NETGEAR

N750 Wireless Dual Band Gigabit Router WNDR4000

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

March 2011
202-10781-02
v1.0

©2010 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. 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.

Contents

Chapter 1 Hardware Setup

Unpack Your Wireless Router 8
Hardware Features 8
Front Panel 8
Back Panel 10
Label 10
Router Stand 11
Position Your Router 11
Cable Your Router 12
Verify the Cabling 13

Chapter 2 Set Up Your Internet Connection

Wireless Router Setup Preparation 16
Use Standard TCP/IP Properties for DHCP 16
Replace an Existing Router 16
Gather ISP Information 16
Log In to the Router 17
Upgrade Firmware 18
Router Interface 18
Setup Wizard 19
Manual Setup (Basic Settings) 20
Unsuccessful Internet Connection 23
Change Password 23
Log Out Manually 24
Types of Logins 24

Chapter 3 Wireless Settings

Wireless Security Compatibility 26
Security Basics 26
Wireless Security Options 26
Turn Off Wireless Connectivity 26
Disable SSID Broadcast 27
Restrict Access by MAC Address 27
Add Clients (Computers or Devices) to Your Network 27
Manual Method 27
Wi-Fi Protected Setup (WPS) Method 28
Wireless Settings Screen 29
Consider Every Device on Your Network 29
View or Change Wireless Settings 30

Wireless Settings Screen Fields 31
Set Up WPA Security Option and Passphrase 32
Wireless Guest Networks 32

Chapter 4 Content Filtering Settings

Logs 35
Examples of Log Messages 36
Keyword Blocking of HTTP Traffic 37
Delete Keyword or Domain 37
Specify a Trusted Computer 38
Block Services 38
Set the Time Zone 40
Schedule Services 41
Turn On Security Event Email Notification 42
Port Forwarding 43
Add a Custom Service 44
Application Example: Making a Local Web Server Public 45
Port Triggering 46

Chapter 5 Network Maintenance

Upgrade the Firmware 50
Automatic Firmware Check 50
Stop the Automatic Firmware Check 51
Manually Check for Firmware Upgrades 51
Manage the Configuration File 52
Back Up 52
Restore 53
Erase 53
View Router Status 53
Internet Port Settings 53
LAN Port (Local Ports) 54
Wireless Port 54
Show Statistics 54
Connection Status 55
View Attached Devices 56

Chapter 6 USB Storage

USB Drive Requirements 58
File-Sharing Scenarios 58
Share Photos within Your Home Network 58
Share Large Files with FTP over the Internet 59
USB Storage Basic Settings 59
Basic Settings Screen Fields and Buttons 60
Edit a Network Folder 60
USB Storage Advanced Settings 61
Create a Network Folder 63

Unmount a USB Drive 63
Approved USB Devices 64
Connect to the USB Drive from a Remote Computer 64
Locate the Internet Port IP Address 65
Access the Modem Router's USB Drive Remotely with FTP 65
Connect to the USB Drive with Microsoft Network Settings 65
Enabling File and Printer Sharing 65

Chapter 7 Advanced Settings

WAN Setup 68
Default DMZ Server 69
Dynamic DNS 70
LAN Setup 71
LAN Setup Screen Settings 72
IP Address Reservation 72
Quality of Service (QoS) 73
QoS for Internet Access 73
Advanced Wireless Settings 74
Wireless Advanced Settings (2.4 GHz and 5 GHz) 75
WPS Settings 75
Wireless Card Access List 75
Remote Management Access 76
Static Routes 78
Static Route Example 78
Add a Static Route 79
Universal Plug and Play 80
IPv6 81
Traffic Meter 81
Advanced USB Settings 83
Wireless Bridging and Repeating Networks 83
Set Up a Repeater with Wireless Client Association 85

Chapter 8 Troubleshooting

Quick Tips 88
Sequence to Restart Your Network 88
Power LED 88
Check Ethernet Cable Connections 88
Wireless Settings 88
Network Settings 89
Troubleshooting with the LEDs 89
Power LED Is Off or Blinking 89
LEDs Never Turn Off 89
Internet or Ethernet Port LEDs Are Off 90
Wireless LED Is Off 90
Cannot Log In to the Wireless Router 90
Cannot Access the Internet 91
Changes Not Saved 92

Incorrect Date or Time 92
Wireless Connectivity 93
Wireless Signal Strength 93
Restoring the Factory Settings and Password 93

Appendix A Supplemental Information

Factory Settings 94
Technical Specifications 96

Appendix B Notification of Compliance

Index

Hardware Setup

1

The *N750 Wireless Dual Band Gigabit Router WNDR4000 User Manual* provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It has is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (PCs, gaming consoles, and so on) that you connect to your home network.

For more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

If you have not already set up your new wireless router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Set Up Your Internet Connection* explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Wireless Router*
- *Hardware Features*
- *Position Your Router*
- *Cable Your Router*
- *Verify the Cabling*

Unpack Your Wireless Router

Your box should contain the following items:

- N750 Wireless Dual Band Gigabit Router WNDR4000
- Router stand
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- *Resource CD*
- Installation guide with cabling and wireless router setup instructions

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you need to return the product for repair.

Hardware Features

Before you cable your wireless router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The wireless router front panel has the status LEDs and icons shown in the figure. Note that the Wireless and WPS icons are buttons.

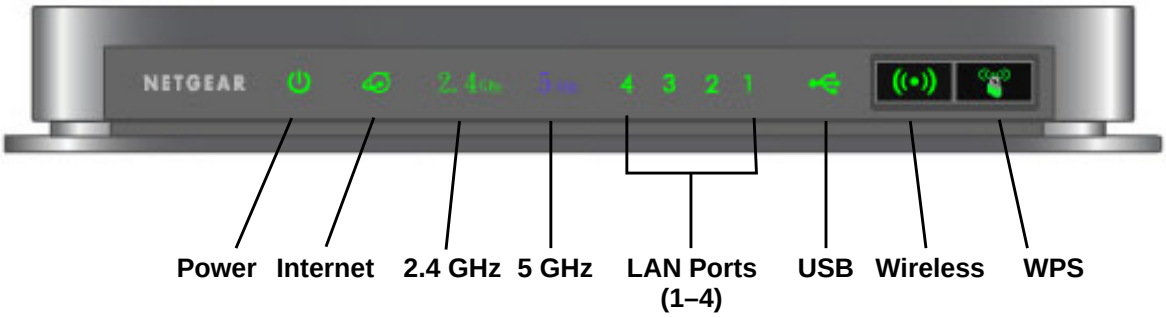


Figure 1. Front panel LEDs and icons

The following table describes the LEDs, icons, and buttons on the front panel from left to right.

Icon	Description
Power	• **Solid amber**. The unit is starting up after being powered on. • **Solid green**. Power is supplied to the wireless router. • **Off**. Power is not supplied to the wireless router. • **Blinking green**. The firmware is corrupted. See *www.netgear.com/support*. • **Blinking amber**. The firmware is upgrading, or the **Restore Factory Settings** button was pressed.
Internet	• **Solid green**. An IP address has been received; ready to transmit data. • **Solid amber**. The Ethernet cable connection to the modem has been detected. • **Off**. No Ethernet cable is connected to the modem.
2.4 GHz	• **Solid green**. The 2.4 GHz wireless radio is operating. • **Off**. The 2.4 GHz wireless radio is off.
5 GHz	• **Solid blue**. The 5 GHz wireless radio is operating. • **Off**. The 5 GHz wireless radio is off.
LAN	• **Solid green**. The LAN port has detected a 1 Gbps link with an attached device. • **Solid amber**. The LAN port has detected a 10/100 Mbps link with an attached device. • **Off**. No link is detected on this port.
USB	• **Solid green**. The USB device had been accepted by the router and is ready to be used. • **Blinking green**. The USB device is in use. • **Off**. No USB device is connected, or the **Safely Remove Hardware** button has been clicked and it is now safe to remove the attached USB device.
Wireless button	Pressing this button turns the wireless radios on and off. • **On**. The 2.4 GHz and 5 GHz wireless radios are on. • **Off**. The 2.4 GHz and 5 GHz wireless radios are off, and the 24 GHz and 5 GHz LEDs are off.
WPS button	Pressing this button allows you to use Wi-Fi Protected Setup (WPS) to add a wireless device or computer to your network (see *Wi-Fi Protected Setup (WPS) Method* on page 28. The WPS LED blinks for 2 minutes during this process.

Back Panel

The back panel has the On/Off button and port connections as shown in the figure.

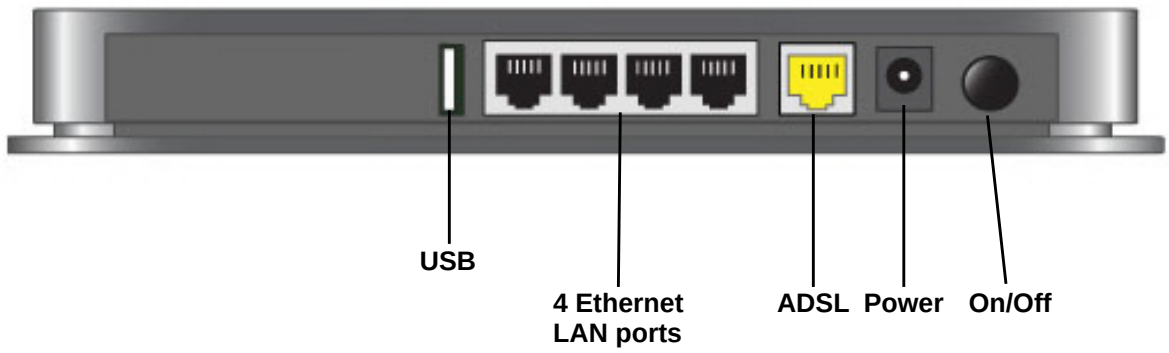


Figure 2. Back panel

Label

The label on the bottom of the wireless router shows the Restore Factory Settings button, WPS PIN, login information, MAC address, and serial number.

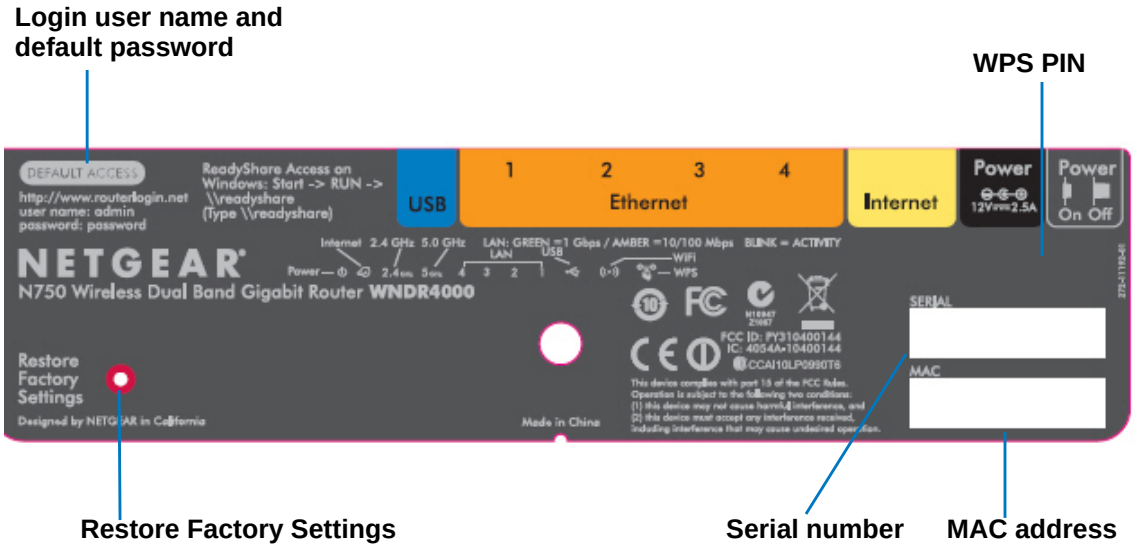
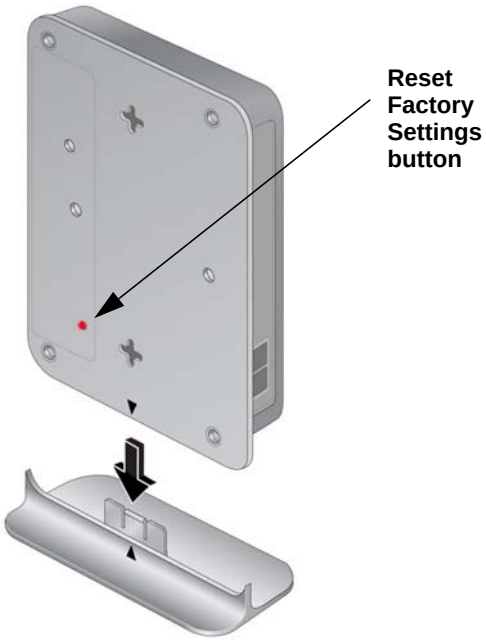


Figure 3. Label on wireless router bottom

See *Factory Settings* on page 94 for information about restoring factory settings.

Router Stand

For optimal wireless network performance, use the stand (included in the package) to position your wireless router upright.



1. Orient your wireless router vertically.
2. Insert the tabs of the stand into the slots on the bottom of your wireless router as shown.
3. Place your wireless router in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).

Position Your Router

The wireless router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your wireless router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your wireless router:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the wireless router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, PCs, or the base of a cordless phone or 2.4 GHz cordless phone.

- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.
- With the antennas in a vertical position to provide the best side-to-side coverage or in a horizontal position to provide the best up-and-down coverage, as applicable.

When you use 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).

Cable Your Router

The installation guide that came in the box has a cabling diagram on the first page. This section walks you through cabling with detailed illustrations.

1. Connect the wireless router, the computer, and the modem.
2. Turn off and unplug the modem. If your modem has a backup battery, remove it as well.
3. Locate the Ethernet cable (**1**) that connects your computer to the modem.

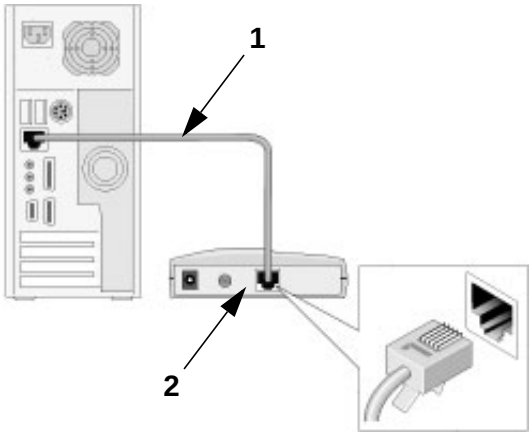


Figure 4. Disconnect the modem from your computer

4. Disconnect the cable from the modem (**2**). You will connect it to the router later.

5. Locate the Ethernet cable that came with the NETGEAR product. Securely insert that Ethernet cable into your modem and into the Internet port of the wireless router (**3**).

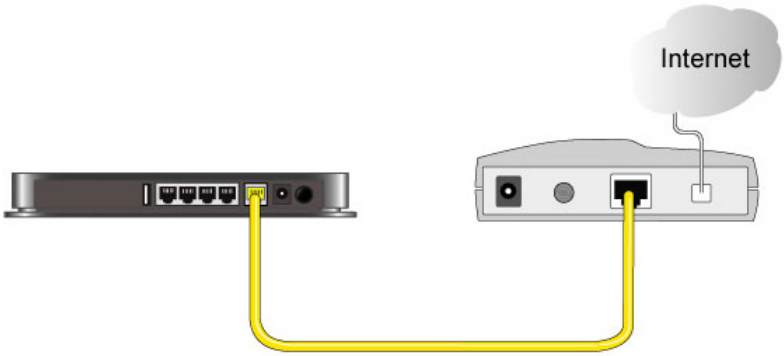


Figure 5. Connect the modem to the router

6. Locate the cable you removed from the modem in step 2. Securely insert that cable (**4**) into a LAN port on the router such as LAN port 1.

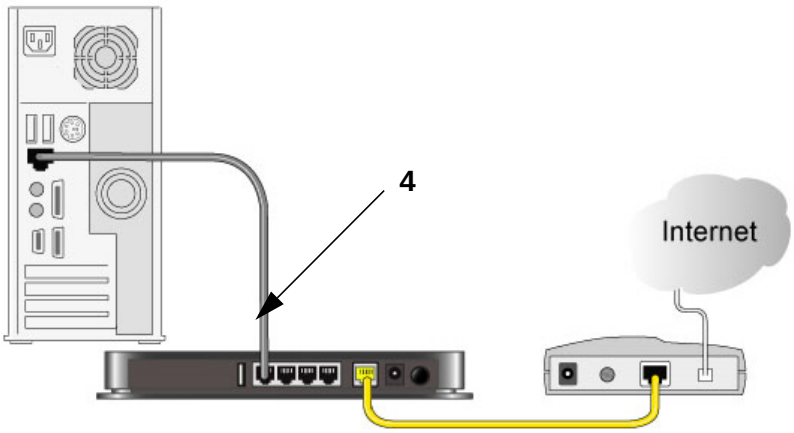


Figure 6. Connect the router to your computer

7. Your network cables are connected, and you are ready to start your network. It is important that you start your network in the correct sequence (first power on the modem, and after it finishes starting up, power on the router).

