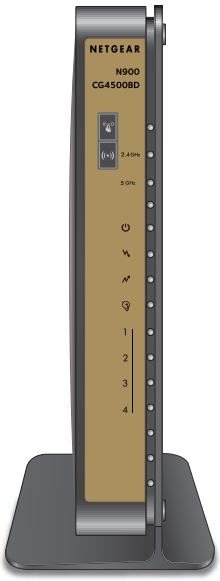
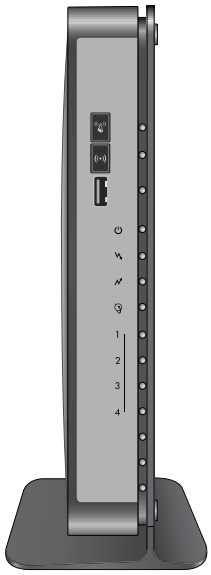
NETGEAR®

AC1900, N900, and N450 WiFi Cable Data Gateways

Models C6300BD, CG4500BD, and CG3000Dv2

User Manual





September 2014
202-11434-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

For technical support, contact Cox Support.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11434-01	September 2014	First publication

Contents

Chapter 5 Manage the Firewall and Secure Your Network

Chapter 6 Manage and Monitor Your Network

Chapter 7 Share USB Drives Attached to the Cable Data Gateway

Chapter 8 Configure Advanced Features

Chapter 9 Diagnostics and Troubleshooting

Appendix A Factory Default Settings and Specifications

Hardware Overview

1

This manual is for the following NETGEAR® WiFi cable data gateway models:

- AC1900 WiFi Cable Data Gateway, Model C6300BD
- N900 WiFi Cable Data Gateway, Model CG4500BD
- N450 WiFi Cable Data Gateway, Model CG3000Dv2[1]

Note: In this manual, unless stated by individual model name, these models are referred as the *cable data gateway*.

This chapter contains the following sections:

Note: For more information about the topics covered in this manual, visit the support website at *support.netgear.com*. However, for technical support, contact Cox Support.

Note: In this user guide, the terms *wireless* and *WiFi* mean the same thing.

1. The N450 WiFi Cable Data Gateway might also be referred to as the N450 WiFi Cable Modem Router.

Introduction

The cable data gateway provides you with an easy and secure way to set up a WiFi home network with fast access to the Internet over a cable network. It lets you block unsafe Internet content and applications and protects the devices (WiFi devices, computers, gaming consoles, and so on) that you connect to your home network.

To set up your new cable data gateway, use the installation guide that comes in the package. This chapter provides supplemental information that might help you with the setup.

For information about positioning your cable data gateway, see *Position Your WiFi Cable Data Gateway* on page 20.

Hardware Features of the AC1900 WiFi Cable Data Gateway

This section describes the physical aspects of the AC1900 WiFi Cable Data Gateway, Model C6300BD. This model supports 802.11ac, provides radios for both the 2.4 GHz and 5 Ghz band, and can support WiFi throughput of up to 1900 Mbps.

Front Panel of the AC1900 WiFi Cable Data Gateway

The front panel contains control buttons and status LEDs. Use the LEDs to verify status and connections.

Note: For optimal performance, keep the cable data gateway vertical in the stand and do not detach the stand. Do not mount this unit to a wall; it is not suitable for wall mounting.

