NETGEAR®

N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700v2

User Manual

June 2014
202-10918-05

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

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

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

Compliance

For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.

See the regulatory compliance document before connecting the power supply.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice.

Contents

Chapter 1 Hardware Setup

Chapter 2 Get Started with NETGEAR Genie

Chapter 3 Genie Basic Settings

Chapter 7 Security

Chapter 8 Administration

Chapter 9 Advanced Settings

Chapter 10 Troubleshooting

Appendix A Supplemental Information

Index

Hardware Setup

Get to know your wireless router

1

The NETGEAR N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700v2 is the ultimate integrated ADSL networking gateway. It offers concurrent dual-band technology that allows devices to avoid interference and also ensures top speeds and the greatest range for demanding applications, such as streaming HD video and multiplayer gaming. Complete with a built-in ADSL modem, it is compatible with all major ADSL Internet service providers. The Gigabit port on the WAN side also has an option to connect to a fiber or cable modem.

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 3, Genie Basic Settings*, explains how to set up your Internet connection.

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

This chapter contains the following sections:

- *Product Specifications*
- *Unpack Your New Router*
- *Hardware Features*
- *Position Your Wireless Router*
- *ADSL Microfilters*
- *Cable Your N600 Wireless Modem Router*
- *Verify the Cabling*

Product Specifications

- **All-in-one**. Built-in ADSL2+ modem and WAN Gigabit-Ethernet port for cable or fiber combined with a wireless router create the ultimate integrated home gateway.
- **Concurrent dual band**. Ensures top speeds and the greatest range while minimizing interference.
- **Faster multimedia streaming**. Provides Wireless-N speed for streaming HD videos, simultaneous downloads, and online gaming in addition to basic Internet applications.
- **Shared storage**. Two (2) ports for ReadySHARE® USB storage access provide fast and easy shared access to an external USB storage device.
- **Live Parental Controls**. Keep your Internet experience safe.
- **Guest network access**. Provides separate security and access restrictions for guests using the network.
- **Secured connection**. Push 'N' Connect ensures a quick and secure network connection.
- **Broadband usage meter**. Monitors Internet traffic and sends customized reports to help keep costs under control.
- **Easy installation**. Connect to computer and open your browser to install.
- **Compatibility**. Compatible with all major ADSL Internet service providers (ISPs).
- **Broadband usage meter**. Monitors Internet traffic and sends customized reports to help keep costs under control.

Package Contents

- N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700v2
- Ethernet cable
- Phone cable and filter
- Power adapter, localized to country of sale

Warranty

- NETGEAR 1-year warranty

System Requirements

- Broadband Internet service
  - ADSL broadband Internet service
  - Cable or fiber: Connects to cable modem or fiber termination node through the Gigabit-Ethernet WAN port
- 802.11 a/b/g/n 2.4 or 5.0 GHz specification wireless adapter or an Ethernet adapter and cable for each computer
- Microsoft Windows 7, Vista, XP, 2000, Me, Mac OS, UNIX, or Linux

- Microsoft Internet Explorer 5.0, Firefox 2.0, Safari 1.4, or later
- Use with an N600 Wireless Dual Band USB Adapter (WNDA3100 for maximum performance)

Standards

- IEEE 802.11 b/g/n 2.4 GHz
- IEEE 802.11 a/n 5.0 GHz
- Five (5) 10/100/1000 (1 WAN and 4 LAN) Gigabit Ethernet ports
- Two (2) USB 2.0 ports
- One (1) ADSL2+ port

Performance

- All-in-one. High-speed ADSL2+ modem (built-in) and WAN Gigabit-Ethernet port for cable or fiber
- Powerful dual-core (400 MHz each) processor
- High-speed access to external USB storage using two USB 2.0 ports
- Memory: 32 MB flash and 64 MB RAM
- Five (5) (1 WAN, 4 LAN) Gigabit-Ethernet ports
- Advanced Quality of Service (QoS)

Security

- Wi-Fi Protected Access® (WPA/WPA2-PSK) and WEP
- Double firewall protection (SPI and NAT firewall)
- Denial-of-service (DoS) attack prevention

Ease of Use

- Easy installation. Connect to computer and open your browser to install
- Push 'N' Connect using Wi-Fi Protected Setup® (WPS)

Physical Specifications

- Dimensions: 223 x 153 x 31 mm (8.8 x 6.0 x 1.2 inches)
- Weight: 0.5 kg (1.2 lb)

Advanced Features

- Live Parental Controls with flexible and customizable filter settings.
- Simultaneous dual band. 2.4 GHz and 5 GHz operation.

- Two (2) ports for ReadySHARE® USB storage access. Supports FAT16/32, NTFS Read/Write.
- DLNA®. Stream media to DLNA media players.
- Multiple SSID guest networks (separate security and access restrictions).
- Broadband usage meter measures Internet usage.
- Power and Wi-Fi On/Off buttons.

NETGEAR Green Features

Power On/Off button

80% recycled packaging

CEC (California Efficiency)

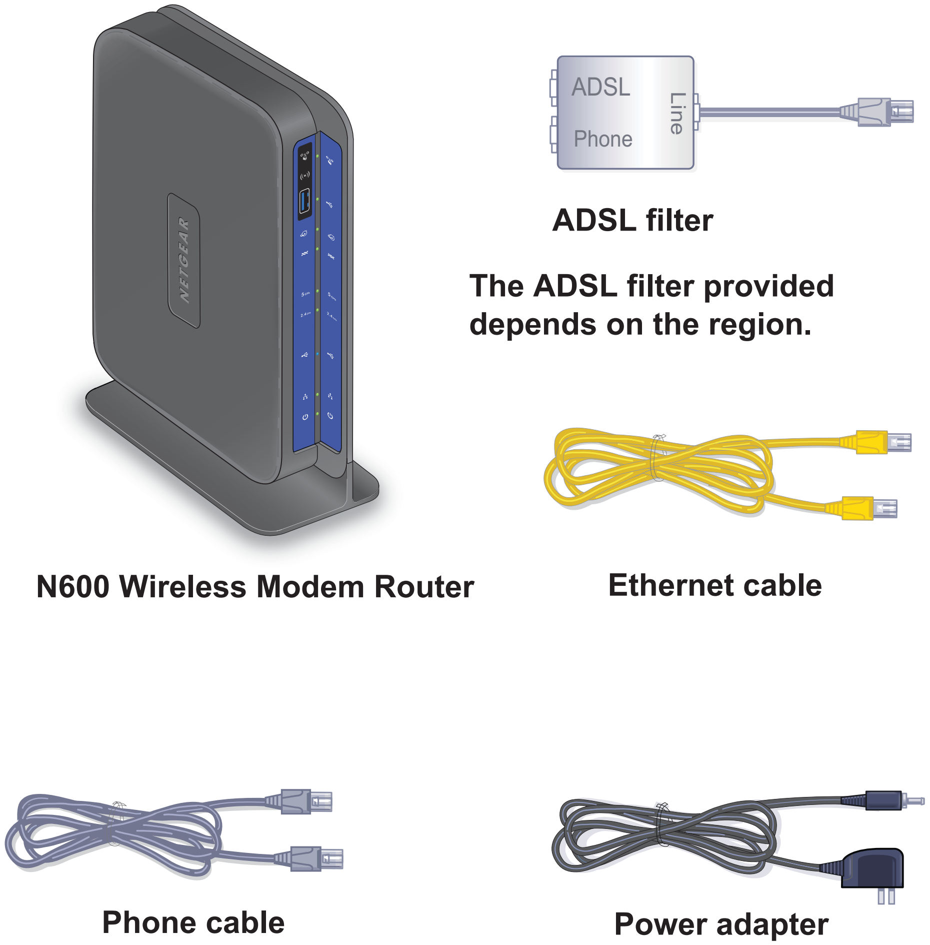
RoHS

WEEE

Unpack Your New Router

Your box should contain the following items:

- N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700v2
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters and splitters (quantity and type vary by region)
- Installation guide with cabling and router setup instructions.



ADSL filter

The ADSL filter provided depends on the region.

N600 Wireless Modem Router

Ethernet cable

Phone cable

Power adapter

Figure 1. Box contents

Hardware Features

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

Label

The label on the bottom of the wireless modem router shows the router's Restore Factory Settings button, WiFi network name (SSID), network key (password), and MAC address.

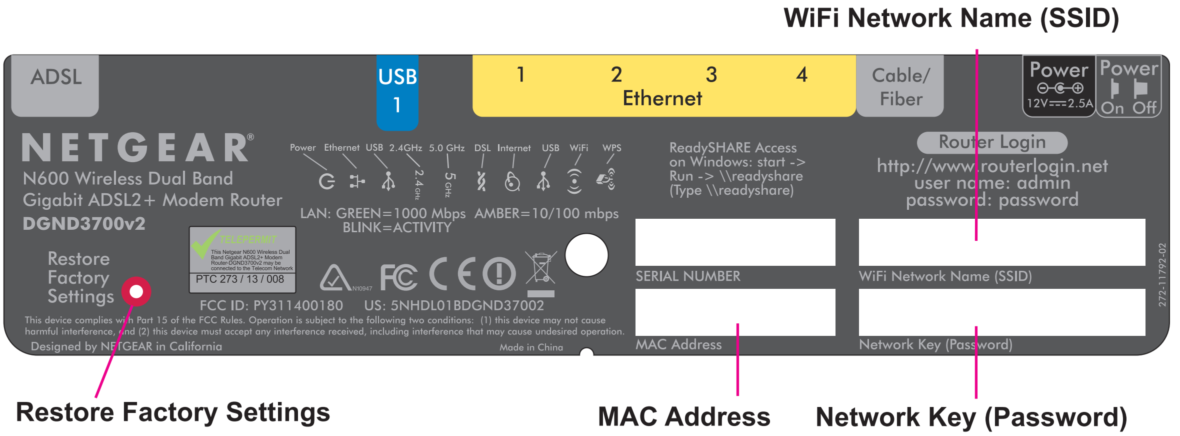

WiFi Network Name (SSID)
ADSL
USB 1
1 2 3 4 Ethernet
Cable/ Fiber
Power 12V⎓2.5A
Power On Off
NETGEAR
N600 Wireless Dual Band Gigabit ADSL2+ Modem Router
DGND3700v2
Power Ethernet USB 2.4GHz 5.0 GHz DSL Internet USB WiFi WPS
LAN: GREEN=1000 Mbps AMBER=10/100 mbps BLINK=ACTIVITY
ReadySHARE Access on Windows: start -> Run -> \\readyshare (Type \\readyshare)
Router Login
http://www.routerlogin.net
user name: admin
password: password
Restore Factory Settings
PTC 273 / 13 / 008
FCC ID: PY311400180
US: 5NHDL01BDGND37002
SERIAL NUMBER
WiFi Network Name (SSID)
MAC Address
Network Key (Password)
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.
Designed by NETGEAR in California
Made in China
272-11792-02
Restore Factory Settings
MAC Address
Network Key (Password)

Figure 2. Label on router bottom

See *Factory Settings* on page 142 for information about the Restore Factory Settings button and the factory setting values.

Back Panel

The back panel has the Power On/Off button and port connections shown in the figure:

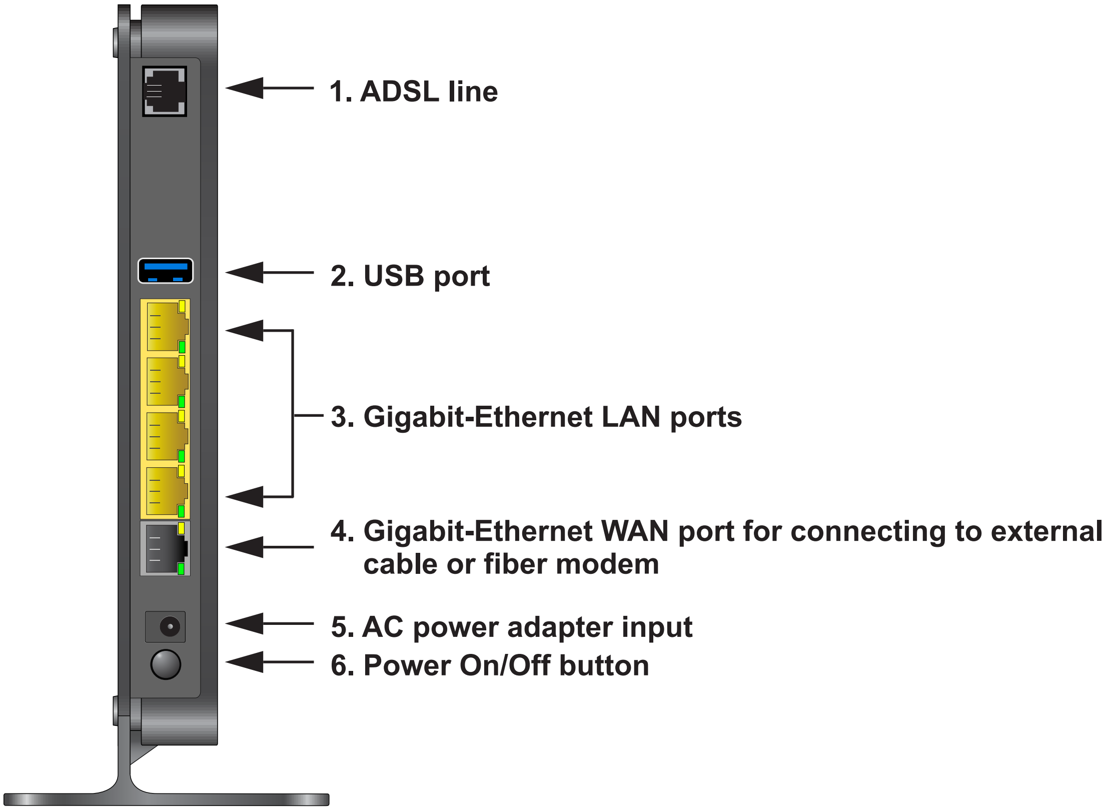

1. ADSL line
2. USB port
3. Gigabit-Ethernet LAN ports
4. Gigabit-Ethernet WAN port for connecting to external cable or fiber modem
5. AC power adapter input
6. Power On/Off button

Figure 3. Back panel port connections

Viewed from top to bottom, the back panel contains the following elements:

1. RJ-11 asynchronous DSL (ADSL) port for connecting the wireless modem router to an ADSL line

> **Note:** An ADSL port is capable of sending data over an ADSL line at one speed and receiving it at another speed.

2. USB port for connecting USB storage devices like flash drives or hard drives
3. Four Gigabit-Ethernet RJ-45 LAN ports for cabling the wireless modem router to the local computers
4. One Gigabit-Ethernet WAN port for connecting the wireless modem router to a fiber or cable modem

Note: You can use either the ADSL or Gigabit-Ethernet port for WAN connectivity.

5. AC power adapter input
6. Power On/Off button

Front Panel

The wireless modem router front panel has the 10 status LEDs, icons, and ports shown in the figure. Note that the Wireless and WPS icons are buttons.

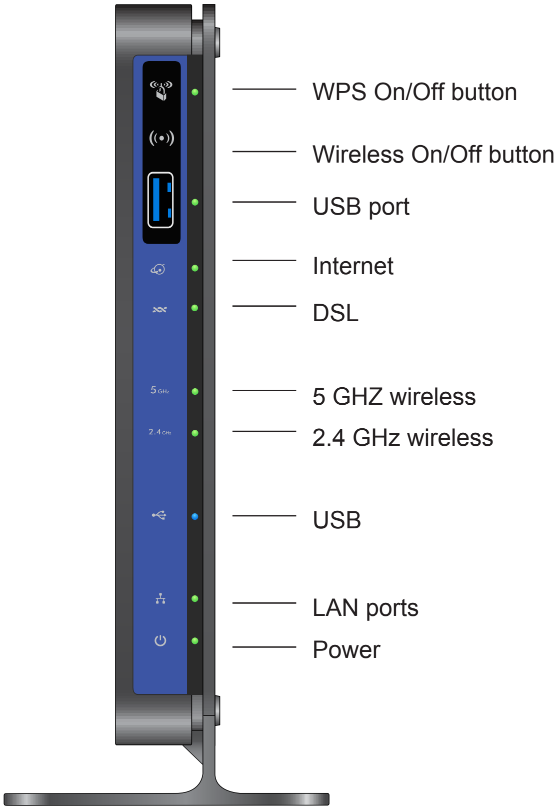


Figure 4. Front panel LEDs

The following tables describe the LEDs, icons, and buttons on the front panel from top to bottom.

Table 1. WPS button and LED

Icon	LED Activity	Description
	Solid green	Indicates that wireless security has been enabled.
	Blinking green	WPS-capable device is connecting to the device.
	Off	WPS is not enabled. For information about the use of this button, see *Wi-Fi Protected Setup (WPS) Method* on page 27.

Table 2. Wireless button

Icon	Description
((•))	For information about the use of this button, see *Wireless Connectivity* on page 137.

Table 3. USB port

Icon	Description
	USB port for connecting USB storage devices like flash drives or hard drives.

Table 4. Internet LED

Icon	LED Activity	Description
	Solid green	You have an Internet connection. If this connection is dropped due to an idle time-out but the connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off.
	Solid red	The Internet (IP) connection failed. See *Cannot Access the Internet* on page 134 for troubleshooting information.
	Blinking green	Data is being transmitted over the Internet connection.
	Off	No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).

Table 5. DSL LED

Icon	LED Activity	Description
●	Solid green	You have an ADSL connection. In technical terms, the ADSL port is synchronized with an ISP's network-access device.
	Blinking green	Indicates that the wireless modem router is negotiating the best possible speed on the ADSL line.
	Off	The unit is off or there is no IP connection.

Table 6. 5 GHz Wireless LED

Icon	LED Activity	Description
5 GHz ●	Solid blue	There is wireless connectivity.
	Blinking blue	Data is being transmitted or received over the 5 GHz wireless link.
	Off	There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.

Table 7. 2.4 GHz Wireless LED

Icon	LED Activity	Description
2.4 GHz ●	Solid green	There is wireless connectivity.
	Blinking green	Data is being transmitted or received over the 2.4 GHz wireless link.
	Off	There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.

Table 8. USB LED

Icon	LED Activity	Description
●	Solid green	A USB port has detected a USB device.
	Blinking green	Data is being transmitted or received.
	Off	No link is detected on these ports.

Table 9. LAN LED

Icon	LED Activity	Description
🖧 ●	Solid green	A LAN port has detected an Ethernet link with a device.
	Blinking green	Data is being transmitted or received.
	Off	No link is detected on these ports.

Table 10. Power On/Off LED

Icon	LED Activity	Description
⏻ ●	Solid green	Power is supplied to the router.
	Solid red	POST (power-on self-test) failure or a device malfunction has occurred.
	Off	Power is not supplied to the router.
	Restore Factory Settings	Light blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for six seconds. The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the gateway resets to the factory defaults.

Position Your Wireless Router

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

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the wireless modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Note: The DGND3700 should be put in a vertical position only.

Also be aware that when you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).

ADSL Microfilters

If this is the first time you have cabled a wireless router between an ADSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your N600 Wireless Modem Router* on page 20.

An ADSL microfilter is a small in-line device that filters ADSL interference out of standard phone equipment that shares the same line with your ADSL service. Every telephone device that connects to a telephone line that provides ADSL service needs an ADSL microfilter to filter out the ADSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries ADSL service. That depends on the ADSL service setup in your home.

Note: Often the ADSL microfilter is included in the box with the wireless modem router. If you purchased the wireless modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter (Not Included)

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The wireless modem router plugs directly into a separate ADSL line. Plugging the wireless modem router into the phone jack blocks the Internet connection. If you do not have a separate ADSL line for the router, the best thing to do is to use an ADSL microfilter with a built-in splitter.

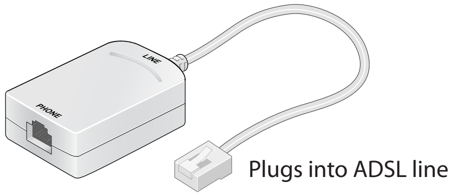


Figure 5. One-line ADSL microfilter

Second best when you do not have a separate ADSL line for the router is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter (Included)

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the wireless modem router and your telephone equipment. Plug the ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the wireless modem router into the jack labeled ADSL.

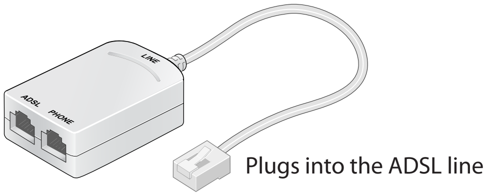


Figure 6. Two-line ADSL microfilter with built-in splitter

Summary

- One-line ADSL microfilter (not included). Use with a phone or fax machine.
- Splitter (not included). Use with a one-line ADSL microfilter to share an outlet with a phone and the wireless modem router.
- Two-line ADSL microfilter with built-in splitter (included). Use to share an outlet with a phone and the wireless modem router.

Cable Your N600 Wireless Modem Router

WARNING:

DO *not* stack equipment, or place equipment in tight spaces, or in drawers. Be sure your equipment is surrounded by at least 2 inches of air space. The unit should not be wall mounted.

The installation guide that came in the box has a cabling diagram on the first page.

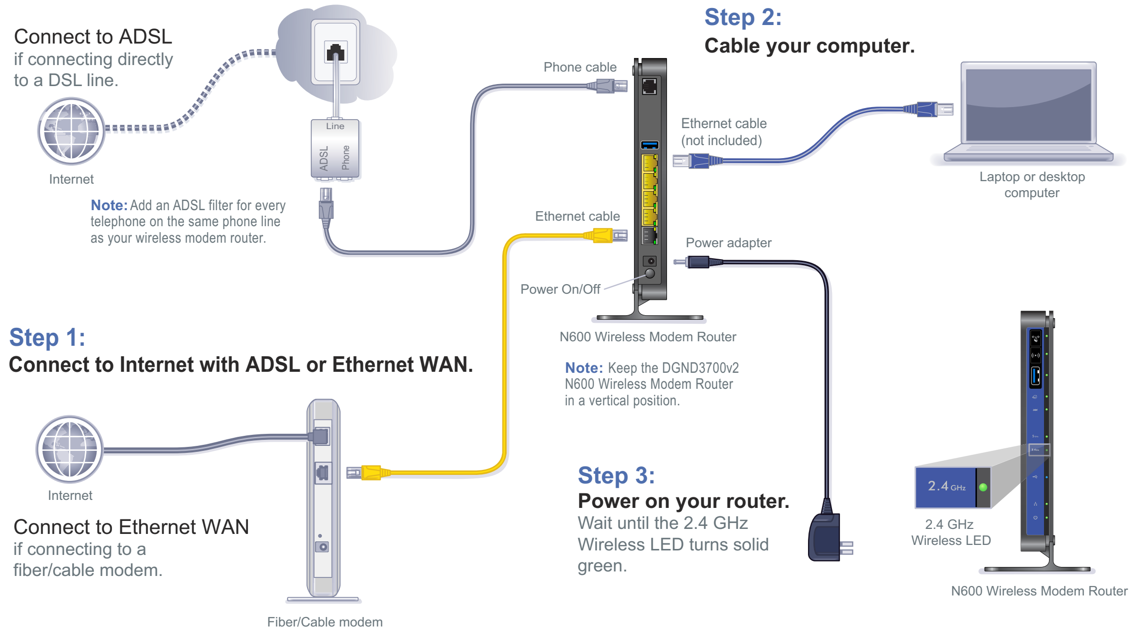

Connect to ADSL
if connecting directly
to a DSL line.
Internet
Line
ADSL
Phone
Note: Add an ADSL filter for every telephone on the same phone line as your wireless modem router.
Phone cable
Step 2:
Cable your computer.
Ethernet cable
(not included)
Laptop or desktop computer
Ethernet cable
Power adapter
Power On/Off
N600 Wireless Modem Router
Note: Keep the DGND3700v2 N600 Wireless Modem Router in a vertical position.
Step 1:
Connect to Internet with ADSL or Ethernet WAN.
Internet
Connect to Ethernet WAN
if connecting to a
fiber/cable modem.
Fiber/Cable modem
Step 3:
Power on your router.
Wait until the 2.4 GHz Wireless LED turns solid green.
2.4 GHz
2.4 GHz
Wireless LED
N600 Wireless Modem Router

Figure 7. Cabling diagram

CAUTION:

Incorrectly connecting a filter to your wireless modem router blocks your ADSL connection.

Verify the Cabling

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

- ⏻ The Power LED is green when the modem router is turned on.
- 🖧 The LAN port LED is green when a computer is cabled to the router by an Ethernet cable.
- 2.4 GHz 5 GHz The Wireless LEDs are lit when the modem router is turned on.

- The DSL LED is green when you have an ADSL connection.
- The Internet LED is green when there is an Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

Get Started with NETGEAR Genie

2

Connect to the wireless modem router

This chapter explains how to use NETGEAR Genie to set up your wireless modem router after you complete cabling as described in the installation guide and in the previous chapter in this book.

This chapter contains the following sections:

Prepare to Set Up the Wireless Modem Router

You can set up your wireless modem router with the NETGEAR Genie automatically, or you can use the Genie menus and screens to set up your wireless modem router manually. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, computers, and other devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

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

Gather ISP Information

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

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP; this is rare)

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the wireless modem router. See *Basic Wireless Settings* on page 35 for information about the wireless modem router’s preconfigured security settings.

Types of Logins and Access

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

- **Wireless modem router login** logs you in to the wireless modem router interface from NETGEAR Genie. See *Use NETGEAR Genie after Installation* on page 25 for details about this login.

  Wireless network key or password. Your wireless modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label located on the bottom of your wireless modem router.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

NETGEAR Genie Setup

NETGEAR Genie runs on any device with a web browser. It is the easiest way to set up the wireless modem router because it automates many of the steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

➢ **To use NETGEAR Genie to set up your wireless modem router:**

1. Turn the wireless modem router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable to your wireless modem router.
3. Launch your Internet browser.
   - If this is the first time you are setting up the Internet connection for your wireless modem router, the browser automatically goes to http://www.routerlogin.net, and the NETGEAR Genie screen displays.
   - If you already used the NETGEAR Genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR Genie screen. See *Use NETGEAR Genie after Installation* on page 25.
4. Follow the onscreen instructions to complete NETGEAR Genie setup. NETGEAR Genie guides you through connecting the wireless modem router to the Internet.

➢ **If the browser cannot display the web page:**

- Make sure that the computer is connected to one of the four Gigabit-Ethernet LAN ports, or wirelessly to the wireless modem router.
- Make sure that the wireless modem router is fully up and running. Its Wireless LEDs should turn on.
- Close and reopen the browser to make sure the browser does not cache the previous page.

- Browse to **http://routerlogin.net**.
- If your computer is set to a static or fixed IP address (this is uncommon), change the setting to obtain an IP address automatically from the wireless modem router.

➢ **If the wireless modem router does not connect to the Internet:**

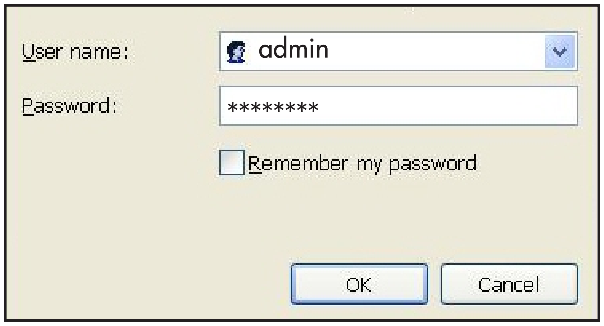
1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 10, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR Genie after Installation

When you first set up your wireless modem router, NETGEAR Genie automatically starts when you launch an Internet browser on a computer that is connected to the wireless modem router. You can use NETGEAR Genie again if you want to view or change settings for the wireless modem router.

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

   The login window displays:



User name: admin

Password: ********

□ Remember my password

3. Enter **admin** for the wireless modem router user name and **password** for the wireless modem router password, both in lowercase letters.

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

Upgrade Wireless Modem Router Firmware

When you set up your wireless modem router and are connected to the Internet, the wireless modem router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. See *Upgrade the Wireless Modem Router Firmware* on page 84 for more information about upgrading firmware.

Click the message when it shows up, and click **Yes** to upgrade the wireless modem router with the latest firmware. After the upgrade, the wireless modem router restarts.

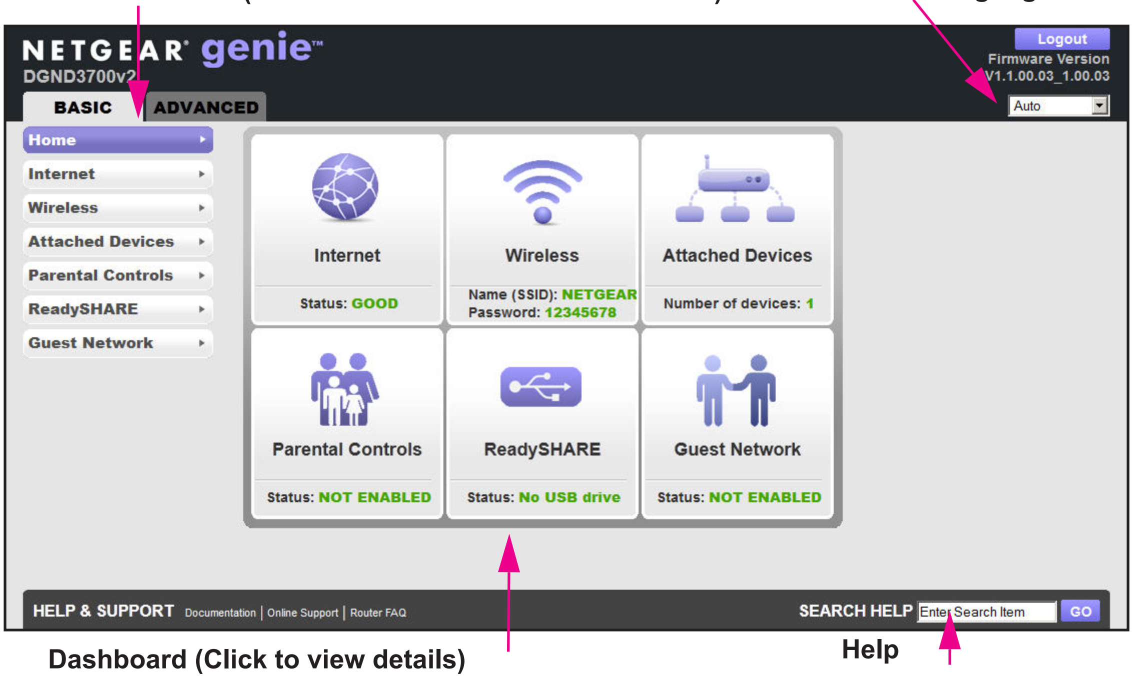
CAUTION:

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

Wireless Modem Router Dashboard (Basic Home Screen)

The wireless modem router Basic Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is an Advanced tab that is used to access additional menus and screens.

Menus (Click the Advanced tab to view more) **Language**



Firmware Version V1.1.00.03_1.00.03

Auto

Status: GOOD

Name (SSID): NETGEAR
Password: 12345678

Number of devices: 1

Status: NOT ENABLED

Status: No USB drive

Status: NOT ENABLED

Enter Search Item

Dashboard (Click to view details) **Help**

Figure 8. Wireless modem router Basic Home screen with dashboard, language, and online help

- **Home. This dashboard screen displays when you log in to the** wireless modem router**.**
- **Internet**. Set, update, and check the ISP settings of your wireless modem router.

- **Wireless**. View or change the wireless settings for your wireless modem router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.
- **ReadySHARE**. If you connected a USB storage device to the wireless modem router, then it is displayed here.
- **Guest Network**. Set up a guest network to allow visitors to use your wireless modem router's Internet connection.
- **Advanced tab**. Set the wireless modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 9, Advanced Settings*. Using this tab requires a solid understanding of networking concepts.
- **Help & Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network. See *Guest Networks* on page 39 for instructions on how to set up a guest network.

Manual Method

➢ **To connect manually:**

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

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard for easily adding computers and other devices to a home network while maintaining security. To use WPS, make sure that all wireless devices to be connected to the network are Wi-Fi certified and support WPS. During the connection process, the client gets the security settings from the wireless modem router so that every device in the network has the same security settings.

➢ **To use WPS to join the wireless network:**

If your wireless device supports WPS (Push 'N' Connect), follow these steps:

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

Genie Basic Settings

3

Your Internet connection and network

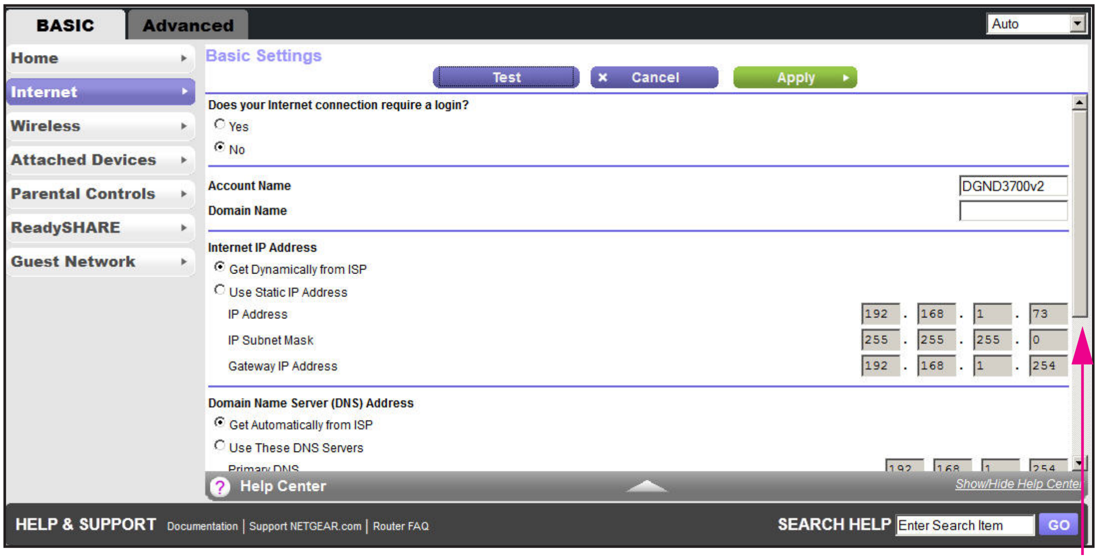
This chapter contains the following sections:

- *Internet Basic Settings*
- *Attached Devices*
- *Parental Controls*
- *ReadySHARE USB Storage and Printer*
- *Basic Wireless Settings*
- *Guest Networks*

Internet Basic Settings

The Internet Basic Settings screen is where you view or change ISP information.

1. From the Basic Home screen, select **Internet**. The following screen displays:



Basic Settings

Does your Internet connection require a login?
○ Yes
● No

Account Name: DGND3700v2
Domain Name:

Internet IP Address
● Get Dynamically from ISP
○ Use Static IP Address
IP Address: 192 . 168 . 1 . 73
IP Subnet Mask: 255 . 255 . 255 . 0
Gateway IP Address: 192 . 168 . 1 . 254

Domain Name Server (DNS) Address
● Get Automatically from ISP
○ Use These DNS Servers
Primary DNS: 192 . 168 . 1 . 254

Scroll to view more settings

The fields that display in the Internet Basic Settings screen depend on whether or not your Internet connection requires a login.

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

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
3. Click **Apply** to save your settings.
4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 10, Troubleshooting*.

Internet Basic Settings Screen Fields

The following descriptions explain all of the possible fields in the Internet Basic Settings screen. Note that which fields display in this screen depends on whether or not an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

These fields display when no login is required:

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

These fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation**. ISP types. The choices are PPPoE or PPPoA.
- **Login**. The login name provided by your ISP. This is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **Idle Timeout (In minutes)**. If you want to change the login time-out, enter a new value in minutes. This determines how long the wireless modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's wireless modem router to which your wireless modem router will connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

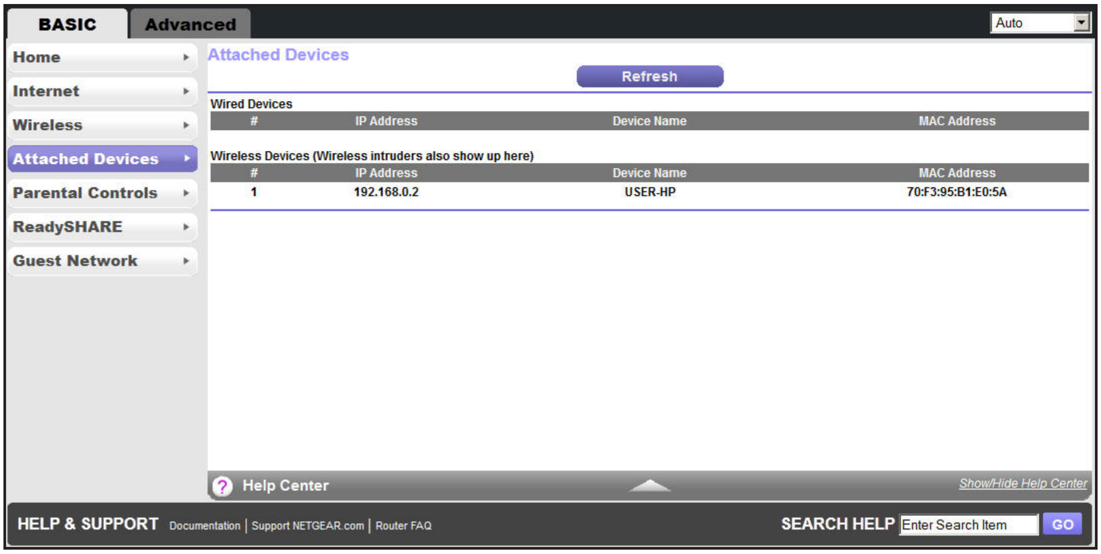
- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the wireless modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Wireless Modem Router MAC Address. The Ethernet MAC address used by the wireless modem router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your wireless modem router to use your computer's MAC address (this is also called cloning).

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The wireless modem router will capture and use the MAC address of the computer that you are now using. You have to use the one computer that is allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

Attached Devices

You can view all computers or devices that are currently connected to your network here. From the Basic Home screen, select **Attached Devices** to display the following screen:



Wired Devices

#	IP Address	Device Name	MAC Address

Wireless Devices (Wireless intruders also show up here)

#	IP Address	Device Name	MAC Address
1	192.168.0.2	USER-HP	70:F3:95:B1:E0:5A

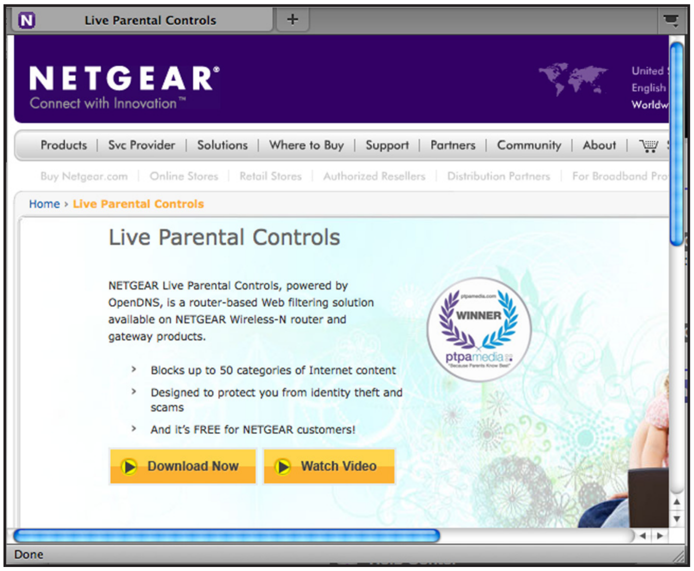
Wired devices are connected to the wireless modem router with Ethernet cables. Wireless devices have joined the wireless network.

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the wireless modem router assigned to this device when it joined the network. Note that this number can change if a device is disconnected and rejoins the network.
- **Device Name**. If the device name is known, it is shown here.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

You can click **Refresh** to update this screen.

Parental Controls

The first time you select Parental Controls from the Basic Home screen, you are automatically directed to the Internet, where you can learn more about Live Parental Controls or download the application. The following screen displays:


Live Parental Controls
NETGEAR
Connect with Innovation™
United
English
Worldw
Products | Svc Provider | Solutions | Where to Buy | Support | Partners | Community | About
Buy Netgear.com | Online Stores | Retail Stores | Authorized Resellers | Distribution Partners | For Broadband Pro
Home › Live Parental Controls
WINNER
ptpamedia
Download Now
Watch Video
Done

Live Parental Controls

NETGEAR Live Parental Controls, powered by OpenDNS, is a router-based Web filtering solution available on NETGEAR Wireless-N router and gateway products.

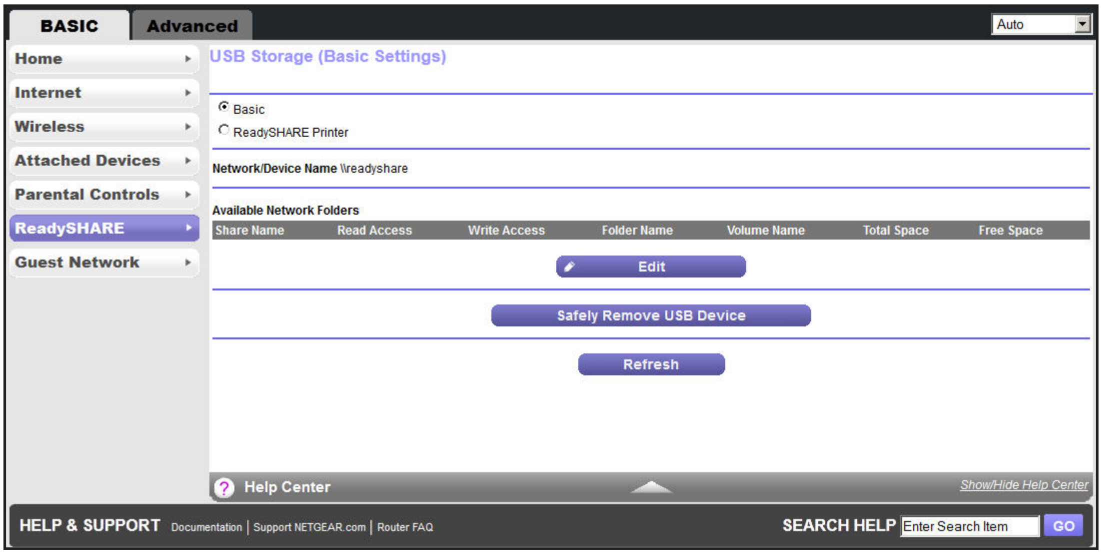
- Blocks up to 50 categories of Internet content
- Designed to protect you from identity theft and scams
- And it's FREE for NETGEAR customers!

ReadySHARE USB Storage and Printer

You can view information about a USB storage device that is connected to the wireless modem router’s USB port here.

USB Storage (Basic Settings)

From the Basic Home screen, select **ReadySHARE** to display the USB Storage (Basic Settings) screen:



USB Storage (Basic Settings)

● Basic
○ ReadySHARE Printer

Network/Device Name \\readyshare

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space

This screen displays the following when Basic is selected:

- **Network/Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the wireless modem router.
- **Available Network Folders**. The folders on the USB device.

  Share Name. If only one device is connected, the default share name is USB_Storage. You can click the name shown, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.

  Read and Write Access. Show the permissions and access controls on the network folder: All – no password (the default) allows all users to access the network folder. The user name (account name) for All – no password is guest. The password for admin is the same one that you use to log in to the wireless modem router. By default, it is **password**.

  Folder Name. Full path used by the network folder.

  Volume Name. Volume name from the storage device (either USB drive or HDD).

  Total and Free Space. Show the current utilization of the storage device.
- **Edit**. Click the **Edit** button to edit the Available Network Folders settings.

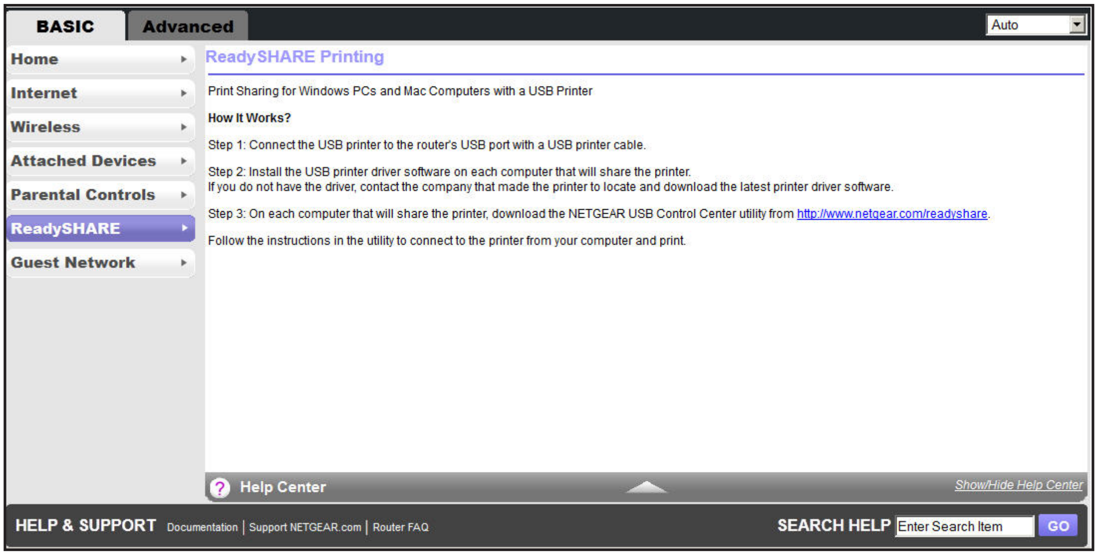
- **Safely Remove a USB Device**. Click to safely remove the USB device attached to your wireless modem router.

You can click **Refresh** to update this screen.

For more information about USB storage, see *Chapter 5, USB Storage*.

ReadySHARE Printer

From the Basic Home screen, select **ReadySHARE**, and from the USB Storage (Basic Settings) screen, select **ReadySHARE Printer** to display the following screen:



ReadySHARE Printing

Print Sharing for Windows PCs and Mac Computers with a USB Printer

How It Works?

Step 1: Connect the USB printer to the router's USB port with a USB printer cable.

Step 2: Install the USB printer driver software on each computer that will share the printer.
If you do not have the driver, contact the company that made the printer to locate and download the latest printer driver software.

Step 3: On each computer that will share the printer, download the NETGEAR USB Control Center utility from http://www.netgear.com/readyshare.

Follow the instructions in the utility to connect to the printer from your computer and print.

For more information about USB printing, see *Chapter 6, USB Printer Control*.

Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The N600 Modem 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 bottom of the unit.

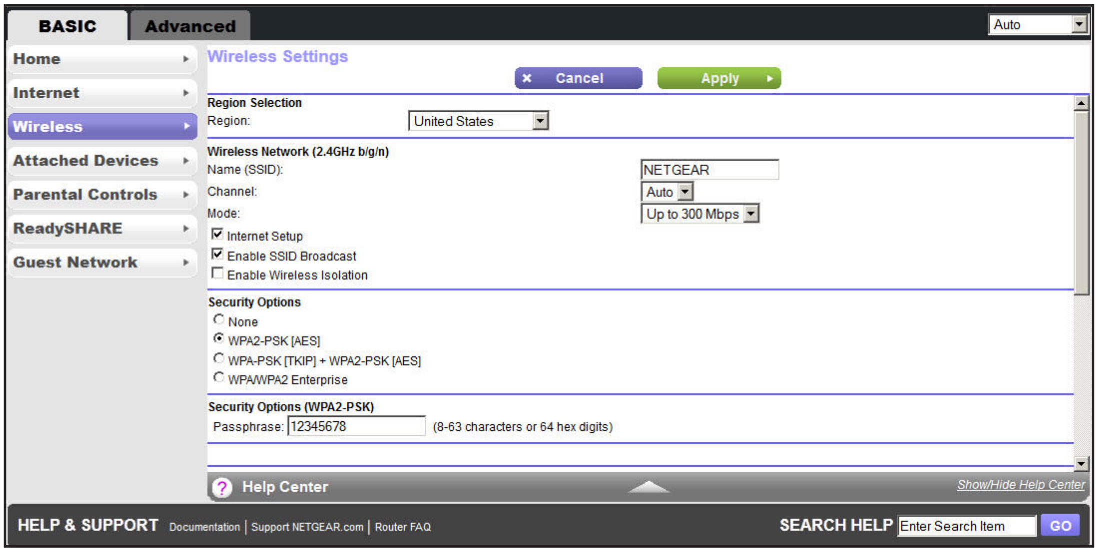
Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

NETGEAR recommends that you do not change your preset security settings. If you do decide to 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 Apply. To avoid this problem, use a computer with a wired connection to access the wireless modem router.

➢ To view or change basic wireless settings:

1. On the Basic Home screen, select **Wireless** to display the Wireless Settings screen.



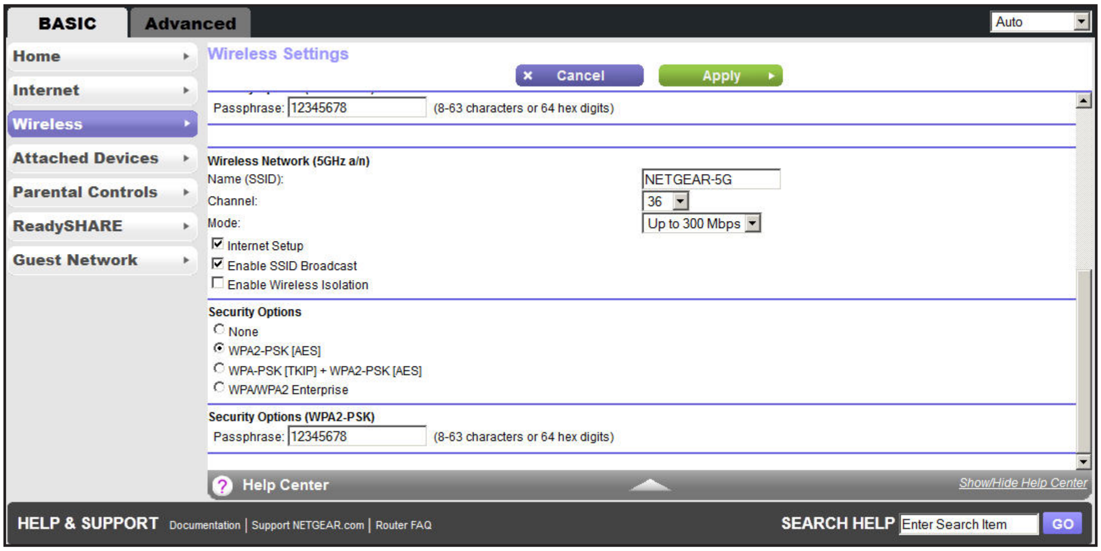
Wireless Settings

Region Selection
Region: United States

Wireless Network (2.4GHz b/g/n)
Name (SSID): NETGEAR
Channel: Auto
Mode: Up to 300 Mbps
☑ Internet Setup
☑ Enable SSID Broadcast
☐ Enable Wireless Isolation

Security Options
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise

Security Options (WPA2-PSK)
Passphrase: 12345678 (8-63 characters or 64 hex digits)



Wireless Settings

Passphrase: 12345678 (8-63 characters or 64 hex digits)

Wireless Network (5GHz a/n)
Name (SSID): NETGEAR-5G
Channel: 36
Mode: Up to 300 Mbps
☑ Internet Setup
☑ Enable SSID Broadcast
☐ Enable Wireless Isolation

Security Options
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise

Security Options (WPA2-PSK)
Passphrase: 12345678 (8-63 characters or 64 hex digits)

The screen sections, settings, and procedures are explained in the following sections.

2. Make any changes that are needed, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
    - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.

- Does your wireless device or computer show up on the Attached Devices screen? If it does, then it is connected to the network.
- If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your wireless modem router.

Wireless Settings Screen Fields

Region. The location where the wireless modem router is used. Select from the countries in the list. Note that in the United States, the region is fixed to United States and is not changeable.

Wireless Network

Note: These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and ***NETGEAR strongly recommends that you do not change this.***

Channel. This setting is the wireless channel used by the gateway. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

Mode. Up to 130 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 300 Mbps setting allows 802.11n devices to connect at this speed.

Enable SSID Broadcast. This setting allows the wireless modem router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box, and click **Apply**.

Enable Wireless Isolation. If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

Security Options Settings

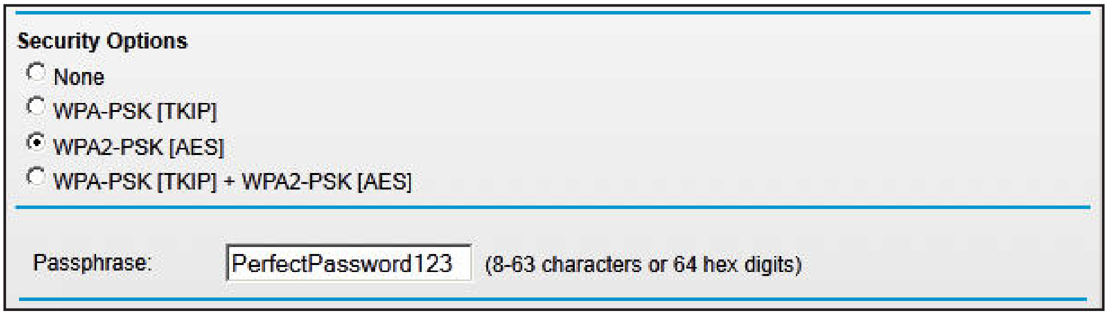
Note: These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

The Security Options section of the Wireless Setup screen lets you change the security option and passphrase. Please note that ***NETGEAR recommends that you not change the security option or passphrase,*** but if you want to change these settings, this section explains how. ***Do not disable security***.

Change WPA Security Option and Passphrase

Note: These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

1. Under Security Options, select the WPA option you want.



Security Options

○ None
○ WPA-PSK [TKIP]
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Passphrase: PerfectPassword123 (8-63 characters or 64 hex digits)

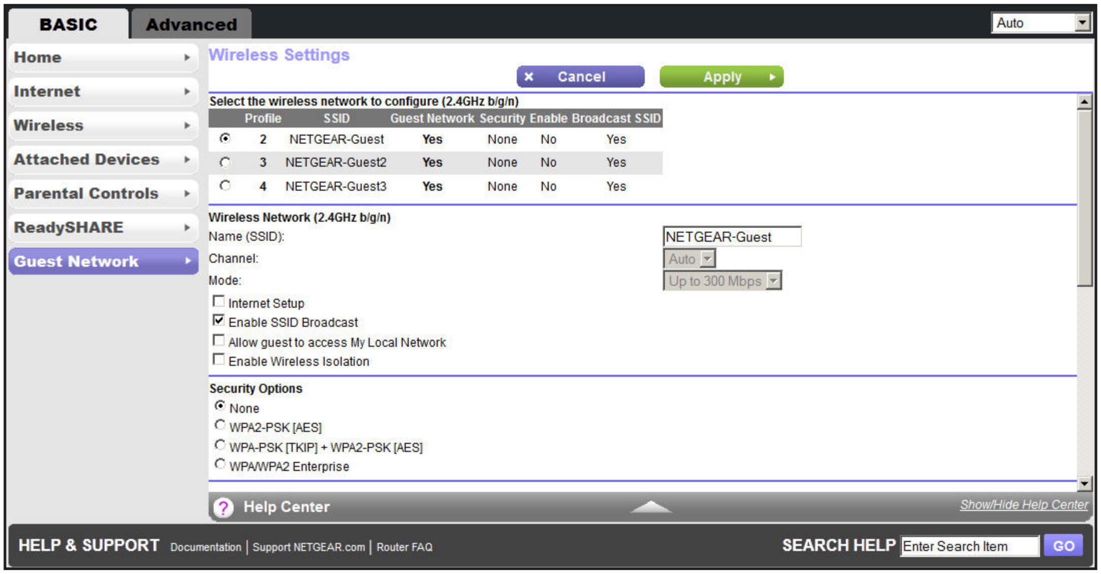
2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Guest Networks

Adding a guest network allows visitors at your home to use the Internet without providing them with 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. From the Basic Home screen, select **Guest Network** to display the following screen:



Wireless Settings

Select the wireless network to configure (2.4GHz b/g/n)

	Profile	SSID	Guest Network	Security	Enable	Broadcast SSID
●	2	NETGEAR-Guest	Yes	None	No	Yes
○	3	NETGEAR-Guest2	Yes	None	No	Yes
○	4	NETGEAR-Guest3	Yes	None	No	Yes

Wireless Network (2.4GHz b/g/n)

Name (SSID): NETGEAR-Guest

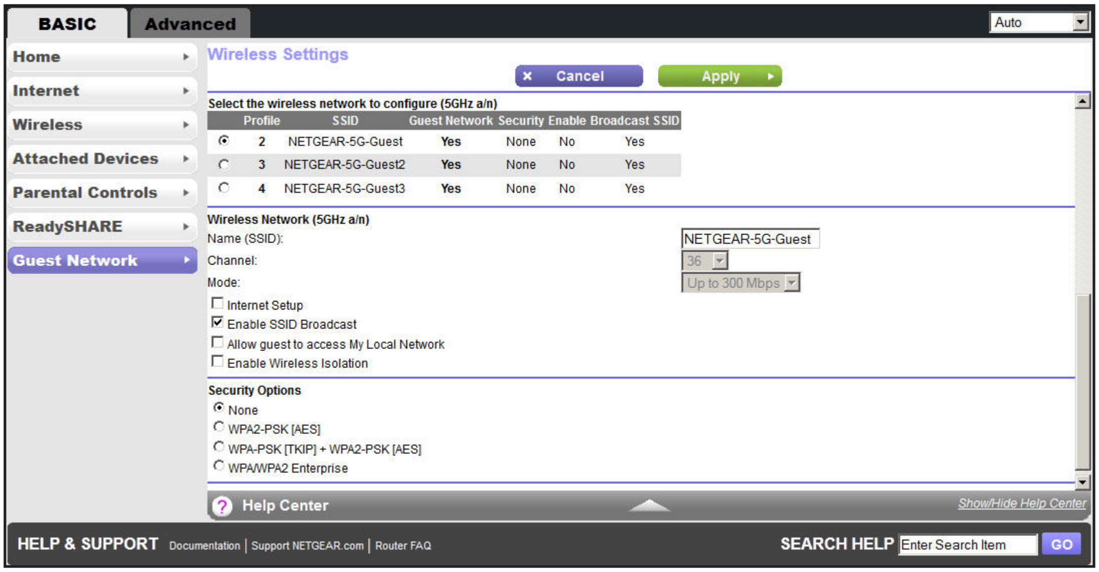
Channel: Auto

Mode: Up to 300 Mbps

□ Internet Setup
☑ Enable SSID Broadcast
□ Allow guest to access My Local Network
□ Enable Wireless Isolation

Security Options

● None
○ WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise



Wireless Settings

Select the wireless network to configure (5GHz a/n)

	Profile	SSID	Guest Network	Security	Enable	Broadcast SSID
●	2	NETGEAR-5G-Guest	Yes	None	No	Yes
○	3	NETGEAR-5G-Guest2	Yes	None	No	Yes
○	4	NETGEAR-5G-Guest3	Yes	None	No	Yes

Wireless Network (5GHz a/n)

Name (SSID): NETGEAR-5G-Guest

Channel: 36

Mode: Up to 300 Mbps

□ Internet Setup
☑ Enable SSID Broadcast
□ Allow guest to access My Local Network
□ Enable Wireless Isolation

Security Options

● None
○ WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]
○ WPA/WPA2 Enterprise

2. Select any of the following wireless settings:

Note: These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

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 access My Local Network. If this check box is selected, any user who connects to this SSID has access to your local network, not just Internet access.

Enable Wireless Isolation. If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

3. 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 nonguest SSID.

4. Select a security option from the list. The security options are described in *Guest Network Wireless Security Options* on page 40.
5. Click **Apply** to save your selections.

Guest Network Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.

This section presents an overview of the security options and provides guidance on when to use which option. Note that it is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend this.

Wi-Fi Protected Access (WPA) encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA-PSK uses a passphrase to perform authentication and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.

WPA2-PSK is stronger than WPA. It is advertised to be indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is usually implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring their WPA settings.

Genie Advanced Home

4

Specify custom settings

This chapter contains the following sections:

- *Setup Wizard*
- *WPS Wizard*
- *VPN Wizard*
- *Setup Menu*
- *ADSL Setup*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

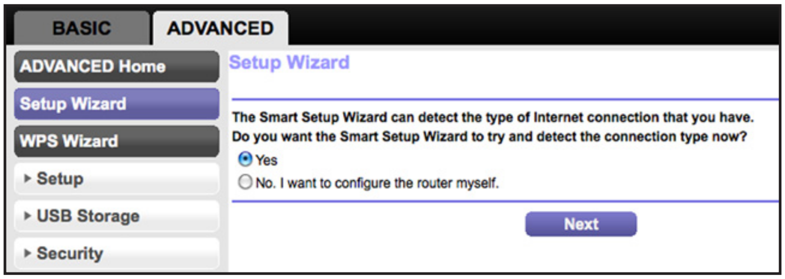
Some selections on the Advanced Home screen are described in separate chapters:

- **USB Storage**. See *Chapter 5, USB Storage*.
- **Security**. See *Chapter 7, Security*.
- **Administration**. See *Chapter 8, Administration*.
- **Advanced Setup**. See *Chapter 9, Advanced Settings*.

Setup Wizard

The NETGEAR Genie installation process is launched the first time you set up the wireless modem router. After setting up the wireless modem router the first time, if you want to perform this task again, you can run Setup Wizard from the Advanced tab of the Genie.

1. Select **Setup Wizard** to display the following screen:

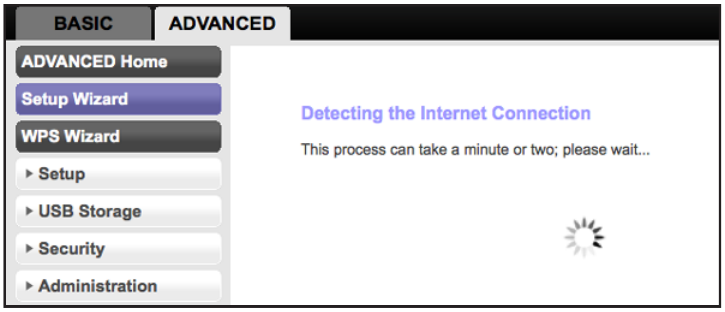


Setup Wizard

The Smart Setup Wizard can detect the type of Internet connection that you have.
Do you want the Smart Setup Wizard to try and detect the connection type now?

● Yes
○ No. I want to configure the router myself.

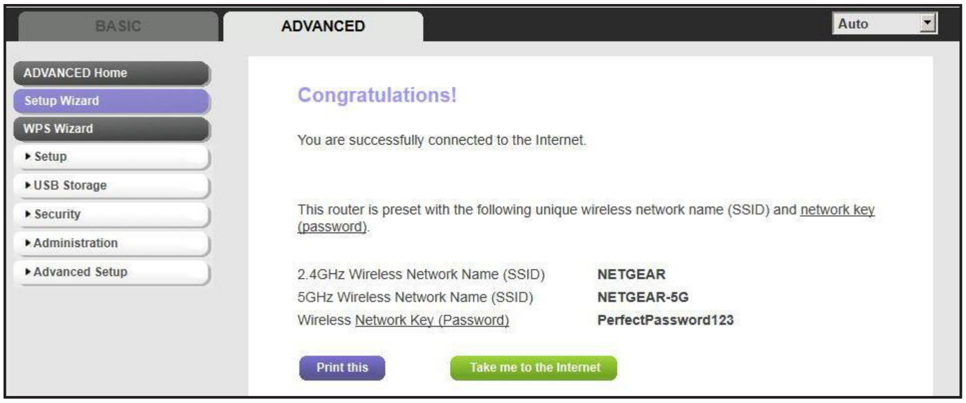
2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, you are taken to the Internet Setup screen (see *Internet Basic Settings* on page 30).
3. If you selected Yes, click **Next**. The following screen displays:



Detecting the Internet Connection

This process can take a minute or two; please wait...

The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. The following screen displays:



Congratulations!

You are successfully connected to the Internet.

This router is preset with the following unique wireless network name (SSID) and network key (password).

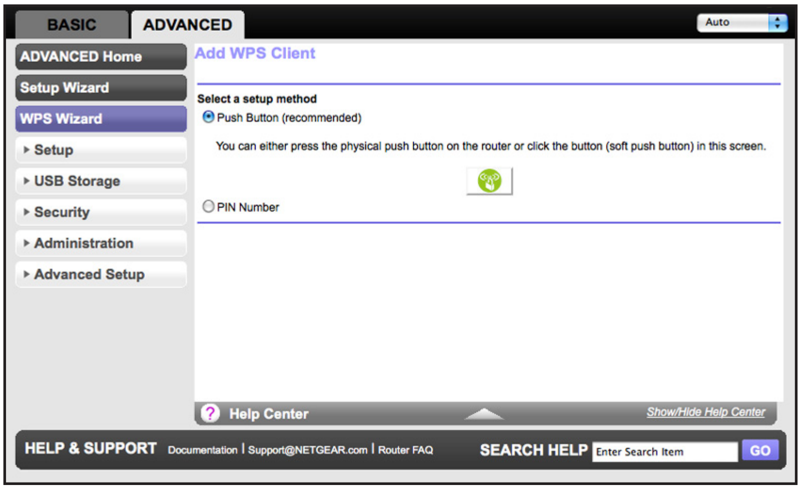
2.4GHz Wireless Network Name (SSID)	NETGEAR
5GHz Wireless Network Name (SSID)	NETGEAR-5G
Wireless Network Key (Password)	PerfectPassword123

WPS Wizard

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device you need to either press its WPS button or locate its WPS PIN.

➢ To use the WPS Wizard:

1. Select **Advanced > WPS Wizard**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).



Add WPS Client

Select a setup method

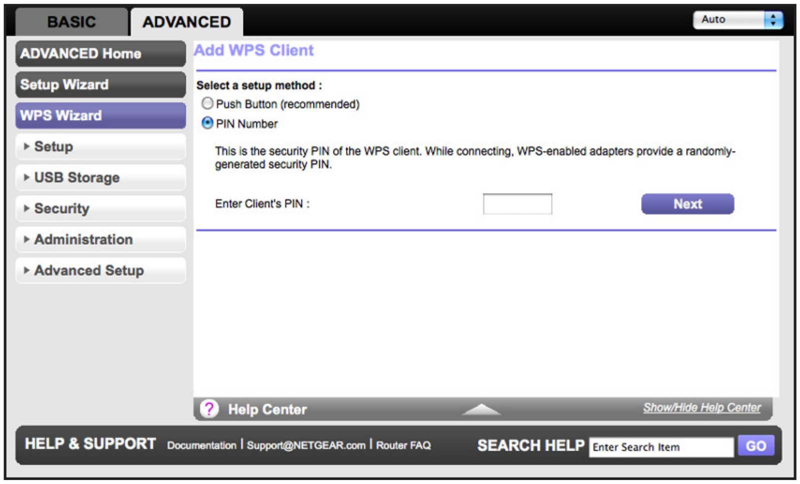
● Push Button (recommended)

You can either press the physical push button on the router or click the button (soft push button) in this screen.

○ PIN Number

You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.
   - To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button located on the top of the wireless modem router. Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
   - To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.



Add WPS Client

Select a setup method :

○ Push Button (recommended)

● PIN Number

This is the security PIN of the WPS client. While connecting, WPS-enabled adapters provide a randomly-generated security PIN.

Enter Client's PIN :

Within two minutes, go to the client device and use its WPS software to join the network without entering a password.

The wireless modem router attempts to add the WPS-capable device. The WPS LED on the top of the wireless modem router blinks green. When the wireless modem router establishes a WPS connection, the LED is solid green, and the wireless modem router WPS screen displays a confirmation message.

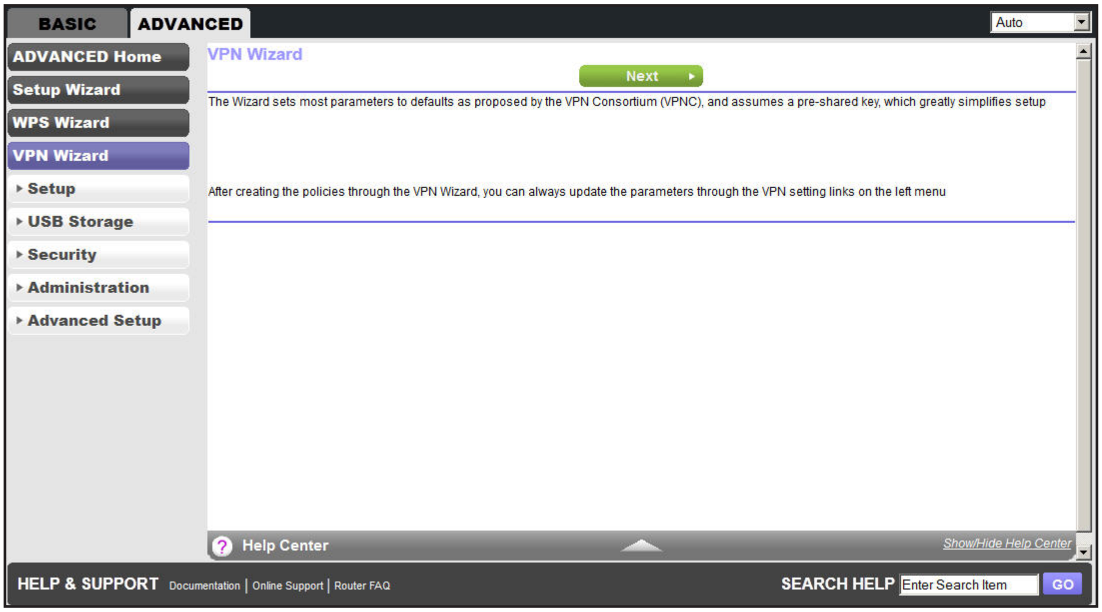
4. Repeat Step 2 and Step 3 to add another WPS client to your network.

VPN Wizard

The VPN Wizard asks you series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard sets the parameters for the network connection, Security Association, traffic selectors, authentication algorithm, and encryption. These parameters are based on the VPNC recommendations. More information about the VPNC recommendations is presented in the VPN Wizard summary page.

➢ To use the VPN Wizard:

1. Select **ADVANCED > VPN Wizard**.

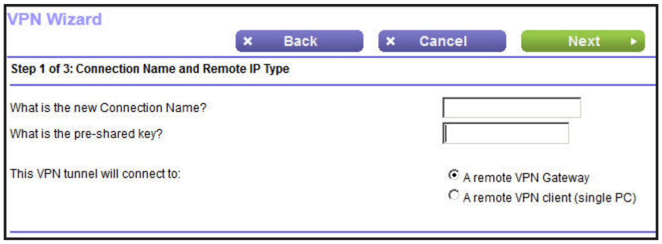


VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup

After creating the policies through the VPN Wizard, you can always update the parameters through the VPN setting links on the left menu

2. Click the **Next** button.



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name?

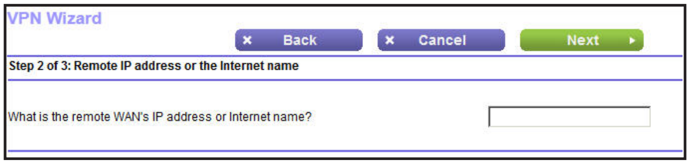
What is the pre-shared key?

This VPN tunnel will connect to:
● A remote VPN Gateway
○ A remote VPN client (single PC)

Enter the requested information:

- **Connection name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN endpoint. Rather, it is used to help you manage the VPN settings.
- **Pre-shared key**. The key has to be entered both here and on the remote VPN Gateway or the remote VPN client. This method does not require using a CA (Certificate Authority).
- **VPN tunnel connection**. The wizard has to know if you are planning to connect to a remote gateway or setting up the connection for a remote client or computer to establish a secure connection to this device.

3. Click the **Next** button.



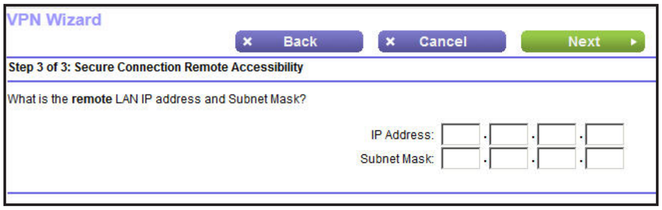
VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name?

Enter the remote IP address of the gateway you want to connect to, or provide the Internet name of the gateway. The Internet name is the fully qualified domain name, as set up in a Dynamic DNS service.

4. Click the **Next** button.



Step 3 of 3: Secure Connection Remote Accessibility

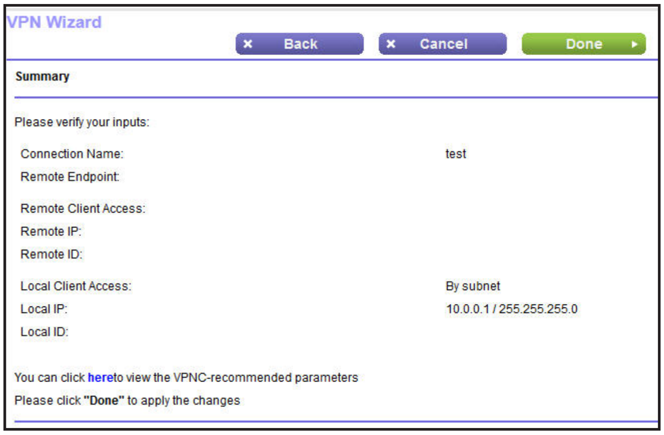
What is the **remote** LAN IP address and Subnet Mask?

IP Address: [ ].[ ].[ ].[ ]
Subnet Mask: [ ].[ ].[ ].[ ]

Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel fails to connect.
- The IP address range used on the remote LAN has to be different from the IP address range used on the local LAN.

5. Click the **Next** button.



Summary

Please verify your inputs:

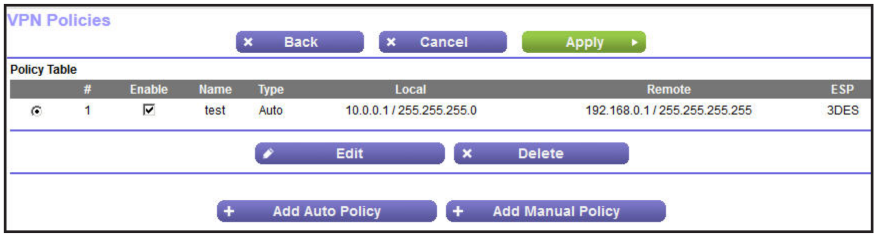
Connection Name:	test
Remote Endpoint:	
Remote Client Access:	
Remote IP:	
Remote ID:	
Local Client Access:	By subnet
Local IP:	10.0.0.1 / 255.255.255.0
Local ID:	

You can click hereto view the VPNC-recommended parameters

Please click **"Done"** to apply the changes

This screen shows the summary of the Wizard configuration with a link to view the VPNC recommended parameters (click the **here** link to view the VPNC-recommended parameters).

6. Click the **Done** button.



Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
●	1	☑	test	Auto	10.0.0.1 / 255.255.255.0	192.168.0.1 / 255.255.255.255	3DES

For information about how to add or modify VPN policies, see *VPN Policies* on page 123.

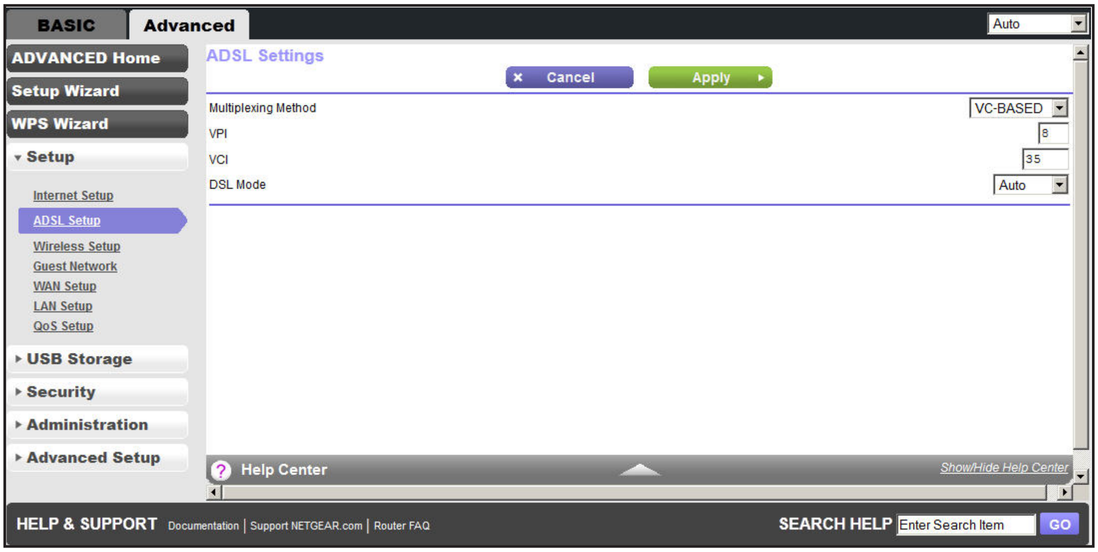
Setup Menu

Select **ADVANCED > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup**. This is a shortcut to the same Internet Basic Settings screen that you can access from the dashboard on the Basic Home screen. See *Internet Basic Settings* on page 30.
- **ADSL Setup**. Internet (ADSL) setup. See *ADSL Setup* on page 48.
- **Wireless Setup**. This is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the Basic Home screen. See *Basic Wireless Settings* on page 35.
- **Guest Network**. This is a shortcut to the same Wireless Settings (for guest networks) screen that you can access from the dashboard on the Basic Home screen. See *Guest Networks* on page 39.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 49.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 52.
- **QoS Setup**. Quality of Service (QoS) setup. See *Quality of Service (QoS) Setup* on page 55.

ADSL Setup

The ADSL Settings screen lets you configure the multiplexing method and virtual circuit of your ADSL connection. The default parameters should be correct to match the system used by your ISP. Select **Advanced > Setup > ADSL Setup** to view the following screen:



ADSL Settings

Multiplexing Method: VC-BASED

VPI: 8

VCI: 35

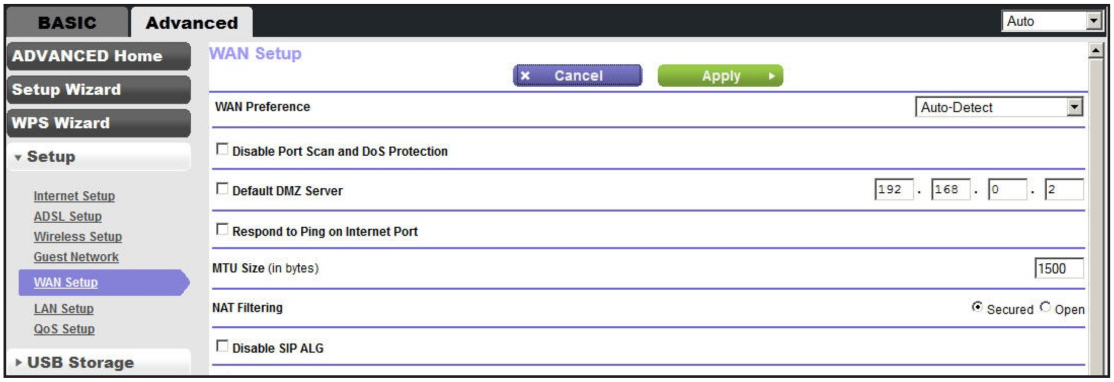
DSL Mode: Auto

- **Multiplexing Method**. Your ISP will indicate whether your multiplexing method is VC-BASED or LLC-BASED.

- **VPI, VCI**. Your ISP will indicate which VPI/VCI combination is used for your service.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the wireless modem router to respond to a ping on the WAN (Internet) port. Select **Advanced > Setup > WAN Setup** to view the following screen:



WAN Preference: Auto-Detect

□ Disable Port Scan and DoS Protection

□ Default DMZ Server 192 . 168 . 0 . 2

□ Respond to Ping on Internet Port

MTU Size (in bytes): 1500

NAT Filtering: ● Secured ○ Open

□ Disable SIP ALG

- **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, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games and/or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the wireless modem router to respond to a ping from the Internet, select this check box. Use this only as a diagnostic tool because it allows your wireless modem router to be discovered. Do not select this check box unless you have a specific reason.
- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. See *Change the MTU Size* on page 50.
- **NAT Filtering**. Network Address Translation (NAT) determines how the wireless modem router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.
- **Disable SIP ALG**. Some VoIP applications do not work well with the SIP ALG. Enabling this option to turn off the SIP ALG might help your VoIP devices to create/accept a call through the router.

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 wireless modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer’s IP address is entered as the default DMZ server.

WARNING:

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

Incoming traffic from the Internet is usually discarded by the wireless modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

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 have to be split or “fragmented” to accommodate the device with the smallest MTU.

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

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that will not open, or displays only part of a web page
  - Yahoo email

  - MSN portal
  - 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 websites, frames within websites, secure login pages, or 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. The following table describes common MTU sizes and applications.

Table 11. 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 wireless modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not 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. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size between 64 and 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The wireless modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless modem router’s default LAN IP configuration is:

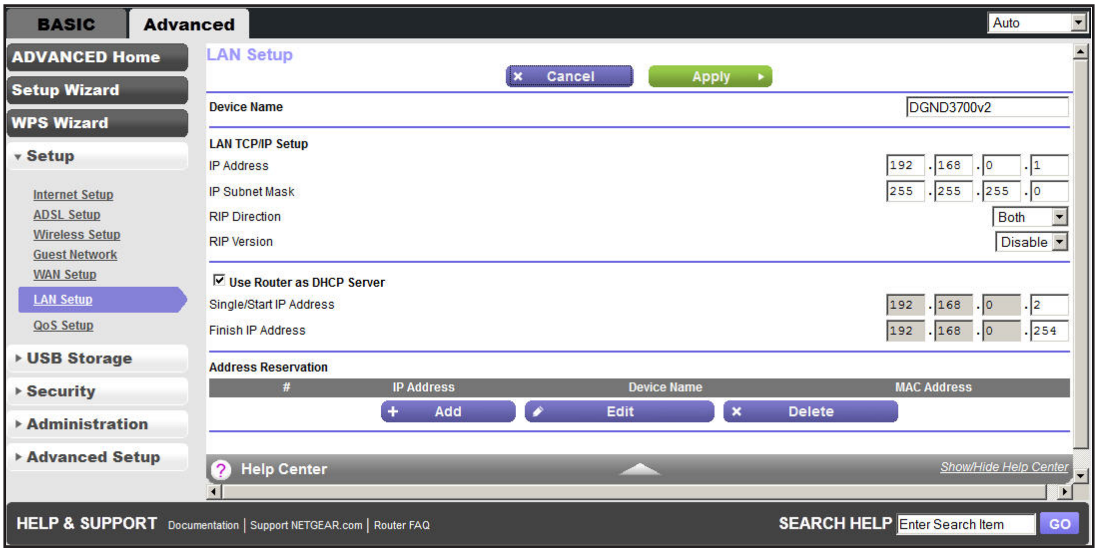
- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

➢ To change the LAN settings:

Note: If you change the LAN IP address of the wireless modem router while connected through the browser, you will be disconnected. You will have to open a new connection to the new IP address and log in again.

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



LAN Setup

Device Name: DGND3700v2

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disable

☑ Use Router as DHCP Server

Single/Start IP Address: 192 . 168 . 0 . 2

Finish IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

2. Enter the settings that you want to customize. These settings are described in the following section, *LAN Setup Screen Settings*.
3. Click **Apply** to save your changes.

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the wireless modem router.
- **IP Subnet Mask**. The LAN subnet mask of the wireless modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or wireless modem router.
- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **RIP Version**. This controls the format and the broadcasting method of the RIP packets that the wireless modem router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.
  - **RIP-1** is universally supported. It is adequate for most networks, unless you have an unusual network setup.
  - **RIP-2** 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.

Use Router as a DHCP Server

This check box is usually selected so that the wireless modem router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the wireless modem router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the wireless modem router.

Address Reservation

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

Use the Wireless Modem Router as a DHCP Server

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

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless modem router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

The wireless modem 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 wireless modem router’s LAN IP address)
- DNS server IP address (the wireless modem router’s LAN IP address)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, you need to set your computers’ IP addresses manually or they will not be able to access the wireless modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the wireless modem router’s DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the wireless modem router’s LAN subnet, such as 192.168.1.x.)
3. 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.

4. Click **Apply** to enter the reserved address into the table.

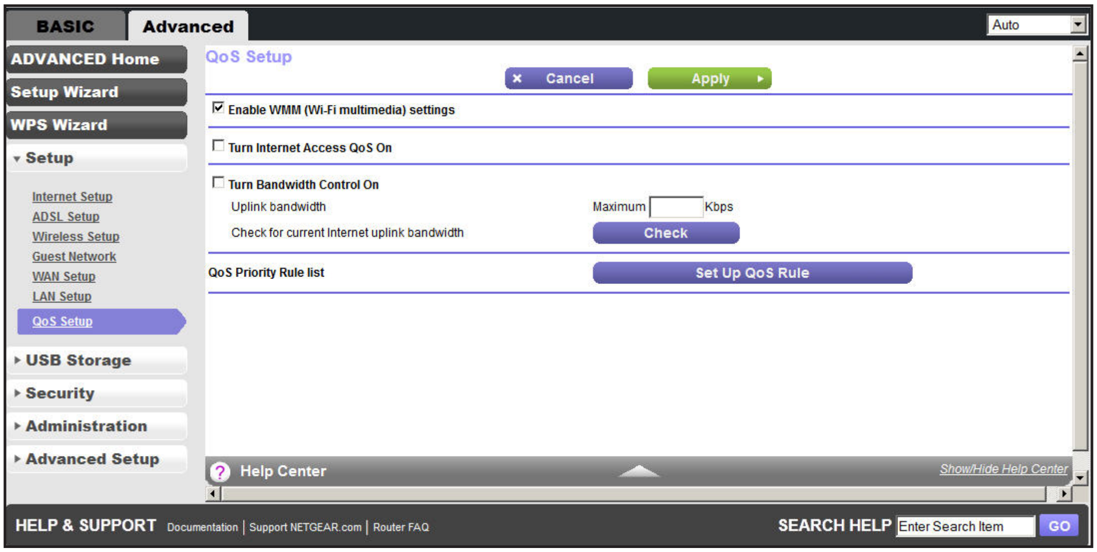
   The reserved address is not assigned until the next time the computer contacts the wireless modem router’s DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The N600 Modem Router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

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



QoS Setup

☑ Enable WMM (Wi-Fi multimedia) settings

□ Turn Internet Access QoS On

□ Turn Bandwidth Control On

Uplink bandwidth Maximum Kbps

Check for current Internet uplink bandwidth

QoS Priority Rule list

Enable WMM QoS for Wireless Multimedia Applications

The N600 Modem Router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

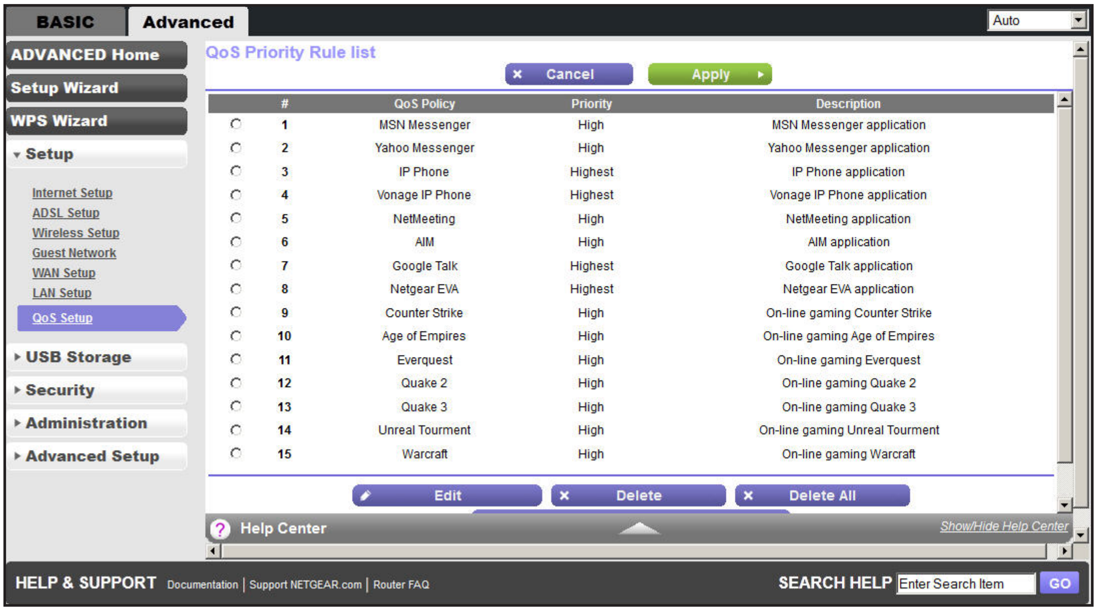
- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the wireless modem router
- A specific device by MAC address

To specify prioritization of traffic, you have to create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

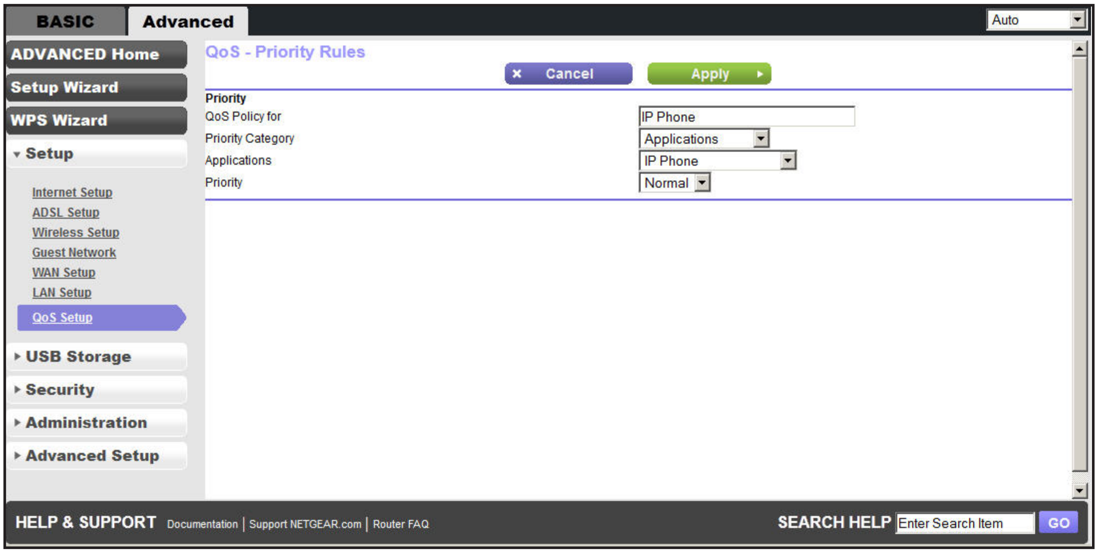
1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS rule** button to see the existing priority rules. On this screen you can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all of the rules by simply clicking the **Delete All** button.



QoS Priority Rule list

	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	Netgear EVA application
○	9	Counter Strike	High	On-line gaming Counter Strike
○	10	Age of Empires	High	On-line gaming Age of Empires
○	11	Everquest	High	On-line gaming Everquest
○	12	Quake 2	High	On-line gaming Quake 2
○	13	Quake 3	High	On-line gaming Quake 3
○	14	Unreal Tourment	High	On-line gaming Unreal Tourment
○	15	Warcraft	High	On-line gaming Warcraft

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:

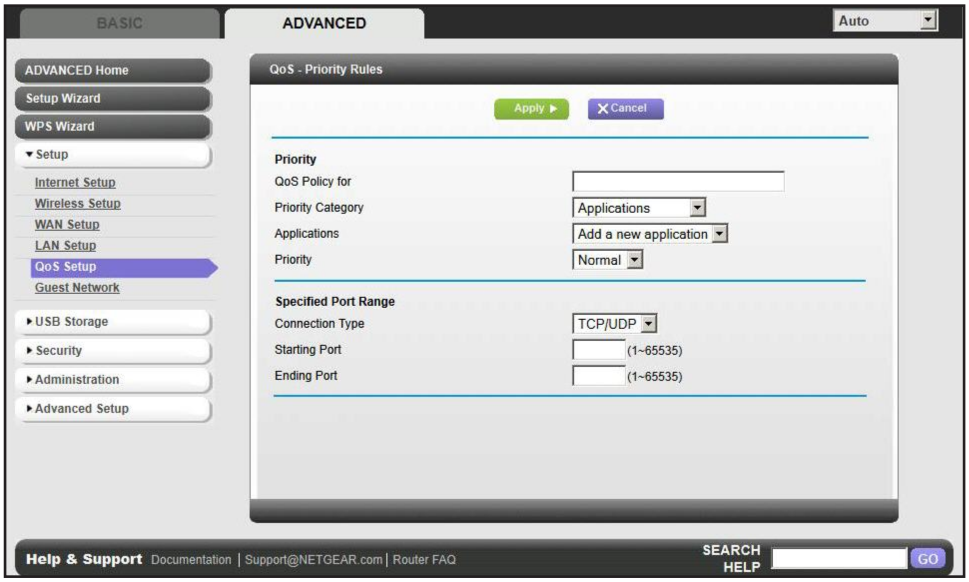


QoS - Priority Rules

Priority

QoS Policy for	IP Phone
Priority Category	Applications
Applications	IP Phone
Priority	Normal

4. In the QoS Policy for field, type the name of the application or game.
5. In the Priority Category list, select either **Applications** or **Online Gaming**. In either case, a list of applications or games displays in the list.
6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.
    a. If you add a new entry, the QoS - Priority Rules screen expands as shown:



Priority

QoS Policy for

Priority Category: Applications

Applications: Add a new application

Priority: Normal

Specified Port Range

Connection Type: TCP/UDP

Starting Port (1~65535)

Ending Port (1~65535)

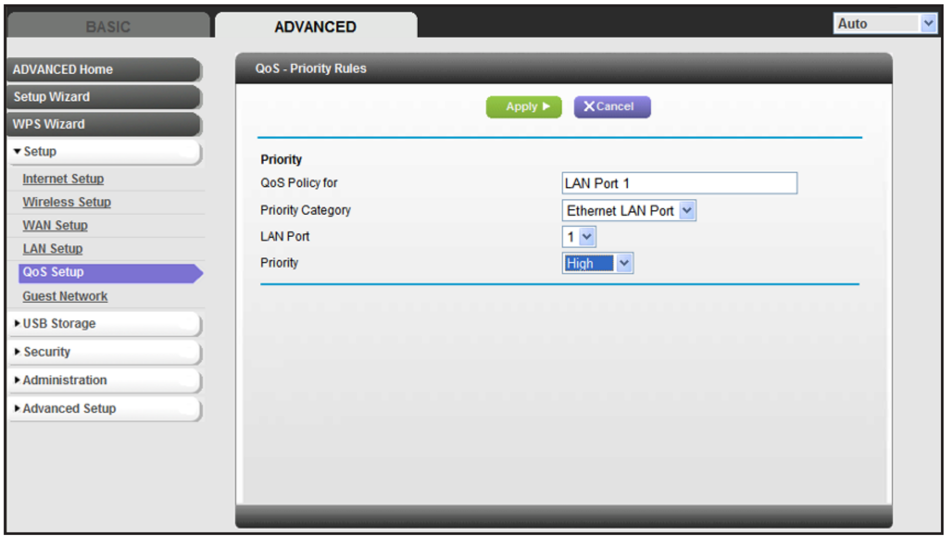
    b. In the QoS Policy for field, enter a descriptive name for the new application or game.
    c. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.
7. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a Wireless Modem Router LAN Port

➢ **To create a QoS policy for a device connected to one of the wireless modem router's LAN ports:**

1. Select **Advanced > Setup > QoS Setup** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button.
3. Click the **Add Priority Rule** button.

4. From the Priority Category list, select **Ethernet LAN Port**, as shown in the following figure:



Priority

QoS Policy for: LAN Port 1

Priority Category: Ethernet LAN Port

LAN Port: 1

Priority: High

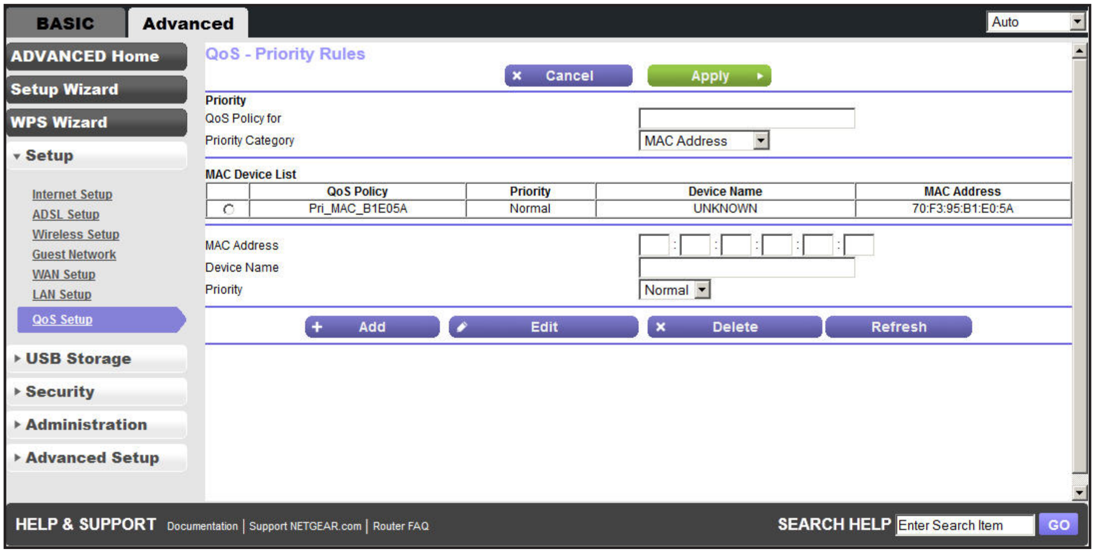
5. From the LAN port list, select the LAN port that will have a QoS policy.
6. From the Priority list, select the priority that this port’s traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **Advanced > Setup > QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays.
2. Click **Add Priority Rule**.

3. From the Priority Category list, select **MAC Address** to display the following screen:



QoS - Priority Rules

Priority

QoS Policy for	
Priority Category	MAC Address

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
○	Pri_MAC_B1E05A	Normal	UNKNOWN	70:F3:95:B1:E0:5A

MAC Address	: : : : :
Device Name	
Priority	Normal

4. If the device to be prioritized appears in the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you have to complete these fields manually.
5. From the Priority list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest. Click **Add** to add this rule to MAC Device List.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Edit or Delete an Existing QoS Policy

➤ **To edit or delete a QoS policy:**

1. Select **Advanced > QoS Setup** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply** in the QoS Setup screen to save your changes.

USB Storage

5

Access and configure a USB storage drive

This chapter describes how to access and configure a USB storage drive attached to your wireless modem router. Be aware that the USB port on the wireless modem router can be used to connect only to USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the wireless modem router USB port.

This chapter contains the following sections:

- *USB Drive Requirements*
- *ReadySHARE Access*
- *File-Sharing Scenarios*
- *USB Storage Basic Settings*
- *USB Storage Advanced Settings*
- *Safely Remove a USB Drive*
- *Media Server Settings*
- *Specify Approved USB Devices*
- *Connect to the USB Drive from a Remote Computer*

USB Drive Requirements

The wireless modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table. Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

Table 12. USB drive speeds

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

The wireless modem router should work with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the wireless modem router, go to:

http://kbserver.netgear.com/readyshare

The wireless modem router supports both read and write access for FAT16, FAT32, and NTFS.