Verify the Cabling

Verify that your wireless router is cabled correctly by checking the wireless router LEDs. Turn on the wireless router by pressing the **On/Off** button on the back.

- The Power LED is green when the wireless router is turned on.
- The LAN ports are green for each PC cabled to the wireless router by an Ethernet cable.

- The 2.4 GHz N/G-Band LED is on, and the 5.0 GHz N-Band LED is on.
- The Internet LED is on. If it is not, make sure that the Ethernet cable is securely attached to the wireless router Internet port and the modem, and that the modem is powered on.

Verify that the LAN 1 LEDs (1 through 4) are lit for any computers cabled to the wireless router by an Ethernet cable.

Set Up Your Internet Connection

2

This chapter explains how to set up your Internet connection using one of two methods: the Setup Wizard, or manual setup. If you have already set up your wireless router using one of these methods, the initial setup is complete. Refer to this chapter if you want to become familiar with the wireless router menus and screens, view or adjust the initial settings, or change the wireless router password and login time-out.

This chapter contains the following sections:

- *Wireless Router Setup Preparation*
- *Log In to the Router*
- *Upgrade Firmware*
- *Router Interface*
- *Setup Wizard*
- *Manual Setup (Basic Settings)*
- *Unsuccessful Internet Connection*
- *Change Password*
- *Log Out Manually*
- *Types of Logins*

Wireless Router Setup Preparation

You can set up your wireless router with the Setup Wizard as described in *Setup Wizard* on page 19, or manually as described in *Manual Setup (Basic Settings)* on page 20. However, before you start the setup process, you need to have your ISP information and to make sure the laptops, PCs, and other devices in the network have the settings described here.

Note: For a Macintosh or Linux system, you have to use manual setup.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you have to change the settings back so that it uses Dynamic Host Configuration Protocol (DHCP).

Replace an Existing Router

To replace an existing router, disconnect it and set it aside before starting the wireless router setup.

Gather ISP Information

You need the following information to set up your wireless router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your wireless router Internet connection is set up, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your wireless router automatically logs you in.

- Active Internet service provided by a DSL account
- The ISP configuration information for your DSL account
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
  - Host and domain names

Depending on how your ISP set up your Internet account, you could need to know one or more of these settings for a manual setup:

- Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
- Multiplexing method
- Host and domain names

Log In to the Router

Log in to the wireless router to view or change settings or to set up the wireless router.

1. Type **wwww.routerlogin.net** in the address field of your browser and press **Enter** to display the login window.

2. Enter **admin** for the user name and **password** for the password, both in lowercase letters.

Note: The wireless router user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 24 for more information.

The wireless router screen displays as described in *Router Interface* on page 18.

If you do not see the login prompt:

1. Check the LEDs on the wireless router front panel to make sure that the wireless router is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the wireless router is connected to a LAN port.
2. If you connected the Ethernet cable and quickly launched your browser and typed in the wireless router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the wireless router wirelessly, NETGEAR recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the wireless router.
4. If you cannot connect to the wireless router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation.

Upgrade Firmware

When you log in, if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest firmware. See *Upgrade the Firmware* on page 50, for more information about upgrading firmware.

Click **Yes** to check for new firmware (recommended). The wireless router checks the NETGEAR database for new firmware.

- If no new firmware is available, click **No** to exit. You can check for new firmware later.
- If new firmware is available, click **Yes** to upgrade the wireless router with the latest firmware. After the upgrade, the wireless router restarts.

CAUTION:

Do not try to go online, turn off the wireless router, shut down the computer, or do anything else to the wireless router until the wireless router finishes restarting and the Power LED has stopped blinking for several seconds.

You cannot upgrade firmware until you have established your Internet connection as described in *Setup Wizard* on page 19.

Router Interface

The wireless router interface lets you view or change the wireless router settings. The left column has menus, and the right column provides online help. The middle column is the screen for the current menu option.

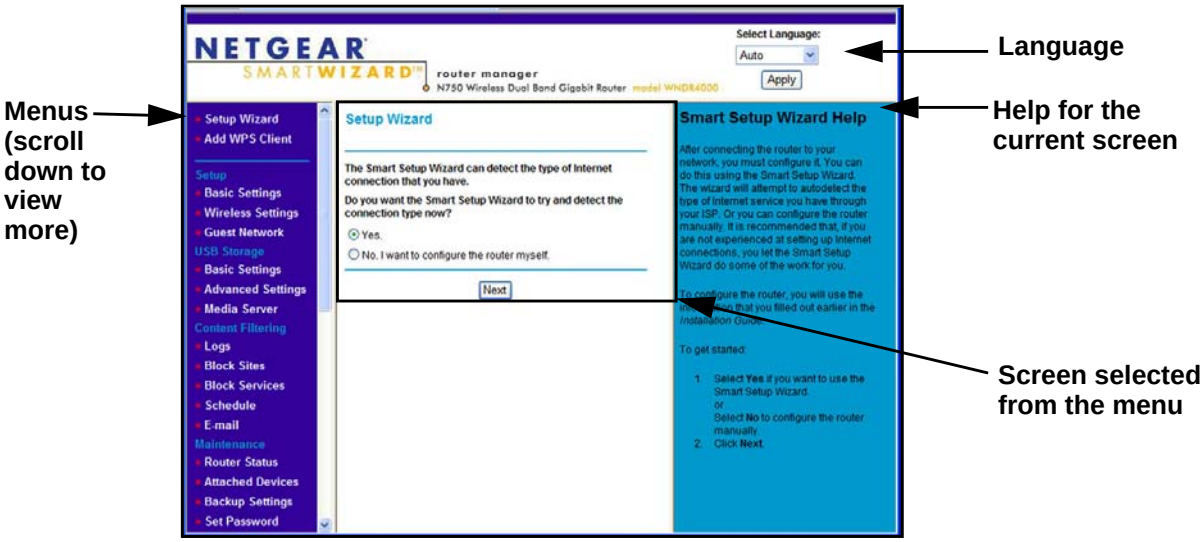


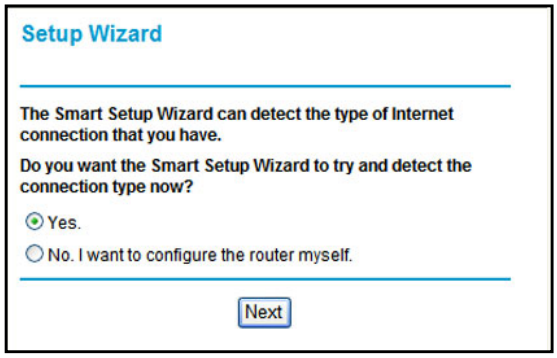
Figure 1. Router interface

- **Setup Wizard**. Specify the language and location, and automatically detect the Internet connection. See *Setup Wizard* on page 19.
- **Add WPS Client**. Add WPS-compatible wireless devices and other equipment to your wireless network. See *Wi-Fi Protected Setup (WPS) Method* on page 28.
- **Setup menu**. Set, upgrade, and check the ISP and wireless network settings of your wireless router. See *Manual Setup (Basic Settings)* on page 20 and *Chapter 3, Wireless Settings* for information about settings.
- **Content Filtering menu**. View and configure the wireless router firewall settings to prevent objectionable content from reaching your PCs. See *Chapter 4, Content Filtering Settings*.
- **Maintenance menu**. Administer and maintain your wireless router and network. See *Chapter 5, Network Maintenance*.
- **Advanced menu**. Set the wireless router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 7, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.
- **Web Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Setup Wizard

If you do not use the NETGEAR Genie, you have to log in to the wireless router to set the country, language, and Internet connection. If you performed the NETGEAR Genie setup, the country, language, Internet, and wireless network settings are already configured.

1. From the top of the wireless router menu, select **Setup Wizard** to display the following screen:



2. Select either **Yes** or **No, I want to configure the router myself**. If you selected No, proceed to *Manual Setup (Basic Settings)* on page 20.
3. If you selected Yes, click **Next**.

   With automatic Internet detection, the Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

Note: The Setup Wizard cannot detect a Point-to-Point Tunneling Protocol (PPTP) connection. If your ISP uses PPTP, you have to set your Internet connection through the screen described in *Manual Setup (Basic Settings)* on page 20.

Manual Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the router myself in the Setup Wizard and is also available from the wireless router menu. It is where you view or change ISP information. The fields that display vary depending on whether or not your Internet connection requires a login.

Note: Check that the country is set as described *Setup Wizard* on page 19 before proceeding with the manual setup.

1. Select **Set Up > Basic Settings**, and select **Yes** or **No** depending on whether or not your ISP requires a login. *Figure 2, Basic Settings screen without (left) and with (right) login* shows both forms of the Basic Settings screen.
   - **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, as needed.
2. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the DSL settings, and see *Unsuccessful Internet Connection* on page 23 for more information.
3. If no login is required, you can specify the MAC Address setting.
4. Click **Apply** to save your settings.

5. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, and see *Chapter 8, Troubleshooting*.

ISP *does not* require login **ISP *does* require login**

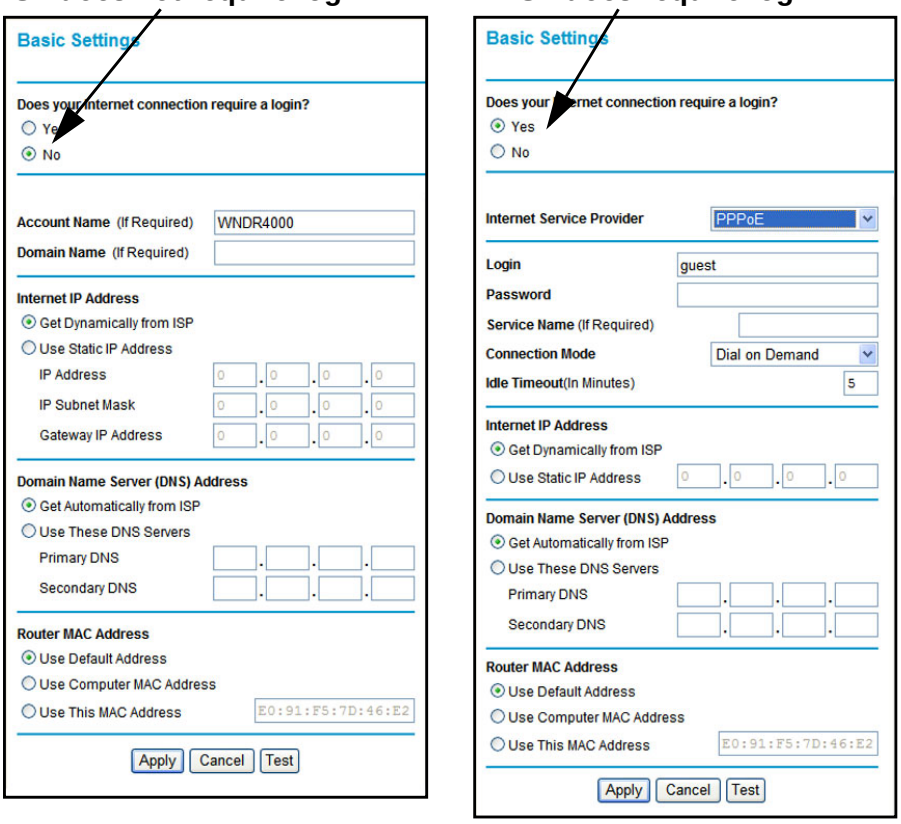


Figure 2. Basic Settings screen without (left) and with (right) login

Some of the fields in this screen change when you select the Yes or No radio button for an ISP login.

- **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
- **No**. Enter the account and domain names, as needed.

No ISP Login

- **Account Name**. Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name**. Enter the domain name provided by your ISP.

ISP Login

- **Internet Service Provider**.

  PPTP (Point-to-Point Tunneling Protocol). This is used primarily in Austrian DSL services.

Telstra Bigpond. This setting is only for older cable modem service accounts that still require a Bigpond login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cable modem accounts should select **No** for Does your Internet connection require a login?.

Other. This is the default setting. It is for PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide.

- **Login**. The login name provided by your ISP. This is often an e-mail address.
- **Password**. The password provided by your ISP.
- **Service Name**. If your ISP provided a service name, enter it here.
- **Connection Mode**. Specify when the router will connect to and disconnect from the Internet.

  Always On. The router logs in to the Internet immediately after booting and never disconnects.

  Dial on Demand. The router logs in only when outgoing traffic is present and logs out after the idle time-out.

  Manually Connect. The router logs in or logs out only when you click **Connect** or **Disconnect** in the Router Status screen.

- **Idle Timeout**. If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.
- **Internet IP Address**

  Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.

  Use Static IP Address. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's wireless router to which your wireless router will connect.

Domain Name and MAC Address Fields

- **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 servers. Your ISP automatically assigns this address.

  Use These DNS Servers. If you know that your ISP does not automatically transmit DNS addresses to the wireless router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

- **Router MAC Address**. The Ethernet MAC address that will be used by the wireless router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept

traffic only from the MAC address of that computer. This feature allows your wireless router to masquerade as that computer by “cloning” its MAC address.

Use Default Address. Use the default MAC address of the router (normally the LAN MAC address).

Use Computer MAC Address. The wireless router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP.

Use This MAC Address. Enter the MAC address that you want to use.

Unsuccessful Internet Connection

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.
4. If you cannot connect to the wireless router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation.

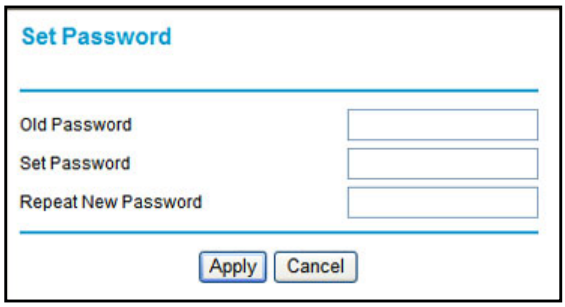
Change Password

For security reasons, the wireless router has its own user name of admin with a password that defaults to password. You can and should change the password to a secure password that is easy to remember. The ideal password contains no dictionary words from any language and is a mixture of upper-case and lower-case letters, numbers, and symbols. It can be up to 30 characters.

Note: The wireless router user name and password are not the same as the user name and password for logging in to your Internet connection. See *Types of Logins* on page 24 for more information about login types.

To change the password:

1. Select **Maintenance > Set Password** to display the following screen:



2. Enter the old password.
3. Enter the new password twice.
4. Click **Apply** to save your changes.

   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. See *Back Up* on page 52 for information about backing up your network configuration.

Log Out Manually

The wireless router interface provides a Logout command at the bottom of the wireless router menus. Log out when you expect to be away from your computer for a relatively long period of time.

Types of Logins

There are three separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Router login** logs you in to the wireless router interface. See *Log In to the Router* on page 17 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wi-Fi network name and passphrase** logs you in to your wireless network. This login can be found on the label on the bottom of your unit. See *Chapter 3, Wireless Settings* for more information.

Wireless Settings

3

This chapter describes how to use the Wireless Settings screens to view and change (if needed) your wireless network settings. Security features to prevent objectionable content from reaching your PCs are covered in *Chapter 4, Content Filtering Settings*.

This chapter contains the following sections:

- *Wireless Security Compatibility*
- *Security Basics*
- *Add Clients (Computers or Devices) to Your Network*
- *Wireless Settings Screen*
- *Wireless Guest Networks*

Wireless Security Compatibility

A wireless client is the wireless device or computer that will connect to your wireless router. Most PCs and laptops come with a wireless adapter installed, but if it is outdated or slow, you can purchase a new wireless USB adapter to plug into a USB port. Make sure the wireless adapter in each client in your wireless network supports WPA or WPA2 wireless security.

Note: If you connect devices to your wireless router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 28, those devices assume the security settings of the wireless router.

Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to use the security features available to you. Your wireless router has the security features described here and in *Chapter 4, Content Filtering Settings*.

- Wireless security options
- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption. WPA2 is the latest and most secure, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. Note that it is also possible to use your router without wireless security. NETGEAR does *not* recommend this. You can view or change the wireless security options in the Wireless Settings screen. See *Wireless Settings Screen* on page 29.

Turn Off Wireless Connectivity

You can turn off the wireless connectivity of the wireless router by pressing the Wireless **On/Off** button on its front panel . For example, if you use your laptop to wirelessly connect to your wireless router and you take a business trip, you can turn off the wireless portion of the wireless router while you are traveling. Other members of your household who use computers connected to the wireless router through Ethernet cables can still use the wireless router.

