

Specify a DNS Account That You Already Have

If you already have a Dynamic DNS account with NETGEAR no-ip, www.no-ip.com, or www.DynDNS.org, you can set up the router to use your account.

➤ **To set up Dynamic DNS if you already have an account:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Settings > Dynamic DNS**.

5. Select the **Use a Dynamic DNS Service** check box.
6. In the **Service Provider** list, select one of the following:
 - **NETGEAR**
 - **www.no-ip.com**
 - **www.DynDNS.org**
7. Select the **Yes** radio button.

The screen adjusts and displays the Show Status, Cancel, and Apply buttons.
8. In the **Host Name** field, type the host name (sometimes called the domain name) for your account.
9. For a www.no-ip or www.DynDNS account, in the **User Name** field, enter the user name for your account.

10. For a NETGEAR account at www.no-ip, in the **Email** field, type the email address for your account.
11. In the **Password (6-32 characters)** field, type the password for your DDNS account.
12. Click the **Apply** button.
Your changes are saved.
13. To verify that your Dynamic DNS service is enabled in the router, click the **Show Status** button.
A message displays the Dynamic DNS status.

Change the Dynamic DNS Settings

➤ **To change your settings:**

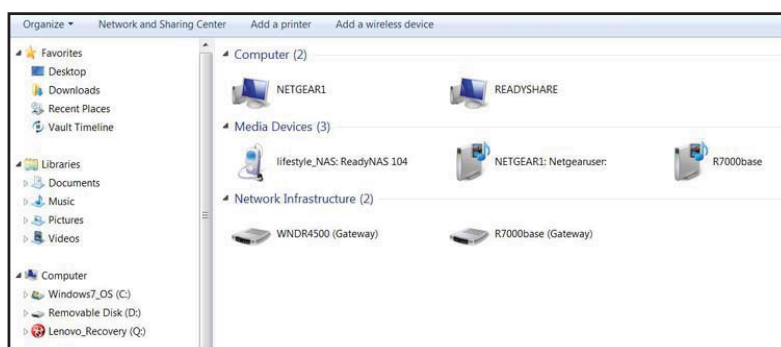
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > Advanced Settings > Dynamic DNS**.
5. Change your DDNS account settings as necessary.
6. Click the **Apply** button.
Your changes are saved.

Use Your Dynamic DNS Account

➤ **To use your Dynamic DNS account to access your home network:**

1. Launch an Internet browser on your computer or wireless device.
2. In the URL field, type your host name (sometimes called a domain name).

3. In Windows File Manager, select the **Network** folder.



The network resources display. The ReadySHARE icon is in the computers section and the remote R7000 icon is in the Media Devices section (if DLNA is enabled in the router).

4. If the icons do not display, click the **Refresh** button to update the screen.

If the local LAN and the remote LAN are using the same IP scheme, the remote R7000 icon does not display in the Media Devices and Network Infrastructure sections.

5. To access the router's USB drive, click the **ReadySHARE** icon.
6. To access media on the router's network, click the **R7000** icon.

Set Up Your Personal FTP Server

➤ To set up your personal account and use FTP:

1. Get your free NETGEAR Dynamic DNS domain name.

See *Your Personal FTP Server* on page 77.

2. Make sure that your Internet connection is working.

Your router must use a direct Internet connection. It cannot connect to a different router to access the Internet.

3. Connect a USB hard disk drive to a USB port on the router.
4. Set up FTP access in the router.

See *Set Up FTP Access Through the Internet* on page 75.

5. On your WAN PC, you can FTP to your router using `ftp://yourname.mynetgear.com`.

8. Use the Router as a Media Server

8

This chapter contains the following sections:

- *Specify ReadyDLNA Media Server Settings*
- *Play Music from a USB Drive with iTunes Server*
- *Play Media from a USB Drive on TiVo*

Specify ReadyDLNA Media Server Settings

By default, the router acts as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV-compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

➤ **To specify media server settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. \Select **ADVANCED > USB Storage > Media Server**.

5. Specify the settings:
 - **Enable Media Server.** Select this check box to enable this device to act as a media server.
 - **Enable TiVo support.** Select this check box if you want to play ReadyNAS media on your TiVo device. See the [Play Media from a USB Drive on TiVo](#) on page 85.
 - **Media Server Device Name.** Specify the name of the media server.

6. Click the **Apply** button.

Your changes are saved.

Play Music from a USB Drive with iTunes Server

iTunes Server lets you play music with your Windows or Mac iTunes app from a USB drive that is connected to the router USB port. You can also use the Apple Remote app from an iPhone or iPad to play music on any AirPlay devices, such as Apple TV or AirPlay-supported receivers.



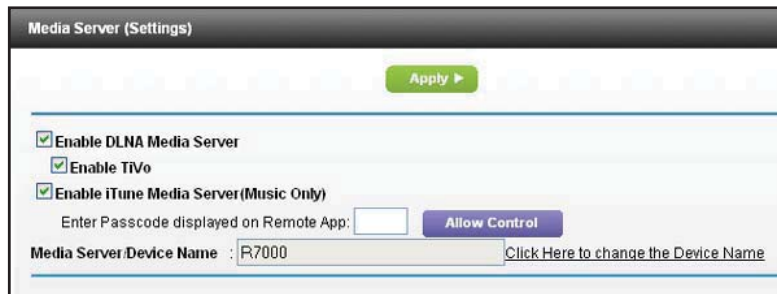
Figure 11. Play music on a USB drive with iTunes

Supported music file formats are MP3, AAC, FLAC, The maximum number of music file supported is 10,000 WAV and WMA3

➤ **To specify iTunes server settings:**

1. On your iPhone or iPad, find and connect to the WiFi network.
2. Launch the Remote App.
3. Click the **Add an iTunes Library** button.
A passcode displays.
4. Specify the passcode in the router.
 - a. Launch an Internet browser from a computer or wireless device that is connected to the network.
 - b. Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.
A login screen displays.
 - c. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.

- d. Select **ADVANCED > USB Storage > Media Server**.



- e. Leave the **Enable iTunes Media Server (Music Only)** check box selected.
f. Enter the passcode and click the **Allow Control** button.
g. Click the **Apply** button.

Your changes are saved.

On your iPhone or iPad, the ReadySHARE music library displays in the Remote app.

You can play this music to Airplay devices.

Play Media from a USB Drive on TiVo

You can set up your TiVo to access media files stored on a USB device that is connected to your router. The TiVo must be on the same network as the router. This feature supports the following file formats:

- **Video.** See and play mpeg1, and mpeg2 files.
- **Music.** See and play MP3 files.
- **Pictures.** View images in jpg format.

You can use the TiVo (Series 2 and up) Home Media Option to play photos and music on your Windows or Mac computer in your TiVo user interface.

➤ To set up the router to work with TiVo:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > USB Storage > Media Server**.
5. Make sure that the **Enable TiVo support** check box is selected.

➤ To play videos:

1. On the TiVo, select **TiVo Central > My Shows**.

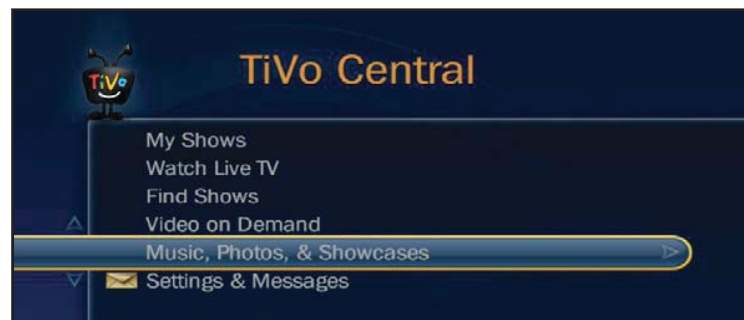


2. Go to the bottom of the list and select the R7000.

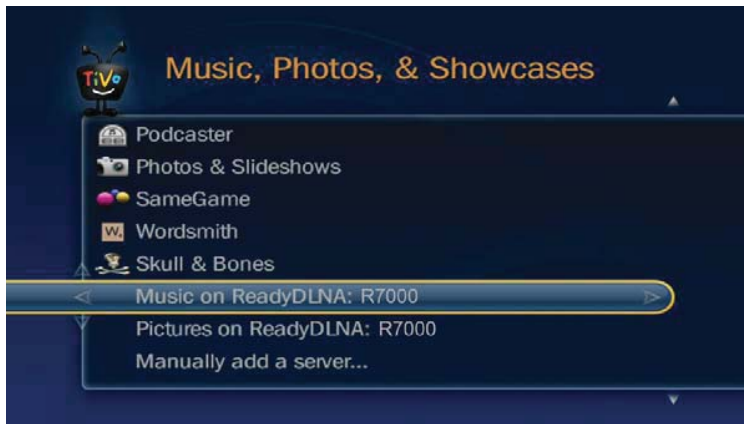


➤ To play music or view photos:

1. On the TiVo, select **TiVo Central > Music, Photos, & Showcases**.



2. Select an item to play or watch.



➤ **To copy TiVo files to a computer:**

Use the TiVo Desktop accessory, available at
<https://www3.tivo.com/store/accessories-software.do>.

9. Share a USB Printer

9

The ReadySHARE Printer utility lets you share a USB printer that is connected to the USB port on your router. You can share this USB printer among the Windows and Mac computers on your network.

This chapter contains the following sections:

- *Install the Printer Driver and Cable the Printer*
- *Download the ReadySHARE Printer Utility*
- *Install the ReadySHARE Printer Utility*
- *Use the Shared Printer*
- *View or Change the Status of a Printer*
- *Use the Scan Feature of a Multifunction USB Printer*
- *Change NETGEAR USB Control Center Settings*

Install the Printer Driver and Cable the Printer

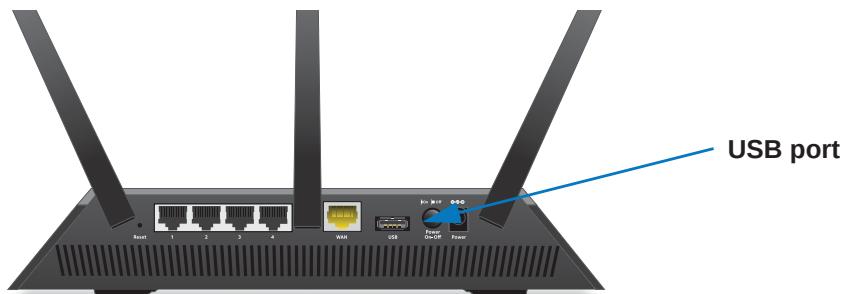
Some USB printer manufacturers (for example, HP and Lexmark printers) request that you do not connect the USB cable until the installation software prompts you to do so.

