



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for NETGEAR WN604. You'll find the answers to all your questions on the NETGEAR WN604 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual NETGEAR WN604
User guide NETGEAR WN604
Operating instructions NETGEAR WN604
Instructions for use NETGEAR WN604
Instruction manual NETGEAR WN604

NETGEAR

Wireless N150 Access Point
WN604
User Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

October 2011
202-10623-02
v1.0



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>

Manual abstract:

@@ netgear. @@ netgear. @@And/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. 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. 13 Configure the System Settings for Your Location. 57 Cannot Access the Internet or the LAN Wirelessly . Getting Started 1 This chapter covers the following topics: •••••About the Access Point Compatible NETGEAR Switches System Requirements What's In the Box Hardware Description For more information about the topics covered in this manual, visit the support website at <http://support>.

5 Wireless N150 Access Point WN604 About the Access Point The Wireless N150 Access Point WN604 is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. The access point provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. typically , an individual in-building access point provides a maximum connectivity area with about a 500-foot radius. Consequently, the access point can support a small group of users in a range of several hundred feet.

Most access points can handle between 10 and 30 users simultaneously per radio. The access point acts as a bridge between the wired LAN and wireless clients. Connecting multiple access points through a wired Ethernet backbone can extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point to another and still maintain seamless connection to the network.

Compatible NETGEAR Switches For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance website (WECA; see www). The following NETGEAR switches work with the WN604 Wireless Access Point: •••••••• FS108P - ProSafe™ 8 Port 10/100 Switch with 4 Port PoE FS116P ProSafe 16 Port 10/100 Desktop Switch with 8 Port PoE FS726TP - ProSafe 24 Port 10/100 Smart Switch with 2 Gigabit Ports and 12 Port PoE FS728TP - ProSafe 24+4 10/100 Smart Switch with full PoE FS752TPS - ProSafe 48 Port 10/100 Stackable Smart Switch with 4 Gigabit Ports and 24 Port PoE FSM7328PS - ProSafe 24-port 10/100 L3 Managed Stackable Switch with 24 PoE Ports FSM7352PS-ProSafe 48 Port 10/100 L3 Managed Stackable Switch with 4 Gigabit Ports and PoE GS724TP-ProSafe GS724TP 24-Port Gigabit Smart Switch and PoE GS748TP-ProSafe GS748TP 48-Port Gigabit Smart Switch and PoE Getting Started 6 Wireless N150 Access Point WN604 System Requirements Before installing the access point, make sure your system meets these requirements: ••••••A 10/100 Mbps LAN device such as a hub or switch The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it A 100–240 V, 50–60 Hz AC power source A web browser for configuration such as Microsoft Internet Explorer 6. 0 or later , or Mozilla 3. 0 or later At least one computer with the TCP/IP protocol installed 802. 11b/g/n-compliant devices What's In the Box The package contains the following: ••••••Wireless N150 Access Point WN604 Ethernet cable Power adapter Vertical stand feet (2) Installation Guide Resource CD Contact your reseller or customer support in your area if there are any missing or damaged parts. Keep the original packing materials, and use the packing materials to repack the access point if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR website at: www. Hardware Description This section describes the front, rear, and side hardware functions of the access point. Getting Started 7 Wireless N150 Access Point WN604 Front Panel The access point front hardware functions are described below. power WPS Wi-Fi Figure 1.

WN604 front panel LAN ports 1–4 The following table explains the LED indicators on the front panel. Power is on and the access point is ready. The wireless radio is up and running without wireless data transmission. The wireless interface is turned off. After initial set up, use an Ethernet port to connect to an Ethernet LAN through a device such as a hub, switch, router, or PoE switch. The Reset button has two functions: ••Reboot. When pressed and released quickly, the access point restarts. reset to Factory Defaults. This button can also be used to clear all data and restore all settings to the factory default values. You can use this button to turn the wireless radio off and on.

You can also schedule the wireless radio. See Schedule the Wireless Radio on page 46. wPS button. You can use WPS to add clients to the WN604 wireless network without typing the WPA or WPA2 password. see Wireless Security Options on page 27.

Product Label The label on the bottom of the access point includes the MAC address, serial number, security PIN, and the default IP address for logging in to the access point. figure 4. The label is located on the bottom of the access point Getting Started 10 2. Installation and Basic Configuration 2 This chapter contains the following sections: ••••••••••Log In to the Access Point Install the Access Point Set the Time Set Basic IP Options Configure Wireless Access Deploy the Access Point Wireless Settings Wireless Settings Configure Basic QoS Settings Set Up and Test Basic Wireless Connectivity 11 Wireless N150 Access Point WN604 Log In to the Access Point The access point is set, by default, with the IP address of 192. Prepare a computer with an Ethernet adapter.

a. If this computer is part of your network, record its TCP/IP configuration settings. b. Configure the computer with a static IP address of 192. Connect an Ethernet cable from the access point to the computer. 3. Power up the access point. a. Connect the power adapter and plug it into an electrical outlet. b.

