23 Wireless-N 150 Router WNR612v2 User Manual 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 Add WPS Client screen (see Using Push 'N' Connect (WPS) to Configure Your Wireless Network on page 18) 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.

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 device's unique 12-character physical address, containing the hexadecimal characters 09, af, or AF 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 router's Attached Devices screen. To restrict access based on MAC addresses: 1. Select Wireless Settings under Advanced in the main menu. 2. In the Advanced Wireless Settings screen, click Setup Access List to display the Wireless Card Access List. 3. Click Add to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

24 | Chapter 2: Wireless Configuration Wireless-N 150 Router WNR612v2 User Manual 4. 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 router'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. 7. Select the Turn Access Control On check box. Note: If you connected wirelessly to the router, make sure your computer is on the access control list before you select Turn Access Control On, and click Apply. Otherwise, you will be disconnected and will have to use another computer that is on the access control list to log in to the router.

8. Click Apply to save your Wireless Card Access List settings. Now, only devices on this list can wirelessly connect to the wireless router. Tip: MAC address filtering adds an obstacle against unwanted access to your network, but NETGEAR recommends that you also use wireless security. Without wireless security, your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them.

Chapter 2: Wireless Configuration | 25 3. Protecting Your Network 3 This chapter describes how to use the content filtering and reporting features of the wireless router to protect your network. This chapter includes the following sections: · · · · · Blocking Access to Internet Sites on page 27 Blocking Access to Internet Services on page 28 Scheduling Blocking on page 30 Viewing Logs of Web Access or Attempted Web Access on page 30 Email Alerts and Web Access Log Notifications on page 31 Chapter 3: Protecting Your Network | 26 Wireless-N 150 Router WNR612v2 User Manual Protecting Access to Your Wireless Router For security reasons, the wireless router has its own user name and password. Also, after a period of inactivity for a set length of time, the login automatically disconnects. You can use the following procedures to change the wireless router's password and the period for the administrator's login time-out. Note: The user name and password are not the same as any other user name or password your might use to log in to your Internet connection. NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper case and lower case letters, numbers, and symbols. Your password can be up to 30 characters. Changing the Administrator Password 1.

In the main menu, under Maintenance, select Set Password. 2. To change the password, first enter the old password, and then enter the new password twice. 3. Click Apply to save your changes. Note: After changing the password, you are required to log in again to continue the configuration. If you have backed up the wireless router settings previously, you should do a new backup so that the saved settings file includes the new password. Blocking Access to Internet Sites The Wireless-N 150 Router WNR612v2 allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. Keyword application examples: · · If the keyword XXX is specified, the URL www.

zzzyyqq.com/xxx.html is blocked. If the keyword .com is specified, only websites with other domain suffixes (such as .

edu, .org, or .gov) can be viewed. Chapter 3: Protecting Your Network | 27 Wireless-N 150 Router WNR612v2 User Manual To block access to Internet sites: 1. Select Block Sites under Content Filtering in the main menu.

The Block Sites screen displays. 2. Enable keyword blocking by selecting either Per Schedule or Always. To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see Scheduling Blocking on page 30. 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.

Delete a keyword or domain name by selecting it from the list and clicking Delete Keyword. 4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the Trusted IP Address fields.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address. 5. Click Apply to save all your settings in the Block Sites screen. Blocking Access to Internet Services The wireless router allows you to block computers on your network from using Internet services that you specify. This is called service blocking or port filtering. Services are performed by server computers at the request of client computers.

For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network requests a service from a server computer on the Internet, it is identified by a service number or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet with destination port number 80 is an HTTP (Web server) request. 28 | Chapter 3: Protecting Your Network Wireless-N 150 Router WNR612v2 User Manual To block access to Internet services: 1.

Select Block Services under Content Filtering in the main menu. The Block Services screen displays. 2. In the Services Blocking section of the screen, select either the Per Schedule or Always radio button, and then click Apply. To block by schedule, be sure to specify a time period in the Schedule screen (see Scheduling Blocking on page 30.

) To add Internet services you want to block: 1. On the Block Services screen, click Add. 2. The Block Services Setup screen displays. 3. From the Service Type list, select the application or service to be allowed or blocked. 4. To add a service or application to the Service Type list, select User Defined. · Find out which port number or range of numbers the application uses (these numbers often fall within the range 1024 to 65535). You can check the Internet Engineering Task Force (IETF) RFC1700, "Assigned Numbers," or contact the publisher of the application, or user groups.

· 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. 6. Click Add to enable your Block Services Setup selections. 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. Chapter 3: Protecting Your Network | 29 Wireless-N 150 Router WNR612v2 User Manual Scheduling Blocking The wireless router allows you to specify when blocking is enforced.