Note: Some USB external hard drives and flash drives require drivers to be loaded into the computer before the computer can access the USB device. Such USB devices will not work with the wireless modem router.

ReadySHARE Access

Once you have set up your wireless modem router, you can connect any USB storage device and share the contents with other users on your network.

You can access your USB device in any of the following ways:

- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, select **Start > Run**, and enter **\\readyshare** in the dialog box. Click **OK**.
- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, open Internet Explorer or Safari, and enter **\\readyshare** in the address bar.
- On Mac OS X (version 10.2 or later), enter **smb://readyshare** in the address bar.
- In My Network Places, enter **\\readyshare** in the address bar.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any Windows, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia such as MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. You might want to store files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and Windows computers by using the USB drive as a go-between across the systems.
- Sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Share Photos

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

➢ **To share files with your friends and family:**

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

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

2. If you want to specify read-only access or to allow access from the Internet, see *USB Storage Advanced Settings* on page 65.

Store Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server.

- One family member has photos on a Macintosh computer that she wants to print.
- The photo-capable color printer is directly attached to a computer, but not shared on the network.
- The Mac and PC are not visible to each other on the network.

➢ **To print photos from a Mac on the printer attached to a PC:**

1. On the Mac, access the USB drive by typing **\\readyshare** in the address field of a web browser. Then copy the photos to the USB drive.
2. On the PC, use a web browser or Microsoft Networking to copy the files from the USB drive to the PC. Then print the files.

Share Large Files over the Internet

Sending files that are larger than 5 MB can pose a problem for many email systems. The wireless modem router allows you to share very large files such as PowerPoint presentations or .zip files over the Internet. FTP can be used to easily download shared files from the wireless modem router.

Sharing files with a remote colleague involves the following considerations:

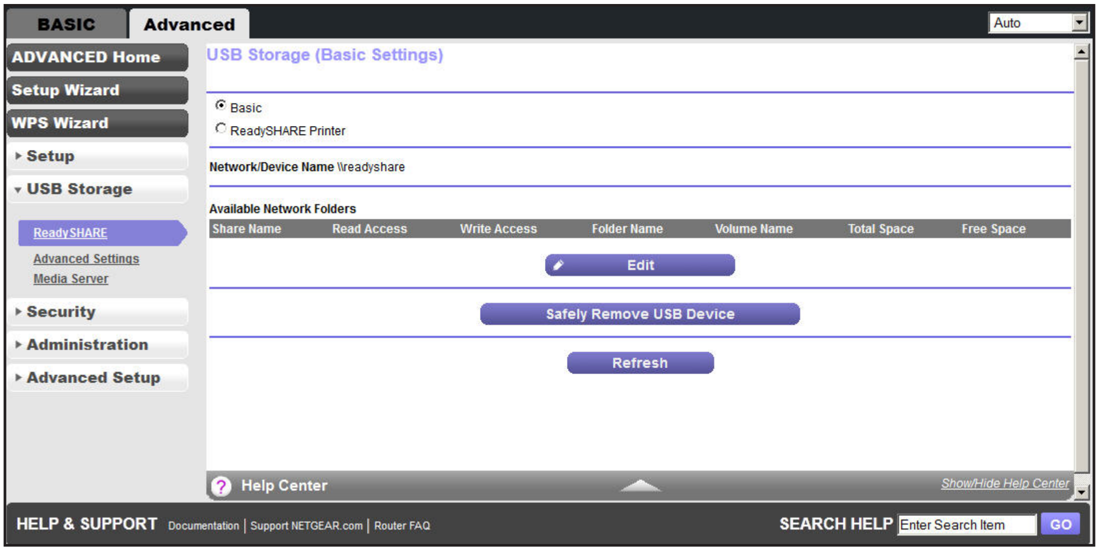
- There are two user accounts: admin and guest. The password for admin is the same one that you use to access the wireless modem router. By default, it is **password**. The guest user account has no password.
- On the FTP site, the person receiving the files should use the guest user account and enter any password (FTP requires that you type something in the password field).
- Be sure to select the **FTP (via Internet)** check box in the USB Storage (Advanced Settings) screen. This option supports both downloading and uploading of files.

Note: You can enable the HTTP (via Internet) option on the USB Storage (Advanced Settings) screen to share large files. This option supports downloading files only.

USB Storage Basic Settings

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

You can access this feature through **Basic > ReadySHARE**, or through **Advanced > USB Storage > ReadySHARE**. The USB Storage (Basic Settings) screen displays:



USB Storage (Basic Settings)

● Basic
○ ReadySHARE Printer

Network/Device Name \\readyshare

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space

By default, the USB storage device is available to all computers on your local area network (LAN).

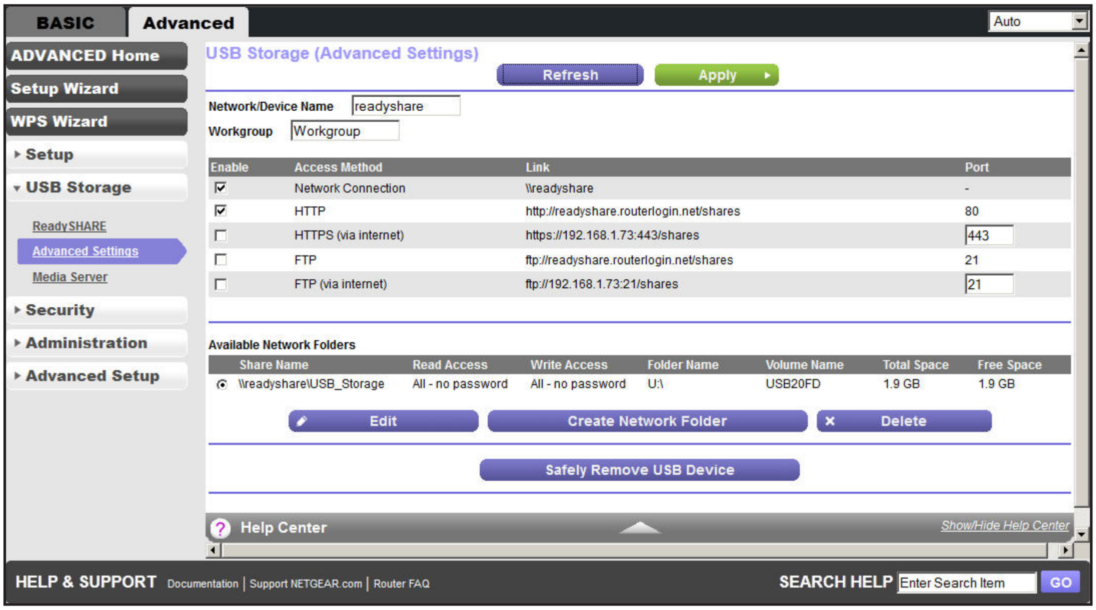
➢ **To access your USB device:**

1. Click the network device name or the share name in your computer’s network folders list.
2. For SMB://readyshare, click **Connect**.

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

Add or Edit a Network Folder

1. You can access this feature by selecting **Basic > ReadyShare > Edit**, or **Advanced > USB Storage > Advanced Settings**.



USB Storage (Advanced Settings)

Network/Device Name: readyshare

Workgroup: Workgroup

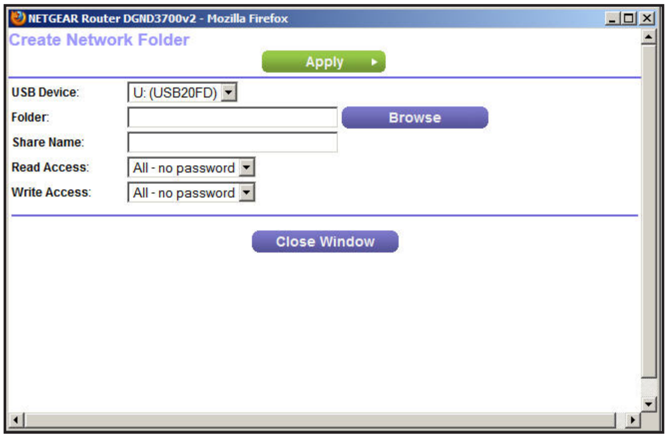
Enable	Access Method	Link	Port
☑	Network Connection	\\readyshare	-
☑	HTTP	http://readyshare.routerlogin.net/shares	80
□	HTTPS (via internet)	https://192.168.1.73:443/shares	443
□	FTP	ftp://readyshare.routerlogin.net/shares	21
□	FTP (via internet)	ftp://192.168.1.73:21/shares	21

Available Network Folders

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
●	\\readyshare\USB_Storage	All - no password	All - no password	U:\	USB20FD	1.9 GB	1.9 GB

2. Specify the changes that you want to make:

- To add a folder, click **Create Network Folder**.



USB Device:	U: (USB20FD)
Folder:	
Share Name:	
Read Access:	All - no password
Write Access:	All - no password

- To edit a folder, select its radio button, and then click **Edit**.

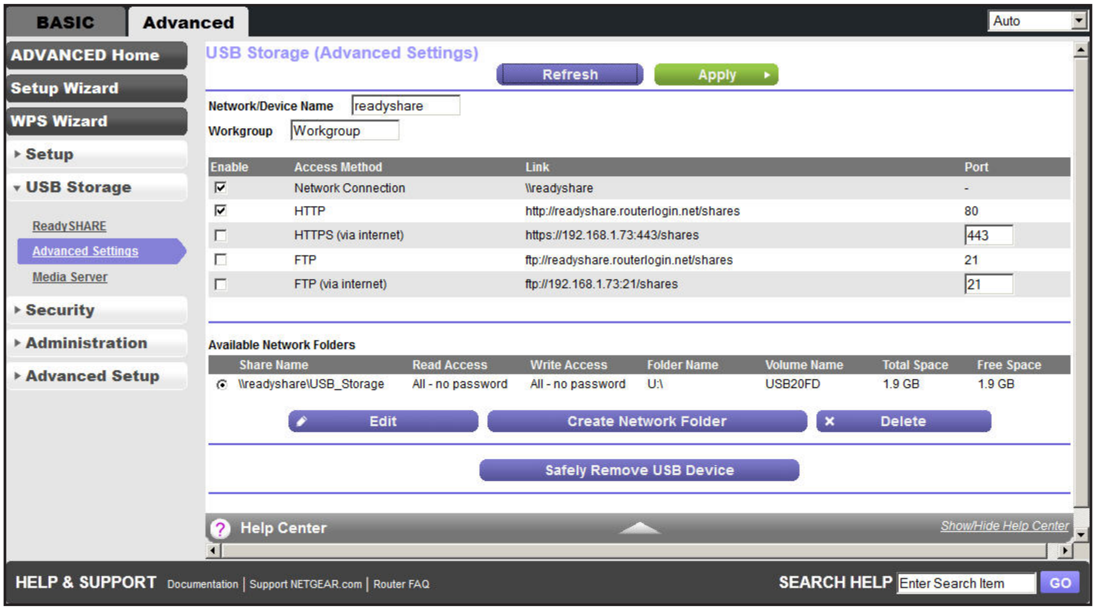
3. You can use this screen to select a folder, to change the share name, or to change the read access or write access from All - no password to **admin**.

   The user name (account name) for All - no password is guest. The password for admin is the same one that is used to log in to the wireless modem router. By default, it is password.

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

USB Storage Advanced Settings

You can set up the device name, workgroups, and network folders for your USB device. On the Advanced tab, select **USB Storage > Advanced Settings** to display the following screen:



Network/Device Name	readyshare
Workgroup	Workgroup

Enable	Access Method	Link	Port
☑	Network Connection	\\readyshare	-
☑	HTTP	http://readyshare.routerlogin.net/shares	80
□	HTTPS (via internet)	https://192.168.1.73:443/shares	443
□	FTP	ftp://readyshare.routerlogin.net/shares	21
□	FTP (via internet)	ftp://192.168.1.73:21/shares	21

Available Network Folders

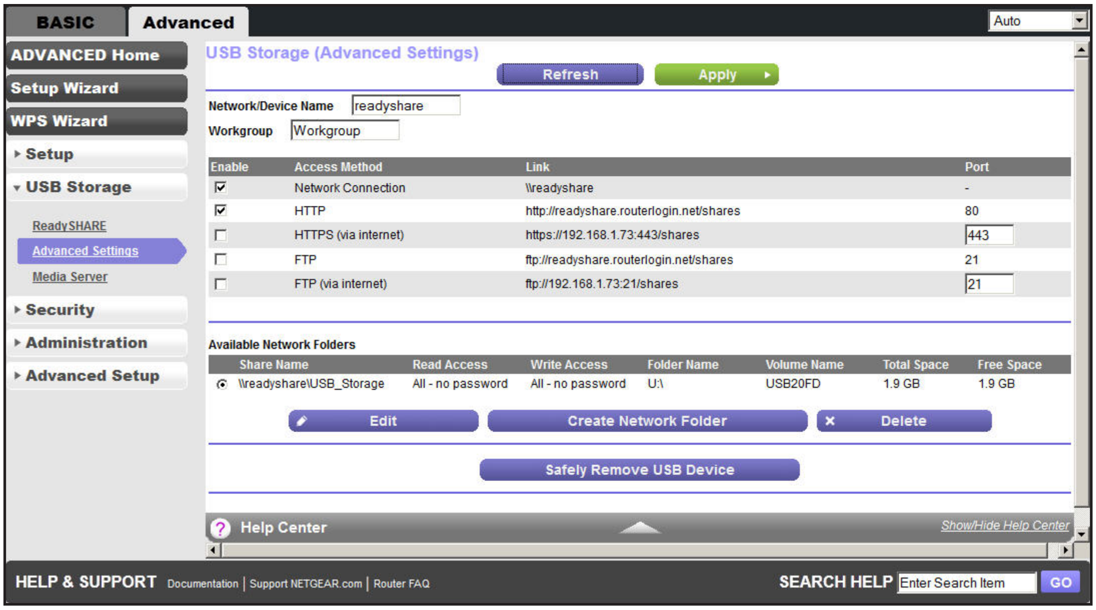
	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
●	\\readyshare\USB_Storage	All - no password	All - no password	U:\	USB20FD	1.9 GB	1.9 GB

You can use this screen to specify access to the USB storage device.

- **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the wireless modem router.
- **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.
- **Access Method**. The access methods are described here.
    - **Network Connection**. Enabled by default, this connection allows all users on the LAN to have access to the USB drive.
    - **HTTP**. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.
    - **HTTP (via internet)**. Disabled by default. If you enable this setting, remote users can type **http://<*public IP address*>/shares** (for example, **http://1.1.10.102/shares**) or a URL domain name to access the USB drive over the Internet. This setting supports file uploading only.
    - **FTP**. Disabled by default.
    - **FTP (via internet)**. Disabled by default. If you enable this setting, remote users can access the USB drive through FTP over the Internet. This setting supports both downloading and uploading of files.

Available Network Folders

You might need to scroll down to view this section of the screen:



USB Storage (Advanced Settings)

Network/Device Name: readyshare

Workgroup: Workgroup

Enable	Access Method	Link	Port
☑	Network Connection	\\readyshare	-
☑	HTTP	http://readyshare.routerlogin.net/shares	80
□	HTTPS (via internet)	https://192.168.1.73:443/shares	443
□	FTP	ftp://readyshare.routerlogin.net/shares	21
□	FTP (via internet)	ftp://192.168.1.73:21/shares	21

Available Network Folders

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
●	\\readyshare\USB_Storage	All - no password	All - no password	U:\	USB20FD	1.9 GB	1.9 GB

- **Share Name**. If only 1 device is connected, the default share name is USB_Storage. You can click the name shown, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.

- **Read and Write Access**. Show the permissions and access controls on the network folder: All - no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the wireless modem router.
- **Folder Name**. Full path used by the network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total and Free Space**. Show the current utilization of the storage device.

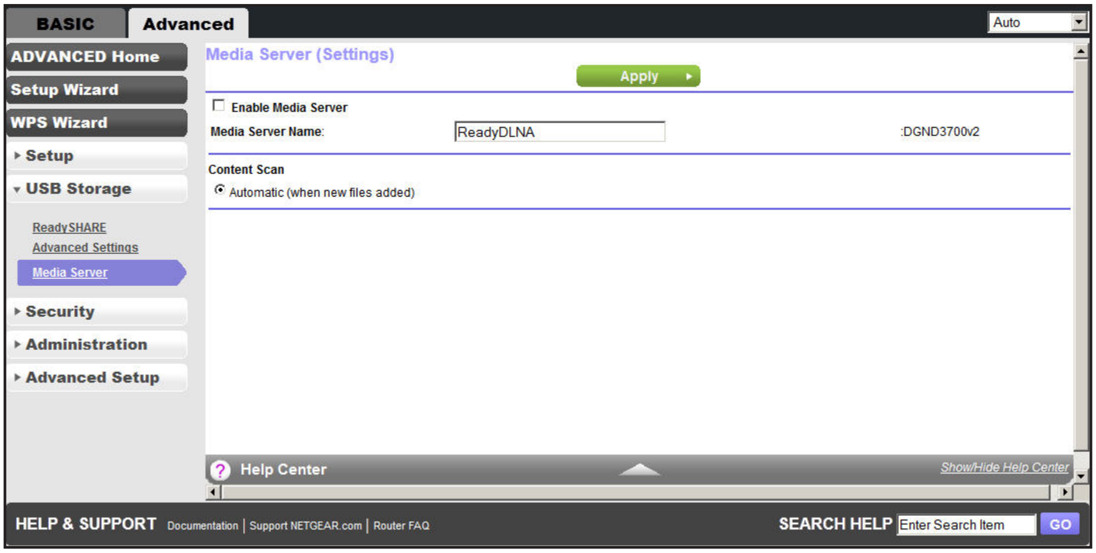
Safely Remove a USB Drive

To safely remove a USB disk drive so that no users can access it, select **USB Storage > Basic Settings**, and click the **Safely Remove USB Device** button. This takes the drive offline.

Media Server Settings

By default, the wireless modem router is set up to act as a Ready DLNA Media server, which lets you view movies and photos on DLNA/UPnP AV–compliant media players, such as Xbox360, Playstation, and NETGEAR’s Digital Entertainer Live.

To view these settings, select **Advanced > USB Storage > Media Server** to display the following screen:



Media Server (Settings)

□ Enable Media Server

Media Server Name: ReadyDLNA :DGND3700v2

Content Scan

● Automatic (when new files added)

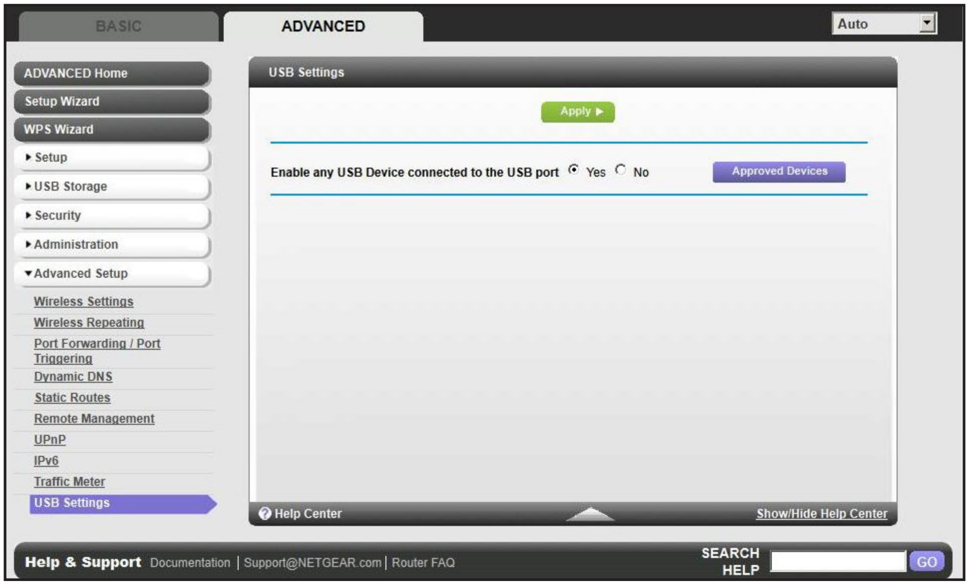
By default the Enable Media Server check box and the Automatic (when new files are added) radio button are selected. When these options are selected, the wireless modem router scans for media files whenever new files are added to the ReadySHARE USB hard drive.

Specify Approved USB Devices

For more security, you can set up the wireless modem router to share approved USB devices only. You can access this feature from the Advanced Setup menu on the Advanced tab.

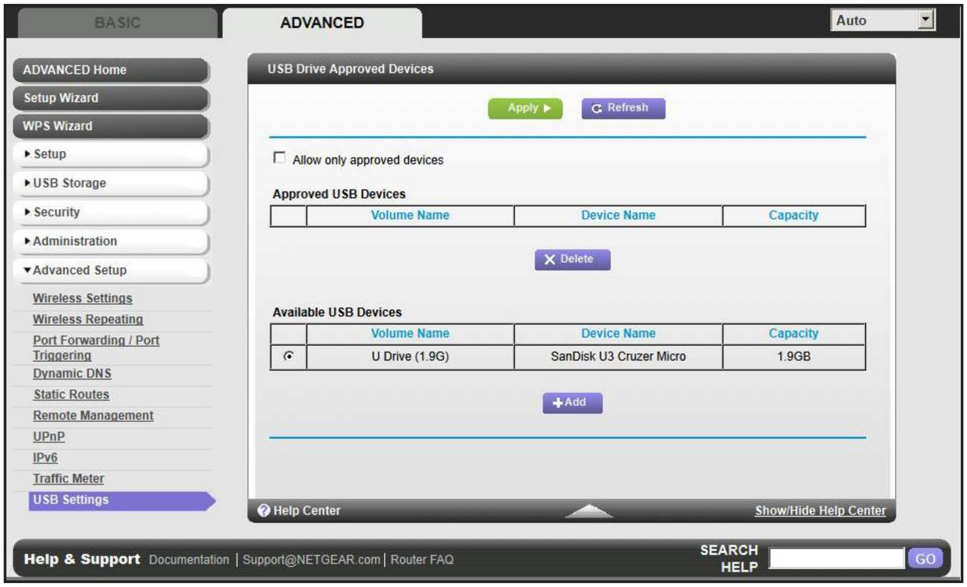
➢ **To set up approved USB devices:**

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



Enable any USB Device connected to the USB port ● Yes ○ No

2. **Click the Approved Devices** button. The USB Drive Approved Devices screen displays:



□ Allow only approved devices

Approved USB Devices

	Volume Name	Device Name	Capacity

Available USB Devices

	Volume Name	Device Name	Capacity
●	U Drive (1.9G)	SanDisk U3 Cruzer Micro	1.9GB

This screen shows the approved USB devices and the available USB devices. You can remove or add approved USB devices.

3. To add an approved USB device, select it from the Available USB Devices list, and then click **Add**.
4. Select the **Allow only approved devices** check box.
5. Click **Apply** so that your change takes effect.

If you want to work with another USB device, you have to first click the **Safely Remove USB Device** button for the currently connected USB device. Connect the other USB device, and repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers with a web browser, you have to use the wireless modem router's Internet port IP address. If you are using Dynamic DNS, you can type the DNS name, rather than the IP address. You can view the wireless modem router's Internet IP address from the dashboard on the Basic Home screen or the Advanced Home screen.

Access the Wireless Modem Router's USB Drive Remotely Using FTP

➢ **To connect to the wireless modem router's USB drive using a web browser:**

1. Connect to the wireless modem router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Netscape Navigator, for example:

   ftp://10.1.65.4

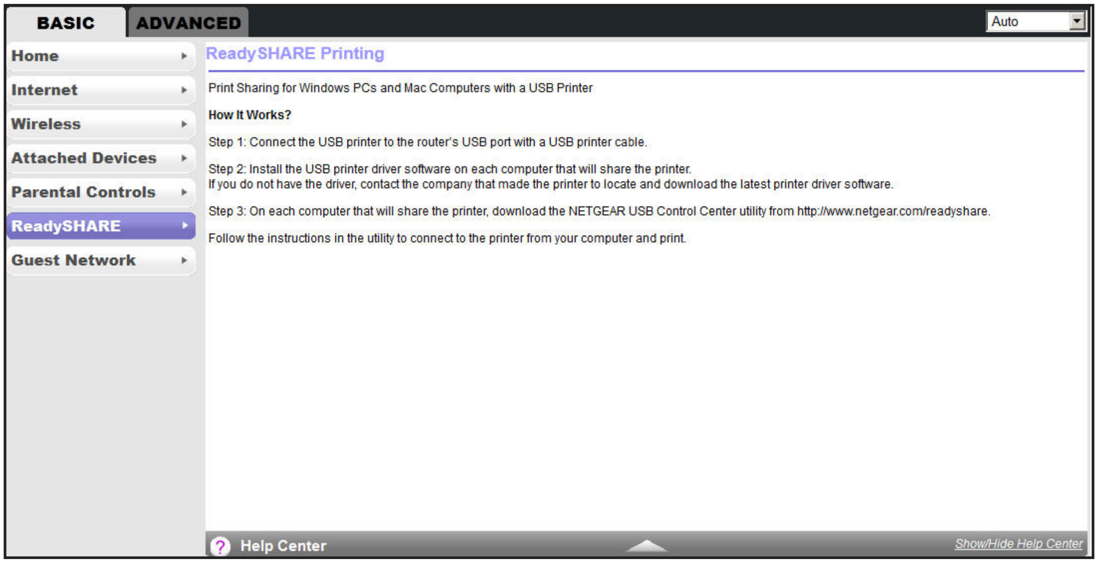
   If you are using Dynamic DNS, you can type the DNS name, rather than the IP address.
2. Type the account name and password for the account that has access rights to the USB drive. The user name (account name) for All - no password is **guest**.
3. The directories of the USB drive that your account has access to are displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

USB Printer Control

6

Access and configure a USB printer

This chapter describes how to access and configure a USB printer attached to your wireless modem router.



ReadySHARE Printing

Print Sharing for Windows PCs and Mac Computers with a USB Printer

How It Works?

Step 1: Connect the USB printer to the router's USB port with a USB printer cable.

Step 2: Install the USB printer driver software on each computer that will share the printer.
If you do not have the driver, contact the company that made the printer to locate and download the latest printer driver software.

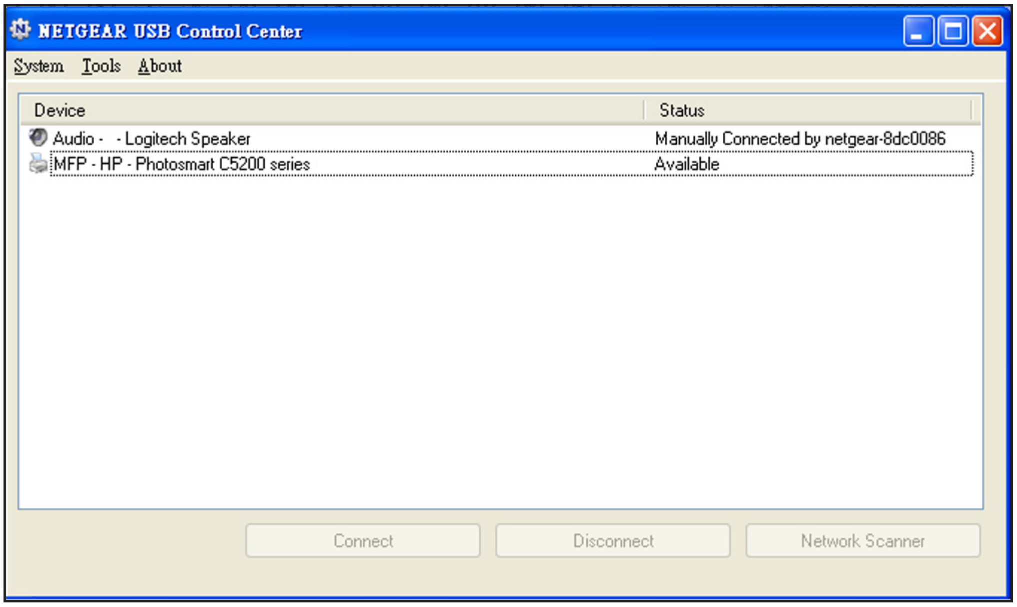
Step 3: On each computer that will share the printer, download the NETGEAR USB Control Center utility from http://www.netgear.com/readyshare.

Follow the instructions in the utility to connect to the printer from your computer and print.

The USB Control Center utility allows you to control a shared USB device from your computer that is connected to the USB port on your router. The utility allows you to control a printer.

The utility has to be installed on each computer on your network from which you want to control the device. You can download this utility at *www.netgear.com/landing/en-us/readyshare.aspx*.

When you launch the USB Control Center utility, a screen similar to the following displays:



Device	Status
Audio - - Logitech Speaker	Manually Connected by netgear-8dc0086
MFP - HP - Photosmart C5200 series	Available

This is the main screen, which shows a device icon, the description for this USB device, and its status.

- **Available**. The device is available from the computer that you are using.
- **Waiting to Connect**. You need to connect to this device from the computer that you are using. If this is the first time you are connecting, you might be prompted to install the device driver.

The following menu selections are available:

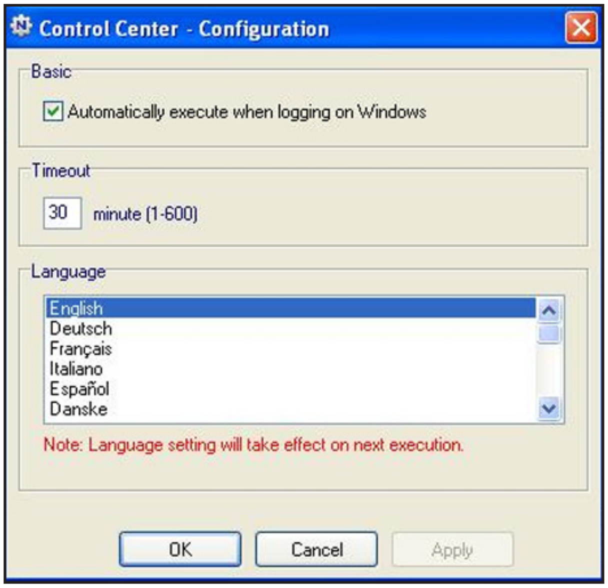
- **System**. Exit the utility.
- **Tools**. Access the Control Center Configuration to set up your shared USB device. See the following section, *Control Center Configuration*.
- **About**. View details about the USB Control Center software.

This chapter includes the following sections:

- *Control Center Configuration*
- *USB Printer*
- *Scan with a Multifunction Printer*
- *USB Speaker*

Control Center Configuration

Select **Tools > Configuration** to display the following screen:



Control Center - Configuration

Basic

☑ Automatically execute when logging on Windows

Timeout

30 minute (1-600)

Language

English
Deutsch
Français
Italiano
Español
Danske

Note: Language setting will take effect on next execution.

Automatically execute when logging on Windows. Select this check box to have the utility start automatically when you are logged in to Windows.

Timeout. Specify the time-out value for holding the USB resource when it is not in use.

Language. Select the display language for this utility.

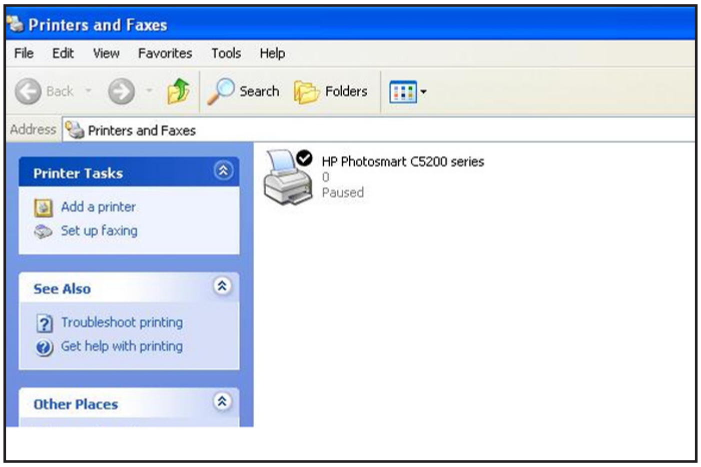
USB Printer

The first time you use a printer, you need to click **Connect**. You might be asked to install the driver for this printer. After the driver is installed, the printer status changes to Available.

Note: Some USB printers (for example: HP and Lexmark printer) request that you do not connect the USB cable until you are prompted by the installation software.

If the USB printer is detected and connected automatically, you need to disconnect the printer, and then wait for the prompt asking you to click **Connect**.

Once the printer shows Available status, the grayed out Paused state no longer displays in the Windows Printers and Faxes window.



This USB printer is ready. The utility does not need to always hold the connection of this USB printer. Once there is any print job for this printer, the USB utility connects to this USB printer automatically, then prints. After the print job is done, the printer status returns to the Paused state.

Scan with a Multifunction Printer

You can use the scan feature of a multifunction printer.

1. Make sure that the printer’s status shows as Available.
2. Click the **Network Scanner** button.

   This activates the scanner window that is used to perform the scans.

USB Speaker

➢ **To control a USB speaker:**

1. Select the USB speaker.
2. Click the **Connect** button to connect this speaker, or click **Disconnect** to disconnect the speaker.

   If you click Connect, and someone else is already connected to the speaker, a request is sent to that person. The person who receives the request can click an Accept or Reject button.

If someone is connected to the speaker and it is not being used (the router does not detect any activity), the router holds the connection for the amount of time that is in the timeout value, and then makes it available.