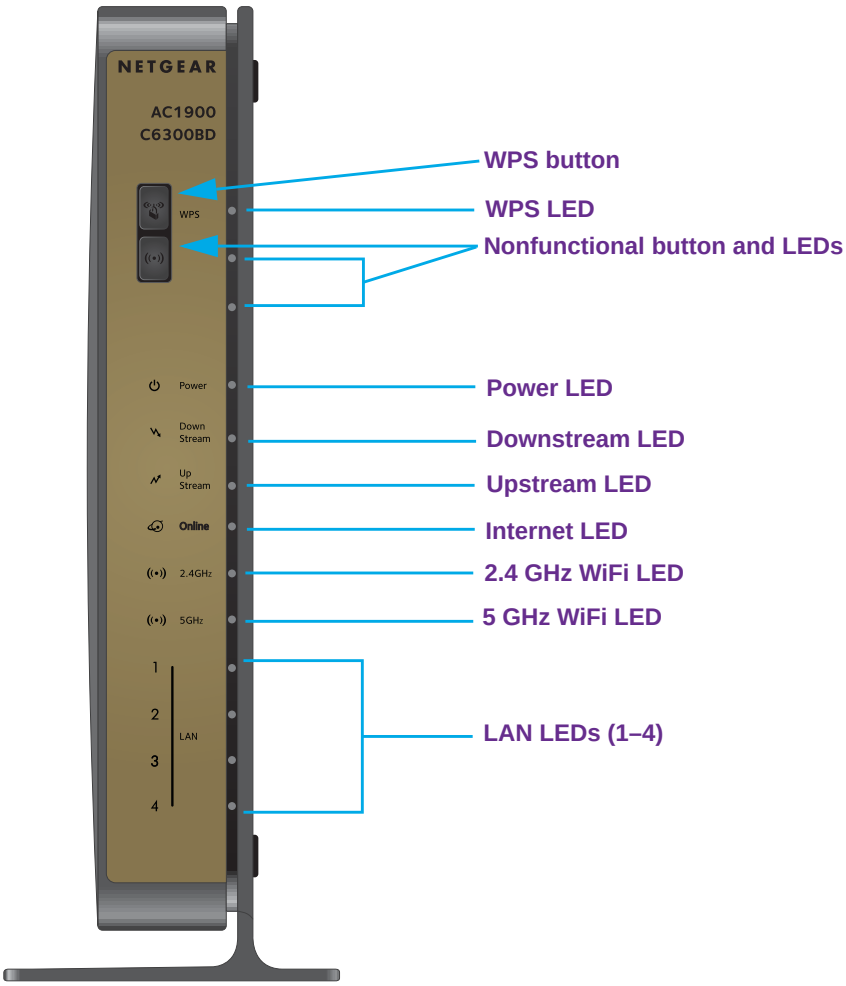


Figure 1. Front panel LEDs and buttons of the AC1900

You can use the LEDs to verify status and connections. The following table lists and describes each LED and the WPS button on the front panel.

Table 1. Front panel LEDs and button of the AC1900

LED	Icon	Description
WPS button and LED		Press the **WPS** button to open a two-minute window for the cable data gateway to connect with other WPS-enabled devices. The WPS LED blinks green during this two-minute period. For more information about using the WPS method to implement WiFi security, see the following sections: • *Join the WiFi Network of the WiFi Cable Data Gateway* on page 26 • *Use the WPS Wizard to Add a Device to the WiFi Network* on page 52

Table 1. Front panel LEDs and button of the AC1900 (continued)

LED	Icon	Description
Power		• **Solid green**. The gateway is receiving power. • **Blinking green**. The gateway is powering on. • **Solid red**. The gateway is performing a self-test or the thermal cutoff circuit was triggered. **Note:** **Off**. The gateway is not receiving power.If the Power LED lights red or blinks red at any other time than while booting, see *Troubleshoot with the LEDs* on page 155.
Downstream		• **Solid blue**. More than one downstream channel is locked. • **Solid green**. One downstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for a downstream channel. • **Off**. No downstream channel is locked.
Upstream		• **Solid blue**. More than one upstream channel is locked. • **Solid green**. One upstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for an upstream channel. • **Off**. No upstream channel is locked.
Online		• **Solid green**. The cable data gateway is connected to the Internet. • **Slow blinking green**. The cable data gateway is receiving DHCP information from the cable provider's cable modem termination system (CMTS). • **Fast blinking green**. The cable data gateway is downloading a configuration file from the cable provider's CMTS. • **Off**. The cable data gateway is not connected to the Internet. **Note:** The Online LED is also referred to as the Internet LED.
2.4 GHz WiFi		• **Solid green**. The 2.4 GHz WiFi radio is functioning and available for use. • **Blinking green**. The 2.4 GHz WiFi radio is processing traffic. • **Off**. The 2.4 GHz WiFi radio is disabled. (If the radio is disabled, see *Control the WiFi Radios* on page 109.)
5 GHz WiFi		• **Solid green**. The 5 GHz WiFi radio is functioning and available for use. • **Blinking green**. The 5 GHz WiFi radio is processing traffic. • **Off**. The 5 GHz WiFi radio is disabled. (If the radio is disabled, see *Control the WiFi Radios* on page 109.)
LAN		The type of Ethernet connection determines the LED color: • A green LED indicates a 1,000 Mbps connection. • An amber LED indicates a 100/10 Mbps connection. The LED functions are as follows: • **Solid green or amber**. The Ethernet port is connected to a powered-on device. • **Blinking green or amber**. Data is being transmitted or received on the Ethernet port. • **Off**. The Ethernet port does not detect a powered-on device.