To schedule blocking: 1. Select Schedule under Content Filtering in the main menu. The Schedule screen displays. 2. Configure the schedule for blocking keywords and services.

a. Days to Block. 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. Click Apply.

b. Time of Day to Block. Select a start and end time in 24-hour format. Select All Day for 24-hour blocking. Click Apply. c. Time Zone. To verify and set the time zone: · Time Zone. To select your local time zone, use the drop-down list. This setting is used for the blocking schedule and for time-stamping log entries.

· Automatically Adjust for Daylight Savings Time. If your region supports daylight savings time, select this check box. The router will automatically adjust the time at the start and end of the daylight savings time period. 3. Click Apply to save your settings. 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. 30 | Chapter 3: Protecting Your Network Wireless-N 150 Router WNR612v2 User Manual Select Logs under Content Filtering in the main menu. The Logs screen displays.

The following table describes the log entries. Field Date and time Source IP Target address Action Description The date and time the log entry was recorded. The IP address of the initiating device for this log entry. The name or IP address of the website or newsgroup visited or to which access was attempted. Whether the access was blocked or allowed.

To refresh the log screen, click the Refresh button. To clear the log entries, click the Clear Log button. To email the log immediately, click the Send Log button. Email Alerts and Web Access Log Notifications To receive logs and alerts by email, you must provide your email account information. Chapter 3: Protecting Your Network | 31 Wireless-N 150 Router WNR612v2 User Manual To configure email alert and web access log notifications: 1.

Select E-mail under Content Filtering in the main menu. The E-mail screen displays. 2. Select the Turn E-mail Notification On check box. a. Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com) in the Your Outgoing Mail Server field. You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages will not be sent by email.

b. Enter the email address to which logs and alerts are sent in the Send To This E-mail Address field. This email address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by email. 3. 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: · Send alert immediately. Select this check box for immediate notification of attempted access to a blocked site or service. · Send Logs According to this Schedule. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

Day. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily. Time. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly. If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the Wireless Router's memory. If the Wireless Router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents. 5. Click Apply to save your settings. So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time in the Scheduling screen (see Scheduling Blocking on page 30).

32 | Chapter 3: Protecting Your Network 4. Customizing Your Network 4 This chapter describes how to configure advanced networking features of the wireless router, including LAN, WAN, and routing settings.

It contains the following sections: · · · · Using the LAN IP Setup Options on page 34" Using a Dynamic DNS Service on page 37 Configuring the WAN Setup Options on page 38 Configuring Static Routes on page 41 Chapter 4: Customizing Your Network | 33 Wireless-N 150 Router WNR612v2 User Manual Using the LAN IP Setup Options The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP). To configure LAN IP settings, select LAN Setup under Advanced in the main menu. The LAN Setup screen displays. Configuring a Device Name The device name is a user-friendly name for the router. This name is shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The Device Name field cannot be blank. The default name is WNR612v2. Configuring LAN TCP/IP Setup Parameters These are advanced settings that you might configure if you are a network administrator and your network contains multiple routers. The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server (see Using the Router as a DHCP Server on page 35). Note: If you change the LAN IP address of the router while connected through the browser, you will be disconnected.

You must then open a new connection to the new IP address and log in again. The router's default LAN IP configuration is: · LAN IP address. 192.168.1. 1 34 | Chapter 4: Customizing Your Network Wireless-N 150 Router WNR612v2 User Manual · Subnet mask. 255.255.255.0 These addresses are part of the designated private address range for use in private networks and should be suitable for most applications.

If your network has a requirement to use a different IP addressing scheme, you can make those changes in this screen. The LAN IP settings are: · · IP Address. The LAN IP address of the router. IP Subnet Mask. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. RIP Direction. RIP allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.

· When set to Both or In Only, the router incorporates the RIP information that it receives. When set to Both or Out Only, the router broadcasts its routing table periodically. · RIP Version. This controls the format and the broadcasting method of the RIP packets sent by the router. (It recognizes both formats when receiving.) The default setting is Disabled. RIP-1 is universally supported. RIP-1 is usually adequate unless you have an unusual network setup. RIP-2B carries more information than RIP-1 and uses subnet broadcasting. RIP-2M carries more information than RIP-1 and uses multicasting.

Using the Router as a DHCP Server By default, the router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. Note: For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

Click the link to the online document TCP/IP Networking Basics in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network. To specify a pool of IP addresses to be assigned, set the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168. 1.2 and 192.168.1.254, although you might wish to save part of the range for devices with fixed addresses. Chapter 4: Customizing Your Network | 35 Wireless-N 150 Router WNR612v2 User Manual The router delivers the following parameters to any LAN device that requests DHCP: · · · · · An IP address from the range you have defined Subnet mask Gateway IP address (the router's LAN IP address) Primary DNS server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address) Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen) To use another device on your network as the DHCP server, or to manually specify the network settings of all of your computers, clear the Use Router as DHCP Server check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router. Using Address Reservation When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

To reserve an IP address: 1. Click Add. 2. In the IP Address field, enter the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as 192.168.1.x.) 3. Enter the MAC address of the computer or server.

Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices screen and paste it here. 4. Click Apply to enter the reserved address into the table. Note: The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

36 | Chapter 4: Customizing Your Network Wireless-N 150 Router WNR612v2 User Manual To edit or delete a reserved address entry: 1. Click the button next to the reserved address you want to edit or delete. 2. Click Edit or Delete. Using a Dynamic DNS Service If your Internet Service Provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service, which allows you to register your domain to their IP address, and forwards traffic directed at your domain to your frequently changing IP address.

Note: If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service will not work because private addresses are not routed on the Internet. Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.

org. You must first visit their website at www.dyndns.org and obtain an account and host name, which you specify in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at hostname.dyndns.org. Select Dynamic DNS under Advanced in the main menu. The Dynamic DNS screen displays.

Chapter 4: Customizing Your Network | 37 Wireless-N 150 Router WNR612v2 User Manual To configure for a Dynamic DNS service: 1. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list. For example, for DynDNS.org, select www.dynDNS.

org. 2. Select the Use a Dynamic DNS Service check box. 3. Select the name of your Dynamic DNS service provider.

*4. Enter the host name (or domain name) that your Dynamic DNS service provider gave you. 5. Enter the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name. 6. Enter the password (or key) for your Dynamic DNS account. 7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use Wildcards check box to activate this feature. For example, the wildcard feature causes *.*

yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. 8. Click Apply to save your configuration. Configuring the WAN Setup Options The WAN Setup options let you do the following: · · · · Disable Port Scan and DoS Protection. Configure a DMZ (demilitarized zone) server. Enable the wireless router to respond to a ping on the WAN (Internet) port.

Disable IGMP Proxying The IGMP Proxying function lets a LAN PC receive the multicast traffic is interested in from the Internet. You can click this check box to disable the function if you do not need it. Change the Maximum Transmit Unit (MTU) size. Disable DIP ALG Some SIP applications have their own way to work around the NAT firewall issue, and the SIP ALG would conflict with those solutions. In most cases, you do not have to disable the SIP ALG. However, if your SIP applications cannot work with the router, you can disable the SIP ALG and try the applications again. Click the check box to disable SIP ALG. Enable IPv6 Pass-Through IPv6 pass-through is disabled by default. If you have IPv6 capable devices in your configuration and would like to use IPv6 instead of IPv4, you can click this check box to enable IPv6 Pass)-Through. · · · 38 | Chapter 4: Customizing Your Network Wireless-N 150 Router WNR612v2 User Manual Select WAN Setup under Advanced in the main menu.

The WAN Setup screen displays. Disabling Port Scan and DOS Protection The Port Scan and DOS Protection feature protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The Port Scan and Dos Protection feature should be disabled only in special circumstances, such as when you are troubleshooting application issues. Setting Up a Default DMZ Server The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server. WARNING! DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

Incoming traffic from the Internet is usually discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server. The WAN Setup screen lets you configure a default DMZ server. Chapter 4: Customizing Your Network | 39 Wireless-N 150 Router WNR612v2 User Manual To assign a computer or server to be a default DMZ server: 1. Select the Default DMZ Server check box. 2. In the Default DMZ Server fields, enter the IP address for that computer or server. 3. Click Apply.

Responding to a Ping on the Internet (WAN) Port If you want the router to respond to a ping from the Internet, select the Respond to Ping on Internet Port check box. This should be used only as a diagnostic tool, since it allows your router to be discovered by Internet scanners. Do not select this check box unless you have a specific reason to do so, such as when troubleshooting your connection. Setting the MTU Size The normal MTU value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1450 for PPTP connections. For some ISPs, you might need to reduce the MTU size, but this is rarely required and should not be done unless you are sure it is necessary for your ISP connection.

To change the MTU size: 1. In the MTU Size field, enter a new size between 64 and 1500. 2. Click Apply to save the new configuration. Disabling IGMP Proxying The IGMP Proxying function lets a LAN PC receive the multicast traffic it is interested in from the Internet.

If you do not need this function, you can click the Disable IGMP Proxying check box to disable this function. Disabling SIP ALG Some SIP applications have their own way to work around the NAT firewall issue, and the SIP ALG would conflict with those solutions. In most cases, you do not have to disable the SIP ALG. However, if your SIP applications cannot work with the router, you can disable the SIP ALG and try the applications again. To disable SIP ALG, click the Disable SIP ALG check box. Enabling IPv6 Pass-Through IPv6 pass-through is disabled by default. If you have IPv6-capable devices in your configuration and would like to use those devices instead of IPv4, you can click the Enable IPv6 Pass-Through check box to enable the IPv6 Pass-Through function. 40 | Chapter 4: Customizing Your Network Wireless-N 150 Router WNR612v2 User Manual Configuring NAT Filtering Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning.