

Chapter 6

Fine-Tuning Your Network

This chapter describes how to modify the configuration of the RangeMax NEXT Wireless Router WNR834B to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes:

- [Allowing Inbound Connections To Your Network](#)
- [Configuring Port Forwarding to Local Servers](#)
- [Configuring Port Triggering](#)
- [Using Universal Plug and Play](#)
- [Optimizing Wireless Performance](#)
- [Changing the MTU](#)
- [Optimizing Your Network Bandwidth](#)
- [Overview of Home and Small Office Networking Technologies](#)

Allowing Inbound Connections To Your Network

By default, the WNR834B router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you may need to create exceptions to this rule for the following purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work properly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: Port Forwarding and Port Triggering. This section explains how a normal outbound connection works, followed by two examples explaining how Port Forwarding and Port Triggering operate and how they differ.

How Your Computer Communicates With A Remote Computer Through Your Router

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

- a. You open Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.
- b. You ask your browser to get a Web page from the Web server at *www.example.com*. Your computer composes a Web page request message with the following address and port information:
 - The source address is your computer's IP address.
 - The source port number is 5678, the browser session.
 - The destination address is the IP address of *www.example.com*, which your computer finds by asking a DNS server.
 - The destination port number is 80, the standard port number for a Web server process.

Your computer then sends this request message to your router.

- c. Your router creates an entry in its internal session table describing this communication session between your computer and the Web server at *www.example.com*. Before sending the Web page request message to *www.example.com*, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
 - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
 - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the Web server at *www.example.com*.

- d. The Web server at *www.example.com* composes a return message with the requested Web page data. The return message contains the following address and port information:
 - The source address is the IP address of *www.example.com*.
 - The source port number is 80, the standard port number for a Web server process.
 - The destination address is the public IP address of your router.
 - The destination port number is 33333.

The Web server then sends this reply message to your router.

- e. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:
 - The source address is the IP address of *www.example.com*.
 - The source port number is 80, the standard port number for a Web server process.
 - The destination address is your computer's IP address.
 - The destination port number is 5678, the browser session that made the initial request.

Your router then sends this reply message to your computer, which displays the Web page from *www.example.com*.

- f. When you finish your browser session, your router eventually senses a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

How Port Triggering Changes the Communication Process

In the preceding example, requests are sent to a remote computer by your router from a particular service port number and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the Port Triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates 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.” Using steps similar to the preceding example, the following sequence shows the effects of the Port Triggering rule you have defined:

- a. You open an IRC client program, beginning a chat session on your computer.
- b. 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.
- c. 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.
- d. **Noting your Port Triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.**
- e. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.
- f. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session 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.
- g. **Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is 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.**
- h. 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.

To configure Port Triggering, you need to know which inbound ports the application needs. Also, you need to know the outbound port number that will trigger the opening of the inbound ports. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups..



Note: Only one computer at a time can use the triggered application.

How Port Forwarding Changes the Communication Process

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you may need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router will ignore any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the Port Forwarding feature.

A typical application of Port Forwarding can be shown by reversing the client/server relationship from our previous Web server example. In this case, a remote computer's browser needs to access a Web server running on a computer in your local network. Using Port Forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a Web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the Port Forwarding rule you have defined:

- a. The user of a remote computer opens Internet Explorer and requests a Web page from *www.example.com*, which resolves to the public IP address of your router. The remote computer composes a Web page request message with the following destination information:
 - The destination address is the IP address of *www.example.com*, which is the address of your router.
 - The destination port number is 80, the standard port number for a Web server process.The remote computer then sends this request message through the Internet to your router.
- b. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. **Your Port Forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:**
 - **The destination address is replaced with 192.168.1.123.****Your router then sends this request message to your local network.**
- c. Your Web server at 192.168.1.123 receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.
- d. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from *www.example.com*.

To configure Port Forwarding, you need to know which inbound ports the application needs. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups.

How Port Forwarding Differs From Port Triggering

- Port Triggering can be used by any computer on your network, although only one computer may use it at a time.
- Port Forwarding is configured for a single computer on your network.
- Port Triggering does not need to know the computer's IP address in advance. The IP address will be captured automatically.
- Port Forwarding requires that you specify the computer's IP address during configuration, and the IP address must never change.
- Port Triggering requires specific outbound traffic to open the inbound ports, and the triggered ports will be closed after a period of no activity.
- Port Forwarding is always active and does not need to be triggered.

Configuring Port Forwarding to Local Servers

Using the Port Forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you may make a local Web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding menu to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in [“Setting Up a Default DMZ Server” on page 5-7](#).

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



Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your WNR834B router. See [“Using Address Reservation” on page 5-4](#) for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. From the main menu of the browser interface, under Advanced, click on Port Forwarding /Port Triggering to view the port forwarding menu.

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding
 Port Triggering

Service Name: AIM
Server IP Address: 192 . 168 . 1 . [] Add

#	Service Name	Start Port	End Port	Server IP Address
---	--------------	------------	----------	-------------------

Edit Service Delete Service

Add Custom Service

Figure 6-1

2. From the Service Name box, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, [“Adding a Custom Service”](#).
3. In the corresponding Server IP Address box, enter the last digit of the IP address of your local computer that will provide this service.
4. Click Add. The service will appear in the list on the menu.

Adding a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you must first determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups. When you have the port number information, follow these steps:

1. From the main menu of the browser interface, under Advanced, click Port Forwarding /Port Triggering.

2. Click Add Custom Service.

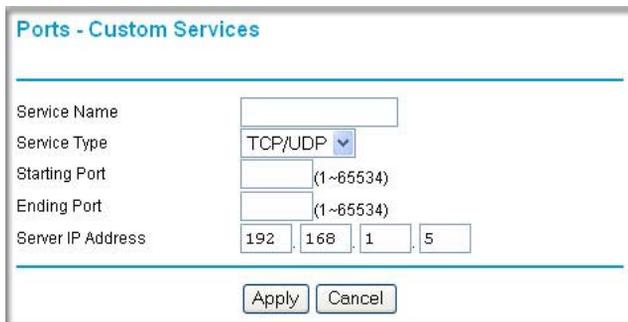


Figure 6-2

3. In the Service Name box, type a descriptive name.
4. In the Service Type box, select the protocol. If you are unsure, select TCP/UDP.
5. In the Starting Port box, type the beginning port number.
 - If the application uses only a single port, type the same port number in the Ending Port box.
 - If the application uses a range of ports, type the ending port number of the range in the Ending Port box.
6. In the Server IP Address box, type the IP address of your local computer that will provide this service.
7. Click Apply. The service will appear in the list in the Port Forwarding /Port Triggering menu.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry:

1. In the table, select the button next to the service name.
2. Click Edit Service or Delete Service.

Application Example: Making a Local Web Server Public

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

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP Address Reservation, as explained in [“Using Address Reservation” on page 5-4](#). In this example, your router will always give your Web server an IP address of 192.168.1.33.
2. Configure the Port Forwarding menu to forward the HTTP service to the local address of your Web server at 192.168.1.33.
HTTP (port 80) is the standard protocol for Web servers.
3. (Optional) Register a host name with a Dynamic DNS Service and configure your router to use the name as described in [“Using a Dynamic DNS Service” on page 5-5](#).
To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS Service, the remote user can reach your server by a user-friendly Internet name, such as *mynetgear.dyndns.org*.

Configuring Port Triggering

Port Triggering is a dynamic extension of Port Forwarding that is useful when:

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

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

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



Note: If you use applications such as multi-player gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in [“Using Universal Plug and Play” on page 6-12](#).

To configure Port Triggering, you need to know which inbound ports the application needs. Also, you need to know the outbound port number that will trigger the opening of the inbound ports. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups.

To set up Port Triggering:

1. In the main menu, under Advanced, Select Port Forwarding/Port Triggering.
2. Select the Port Triggering radio button. The Port Triggering screen appears.

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding

Port Triggering

Disable Port Triggering

Port Triggering Timeout (in minutes)

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User
<input type="radio"/>	1	<input checked="" type="checkbox"/>	dialpad_1	TCP:51200	TCP/UDP:51200	ANY
<input type="radio"/>	2	<input checked="" type="checkbox"/>	dialpad_2	TCP:51201	TCP/UDP:51201	ANY
<input type="radio"/>	3	<input checked="" type="checkbox"/>	paltalk_1	TCP:2090	TCP/UDP:2090	ANY
<input type="radio"/>	4	<input checked="" type="checkbox"/>	paltalk_2	TCP:2091	TCP/UDP:2091	ANY
<input type="radio"/>	5	<input checked="" type="checkbox"/>	quicktime	TCP:554	TCP/UDP:6970..6990	ANY
<input type="radio"/>	6	<input checked="" type="checkbox"/>	starcraft	TCP:6112	TCP/UDP:6112	ANY

Figure 6-3

3. Deselect the checkbox for Disable Port Triggering.



Note: If the Disable Port Triggering checkbox is selected after configuring port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it will not be used.

4. For Port Triggering Timeout, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound port(s). The inbound port(s) close when the inactivity timer expires. This is required because the router cannot be sure when the application has terminated.

5. Click Add Service.

Port Triggering - Services

Service

Service Name

Service User

. . .

Service Type

Triggering Port (1~65535)

Required Inbound Connection

Connection Type

Starting Port (1~65535)

Ending Port (1~65535)

Figure 6-4

6. In the Service Name box, type a descriptive service name.
7. Under Service User, select Any (default) to allow this service to be used by any computer on the Internet. Otherwise, select Single address and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the Service Type, either TCP or UDP or both (TCP/UDP). If you are not sure, select TCP/UDP.
9. In the Triggering Port box, enter the outbound traffic port number that will cause the inbound ports to be opened.
10. Enter the inbound connection port information such as Connection Type, Starting Port, and Ending Port boxes.
11. Click Apply. The service appears in the Port Triggering Portmap Table.

Using Universal Plug and Play

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



Note: If you use applications such as multi-player gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should enable UPnP.

From the main menu of the browser interface, under Advanced, click UPnP. The UPnP menu appears.

UPnP

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Figure 6-5

The available settings and displays in this menu are:

- Turn UPnP On
UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

- **Advertisement Period**
The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
- **Advertisement Time To Live**
The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value.
- **UPnP Portmap Table**
The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, please see [“Wireless Communications” in Appendix B](#).

The following list describes how to optimize wireless router performance.

- **Identify critical wireless links.**
If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without losing connectivity. This also means that devices that are further away may be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.

- Choose placement carefully.
For best results, place your router:
 - Near the center of the area in which your computers will operate.
 - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Avoid obstacles to wireless signals.
 - Keep wireless devices at least two feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
 - Keep away from large amounts of water such as fish tanks and water coolers.
- Reduce interference.
Avoid windows unless communicating between buildings.
Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
 - Computers and fax machines (no closer than one foot)
 - Copying machines, elevators, and cell phones (no closer than 6 feet)
 - Microwave ovens (no closer than 10 feet)
- Choose your settings.
 - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.
 - Turn off SSID Broadcast, and change the default SSID. Other nearby devices may automatically try to connect to your network several times a second, which can cause significant performance reduction.

Changing the MTU

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets must be split or “fragmented” to accommodate the one with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value may fix one problem but cause another. Leave MTU unchanged unless:

- You have problems connecting to your ISP, or other Internet service, and either the technical support of the ISP or of NETGEAR recommends changing MTU. These may require an MTU change:
 - A secure Web site that won't open, or only displays part of a Web page
 - Yahoo email
 - MSN
 - America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems..



Note: An incorrect MTU setting can cause Internet communication problems such as the inability to access certain Web sites, frames within Web sites, secure login pages, FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. [Table 6-1](#) describes common MTU sizes and applications.

Table 6-1. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for ping. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you don't have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

To change the MTU size:

1. In the Advanced section of the main menu, click WAN Setup.
2. Under MTU Size, enter a new size between 64 and 1500.

3. Click Apply to save the new configuration.

Optimizing Your Network Bandwidth

As your network grows, it may consist of several segments of different networking technologies, each providing different throughput. In planning your network, you should first consider which devices will have the heaviest traffic flow between them. Examples are:

- A media center in one room streaming high-definition video from a server in another room
- A storage device that is used for backing up your computers

Next, consider the throughput of your network devices. Where possible, make the heaviest-traffic connections using higher-speed technologies, with no lower-speed bottlenecks in the path.

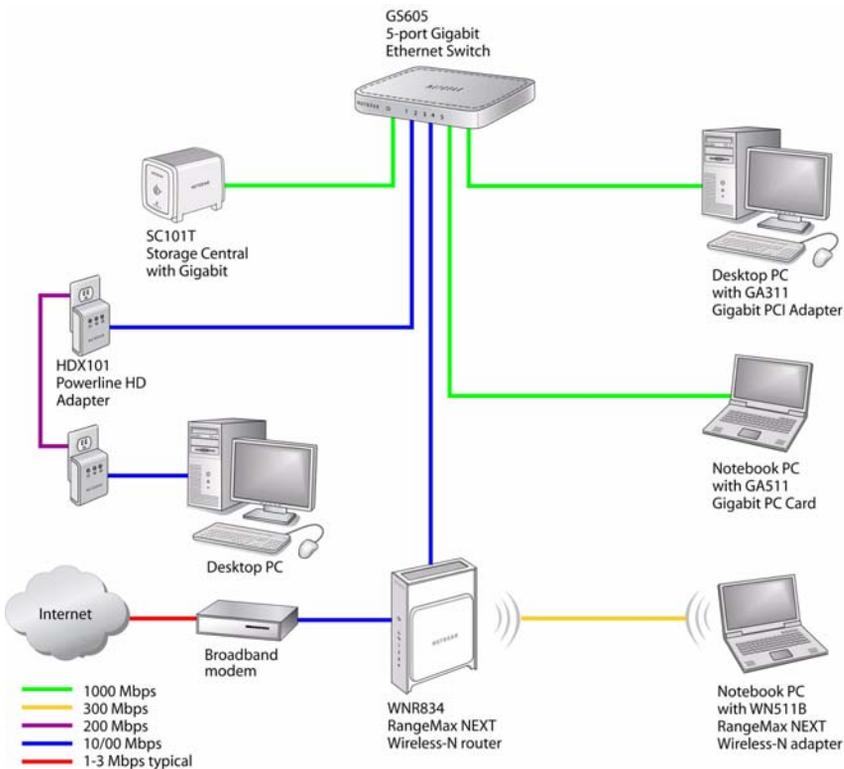


Figure 6-6

Figure 6-6 shows an example network using multiple networking technologies. In this network, the two PCs with gigabit (1000 Mbps) Ethernet adapters have a gigabit connection through the GS605 switch to the storage server. This connection should allow for extremely fast backups or quick access to large files on the server. The PC connected through a pair of Powerline HD adapters is limited to the 200 Mbps speed of the Powerline HD connection. Although any of the links in this example would be sufficient for high-traffic applications such as streaming HD video, the use of older devices such as 10 Mbps Ethernet or 802.11b wireless would create a significant bottleneck.

Overview of Home and Small Office Networking Technologies

Common connection types and their speed and security considerations are:

- **Broadband Internet**

Your Internet connection speed is determined by your modem type, such as ADSL or cable modem, as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL and cable modem connections are asymmetrical, meaning they have a lower data rate *to* the Internet (upstream) than *from* the Internet (downstream). Keep in mind that when you connect to someone else who also has an asymmetrical connection, the data rate between your sites is limited by each side's upstream data rate. A typical residential ADSL or cablemodem connection provides a downstream throughput of about one to three megabits per second (Mbps). Newer technologies such as ADSL2+ and Fiber to the Home (FTTH) will increase the connection speed to tens of Mbps.

- **Wireless**

Your RangeMax NEXT Wireless Router WNR834B provides a wireless data throughput of up to 300 Mbps using technology called Multiple-Input Multiple-Output (MIMO), in which multiple antennas transmit multiple streams of data. The use of multiple antennas also provides excellent range and coverage. With the introduction of the newer WPA and WPA2 encryption and authentication protocols, wireless security is extremely strong.

To get the best performance, use RangeMax NEXT adapters such as the WN511B for your computers. Although the RangeMax NEXT router is compatible with older 802.11b and 802.11g adapters, the use of these older wireless technologies in your network can result in lower throughput overall (typically less than 10 Mbps for 802.11b and less than 40 Mbps for 802.11g). In addition, many older wireless products do not support the latest security protocols, WPA and WPA2.

- **Powerline**

For connecting rooms or floors that are blocked by obstructions or are distant vertically, consider networking over your building's AC wiring. NETGEAR's Powerline HD family of products delivers up to 200 Mbps to any outlet, while the older generation XE family of products delivers 14 Mbps or 85 Mbps. Data transmissions are encrypted for security, and you can configure an individual network password to prevent neighbors from connecting.

The Powerline HD family of products can coexist on the same network with older generation XE family products or HomePlug 1.0 products, but they are not interoperable with these older products.

- **Wired Ethernet**

As gigabit-speed Ethernet ports (10/100/1000 Mbps) become common on newer computers, wired Ethernet remains a good choice for speed, economy, and security. Gigabit Ethernet can extend up to 100 meters with twisted-pair wiring of CAT-5e or better. A wired connection is not susceptible to interference, and eavesdropping would require a physical connection to your network.



Note: Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

Assessing Your Speed Requirements

Because your Internet connection is likely to operate at a much lower speed than your local network, faster local networking technologies may not improve your Internet experience. However, many emerging home applications require high data rates. For example:

- Streaming HD video requires 10 to 30 Mbps per stream. Because latency and packet loss can disrupt your video, plan to provide at least twice the capacity you need.
- Streaming MP3 audio requires less than 1 Mbps per stream and does not strain most modern networks. Like video, however, streaming audio is also sensitive to latency and packet loss, so a congested network or a noisy link can cause problems.

- Backing up computers over the network has become popular due to the availability of inexpensive mass storage. [Table 6-2](#) shows the time to transfer one gigabyte (1 GB) of data using various networking technologies.

Table 6-2. Theoretical Transfer Time for 1 Gigabyte

Network Connection	Theoretical Raw Transfer Time
Gigabit Wired Ethernet	8 seconds
RangeMax NEXT Wireless-N	26 seconds
Powerline HD	40 seconds
100 Mbps Wired Ethernet	80 seconds
802.11g wireless	150 seconds
802.11b wireless	700 seconds
10 Mbps Wired Ethernet	800 seconds
Cable Modem (3 Mbps)	2700 seconds
Analog Modem (56 kbps)	144,000 seconds (40 hours)