➤ **To install the driver and cable the printer:**

1. On each computer on your network that shares the USB printer, install the driver software for the USB printer.

If you do not have the printer driver, contact the printer manufacturer.

2. Use a USB printer cable to connect the USB printer to the router USB port.



Download the ReadySHARE Printer Utility

The utility works on Windows and Mac computers.

➤ **To download the utility:**

1. Visit www.netgear.com/readysware.



2. In the ReadySHARE Printer pane, click the **PC Utility** or **Mac Utility** link.
3. Follow the onscreen instructions to download the file.

Install the ReadySHARE Printer Utility

You must install the ReadySHARE Printer utility on each computer that will share the printer. After you install it, the utility displays as NETGEAR USB Control Center on your computer.

➤ **To install the utility:**

1. Double-click the ReadySHARE Printer utility setup file that you downloaded.

The InstallShield wizard displays.



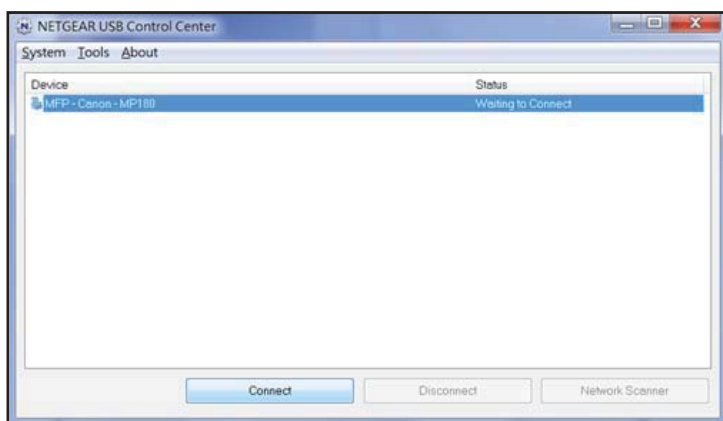
2. Follow the wizard instructions to install NETGEAR USB Control Center.

After the InstallShield Wizard completes the installation, the NETGEAR USB Control Center prompts you to select a language:



3. Select a language from the list and click the **OK** button.

The NETGEAR USB Control Center displays the main screen.



Some firewall software, such as Comodo, blocks NETGEAR USB Control Center from accessing the USB printer. If you do not see the USB printer displayed in the screen, you can disable the firewall temporarily to allow the utility to work.

4. Select the printer and click the **Connect** button.

The printer status changes to Manually connected by *Mycomputer*. Now, only your computer can use the printer.

5. Click the **Disconnect** button.

The status changes to Available. Now all computers on the network can use the printer.

6. To exit the utility, select **System > Exit**.

Use the Shared Printer

For each computer, after you click the **Connect** and **Disconnect** buttons once, the utility automatically manages the printing queue and handling. By default, the utility starts automatically whenever you log on to Windows and runs in the background.

➤ To manually connect and print:

1. Click the NETGEAR USB Control Center icon .

The main screen displays.

2. Click the **Connect** button.

The printer status changes to Manually connected by *Mycomputer*. Now, only the computer you are using can use this printer.

3. Use the print feature in your application to print your document.
4. To release the printer so that all computers on the network can use it, click the **Disconnect** button.

➤ **To print and release the printer to any computer on the network:**

1. To print your document, use the print feature in your application.

The NETGEAR USB Control Center automatically connects your computer to the USB printer and prints the document. If another computer is already connected to the printer, your print job goes into a queue to wait to be printed.

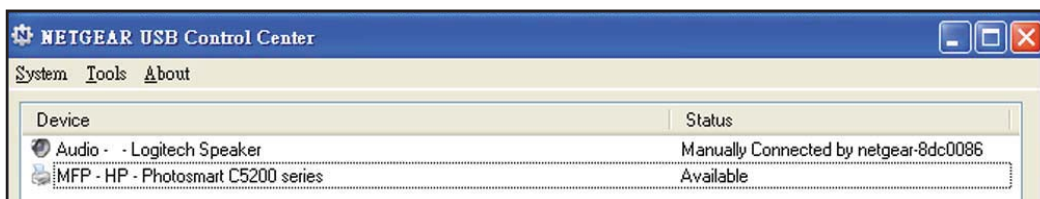
2. If your document does not print, use the NETGEAR USB Control Center to check the status.

View or Change the Status of a Printer

➤ **To view or change the status:**

1. Click the NETGEAR USB Control Center icon .

The main screen displays.



The Status column shows the status for each device:

- **Available.** No print jobs are in process. You can use the USB printer from any computer in the network.
 - **Connected.** Your computer is connected to the printer and will be released when your print job is done.
 - **Manually Connected by.** Only the connected computer can use the printer.
 - **Waiting to Connect.** Your computer is not connected to the shared printer yet.
2. To print from your computer when the status shows Manually connected by to another computer, click the **Disconnect** button.

The printer is released from the connection and the status changes to Available.

3. To print from your computer when the status shows Waiting to Connect:

- a. Click the **Connect** button.

The printer status changes to Manually connected by *Mycomputer*. Now, only your computer can use the printer.

- b. To allow the printer to be shared, click the **Disconnect** button.

The printer is released from the connection and the status changes to Available.

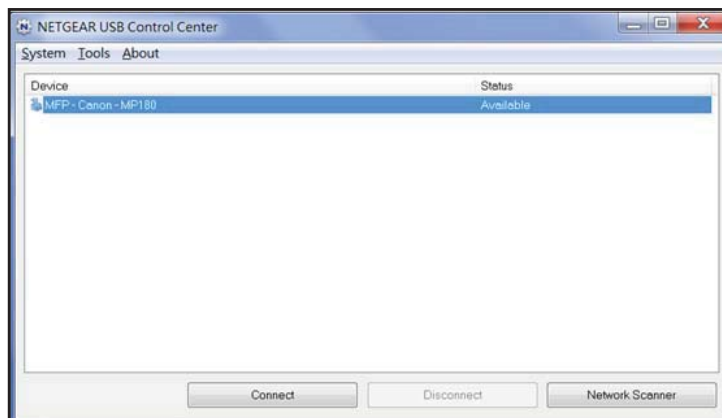
Use the Scan Feature of a Multifunction USB Printer

If your USB printer supports scanning, you can also use the USB printer for scanning. For example, the USB printer displayed in the Windows Printers and Faxes window is ready for print jobs.



➤ **To use the scan feature of a multifunction USB printer:**

1. Launch the NETGEAR USB Control Center.
2. Make sure that the printer status shows as Available.
3. Click the **Network Scanner** button.



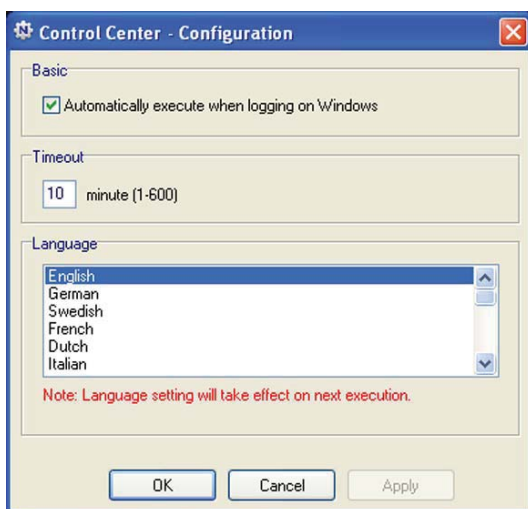
The scanner screen displays so that you can use the USB printer for scanning.

Change NETGEAR USB Control Center Settings

You can stop the NETGEAR USB Control Center from starting automatically when you log in to Windows. You can also change the language and specify the time-out to release the printer connection.

➤ **To turn off automatic NETGEAR USB Control Center startup:**

1. Select **Tools > Configuration**.



2. Clear the **Automatically execute when logging on Windows** check box.
3. Click the **OK** button.

Your change is saved.

➤ **To change the language:**

1. Select **Tools > Configuration**.
2. In the **Language** list, select a language.
3. Click the **OK** button.

The next time NETGEAR USB Control Center starts, the language changes.

➤ **To specify the time-out:**

1. Select **Tools > Configuration**.
2. In the **Timeout** field, type the number of minutes.

The time-out is the number of minutes that a computer holds its connection to the printer when the connection isn't being used.

3. Click the **OK** button.

Your change is saved.

10. Specify Network Settings

10

This chapter includes the following sections:

- *View WAN Settings*
- *Set Up a Default DMZ Server*
- *Change the Router's Device Name*
- *Change the LAN TCP/IP Settings*
- *Specify the IP Addresses that the Router Assigns*
- *Disable the DHCP Server Feature in the Router*
- *Reserve LAN IP Addresses*
- *Use the WPS Wizard for WiFi Connections*
- *Specify Basic WiFi Settings*
- *Change the WiFi Security Option*
- *Set Up a Guest Network*
- *Control the Wireless Radios*
- *Set Up a Wireless Schedule*
- *Specify WPS Settings*
- *Use the Router as a Wireless Access Point*
- *Set Up the Router*
- *Set Up a Wireless Distribution System*

View WAN Settings

You can view or configure wide area network (WAN) settings for the Internet port. You can set up a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping to its WAN (Internet) port.