Back Panel of the AC1900 WiFi Cable Data Gateway

The back panel contains ports, connectors, and a recessed button.

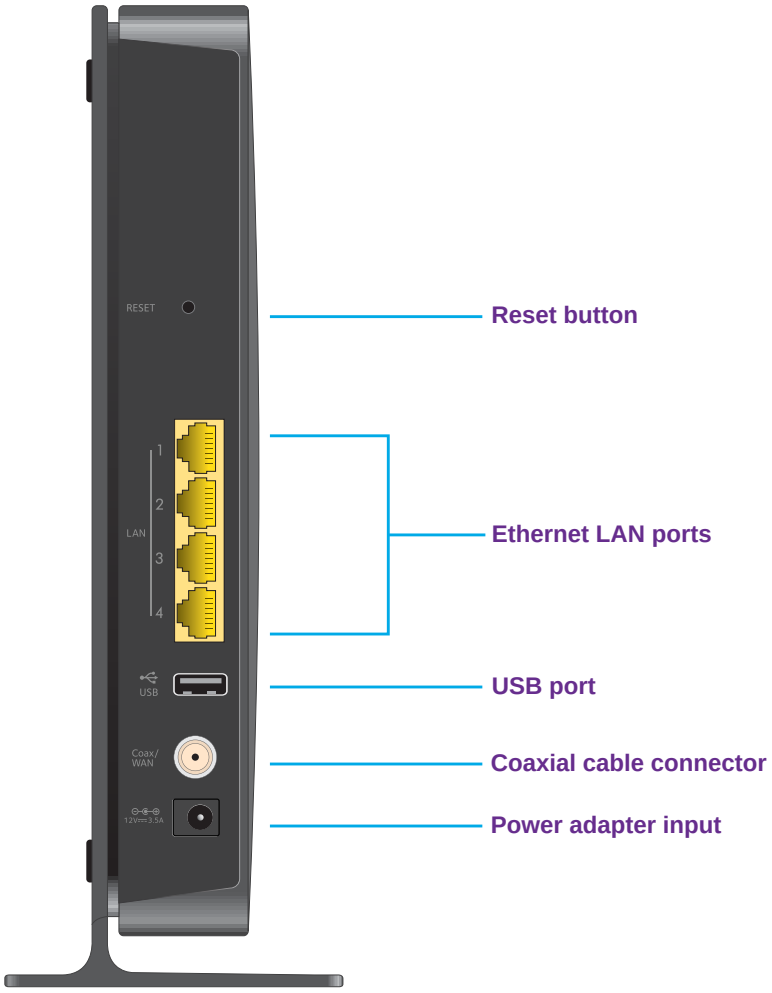


Figure 2. Back panel connections and button of the AC1900

The back panel includes the following components, viewed from top to bottom:

- **Recessed Reset button**. To set the gateway to the original factory settings, press and hold the **Reset** button for at least seven seconds. For more information, see *Return the WiFi Cable Data Gateway to Its Factory Default Settings* on page 94.
- **Four 10/100/1000 Mbps Ethernet LAN ports**. Use these ports to connect local computers to the Ethernet LAN of the cable data gateway.
- **USB port**. The USB 2.0 port lets you connect a USB hard drive or flash drive to the cable data gateway.
- **Coaxial cable connector**. Attach a coaxial cable to the cable service provider's connection.
- **Power input connector**. Attach the power adapter cable to this input.

Product Label of the AC1900 WiFi Cable Data Gateway

The label on side panel of the cable data gateway shows the login information, MAC address, serial number, WiFi network names, and WiFi password (key).