Make sure that the Power On/Off button on the rear panel is in the On position (pressed in). □ •The LAN LED is on for the LAN port that is connected to your powered-on computer. Type admin in the User name field and password in the Password field, both in lower-case letters, and click Login.



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

[WN604 user guide](#)

<http://yourpdfguides.com/dref/5323165>

Installation and Basic Configuration 12 Wireless N150 Access Point WN604 Your web browser finds the access point and displays the General Settings screen. Install the Access Point Before installing the access point, make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b/g/n wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown in System Requirements on page 7. Tip: Before mounting the access point in a high location, first set up and test the access point to verify wireless network connectivity. NETGEAR recommends that you configure the access point in this sequence: 1.

Configure the System Settings for Your Location When you log in, the Configuration tab is selected and the General screen is displayed. This is where you specify your location. The access point uses this setting to determine which channels should be used for wireless communication. *Installation and Basic Configuration 13 Wireless N150 Access Point WN604* □ To set up the access point for your location: 1. log in as described in the previous section. The Configuration tab is selected and the General screen is displayed: 2. If you want to change the default access point name, in the Access Point Name field, type a meaningful name. This unique name is the access point NetBIOS name. The default access point name is located on the bottom label of your product. The default is netgearxxxxxx, where xxxxxx represents the last 6 digits of the WN604 MAC address.

You can modify the default name with a unique name up to 15 characters long. 3. From the Country/Region drop-down list, select the region where the access point is located (the default country/region is the United States). Note: If your country or region is not listed, check with NETGEAR support. *Installation and Basic Configuration 14 Wireless N150 Access Point WN604 Set the Time* □ To configure your time settings: 1. From the drop-down list, select the local time zone for your access point from a list of all available time zones. Enable NTP client to synchronize the time of the access point with an NTP server. the default is Enable. Note: You need an Internet connection to get the current time. ••Use Custom NTP Server.

Select this check box if you have a custom NTP server. Enter the host name or the IP address of the custom NTP server. Set Basic IP Options The basic IP settings for your access point are entered on this screen. Most of the default settings work in most cases. However, if your access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields. *Installation and Basic Configuration 15 Wireless N150 Access Point WN604* □ To configure the basic IP settings of your access point: 1. Enter the settings for the access point. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point gets its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the access point to your LAN. iP Address. Enter the IP address of your access point. The default IP address is 192. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP. iP Subnet Mask. The access point automatically calculates the subnet mask based on the IP address that you assign. Otherwise, you can use 255.

Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the access point is connected. primary DNS Servers. This is the address of the primary Domain Name Server used by stations on your LAN. secondary DNS Servers. This is the address of the secondary Domain Name Server used by stations on your LAN. network Integrity Check. Select this check box to enable the access point to validate that the upstream link is active before allowing wireless associations. If you set this option, you have to ensure that your default gateway is configured. *Installation and Basic Configuration 16 Wireless N150 Access Point WN604 Configure Wireless Access* □ To configure your wireless settings for 11b/bg/ng: 1. Enter the wireless settings for your area. When you have completed the setup steps, you can deploy the access point in your network. If needed, you can now reconfigure the computer that you set to use the static IP back to its original TCP/IP settings. Deploy the Access Point □ To deploy the access point: 1. Disconnect the access point and position it where it will be deployed.

The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices. 2. Lift the antenna so that it is vertical. Note: Refer to the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter. 3. Connect an Ethernet ca you wish to use on your wireless LAN. The wireless channel in use is between 1 and 11 for United States and Canada, 1 and 13 for Europe and Australia. the default is Auto. It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and slow data transfers). Should this happen, you might need to experiment with different channels to see which is the best.

Alternatively, you can select the Auto channel option for the AP to intelligently pick the channel with least interference. When selecting or changing channels, some points to bear in mind: ••Access points use a fixed channel. You can select the channel that provides the least interference and best performance. In the USA and Canada, 11 channels are available. If you are using multiple access points, it is better if adjacent access points use different 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). wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen only when the various access points are using the same SSID. •MCS Index/Data Rate.

From the drop-down list, select the available transmit data rate of the wireless network. Also, depending on the band selected, the set of rates varies. The possible data rates supported are: *Installation and Basic Configuration 20 Wireless N150 Access Point WN604* ••••Data rates for channel width = 20 MHz and guard interval=short (400 ms): Best, 7. Data rates for channel width = 20 MHz and guard interval=long (800 ms): Best, 6. 5 Mbps. Data rates for channel width = 40 MHz and guard interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps.