➤ **To view the WAN settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

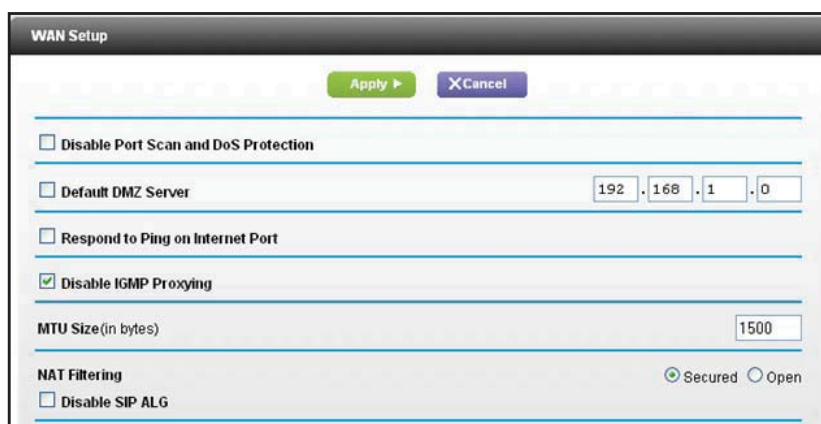
A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Setup > WAN Setup**.



The screenshot shows the WAN Setup configuration interface. At the top, there are 'Apply' and 'Cancel' buttons. Below them are several settings:

- ☐ Disable Port Scan and DoS Protection
- ☐ Default DMZ Server: 192 . 168 . 1 . 0
- ☐ Respond to Ping on Internet Port
- ☒ Disable IGMP Proxying
- MTU Size (in bytes): 1500
- NAT Filtering: ☒ Secured ☐ Open
- ☐ Disable SIP ALG

The following settings display:

- **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. Select this check box only in special circumstances.
- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing, but it makes the firewall security less effective. See [Set Up a Default DMZ Server](#) on page 97.
- **Respond to Ping on Internet Port.** This feature allows your router to be discovered. Use this feature only as a diagnostic tool or if you have a specific reason.
- **Disable IGMP Proxying.** IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.

- **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. Change the MTU only if you are sure that it is necessary for your ISP connection. See [Change the MTU Size](#) on page 37.
 - **NAT Filtering.** Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall, but allows almost all Internet applications to work.
5. Click the **Apply** button.
- Your changes are saved.

Set Up a Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the default DMZ server.



WARNING:

DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

The router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have the router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➤ To set up a default DMZ server:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Setup > WAN Setup**.
5. Select the **Default DMZ Server** check box.
6. Type the IP address.
7. Click the **Apply** button.

Your change takes effect.

Change the Router's Device Name

The router's device name is R7000. This device name displays in file manager when you browse your network.

➤ **To change the router's device name:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Setup > LAN Setup**
5. In the Device Name field, type a new name.
6. Click the **Apply** button.

Your change is saved.

Change the LAN TCP/IP Settings

The router is preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The 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 designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings

You might want to change these settings if you need a specific IP subnet that one or more devices on the network uses, or if you have competing subnets with the same IP scheme.

➤ To change the LAN TCP/IP settings:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Setup > LAN Setup**.

LAN Setup

Apply Cancel

Device Name: R7000

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disabled

☒ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

+ Add Edit Delete

5. In the **IP Address** field, type the IP address.

6. In the **IP Subnet Mask**, type the subnet mask of the router.

The IP address and subnet mask identifies which addresses are local to a specific device and which must be reached through a gateway or router.

7. Change the RIP settings.

Router Information Protocol (RIP) allows a router to exchange routing information with other routers.

- a. In the **RIP Direction** list, select one of the following:

- **Both.** The router broadcasts its routing table periodically and incorporates information that it receives.
- **Out Only.** The router broadcasts its routing table periodically.
- **In Only.** The router incorporates the RIP information that it receives.

- b. In the **RIP Version** list, select one of the following:

- **Disabled.** This is the default setting.
 - **RIP-1.** This format is universally supported. It is adequate for most networks, unless you have an unusual network setup.
 - **RIP-2.** This format carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
8. Click the **Apply** button.
- Your changes are saved.
- If you changed the LAN IP address of the router, you are disconnected when this change takes effect.
9. To reconnect, close your browser, relaunch it, and log in to the router

Specify the IP Addresses that the Router Assigns

By default, the router acts as a Dynamic Host Configuration Protocol (DHCP) server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router.

These addresses must be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you can save part of the range for devices with fixed addresses.

- **To specify the pool of IP addresses that the router assigns:**
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
 2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
 3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.

4. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' configuration window. At the top, there are 'Apply' and 'Cancel' buttons. Below is the 'Device Name' field set to 'R7000'. The 'LAN TCP/IP Setup' section includes fields for 'IP Address' (192.168.1.1), 'IP Subnet Mask' (255.255.255.0), 'RIP Direction' (Both), and 'RIP Version' (Disabled). The 'Use Router as DHCP Server' checkbox is checked. Below this, the 'Starting IP Address' is 192.168.1.2 and the 'Ending IP Address' is 192.168.1.254. At the bottom, there is an 'Address Reservation' table with columns for '#', 'IP Address', 'Device Name', and 'MAC Address', and buttons for '+Add', 'Edit', and 'Delete'.

5. Make sure that the **Use Router as DHCP Server** check box is selected.
6. Specify the range of IP addresses that the router assigns:
 - a. In the **Starting IP Address** field, type the lowest number in the range.
This IP address must be in the same subnet as the router.
 - b. In the **Ending IP Address** field, type the number at the end of the range of IP addresses.
This IP address must be in the same subnet as the router.
7. Click the **Apply** button.
Your settings are saved.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- DNS server IP address (the router's LAN IP address)

Disable the DHCP Server Feature in the Router

By default, the router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router.

You can use another device on your network as the DHCP server, or specify the network settings of all your computers.

➤ **To disable the DHCP server feature in the router:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > Setup > LAN Setup**.
5. Clear the **Use Router as DHCP Server** check box.
6. Click the **Apply** button.
7. (Optional) If this service is disabled and no other DHCP server is on your network, set your computer IP addresses manually so that they can access the router.

Reserve LAN IP Addresses

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Assign reserved IP addresses to computers or servers that require permanent IP settings.

➤ **To reserve an IP address:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > Setup > LAN Setup**.
5. In the Address Reservation section of the screen, click the **Add** button.
6. In the **IP Address** field, type the IP address to assign to the computer or server.
Choose an IP address from the router's LAN subnet, such as 192.168.1.x.
7. Type the MAC address of the computer or server.

Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

8. Click the **Apply** button.

The reserved address is entered into the table.

The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

➤ **To edit a reserved address entry:**

1. Select the radio button next to the reserved address.
2. Click the **Edit** button.
3. Change the settings.
4. Click the **Apply** button.

Your changes are saved.

➤ **To delete a reserved address entry:**

1. Select the radio button next to the reserved address.
2. Click the **Delete** button.

The address is removed.

Use the WPS Wizard for WiFi Connections

The WPS Wizard helps you add a wireless computer or device to your WiFi network without typing the WiFi password.

➤ **To use the WPS Wizard:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > WPS Wizard**.

5. Click the **Next** button.



6. Select the radio button for the setup method that you want to use:
 - **Push button.** Click the **WPS** button on this screen.
 - **PIN Number.** The screen adjusts. Enter the client security PIN, and click the **Next** button.
7. Within two minutes, go to the client device and use its WPS software to connect to the WiFi network.

The WPS process automatically sets up your wireless computer with the network password when it connects. The router WPS screen displays a confirmation message.

Specify Basic WiFi Settings

The router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the router label.

Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

NETGEAR recommends that you do not change your preset security settings. If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

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

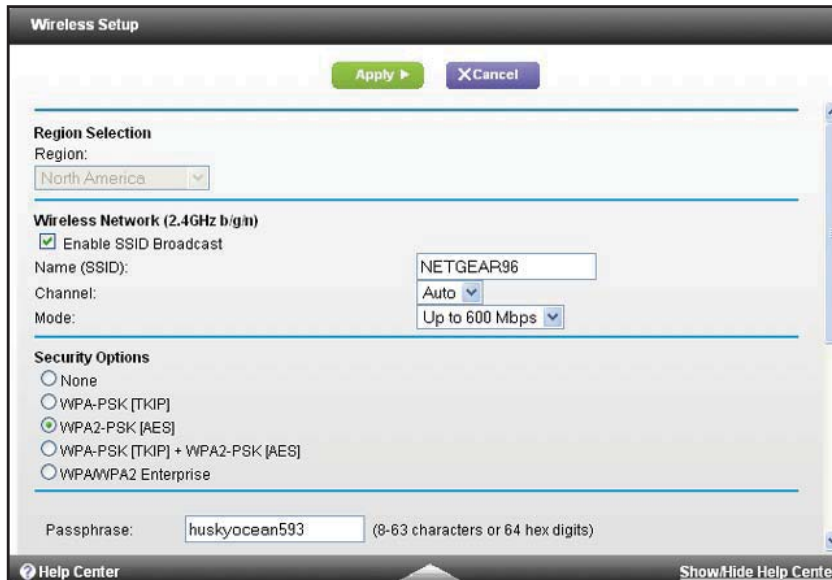
➤ **To specify basic wireless settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **Wireless**.

The screenshot shows the 'Wireless Setup' window. At the top, there are 'Apply' and 'Cancel' buttons. Below is the 'Region Selection' section with a 'Region:' dropdown menu set to 'North America'. The 'Wireless Network (2.4GHz b/g/n)' section includes a checked 'Enable SSID Broadcast' checkbox, a 'Name (SSID):' text field containing 'NETGEAR96', a 'Channel:' dropdown set to 'Auto', and a 'Mode:' dropdown set to 'Up to 600 Mbps'. The 'Security Options' section has radio buttons for 'None', 'WPA-PSK (TKIP)', 'WPA2-PSK (AES)' (which is selected), 'WPA-PSK (TKIP) + WPA2-PSK (AES)', and 'WPA/WPA2 Enterprise'. At the bottom, there is a 'Passphrase:' text field with 'huskyocean593' and a note '(8-63 characters or 64 hex digits)'. A 'Help Center' link is in the bottom left, and 'Show/Hide Help Center' is in the bottom right.