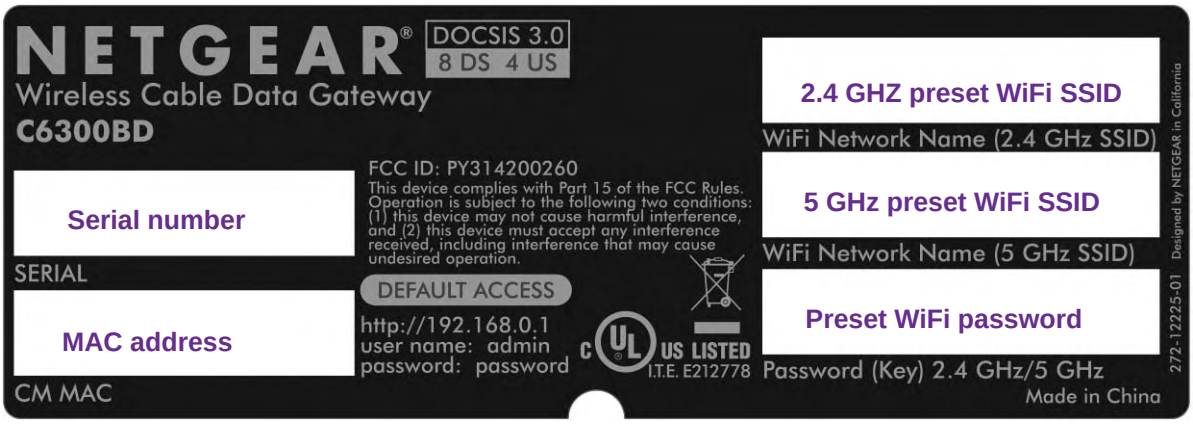


Figure 3. Product label of the AC1900

Hardware Features of the N900 WiFi Cable Data Gateway

This section describes the physical aspects of the N900 WiFi Cable Data Gateway, Model CG4500BD. This model provides radios for both the 2.4 GHz and 5 Ghz band and can support WiFi throughput of up to 900 Mbps.

Front Panel of the N900 WiFi Cable Data Gateway

The front panel contains control buttons and status LEDs. Use the LEDs to verify status and connections.

Note: For optimal performance, keep the cable data gateway vertical in the stand and do not detach the stand. Do not mount this unit to a wall; it is not suitable for wall mounting.