Disable SSID Broadcast

By default, the wireless router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices will not find your wireless router unless they are configured with the same SSID.

Note: Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific PCs based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the wireless router. The wireless station MAC address filtering adds additional security protection to the wireless security option that you have in force. The access list determines which wireless hardware devices are allowed to connect to the wireless router by MAC address. See *Advanced Wireless Settings* on page 74 for the procedure.

Add Clients (Computers or Devices) to Your Network

Choose either the manual or the WPS method to add wireless computers or devices to your wireless network.

Manual Method

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your wireless router. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default Wi-Fi network name (SSID) and select it. The default Wi-Fi network name (SSID) is located on the product label on the bottom of the wireless router.
3. Enter the wireless router passphrase and click **Connect**. The default wireless router passphrase is located on the product label on the bottom of the wireless router.
4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard that lets you easily join a secure wireless network with WPA or WPA2 wireless security. The wireless router automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.[1]

Note: If the wireless network name (SSID) changes each time you add a WPS client, the Keep Existing Wireless Settings check box on the Advanced Wireless Settings screen has been cleared. See *Advanced Wireless Settings* on page 74 for more information about this setting.

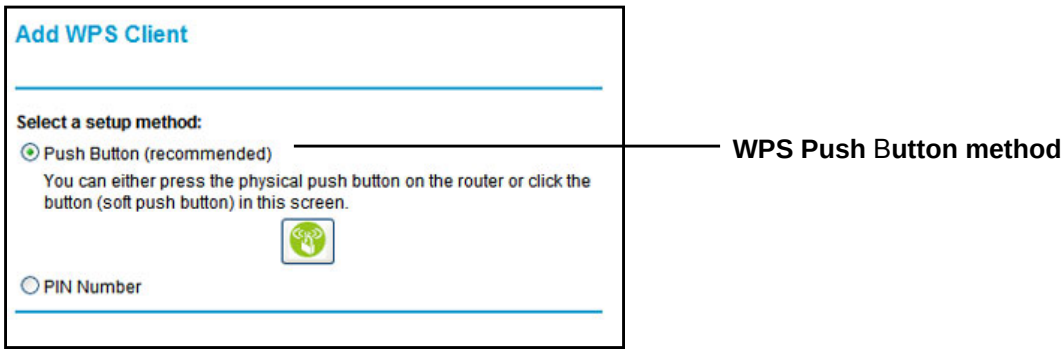
You can use a WPS button or the wireless router interface method to add wireless computers and devices to your wireless network.

WPS Button Method

1. Press the **WPS** button on the wireless router front panel.
2. Within 2 minutes, press the **WPS** button on your wireless computer or device, or follow the WPS instructions that came with the computer. The device is now connected to your wireless router.
3. Repeat steps 1–2 to add other WPS wireless computers or devices.

Router Interface Method

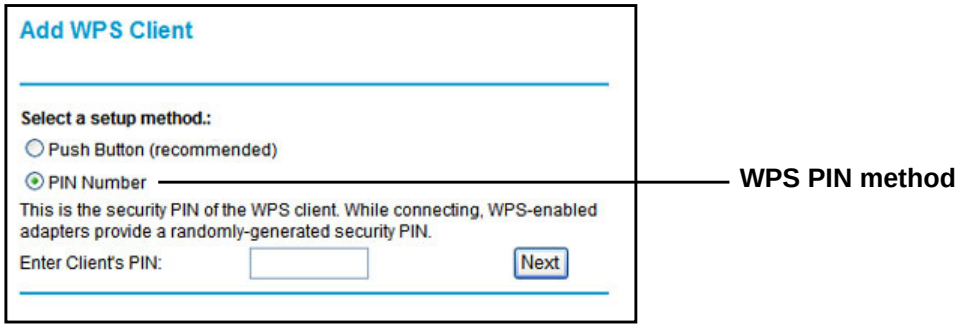
1. Select **Add WPS Client** at the top of the wireless router menus.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



3. Select either **Push Button** or **PIN Number**. With either method, the wireless router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.

1. For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org.

The PIN method displays this screen so you can enter the client security PIN number:



While the wireless router attempts to connect, the WPS LED on the front of the wireless router blinks green. When the wireless router establishes a WPS connection, the LED is solid green, and the wireless router WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

Wireless Settings Screen

The Wireless Settings screen lets you view or change the wireless network settings. When you set up security, note the new settings and save them in a secure location.

Note: If you use a wireless computer to change the wireless network name (SSID) or security options, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the wireless router.

Consider Every Device on Your Network

Before you begin, check the following:

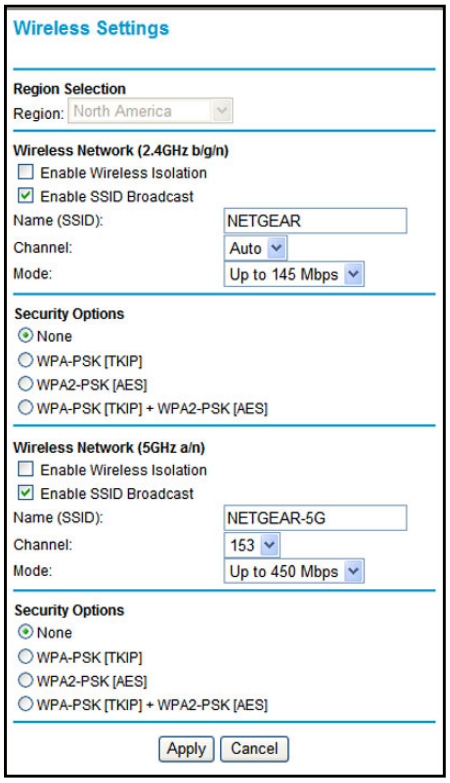
- Every wireless computer has to be able to obtain an IP address by DHCP from the wireless router as described in *Use Standard TCP/IP Properties for DHCP* on page 16.
- Each computer or wireless adapter in your network has to have the same SSID and wireless mode (bandwidth/data rate) as the wireless router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network has to match the wireless router. For example, if you select a security option that requires a passphrase, be sure to use same passphrase for each wireless computer in the network.

View or Change Wireless Settings

Your wireless router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your wireless router. You view or change these settings in the Wireless Settings screen. You can also use this screen to set up guest wireless networks.

To view or change wireless settings:

1. Select **Setup > Wireless Settings** to display the following screen.



2. Select the wireless network that you want to configure.
3. Make any changes that are needed, and click **Apply** when done to save your settings.

> **Note:** The screen sections, settings, and procedures are explained in the following sections.

4. Set up and test your computers for wireless connectivity:
   a. Use your wireless computer or device to join your network. When prompted, enter the network password.
   b. From the wirelessly connected computer, make sure that you can access the Internet.

Wireless Settings Screen Fields

Region

The location where the wireless router is used. It might not be legal to operate the wireless router in a region other than the regions listed.

Wireless Network (for 2.4 GHz b/g/n and 5 GHz a/n)

The primary network is the one that you usually use. You can set up guest networks too. You can customize access so that people who use their computers to access your guest network can use the Internet, but they do not have access to the rest of your home network.

- **Enable Wireless Isolation**. When this check box is selected, wireless stations cannot communicate with each other or with stations on the wired network. By default, this check box is not selected.
- **Enable SSID Broadcast**. This setting allows the wireless router to broadcast its SSID so that a wireless station can display this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear this check box and click **Apply**.
- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID for your primary network is randomly generated, and there is typically no need to change it. If you want to set up guest networks, NETGEAR does recommend that you customize the default guest network names (SSIDs).
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.
- **Mode**. Up to 150 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. NETGEAR recommends that you set up wireless security for your primary network and wireless router and for each guest network that you plan to use.

- **None**. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security.
- **WPA-PSK [TKIP]** (WiFi Protected Access Pre-Shared Key). Allow only computers configured with WPA to connect to the wireless router. When you select this option, this additional area displays. Enter the WPA passphrase (network key). The passphrase has to be between 8 and 63 ASCII characters or exactly 64 hex digits.
- **WPA2-PSK [AES]** (Wi-Fi Protected Access with 2 Pre-Shared Keys). Allow only computers set up with WPA2 to connect to the wireless router. When you select this option, this additional area displays. Enter the WPA passphrase (network key). The passphrase has to be between 8 and 63 ASCII characters or exactly 64 hex digits.

- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. Allow computers set up with either WPA-PSK or WPA2-PSK security to connect to the wireless router. When you select this option, this additional area displays on your screen. Enter the WPA passphrase (network key). The passphrase has to be between 8 and 63 ASCII characters or exactly 64 hex digits.

Set Up WPA Security Option and Passphrase

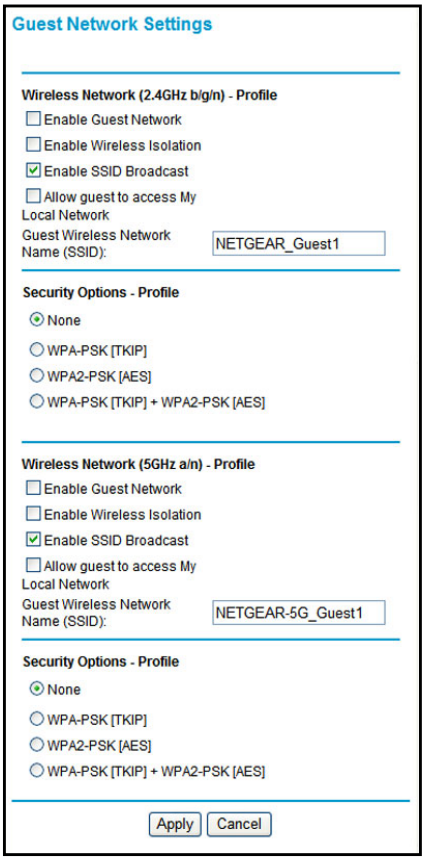
1. In the Security Options section, select the WPA option that you want.
2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.
3. Click **Apply**.

Wireless Guest Networks

Adding a guest network allows visitors at your home to use the Internet without having to know your wireless security key. You can add a guest network to each wireless network, b/g/n 2.4 GHz or a/n 5 GHz. You can configure wireless guest networks and specify the security options for each wireless guest network.

To set up a wireless guest network:

1. Select **Setup > Guest Network**. The following screen displays:



2. Select the **Enable Guest Network** check box to enable each guest network that you want to use. Both 2.4 GHz b/g/n) and 5 GHz a/n are available.
3. Specify the settings for the network.

   You can specify whether the SSID broadcast is enabled, and whether you want to allow guests to access your local network. You can also change the SSID.

   - NETGEAR strongly recommends that you change the SSID to a different name. Note that the SSID is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.
   - For guest networks, wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
4. Select a security option for the guest network and specify the password.
5. When you have finished making changes, click **Apply**.

Content Filtering Settings

4

This chapter explains how to use the basic firewall features of the wireless router to prevent objectionable content from reaching the PCs and other devices connected to your network.

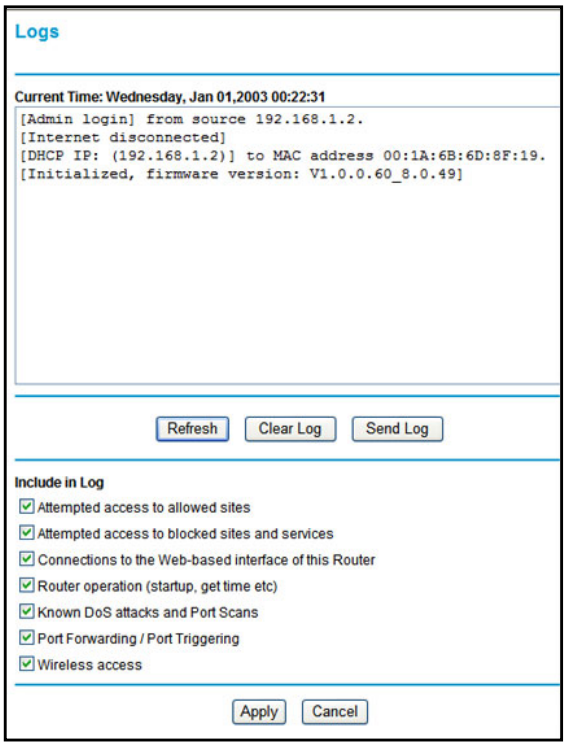
This chapter contains the following sections:

- *Logs*
- *Keyword Blocking of HTTP Traffic*
- *Block Services*
- *Set the Time Zone*
- *Schedule Services*
- *Turn On Security Event Email Notification*
- *Port Forwarding*
- *Port Triggering*

Logs

The wireless router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites screen, the Logs screen show you when someone on your network tries to access a blocked site. If you enable email notification, you will receive these logs in an email message.

To view the log, select **Content Filtering > Logs**. A screen similar to the following displays:



The Include in Log check boxes allow you to select which events are logged. The security log entries include the following information:

- **Date and time**.The date and time the log entry was recorded.
- **Description or action**. The type of event and what action was taken, if any.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Source port and interface**. The service port number of the initiating device, and whether it originated from the LAN or WAN.
- **Destination**. The name or IP address of the destination device or website.
- **Destination port and interface**. The service port number of the destination device, and whether it is on the LAN or WAN.

Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the time stamp as day, year-month-date hour:minute:second.

Activation and Administration

```
Tue, 2010-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2010-05-21 18:55:00 - Administrator login successful-IP:192.168.0.2
Thu, 2010-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

[This entry shows an administrator logging into and out from IP address 192.168.0.2.]

```
Tue, 2010-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2010-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

Dropped Packets

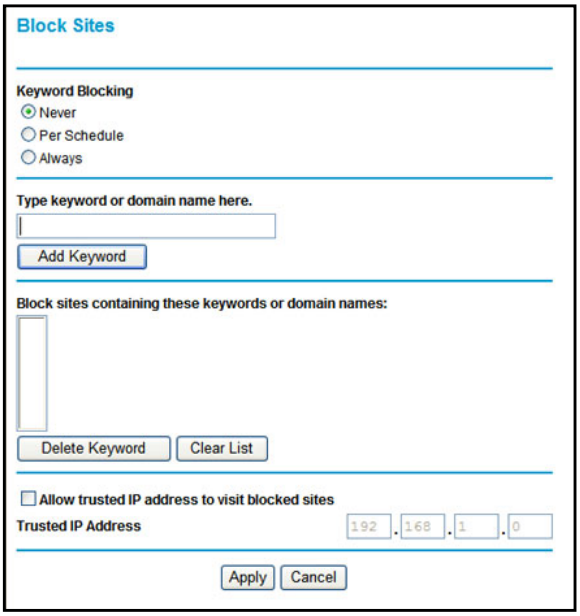
```
Wed, 2010-05-22 07:15:15 - TCP packet dropped -
Source:64.12.47.28,4787,WAN - Destination:134.177.0.11,21,LAN - [Inbound
Default rule match]
Sun, 2010-05-22 12:50:33 - UDP packet dropped -
Source:64.12.47.28,10714,WAN - Destination:134.177.0.11,6970,LAN -
[Inbound Default rule match]
Sun, 2010-05-22 21:02:53 - ICMP packet dropped -
Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound Default rule
match]
```

These entries show an inbound FTP (port 21) packet, a User Datagram Protocol (UDP) packet (port 6970), and an Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a scheduled.

1. Select **Security > Block Sites**.The following screen displays:



2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The Keyword list. supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

Delete Keyword or Domain

1. Select the keyword or domain that you want to delete from the list.
2. Click **Delete Keyword** and click **Apply** to save your changes.

Specify a Trusted Computer

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

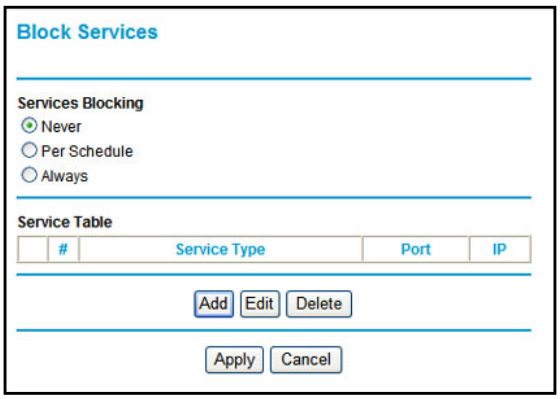
Block Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

You can block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can add an outbound rule to block Internet access from a local computer based on the computer, Internet site, time of day, and type of service.

To block access to Internet services:

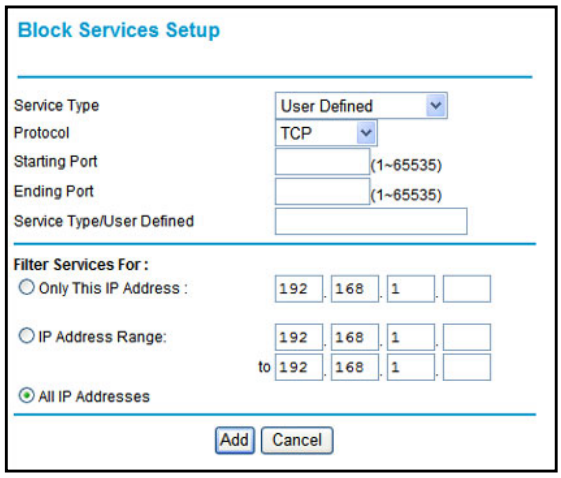
1. Select **Content Filtering > Block Services**. The Block Services screen displays.



2. Enable service blocking by selecting either **Per Schedule** or **Always**, and then click **Apply**.

   To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see *Schedule Services* on page 41.

3. Specify a service for blocking by clicking **Add**. The Block Services Setup screen displays.



4. From the Service Type list, select the application or service to be allowed or blocked. The list includes several common services, but you are not limited to these choices. To add any services or applications that are not listed, select **User Defined**.

   Note: *To define a service, first you have to know the port number or range of numbers used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force* (IETF at *http://www.ietf.org/*) *and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.*

   - If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
   - Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

5. Select the radio button for the IP address configuration that you want to block, and then enter the IP addresses in the appropriate fields.

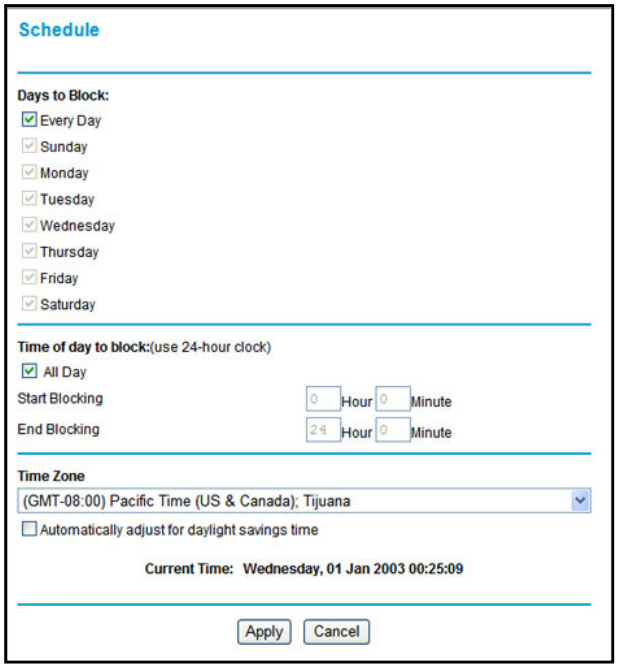
   You can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

6. Click **Add** to enable your Block Services Setup selections.

Set the Time Zone

The wireless router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

1. Select **Security > Schedule**. The following screen displays



2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.
3. If your time zone is in daylight savings time, select the **Automatically adjust for daylight savings time** check box to add one hour to standard time.

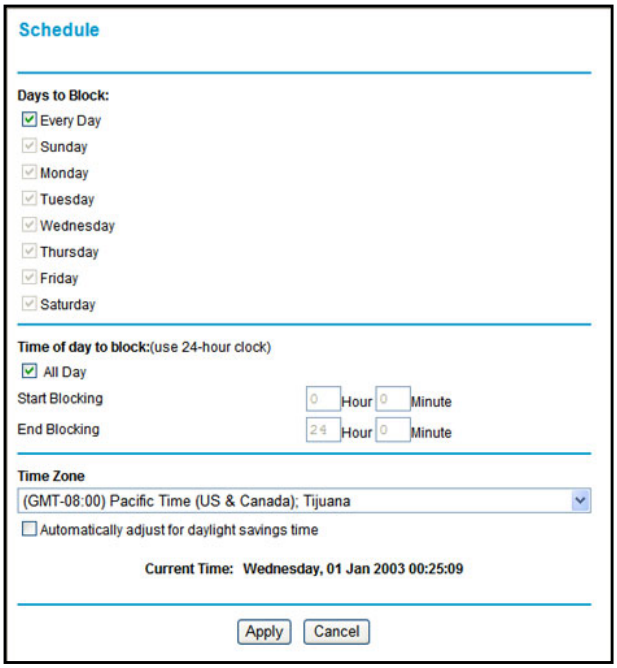
   Note: *If your region uses daylight savings time, select* ***Automatically adjust for daylight savings time*** *on the first day and clear it after the last day.*

4. Click **Apply** to save your settings.

Schedule Services

If you enabled service blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Select **Security > Schedule**. The following screen displays:



2. To block Internet services based on a schedule, select **Every Day** or select one or more days.
3. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the Start Blocking and End Blocking fields.

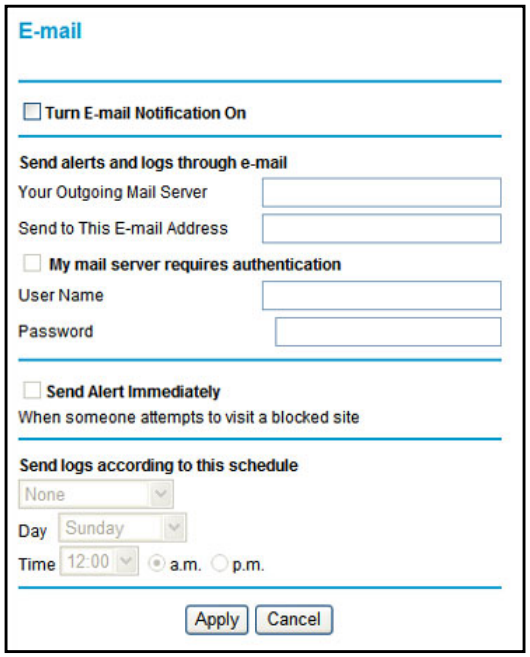
   Note: *Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.*

4. Click **Apply** to save your settings.

Turn On Security Event Email Notification

To receive logs and alerts by email, provide your email information in the Email screen and specify which alerts you want to receive and how often.

Select **Content Filtering > E-mail** to display the following screen:



- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the wireless router.
- **Send to This E-mail Address**. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **Your Outgoing Mail Server**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **My mail server requires authentication**. If you use an outgoing mail server provided by your current ISP, you do not need to select this check box. If you use an email account that is not provided by your ISP, select this check box, and enter the required user name and password information.
- **Send Alerts Immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

- **Days** specifies which day of the week to send the log. This is relevant when the log is sent weekly.
- **Time** specifies the time of day to send the log. This is relevant when the log is sent daily or weekly.

Note: If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the wireless router's memory. If the wireless router cannot email the log file, the log buffer might fill up. In this case, the wireless router overwrites the log and discards its contents.

Port Forwarding

Because the wireless router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, with port forwarding you can make a local server (for example, a Web server or game server) visible and available to the Internet.

Note: Some residential broadband ISP accounts do not let you run server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Port forwarding tells the wireless router to direct inbound traffic for a particular service to one local server based on the destination port number. Port forwarding opens holes in your firewall. Enable only those ports that are necessary for your network.

Before starting, you need to determine which type of service, application, or game you will provide, and the local IP address of the computer that will provide the service. Be sure the computer's IP address never changes.

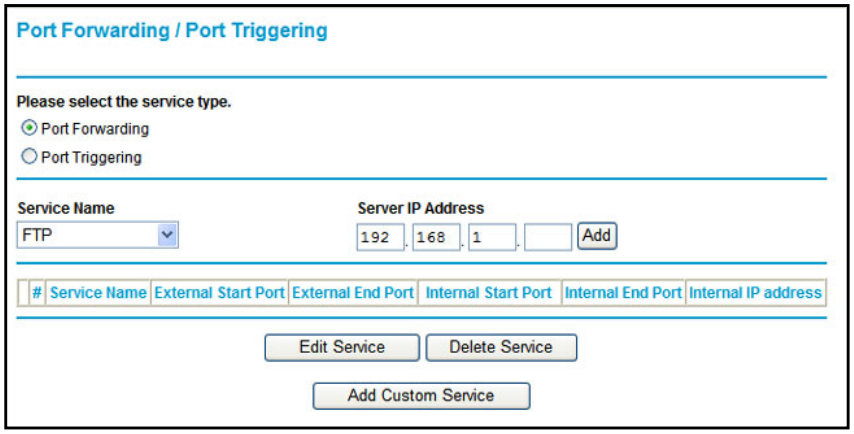
The following are some considerations for port forwarding:

- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen described in *Dynamic DNS* on page 75 so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN Setup screen to keep the computer's IP address constant.

- Local computers access the local server using the computer's local LAN address. Attempts by local computers to access the server using the external WAN IP address fail.

To configure port forwarding to a local server:

1. Select **Advanced > Port Forwarding/Port Triggering**.
2. Select the **Port Forwarding** radio button as the service type as shown in the following figure:



3. From the Service Name list, select the service or game that you will host on your network.

   If the service does not appear in the list, you can add a custom service as described in the following section..
4. In the Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
5. Click **Add**. The service appears in the list in the screen.

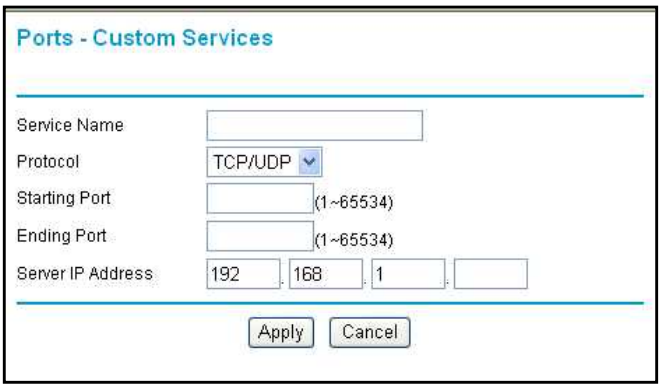
Note: To edit or delete a port forwarding entry in the table, select the button next to the service name and click **Edit Service** or **Delete Service**.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you need to know which port number or range of numbers is used by the application. You can usually find out by contacting the publisher of the application or user groups or newsgroups.

To add a custom service:

1. On the Port Triggering screen, click the **Add Custom Service** button. The following screen displays:



2. In the Service Name field, enter a descriptive name.
3. In the Protocol field, select the protocol. If you are unsure, select **TCP/UDP**.
4. In the Starting Port field, enter the first port number.
   - If the application uses only a single port, enter the same port number in the Ending Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
5. In the Server IP Address field, enter the IP address of your local computer that will provide this service.
6. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Application Example: Making a Local Web Server Public

If you host a Web server on your local network, you can use port forwarding to allow Web requests from anyone on the Internet to reach your Web server.

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP address reservation, as explained in *IP Address Reservation* on page 72. In this example, your router will always give your Web server an IP address of 192.168.1.33.
2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your Web server at **192.168.1.33**.

   HTTP (port 80) is the standard protocol for Web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in *Dynamic DNS* on page 70.

   To access your Web server from the Internet, a remote user needs to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS

service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound “trigger” port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

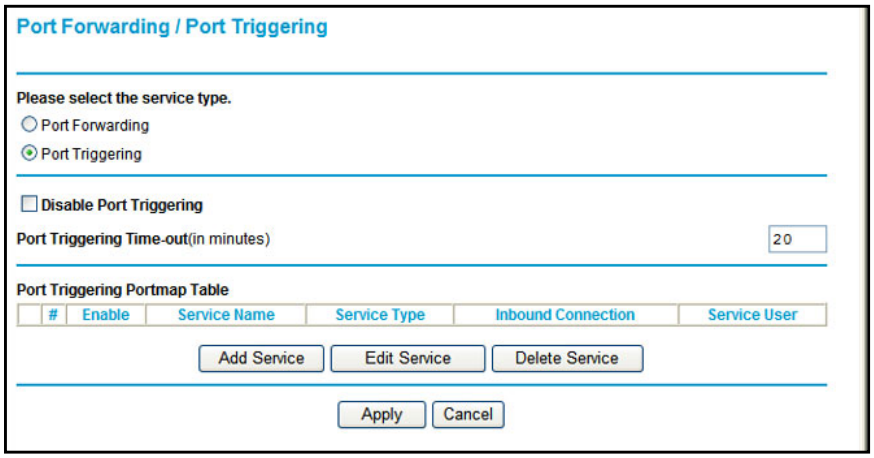
Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 80.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

To set up port triggering:

1. Select **Advanced > Port Forwarding/Port Triggering**. The Forwarding/Port Triggering screen displays.

2. Select the **Port Triggering** radio button. The port triggering information displays.

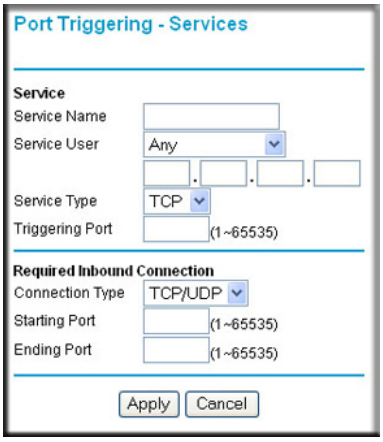


3. Clear the **Disable Port Triggering** check box.

   If you set up port triggering and then select the **Disable Port Triggering** check box, port triggering is disabled, but the port triggering set up is retained even though it is not used.

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add Service** to display the following screen:



6. In the Service Name field, type a descriptive service name.

7. In the Service User field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.

9. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Network Maintenance

5

This chapter describes the wireless router settings for administering and maintaining the wireless router and home network.

This chapter contains the following sections:

- *Upgrade the Firmware*
- *Manually Check for Firmware Upgrades*
- *Manage the Configuration File*
- *View Router Status*
- *View Attached Devices*

Upgrade the Firmware

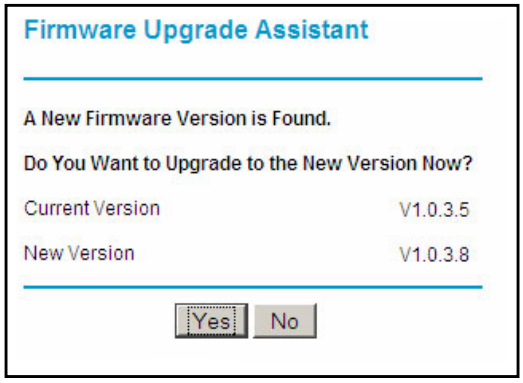
The wireless router firmware (routing software) is stored in flash memory. By default, when you log in to your wireless router, it checks the NETGEAR website for new firmware and alerts you if there is a newer version.

WARNING!

When uploading firmware to the wireless router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

Automatic Firmware Check

When automatic firmware checking is on, the wireless router performs the check and notifies you if an upgrade is available or not as shown here.



1. Click **Yes** to allow the wireless router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your wireless router restarts.
2. Go to the WNDR4000 support page at *http://www.netgear.com/support.* and read the new firmware release notes to determine whether you need to reconfigure the wireless router after upgrading.

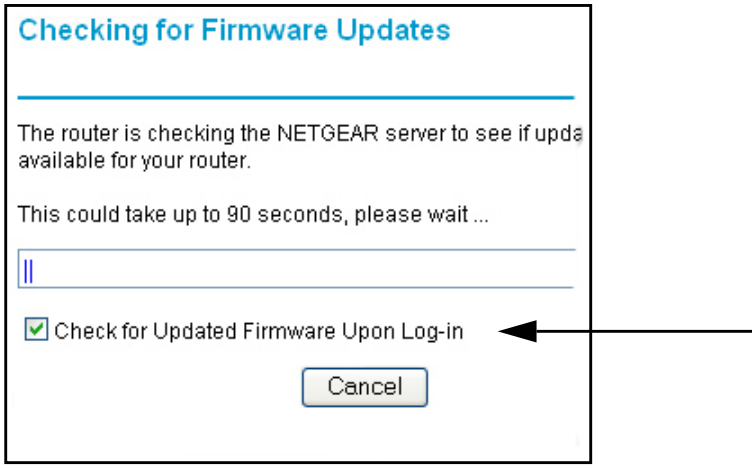
Note: If you get a “Firmware needs to be reloaded” message, it means that a problem has been detected with the wireless router’s firmware. Follow the prompts to correct the problem, or see *Incorrect Date or Time* on page 92 for a description of the steps.

Stop the Automatic Firmware Check

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See the following section, *Manually Check for Firmware Upgrades* .

To turn off the automatic firmware check at login:

1. Select **Maintenance > Router Upgrade**. The following screen displays:



2. Clear the **Check for Updated Firmware Upon Log-in** check box.

Manually Check for Firmware Upgrades

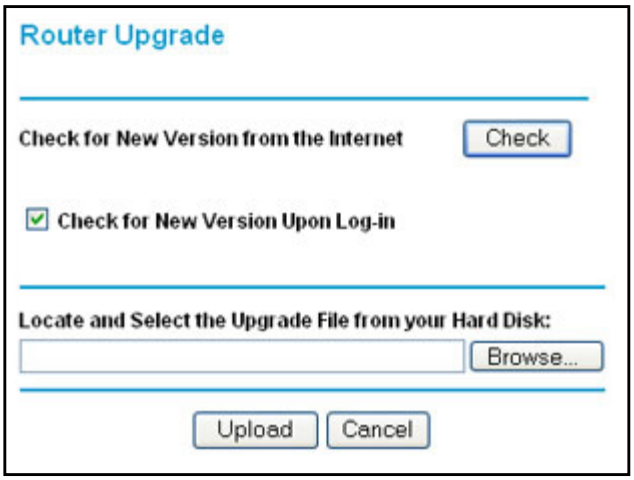
You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

WARNING!