5. In the **Region** list, select your region. In some locations, you cannot change this setting.

6. To control the SSID broadcast, select or clear the **Enable SSID Broadcast** check box.

When this check box is selected, the router broadcasts its network name (SSID) so that it displays when you scan for local WiFi networks on your computer or wireless device.

7. To allow computers or wireless devices that join the network to use the Internet but not to access each other or access Ethernet devices on the network, select the **Enable Wireless Isolation** check box.

8. To change the network name (SSID), type a new name in the **Name (SSID)** field.

The name can be up to 32 characters long and it is case-sensitive. The default SSID is randomly generated and is on the router's label. If you change the name, make sure to write down the new name and keep it in a safe place.

9. To change the wireless channel, select a number in the **Channel** list.

In some regions, not all channels are available. 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.

When you use multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is four channels (for example, use Channels 1 and 5, or 6 and 10).

10. To change the mode, select it from the Mode list.

For 2.4 GHz, **Up to 600 Mbps** is the default setting. The other settings are **Up to 289 Mbps** and **Up to 54 Mbps**.

At 5 GHz, **Up to 1300 Mbps** is the default setting, which allows 802.11ac and 802.11a wireless devices to join the network. The other settings are **Up to 600 Mbps** and **Up to 289 Mbps**.

11. Click the **Apply** button.

Your settings are saved.

If you connected wirelessly to the network and you changed the SSID, you are disconnected from the network.

12. Make sure that you can connect wirelessly to the network with its new settings.

If you cannot connect wirelessly, check the following:

- Is your computer or wireless device connected to another wireless network in your area? Some wireless devices automatically connect to the first open network without wireless security that they discover.
- Is your computer or wireless device trying to connect to your network with its old settings (before you changed the settings)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

Change the WiFi Security Option

Your router comes with preset WPA2 or WPA security. The password that you enter to connect to your network is unique to your router and is on the router label. NETGEAR recommends that you use the preset security, but you can change them. NETGEAR recommends that you do not disable security.

➤ **To change the WPA settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.

A login screen displays.

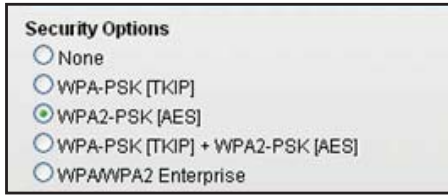
3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **Wireless**.

5. Under **Security Options**, select a radio button for a WPA option.



The screenshot shows a box titled "Security Options" with five radio button options. The third option, "WPA2-PSK [AES]", is selected, indicated by a green dot in the center of the radio button.

Security Options
☐ None
☐ WPA-PSK [TKIP]
☒ WPA2-PSK [AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
☐ WPA/WPA2 Enterprise

The WPA2 options use the newest standard for the strongest security, but some older computers and wireless devices cannot use WPA2. By default, the **WPA-PSK [TKIP] + WPA2-PSK [AES]** radio button is selected so that new or old computers and wireless devices can connect to the WiFi network by using either WPA2 or WPA security.

The Passphrase field displays.

6. In the **Passphrase** field, enter the network key (password) that you want to use.
It is a text string from 8 to 63 characters.
7. Write down the new password and keep it in a secure place for future reference.
8. Click the **Apply** button.
Your changes are saved.

Set Up a Guest Network

A guest network allows visitors at your home to use the Internet without using your wireless security key. You can add a guest network to each wireless network: 2.4 GHz b/g/n and 5.0 GHz a/n.

➤ **To set up a guest network:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **Guest Network**.

5. Select any of the following wireless settings:

- **Enable Guest Network.** When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
- **Enable SSID Broadcast.** If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.
- **Allow guest to see each other and access my local network.** If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.

6. Give the guest network a name.

The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.

7. Select a radio button for a security option.

The WPA2 options use the newest standard for the strongest security, but some older computers and wireless devices cannot use it. NETGEAR recommends that you select the **WPA-PSK [TKIP] + WPA2-PSK [AES]** radio button. This setting protects your WiFi network and lets computers and wireless devices can connect to the WiFi network by using either WPA2 or WPA security.

8. Click the **Apply** button.

Your settings are saved.

Control the Wireless Radios

The router has internal wireless radios that broadcast signals in the 2.4 GHz and 5 GHz range. By default, they are on so that you can connect wirelessly to the router. When the wireless radios are off, you can still use an Ethernet cable for a LAN connection to the router.

You can turn the wireless radios on and off with the **WiFi On/Off** button on the router, or you can log in to the router and enable or disable the wireless radios. If you are close to the router, it might be easier to press its **WiFi On/Off** button. If you are away from the router or have already logged in it might be easier to enable or disable them. You can also turn the WiFi radios off and on based on a schedule. (See [Set Up a Wireless Schedule](#) on page 110).

Use the WiFi On/Off Button

➤ **To turn the wireless radios off and on with the WiFi On/Off button:**

Press the **WiFi On/Off** button on the top of the router for two seconds.

If you turned off the wireless radios, the WiFi On/Off LED and the WPS LED turn off. If you turned on the wireless radios, the WiFi On/Off LED and the WPS LED light.

Enable or Disable the Wireless Radios

If you used the WiFi On/Off button to turn off the wireless radios, you can't log in to the router to turn them back on. You must press the **WiFi On/Off** button again for two seconds to turn the wireless radios back on.

➤ **To enable or disable the wireless radios:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

5. Select or clear the **Enable Wireless Radio** check boxes in the 2.4 GHz and 5 GHz sections of the screen.

Clearing this check box turns off the WiFi feature of the router.

6. Click the **Apply** button.

If you turned off both wireless radios, the WiFi On/Off LED and the WPS LED turn off. If you turned on the wireless radios, the WiFi On/Off LED and the WPS LED light.

Set Up a Wireless Schedule

You can use this feature to turn off the wireless signal from your router at times when you do not need a wireless connection. For example, you might turn it off for the weekend if you leave town.

➤ To set up the wireless schedule:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

5. Click the **Add a new period** button.

6. Use the lists, radio buttons, and check boxes to set up a period during which you want to turn off the wireless signal.
7. Click the **Apply** button.
The Advanced Wireless Settings screen displays.
8. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
9. Click the **Apply** button.

Specify WPS Settings

Wi-Fi Protected Setup (WPS) lets you join the WiFi network without typing the WiFi password.

➤ To specify WPS Settings:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Router's PIN field displays the PIN that you use on a registrar (for example, from the Network Explorer on a Vista Windows computer) to configure the router's wireless settings through WPS.

5. (Optional) Select or clear the **Disable Router's PIN** check box.

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

6. (Optional) Select or clear the **Keep Existing Wireless Settings** check box.

By default, the Keep Existing Wireless Settings check box is selected. NETGEAR recommends that you leave this check box selected.

If you clear this check box, the next time a new wireless client uses WPS to connect to the router, the router wireless settings change to an automatically generated random SSID and security key.

7. Click the **Apply** button.

Your changes are saved.

Use the Router as a Wireless Access Point

You can set up the router to run as an access point (AP) on the same local network as another router.

➤ To set up the router as an AP:

1. Use an Ethernet cable to connect the Internet port of this router to a LAN port in the other router.

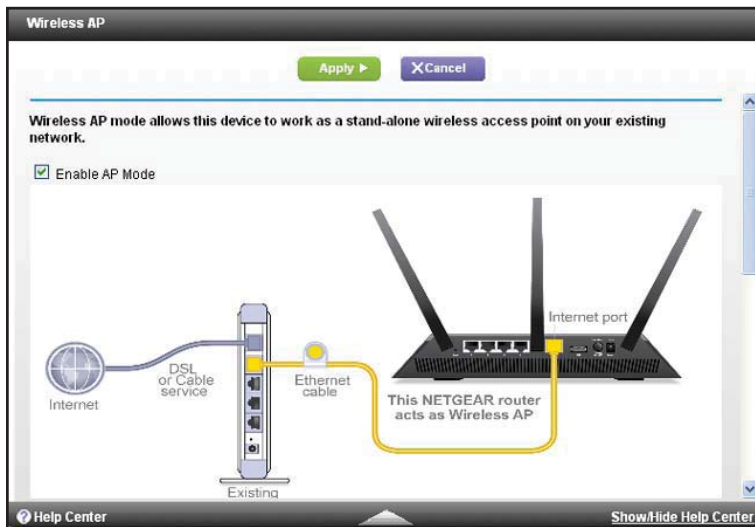


2. Launch an Internet browser from a computer or wireless device that is connected to the network.
3. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.
A login screen displays.
4. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > Wireless AP**.



6. Select the **Enable AP Mode** check box.

7. Scroll down and select the radio button for the IP address setting that you want to use:

- **Get dynamically from existing router.** The other router on the network assigns an IP address to this router while this router is in AP mode.
- **Enable fixed IP settings on this device (not recommended).** Use this setting if you want to manually assign a specific IP address to this router while it is in AP mode. Using this option effectively requires advanced network experience.

Note: To avoid interference with other routers or gateways in your network, NETGEAR recommends that you use different wireless settings on each router. You can also turn off the wireless radio on the other router or gateway and use the R7000 only for wireless client access.

8. Click the **Apply** button.

The IP address of the router changes, and you are disconnected.

9. To reconnect, close and restart your browser and type **http://www.routerlogin.net**.

11. Manage Your Network

11

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

This chapter includes the following sections:

- *Update the Router Firmware*
- *Change the admin Password*
- *Recover the admin Password*
- *View Router Status*
- *View Logs of Router Activity*
- *Monitor Internet Traffic*
- *Create Custom Static Routes*
- *View Devices Currently on the Network*
- *Manage the Router Configuration File*
- *Remote Management*

Update the Router Firmware

The router firmware (routing software) is stored in flash memory. You might see a message at the top of the genie screens when new firmware is available. You can respond to that message to update the firmware, or you can check to see if new firmware is available, and to update your product.

➤ **To check for new firmware and update your router:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Router Update**.

5. Click the **Check** button.

The router finds new firmware information if any is available and displays a message asking if you want to download and install it.

6. Click the **Yes** button.

The router locates and downloads the firmware and begins the update.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the router.