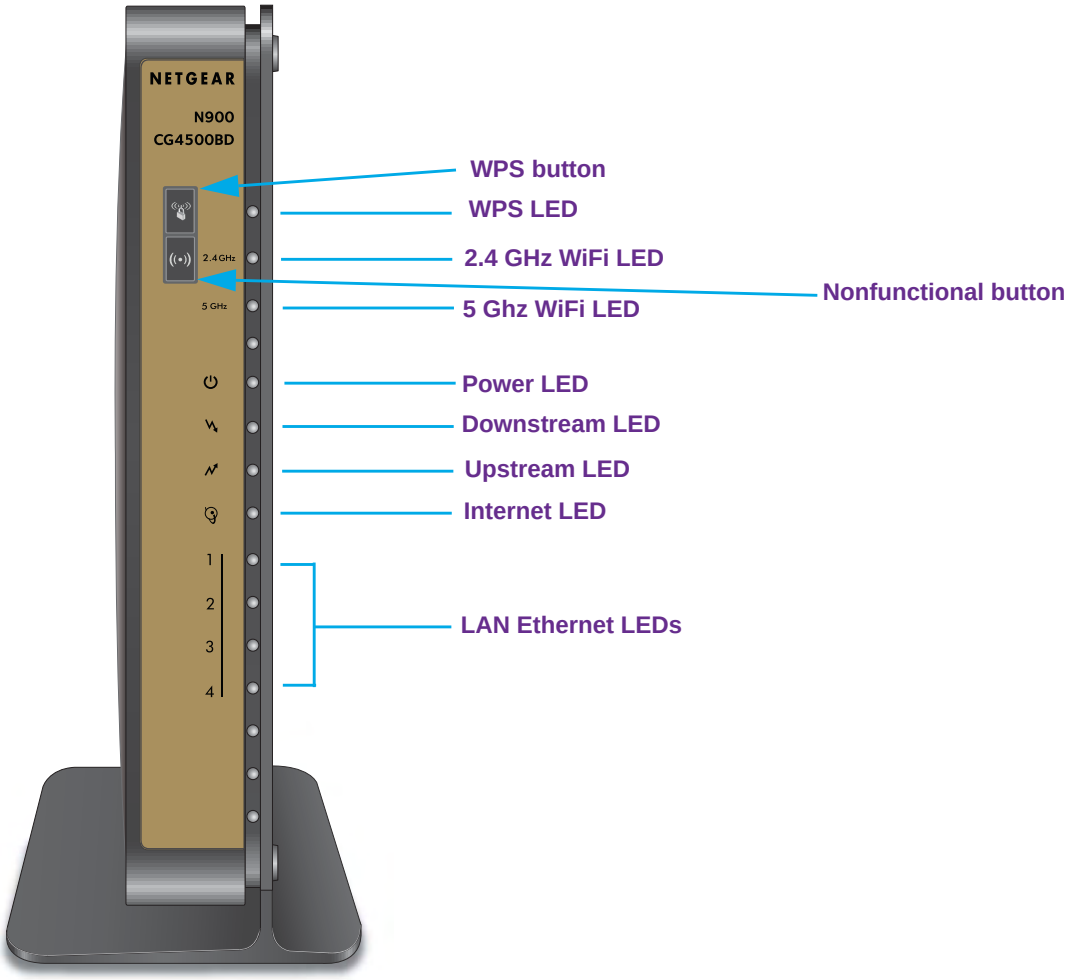


Figure 4. Front panel buttons and LEDs of the N900

You can use the LEDs to verify status and connections. The following table lists and describes each LED and the WPS button on the front panel.

Table 2. LEDs and front panel buttons of the N900

LED	Icon	Description
WPS button and LED		Press the **WPS** button to open a two-minute window for the cable data gateway to connect with other WPS-enabled devices. The WPS LED blinks green during this two-minute period. For more information about using the WPS method to implement WiFi security, see the following sections: • *Join the WiFi Network of the WiFi Cable Data Gateway* on page 26 • *Use the WPS Wizard to Add a Device to the WiFi Network* on page 52
2.4 GHz WiFi		• **Solid green**. The 2.4 GHz WiFi radio is functioning and available for use. • **Blinking**. The 2.4 GHz WiFi radio is processing traffic. • **Off**. The 2.4 GHz WiFi radio is disabled. (If the radio is disabled, see *Control the WiFi Radios* on page 109.)

Table 2. LEDs and front panel buttons of the N900 (continued)

LED	Icon	Description
5 GHz WiFi		• **Solid green**. The 5 GHz WiFi radio is functioning and available for use. • **Blinking**. The 5 GHz WiFi radio is processing traffic. • **Off**. The 5 GHz WiFi radio is disabled. (If the radio is disabled, see *Control the WiFi Radios* on page 109.)
Power		• **Solid green**. The gateway is receiving power. • **Blinking green**. The gateway is powering on. • **Blinking red**. The cable data gateway is performing a self-test or the thermal cutoff circuit was triggered. • **Off**. The cable data gateway is not receiving power. **Note:** If the Power LED lights red or blinks red at any other time than while booting, see *Troubleshoot with the LEDs* on page 155.
Downstream		• **Solid blue**. More than one downstream channel is locked. • **Solid green**. One downstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for a downstream channel. • **Off**. No downstream channel is locked.
Upstream		• **Solid blue**. More than one upstream channel is locked. • **Solid green**. One upstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for an upstream channel. • **Off**. No upstream channel is locked.
Internet		• **Solid green**. The cable data gateway is connected to the Internet. • **Slow blinking green**. The cable data gateway is receiving DHCP information from the cable provider's cable modem termination system (CMTS). • **Fast blinking green**. The cable data gateway is downloading a configuration file from the cable provider's CMTS. • **Off**. The cable data gateway is not connected to the Internet.
LAN		The type of Ethernet connection determines the LED color: • A green LED indicates a 1,000 Mbps connection. • An amber LED indicates a 100/10 Mbps connection. The LED functions are as follows: • **Solid green or amber**. The Ethernet port is connected to a powered-on device. • **Blinking green or amber**. Data is being transmitted or received on the Ethernet port. • **Off**. The Ethernet port does not detect a powered-on device.

Back Panel of the N900 WiFi Cable Data Gateway

The back panel contains ports, connectors, and a recessed button.