When uploading firmware to the wireless router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

1. Select **Maintenance > Router Status** and make a note of the wireless router firmware version number.
2. Go to the WNDR4000 support page on the NETGEAR website at *http://www.netgear.com/support.*
3. If the firmware version on the NETGEAR website is newer than the firmware on your wireless router, download the file to your computer.

4. Select **Maintenance > Router Upgrade** to display the following screen:



5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img).
6. Click **Upload** to send the firmware to the wireless router.

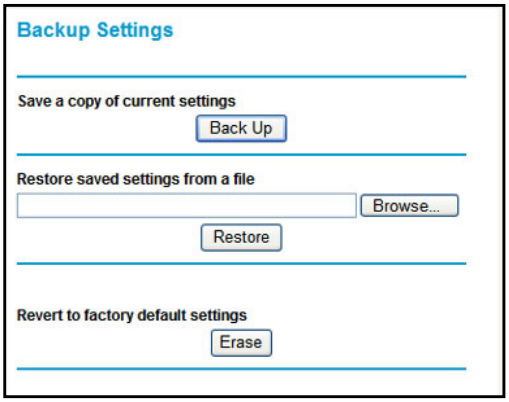
   When the upload is complete, your wireless router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the wireless router after upgrading.

Manage the Configuration File

The wireless router configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or used to revert to factory default settings.

Back Up

1. Select **Maintenance > Backup Settings** to display the following screen:



2. Click **Save** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the wireless router.

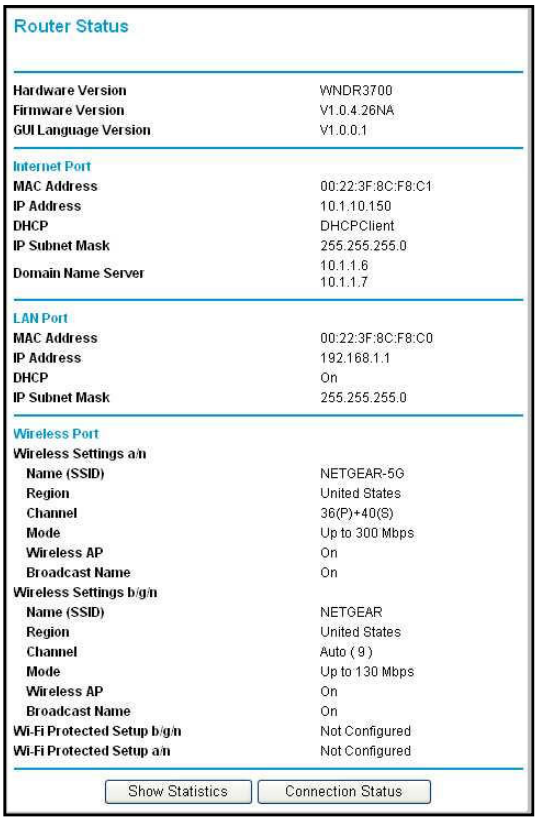
Upon completion, the wireless router reboots.

Erase

Click the **Erase** button to reset the wireless router to its factory default settings. Erase sets the password to **password**, and the LAN IP address to **192.168.1.1**, and enables the wireless router's DHCP.

View Router Status

Select **Maintenance > Router Status** to display this screen. The Router Status screen provides status and usage information.



Hardware and Firmware Version. The model of the hardware and the currently running firmware version.

GUI Language Version. The currently selected language.

Internet Port Settings

MAC Address. The Ethernet MAC address of the DSL port.

IP Address. The DSL port IP address. If no address is shown, the wireless router cannot connect to the Internet.

DHCP. Usually this is set to DHCP Client because the router obtains an IP address dynamically from the ISP. If set to None, the router uses a fixed IP address on the WAN.

IP Subnet Mask. The DSL port IP subnet mask.

Gateway IP Address. The IP address used as a gateway to the Internet for computers configured to use DHCP.

Domain Name Server. The wireless router DNS server IP addresses. These addresses are usually obtained dynamically from the ISP.

LAN Port (Local Ports)

MAC Address. The wireless router LAN port Ethernet MAC address.

IP Address. The wireless router LAN port IP address. The default is 192.168.1.1.

DHCP. If Off, the wireless router does not assign IP addresses to PCs on the LAN. If On, the wireless router does assign IP addresses to PCs on the LAN.

IP Subnet Mask. The IP subnet mask used by the wireless router LAN. The default is 255.255.255.0.

Wireless Port

See *Wireless Settings Screen* on page 29 for a more detailed description of these settings.

Name (SSID). The Wi-Fi network name (SSID) for the wireless network. The default for a or n operation is NETGEAR-5G. The default for b or g operation is NETGEAR.

Region. The country where the unit is set up for use.

Channel. The current channel, which determines the operating frequency.

Mode. The current Mbps setting.

Wireless AP. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

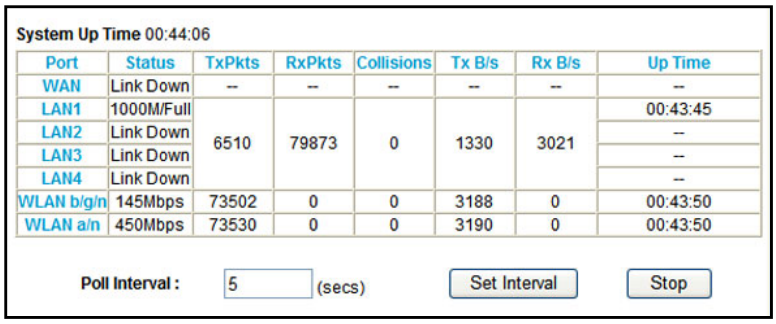
Broadcast Name. Indicates if the wireless router is configured to broadcast its SSID.

Wi-Fi Protected Setup b/g/n. This indicates whether Wi-Fi Protected Setup is configured for the b/g/n network.

Wi-Fi Protected Setup a/n. Indicates whether Wi-Fi Protected Setup is configured for the a/n network.

Show Statistics

Click the **Show Statistics** button on the Router Status screen to display a screen similar to this:



System Up Time 00:44:06

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link Down	--	--	--	--	--	--
LAN1	1000M/Full	6510	79873	0	1330	3021	00:43:45
LAN2	Link Down						--
LAN3	Link Down						--
LAN4	Link Down						--
WLAN b/g/n	145Mbps	73502	0	0	3188	0	00:43:50
WLAN a/n	450Mbps	73530	0	0	3190	0	00:43:50

Poll Interval : 5 (secs) Set Interval Stop

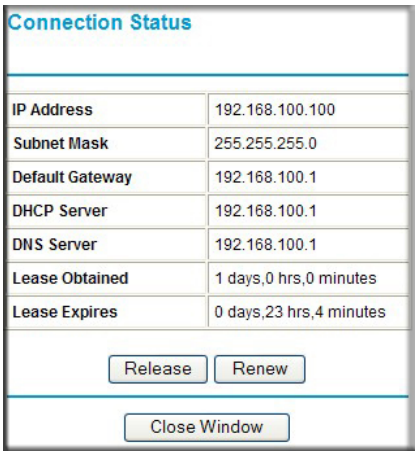
Port

The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted since reset or manual clear.
- **RxPkts**. The number of packets received since reset or manual clear.
- **Collisions**. The number of collisions since reset or manual clear.
- **Tx B/s**. The current line utilization—percentage of current bandwidth used.
- **Rx B/s**. The average line utilization.
- **Up Time**. The time elapsed since the last power cycle or reset.

Connection Status

In the Router Status screen, click the **Connection Status** button to display a screen similar to this:



IP Address. The IP address that is assigned to the router.

Subnet Mask. The subnet mask that is assigned to the router.

Default Gateway. The IP address for the default gateway that the router communicates with.

DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.

DNS Server. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

Lease Obtained. The date and time that the lease was obtained.

Lease Expired. The date and time that the lease will expire.

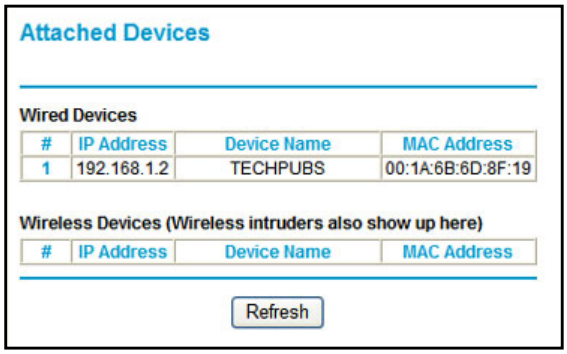
- Click the **Release** button to release the connection status items (that is, all items return to 0).

- Click the **Renew** button to refresh the screen.
- Click the **Close Window** button to close the Connection Status screen.

View Attached Devices

The Attached Devices screen shows all IP devices that the wireless router has discovered on the local network.

Select **Maintenance > Attached Devices**. The following screen displays:



For each device, the table shows the IP address, the device name if available, and the Ethernet MAC address. Note that if the wireless router is rebooted, the table data is lost until the wireless router rediscovers the devices. To force the wireless router to look for attached devices, click the **Refresh** button.

USB Storage

6

This chapter describes how to access and configure a USB storage drive attached to your wireless router.

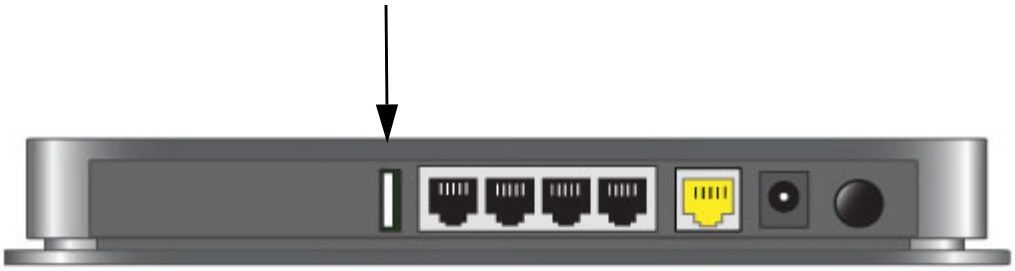


Figure 1. USB port on rear panel.

The USB port on the wireless router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the USB port.

This chapter includes the following sections:

- *USB Drive Requirements*
- *File-Sharing Scenarios*
- *USB Storage Basic Settings*
- *Edit a Network Folder*
- *USB Storage Advanced Settings*
- *Unmount a USB Drive*
- *Approved USB Devices*
- *Connect to the USB Drive from a Remote Computer*
- *Connect to the USB Drive with Microsoft Network Settings*

USB Drive Requirements

The wireless router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table.

Bus	Speed/Second
USB 1.1	12 Mbits
USB 2.0	480 Mbits

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables. The wireless router should work with USB 2.0-compliant or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the wireless router, go to *http://kbserver.netgear.com/readyshare/*.

When selecting a USB device, bear in mind the following:

- The USB port on the wireless router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- According to the USB 2.0 specification, the maximum available power is 5V @ 0.5A. If a USB device exceeds this requirement, it might not function or might function erratically. Check the documentation for your USB device to be sure.
- The wireless router supports FAT, FAT32, NTFS (read only), and NTFS with compression format enabled (read only).

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes.

Share Photos within Your Home Network

You can create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo-sharing site.

1. Insert your USB drive into the USB port on the wireless router either directly or with a USB cable.

   Computers on your local area network (LAN) can access this USB drive using a Web browser or Microsoft networking.

2. If you want to specify read-only access, or to allow access from the Internet, see *USB Storage Advanced Settings* on page 61.

Share Large Files with FTP over the Internet

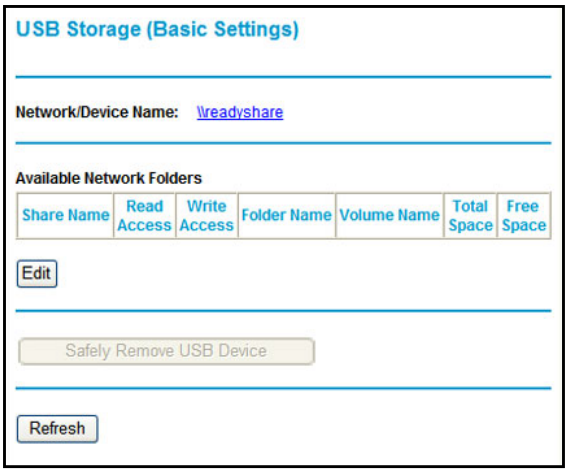
1. To protect your network, set up security if someone else will be downloading the files. Create a user name and password with appropriate access.
2. If you want to limit USB drive access to only read access, from the wireless router USB Storage (Basic Settings) screen, click **Edit**. In the Write Access field, select **admin**, and then click **Apply**.

   The password for admin is the same one that you use to access the wireless router. By default it is **password**.
3. Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See *USB Storage Advanced Settings* on page 61.

USB Storage Basic Settings

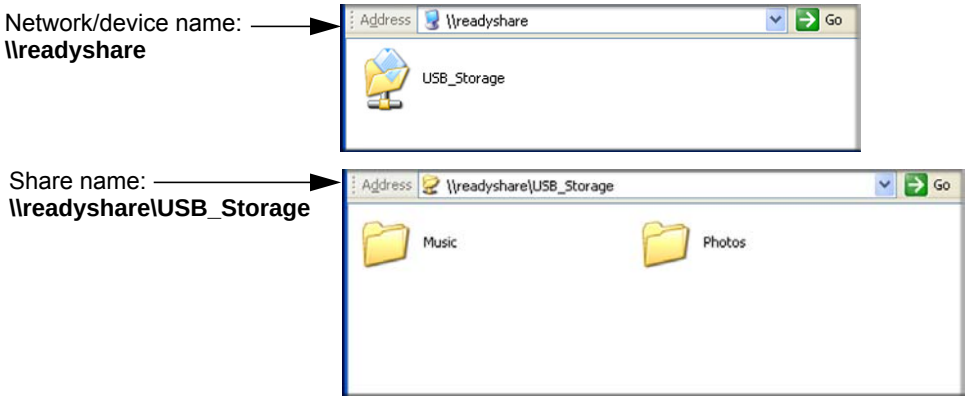
You can view or edit basic settings for the USB storage device attached to your wireless router.

1. Select **USB > Basic Settings**. The following screen displays:



   By default, the USB device is available to all computers on your local area network (LAN).
2. To access your USB device, do one of the following:
   - Click the network or device name.
   - Click the share name.

- Type **\\readyshare** in the address field of your Web browser.



If you logged in to the wireless router before you connected your USB device, you might not see your USB device in the wireless router screens until you log out and then log in again.

Basic Settings Screen Fields and Buttons

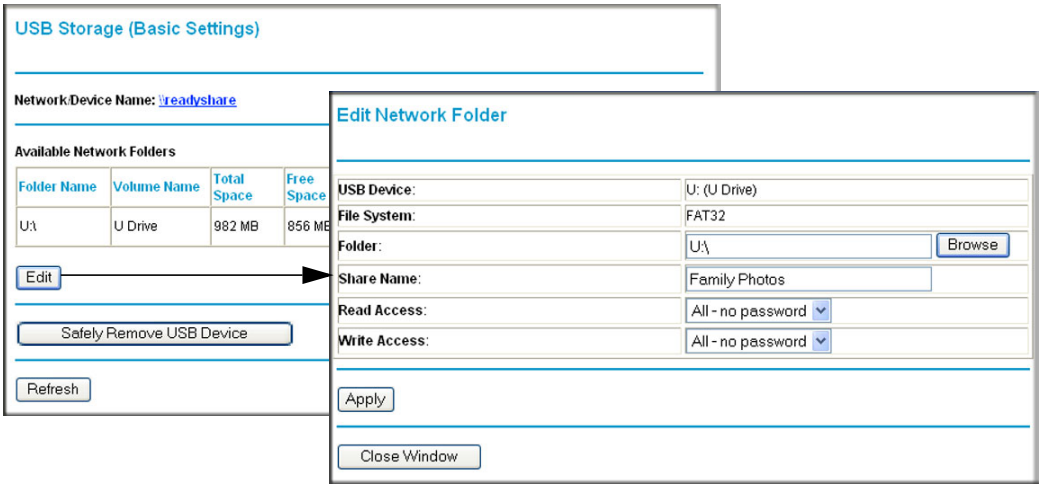
- **Network Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the wireless router.
- **Folder Name**. Full path of the network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total/Free Space**. Shows the current utilization of the storage device.
- **Share Name**. You can click the name shown, or you can type it in the address field of your Web browser.