When the upload is complete, your router restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to find out if you need to reconfigure the router after upgrading.

Change the admin Password

This feature let you change the default password that is used to log in to the router with the user name admin. This password is not the one that you use for WiFi access. The label on your router shows your unique wireless network name (SSID) and password for wireless access.

➤ **To set the password for the user name admin:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

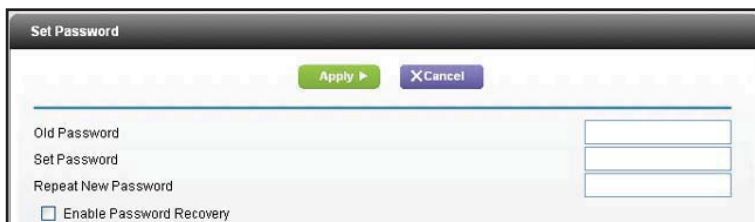
A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Set Password**.



5. Type the old password, and type the new password twice.
6. If you want to be able to recover the password, select the **Enable Password Recovery** check box.

NETGEAR recommends that you enable password recovery.

7. Click the **Apply** button.

Your changes take effect.

Recover the admin Password

NETGEAR recommends that you enable password recovery if you change the password for the router user name admin. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➤ **To set up password recovery:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Set Password**.
5. Select the **Enable Password Recovery** check box.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.

Your changes are saved.

➤ **To recover your password:**

1. In the address field of your browser, type **www.routerlogin.net**.

A login screen displays.

2. Click **Cancel**.

If password recovery is enabled, you are prompted to answer two security questions.

3. Enter the saved answers to the security questions.
4. Enter the serial number of your router.

The serial number is on the router's label.

View Router Status

➤ **To view router status and usage information:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

Router Information		Internet Port	
Hardware Version	R7000	MAC Address	44:94:FC:44:52:F4
Firmware Version	V1.0.0.156_1.0.15	IP Address	10.1.10.13
GUI Language Version	V1.0.0.156_2.1.31.7	Connection	DHCP
LAN Port		IP Subnet Mask	255.255.255.0
MAC Address	44:94:FC:44:52:F3	Domain Name Server	75.75.75.75
IP Address	192.168.1.1		75.75.76.76
DHCP	On		
Reboot		Show Statistics Connection Status	

Wireless Settings (2.4GHz)		Wireless Settings (5GHz)	
Name (SSID)	NETGEAR96	Name (SSID)	NETGEAR96-5G
Region	North America	Region	North America
Channel	Auto (4)	Channel	149 + 153(P) + 157 + 161
Mode	Up to 600 Mbps	Mode	Up to 1300 Mbps
Wireless AP	On	Wireless AP	On
Broadcast Name	On	Broadcast Name	On
Wi-Fi Protected Setup	Configured	Wi-Fi Protected Setup	Configured

Guest Network (2.4 GHz)		Guest Network (5 GHz)	
Name (SSID)	NETGEAR-Guest	Name (SSID)	NETGEAR-5G-Guest
Wireless AP	Off	Wireless AP	Off
Broadcast Name	On	Broadcast Name	On
Allow guests to see each other and access Off my local network		Allow guests to see each other and access Off	

5. For information about the displayed settings, click the **Show/Hide Help Center** link at the bottom of the screen.

Display Internet Port Statistics

➤ To display Internet port statistics:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
4. The BASIC Home screen displays
5. Click the **ADVANCED** tab.

6. In the Internet Port pane, click the **Show Statistics** button.

Show Statistics							
System Up Time 00:09:15							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	1000M/Full	887	7078	0	308	3584	00:06:57
LAN1	Link Down	1872	1600	0	3474	432	--
LAN2	Link Down						--
LAN3	1000M/Full						00:09:15
LAN4	Link Down						--
2.4G WLAN b/g/n	217M	0	0	0	0	0	00:08:57
5G WLAN a/n/ac	1300M	0	0	0	0	0	00:08:57

Poll Interval: (5~86400 Seconds)

The following information displays:

- **System Up Time.** The time elapsed since the router was last restarted.
 - **Port.** The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:
 - **Status.** The link status of the port.
 - **TxPkts.** The number of packets transmitted on this port since reset or manual clear.
 - **RxPkts.** The number of packets received on this port since reset or manual clear.
 - **Collisions.** The number of collisions on this port since reset or manual clear.
 - **Tx B/s.** The current transmission (outbound) bandwidth used on the WAN and LAN ports.
 - **Rx B/s.** The current reception (inbound) bandwidth used on the WAN and LAN ports.
 - **Up Time.** The time elapsed since this port acquired the link.
 - **Poll Interval.** The interval at which the statistics are updated in this screen.
7. To change the polling frequency, enter a time in seconds in the Poll Interval field and click the **Set Interval** button.
8. To stop the polling entirely, click the **Stop** button.

Check the Internet Connection Status

➤ To check the Internet connection status:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Click the **ADVANCED** tab.
5. In the Internet Port pane, click the **Connection Status** button.

Connection Status	
IP Address	10.1.10.16
Subnet Mask	255.255.255.0
Default Gateway	10.1.10.1
DHCP Server	10.1.10.1
DNS Server	75.75.75.75 75.75.76.76
Lease Obtained	7 days,0 Hours,0 minutes
Lease Expires	6 days,23 Hours,52 minutes
Release Renew	
Close Window	

The following information displays:

- **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 when the lease was obtained.
 - **Lease Expires.** The date and time that the lease expires.
6. To return the status of all items to 0, click the **Release** button.
 7. To refresh the screen, click the **Renew** button.
 8. To exit the screen, click the **Close Window** button.

View Logs of Router Activity

The log is a detailed record of the websites you have accessed or attempted to access and other router actions. Up to 256 entries are stored in the log. Log entries display only when keyword blocking is enabled and no log entries are made for the trusted user.

➤ To view logs:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

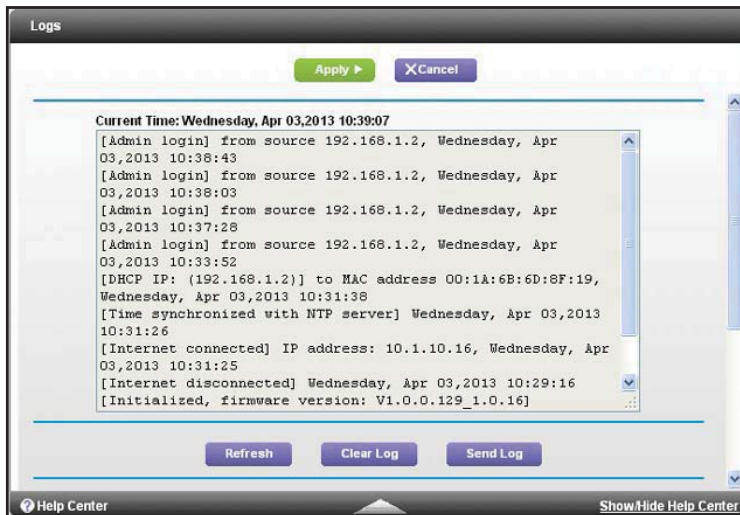
A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Logs**.



The log screen shows the following information:

- **Date and time.** The date and time the log entry was recorded.
- **Source IP.** The IP address of the initiating device for this log entry.
- **Target address.** The name or IP address of the website or news group visited or to which access was attempted.
- **Action.** The action that occurred, such as whether Internet access was blocked or allowed.

5. To refresh the log screen, click the **Refresh** button.
6. To clear the log entries, click the **Clear Log** button.
7. To email the log immediately, click the **Send Log** button.

Monitor Internet Traffic

Traffic metering allows you to monitor the volume of Internet traffic that passes through the router Internet port. You can set limits for traffic volume.

➤ To monitor Internet traffic:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

Scroll to view more settings

5. Select the **Enable Traffic Meter** check box.

6. (Optional) Control the volume of Internet traffic.

You can use either the traffic volume control feature or the connection time control feature:

- Select the **Traffic volume control by** radio button and then select one of the following options:
 - **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.
- Select the **Connection time control** radio button and enter the allowed hours in the Monthly limit field.

7. (Optional) If your ISP charges for extra data volume when you make a new connection, enter the extra data volume in MB in the Round up data volume for each connection by field.

8. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

If you want the traffic counter to start immediately, click the **Restart Counter Now** button.

9. In the Traffic Control section, specify whether the router should issue a warning message before the monthly limit of Mbytes or hours is reached.

By default, the value is 0 and no warning message is issued. You can select one of the following to occur when the limit is attained:

- The Internet LED blinks green or amber.
- The Internet connection is disconnected and disabled.

10. Click the **Apply** button.

The Internet Traffic Statistics section helps you to monitor the data traffic.

11. To update the Traffic Statistics section, click the **Refresh** button.

12. To display more information about the data traffic on your router and to change the poll interval, click the **Traffic Status** button.

Create Custom Static Routes

Static routes provide more routing information to your router. Typically, you do not need to add static routes unless you have multiple routers or multiple IP subnets on your network.

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

- Your main 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 set up your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you try to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the company firewall is likely to deny the request.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. Here is an 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 should be forwarded to the ISDN router at 192.168.1.100.
- A metric value of 1 works because the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

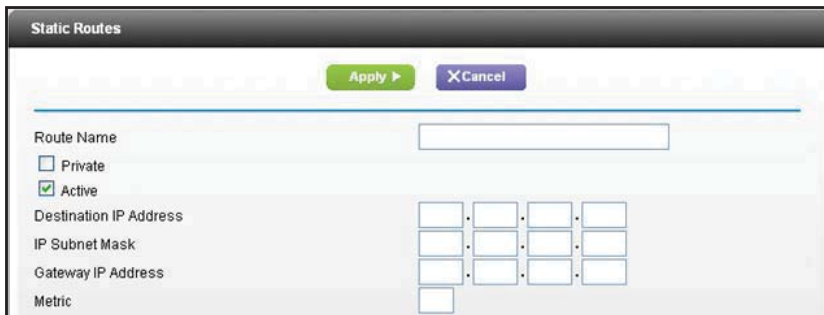
➤ **To set up a static route:**

- 1.** Launch an Internet browser from a computer or wireless device that is connected to the network.
- 2.** Type **<http://www.routerlogin.net>** or **<http://www.routerlogin.com>**.
A login screen displays.
- 3.** Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Static Routes**.
5. Click the **Add** button.