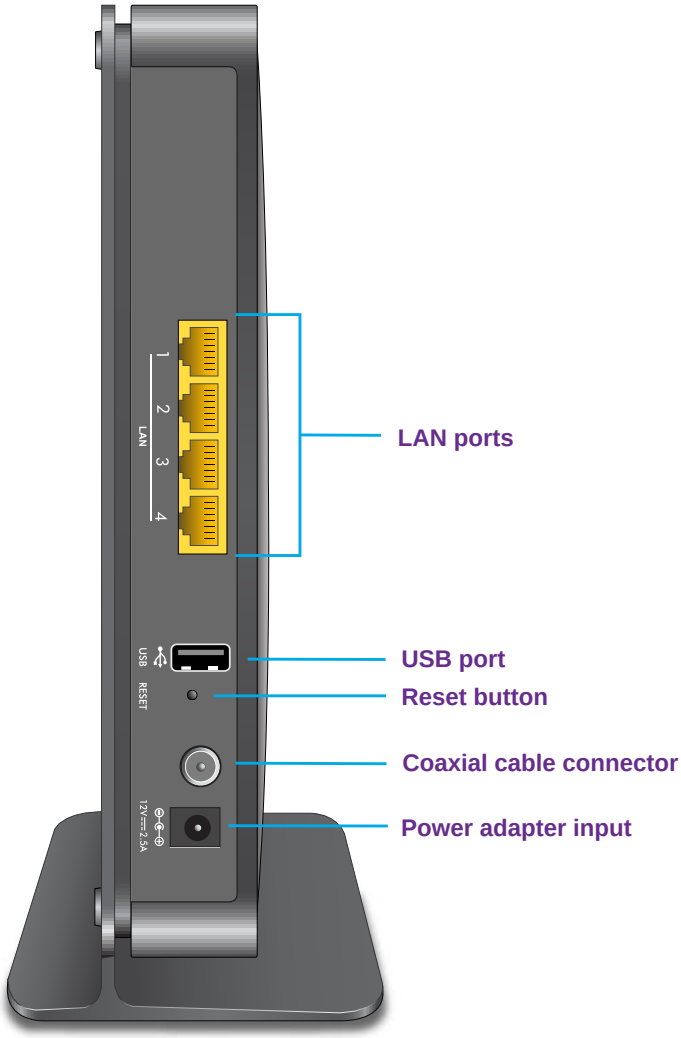


Figure 5. Back panel connections and button of the N900

The back panel includes the following components, viewed from top to bottom:

- **Four 10/100/1000 Mbps Ethernet LAN ports**. Use these ports to connect local computers to the Ethernet LAN of the cable data gateway.
- **USB port**. The USB 2.0 port lets you connect a USB hard drive or flash drive to the cable data gateway.
- **Recessed Reset button**. To set the gateway to the original factory settings, press and hold the **Reset** button for at least seven seconds. For more information, see *Return the WiFi Cable Data Gateway to Its Factory Default Settings* on page 94.
- **Coaxial cable connector**. Attach a coaxial cable to the cable service provider's connection.
- **Power input connector**. Attach the power adapter cable to this input.

Product Label of the N900 WiFi Cable Data Gateway

The label on the side panel of the cable data gateway shows the login information, MAC address, serial number, WiFi network names, and WiFi password (key).

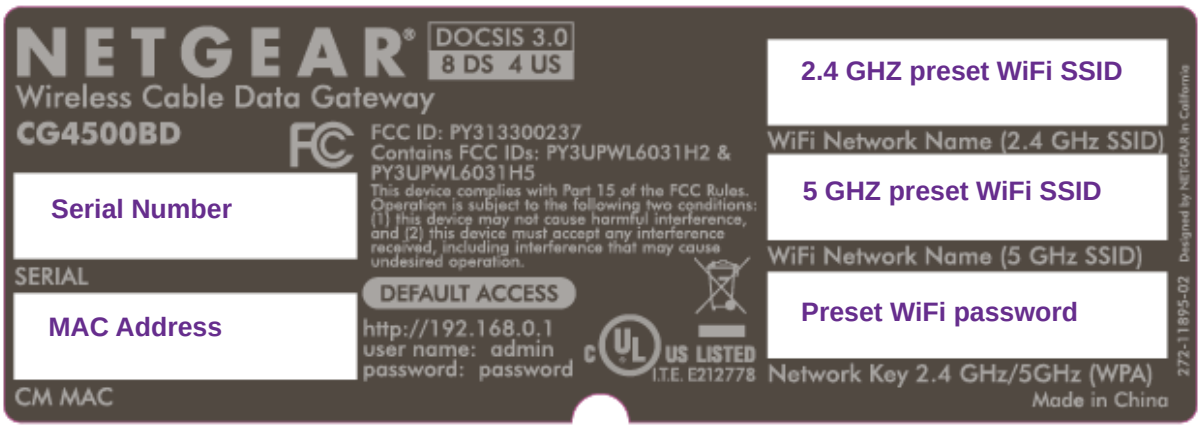


Figure 6. Product label of the N900

Hardware Features of the N450 WiFi Cable Data Gateway

This section describes the physical aspects of the N450 WiFi Cable Data Gateway, Model CG3000Dv2. This model provides one radio for the 2.4 GHz band and can support WiFi throughput of up to 450 Mbps.

Note: For optimal performance, keep the cable data gateway vertical in the stand and do not detach the stand. Do not mount this unit to a wall; it is not suitable for wall mounting.