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>

Data rates for channel width = 40 MHz and guard interval=long: Best, 13. From the drop-down list, select the desired channel width. •••20 MHz. This is the static, legacy mode.

This is the static, high-throughput mode. Legacy clients cannot connect in this mode. 20/40 MHz. This is the dynamic, compatibility mode. guard Interval. From the drop-down list, select the desired guard interval. The guard interval protects from interference from other transmissions. From the drop-down list, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more APs are close together and use the same channel frequency.

the default is Full. (The transmit power might vary depending on the local regulatory regulations. WMM allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also have to support WMM.

Select the Disable radio button to disable WMM power save. 4. Click Apply to save your settings Set Up and Test 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. Note: If you are configuring the access point from a wireless computer and you change the SSID, channel, or security profile settings, you will lose your wireless connection when you click Apply.

To connect to the wireless network, you have to change the wireless settings of your computer to match the new settings. Verify that the correct country/region in which the wireless interface will operate has been selected. Ensure that the auto channel (default) feature is selected for your network. This feature selects a channel that has the least interference. It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your access point. For initial configuration and testing, the Network Authentication setting is set to Open System and the default SSID to NETGEAR_11ng. (For more information about configuring a profile, see Security Profiles on page 25.) Note: The SSID of any station has to match the SSID you configured in the access point. If they do not match, you will not get a wireless connection to the access point.

Configure and test your PCs for wireless connectivity. Set up the wireless adapters of your PCs to have the same SSID that you configured in the WN604. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WN604. Once your PCs have basic wireless connectivity, you can configure the advanced wireless security functions. □•••Security Profiles Wireless Security Options Manually Configure Security Wi-Fi Protected Setup (WPS) Restrict Wireless Access by MAC Address 24 Wireless N150 Access Point WN604 Security Profiles Security profiles let you configure unique security settings for each SSID. You can configure only one wireless security profile. You can set up a single security profile for 802. 11b/bg/ng, which is the default profile. Enter the wireless network name (SSID) for the wireless network. If the name is broadcast, it can be easily detected by clients.

4. From the Network Authentication drop-down list, select the network authentication type you want to use for this profile. 5. Select the data encryption strength from the drop-down list. If enabled, the associated wireless clients cannot communicate with each other.

The following sections explain the fields on this screen and how to set up security. Edit Security Profile Screen Fields An overview of the information that is required to set up a security profile follows: Profile Definition Wireless Network Name (SSID). This is the name of your wireless network. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network Configure Security 25 Wireless N150 Access Point WN604 "discovery" feature of some products such as Windows XP, Vista, and Unix systems, but the data is still fully exposed to a determined snooper using specialized test equipment like wireless sniffers.

The access point is set by default as an open system with no authentication. When setting up network authentication, bear in mind the following: •• If you are using access point mode, then all options are available. In bridge mode some options might be unavailable. legacy adapters might not support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings. You can configure the access point to use the types of network authentication shown in the following table. This is used with WEP encryption. You enter at least one shared key. TKIP or TKIP + AES encryption and enter the WPA passphrase (network key).

WPA2-PSK Select this only if all clients support WPA2. If selected, you have to (WPA2 is a later version of WPA) use AES or TKIP + AES encryption and enter the WPA passphrase (Network key). WPA-PSK and WPA2-PSK This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you have to use TKIP + AES encryption and enter the WPA passphrase (Network key). a. All options are available if using access point mode. In bridge modes some options might be unavailable. data Encryption. The available options depend on the Network Authentication setting selected (see Table 2); otherwise, the default is None. Proprietary mode that works only with other wireless devices that support this mode.

TKIP. This is the standard encryption method used with WPA and WPA2. AES. This is the standard encryption method for WPA2. configure Security 26 Wireless N150 Access Point WN604 • TKIP + AES.

This setting supports both WPA and WPA2. broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. passphrase. To use the passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button.

You can also enter the keys directly. These keys have to match the other wireless stations. key 1 , Key 2 , Key 3 , Key 4. If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used only to decrypt received data. WPA Preshared Key Passphrase. If using WPA-PSK or WPA2-PSK, enter the passphrase here. All wireless stations have to use the same passphrase (network key). The network key has to be from 8 to 64 characters in length.

wireless Client Security Separation.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5323165)

[WN604 user guide](http://yourpdfguides.com/dref/5323165)

<http://yourpdfguides.com/dref/5323165>

If enabled, the associated wireless clients cannot communicate with each other. (This feature is intended for hotspots and other public access situations.) The default is Disabled. Wireless Security Options Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The access point provides highly effective security features. Deploy the security features appropriate to your needs. There are several ways you can enhance the security of your wireless network: • Restrict access based on MAC address. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WN604.

MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. 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 the wireless network "discovery" feature of some products such as Windows XP, Vista, and Unix systems, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. The very strong authentication along with dynamic per frame rekeying of WPA makes it virtually impossible to compromise.

NETGEAR recommends that you use WPA2 or WPA for stronger wireless security. ••• Configure Security 27 Wireless N150 Access Point WN604 Note: WEP and TKIP provide only legacy rates of operation. So, AES is the recommended solution to use the 802.11n rates and speed. Manually Configure Security The following sections explain how to manually configure security.

Note: If you use a wireless computer to change wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the access point from a wired computer to make any further changes. configure WPA2, or WPA2 + WPA, or WPA The process of setting up WPA2, WPA, or WPA2 + WPA is very similar. Consult the product document for your wireless clients and for instructions on configuring client WPA2 settings. From the Network Authentication drop-down list, select the option that you want to use to secure your network. NETGEAR recommends WPA2, but you can select any of the following, depending on whether your client devices support WPA2: Configure Security 28 Wireless N150 Access Point WN604 ••• WPA2-PSK. With this setting, only wireless clients that support WPA2 can access the wireless network. By default, the Data Encryption field is set to AES. wPA-PSK & WPA2-PSK. Wireless clients using WPA2 or WPA can access the wireless network.

By default, the Data Encryption field is set to TKIP+AES. wPA-TKIP. Wireless clients using WPA can access the wireless network. 3. In the WPA Passphrase (Network Key) field, enter the password that you want to use to secure the wireless network. If it is enabled, associated wireless clients cannot communicate with each other. (This feature is intended for hotspots and other public access situations. From the Network Authentication drop-down list, select either Open System or Shared Key authentication. 3. From the Data Encryption drop-down list, select encryption strength (64 bits, 128 bits, or 152 bits).

4. You manually or automatically program the four data encryption keys. These values have to be identical on all PCs and access points in your network. select one of the following: • Automatic. Enter a word or group of printable characters in the Passphrase field and click the Generate Keys button. The four key fields are automatically populated with key values. • Manual. Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit, 26 digits for 128-bit, and 32 digits for 152-bit (any combination of 0-9, a-f, or A-F). configure Security 29 Wireless N150 Access Point WN604 5. Select the key to be used as the default key by selecting the radio button.

(Data transmissions are always encrypted using the default key. If it is enabled, associated wireless clients cannot communicate with each other. (This feature is intended for hotspots and other public access situations. Wi-Fi Protected Setup (WPS) WPS is a simple method that lets you easily and securely add a client to the wireless network without typing the WPA2 or WPA password. wPS is compatible with WPA2 and WPA security. The wireless client has to support WPS for this method to work. Select the Enable radio button to enable WPS on your access point. 3. Adjust the other settings on the screen as needed. • Router's PIN.

This is the PIN that a registrar can use to configure the access point's wireless settings through WPS. This PIN is also on the product label. You can use an external registrar to configure the access point's SSID and security settings through WPS, and you will be prompted to enter the PIN that is displayed here.

Note: By using this WPS PIN, an external registrar can set or get the access point's wireless settings through WPS, and apply the settings to connect itself to the access point. • Disable Router's PIN. Select this check box if you want to disable the access point's PIN. An external registrar can only configure the access point's wireless settings through WPS only when the PIN is enabled. By default, this check box is not selected. configure Security 30 Wireless N150 Access Point WN604 • Keep Existing Wireless Settings. Select this check box if you want to keep the current wireless settings the same when you use WPS to add a client device.

4. Click Apply so that your changes take effect. Use WPS to Add a Client to the Wireless Network WPS is compatible with WPA2 and WPA security. The wireless client has to support WPS for this method to work. Check the documentation that came with the wireless client machine.

You can use the WPS button on the side of the access point, or you can log in to the access point and use the Add WPS Client feature. □ To add a client using the WPS button: 1. Press the WPS button located on the side of the access point. The WPS LED on the front of the access point flashes. The access point tries to associate with a wireless client.