Security

7

Keep unwanted content out of your network

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

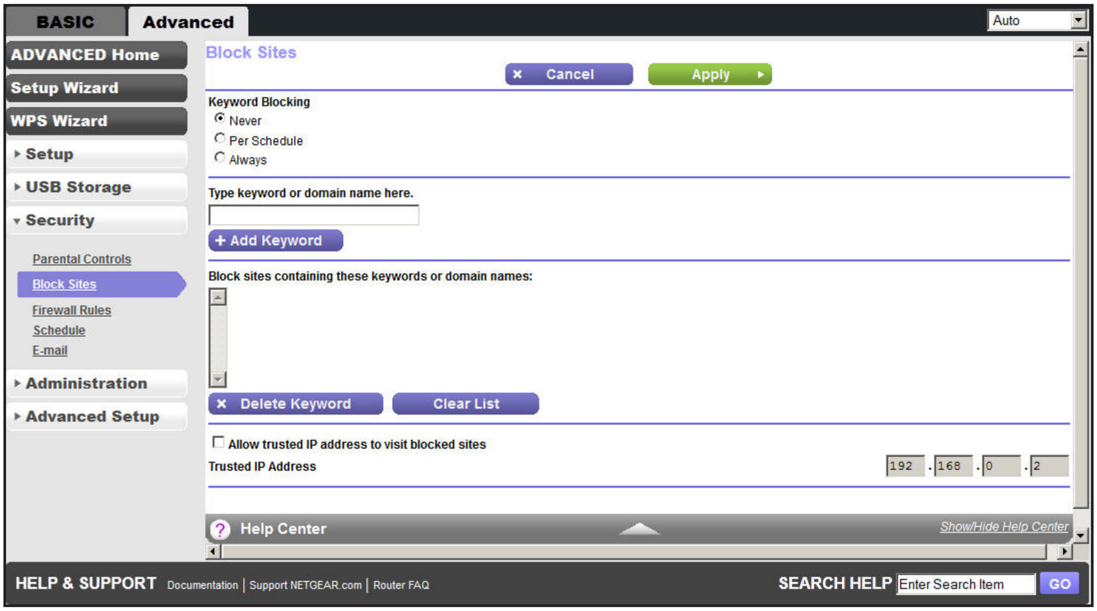
This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Firewall Rules*
- *Schedule for Firewall Rules*
- *Security Event Email Notifications*

Keyword Blocking of HTTP Traffic

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

1. Select **Advanced > Security > Block Sites** to display the following screen:



Block Sites

Keyword Blocking
● Never
○ Per Schedule
○ Always

Type keyword or domain name here.

Block sites containing these keywords or domain names:

□ Allow trusted IP address to visit blocked sites

Trusted IP Address 192 . 168 . 0 . 2

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

   The Keyword list supports up to 32 entries. Here are some sample entries:

   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

To delete a keyword or domain:

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword,** and then **Apply** to save your changes.

To specify a trusted computer:

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

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

Firewall Rules

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

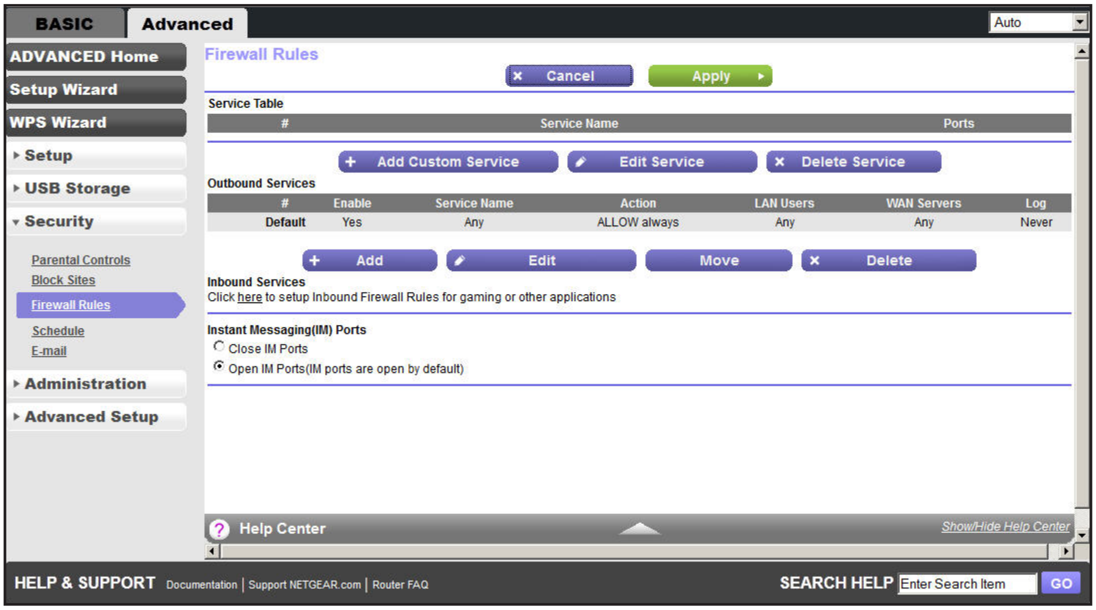
The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the wireless modem router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Firewall Rules screen lets you to block or allow specific Internet traffic services by computers on your network. This is called service blocking or port filtering.

Note: This feature is for Advanced Administrators only. Incorrect configuration can cause serious problems.

- **To create firewall rules:**

1. Select **Advanced > Security > Firewall Rules** to display the following screen:



Service Table

#	Service Name	Ports

Outbound Services

#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

Click here to setup Inbound Firewall Rules for gaming or other applications

Instant Messaging(IM) Ports

○ Close IM Ports

● Open IM Ports(IM ports are open by default)

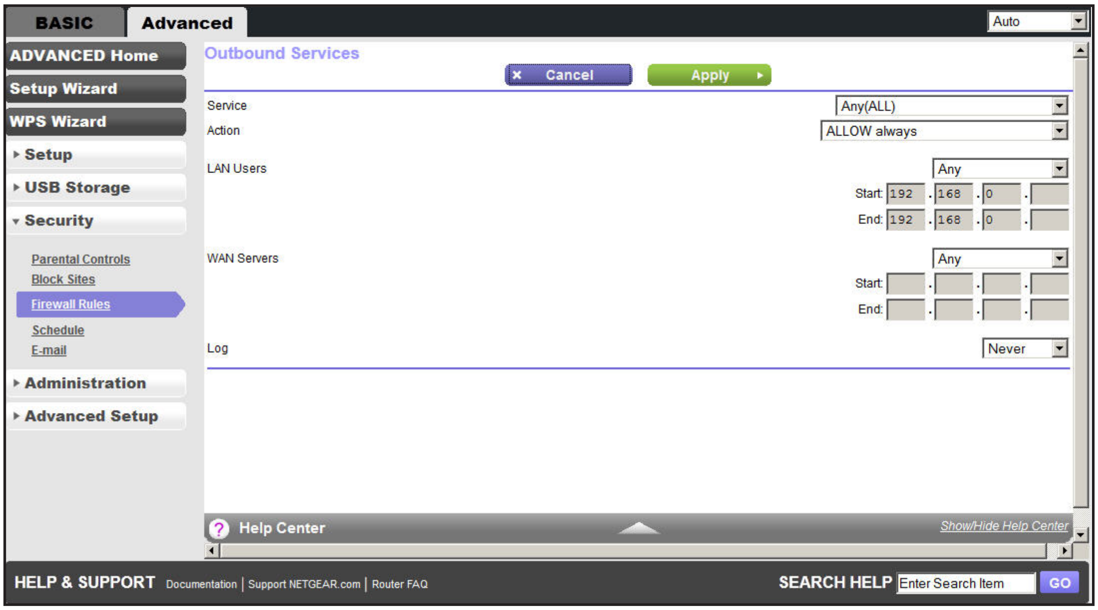
The Firewall Rules screen lists all firewall rules that have been changed from their default setting. The default rules allow all outgoing traffic and block all incoming traffic.

- To change the firewall rules for outbound traffic, you need to add it from the Outbound Services screen as described in *Step 2*.
- To change the firewall rules for inbound traffic, you need to add it from the Port Forwarding/Port Triggering screen as described in *Port Forwarding and Triggering* on page 105.

The Outbound Services and Port Forwarding/Inbound Services screens list the available services you can allow or block. You can also define your own custom services to allow or block with the Add Service screen as described in *Add Custom Services to Allow or Block* on page 80. Once you add your own custom services, they are available on the Outbound Services and Port Forwarding/Inbound Services screens.

You can also specify whether these services are always allowed or blocked, or allowed or blocked per schedule as described in *Schedule for Firewall Rules* on page 81.

2. **Outbound Services**. To allow or block an outbound service, click **Add** to display the following screen:



Outbound Services

Service: Any(ALL)

Action: ALLOW always

LAN Users: Any
Start: 192 . 168 . 0 .
End: 192 . 168 . 0 .

WAN Servers: Any
Start: . . .
End: . . .

Log: Never

Use the Outbound Services screen to define a new Outbound Firewall rule, or edit an existing rule. The outbound firewall rules are used to block or allow access by computers on your network to services or applications on the Internet.

a. **Service**. Select the service or application to be covered by this rule. If the service or application you want does not appear in the list, you have to define it as described in *Add Custom Services to Allow or Block* on page 80.

b. **Action**. Select the action you want for traffic covered by this rule:

   - **BLOCK always**. Always block the traffic covered by this rule.

- **BLOCK by schedule, otherwise Allow**. Allow the traffic covered by this rule, unless it is blocked according to the schedule specified on the Schedule screen in *Schedule for Firewall Rules* on page 81.
- **ALLOW always**. Always allow the traffic covered by this rule (this selection is the default setting).
- **ALLOW by schedule, otherwise Block**. Block the traffic covered by this rule, unless it is blocked accourding to the schedule specified on the Schedule screen in *Schedule for Firewall Rules* on page 81.

ALLOW rules are useful only when the traffic is already covered by a BLOCK rule. You would use these rules when you want to allow a subset of traffic that is currently blocked by another rule.

c. **LAN Users**. These settings determine which computers on your network are affected by this rule, based on their source (LAN) IP address. Select the option you want:

- **Any**. All local IP addresses are covered by this choice.
- **Address range**. You have to fill in the Start and Finish fields when this option is selected.
- **Single address**. Enter the required address in the Start field.

d. **WAN Servers**. These settings determine which Internet locations are covered by the rule, based on their destination (WAN) IP address. Select the option you want:

- **Any**. All Internet IP address are covered by this choice.
- **Address range**. You have to fill in the Start and Finish fields when this option is selected.
- **Single address**. Enter the required address in the Start field.

e. **Log**. This setting determines whether traffic covered by this rule is logged. Select the action you want:

- **Always**. This choice always logs traffic that is covered by this rule, whether it matches or not. (This feature is useful when you are debugging your rules.)
- **Never**. This choice never logs traffic covered by this rule, whether it matches or not.

f. Click **Apply** to have your changes take effect, or click **Cancel** to return to the previous screen.

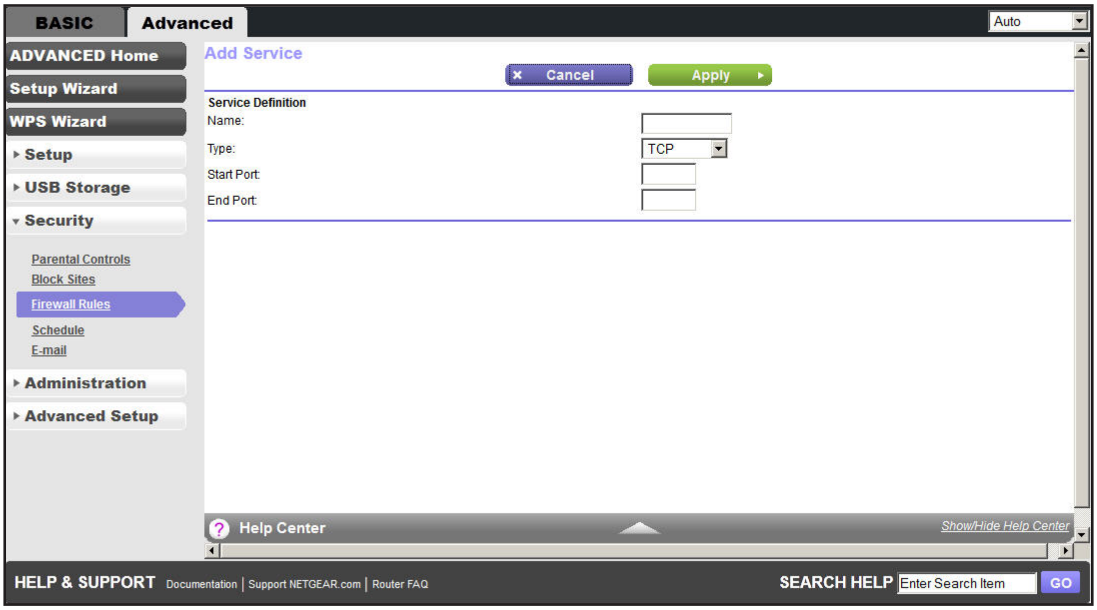
3. **Inbound Services**. To allow or block an inbound service, click **here** to set up inbound firewall rules for gaming or other applications. You are redirected to the Port Forwarding/Port Triggering screen as described in *Port Forwarding and Triggering* on page 105.
4. Click **Apply** to enable your Firewall Rules selections.

Add Custom Services to Allow or Block

You can define your own incoming and outgoing custom services to allow or block. Once you add your own custom services, they will be available on the Outbound Services screen (as described in *Firewall Rules* on page 77) and the Port Forwarding/Inbound Services screen (as described in *Port Forwarding and Triggering* on page 105).

➢ **To add a custom service:**

1. Click **Add Custom Service** to add a service. The Add Service screen displays:



Service Definition
Name:
Type: TCP
Start Port:
End Port:

The Add Service screen allows you to specify or edit your own custom service definition. You can then use the custom service when creating firewall rules.

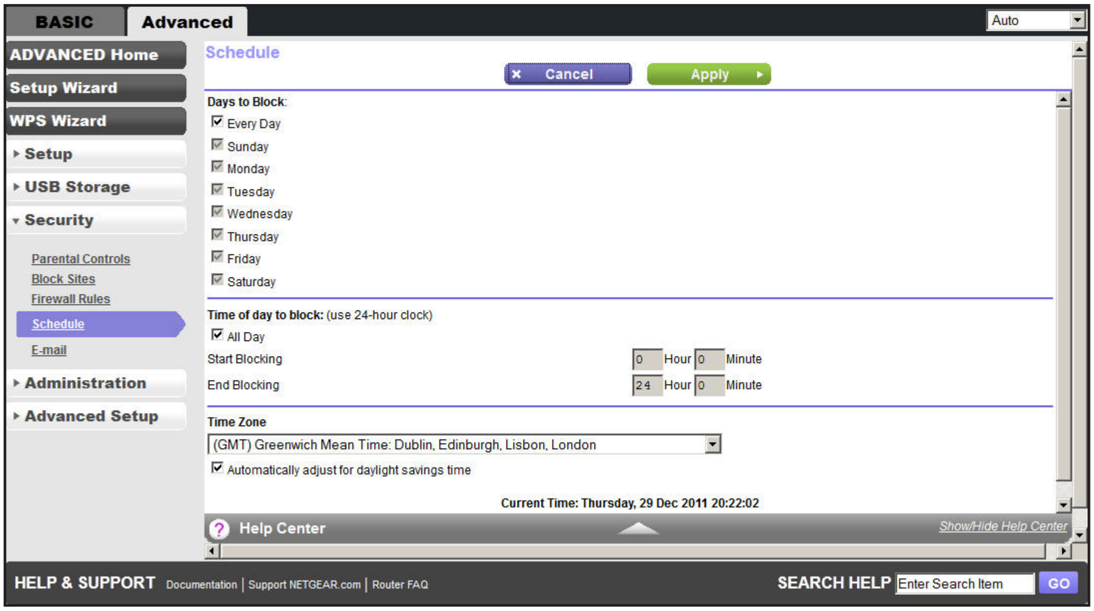
2. To add a service for blocking, first determine which port number or range of numbers is used by the application.
3. **Name**. In the Name field, enter a suitable name for this service.
4. **Type**. Select the correct type for this service (if in doubt, select TCP/UDP):
   - TCP
   - UDP
   - TCP/UDP
5. **Start Port** and **End Port**. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
6. Click **Apply** to save your information and return to the previous screen.

Schedule for Firewall Rules

You can specify the days and time that you want to block Internet access.

➢ To specify the firewall rule schedule:

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



Schedule

Days to Block:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day to block: (use 24-hour clock)

☑ All Day

Start Blocking 0 Hour 0 Minute

End Blocking 24 Hour 0 Minute

Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

☑ Automatically adjust for daylight savings time

Current Time: Thursday, 29 Dec 2011 20:22:02

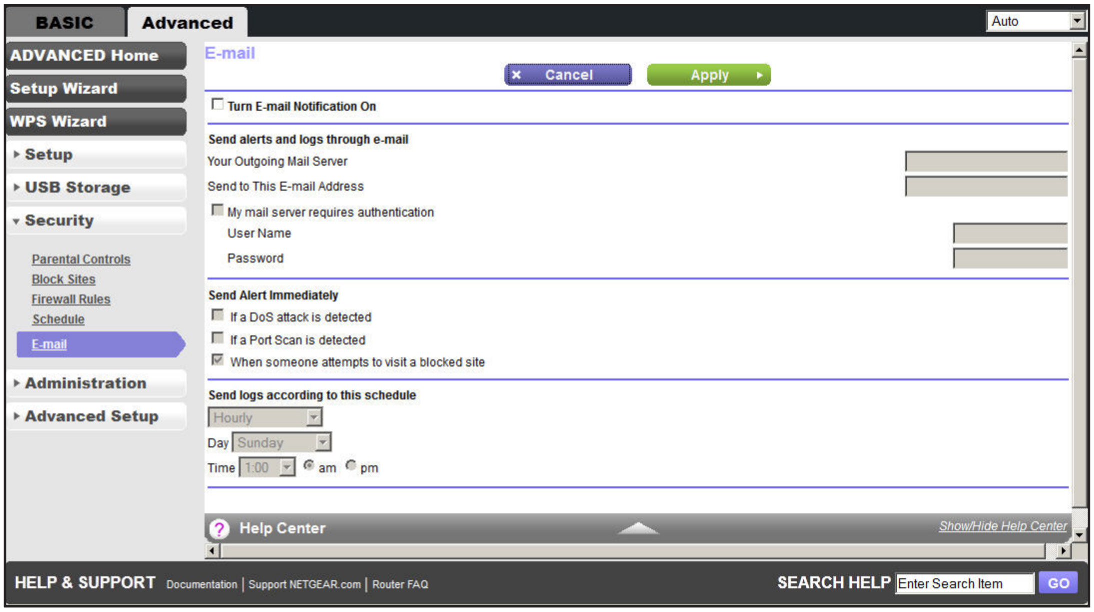
2. Set up the schedule for blocking keywords and services.
   - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour format, or select **All Day** for 24-hour blocking.
3. Select your time zone from the list. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply** to save your settings.

Security Event Email Notifications

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

➢ **To set up email notifications:**

1. Select **Advanced > Security > E-mail** to display the following screen:



E-mail

□ Turn E-mail Notification On

Send alerts and logs through e-mail

Your Outgoing Mail Server

Send to This E-mail Address

□ My mail server requires authentication

User Name

Password

Send Alert Immediately

□ If a DoS attack is detected

□ If a Port Scan is detected

☑ When someone attempts to visit a blocked site

Send logs according to this schedule

Hourly

Day Sunday

Time 1:00 ● am ○ pm

2. To receive email logs and alerts from the wireless modem router, select the **Turn E-mail Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent by email.
4. In the Send to This Email Address field, enter the email address to which logs and alerts are sent. This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent by email.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. You can have email alerts sent immediately when someone attempts to visit a blocked site, and you can specify that logs are sent automatically.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, the log is cleared from the wireless modem router's memory. If the wireless modem router cannot email the log file, the log buffer might fill up. In this case, the wireless modem router overwrites the log and discards its contents.
7. Click **Apply** to save your settings.

8 Administration

Manage your network

This chapter describes the settings for administering and maintaining your wireless modem router and home network. See also *Remote Management* on page 118 for information about upgrading or checking the status of your wireless modem router over the Internet, and *Traffic Meter* on page 121 for information about monitoring the volume of Internet traffic passing through your wireless modem router's Internet port.

This chapter includes the following sections:

- *Upgrade the Wireless Modem Router Firmware*
- *View Wireless Modem Router Status*
- *View VPN Status*
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Set Password*
- *Diagnostics*

Upgrade the Wireless Modem Router Firmware

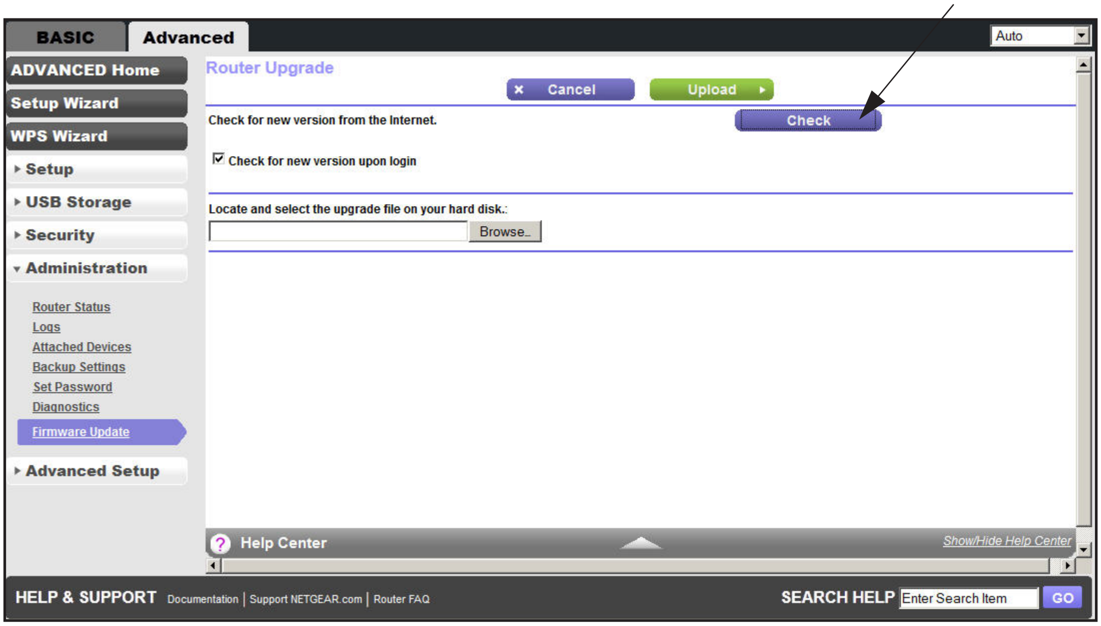
The wireless modem router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the Advanced tab. You might see a message at the top of the Genie screens when new firmware is available for your product.

You can use the Check button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

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

1. Select **Advanced > Administration > Firmware Update** to display the following screen:

Click Check.



Router Upgrade

Check for new version from the Internet.

☑ Check for new version upon login

Locate and select the upgrade file on your hard disk.:

2. Click **Check**.

   The wireless modem router finds new firmware information if any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).

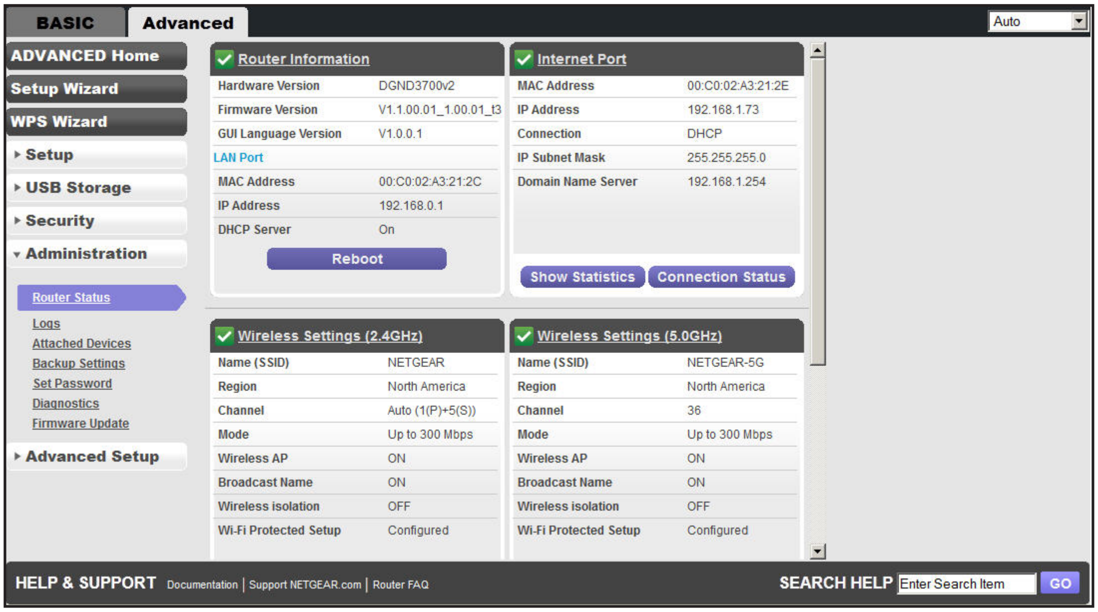
WARNING:

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

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

View Wireless Modem Router Status

To view wireless modem router status and usage information, select **Advanced Home**, or select **Administration > Router Status** to display the following screen:



Router Information

Hardware Version	DGND3700v2
Firmware Version	V1.1.00.01_1.00.01_t3
GUI Language Version	V1.0.0.1
LAN Port	
MAC Address	00:C0:02:A3:21:2C
IP Address	192.168.0.1
DHCP Server	On

Internet Port

MAC Address	00:C0:02:A3:21:2E
IP Address	192.168.1.73
Connection	DHCP
IP Subnet Mask	255.255.255.0
Domain Name Server	192.168.1.254

Wireless Settings (2.4GHz)

Name (SSID)	NETGEAR
Region	North America
Channel	Auto (1(P)+5(S))
Mode	Up to 300 Mbps
Wireless AP	ON
Broadcast Name	ON
Wireless isolation	OFF
Wi-Fi Protected Setup	Configured

Wireless Settings (5.0GHz)

Name (SSID)	NETGEAR-5G
Region	North America
Channel	36
Mode	Up to 300 Mbps
Wireless AP	ON
Broadcast Name	ON
Wireless isolation	OFF
Wi-Fi Protected Setup	Configured

Wireless Modem Router Information

Hardware Version. The wireless modem router model.

Firmware Version. The version of the wireless modem router firmware. It changes if you upgrade the wireless modem router firmware.

GUI Language Version. The localized language of the user interface.

LAN Port.

- **MAC Address**. The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the wireless modem router.
- **IP Address**. The IP address being used by the Ethernet (LAN) port of the wireless modem router. The default is 192.168.1.1.
- **DHCP Server**. Identifies whether the wireless modem router's built-in DHCP server is active for the LAN-attached devices.

Internet Provider (WAN) Setup

MAC Address. The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the wireless modem router.

IP Address. The IP address being used by the Internet (WAN) port of the wireless modem router. If no address is shown or the address is 0.0.0, the wireless modem router cannot connect to the Internet.

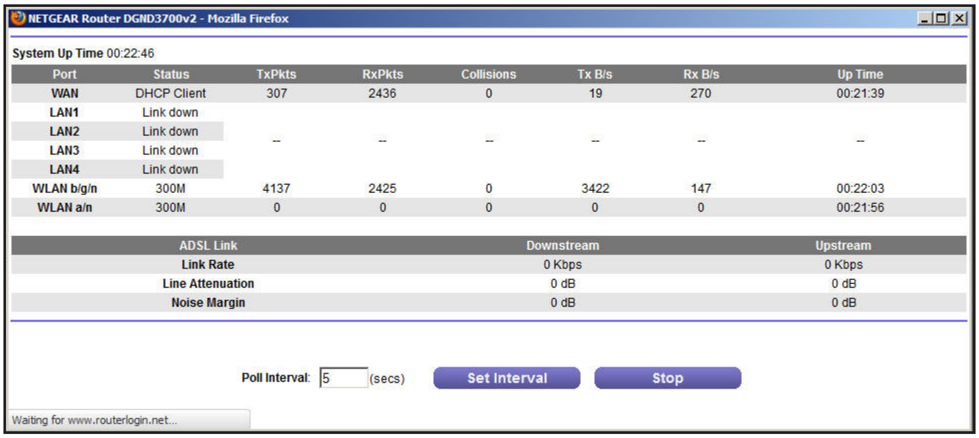
Connection. This shows if the wireless modem router is using a fixed IP address on the WAN. If the value is DHCP Client, the wireless modem router obtains an IP address dynamically from the ISP.

IP Subnet Mask. The IP subnet mask being used by the Internet (WAN) port of the wireless modem router.

Domain Name Server. The Domain Name Server addresses being used by the wireless modem router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Statistics Button

On the Router Status screen, in the Internet Port pane, click the **Show Statistics** button to display the following screen:



NETGEAR Router DGND3700v2 - Mozilla Firefox

System Up Time 00:22:46

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	DHCP Client	307	2436	0	19	270	00:21:39
LAN1	Link down	--	--	--	--	--	--
LAN2	Link down						
LAN3	Link down						
LAN4	Link down						
WLAN b/g/n	300M	4137	2425	0	3422	147	00:22:03
WLAN a/n	300M	0	0	0	0	0	00:21:56

ADSL Link	Downstream	Upstream
Link Rate	0 Kbps	0 Kbps
Line Attenuation	0 dB	0 dB
Noise Margin	0 dB	0 dB

Poll Interval: 5 (secs)

Set Interval
Stop
Waiting for www.routerlogin.net...

Figure 9. System up time and poll interval statistics

System Up Time. The time elapsed since the wireless modem router was last restarted.

Port. The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:

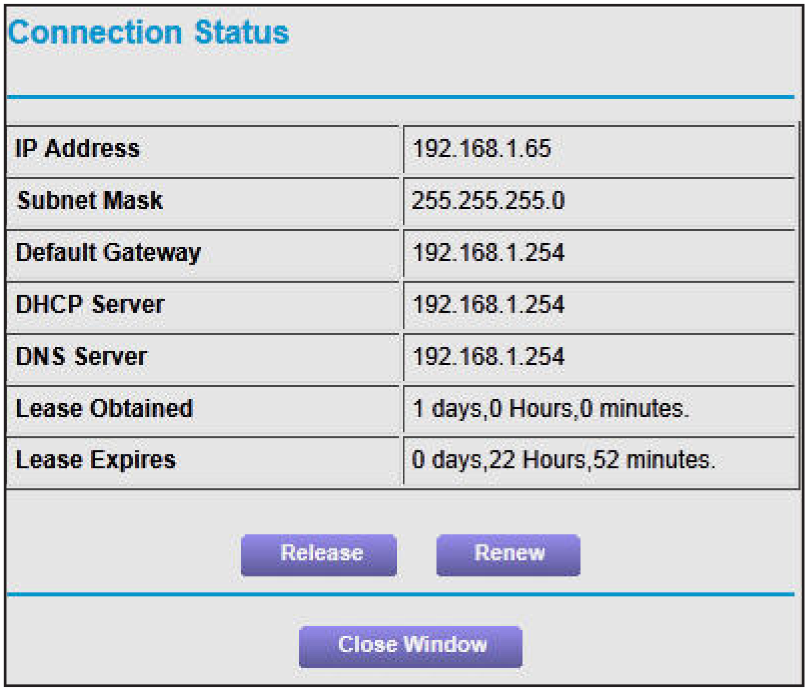
- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted on this port since reset or manual clear.
- **RxPkts**. The number of packets received on this port since reset or manual clear.
- **Collisions**. The number of collisions on this port since reset or manual clear.
- **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.

To change the polling frequency, enter a time in seconds in the Poll Interval field, and click **Set Interval**.

To stop the polling entirely, click **Stop**.

Connection Status Button

On the Router Status screen in the Internet Port pane, click the **Connection Status** button to view connection status information.



Connection Status

IP Address	192.168.1.65
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DHCP Server	192.168.1.254
DNS Server	192.168.1.254
Lease Obtained	1 days,0 Hours,0 minutes.
Lease Expires	0 days,22 Hours,52 minutes.

Figure 10. View connection status information

The Release button returns the status of all items to 0. The Renew button refreshes the items. The Close Window button closes the Connection Status screen.

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

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

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

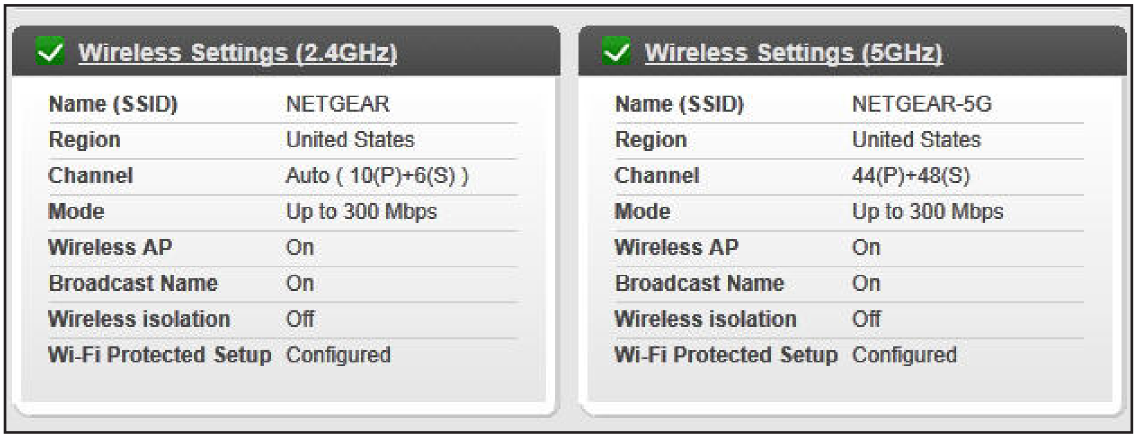
DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the wireless modem router.