Front Panel of the N450 WiFi Cable Data Gateway

The front panel contains control buttons, status LEDs, and a USB 2.0 port. Use the USB port to connect a USB hard drive or flash drive to the cable data gateway. Use the LEDs to verify status and connections.

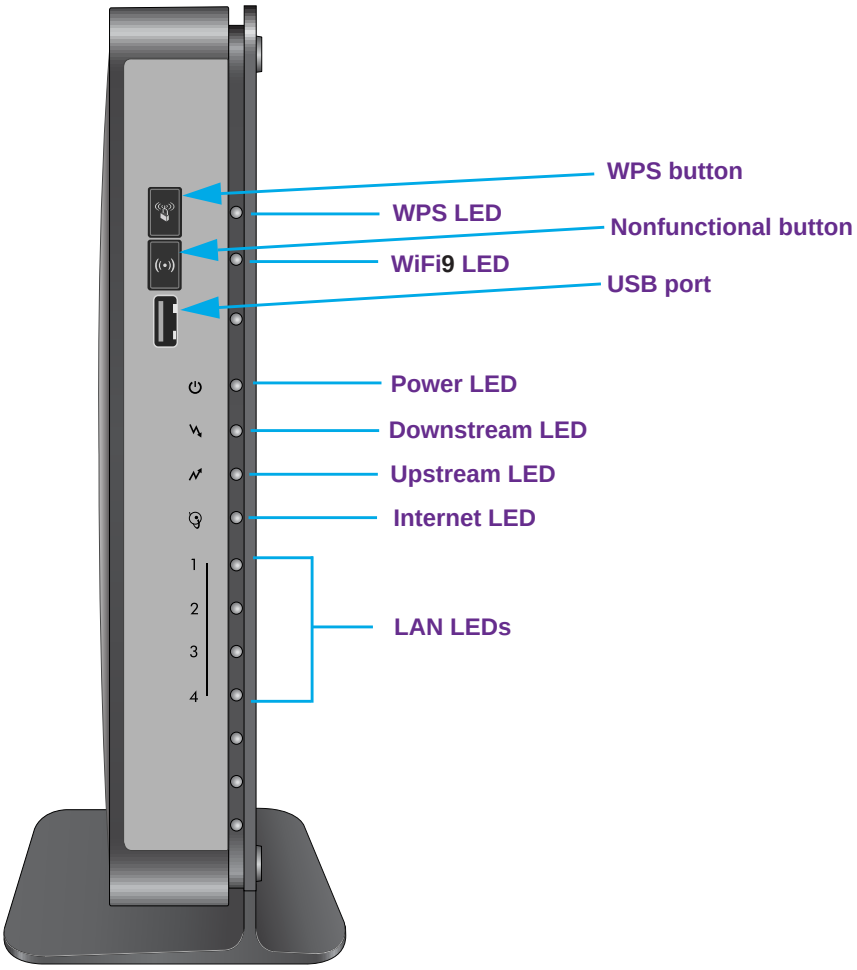


Figure 7. Front panel buttons and LEDs of the N450

You can use the LEDs to verify status and connections. The following table lists and describes each LED and button on the front panel.

Table 3. LEDs and front panel buttons of the N450

LED	Icon	Description
WiFi LED		• **Solid green**. The WiFi radio is functioning and available for use. • **Blinking green**. The WiFi radio is processing traffic. • **Off**. The WiFi radio is disabled. (If the radio is disabled, see *Control the WiFi Radios* on page 109.) **Note:** The WiFi button is disabled for this product.
WPS button and LED		Press the **WPS** button to open a two-minute window for the cable data gateway to connect with other WPS-enabled devices. The WPS LED blinks green during this two-minute period. For more information about using the WPS method to implement WiFi security, see the following sections: • *Join the WiFi Network of the WiFi Cable Data Gateway* on page 26 • *Use the WPS Wizard to Add a Device to the WiFi Network* on page 52

Table 3. LEDs and front panel buttons of the N450 (continued)