Follow the WPS instructions that came with it to press a WPS button. The wireless client attempts to join the wireless network. If it successfully joins, then it is automatically configured with the wireless network SSID and wireless security. σ To add a client when logged in to the access point: 1. Select either the Push Button (Recommended) button or the PIN (Personal Identification Number) button. The Push Button method is easier, while the PIN method is more secure. □ The Push Button method lets you add a client with the WPS push button on the side panel of the WN604 and the push button on the client). □ The PIN method requires you to enter the wireless client's PIN, which should be displayed on the client's utility interface.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5323165)

[WN604 user guide](http://yourpdfguides.com/dref/5323165)

<http://yourpdfguides.com/dref/5323165>

A progress bar on the Connecting to New Wireless Client screen shows the status of the wireless connection. If the wireless settings changed, you are notified.

You can click OK to view the new settings: 4. If the settings have not changed, you can click the Success message to return to the Add WPS Client screen. 5. In case of an error in completing the WPS process, refer to the online help. Restrict Wireless Access by MAC Address Access control lets you block the network access privilege of any specified stations through the access point. When you enable access control, the access point accepts only connections from clients on the selected access control list. this provides an additional layer of security. @@Otherwise, you will be disconnected when you click Apply. @@@@The access point uses the local MAC address table for access control. 3.

@@If you have not entered any wireless stations, this list is empty. @@ 5. @@@@ 6. @@@@ configure Security 33 4. @@@@ 1. @@ 2. @@Click Browse and browse to the location of the upgrade file. @@The upgrade process typically takes about 2 minutes. @@@@ see Factory Default Settings on page 6. σ To back up your current settings: 1.

Your browser extracts the configuration settings from the access point and prompts you for a location on your computer to store the file. Enter the full path to the backup file on your computer, or click the Browse button to locate the file. After completing the upload, the WN604 reboots automatically. After a restore, the access point password is password, the default LAN IP address is 192. 230, and the access point name is reset to the name on the label on the bottom of the unit. Management 37 Wireless N150 Access Point WN604 Change the Administrator Password The user name of admin cannot be changed. the default password is password. You should change this to a more secure password. First enter the old password in the Current Password field. 3.

Then enter the new password twice—once in the New Password field and again in the Repeat New Password field. Management 38 Wireless N150 Access Point WN604 Enable the SysLog Server The syslog screen allows you to enable the syslog option if you have a syslog server on your LAN. Select the Enable Syslog check box if you have a syslog server on your LAN. 3. Enter the IP address of your SysLog server and the port number your syslog server is configured to use. •Syslog Server IP Address. The access point sends all the syslogs to the specified IP address if the syslog option is enabled. •Port Number. The port number configured in the syslog server on your LAN. The Logs screen displays: The Logs screen displays the access point system activity.

You can click Refresh to update the display, click Clear to clear the log content, or click Save As to save the log contents into a file on a disk drive. Management 40 Wireless N150 Access Point WN604 View Summary Information The System screen, which you access through the Monitoring tab, provides a summary of the current access point configuration settings, including current IP settings and current wireless settings. This information is read-only, so any changes have to be made on other screens. To navigate to this screen, select Monitoring > System: System Screen Fields This section describes the fields in this screen. You can change the default name in the General screen (Configuration > General).

ethernet MAC Address. The Media Access Control address (MAC address) of the access point's Ethernet port. wireless MAC Address. The Media Access Control address (MAC address) of the access point's wireless card. country/Region.

The domain or region for which the access point is licensed for use. It might not be legal to operate this access point in a region other than one of those identified in this field. firmware Version. The version of the firmware currently installed. current Time. The current time setting of the access point. management 41 Wireless N150 Access Point WN604 Current IP Settings IP Address. The IP address of the access point. subnet Mask. The subnet mask for the IP address of the access point.

default Gateway. The default gateway for access point communication. DHCP Client. Enabled indicates that the current IP address of the AP was obtained from a DHCP server on your network. Identifies the channel the wireless port is using. Click Refresh to update the Statistics information for each interface.

statistic Screen Fields Wired Ethernet Packets. The number of packets sent and received since the WN604 was restarted. management 42 Wireless N150 Access Point WN604 Bytes. The number of bytes sent and received since the WN604 was restarted. wireless 11b/bg/ng Unicast Packets. The unicast packets sent and received in 802. The broadcast packets sent and received in 802. The multicast packets sent and received in 802. The wireless packets sent and received in 802.

The wireless bytes sent and received in 802. 11n/g mode since the access point was restarted. Available Wireless Station Statistics The Available Wireless Stations table lists all IP devices associated with this access point in the wireless network defined by the wireless network name (SSID). For each device, the table shows the MAC address, BSSID, SSID, channel, rate, state (whether the device is allowed to communicate with the access point or not), type, AID, mode, and status. A wireless network can include multiple wireless access points, all using the same network name (SSID).

This enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point are in the Available Wireless Stations list. Tip: If the access point is rebooted, the table data is lost until the access point rediscovers the devices. To force the access point to look for associated devices, click the Refresh button.

management 44 5. Advanced Configuration 5 This chapter includes the following sections: •••• Schedule the Wireless Radio Advanced Wireless Settings Advanced QoS Settings Enable Wireless Bridging 45 Wireless N150 Access Point WN604 Schedule the Wireless Radio You can schedule the times when the wireless radio is on and off, for any day of the week. This feature depends on the NTP (Network Time Protocol) functionality. if an NTP client request fails , then last configured value of radio status is restored. Also, if the wireless radio is disabled, then the scheduled feature does not work. By default, the On radio button is selected for the Scheduled Wireless On-Off field so that the wireless radio is on all the time.

2. If you want to change this so that the wireless radio is off except when you schedule it to be on, select the Off radio button. 3. For Radio Off Schedule, select the check boxes for each day on which you want to turn off the wireless radio for that entire day. 4. In the Radio On Time and Radio Off Time fields, set the period that the wireless radio is on and off for the days not selected in the radio off schedule.



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>

Advanced Wireless Settings Advanced wireless settings are used to configure and enable various WLAN parameters for the 802.11b/bg/ng modes. The default WLAN parameters usually work well. However, you can use these settings to fine-tune the overall performance of your access point for your environment.

The fields are described in the following section. 3. Click Apply so that your changes take effect. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period.

With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field are fragmented. The fragmentation threshold value has to be larger than the RTS threshold value. The beacon interval specifies the time in milliseconds between 100 and 1000 transmissions, which allows the access point to synchronize the wireless network.

The aggregation length defines the size of aggregated packets. Larger aggregation lengths might sometimes lead to better network performance. Aggregates several MAC frames into a single large frame to achieve higher throughput. RIFS transmissions are shorter than other interframe spaces, and if enabled allow transmission of successive frames at different transmit powers. The delivery traffic indication message specifies the data beacon rate between 1 and 255. A long transmit preamble might provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto settings automatically handles both long and short preambles. Enable this option to include support for additional regulatory domains that are not in the current standard. max Wireless Clients.

The number of wireless clients that can associate with the AP at one time. WME allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WME to function correctly, wireless clients also need to support WME. For most networks, the default QoS queue parameter settings work well. Quality of Service provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data. Specify the AP EDCA (Enhanced Distributed Channel Access) parameters for different types of data transmitted from the access point to the wireless client. • Station EDCA Parameters. Specify the Station EDCA parameters for different types of data transmitted from the wireless client to the access point. if WMM is disabled, you cannot configure Station EDCA parameters.

QoS queues and parameters are described in the following table. 3. Click Apply so that your changes take effect. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Specifies a wait time (in milliseconds) for data frames. Valid values for AIFS are 1 through 255. Upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwMin has to be lower than the value for cwMax.

AIFS (Arbitration Inter-Frame Space) cwMin (Minimum Contention Window) cwMax (Maximum Contention Upper limit (in milliseconds) for the doubling of the random backoff value. valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for Window) cwMax has to be higher than the value for cwMin. max. Burst Length Specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. a packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0. Enable Wireless Bridging The access point lets you build large bridged wireless networks. Select the desired access point mode for your environment: • Wireless Point-to-Point Bridge. In this mode, the access point can communicate with another bridge mode wireless access point, and with wireless clients if this option is enabled.

advanced Configuration 49 Wireless N150 Access Point WN604 • Wireless Point-to-Multi-Point Bridge. Select this only if this WN604 is the master for a group of bridge-mode wireless access points. The other bridge-mode wireless access points has to be set to point-to-point bridge mode, using the MAC address of this WN604. They then send all traffic to this "Master", rather than communicating directly with each other. The WN604 can associate with wireless clients if this option is enabled. • Client. In this mode the access point acts as a client. It is used to extend the LAN of clients that do not have wireless connectivity. If you selected one of the first two options: • Select the security profile whose settings you want to edit. In the Enable Wireless Association table, select the Enable check box for the profile you want to edit.

Click Back to return to the previous screen and enable the profile. This option displays only in client mode. Use it to configure a new MAC address on the AP client if desired. • MAC Clone Address. If the MAC Clone option has been enabled, enter the new MAC address in hexadecimal format.

It is used by the client in place of its default physical address. The following sections help you to physically configure your access point as a point-to-point bridge or a point-to-multi-point bridge. Advanced Configuration 51 Wireless N150 Access Point WN604 Configure a Point-to-Point Bridge AP 1 point-to-point bridge mode AP 2 point-to-point bridge mode Router Hub or switch LAN segment 1 Figure 5. Configure the first access point (AP 1) on LAN segment 1 in point-to-point bridge mode. AP 1 needs to have AP 2's MAC address in its Remote MAC Address field, and AP 2 needs to have AP 1's MAC address in its Remote MAC Address field.