6. In the **Route Name** field, type a name for this static route (for identification purposes only.)
7. Select the **Private** check box if you want to limit access to the LAN only.
If Private is selected, the static route is not reported in RIP.
8. Select the **Active** check box to make this route effective.
9. Type the IP address of the final destination.
10. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
11. Type the gateway IP address, which must be on the same LAN segment as the router.
12. Type a number from 1 through 15 as the metric value.

This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

13. Click the **Apply** button.

The static route is added.

➤ **To edit a static route:**

1. In the table, select the radio button for the route.
2. Click the **Edit** button.

The Static Routes screen adjusts.

3. Edit the route information.
4. Click the **Apply** button.

Your changes are saved.

➤ **To delete a static route:**

1. In the table, select the radio button for the route.
2. Click the **Delete** button.

The route is removed from the table.

View Devices Currently on the Network

You can view all computers or devices that are currently connected to your network.

➤ **To view devices on the network:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **Attached Devices**.

Attached Devices				
Go to Access Control to allow or block devices.				
Access Control: Turned Off				Refresh
Wired Devices				
Status	Device Name	IP Address	MAC Address	Connection Type
Allowed	TECHPUBS	192.168.1.2	00:1A:6B:6D:8F:19	Wired
Wireless Devices (Wireless intruders also show up here)				
Status	Device Name	IP Address	MAC Address	Connection Type

The Wired Devices section lists devices that are connected to the router with Ethernet cables. The Wireless Devices section lists devices that are connected to the wireless network. The following information is displayed:

- **Status.** The status of the device, Allowed or Blocked.
 - **Device Name.** If the device name is known, it is shown here.
 - **IP Address.** The IP address that the router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
 - **MAC Address.** The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
5. To update this screen, click the **Refresh** button.

Manage the Router Configuration File

The configuration settings of the router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➤ **To back up the router's configuration settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Backup Settings**.



5. Click the **Back Up** button.
6. Specify a location on your network.

A copy of the current settings is saved in the location you specified.

Restore Configuration Settings

➤ **To restore configuration settings that you backed up:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Backup Settings**.
5. Click the **Browse** button to find and select the `cfg` file.
6. Click the **Restore** button.

The file is uploaded to the router and the router reboots.



WARNING:

Do not interrupt the reboot process.

Erase the Current Configuration Settings

You can erase the current configuration and restore the factory default settings. You might want to do this if you move the router to a different network. (See *Factory Settings* on page 164).

➤ **To erase the configuration settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **`http://www.routerlogin.net`** or **`http://www.routerlogin.com`**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Backup Settings**.
5. Click the **Erase** button.

The factory default settings are restored. The user name is `admin`, the password is `password`, and the LAN IP address is `192.168.1.1`. DHCP is enabled.

Remote Management

The remote management feature lets you access your router over the Internet to view or change its settings. You need to know the router's WAN IP address to use this feature. For information about remote access using Dynamic DNS, see *Chapter 7, Access the Router's USB Drive Through the Internet*.

Note: Be sure to change the password for the user name admin to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See [Change the admin Password](#) on page 121.

➤ **To set up remote management:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Remote Management**.

5. Select the **Turn Remote Management On** check box.
6. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the router's remote management:

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

Select one of the following:

- To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address to be allowed access.

- To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. Enter a beginning and ending IP address to define the allowed range.
- To allow access from any IP address on the Internet, select the **Everyone** radio button.

7. Specify the port number for accessing the web management interface.

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

8. Click the **Apply** button.

Your changes take effect.

➤ **To use remote access:**

- 1.** Launch an Internet browser on a computer that is not on your home network.
- 2.** 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, enter **http://134.177.0.123:8080** in your browser.

12. Use VPN to Access Your Network 12

This chapter includes the following sections:

- *Set Up a VPN Connection*
- *Specify VPN Service in the Router*
- *Install OpenVPN Software on Your Computer*
- *Use VPN to Access the Router's USB Drive and Media*
- *Use VPN to Access Your Internet Service at Home*

Set Up a VPN Connection

A virtual private network (VPN) lets you use the Internet to securely access your network when you aren't home.

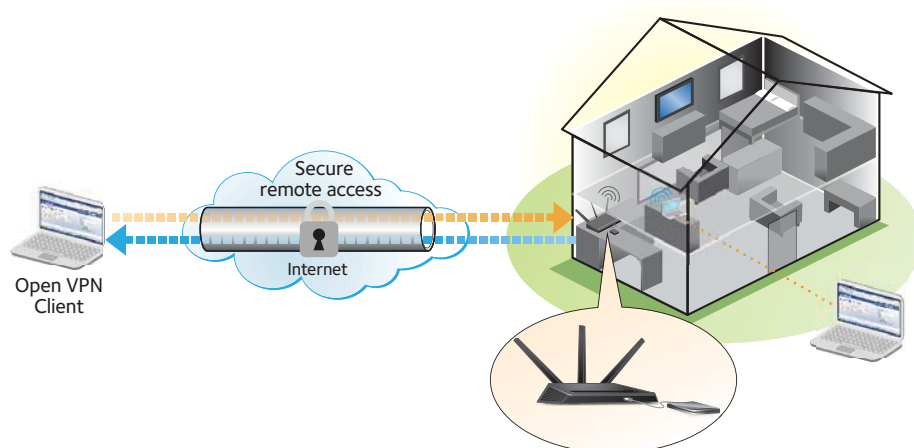


Figure 14. VPN provides a secure tunnel between your home network and a remote computer

This type of VPN access is called a client-to-gateway tunnel. The computer is the client, and the router is the gateway. To use the VPN feature, you must log in to the router and enable VPN, and you must install and run VPN client software on the computer.

Note: The router currently does not support iOS and Android VPN client software.

VPN uses DDNS or a static IP address to connect with your router.

To use a DDNS service, register for an account with a host name (sometimes called a domain name). You use the host name to access your network. The router supports these accounts: NETGEAR www.no-ip.com, www.no-ip.com, and www.DynDNS.org.

If your Internet service provider (ISP) has assigned a static WAN IP address (such as 50.196.x.x or 10.x.x.x) that never changes to your Internet account the VPN can use that IP address to connect to your home network.

Specify VPN Service in the Router

You must specify the VPN service settings in the router before you can use a VPN connection.

➤ **To specify the VPN service:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > VPN Service**.

5. Select the **Enable VPN Service** check box.

By default, the VPN uses the UDP service type and uses port 12974. If you want to customize the service type and port, NETGEAR recommends that you change these settings before you install the OpenVPN software.

6. To change the service type, scroll down and select the **TCP** radio button.
7. To change the port, scroll down to the **Service Port** field, and type the port number that you want to use.
8. Click the **Apply** button.

Your changes are saved. VPN is enabled in the router, but you must install and set up OpenVPN software on your computer before you can use a VPN connection.

Install OpenVPN Software on Your Computer

You must install this software on each computer that you plan to use for VPN connections to your router.

➤ **To install VPN client software:**

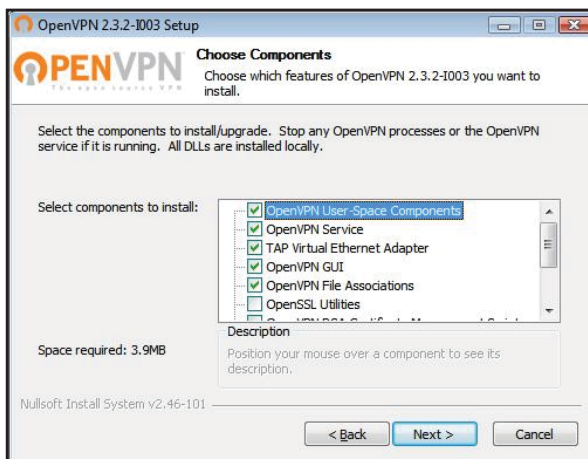
1. Visit <http://openvpn.net/index.php/download/community-downloads.html>.
2. In the Windows Installer section of the screen, double-click the **openVPN-install-xxx.exe** link.
3. Download the file.
4. To install the Open VPN software on your computer, click the **openVPN-install-xxx.exe** file.

The OpenVPN Setup Wizard displays:



5. Click the **Next** button.
6. Read the License Agreement and click the **I Agree** button.

The Choose Components screen displays:



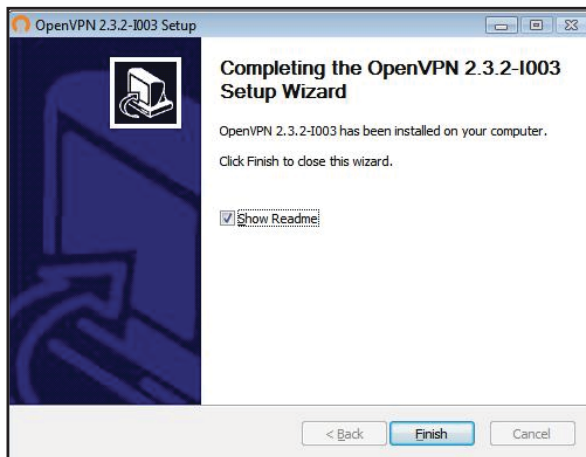
7. Leave the check boxes selected as shown, and click the **Next** button.
8. To specify the destination folder, click the **Browse** button and select a destination folder.

The following screen displays:



9. Click the **Install** button.

The screen displays the progress of the installation and then displays the final installation screen.



10. Click the **Finish** button.
11. Unzip the configuration files that you downloaded and copy them to the folder where the VPN client is installed on your device.
- For a client device with Windows 64-bit system, the VPN client is installed at C:\Program files\OpenVPN\config\ by default.
12. For a client device with Windows, modify the VPN interface name to **NETGEAR-VPN**.
- In Windows, select **Control Panel > Network and Internet > Network Connections**.
 - In the Local Area Connection list, find the local area connection with the device name **TAP-Windows Adapter**.
 - Select the Local Area Connection and change its name (not its device name) to **NETGEAR-VPN**.