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.

Wireless Settings (2.4 GHz and 5 GHz)



✓ Wireless Settings (2.4GHz)

Name (SSID)	NETGEAR
Region	United States
Channel	Auto (10(P)+6(S))
Mode	Up to 300 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

✓ Wireless Settings (5GHz)

Name (SSID)	NETGEAR-5G
Region	United States
Channel	44(P)+48(S)
Mode	Up to 300 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

The following settings are displayed:

Name (SSID). The wireless network name (SSID) used by the wireless modem router. The default names for the 5 GHz ends in -5G to distinguish it from the 2.4 GHz network.

Region. The geographic region where the wireless modem router is being used. It might be illegal to use the wireless features of the wireless modem router in some parts of the world.

Channel. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the wireless modem router will find the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 will not interfere with each other.

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 130 Mbps (default), and Up to 300 Mbps.

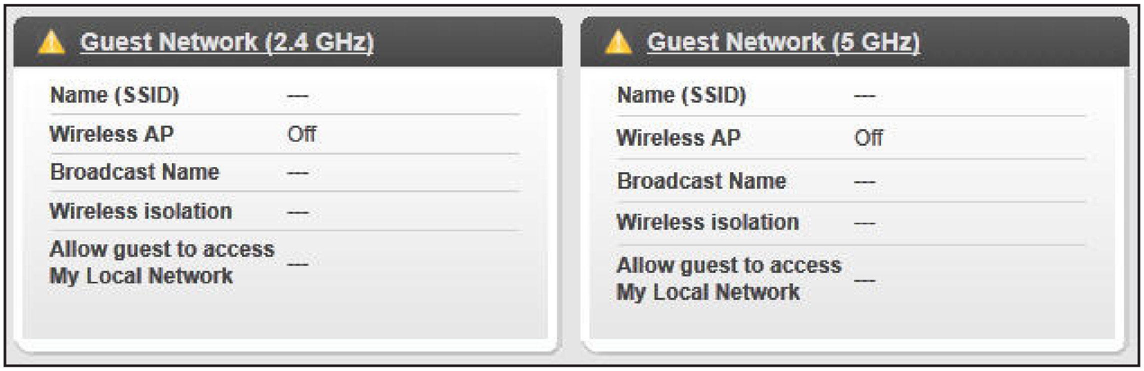
Wireless AP. Indicates whether the radio feature of the wireless modem router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the wireless modem router is broadcasting its SSID.

Wireless Isolation. Indicates whether wireless connections to the wireless modem router are prevented.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

Guest Network (2.4 GHz and 5 GHz)



⚠ Guest Network (2.4 GHz)

Name (SSID)	—
Wireless AP	Off
Broadcast Name	—
Wireless isolation	—
Allow guest to access My Local Network	—

⚠ Guest Network (5 GHz)

Name (SSID)	—
Wireless AP	Off
Broadcast Name	—
Wireless isolation	—
Allow guest to access My Local Network	—

Name (SSID). The 11N wireless network name (SSID) used by the wireless modem router. The default names are NETGEAR-Guest and NETGEAR-5G-Guest.

Wireless AP. Indicates whether the radio feature of the wireless modem router is enabled. If this feature is not enabled, the Wireless LEDs on the front panel are off.

Broadcast Name. Indicates whether the wireless modem router is broadcasting its SSID.

Wireless Isolation. Indicates whether wireless connections to the wireless modem router are prevented.

Allow guest to access My Local Network. Indicates whether any user who connects to this SSID can access local networks associated with the wireless modem router.

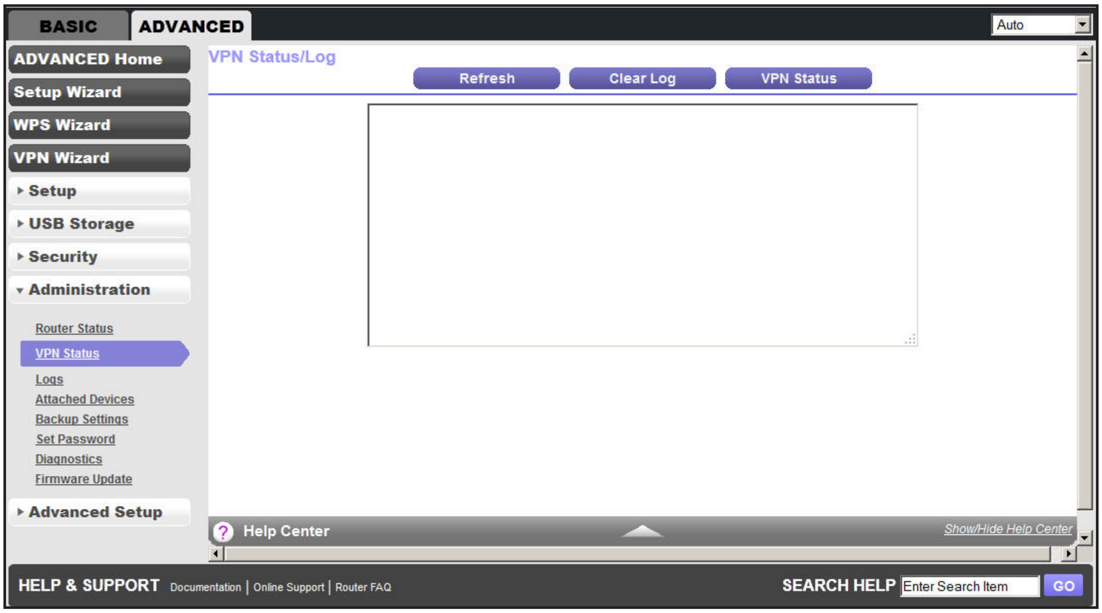
View VPN Status

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

➢ **To view the details of recent VPN activity log:**

1. Select **ADVANCED > Administration > VPN Status**

   The VPN Status/Log screen shows the details of recent VPN activity.

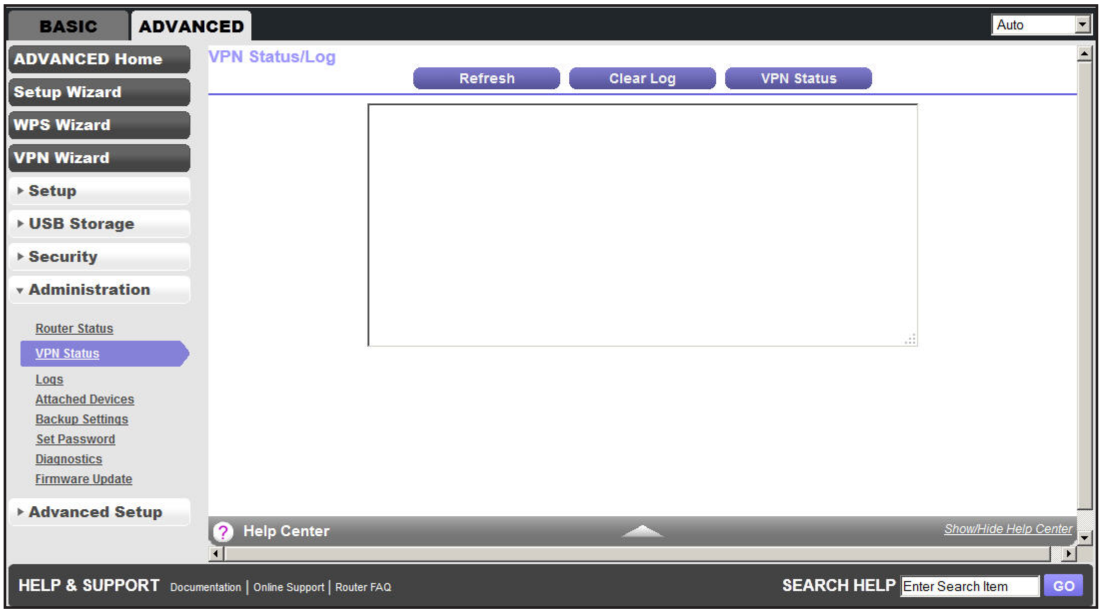


2. (Optional) Click the **Refresh** button to refresh the log screen.

➢ **To clear the VPN activity log:**

1. Select **ADVANCED > Administration > VPN Status**.

The VPN Status/Log screen shows the details of recent VPN activity.



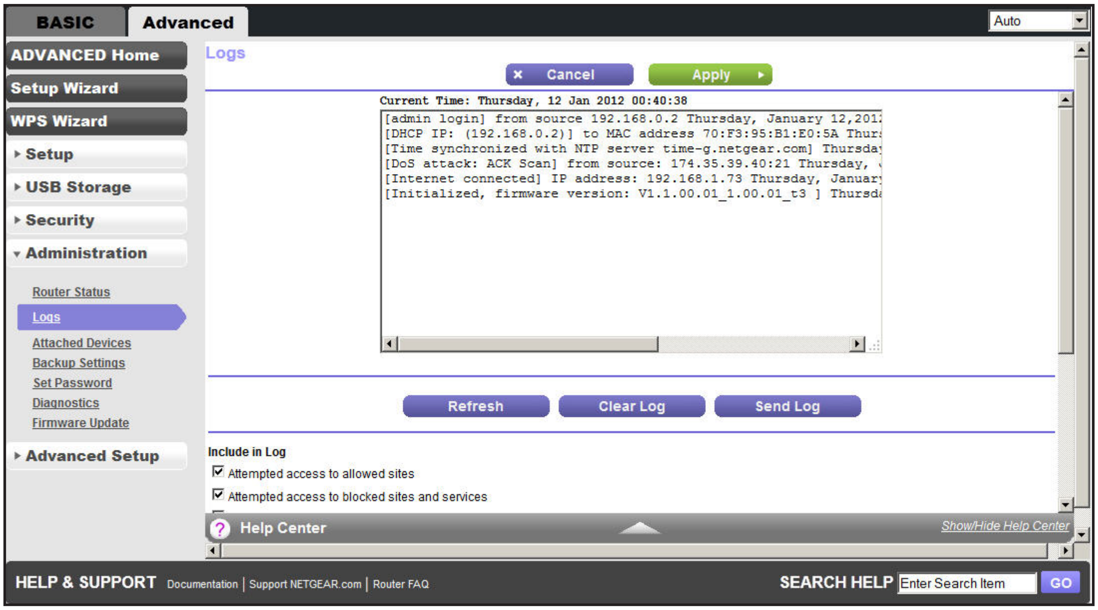
2. Click the **Clear Log** button.

   The log entries are cleared.

View Logs of Web Access or Attempted Web Access

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

Select **Advanced > Administration > Logs**. The Logs screen displays.



```
Current Time: Thursday, 12 Jan 2012 00:40:38
[admin login] from source 192.168.0.2 Thursday, January 12,201
[DHCP IP: (192.168.0.2)] to MAC address 70:F3:95:B1:E0:5A Thur
[Time synchronized with NTP server time-g.netgear.com] Thursda
[DoS attack: ACK Scan] from source: 174.35.39.40:21 Thursday,
[Internet connected] IP address: 192.168.1.73 Thursday, Januar
[Initialized, firmware version: V1.1.00.01_1.00.01_t3 ] Thursd
```

Include in Log

☑ Attempted access to allowed sites

☑ Attempted access to blocked sites and services

The Logs 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**. Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To email the log immediately, click the **Send Log** button.

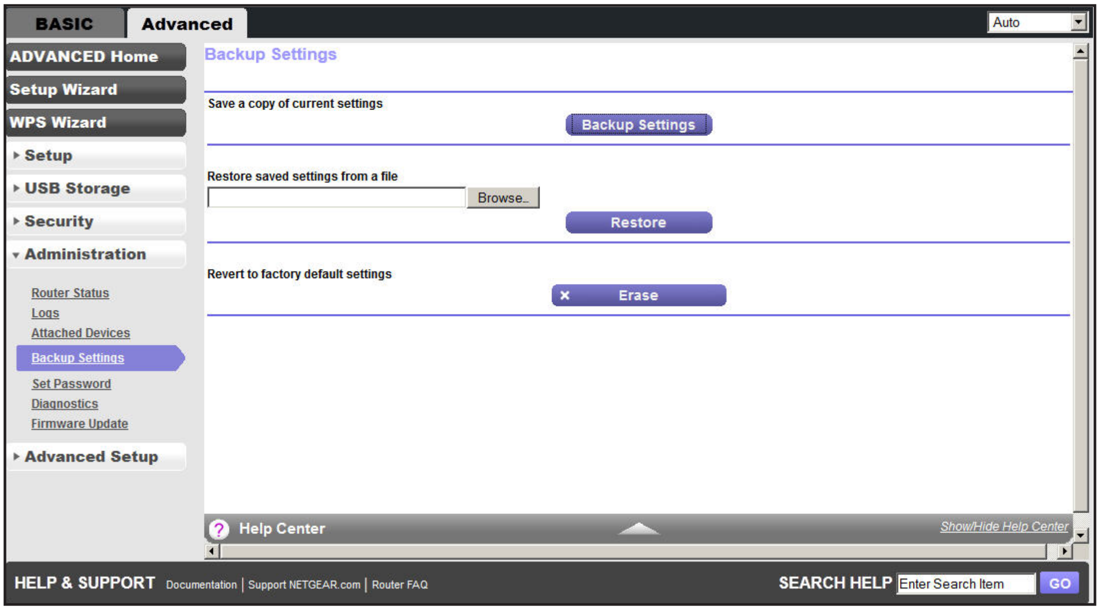
Manage the Configuration File

The configuration settings of the N600 Modem Router are stored within the wireless modem 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 wireless modem router's configuration settings:**

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



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

Restore Configuration Settings

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

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

Upon completion, the wireless modem router reboots.

WARNING:

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the wireless modem router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings.

Either you can use the Restore Factory Settings button on the back of the wireless modem router (see *Factory Settings* on page 142), or you can click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the wireless modem router's DHCP.

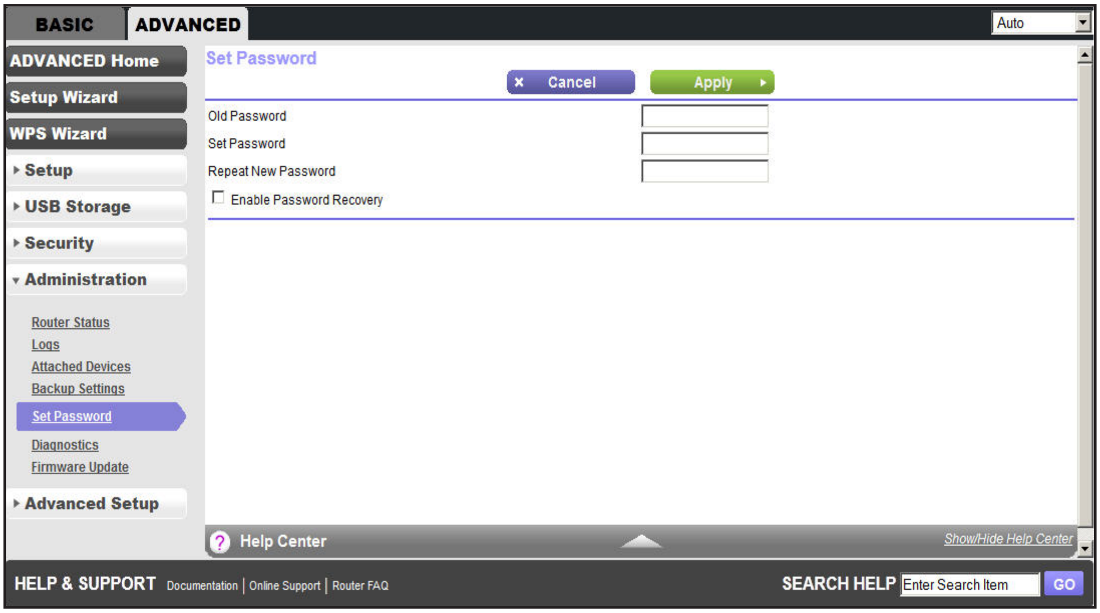
Set Password

This feature allows you to change the default password that is used to log in to the wireless modem router with the user name **admin**.

This is not the same as changing the password for wireless access. The label on the bottom of your wireless modem router shows your unique wireless network name (SSID) and password for wireless access (see *Label* on page 12).

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

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



Set Password

Old Password

Set Password

Repeat New Password

☐ Enable Password Recovery

2. Type the old password, and type the new password twice in the fields on this screen.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.
4. Click **Apply** so that your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router's user name of admin. Then you will have an easy way to 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. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.
3. Click **Apply** to save your changes.

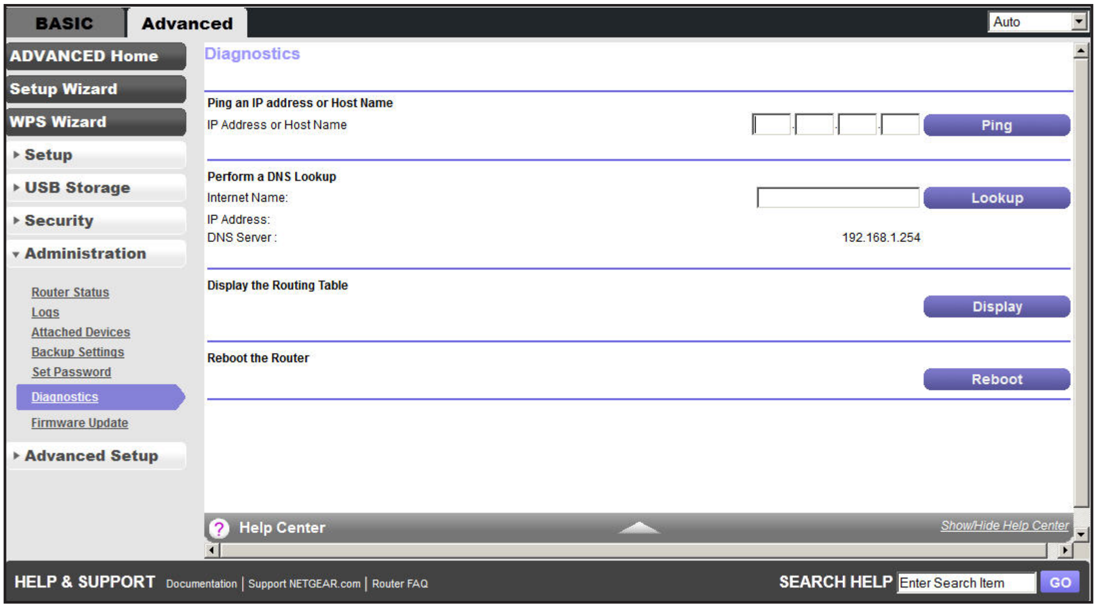
When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Diagnostics

You can perform various diagnostics. For normal operation, these tests are not required.

➢ **To perform diagnostic tests:**

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



Diagnostics

Ping an IP address or Host Name

IP Address or Host Name

Perform a DNS Lookup

Internet Name:

IP Address:

DNS Server : 192.168.1.254

Display the Routing Table

Reboot the Router

2. Perform the following diagnostics as needed:
   - **Ping an IP address or Host Name**. Use this test to send a ping packet request to the specified IP address or host name. This test is often used to test a connection. If the request times out (in other words, no reply is received), this result usually means the destination is unreachable. Note, however, that some network devices can be configured not to respond to a ping.
   - **Perform a DNS Lookup**. A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, do a DNS lookup to find the IP address.
   - **Display the Routing Table**. This operation displays the internal routing table.

- **Reboot the Router**. Click this button to perform a remote restart of the router. Use this operation if the router seems to have become unstable or is not operating normally.

Note: Rebooting will break any existing connections either to the router (such as this one) or through the router (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.

Advanced Settings

9

Fine tuning your network

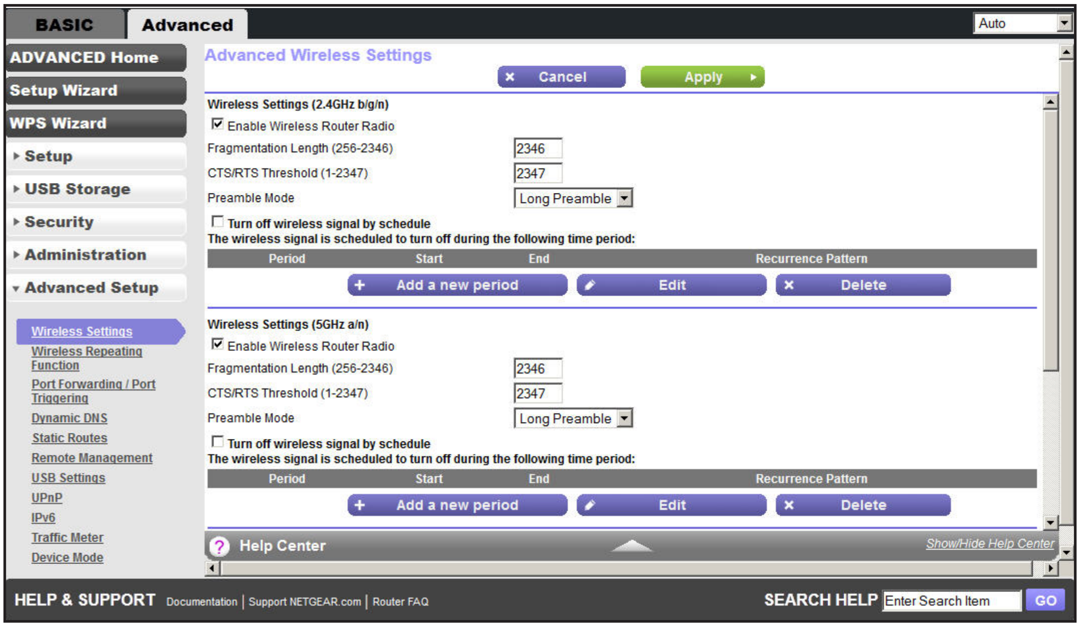
This chapter describes the advanced features of your wireless modem router. The information is for users with a solid understanding of networking concepts who want to set the wireless modem router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Repeating Function (WDS)*
- *Port Forwarding and Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *USB Settings*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*
- *Device Mode*
- *VPN Policies*

Advanced Wireless Settings

Select **Advanced > Advanced Setup > Wireless Settings** to display the Advanced Wireless Settings screen:



Advanced Wireless Settings

Wireless Settings (2.4GHz b/g/n)

☑ Enable Wireless Router Radio

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Long Preamble

□ Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period	Start	End	Recurrence Pattern

Wireless Settings (5GHz a/n)

☑ Enable Wireless Router Radio

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Long Preamble

□ Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period	Start	End	Recurrence Pattern

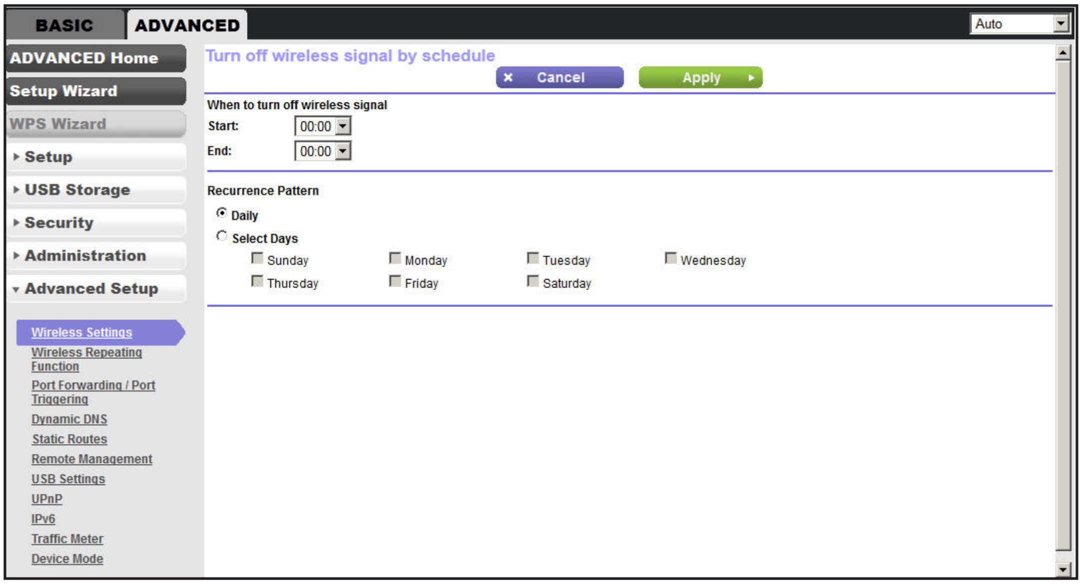
The following settings are available in this screen:

- **Enable Wireless Router Radio**. You can completely turn off the wireless portion of the wireless modem router by clearing this check box. Select this check box again to enable the wireless portion of the wireless modem router. When the wireless radio is disabled, other members of your household can use the wireless modem router by connecting their computers to the wireless modem router with an Ethernet cable.

> **Note:** The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

- **Turn off wireless signal by schedule**. From the Advanced Wireless Settings screen (with the Enable Wireless Router Radio check box selected for the radio band you want to configure), click the **Add a new period** button to display the Turn off wireless signal by schedule screen.

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



Turn off wireless signal by schedule

When to turn off wireless signal

Start: 00:00

End: 00:00

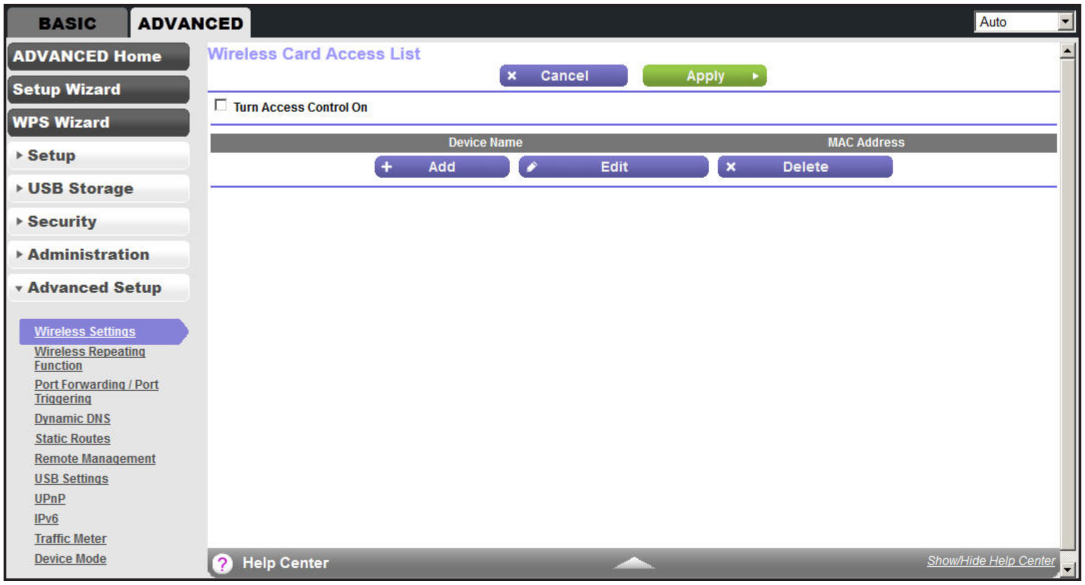
Recurrence Pattern

● Daily

○ Select Days

□ Sunday	□ Monday	□ Tuesday	□ Wednesday
□ Thursday	□ Friday	□ Saturday	

- **WPS Settings**.You can add WPS devices to your network.
- **AP Mode**. You can make the DGND3700v2 function as an access point.
- **Wireless Card Access List.** From the Advanced Wireless Settings screen, click the **Set Up Access List** button to display the Wireless Card Access List screen.

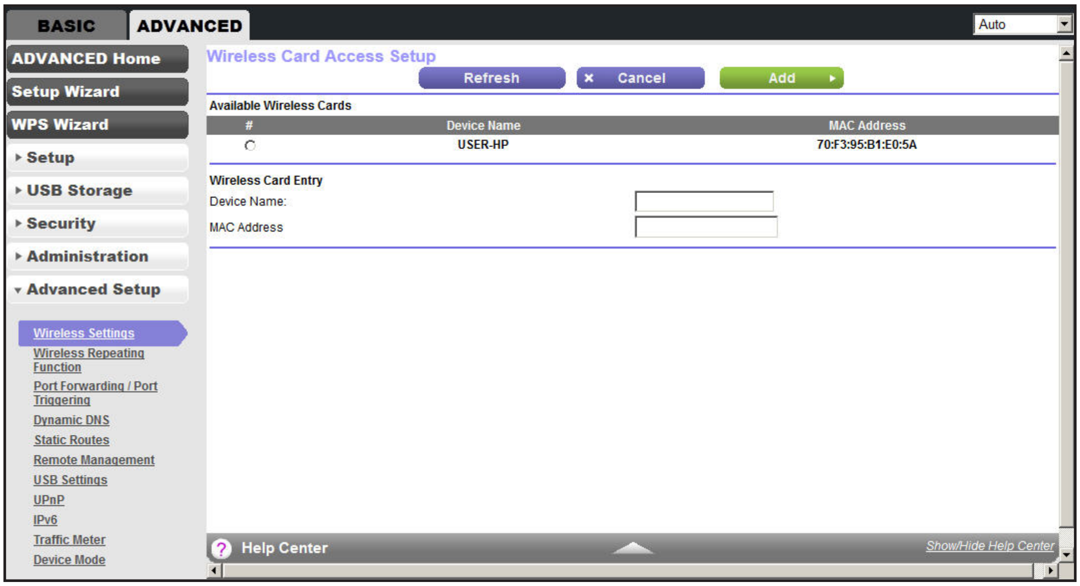


Wireless Card Access List

□ Turn Access Control On

Device Name	MAC Address

From the Wireless Card Access List screen, click **Add** to display the Wireless Card Access Setup screen. On this screen you can restrict access to your network to specific devices based on their MAC address.



Wireless Card Access Setup

Available Wireless Cards

#	Device Name	MAC Address
○	USER-HP	70:F3:95:B1:E0:5A

Wireless Card Entry

Device Name:

MAC Address

Wireless Repeating Function (WDS)

You can set the N600 Modem Router up to be used as a wireless access point (AP). Doing this enables the wireless modem router to act as a wireless repeater. A wireless repeater connects to another wireless wireless modem router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

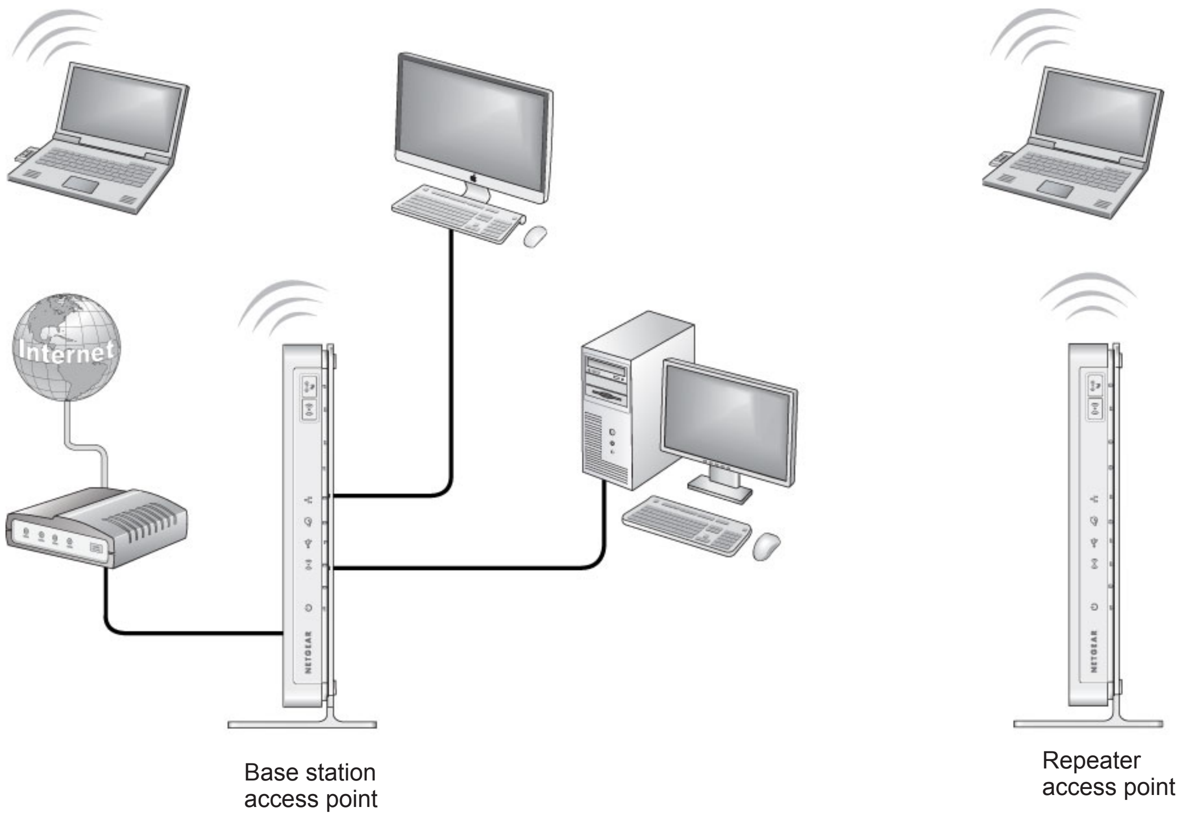


Figure 11. Wireless repeating scenario

Note: If you use the wireless repeating function, you need to select either **WEP** or **None** as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode **Up to 54 Mbps** in the Wireless Settings screen.