  If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read/Write Access**. Shows the network folder permissions and access controls.
  - **All no password** allows all users to access the network folder.
  - **admin** uses the same password that you use to log in to the wireless router.
- **Edit**. You can click the **Edit** button to edit the Available Network folder settings. See the following section, *Edit a Network Folder* .
- **Safely Remove USB Device**. Click this button to safely remove the USB device attached to your wireless router. See *Unmount a USB Drive* on page 63.

Edit a Network Folder

This process is the same from both the USB Storage (Basic Settings) and (Advanced Settings) screens.

1. Click the **Edit** button to open the Edit Network Folder screen:



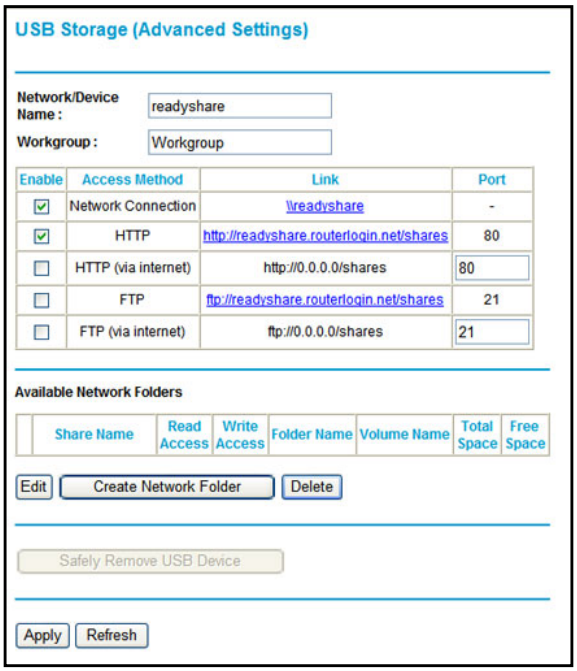
2. You can use this screen to select a folder, to change the share name, or to change read access or write access from All-no password to admin.

   The password for admin is the same one that is used to log in to the wireless router. By default it is password.

3. Click **Apply** for your changes to take effect.

USB Storage Advanced Settings

To configure advanced USB settings, select **USB > Advanced Settings**. The USB Storage (Advanced Settings) screen displays:



You can use this screen to specify access to the USB storage device. The settings are as follows:

- **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the wireless router from your computer.
- **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here.

Access Method

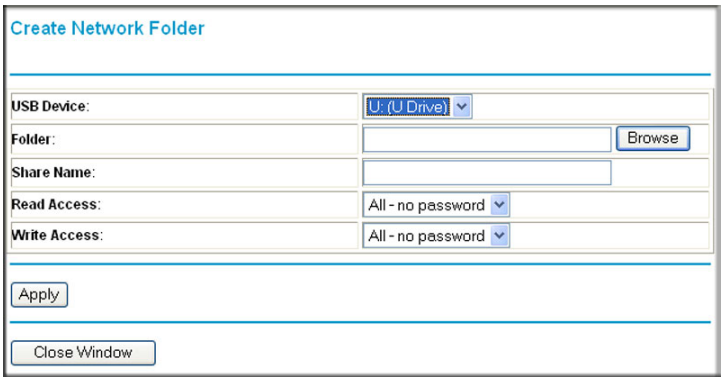
- **Network Connection**. Enabled by default, this allows all users on the LAN to have access to the USB drive.
- **HTTP**. Disabled by default. If you enable this setting, you can type **http://readyshare** to access the USB drive.
- **HTTP (via Internet)**. Disabled by default. If you enable this settings, remote users can type **http://readyshare** to access the USB drive over the Internet.
- **FTP**. Disabled by default.
- **FTP (via Internet)**. Disabled by default. If you enable this settings, remote users can access the USB drive via FTP over the Internet.

Available Network Folders

- **Folder Name**. Full path of the network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total Free Space**. The space currently available on the storage device.
- **Share Name**. You can click the name shown, or you can type it into the address field of your Web browser. If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read/Write Access**. Shows the permissions and access controls on the Network folder. Selecting **All-no password** allows all users to access the network folder. You are prompted to enter the same password that you use to log in to the wireless router.

Create a Network Folder

1. From the USB Storage (Advanced Settings) screen, click the **Create Network Folder** button to open the Create Network Folder screen:



2. Create a folder.
   - You can specify the folder's share name, and change read access and write access from All-no password to admin.
   - The password for admin is the same one that is used to log in to the wireless router. By default it is password.
3. Click **Apply** so that your changes take effect.

Unmount a USB Drive

To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

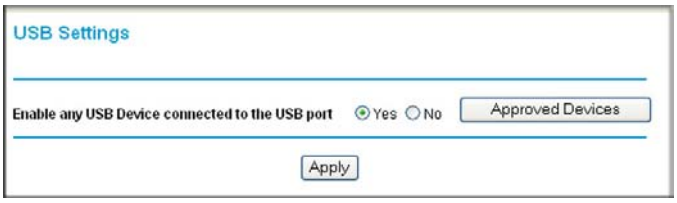
CAUTION:

Unmount the USB drive before physically unplugging it from the wireless router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

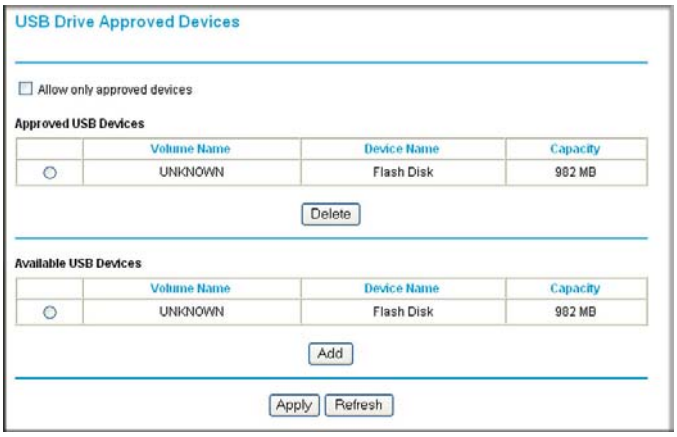
Approved USB Devices

You can specify which USB devices are approved for use when connected to the wireless router.

1. Select **Advanced > USB Settings**. The following screen displays:.



2. Click **Approved Devices** and the following screen displays:



3. On the USB Drive Approved Devices screen, select the USB device from the Available USB Devices list.
4. Click **Add**.
5. Select the **Allow only approved devices** check box.
6. Click **Apply** so that your change takes effect.

If you want to approve another USB device, first use the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you use the wireless router's Internet port IP address.

Locate the Internet Port IP Address

The Router Status screen shows the Internet port IP address:

1. Log in to the wireless router.
2. Select **Maintenance > Router Status**.
3. Record the IP address that is listed for the Internet port. This is the IP address you can use to connect to the wireless router remotely.

Access the Modem Router's USB Drive Remotely with FTP

You can connect to the wireless router's USB drive using a Web browser:

1. Connect to the wireless router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Mozilla Firefox, for example, **ftp://10.1.65.4**. If you are using Dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the name and password of the account that has access rights to the USB drive.

   The directories of the USB drive that your account has access to display, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connect to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You have to be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as dragging and dropping, opening files, or cutting and pasting files from:

- Microsoft Windows Start menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer's network properties have to be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft networking has to be enabled, as described in the following sections.

Note: In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

Configuring Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click **Network Neighborhood** and then select **Properties**. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Add** and follow the installation prompts.

If you have questions about File and Printer Sharing, contact Microsoft for assistance.

Configuring Windows 2000 and Windows XP

Right-click the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Install** and follow the installation prompts.

Advanced Settings

7

This chapter describes the advanced features of your wireless router. The information is for users with a solid understanding of networking concepts who want to set the wireless router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

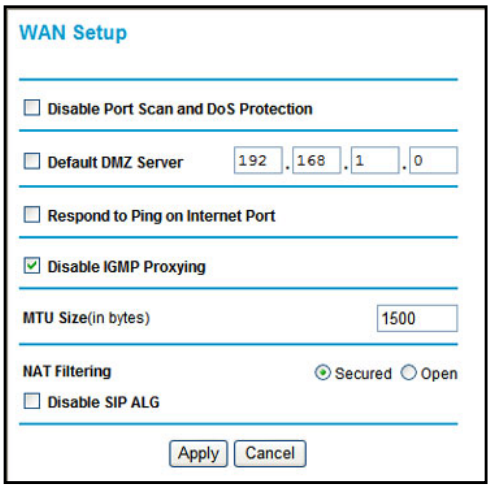
This chapter contains the following sections:

- *WAN Setup*
- *Dynamic DNS*
- *LAN Setup*
- *Quality of Service (QoS)*
- *Advanced Wireless Settings*
- *Remote Management Access*
- *Static Routes*
- *IPv6*
- *Universal Plug and Play*
- *Traffic Meter*
- *Advanced USB Settings*
- *Wireless Bridging and Repeating Networks*

Note: The port forwarding and port triggering features are described in *Port Forwarding* on page 43 and *Port Triggering* on page 46.

WAN Setup

Select **Advanced > WAN Setup** to display the following screen:



The following settings are available:

- **Disable Port Scan and DoS Protection**. The firewall protects your LAN against port scans and denial of service (DoS) attacks. This protection should be disabled only in special circumstances.
- **Default DMZ Server**. The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. See *Default DMZ Server* on page 69.
- **Respond to Ping on Internet WAN Port**. If you want the wireless router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, because it allows your wireless router to be discovered. Do not select this check box unless you have a specific reason to do so.
- **Disable IGMP Proxying**. The IGMP Proxying function lets a PC on the LAN receive multicast traffic from the Internet. Select this check box to disable the function if you do not need it.
- **MTU Size (in bytes)**. The normal Maximum Transmit Unit (MTU) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **NAT Filtering**. By default NAT filtering is used.

Default DMZ Server

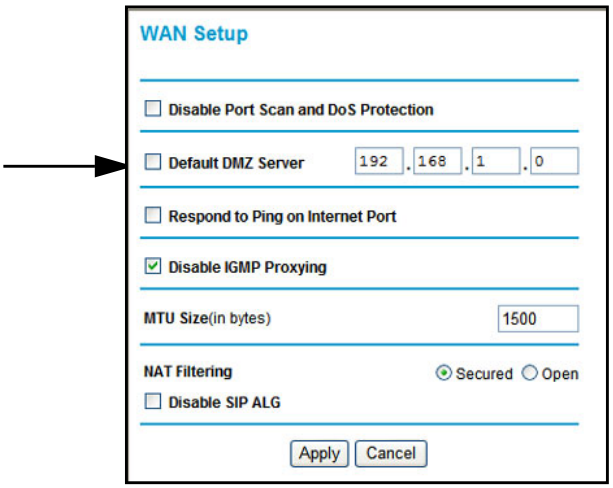
The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. The wireless router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that 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.

Note: For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall. If compromised over the Internet, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the wireless router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports 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.

To assign a computer or server to be a default DMZ server:

1. In the WAN Setup screen, select the **Default DMZ Server** check box. The following screen displays:



2. Type the IP address for that server and click **Apply**.

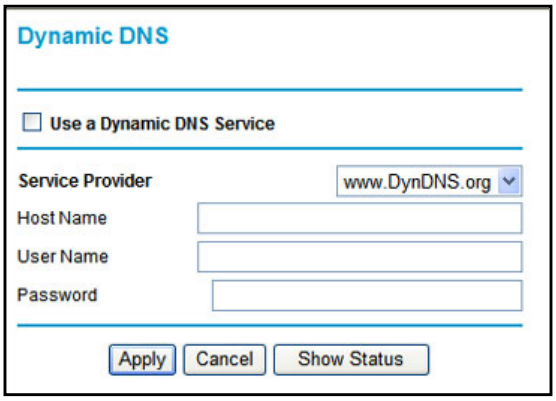
Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name that is linked to your IP address by public Domain Name Servers (DNS). More commonly, Internet accounts have dynamically assigned IP addresses in which the IP addresses change frequently. In this case, use a commercial Dynamic DNS service to register your domain to its IP address and forward traffic directed at your domain to your current IP address.

The wireless router has a client that can connect to a Dynamic DNS service provider. Once you set up Dynamic DNS in the wireless router, when your IP address changes, your wireless router contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

To set up Dynamic DNS:

1. Select **Advanced > Dynamic DNS** to display the following screen.



2. Access the website of one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Type the host name that your Dynamic DNS service provider gave you. This is sometimes called the domain name. If your URL is myName.dyndns.org, your host name is myName.
6. Type the user name for your Dynamic DNS account.
7. Type the password (or key) for your Dynamic DNS account.
8. Click **Apply** to save your settings.

   If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service does not work because private addresses are not routed on the Internet.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and Routing Information Protocol (RIP). The wireless router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless router's default LAN IP configuration is as follows:

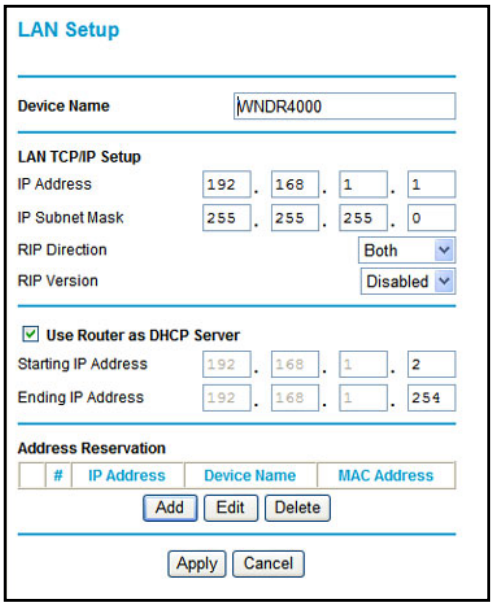
- **LAN IP address**. 192.168.1.1
- **Subnet mask**. 255.255.255.0

These addresses are part of the private address range designated by the Internet Engineering Task Force (IETF *http://www.ietf.org*) for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

Note: If you change the LAN IP address of the wireless router while connected through the browser, you are disconnected. To reconnect, open a new connection to the new IP address and log in.

To change the LAN settings:

1. Select **Advanced > LAN Setup**. The following screen displays:



2. Enter the LAN Setup configuration, and click **Apply** to save your changes.

LAN Setup Screen Settings

- **IP Address**. The LAN IP address of the wireless router.
- **IP Subnet Mask**. The LAN subnet mask of the wireless router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or wireless router.
- **Use Router as DHCP Server**. By default, the wireless router is a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless router's LAN. The assigned default gateway address is the LAN address of the wireless router. IP addresses are assigned to the attached PCs 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.

  For most applications, the default DHCP and TCP/IP settings of the wireless router are satisfactory.
- **Reserved IP Addresses Setup**. 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 wireless router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

IP Address Reservation

To reserve an IP address:

1. Select **Advanced > LAN Setup** and click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the wireless router's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.

   Tip: If the computer is already on your network, 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 wireless router's DHCP server. Reboot the computer or access its IP configuration to force a DHCP release and renew.*

To edit or delete a reserved address entry:

1. Select the radio button next to the reserved address that you want to edit or delete.
2. Click **Edit** or **Delete**.

Quality of Service (QoS)

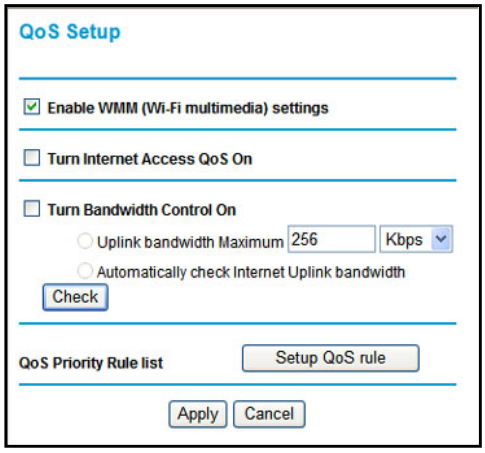
Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The wireless router can provide QoS prioritization over the wireless link and on the Internet connection.

The wireless router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

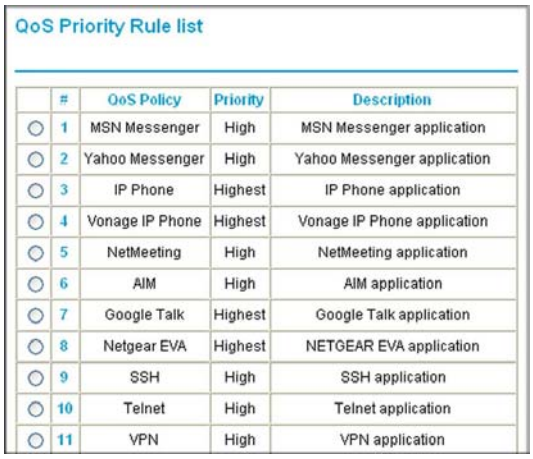
QoS for Internet Access

To specify prioritization of traffic, you need to add or create a policy for the type of traffic.