If you do not change the VPN interface name, the VPN tunnel connection will fail.

Use a VPN Tunnel

After you set up the router to use VPN and install the OpenVPN application on your computer, you can open a VPN tunnel from your computer to your router over the Internet.

For the VPN tunnel to work, the local LAN IP address of the remote R7000 must have a different LAN IP scheme than the local LAN where your VPN client computer is connected. If both networks use the same LAN IP scheme, when the VPN tunnel is established, you cannot access your home router or your home network with the OpenVPN software.

The default LAN IP address scheme for the R7000 is 192.x.x.x. The most common IP schemes are 192.x.x.x, 172.x.x.x, and 10.x.x.x. If you experience a conflict, change the IP scheme either for your home network or for the network with the client VPN computer. For information about changing these settings, see [Change the LAN TCP/IP Settings](#) on page 98.

➤ To open a VPN tunnel:

1. Launch the OpenVPN application with administrator privileges.

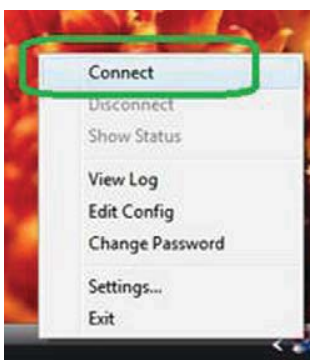


The OpenVPN icon displays in the Windows taskbar.

Tip: You can create a shortcut to the VPN program, then in the settings for the shortcut and select the **run as administrator** check box. Then every time you launch this shortcut, OpenVPN automatically runs with administrator privileges.

2. Right-click the OpenVPN icon.

A menu displays:



3. Select **Connect**.

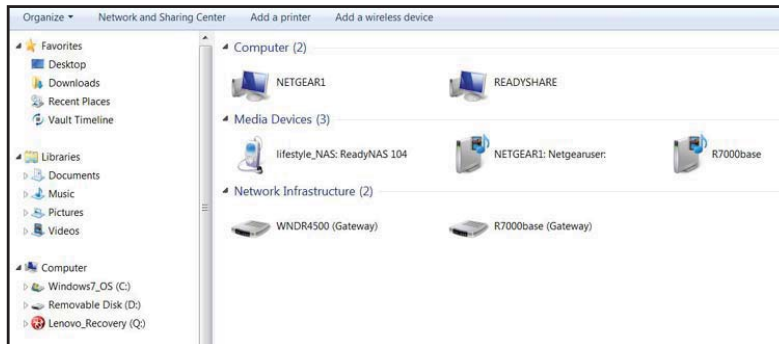
The VPN connection is established. You can do the following:

- Launch an Internet browser and log in to your router.
- Use Windows File Manager to access the router's USB drive and download files.

Use VPN to Access the Router's USB Drive and Media

➤ To access the router's USB drive and download files:

1. In Windows File Manager, select the **Network** folder.



The network resources display. The ReadySHARE icon is in the computers section and the remote R7000 icon is in the Media Devices section (if DLNA is enabled in the router).

2. If the icons do not display, click the **Refresh** button to update the screen.

If the local LAN and the remote LAN are using the same IP scheme, the remote R7000 icon does not display in the Media Devices and Network Infrastructure sections.

3. To access the router's USB drive, click the **ReadySHARE** icon.
4. To access media on the router's network, click the **R7000** icon.

Use VPN to Access Your Internet Service at Home

When you're away from home and you access the Internet, you usually use a local Internet service provider. For example, at a coffee shop you might be given a code that lets you use the coffee shop's Internet service account to surf the web.

Nighthawk lets you use a VPN connection to access your own Internet service when you're away from home. You might want to do this if you travel to a geographic location that doesn't support all the Internet services that you use at home. For example, your Netflix account might work at home, but not in a different country.

Set Up VPN Client Internet Access in the Router

By default, the router is set up to allow VPN connections only to your home network. but you can change the setting to allow Internet access. Accessing the Internet remotely through a VPN might be slower than accessing the Internet directly.

➤ To allow VPN clients to use your home Internet service:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > VPN Service**.
5. On the VPN screen, select the **Enable VPN Service** radio button.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **All sites on the Internet & Home Network** radio button.

When you access the Internet with the VPN connection, instead of using a local Internet service, you use the Internet service from your home network.

7. Click the **Apply** button.

Your settings are saved.

8. Click **For Windows** or **For Non Windows** button and download the configuration files for your VPN clients.

9. Unzip the configuration files and copy them to the folder where the VPN client is installed on your device.

For a client device with Windows 64-bit system, the VPN client is installed at C:\Program files\OpenVPN\config\ by default.

Block VPN Client Internet Access in the Router

By default, the router is set up this way. It allows VPN connections only to your home network, not to the Internet service for your home network. If you changed this setting to allow Internet access, you can change it back.

➤ To allow VPN clients to access only your home network:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.

2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > VPN Service**.
5. Select the **Enable VPN Service** radio button.

6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.

This is the default setting. The VPN connection is only to your home network, not to the Internet service for your home network.

7. Click the **Apply** button.

Your settings are saved.

8. Click **For Windows** or **For Non Windows** button and download the configuration files for your VPN clients.

9. Unzip the configuration files and copy them to the folder where the VPN client is installed on your device.

For a client device with Windows 64-bit system, the VPN client is installed at C:\Program files\OpenVPN\config\ by default.

Use a VPN Tunnel to Access Your Internet Service at Home

➤ To access your Internet service:

1. Set up the router to allow VPN access to your Internet service.
See *Set Up VPN Client Internet Access in the Router* on page 142
2. On your computer, launch the OpenVPN application.
The OpenVPN icon displays in the Windows taskbar.
3. Right-click the icon, and select Select **Connect**.
4. When the VPN connection is established, launch your Internet browser.

13. Specify Internet Port Settings

13

You can use port forwarding and port triggering to set up rules for Internet traffic. You need networking knowledge to set up these features.

This chapter includes the following sections:

- *Set Up Port Forwarding to a Local Server*
- *Set Up Port Triggering*

Set Up Port Forwarding to a Local Server

If you have a server in your home network, you can allow certain types of incoming traffic to reach the server. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

The router can forward incoming traffic with specific protocols to computers on your local network. You can specify the servers for applications and you can also specify a default DMZ server to which the router forwards all other incoming protocols.

➤ **To forward specific incoming protocols:**

1. Decide which type of service, application, or game you want to provide.
2. Find the local IP address of the computer on your network that will provide the service.

The server computer must always have the same IP address. To specify this setting, use the reserved IP address feature. See [Set Up Address Reservation](#) on page 84.

3. Launch an Internet browser from a computer or wireless device that is connected to the network.
4. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

5. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

6. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

Port Forwarding / Port Triggering

Please select the service type.

☒ Port Forwarding
☐ Port Triggering

Service Name: FTP Server IP Address: 192.168.1

#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
Edit Service Delete Service Add Custom Service						

7. Leave the **Port Forwarding** radio button selected as the service type.
8. In the Service Name list, select the service name.

If the service that you want to add is not in the list, create a custom service. See [Add a Custom Port Forwarding Service](#) on page 147.

9. In the Server IP Address field, enter the IP address of the computer that will provide the service.

10. Click the **Add** button.

The service displays in the list.

Add a Custom Port Forwarding Service

➤ To add a custom service:

1. Find out which port number or range of numbers the application uses.

You can usually find this information by contacting the publisher of the application or user groups or news groups.

2. Launch an Internet browser from a computer or wireless device that is connected to the network.

3. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

4. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

6. Leave the **Port Forwarding** radio button selected as the service type.

7. Click the **Add Custom Service** button.

8. In the **Service Name** field, enter a descriptive name.

9. In the **Service Type** field, select the protocol. If you are unsure, select **TCP/UDP**.

10. In the **External Starting Port** field, enter the beginning port number.

If the application uses 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 External Ending Port field.

11. Specify the internal ports by one of these methods:
 - Leave the **Use the same port range for Internal port** check box selected.
 - Type the port numbers in the **Internal Starting Port** and **Internal Ending Port** fields.
12. Type the IP address in the **Internal IP address** field or select the radio button for an attached device listed in the table.
13. Click the **Apply** button.

The service is now in the list on the Port Forwarding/Port Triggering screen.

Edit a Port Forwarding Service

➤ To edit a port forwarding entry:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
5. Leave the **Port Forwarding** radio button selected as the service type
6. In the table, select the radio button next to the service name.
7. Click the **Edit Service** button.
The Ports - Custom Services screen displays.
8. Specify changes to any of the following settings:
 - **Service Name**. Type the service name.
 - **Service Type**. If you are unsure, select **TCP/UDP**.
 - **External Starting Port**: If the application uses a single port, enter the same port number in the **External Ending Port** field. If the application uses a range of ports, enter the ending port number of the range in the **External Ending Port** field.
 - For the internal ports, leave the **Use the same port range for Internal port** check box selected.
 - **Internal IP address**. Type the IP address in the Internal IP address field, or select the radio button for an attached device listed in the table.
9. Click the **Apply** button.
Your changes are saved.

Delete a Port Forwarding Entry

➤ **To delete a port forwarding entry:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the router user name and password.
The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
The BASIC Home screen displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
5. Select the **Port Forwarding** radio button as the service type
6. In the table, select the radio button next to the service name.
7. Click the **Delete Service** button.

Application Example: Make 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.
In this example, your router always gives your web server an IP address of 192.168.1.33.
2. In the Port Forwarding/Port Triggering 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 specify that name in the Dynamic DNS screen of the router.
Dynamic DNS makes it much easier to access a server from the Internet because you can type the name in the Internet browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the Router Implements the Port Forwarding Rule

The following sequence shows the effects of a port forwarding rule:

1. When you type the URL **www.example.com** in your browser, the browser sends a web page request message with the following destination information:

- **Destination address.** The IP address of www.example.com, which is the address of your router.
 - **Destination port number.** 80, which is the standard port number for a web server process.
2. Your router receives the message and finds your port forwarding rule for incoming port 80 traffic.
 3. The router changes the destination in the message to IP address 192.168.1.123 and sends the message to that computer.
 4. Your web server at IP address 192.168.1.123 receives the request and sends a reply message to your router.
 5. Your router performs Network Address Translation (NAT) on the source IP address, and sends the reply through the Internet to the computer or wireless device that sent the web page request.