Wireless Base Station. The wireless modem router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point.

Wireless Repeater. The wireless modem router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

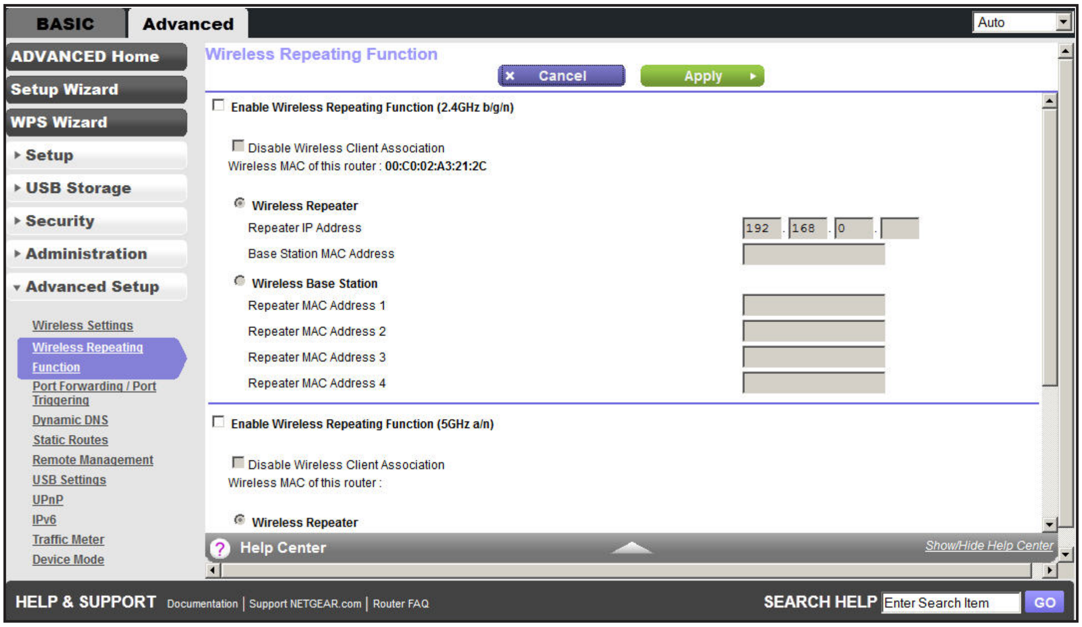
The DGND3700v2 wireless modem router is always in dual-band concurrent mode, unless you turn off one radio. Be aware that if you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless wireless modem router or wireless base station, dual-band concurrent mode is not affected.

For you to set up a wireless network with WDS, the following conditions have to be met for both access points:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) have to be configured to operate in the same LAN network address range as the access points.

Wireless Repeating Function

Select **Advanced > Advanced Setup > Wireless Repeating Function** to view or change wireless repeater settings for the wireless modem router.



Wireless Repeating Function

□ Enable Wireless Repeating Function (2.4GHz b/g/n)

□ Disable Wireless Client Association

Wireless MAC of this router : **00:C0:02:A3:21:2C**

● Wireless Repeater

Repeater IP Address 192 . 168 . 0 .

Base Station MAC Address

○ Wireless Base Station

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

□ Enable Wireless Repeating Function (5GHz a/n)

□ Disable Wireless Client Association

Wireless MAC of this router :

● Wireless Repeater

- **Enable Wireless Repeating Function**. Select the check box for the 2.4 GHz or 5 GHz network to use the wireless repeating function.

Disable Wireless Client Association. If your wireless modem router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- If you are setting up a point-to-point bridge, select this check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- **Wireless MAC of this router**. This field displays the MAC address for your wireless modem router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your wireless modem router is the repeater, select this radio button.

  Repeater IP Address. If your wireless modem router is the repeater, enter the IP address of the other access point.

  Base Station MAC Address. If your wireless modem router is the repeater, enter the MAC address for the access point that is the base station.
- **Wireless Base Station**. If your wireless modem router is the base station, select this radio button.

  Disable Wireless Client Association. If your wireless modem router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

  Repeater MAC Address (1 through 4). If your wireless modem router is the base station, it can act as the “parent” of up to four other access points. Enter the MAC addresses of the other access points in these fields.

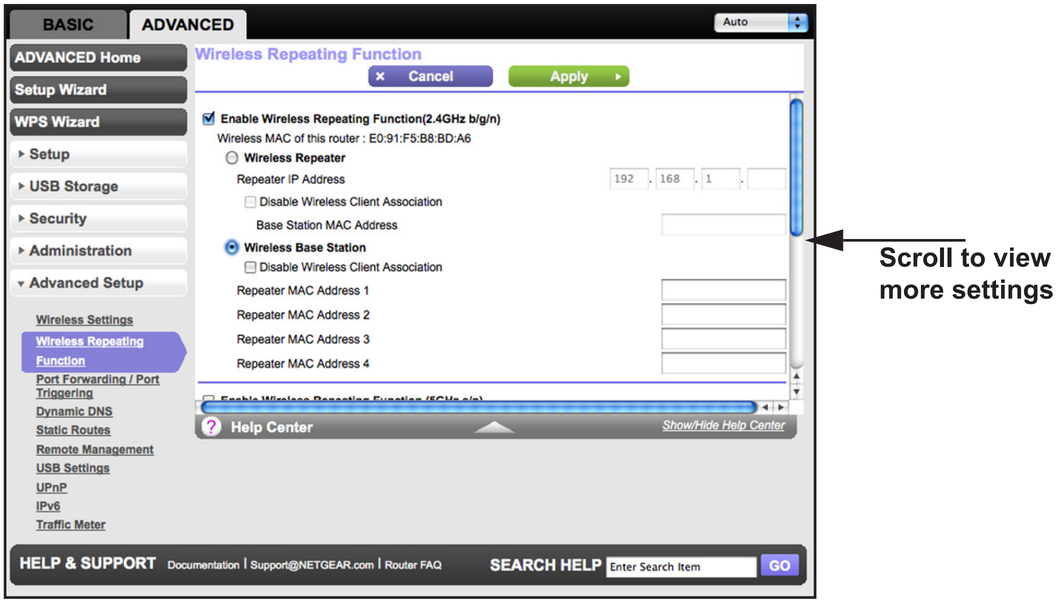
Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option has to be set to None or WEP.

2. Select **Advanced > Advanced Setup > Wireless Repeating Function** to display the Wireless Repeating Function screen.



Wireless Repeating Function

☑ Enable Wireless Repeating Function(2.4GHz b/g/n)

Wireless MAC of this router : E0:91:F5:B8:BD:A6

○ Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

□ Disable Wireless Client Association

Base Station MAC Address

● Wireless Base Station

□ Disable Wireless Client Association

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

> **Note:** If you are using the DGND3700v2 base station with a non-NETGEAR wireless modem router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

➢ **To configure the wireless modem router as a repeater unit:**

1. Log in to the wireless modem router that will be the repeater. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
2. Select **Advanced > Advanced Setup > Wireless Repeating Function**, and select the **Enable Wireless Repeating Function check box** and the **Wireless Repeater** radio button.
3. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP of the base station.

4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the wireless modem router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other access point.

Port Forwarding and Triggering

By default, the wireless modem router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

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

Your wireless modem router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your wireless modem router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your wireless modem router has to modify the source information and 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:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your wireless modem router.

   Source address. Your computer’s IP address.

   Source port number. 5678, which is the browser session.

   Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

   Destination port number. 80, which is the standard port number for a web server process.

3. Your wireless modem 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 wireless

modem 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 wireless modem 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 wireless modem router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your wireless modem router then sends this request message through the Internet to the web server at www.example.com.

4. 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 web server then sends this reply message to your wireless modem router.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. The public IP address of your wireless modem router.

   Destination port number. 33333.

5. Upon receiving the incoming message, your wireless modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the wireless modem router then modifies the message to restore the original address information replaced by NAT. Your wireless modem router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. Your computer’s IP address.

   Destination port number. 5678, which is the browser session that made the initial request.

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

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your wireless modem router from a particular service port number, and replies from the remote computer to your wireless modem router are directed to that port number. If the remote server sends a reply back to a different port number, your wireless modem router does not recognize it and discards 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 wireless modem router, you can tell the wireless modem 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 wireless modem router, “When you initiate a session with destination port 6667, you have to 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:

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 wireless modem router.
3. Your wireless modem router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your wireless modem 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 having observed the destination port number of 6667, your wireless modem router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your wireless modem router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an identify message to your wireless modem router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your wireless modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the wireless modem router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your wireless modem router checks its session table and learns that there is an active session for port 113, associated with your computer. The wireless modem 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 wireless modem router eventually senses a period of inactivity in the communications. The wireless modem 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 number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

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

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your wireless modem router ignores 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 the 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 wireless modem 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:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your wireless modem router. The remote computer composes 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 wireless modem router.

   Destination port number. 80, which is the standard port number for a web server process.

   The remote computer then sends this request message through the Internet to your wireless modem router.

2. Your wireless modem 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 wireless modem router modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your wireless modem router then sends this request message to your local network.

3. 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 wireless modem router.
4. Your wireless modem 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. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

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

Set Up 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 might want to make a local web server, FTP server, or game server visible and available to the Internet.

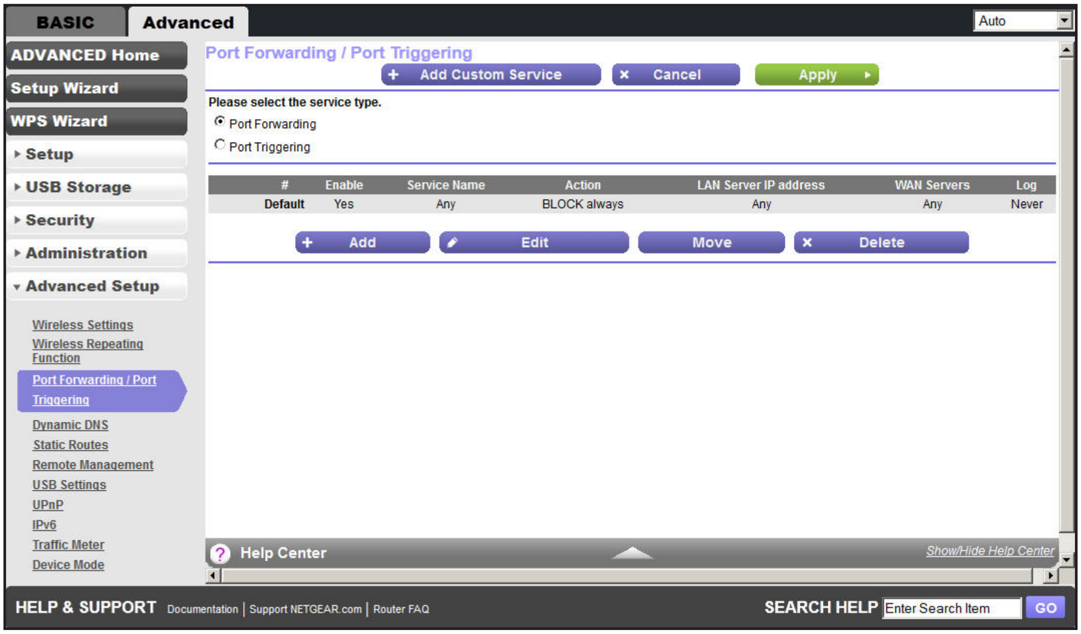
Use the Port Forwarding/Port Triggering screen to configure the wireless modem router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your N600 Modem Router.

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering** to display the following screen:



Port Forwarding / Port Triggering

Please select the service type.

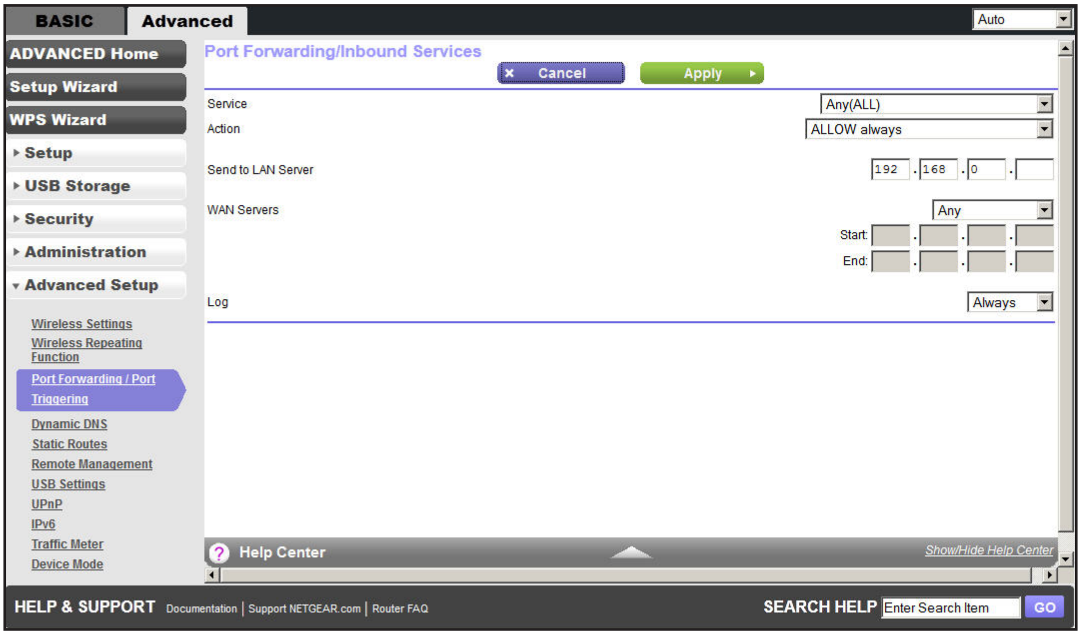
● Port Forwarding

○ Port Triggering

#	Enable	Service Name	Action	LAN Server IP address	WAN Servers	Log
Default	Yes	Any	BLOCK always	Any	Any	Never

Port Forwarding is selected as the service type.

2. Click **Add** to display the following screen:



Port Forwarding/Inbound Services

Service	Any(ALL)
Action	ALLOW always
Send to LAN Server	192 . 168 . 0 .
WAN Servers	Any
	Start: . . .
	End: . . .
Log	Always

3. From the Service list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 111.
4. From the Action list, select the action that you want.

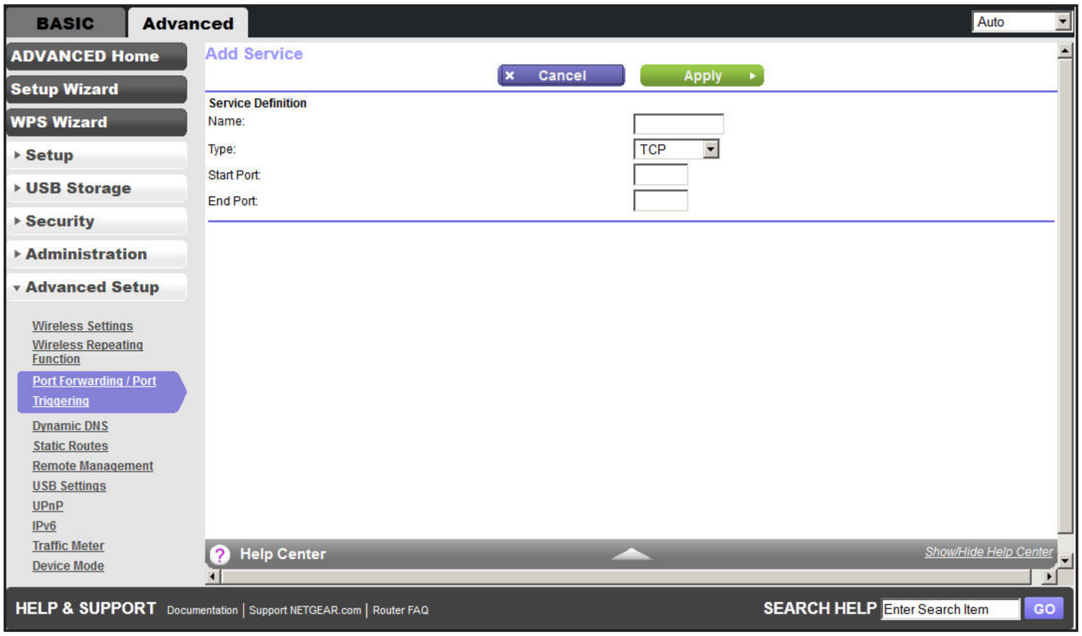
5. In the corresponding Send to LAN Server field, enter the last digit of the IP address of your local computer that will provide this service.
6. Click **Apply**. The service appears in the list in the screen.

Add a Custom Service

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

➢ **To add a custom service:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button to display the following screen:



Service Definition
Name:
Type: TCP
Start Port:
End Port:

4. In the Name field, enter a descriptive name.
5. In the Type list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Start Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the End Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the End Port field.
7. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. In the table, select the radio button next to the service name.
3. 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. In this example, your wireless modem router will always give your web server an IP address of 192.168.1.33.
2. In the Port Forwarding/Port Triggering screen, configure the wireless modem router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your wireless modem router to use the name as described in *Dynamic DNS* on page 114. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

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

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

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

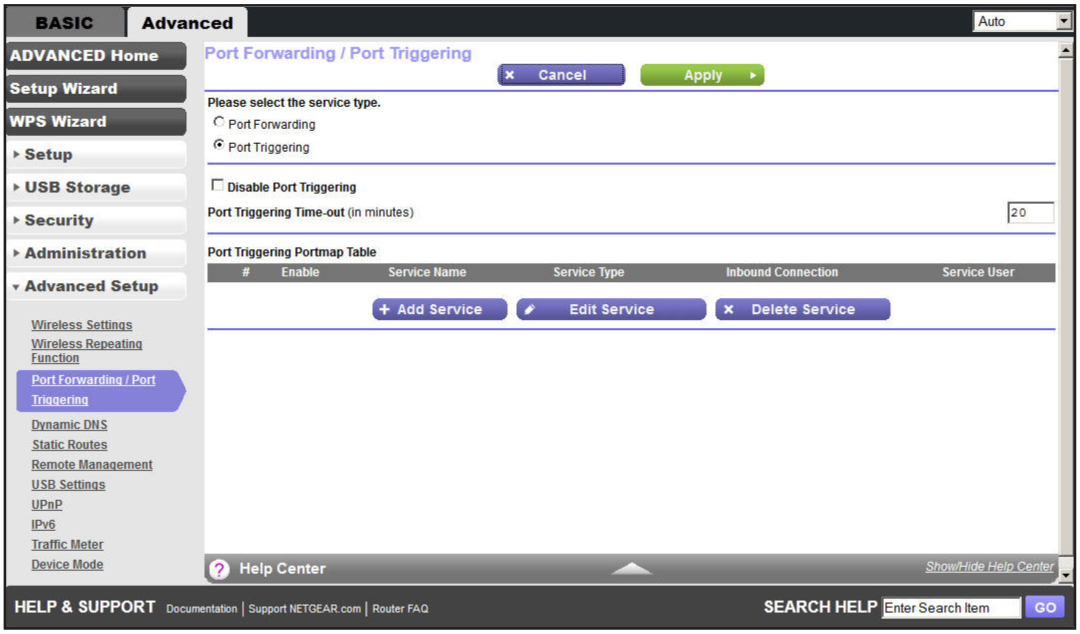
While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 119.

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

➢ To set up port triggering:

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.



Please select the service type.

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Time-out (in minutes) 20

Port Triggering Portmap Table

#	Enable	Service Name	Service Type	Inbound Connection	Service User

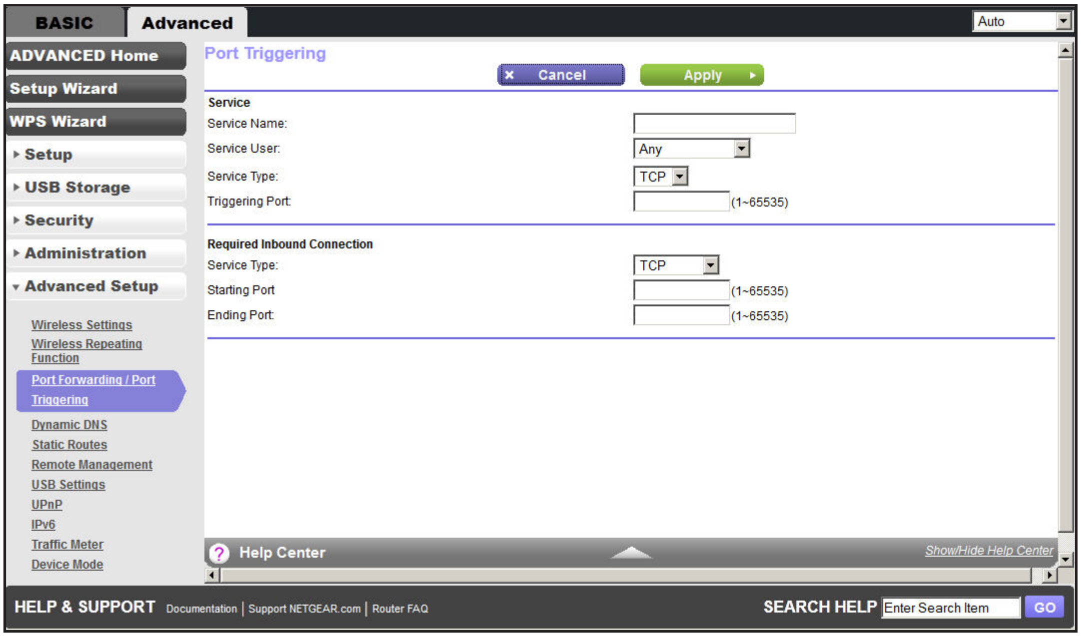
3. Clear the **Disable Port Triggering** check box if it is selected.

   Note: If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the wireless modem router is retained even though it is not used.

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

   This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the wireless modem router cannot be sure when the application has terminated.

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



Port Triggering

Service

Service Name:

Service User: Any

Service Type: TCP

Triggering Port: (1~65535)

Required Inbound Connection

Service Type: TCP

Starting Port (1~65535)

Ending Port: (1~65535)

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

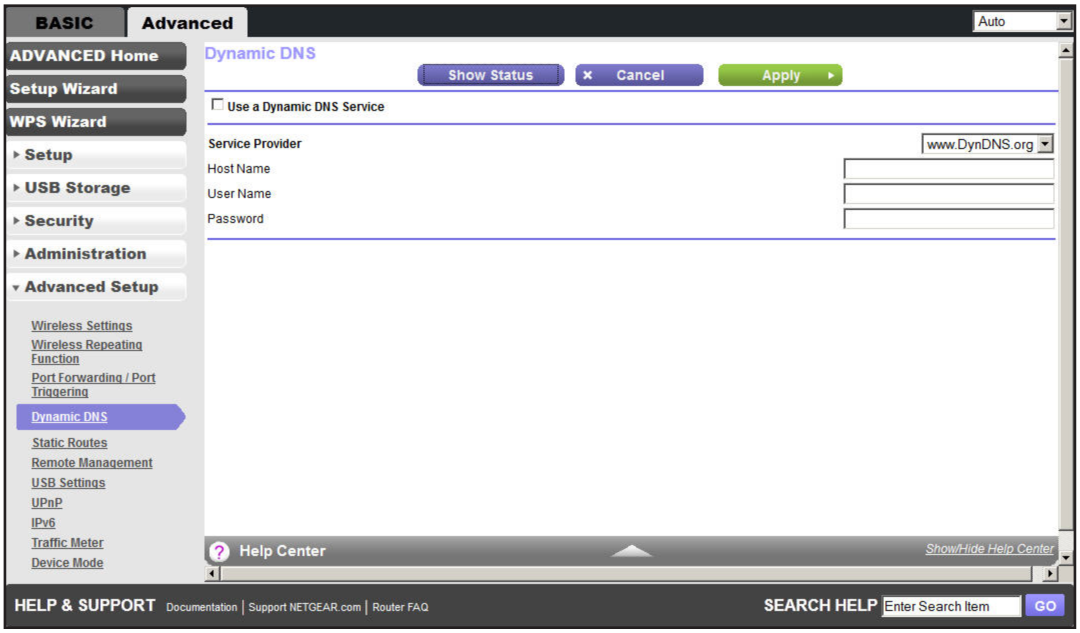
Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

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

Your wireless modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and host name that you configure in the wireless modem router. Then, whenever your ISP-assigned IP address changes, your wireless modem router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your wireless modem router at *http://hostname.dyndns.org*.

On the Advanced tab, select **Advanced Setup > Dynamic DNS** to display the following screen:



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider	www.DynDNS.org
Host Name	
User Name	
Password	

Figure 12. Forward traffic to a changing IP address

➢ To set up Dynamic DNS:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list. For example, for DynDNS.org, select **www.dyndns.org**.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your Dynamic DNS service provider.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. Click **Apply** to save your configuration.

Static Routes

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

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

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

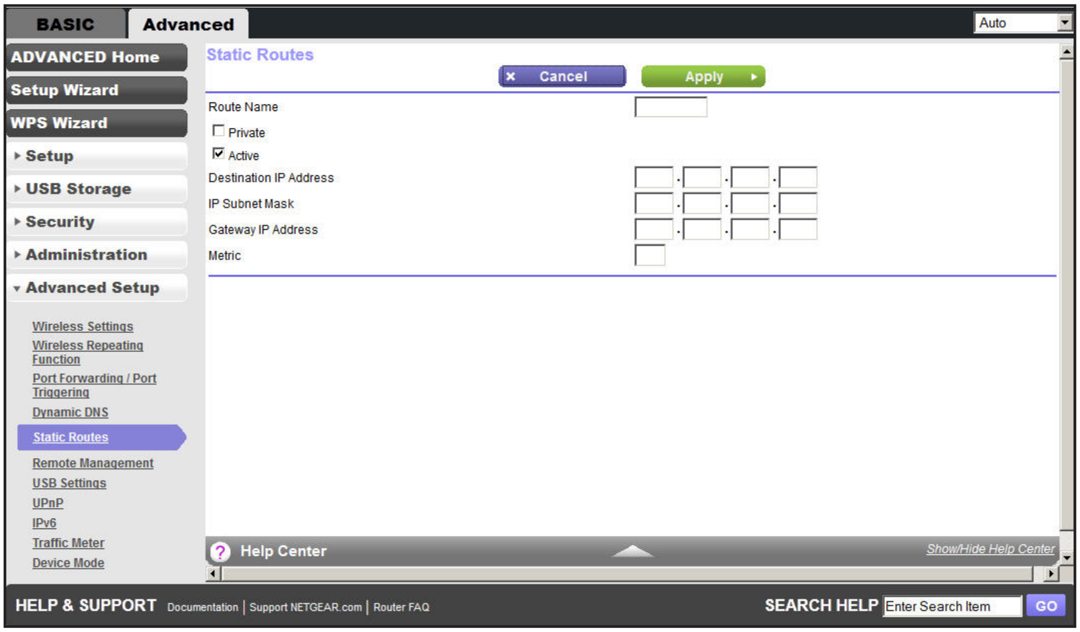
When you first configured your wireless modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your wireless modem router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your wireless modem router that 134.177.0.0 should be accessed through the ISDN wireless modem router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN wireless modem router at 192.168.1.100.
- A metric value of 1 will work since the ISDN wireless modem 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. Select **Advanced > Advanced Setup > Static Routes**, and click **Add** to display the following screen:



Static Routes

Route Name

□ Private

☑ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

2. In the Route Name field, type a **name** for this static route (for identification purposes only.
3. 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.
4. Select the **Active** check box to make this route effective.
5. Type the IP address of the final destination.
6. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
7. Type the gateway IP address, which has to be a wireless modem router on the same LAN segment as the N600 Modem Router.
8. Type a number between 1 and 15 as the metric value.

   This value represents the number of wireless modem 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.

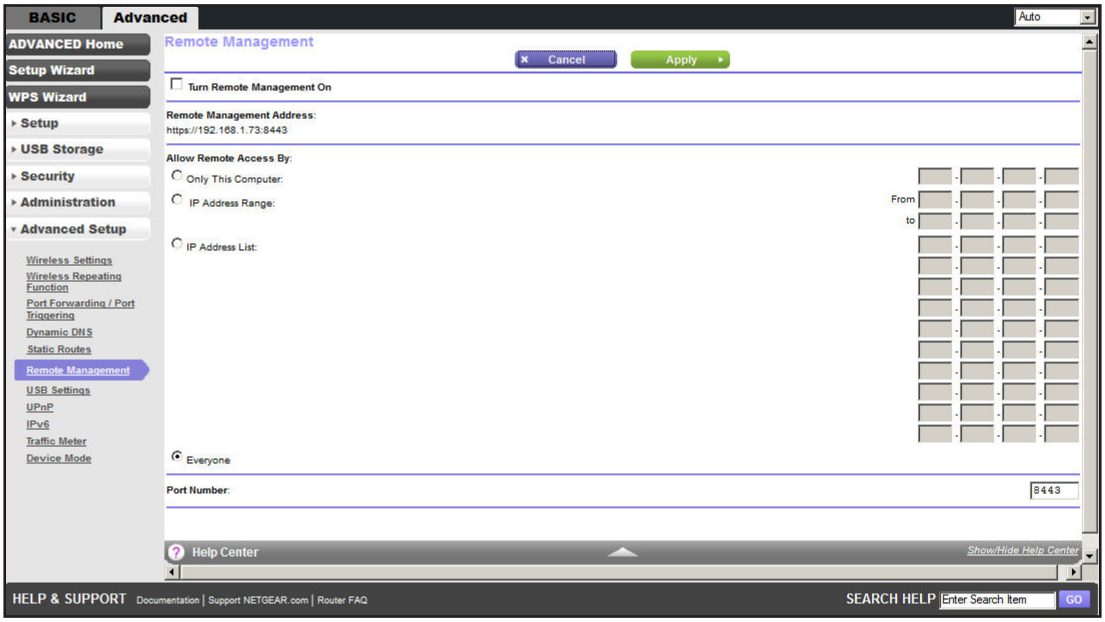
9. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your N600 Modem Router over the Internet.

➢ To set up remote management:

1. Select **Advanced > Advanced Setup > Remote Management**.



Remote Management

□ Turn Remote Management On

Remote Management Address:
https://192.168.1.73:8443

Allow Remote Access By:

○ Only This Computer:

○ IP Address Range: From to

○ IP Address List:

● Everyone

Port Number: 8443

Note: Be sure to change the wireless modem router’s default login password to a very secure password. The ideal password should contain no dictionary words from any language and contain uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

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

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

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

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

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

5. Click **Apply** to have your changes take effect.
6. When accessing your wireless modem router from the Internet, type your wireless modem 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.

USB Settings

For added security, the wireless modem router can be set up to share only approved USB devices. See *Specify Approved USB Devices* on page 68 for the procedure.

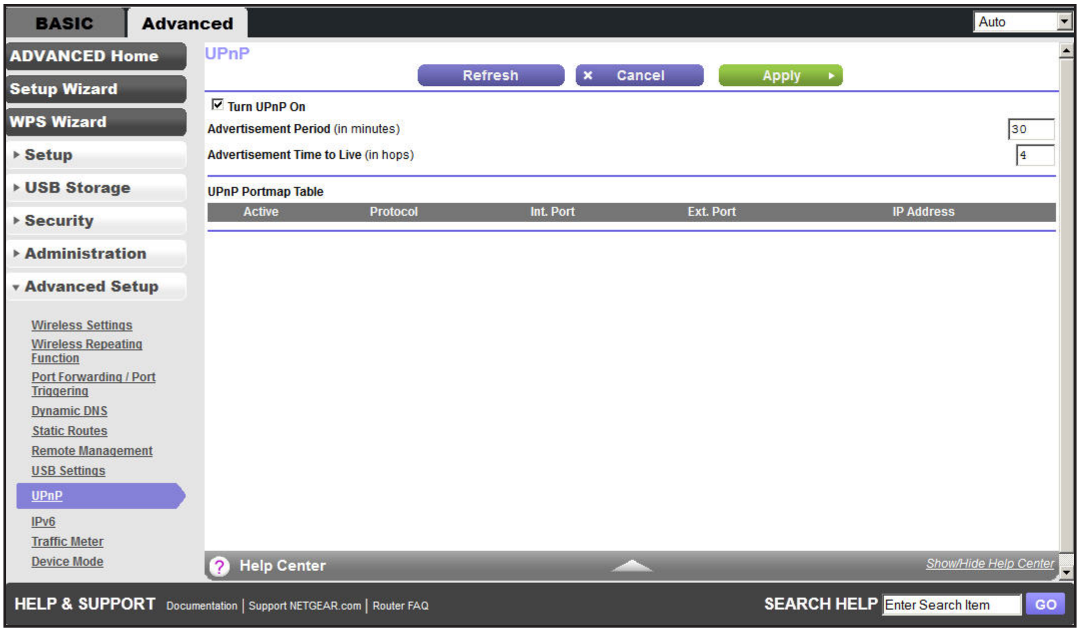
Universal Plug and Play

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 multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ To turn on Universal Plug and Play:

1. Select **Advanced > Advanced Setup > UPnP**. The UPnP screen displays.



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time to Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

2. The available settings and information in this screen are:

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

   Advertisement Period. The advertisement period is how often the wireless modem router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can 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 might 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 wireless modem 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.