1. Select **Advanced > QoS Setup**. The following screen displays:



2. Click **Setup QoS rule**. The QoS Priority Rule list displays:



QoS Priority Rule list

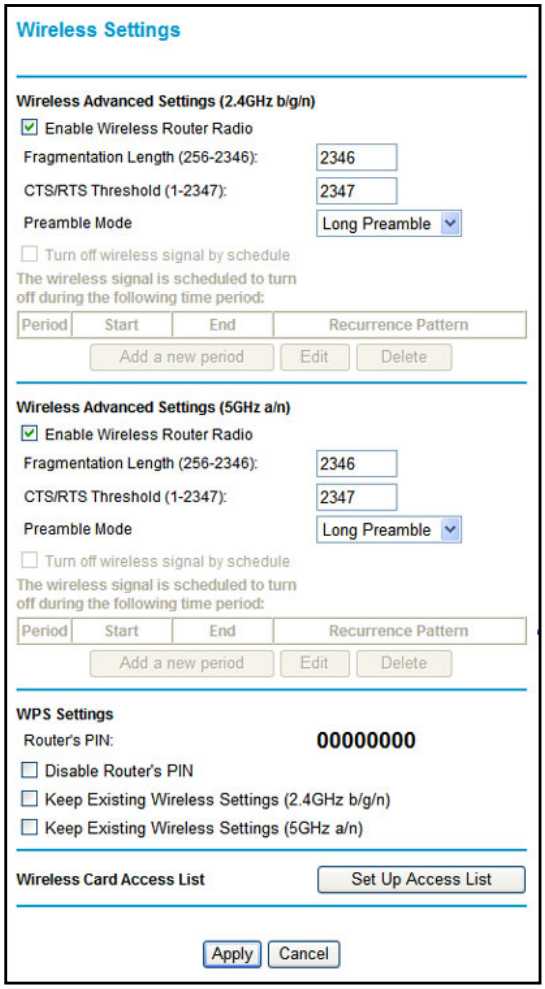
	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	NETGEAR EVA application
○	9	SSH	High	SSH application
○	10	Telnet	High	Telnet application
○	11	VPN	High	VPN application

3. To change a rule, select its radio button, scroll down and click **Edit**.
4. To add a custom rule, click **Add Priority Rule**.
5. Click **Apply** to save your changes and return to the QoS Setup screen.
6. In the QoS Setup screen, click **Apply**.

Advanced Wireless Settings

To view or change advanced wireless settings:

1. Select **Advanced > Wireless Settings** to display the following screen:



2. If you make changes, click **Apply**. Note that the WLAN settings come from the settings you made in the Wireless Settings screen (see *Wireless Settings Screen* on page 29).

Wireless Advanced Settings (2.4 GHz and 5 GHz)

- **Enable Wireless Router Radio**. When this check box is selected, the wireless router works as an access point broadcasting a wireless signal.
- The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode fields are used for testing. Do not change them unless you have a specific reason to do so.

WPS Settings

Router's PIN. The PIN number that you use on a registrar (for example, from the Network Explorer on a Vista Windows PC) to configure the wireless router's wireless settings through WPS. You can also find the PIN on the wireless router label.

The PIN function might temporarily be disabled when the wireless router detects suspicious attempts to break into the wireless router's wireless settings by using the wireless router's PIN through WPS. You can manually enable the PIN function by clearing the Disable Router's PIN check box.

Keep Existing Wireless Settings. By default, the Keep Existing Wireless Settings check box is selected. This allows the wireless router to keep the same SSID and wireless security settings when WPS-enabled devices are added to the network.

If the Keep Existing Wireless Settings check box is not selected, the next time you use WPS to connect WPS-capable devices to your wireless network, the wireless router generates a new random SSID and WPA/WPA2 passphrase. NETGEAR does not recommend this.

Wireless Card Access List

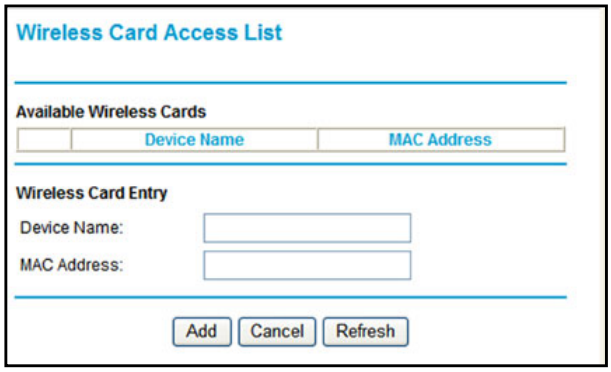
The Wireless Card Access List lets you restrict access to your network to a specific list of devices based on their MAC addresses. This section explains how to set up the list.

1. Select **Advanced > Wireless Settings**, and click the **Set Up Access List** button to display the Wireless Card Access List screen:

   The Turn Access Control On check box is not selected so that any computer configured with the correct wireless network name (SSID) and passphrase can access the network.

2. Select the **Turn Access Control On** check box to enable access restriction by MAC address.

3. Click **Add** to add your computer's MAC address so that you do not lose your wireless connection when you click Apply. If you lose your wireless connection, you have to access the wireless router from a wired computer or from a wireless computer that is on the access control list. The following screen displays:



4. If a wireless station that you want to add is connected to the network, select it from the Available Wireless Cards list and click **Add**.
5. You can enter MAC addresses manually. The MAC address is usually printed on the wireless computer or device, or it might be in the wireless router's DHCP table. The MAC address is 12 hexadecimal digits.

   You can copy and paste the MAC addresses from the wireless router's Attached Devices screen (see *View Attached Devices* on page 56) into the MAC Address field. This screen shows computers connected to the network.
6. Click **Apply** to save your settings.

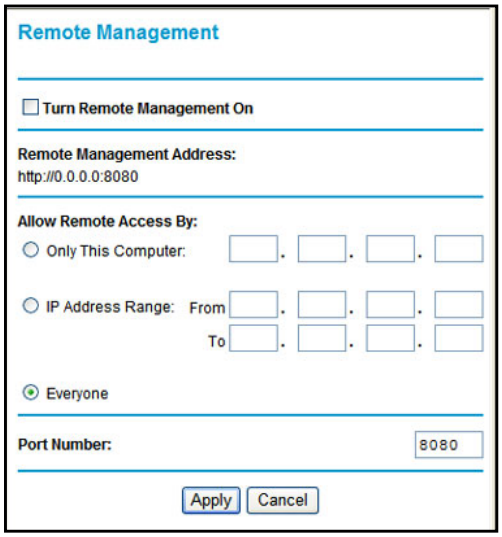
Remote Management Access

The remote management feature allows you to upgrade or check the status of your WNDR4000 router over the Internet.

Note: Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for remote management:

1. Select **Advanced > Remote Management**. The following screen displays:



2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify what external IP addresses will be allowed to access the router's remote management.

> **Note:** For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from any IP address on the Internet, select **Everyone**.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**.
  Enter a beginning and ending IP address to define the allowed range.
- To allow access from a single IP address on the Internet, select **Only This Computer**.
  Enter the IP address that will be allowed access.

4. Specify the port number for accessing the management interface.

   Normal Web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.

When accessing your router from the Internet, type your router's WAN IP address into your browser's address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter **http://134.177.0.123:8080** in your browser.

Static Routes

Static routes provide additional routing information to your wireless router. Under normal circumstances, the wireless router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

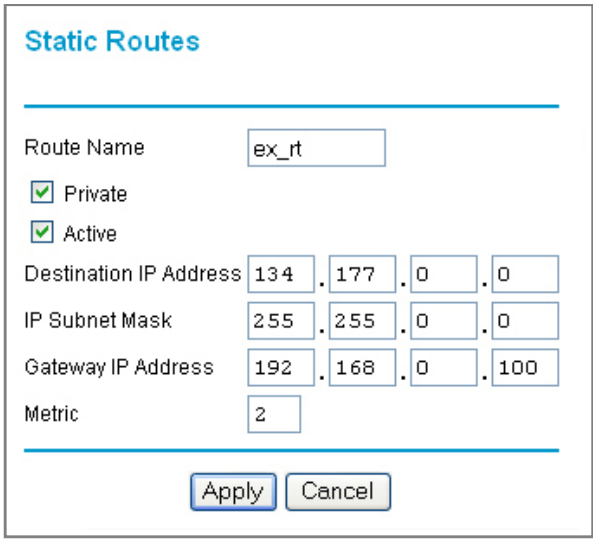
Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you first configured your wireless router, two implicit static routes were created. A default route was created with your ISP as the wireless router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your wireless router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you need to define a static route, telling your wireless router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.



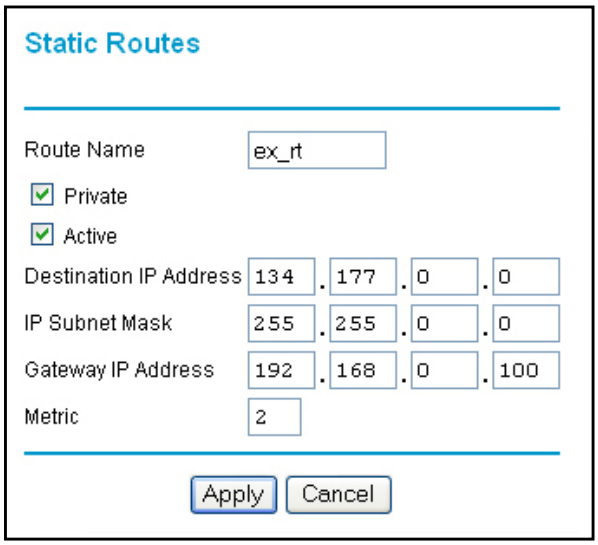
In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses is to be forwarded to the ISDN router at 192.168.0.100.
- The value in the Metric field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The Private check box is selected only as a precautionary security measure in case RIP is activated.

Add a Static Route

1. Select **Advanced > Static Routes** to display the following screen:

2. Click **Add** to open the following screen.

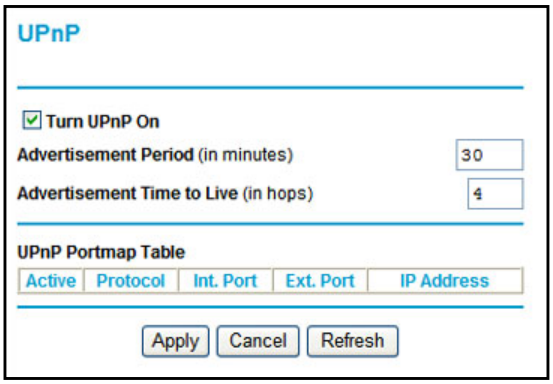


3. Fill in the fields:
   - In the Route Name field, enter a route name for this static route. This name is for identification purpose only.
   - Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
   - Select **Active** to make this route effective.
   - Enter the destination IP address of the final destination.
   - Enter the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
   - Enter the gateway IP address, which has to be a router on the same LAN segment as the wireless router.
   - In the Metric field, enter a number between 2 and 15 as the metric value. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.
4. Click **Apply** to save your changes. The Static Routes table is updated to show the new entry.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Select **Advanced > UPnP** to display the following screen:

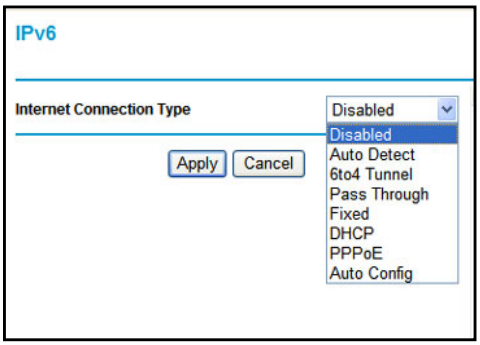


2. Specify the settings as follows:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the wireless router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless router.
   - **Advertisement Period**. The advertisement period is how often the wireless router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time to Live**. This is measured in hops (steps) for each UPnP packet sent. Hops are the steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value is 4 hops, which works for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the wireless router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.
3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the wireless router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

IPv6

The IPv6 feature allows you to configure and check the status of your IPv6 Internet connection.

Select **Advanced > IPv6,** and the following screen displays:



The default setting is Disabled, which turns off the IPv6 function. To turn it on, select your connection type from the Internet Connection Type list and click **Apply**.

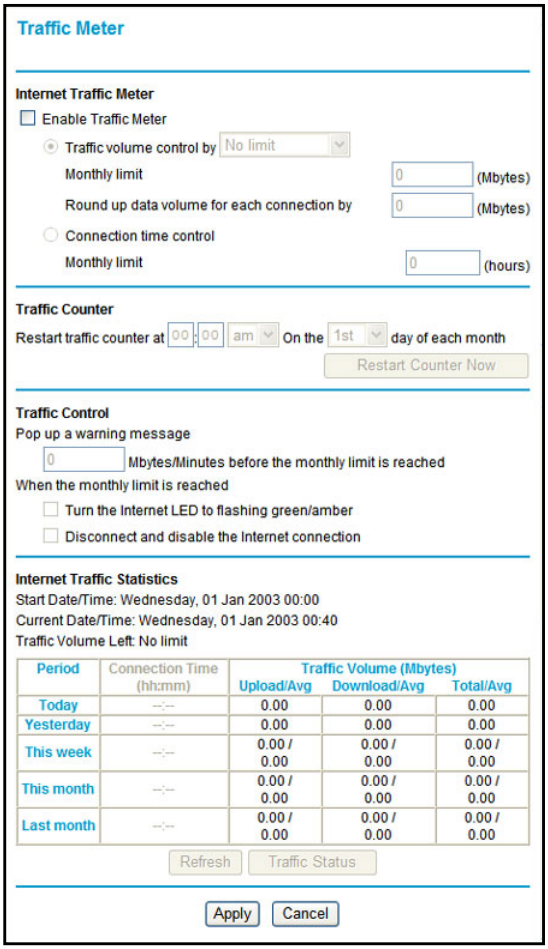
- If your ISP did not specify the connection type, you can select **6to24 Tunnel**.
- If your ISP explicitly indicates that your IPv6 connection is not DHCP, PPPoE, or Fixed IP, or your ISP indicates that it is IPv6 auto config, you can select **Pass Through**.
- If you are not sure about the IPv6 connection, you can use the Setup Wizard to automatically detect your Internet connection type.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your wireless router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

To monitor traffic on your wireless router:

1. Select **Advanced > Traffic Meter**. The following screen displays:



2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both directions**. The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month:
   - By specifying how many Mbytes per month are allowed.
   - By specifying how many hours of traffic are allowed.
5. Set the Traffic Counter to begin at a specific time and date.
6. Set up Traffic Control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.

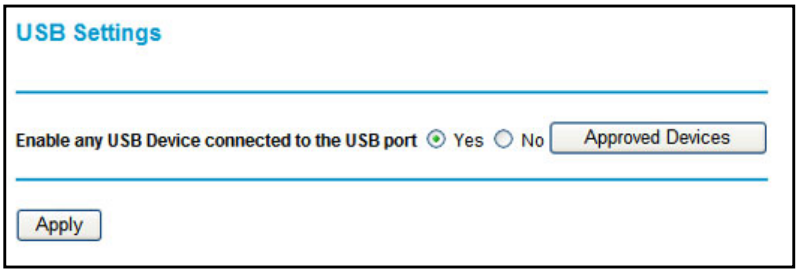
- The Internet connection is disconnected and disabled.

7. Set up Internet Traffic Statistics to monitor the data traffic.
8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your wireless router.
9. Click **Apply** to save your settings.

Advanced USB Settings

For added security, you can specify that only approved USB devices are shared.

1. Select **Advanced > USB**. The following screen displays:

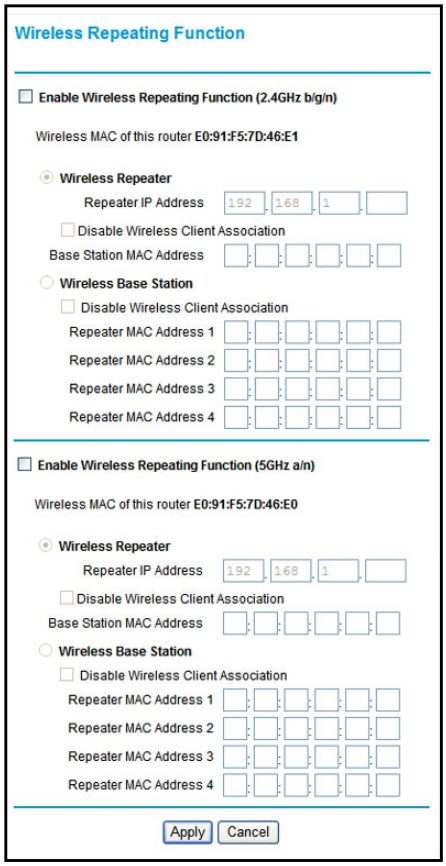


2. Select **No** and click **Apply**.
3. To define the approved devices, click **USB Approved Devices**.

Wireless Bridging and Repeating Networks

With the wireless router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the wireless router with other access points (APs) and wireless devices, you can connect clients using their MAC addresses rather than IP addresses. A repeater with wireless client associations sends all traffic to the remote access point.