Set Up Port Triggering

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

- An application must use port forwarding to more than one local computer (but not simultaneously).
- An application must open incoming ports that are different from the outgoing port.

With port triggering, the router monitors traffic to the Internet from an outbound “trigger” port that you specify. For outbound traffic from that port, the router saves the IP address of the computer that sent the traffic. The router temporarily opens the incoming port or ports that you specify in your rule, and forwards that incoming traffic to that destination.

Port forwarding creates a static mapping of a port number or range of ports to a single local computer. Port triggering can dynamically open ports to any computer when needed and 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), enable Universal Plug and Play (UPnP). See *Improve Network Connections with Universal Plug and Play* on page 49.

Add a Port Triggering Service

➤ **To add a port triggering service:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
5. Select the **Port Triggering** radio button.
6. Click the **Add Service** button.

7. In the **Service Name** field, type a descriptive service name.
8. In the **Service User** list, select **Any**, or select **Single address** and enter the IP address of one computer:
 - **Any** (the default) allows any computer on the Internet to use this service.
 - **Single address** restricts the service to a particular computer.
9. Select the service type, either **TCP** or **UDP** or **TCP/UDP** (both).
If you are not sure, select **TCP/UDP**.
10. In the **Triggering Port** field, enter the number of the outbound traffic port that will open the inbound ports.
11. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.
12. Click the **Apply** button.

The service is now in the Portmap table. You must enable port triggering before the router used port triggering for the service that you added. See the following section.

Enable Port Triggering

➤ To enable port triggering:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.

A login screen displays.

3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
5. Select the **Port Triggering** radio button.

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

If this check box is selected, the router does not use port triggering even if you have specified port triggering settings.

7. In the Port Triggering Timeout field, enter a value up to 9999 minutes.

This value controls how long the inbound ports stay open when the router detects no activity. This value is required because the router cannot detect when the application terminates.

Application Example: Port Triggering for Internet Relay Chat

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering, you can tell the router to open more incoming ports when a particular outgoing port starts a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the router, “When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer.” The following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and observing the destination port number of 6667, your router creates another session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. When your router receives the incoming message to destination port 33333, it checks its session table to see if a session is active for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your router receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

This chapter provides information to help you diagnose and solve problems you might have with your 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*
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

When you need to restart your network, follow this sequence:

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

Check Ethernet Cable Connections

If your device does not power on, make sure that the Ethernet cables are securely plugged in:

The Internet LED on the router is on if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.

If one or more powered-on computers are connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED lights.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly. The wireless network name (SSID) and wireless security settings of the router and wireless computer must match exactly.

If you set up an access list in the Advanced Wireless Settings screen, you must 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 must use 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.

Troubleshoot with the LEDs

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

1. When power is first applied, verify that the Power LED  is lit.
2. After approximately 30 seconds, verify the following:
 - The Power LED is solid white.
 - The Internet LED is lit.
 - The WiFi LED is lit unless you turned off the wireless radio.

You can use the LEDs on the front panel of the router for troubleshooting.

Power LED Is Off or Blinking

- Make sure that the power adapter is securely connected to your router and securely connected to a working power outlet.
- Check that you are using the power adapter that NETGEAR supplied for this product.
- If the Power LED blinks slowly and continuously, the router firmware 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.

Power LED Stays Amber

When the router is turned on, the Power LED turns amber for about 20 seconds and then turns green. If the LED does not turn green, the router has a problem.

If the Power LED is still amber one minute after you turn on power to the router, do the following:

1. Turn off the power and then turn it back on to see if the router recovers.
2. Press and hold the **Reset** button to return the router to its factory settings.

See *Troubleshoot Your Network Using the Ping Utility* on page 161.

If the error persists, you might have a hardware problem. Contact technical support at www.netgear.com/support.

LEDs Never Turn Off

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

If all LEDs are still lit one minute after power-up, do the following:

- Cycle the power to see if the router recovers.

- Press and hold the **Reset** button to return the router to its factory settings. For more information, see *Troubleshoot Your Network Using the Ping Utility* on page 161.

If the error persists, you might have a hardware problem. 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 can be a standard straight-through Ethernet cable or an Ethernet crossover cable.

WiFi LED Is Off

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

Cannot Log In to the Router

If you are unable to log in to the 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 router.
- Make sure that the IP address of your computer is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address is 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 Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated 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 router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. For more information, see *Factory Settings* on page 164.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click the **Refresh** button 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 user name is **admin**, and the default password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR behind an existing router in your network, use bridge mode or set up the router as an access point.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but not the Internet, check to see if the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests 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 www.netgear.com.
2. Access the router interface at www.routerlogin.net.
3. Select **Administration > 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. For more information, see [Sequence to Restart Your Network](#) on page 155.

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 Internet Setup 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 has an IP address, but your computer does not load any web pages from the Internet, it might be due to the following reasons:

- 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**.

Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

➤ To troubleshoot a PPPoE connection:

1. Select **Administration > Router Status**.
2. Click **Connection Status**.
3. Check the Connection Status display to see if your PPPoE connection is up and working.
4. If you don't have a connection, you can attempt to reconnect by clicking the **Connect** button. The router continues to attempt to connect indefinitely.
5. If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There might also be a provisioning problem with your ISP.

Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Internet Browsing

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

- 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, restart your computer.

Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- Your computer might not have the router configured as its default gateway.
Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default 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 the **Never dial a connection**.

Changes Not Saved

If the router does not save the changes you make in the 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.

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 WiFi LED on the front of the router. If it is off, you can press the **WiFi On/Off** button on the router to turn the router wireless radios back on.
If you disabled the router's SSID broadcast, then your wireless network is hidden and does not display in your wireless client's scanning list. (By default, SSID broadcast is enabled.)
- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view 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 **BASIC > Wireless**.

Note: Be sure to click the **Apply** button if you change settings.

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 (1.8 meters) away, and see whether the signal strength improves.
- Are objects between the router and your computer blocking the wireless signal?

Troubleshoot Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➤ **To ping the router from a Windows computer:**

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:
ping www.routerlogin.net
3. Click the **OK** button.

You should see a message like this one:

Pinging <IP address > with 32 bytes of data

If the path is working, you see this message:

Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

If the path is not working, you see this message:

Request timed out

If the path is not functioning correctly, you might have one of the following problems:

- **Wrong physical connections**
For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.
- **Wrong network configuration**
Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type:

ping -n 10 <IP address>

where <IP address> is the IP address of a remote device such as your ISP DNS server.

If the path is functioning correctly, messages like those shown in the previous section display.

If you do not receive replies, check the following:

- Check that your computer has the IP address of your router listed as the default gateway. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If so, configure your router to “clone” or “spoof” the MAC address from the authorized computer.

A Supplemental Information



This appendix covers the following topics:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the router to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router for at least seven seconds. The router resets, and returns to the factory configuration settings shown in the following table.

Table 3. 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	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	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

Nighthawk AC1900 Smart WiFi Router Model R7000

Table 3. Factory default settings (continued)

Feature		Default behavior
Wireless	Wireless communication	Enabled
	SSID name	See router label
	Security	WPA2-PSK (AES)
	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	Up to 600 Mbps at 2.4 GHz, 1300 Mbps at 5 GHz

*. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can 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 4. R7000 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/3.5A DC output
Dimensions	Dimensions: 280 mm x 182 mm x 49 mm (11 in. x 7.17 in. x 1.9 in.)
Weight	Weight: 430 g (0.94 lbs)
Operating temperature	0° to 40° C (32° to 104° 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 802.11ac 2.0 IEEE 802.11n version 2.0 IEEE 802.11n 256QAM 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 range	2.4 GHz 2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI) 5 GHz 5.18–5.24 + 5.745–5.825 GHz (US) 5.18–5.24 GHz (Europe ETSI)
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2

Notification of Compliance



NETGEAR dual band - wireless

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.

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

Products bearing the **CE** marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

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 34 cm between the radiator and your body.

This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Nighthawk AC1900 Smart WiFi Router Model R7000 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.

Nighthawk AC1900 Smart WiFi Router Model R7000

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 and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionner en association avec une autre antenne ou transmetteur.
- This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nighthawk AC1900 Smart WiFi Router Model R7000) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

CAN ICES-3 (B)/NMB-3(B)

Industry Canada

This device complies with RSS 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 40cm between the radiator & your body.

Caution:

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

Ce dispositif est conforme à la norme CNR-247 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.

Nighthawk AC1900 Smart WiFi Router Model R7000

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

Le dispositif pourrait automatiquement cesser d'émettre en cas d'absence d'informations à transmettre, ou une défaillance opérationnelle. Notez que ce n'est pas l'intention d'interdire la transmission des informations de contrôle ou de signalisation ou l'utilisation de codes répétitifs lorsque requis par la technologie.

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 40 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 utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Interference Reduction Table

The following table shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby monitor - analog	20 feet / 6 meters
Baby monitor - digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

For operation within 5.15 ~ 5.25GHz / 5.47 ~5.725GHz frequency range, it is restricted to indoor environment. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 34cm between the radiator & your body.

Industry Canada statement:

This device complies with ISSED's licence-exempt RSS. 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. Le présent appareil est conforme aux CNR d' ISSED applicables aux appareils radio exempts de licence. L'exploitation est autorisée 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.

Caution :

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;
- (iii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- (iv) the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2(3) shall be clearly indicated.
- (v) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5250 à 5350 MHz et de 5470 à 5725 MHz doit être conforme à la limite de la p.i.r.e.;
- (iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- (iv) les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, et énoncée à la section 6.2.2 3), doivent être clairement indiqués.
- (v) De plus, les utilisateurs devraient aussi être avisés que 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.

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 40cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 40cm de distance entre la source de rayonnement et votre corps.