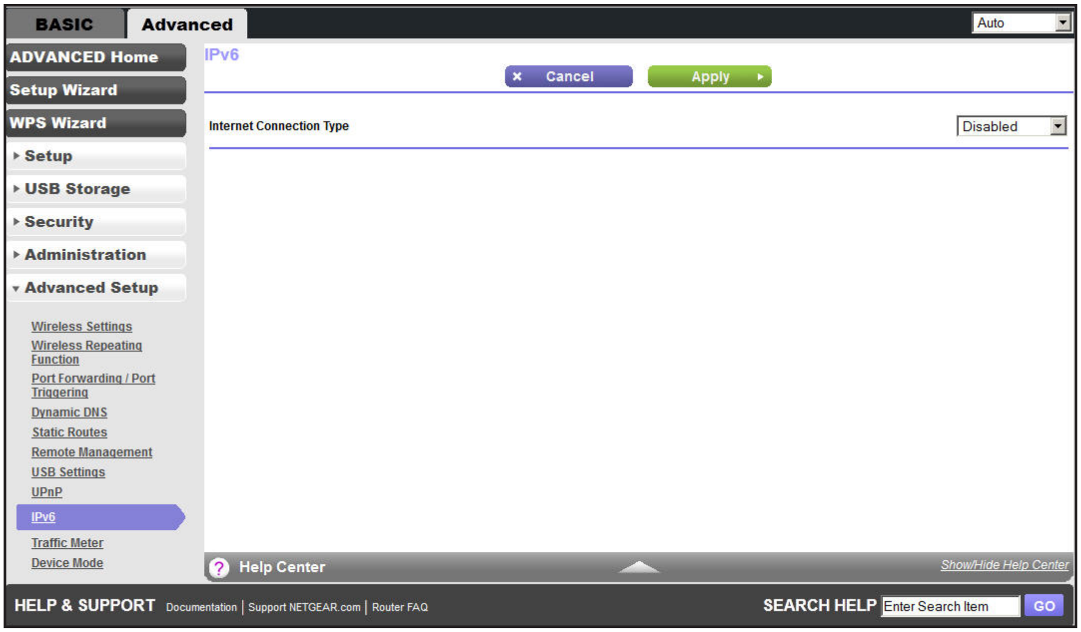
3. Click **Apply** to save your settings.

IPv6

You can use this feature to set up an IPv6 Internet connection type if NETGEAR Genie does not detect it automatically.

➢ **To set up an IPv6 Internet connection type:**

1. Select **Advanced > Advanced Setup > IPv6** to display the following screen:



Internet Connection Type: Disabled

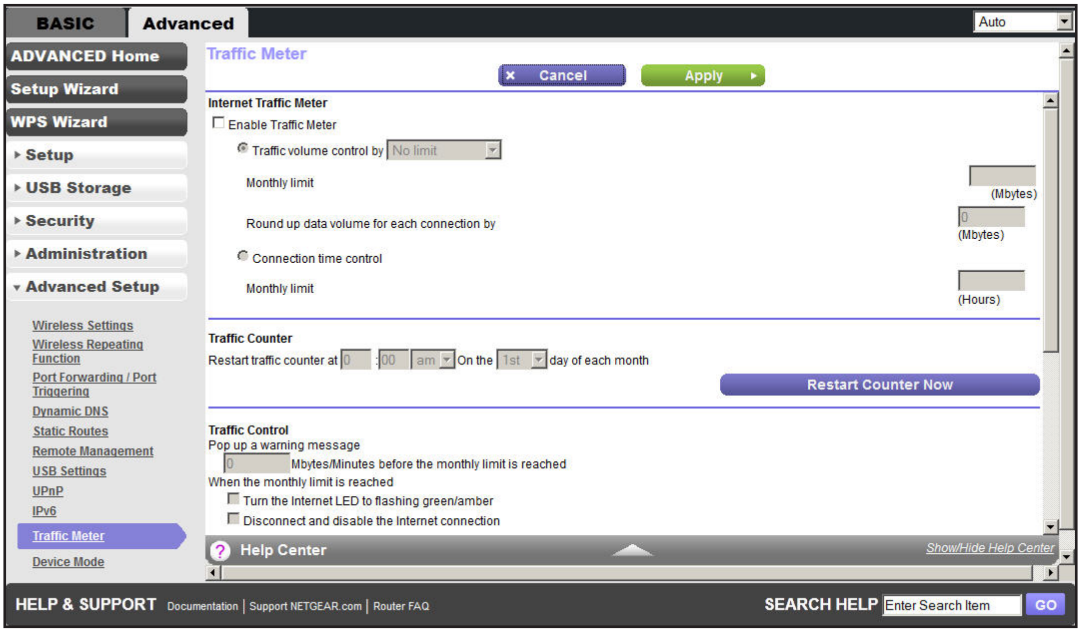
2. Select the IPv6 connection type from the list. Your Internet service provider (ISP) can provide this information.
   - If your ISP did not provide details, you can select **IPv6 Tunnel**.
   - If you are not sure, select **Auto Detect** so that the wireless modem router detects the IPv6 type that is in use.
   - If your Internet connection does not use PPPoE, DHCP, or fixed, but is IPv6, then select **IPv6 auto config**.
3. Click **Apply** so that your changes take effect.

Traffic Meter

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

➢ To monitor Internet traffic:

1. Click **Advanced > Advanced Setup > Traffic Meter** to display the following screen:



Traffic Meter

Internet Traffic Meter

□ Enable Traffic Meter

● Traffic volume control by No limit

Monthly limit (Mbytes)

Round up data volume for each connection by 0 (Mbytes)

○ Connection time control

Monthly limit (Hours)

Traffic Counter

Restart traffic counter at 0 :00 am On the 1st day of each month

Traffic Control

Pop up a warning message

0 Mbytes/Minutes before the monthly limit is reached

When the monthly limit is reached

□ Turn the Internet LED to flashing green/amber

□ Disconnect and disable the Internet connection

2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No Limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.
5. Set the traffic counter to begin at a specific time and date.
6. Set up traffic control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or red.
   - The Internet connection is disconnected and disabled.
7. Set up Internet traffic statistics to monitor the data traffic.
8. Click the **Traffic Status** button to get a live update on Internet traffic status on your wireless modem router.
9. Click **Apply** to save your settings.

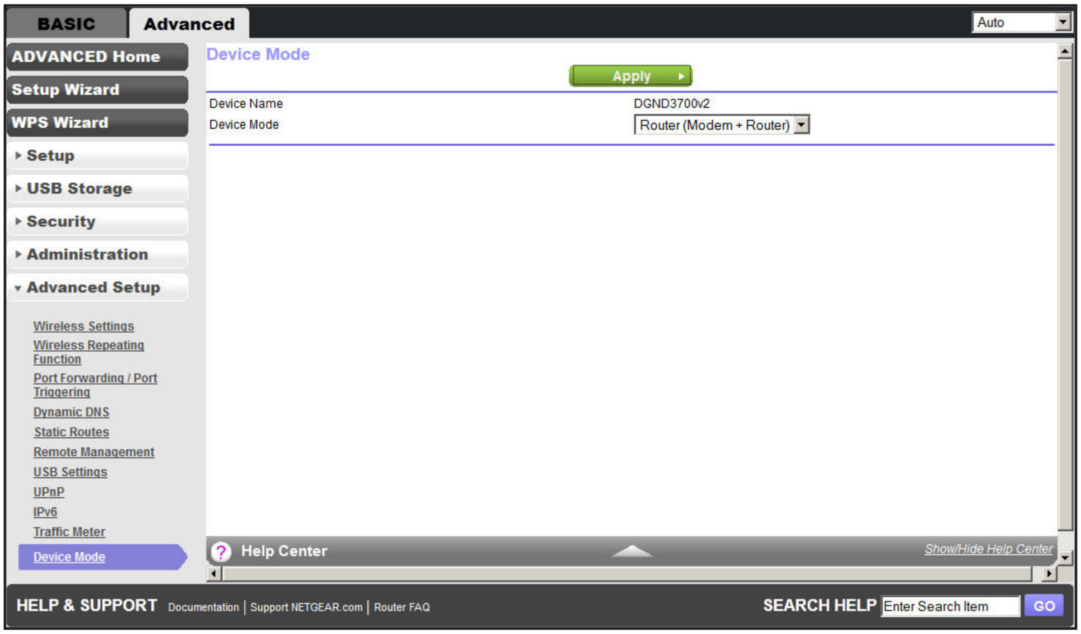
Device Mode

When the wireless modem router is in Router mode, this screen allows switching to Modem mode, where the wireless modem router acts as a pure bridge or DSL modem.

Routing, firewall, wireless support, USB, and the traffic meter are not available in Modem mode. A typical application is a small-to-medium business scenario where the wireless modem router is used for DSL connectivity behind a carrier class router or firewall or security device manager. When the wireless modem router is in Modem mode, this screen allows switching back to Router mode with all of the standard features.

➢ **To switch the device mode:**

1. Click **ADVANCED > Advanced Setup > Device Mode** to display the following screen:



Device Mode

Device Name DGND3700v2

Device Mode Router (Modem + Router)

2. From the Device Mode list, select **Router (Modem + Router)** or **Modem (Modem only)**.
3. Click **Apply** to save your settings.

VPN Policies

Manage your VPN policies from the VPN Policies screen.

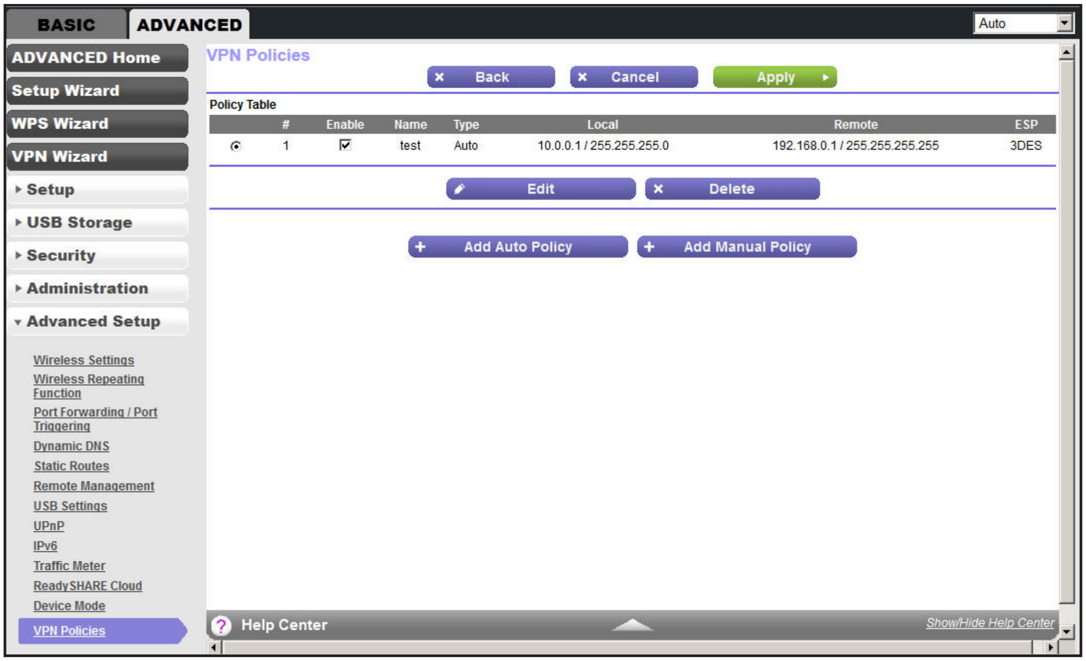
- Traffic covered by a policy is automatically sent through a VPN tunnel.
- Where traffic is covered by two or more policies, the first matching policy is used. In this situation, the order of the policies is important. However, if you only have one policy for each remote VPN endpoint, then the policy order is not important.
- The VPN tunnel is created according to the parameters in the SA (security association).
- The remote VPN endpoint must have a matching SA, or else it refuses the connection.

There are two types of VPN policies:

- **Manual**. All settings (including the keys) for the VPN tunnel are input manually at each end (both VPN endpoints). No third-party server or organization is involved.
- **Auto**. Some parameters for the VPN tunnel are generated automatically. This process requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN endpoints.

➢ To manage the VPN policies:

1. Click **ADVANCED > Advanced Setup > VPN Policies**.



Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
●	1	☑	test	Auto	10.0.0.1 / 255.255.255.0	192.168.0.1 / 255.255.255.255	3DES

The Policy Table contains the following data:

- **Enable**. Use this check box to enable or disable a policy as required. Click **Apply** after you make any changes.
- **Name**. Each policy has a unique name to identify it.
- **Type**. The type is Auto or Manual.
- **Local**. The IP address or address range on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy.
- **Remote**. The IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy.
- **ESP**. Encapsulating Security Payload. This setting specifies the encryption protocol used for the VPN data.

2. Click the appropriate button to manage a VPN policy:
   - **Edit**. Edit (modify) the selected policy. (Select a policy by selecting the radio button.)
   - **Delete**. Delete the selected policy.

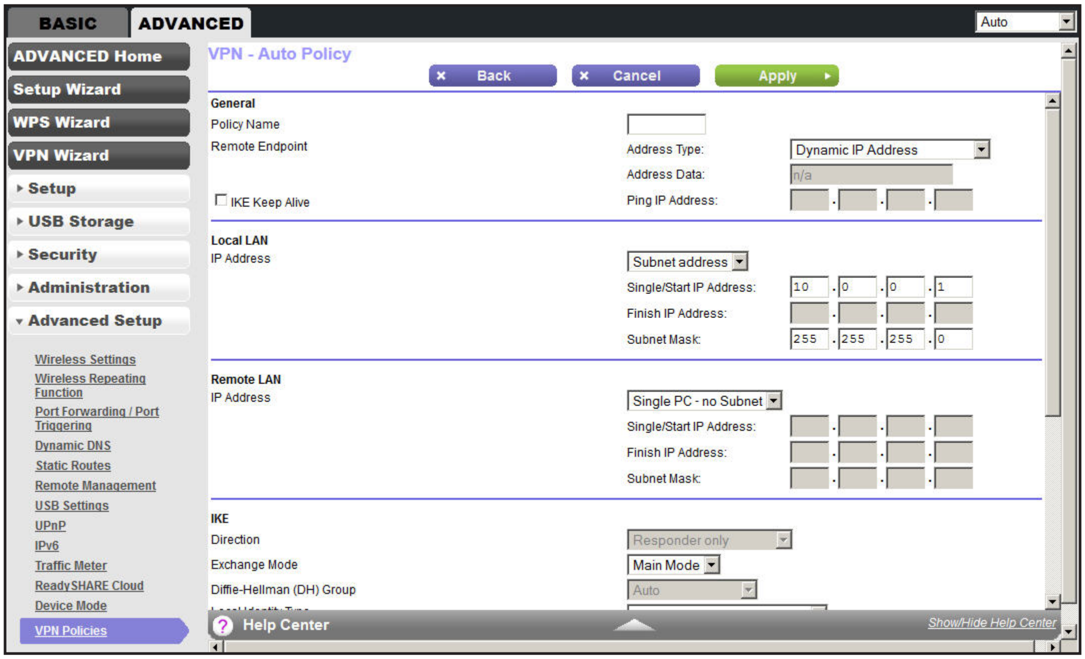
- **Apply**. Save any changes to the Enable setting for each policy.
- **Cancel**. Discard any unsaved changes to the Enable setting for each policy.
- **Add Auto Policy**. Change to the input screen for an Auto policy. When the new policy is saved, it appears in the bottom row of the Policy Table. See *Add or Edit an Auto VPN Policy* on page 125.
- **Add Manual Policy**. Change to the input screen for a Manual policy. When the new policy is saved, it appears in the bottom row of the Policy Table. See *Add or Edit a Manual VPN Policy* on page 128.

Add or Edit an Auto VPN Policy

An Auto VPN policy uses the IKE (Internet Key Protocol) to exchange and negotiate parameters for the IPsec SA (security association). Because of this negotiation, not all of the settings on this VPN gateway have to match the settings on the remote VPN endpoint. Where settings have match, this requirement is indicated.

➢ **To add or edit an Auto VPN Policy:**

1. Click **ADVANCED > Advanced Setup > VPN Policies**.
2. Click the **Add Auto Policy** button.



VPN - Auto Policy

General
Policy Name:
Remote Endpoint — Address Type: Dynamic IP Address
Address Data: n/a
☐ IKE Keep Alive — Ping IP Address: . . .

Local LAN
IP Address: Subnet address
Single/Start IP Address: 10 . 0 . 0 . 1
Finish IP Address: . . .
Subnet Mask: 255 . 255 . 255 . 0

Remote LAN
IP Address: Single PC - no Subnet
Single/Start IP Address: . . .
Finish IP Address: . . .
Subnet Mask: . . .

IKE
Direction: Responder only
Exchange Mode: Main Mode
Diffie-Hellman (DH) Group: Auto

3. Enter or select the following parameters:
   - **General**. These settings identify this policy and determine its major characteristics.
     - **Policy Name**. Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

  - **Remote VPN Endpoint**. If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required.

    Otherwise, select the desired option (IP address or domain name) and enter the address of the remote VPN endpoint you wish to connect to.

    The remote VPN endpoint must have this VPN gateway's address entered as its remote VPN endpoint.
  - **IKE Keep Alive**. Check this check box if you wish to ensure that a connection is kept open, or, if that is not possible, it is quickly reestablished when disconnected.

    The ping IP address has to be associated with the remote endpoint. Either the WAN or a LAN address can be used; a LAN address is preferable. This IP address is pinged to generate some traffic for the VPN tunnel.
- **Local LAN**. These settings identify which computers on your LAN are covered by this policy. For each selection, data must be provided as follows:
  - **Single address**. Enter an IP address in the Single/Start IP address field. Typically, this setting is used when you wish to make a single server on your LAN available to remote users.
  - **Range address**. Enter the starting IP address in the Single/Start IP address field, and the finish IP address in the Finish IP address field. This range must be an address range used on your LAN.
  - **Subnet address**. Enter an IP address in the Single/Start IP address field, and the desired network mask in the Subnet Mask field.

  The remote VPN endpoint must have these IP addresses entered as its remote addresses.
- **Remote LAN**. These settings identify which computers on the remote LAN are covered by this policy. For each selection, data must be provided as follows:
  - **Single PC - no Subnet**. Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required.
  - **Single address**. Enter an IP address in the Single/Start IP address field. This value must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
  - **Range address**. Enter the starting IP address in the Single/Start IP address field, and the finish IP address in the Finish IP address field. This range must be an address range used on the remote LAN.
  - **Subnet address**. Enter an IP address in the Single/Start IP address field, and the desired network mask in the Subnet Mask field.

  The remote VPN endpoint must have these IP addresses entered as its local addresses.
- **IKE**.

  - **Direction/Type**. This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.
  - **Responder only**. Incoming connections are allowed, but outgoing connections are blocked.
  - **Initiator and Responder**. Both incoming and outgoing connections are allowed.
  - **Exchange Mode**. Currently, only Main Mode is supported. Ensure that the remote VPN endpoint is set to use Main Mode.
  - **Diffie-Hellman (DH) Group**. The Diffie-Hellman algorithm is used when the connection exchanges keys. The DH Group setting determines the bit size used in the exchange. This value must match the value used on the remote VPN gateway.
  - **Local Identity Type**. Select the desired option to match the Remote Identity Type setting on the remote VPN endpoint.
  - **WAN IP Address**. Your Internet IP address.
  - **Fully Qualified Domain Name**. Your domain name.
  - **Fully Qualified User Name**. Your name, email address, or other ID.
  - **Local Identity Data**. Enter the data for the selection. If WAN IP Address is selected, no input is required.
  - **Remote Identity Type**. Select the desired option to match the Local Identity Type setting on the remote VPN endpoint.
  - **IP Address**. The Internet IP address of the remote VPN endpoint.
  - **Fully Qualified Domain Name**. The domain name of the remote VPN endpoint.
  - **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.
  - **Remote Identity Data**. Enter the data for the selection. If IP Address is selected, no input is required.
- **Parameters**.
  - **Encryption Algorithm**. The encryption algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN gateway.
  - **Authentication Algorithm**. The authentication algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN gateway.
  - **Pre-shared Key**. The key has to be entered both here and on the remote VPN gateway.
  - **SA Life Time**. This setting determines the time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA lifetime. This setting applies to both IKE and IPSec SAs.
  - **Enable PFS (Perfect Forward Secrecy)**. If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you might need to specify the key group used. For this device, the key group is the same as the DH Group setting in the IKE section.

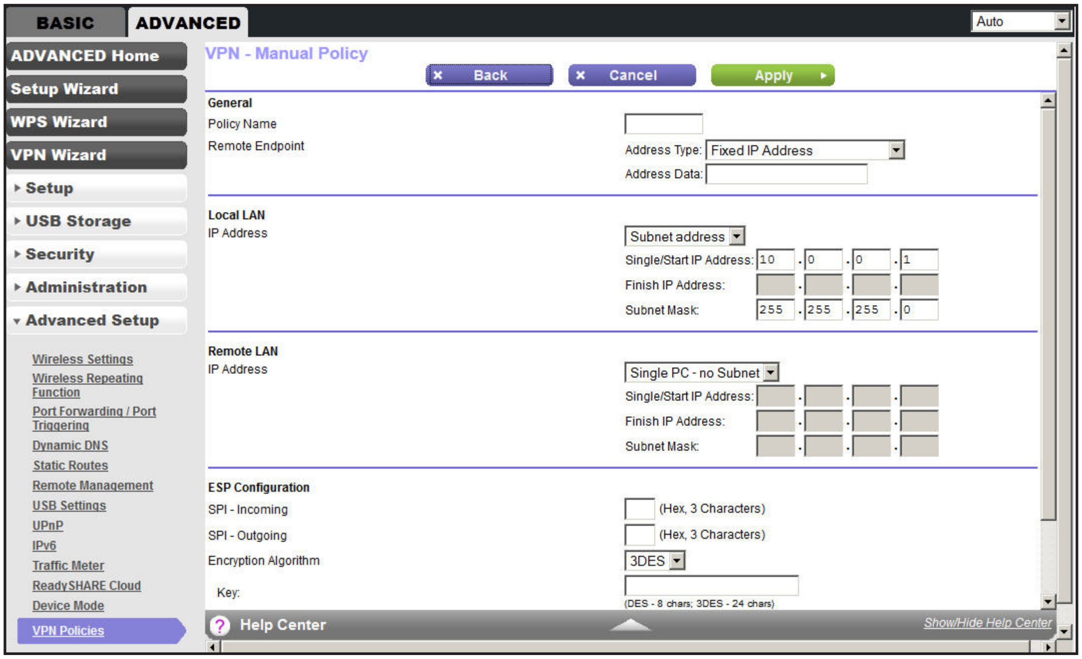
4. Click the **Apply** button when done.

Add or Edit a Manual VPN Policy

A Manual VPN policy requires all settings (including the keys) for the VPN tunnel to be manually input at each end (both VPN endpoints). No third-party server or organization is involved.

➢ **To add or edit a Manual VPN policy:**

1. Click **ADVANCED > Advanced Setup > VPN Policies**.
2. Click the **Add Manual Policy** button.



VPN - Manual Policy

General
Policy Name
Remote Endpoint — Address Type: Fixed IP Address; Address Data:

Local LAN
IP Address — Subnet address
Single/Start IP Address: 10 . 0 . 0 . 1
Finish IP Address: . . .
Subnet Mask: 255 . 255 . 255 . 0

Remote LAN
IP Address — Single PC - no Subnet
Single/Start IP Address: . . .
Finish IP Address: . . .
Subnet Mask: . . .

ESP Configuration
SPI - Incoming (Hex, 3 Characters)
SPI - Outgoing (Hex, 3 Characters)
Encryption Algorithm 3DES
Key: (DES - 8 chars; 3DES - 24 chars)

3. Enter or select the following parameters:
   - **General**. These settings identify this policy and determine its major characteristics.
     - **Policy Name**. Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
     - **Remote VPN Endpoint**. Select the desired option (IP address or domain name) and enter the address or domain name of the remote VPN endpoint you wish to connect to.

       The remote VPN endpoint must have this VPN gateway’s address entered as its remote VPN endpoint.

- **Local LAN**. These settings identify which computers on your LAN are covered by this policy. For each selection, data must be provided as follows:
    - **Single address**. Enter an IP address in the Single/Start IP address field. Typically, this setting is used when you wish to make a single server on your LAN available to remote users.
    - **Range address**. Enter the starting IP address in the Single/Start IP address field, and the finish IP address in the Finish IP address field. This setting must be an address range used on your LAN.
    - **Subnet address**. Enter an IP address in the Single/Start IP address field, and the desired network mask in the Subnet Mask field.

  The remote VPN endpoint must have these IP addresses entered as its remote addresses.

- **Remote LAN**. These identify which computers on the remote LAN are covered by this policy. For each selection, data must be provided as follows:
    - **Single PC - dynamic IP**. Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required.
    - **Single address**. Enter an IP address in the Single/Start IP address field. This setting must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
    - **Range address**. Enter the starting IP address in the Single/Start IP address field, and the finish IP address in the Finish IP address field. This range must be an address range used on the remote LAN.
    - **Subnet address**. Enter an IP address in the Single/Start IP address field, and the desired network mask in the Subnet Mask field.

  The remote VPN endpoint must have these IP addresses entered as its local addresses.

- **ESP Configuration**. ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.
    - **SPI**. Enter the required SPIs. Each policy must have unique SPIs. These settings must match the remote VPN endpoint. The Incoming setting here must match the Outgoing setting on the remote VPN endpoint, and the Outgoing setting here must match the Incoming setting on the remote VPN endpoint.
    - **Encryption**. Select the desired encryption algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters (48-hex characters).
    - **Authentication**. Select the desired authentication algorithm, and enter the key in the field provided. For MD5, the keys should be 16 ASCII characters (32-hex characters). For SHA-1, the keys should be 20 ASCII (40-hex characters).

4. Click the **Apply** button when done.

10 Troubleshooting

Diagnose and solve problems

This chapter provides information to help you diagnose and solve problems you might have with your wireless modem 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*
- *Incorrect Date or Time*
- *Wireless Connectivity*
- *Restore the Factory Settings and Password*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

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

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

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

Wireless Settings

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

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

Network Settings

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

- Wired and wirelessly connected computers need to have network (IP) addresses on the same network as the wireless modem 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 wireless modem router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED ⏻ is on.
2. Verify that the Power LED turns red within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify that:
   - The Power LED is solid green.
   - The Internet LED is on.
   - A numbered Ethernet port LED is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

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

Power LED Is Off or Blinking

- Make sure that the power cord is securely connected to your wireless modem router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 12V DC, 2.5A power adapter that NETGEAR supplied for this product.
- If the Power LED blinks slowly and continuously, the wireless modem router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the wireless modem 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 Red

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

If the Power LED is still red one minute after you turn on power to the wireless modem router:

1. Turn the power off and back on to see if the wireless modem router recovers.
2. Press and hold the **Restore Factory Settings** button to return the wireless modem router to its factory settings. See *Factory Settings* on page 142.

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

LEDs Never Turn Off

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

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

- Cycle the power to see if the wireless modem router recovers.
- Press and hold the **Restore Factory Settings** button to return the wireless modem router to its factory settings. See *Factory Settings* on page 142.

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

Internet or Ethernet Port LEDs Are Off

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

- Make sure that the Ethernet cable connections are secure at the wireless modem 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 wireless modem router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Wireless LEDs Are Off

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

The Push 'N' Connect (WPS) Button Blinks Red

If after you push the WPS function and the button blinks red, check the following:

- Make sure that you are using the button and not the wireless modem router's built-in registrar.
- Check that PIN verification has succeeded for the wireless device you are adding to the wireless network.
- Make sure you have not pressed the WPS button on the top of the wireless modem router after disabling the WPS feature (you logged in to the wireless modem router and disabled this previously).
- Check that the wireless modem router is not in the temporary AP setup locked state (if you are using the wireless repeater function).

Cannot Log In to the Router

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the wireless modem router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the wireless modem router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS 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 wireless modem router, and reboot your computer.
- If your wireless modem router's IP address was changed and you do not know the current IP address, clear the wireless modem router's configuration to factory defaults. This sets the wireless modem router's IP address to 192.168.1.1. This procedure is explained in *Factory Settings* on page 142.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR wireless modem router as an additional router behind an existing router in your network, consider replacing the existing router instead. NETGEAR does not support such a configuration.
- If you are attempting to set up your NETGEAR wireless modem router as a replacement for an ADSL gateway in your network, the wireless modem router cannot perform many gateway services, for example, converting 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 you are unable to access the Internet, first determine whether the wireless modem router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your wireless modem 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 *http://www.netgear.com*.
2. Access the wireless modem router interface at *http://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 wireless modem router has not obtained an IP address from your ISP.

If your wireless modem router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new wireless modem router by restarting your network, as described in *Sequence to Restart Your Network* on page 131.

If your wireless modem 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 Basic Settings screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer’s MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the wireless modem router’s MAC address.
  - Configure your wireless modem router to clone your computer’s MAC address.

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

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the wireless modem 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 wireless modem router configured as its TCP/IP gateway.

  If your computer obtains its information from the wireless modem 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 wireless modem 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. Log in to the wireless modem router.
2. Select **Administration > Router Status**.
3. Click **Connection Status**. If all of the steps indicate OK, then your PPPoE connection is up and working.

If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**. The wireless modem router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

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

Troubleshoot Internet Browsing

If your wireless modem 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 wireless modem 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 wireless modem router configured as its default gateway.

  Reboot the computer, and verify that the wireless modem 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 wireless modem router. You might need to go to Internet

Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

If the wireless modem router does not save changes you have made in the browser interface, check the following:

- When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.
- Click **Refresh** or **Reload** in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

Changes Not Saved

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

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

Incorrect Date or Time

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

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

Wireless Connectivity

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

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

  If not, check the Wireless LEDs on the front of the wireless modem router. They should be lit. If they are not, you can press the **WiFi On/Off** button on the back of the wireless modem router to turn the wireless modem router's wireless radio back on.

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

- 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 wireless modem router, use an Ethernet cable to connect a computer to a LAN port on the wireless modem router. Then log in to the wireless modem router and select **Setup > Wireless Settings** see (*Basic Wireless Settings* on page 35).

  Note: Be sure to click **Apply** if you make changes.

Wireless Signal Strength

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

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

Restore the Factory Settings and Password

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

- Use the Erase function of the wireless modem router (see *Erase* on page 93).
- Use the Restore Factory Settings button on the back of the wireless modem router. See *Factory Settings* on page 142. If you restore the factory settings and the wireless modem router fails to restart, or the green Power LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support at *http://www.netgear.com/support*.

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 by using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

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

➢ **To ping the wireless modem router from a computer running Windows:**

1. From the Windows toolbar, click **Start**, and then select **Run**.
2. In the field provided, type **ping** followed by the IP address of the wireless modem router, as in this example:

   ping www.routerlogin.net

3. Click **OK**.

   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 could have one of the following problems:

- Wrong physical connections

  For a wired connection, make sure that the numbered LAN port LED is on for the port to which you are connected.

  Check that the appropriate LEDs are on for your network devices. If your wireless modem router and computer are connected to a separate Ethernet switch, make sure that the Ethernet LEDs are on for the switch ports that are connected to your computer and wireless modem 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 wireless modem 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 then 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’s DNS server.

If the path is functioning correctly, replies like those shown in the previous section are displayed.

If you do not receive replies:

- Check that your computer has the IP address of your wireless modem router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not be visible in your computer’s Network Control Panel. Verify that the IP address of the wireless modem 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 Basic Settings screen.
- Your ISP could 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, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your wireless modem router to “clone” or “spoof” the MAC address from the authorized computer.

Supplemental Information

A

Factory settings and technical specifications

This appendix provides factory default settings and technical specifications for the N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700v2.

- *Factory Settings*
- *Technical Specifications*

Factory Settings

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

Table 13. 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
	Allow a registrar to configure this router	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
Local network (LAN) continued	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

Table 13. Factory default settings (continued)

Feature		Default Behavior
Wireless	Wireless communication	Enabled
	SSID name	See router label
	Security	Enabled
	Broadcast SSID	Enabled
	Transmission speed	Auto[1]
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 300 Mbps
	Data rate	Best
	Output power	Full
Firewall	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

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

Technical Specifications

Table 14. DGND3700v2 Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	• North America: 120V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • All regions (output): 12V DC @ 2.5A, output
Dimensions	8.8 in. x 6.8 in. x 1.2 in. (223 x 153 x 31 mm)
Weight	1.2 lbs (0.5 kg)
Operating temperature	0° to 40°C (32º to 104ºF)
Operating humidity	90% maximum relative humidity, noncondensing

Table 14. DGND3700v2 Router specifications (continued)

Feature	Description
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, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz IEEE 802.11n, IEEE 802.11a 5.0 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency 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) FCC: 5.25–5.35 GHz (DFS band) 5.47–5.725 GHz (DFS band) 5600–5650 MHz is disabled and unavailable for use CE (Europe ETSI): 5.25–5.35 GHz (DFS band) 5.47–5.725 GHz (DFS band)
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2 Enterprise.

Index