4. Configure and verify the following parameters for both access points: • Verify that the LAN networks of the access points are both configured to operate in the same LAN network address range as the LAN devices. Both use the same ESSID, channel, authentication mode, if any, and security settings if security is in use. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN segment 1 or LAN segment 2.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5323165)

[WN604 user guide](http://yourpdfguides.com/dref/5323165)

<http://yourpdfguides.com/dref/5323165>

Advanced Configuration 52 Wireless N150 Access Point WN604 Configure a Point-to-Multi-Point Wireless Bridge AP 1 point-to-point bridge mode AP 2 (master) point-to-multi-point bridge mode AP 3 point-to-point bridge mode Router 192. Configure the operating mode of the access points. □ Configure the first access point (AP 1) on LAN segment 1 in point-to-point bridge mode with the remote MAC address of AP 2. □ Because it is in the central location, configure AP 2 on LAN segment 2 in point-to-multi-point bridge mode. The MAC addresses of the adjacent APs are required in AP 2. Configure AP 3 on LAN 3 in point-to-point bridge mode with the remote MAC address of AP 2.

• 3. Verify the following parameters for all access points: • Verify that the LAN networks of the access points are configured to operate in the same LAN network address range as the LAN devices. □ • • • Only one access point is configured in point-to-multi-point bridge mode, and all the others are in point-to-point bridge mode. All access points have to be on the same LAN. That is, all the APs LAN IP address must be in the same network. If using DHCP, for all WN604 Wireless Access Points, in the IP Settings section, , DHCP Client should be enabled so that APs obtain IP addresses automatically. All access points use the same SSID, channel, authentication mode, if any, and encryption in use. Advanced Configuration 53 Wireless N150 Access Point WN604 • All point-to-point access points need to have the AP 2 MAC address in their Remote AP MAC address fields. □ A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments. □ Wireless stations can connect to the access points in the preceding illustration.

If you require wireless stations to access any LAN segment, you can add additional access points configured in wireless access point mode to any LAN segment. Note: You can extend this multi-point bridging by adding additional access points configured in point-to-point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories. advanced Configuration 54 6. Troubleshooting 6 This chapter includes the following sections: • • • Troubleshooting with the LEDs Cannot Access the Internet or the LAN Wirelessly Cannot Connect to the Access Point to Configure It Time-Out Error 55 Wireless N150 Access Point WN604 Troubleshooting with the LEDs You can use the LEDs on the front panel of the access point for troubleshooting.

All LEDs Are Off It takes a few seconds for the Power LED to light up. Wait a minute and check the Power LED again. if the access point has no power. □ • Make sure the power adapter is connected to the access point. Make sure the power adapter is connected to a functioning power outlet.

If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet. Make sure you are using the correct NETGEAR power adapter supplied with your access point. □ WiFi LED Is Off The wireless radio is turned off or the antenna is not working.

There are two ways to turn off the wireless radio--the Wireless On/Off button on the side of the access point, and the Schedule Wireless Radio feature. wireless On/Off Figure 7. You can use the Wireless On/Off button to control the wireless radio For information about the Schedule Wireless Radio feature, see Schedule the Wireless Radio on page 46. check the following: 1. Make sure that the wireless radio is turned on. If it is, and the WiFi LED stays off, disconnect the access point from its power source and then plug it in again.

2. Make sure the antenna is securely connected to the access point. 3. Contact NETGEAR technical support if the WiFi LED remains off. troubleshooting 56 Wireless N150 Access Point WN604 LAN LED Is Off There is a hardware connection problem . Check these items: • Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router has to be installed between the access point and the Ethernet LAN or broadband modem. LAN LED does not light up if there is a 10 Mbps link. In such cases, the LAN LED blinks if there is activity.

Make sure the connected device is turned on.

If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable. □ • • Cannot Access the Internet or the LAN Wirelessly There is a configuration problem. Check these items: • • You might not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. restart the computer. The computer with the wireless adapter might not have the correct TCP/IP settings to communicate with the network.

Restart the computer and check that TCP/IP is set up correctly for that network. The usual setting for Windows network properties is to obtain an IP address automatically. □ The access point's default values might not work with your network. Check the access point's default configuration against the configuration of other devices in your network. □ Cannot Connect to the Access Point to Configure It Check these items: • • The access point is correctly installed, LAN connections are OK, and it is powered on.