Select **Advanced > Wireless Repeating Function** to display the following screen:



The process is the same for the 2.4 GHz or 5 GHz wireless network.

- **Enable Wireless Repeating Function (2.4 GHz/5 GHz)**. Select the check box for the 2.4 GHz or 5 GHz network to use the wireless repeating function.
- **Wireless MAC of this router**. This field displays the MAC address for your wireless router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your wireless router is the repeater, select this check box.
- **Repeater IP Address**. If your wireless router is the repeater, enter the IP address of the other access point.
- **Disable Wireless Client Association**. If your wireless router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.
  - If you are setting up a point-to-point bridge, select this check box.
  - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.
- **Base Station MAC Address**. If your wireless router is the repeater, enter the MAC address for the access point that is the base station.

- **Wireless Base Station**. If your wireless router is the base station, select this check box.
- **Disable Wireless Client Association**. If your wireless router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.
- **Repeater MAC Address (1 through 4)**. If your wireless router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

Set Up a Repeater with Wireless Client Association

In the repeater mode with wireless client association, your wireless router sends all traffic to a base station access point. You can set up the wireless router as either the base station (parent) or as the repeater (child) access point.

Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this wireless router.
- You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if your wireless router is the parent access point, it can connect with up to four child access points.

The following figure shows an example of a repeater mode configuration.

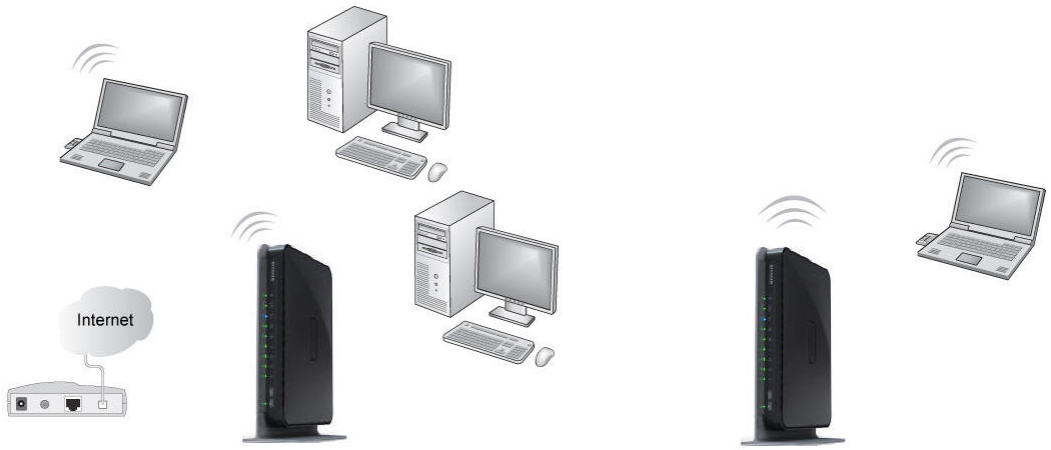


Figure 2. Repeater example

To set up a repeater with wireless client association:

In this example, the wireless router is the base station, but you can set it up to be the repeater with another AP as the base station if you want.

1. Set up your wireless router to be the base station.
   a. In the Wireless Repeating Function screen for your wireless router, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Base Station** radio button.

   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).
   d. Enter the MAC addresses for AP 2 and AP 3 in the Repeater MAC Address 1 and Repeater MAC Address 2 field.
   e. Click **Apply**.
2. Set up AP 2 and AP 3 to be wireless repeaters.
   a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Repeater** radio button.
   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).
   d. Enter the MAC addresses for your wireless router in the Base Station MAC Address field.
   e. Click **Apply**.
3. Verify the following for all access points:
   - Each access point operates in the same LAN network address range as the LAN devices.
   - The access points are on the same LAN. That is, the LAN IP addresses for the access points are in the same network.
   - If you are using DHCP, access point devices are set to Obtain an IP address automatically (DHCP Client) in the Basic Settings screen.
   - Access point devices use the same SSID, channel, authentication mode, and encryption.

Verify connectivity across the LANs. 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 WLAN segments.

Troubleshooting

8

This chapter provides information to help you diagnose and solve problems you might have with your wireless router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log In to the Wireless Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Incorrect Date or Time*
- *Wireless Connectivity*
- *Restoring the Factory Settings and Password*

Quick Tips

This section describes tips for troubleshooting some common problems

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the wireless router and computers.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the wireless router and wait 2 minutes.
5. Turn on the computers.

Power LED

Check the Power LED to verify correct router operation.

If the Power LED does not turn off within 2 minutes after you turn the router on, reset the router according to the instructions in *Restoring the Factory Settings and Password* on page 93.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router is on if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on.
- For each powered-on computer connected to the wireless router by an Ethernet cable, the corresponding numbered router LAN port light is on.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you have to add each wireless computer's MAC address to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers need to have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshooting with the LEDs

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. After approximately 2 minutes, verify that:
   - The Power LED is solid green.
   - The Internet LED is on.
   - A numbered Ethernet port light is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

The LEDs on the front panel of the router can be used for troubleshooting.

Power LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 12V DC, 2.5A power adapter that NETGEAR supplied for this product.
- If the Power LED alternately blinks green every second, the router software is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact Technical Support at *www.netgear.com/support.*

LEDs Never Turn Off

When the router is turned on, the LEDs turns on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router.

If all LEDs are still on 1 minute after power-up:

- Cycle the power to see if the router recovers.

- Clear the router's configuration to factory defaults as explained in *Restoring the Factory Settings and Password* on page 93.

If the error persists, you might have a hardware problem and should contact Technical Support at *www.netgear.com/support*.

Internet or Ethernet Port LEDs Are Off

If either the Ethernet port LEDs or the Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable:

  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Wireless LED Is Off

If the Wireless LED stays off, check to see if the Wireless On/Off button on the router has been pressed. This button turns the wireless radios in the router on and off. The 2.4 GHz and 5 GHz LEDs are lit when the wireless radio is turned on.

Cannot Log In to the Wireless Router

If you are unable to log in to the wireless router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the wireless router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the wireless router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the wireless router, and reboot your computer.
- If your wireless router's IP address was changed and you do not know the current IP address, clear the wireless router's configuration to factory defaults. This sets the wireless router's IP address to 192.168.1.1. This procedure is explained in *Factory Settings* on page 94.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet Service Provider (ISP). Unless your ISP provides a fixed IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

To check the WAN IP address:

1. Start your browser, and select an external site such as *http://www.netgear.com*.
2. Access the main menu of the router's configuration at *http://www.routerlogin.net*.
3. Select **Maintenance > Router Status**.
4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in *Sequence to Restart Your Network* on page 88.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Basic Settings screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to clone your computer's MAC address.

If your router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address.You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address.

- You might be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Changes Not Saved

If the wireless router does not save the changes you make in the wireless router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the old settings might be in the Web browser's cache.

Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The wireless router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. This means the wireless router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just finished setting up the wireless router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The wireless router does not automatically sense daylight savings time. In the Schedule screen, select the **Automatically adjust for daylight savings time** check box.

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

- Does the wireless device or computer that you are using find your wireless network?

  If not, check the 2.4 GHz and 5 GHz LEDs on the front of the router. They should be lit. If they aren't, you can press the **Wireless** button on the front of the router to turn the routers wireless radios back on.

  If you disabled the router's SSID broadcast, then your wireless network is hidden and does not show up in your wireless client's scanning list. (By default, SSID broadcast is enabled.)

- If your wireless device finds the network but you cannot join the network, check to make sure your wireless device is compatible with the network that you selected (2.4 GHz or 5 GHz).
- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to check the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router and select **Setup > Wireless Settings** see (*Wireless Settings Screen* on page 29).

  Note: *Be sure to configure both sections (for 2.4 GHz b/g/n and 5 GHz a/n) on the Wireless Settings screen and to click* ***Apply*** *if you make changes.*

Wireless Signal Strength

If your wireless device finds your network, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal blocked by objects between the router and your computer?

Restoring the Factory Settings and Password

This section explains how to restore the factory settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see *Erase* on page 53).
- Use the Restore Factory Settings button on the bottom of the router. See *Factory Settings* on page 94. If you restore the factory settings and the wireless router fails to restart, or the green Power LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact Technical Support at *http://www.netgear.com/support*.

Supplemental Information

A

This appendix provides factory default settings and technical specifications for the N750 Wireless Dual Band Gigabit Router WNDR4000.

Factory Settings

You can return the wireless router to its factory settings. Use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button on the bottom of the router for at least 7 seconds. The wireless router resets, and returns to the factory settings. Your device returns to the factory configuration settings shown in the following table.

Table 1. Factory Default Settings

Feature		Default Behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	Autosensing
Local network (LAN)	LAN IP	□□□□□□□□□□□□
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	Time zone Daylight Saving time	Disabled
	Allow a registrar to configure this router	Enabled

Table 1. Factory Default Settings (Continued)

Feature		Default Behavior
Local network (LAN) continued	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID names	• 2.4 GHz b/g/n: NETGEAR • 5 GHz a/n: NETGEAR-5G
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	• 2.4 GHz b/g/n: Up to 145 Mbps • 5 GHz a/n: Up to 450 Mbps
	Data rate	Best
	Output power	Full
Firewall	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

**. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.*

Technical Specifications

Table 2. WNDR4000 Router Specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	• North America: 120V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • All regions (output): 12V DC @ 2.5A, output
Dimensions	1.1 in. x 6.89 in. x 4.68 in. (28 x 175 x 119 mm)
Weight	1.2 lbs. (0.5 kg)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
LAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
WAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n draft version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz IEEE 802.11n, IEEE 802.11a 5.0 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency ranges 2.4 Ghz	2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI)
Operating frequency ranges 5 Ghz	5.18–5.24 + 5.745–5.825 GHz (US) 5.18–5.24 GHz (Europe ETSI) FCC: 5.25–5.35 GHz (DFS band) and 5.47–5.725 GHz (DFS band) 5600–5650MHz is disabled and unavailable for use CE (Europe ETSI): 5.25–5.35 GHz (DFS band) and 5.47–5.725 GHz (DFS band)
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2 Enterprise.

Notification of Compliance

NETGEAR Dual Band - Wireless

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: 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, EN301 893 (5Ghz), EN60950-1

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 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 Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N750 Wireless Dual Band Gigabit Router WNDR4000 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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.

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.

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.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Index

A

access
    remote 76
access lists 75
adapter, wireless 26
adding
    custom service 44
alerts, emailing 42
approved USB devices 64
attached devices, viewing 56
automatic firmware checking 50
automatic Internet connection 19

B

back panel 10
backing up configuration 52
Basic Settings screen
    manual setup 20
blocking content and services 34, 37
blocking keywords, examples 37
box contents 8
bridged networks 83

C

cables, checking 88
changes not saved, router 92
compliance 97
configuration file, managing 52
configuration, wireless network 29
configuring
    port triggering 46
    user-defined services 39
connecting USB drive 64
connecting wirelessly 11
connection status, Internet 81
content filtering 34
country setting 19
crossover cable 90
custom service (port forwarding) 44

D

date and time 92
daylight savings time 40, 92
default demilitarized zone (DMZ) server 69
default factory settings 94
    restoring 93
default gateway 55
denial of service (DoS)
    port scans 68
    protection 34
devices, adding 27
DHCP server 55
disabling
    SSID broadcast 27
disconnecting USB drive 63
DNS addresses
    troubleshooting 91
DNS server
    primary 22
    secondary 22
Domain Name Server (DNS) addresses 70
DSL port settings 53
Dynamic DNS 70
Dynamic Host Configuration Protocol (DHCP) server 72

E

electromagnetic emissions 96
email notices 42
erasing configuration file 53
Ethernet cables, checking 88
Ethernet light, troubleshooting and 89, 90

F

factory default settings
    restoring 93
factory settings
    list of 94
    resetting 10
file and printer sharing 65
file sharing 58

filtering content 34
firewalls
inbound rules 43
firmware, upgrading 50
at log in 18
automatic check 50
manually 51
front panel 8
LEDs described 9
FTP, sharing files using 59

H

host name 21
host, trusted 38

I

inbound firewall rules 43
installing
manual setup 20
Setup Wizard 19
Internet connection
troubleshooting 91
Internet connection status 81
Internet light, troubleshooting and 89
Internet port 19
Internet port, no connection 23
Internet Service Provider (ISP), see ISP
Internet traffic statistics 83
IP address 64, 65
DHCP 16
LAN service 71
reserved 72
IP setup, LAN 71
IPv6 81
ISP
account information 16
ISP login 16

K

keywords, blocking traffic using 37

L

label, product 10
LAN ports 54
LAN setup 71
language setting 19
lease, DHCP 55
LEDs
verifying cabling 13
logging in
changing password 23
ISP 16
router 17
types 24
upgrade firmware 18
logs 35, 36
logs, emailing 42

M

MAC address
spoofing 22
MAC address, product label 10
MAC addresses
described 27
filtering by 76
restricting access by 75
maintenance settings 49
managing router remotely 76
manual logout 24
manual setup 20
Maximum Transmit Unit (MTU) 68
menus, described 18
metric, number of routers 79

N

network
correct settings, checking 89
restarting 88
network folder
creating 63
editing 60
Network Time Protocol (NTP) 40, 92
no Internet connection 23

O

online help, router 18
outbound firewall rules 38

P

passphrase, product label 10
password
restoring 93
passwords, see passphrases
plug and play, universal (UPnP) 80
Point-to-Point Tunneling Protocol (PPTP) 20
port numbers 38

port scanning, disabling 68
port triggering
configuring 46
portmap table 80
ports
filtering 38
forwarding 43
listed, back panel 10
positioning the router 11
Power light, troubleshooting and 89
PPPoE (PPP over Ethernet) 22, 91
primary DNS server 22
prioritizing traffic 73

Q

Quality of Service (QoS) 73

R

range of wireless connections 11
releasing connection status 55
remote management 64, 76
removing USB drive 63
renewing connection status 56
repeater mode with wireless client association 85
replace existing router 16
reserved IP address 72
restarting network 88
restore
configuration file 53
factory settings button 94
restoring
default factory settings 93
router interface, described 18
router, status 53
Routing Information Protocol (RIP} 71

S

security 27
security features 26
security options 26
security options, described 26
security PIN 10, 29
security settings 34
sending logs by email 42
serial number, product label 10
service numbers 39
services 38
setting time zone 40
settings, default. *See* default factory settings
Setup Wizard 19
sharing files 58
Simple Mail Transfer Protocol (SMTP) 42
sites, blocking 37
specifications
technical 94
SSID
described 31
disable 27
SSID, product label 10
static routes 78, 79
statistics, viewing 54
status
Internet connection 55
router 53
storage drive. See USB storage

T

TCP/IP
no Internet connection 23
technical specifications 94
technical support 2
time of day 92
time zone, setting 40
time-out
port triggering 47
time-stamping 40
trademarks 2
traffic metering 81, 82
traffic, prioritizing 73
troubleshooting 87
date or time incorrect 92
log in access 90
router changes not saved 92
trusted host 38
Trusted IP Address field 38
trusted wireless stations 76
turn off wireless connectivity 26

U

Universal Plug and Play (UPnP) 80
unmounting USB drive 63
upgrading firmware 50
USB devices 58, 63
USB devices, approved 64
USB storage 57
advanced 83
basic settings 59

connecting 64, 65
creating a network folder 63
editing a network folder 60
user-defined services 39

V

virtual channel identifier (VCI) 16
virtual path identifier (VPI) 16

W

WAN 68
WAN IP address, troubleshooting 91
WAN port
scanning 68
Wi-Fi Multimedia Quality of Service (WMM QoS) 73
Wi-Fi Protected Setup (WPS) 28
adding devices 28
keep existing settings 75
settings 74
wireless adapter 26
wireless bridging and repeating 83
wireless channel 31
wireless connection, troubleshooting 93
wireless connections 11
wireless connectivity 26
wireless distribution system (WDS) 83, 85
wireless isolation 31
Wireless LAN (WLAN) 55
Wireless light, troubleshooting and 90, 91
wireless mode 31
wireless network configuration 29
wireless network name 10
wireless network settings 31
wireless port settings 54
wireless region 31
wireless security 26
wireless security options 26
wireless settings
checking for correct 88
Wireless Settings screen 29
wireless settings, SSID broadcast 31
Wireless Stations Access List 75
WPS button 28
wrong date or time 92