Check that the LAN port LED is green to verify that the Ethernet connection is OK. The default configuration of the WN604 is for a static IP address of 192. Make sure your network configuration settings are correct. If you are using the NetBIOS name of the access point to connect, ensure that your computer and the access point are on the same network segment or that there is a WINS server on your network. If your computer is set to obtain an IP address automatically (DHCP client), restart it. If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the WN604. The access point default IP address is 192. □ • • Troubleshooting 57 Wireless N150 Access Point WN604 Time-Out Error If you get a time-out error when you enter a URL or IP address, try these suggestions. □ Check to see if other PCs work. If they do, ensure that your PC's TCP/IP settings are correct.

If using a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses. If the PCs are configured correctly, but still not working, ensure that the access point is connected and turned on. connect to it and check its settings. If you cannot connect to it, check the LAN and power connections. If the access point is configured correctly, check your Internet connection to make sure that it is working correctly. Supplemental Information A This appendix includes the following sections: • • Factory Default Settings Technical Specifications 5 Wireless N150 Access Point WN604 Factory Default Settings The Reset button has two functions: • • □ Reboot.



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>

When pressed and released quickly, the access point restarts. reset to Factory Defaults. This button can also be used to clear all data and restore all settings to the factory default values. To clear all data and restore the factory default values: 1.

Power off the access point and power it back on. 2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds until the WiFi LED blinks rapidly. □ Your device returns to the factory configuration settings shown in the following table. table 1.

Access point default onfiguration settings Feature Login URL User name (case-sensitive) printed on product label Password (case-sensitive) printed on product label Static IP address Ethernet MAC address Port speed Subnet mask DHCP client Default setting www. Access point default onfiguration settings (continued) Feature Time zone Operating mode Access point name Wireless communication Wi-Fi Protected Setup (WPS) Wireless network name (SSID)

Broadcast network name (SSID) Security Transmission speed Country/Region Scheduled wireless On/Off Default setting USA-Pacific Access point netgearxxxxx where xxxxxx are the last 6 digits of the wireless access point "Ethernet" MAC address. enabled Disabled NETGEAR_11ng Enabled Disabled 1Best1 Varies by region Disabled 80211. B/bg/ng radio frequency channel Auto Output power Wireless card access List WMM support Full All wireless stations allowed Enabled 1. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable) Data rates for channel width = 20 MHz and guard Interval = short (400ms): Best, 7. 2 Mbps Data Rates for Channel Width = 20 MHz and guard Interval = long (800 ms): Best, 6. 5 Mbps, 65 Mbps Data Rates for channel width = 40 MHz and guard Interval = short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps Data Rates for channel width = 40 MHz and guard

Interval = long: Best, 13. 472 GHz (Europe ETSI) 64-bits, 128-bit and 152-bit WEP, AES, TKIP data encryption Web-based configuration and status monitoring Limited by the amount of wireless network traffic generated by each node; maximum 64 supported. Notification of Compliance NETG EAR

Wireless Routers, G ateways, APs Regulatory Compliance Information B Note: 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. Europe – EU Declaration of Conformity Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards: EN300 328 (2.

4Ghz), EN301 489-17 EN60950-1 For complete DoC, visit the NETGEAR EU Declarations of Conformity website at: <http://support.> , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. 4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies. 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. FCC Requirements for Operation in the United States FCC Information to User This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals. @@@@ fCC Declaration of Conformity We , NETGEAR , Inc.

@@Operation is subject to the following two conditions: • This device may not cause harmful interference, and • This device must accept any interference received, including interference that may cause undesired operation. 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: • 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. Notification of Compliance 65 Wireless N150 Access Point WN604 FCC Caution • Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

□ 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. □ For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible. □ This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter. Canadian Department of Communications Radio Interference Regulations This digital apparatus (Wireless N150 Access Point WN604) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>

This Class [B] digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada Industry Canada This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. GPL License Agreement GPL may be included in this product; to view the GPL license agreement go to <ftp://downloads>. For GNU General Public License (GPL) related information, please visit <http://support>. Notification of Compliance 66 Wireless N150 Access Point WN604 Interference Reduction Table The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters). Household Appliance Recommended Minimum Distance (in feet and meters) 30 feet / 9 meters 20 feet / 6 meters 40 feet / 12 meters 20 feet / 6 meters 30 feet / 9 meters 20 feet / 6 meters 20 feet / 6 meters Microwave ovens Baby Monitor - Analog Baby Monitor - Digital Cordless phone - Analog Cordless phone - Digital Bluetooth devices ZigBee Notification of Compliance 67 Index A access control list 33 access point mode 26 activity log 40 AES 802. .



[You're reading an excerpt. Click here to read official NETGEAR WN604 user guide](http://yourpdfguides.com/dref/5323165)
<http://yourpdfguides.com/dref/5323165>