LED	Icon	Description
Power		• **Solid green**. The cable data gateway is receiving power. • **Blinking green**. The cable data gateway is powering on. • **Blinking red**. The cable data gateway is performing a self-test or the thermal cutoff circuit was triggered. • **Off**. The cable data gateway is not receiving power. **Note:** If the Power LED lights red or blinks red at any other time than while booting, see *Troubleshoot with the LEDs* on page 155.
Downstream		• **Solid blue**. More than one downstream channel is locked. • **Solid green**. One downstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for a downstream channel. • **Off**. No downstream channel is locked.
Upstream		• **Solid blue**. More than one upstream channel is locked. • **Solid green**. One upstream channel is locked (channel bonding does not occur). • **Blinking green**. The cable data gateway is scanning for an upstream channel. • **Off**. No upstream channel is locked.
Internet		• **Solid green**. The cable data gateway is connected to the Internet. • **Slow blinking green**. The cable data gateway is receiving DHCP information from the cable provider's cable modem termination system (CMTS). • **Fast blinking green**. The cable data gateway is downloading a configuration file from the cable provider's CMTS. • **Off**. The cable data gateway is not connected to the Internet.
LAN		The type of Ethernet connection determines the LED color: • A green LED indicates a 1,000 Mbps connection. • An amber LED indicates a 100/10 Mbps connection. The LED functions are as follows: • **Solid green or amber**. The Ethernet port is connected to a powered-on device. • **Blinking green or amber**. Data is being transmitted or received on the Ethernet port. • **Off**. The Ethernet port does not detect a powered-on device.

Back Panel of the N450 WiFi Cable Data Gateway

The back panel contains ports, connectors, and a recessed button.

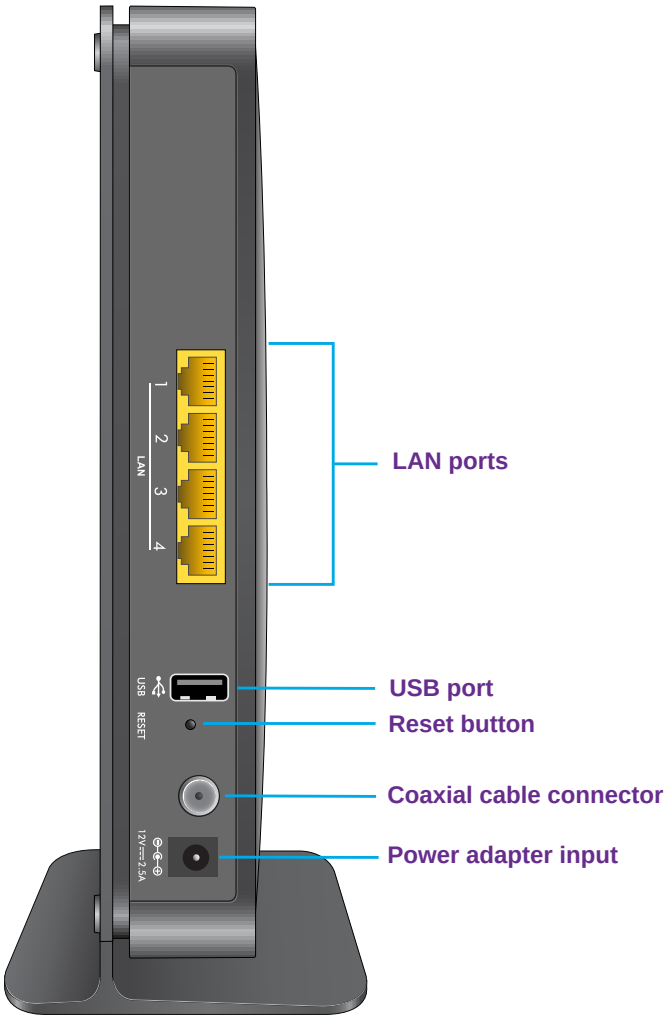


Figure 8. Back panel connections and button of the N450

The back panel includes the following components, viewed from top to bottom:

- **Four 10/100/1000 Mbps Ethernet LAN ports**. Use these ports to connect local computers to the Ethernet LAN of the cable data gateway.
- **USB port**. A second USB 2.0 port lets you connect a USB hard drive or flash drive to the cable data gateway. (The first USB 2.0 port is on the front panel.)
- **Recessed Reset button**. To set the gateway to the original factory settings, press and hold the **Reset** button for at least seven seconds. For more information, see *Return the WiFi Cable Data Gateway to Its Factory Default Settings* on page 94.
- **Coaxial cable connector**. Attach a coaxial cable to the cable service provider's connection.
- **Power input connector**. Attach the power adapter cable to this input.

Product Label of the N450 WiFi Cable Data Gateway

The label on the side panel of the cable data gateway shows the login information, WiFi network name, WiFi password (key), serial number, and MAC address.

Figure 9. Product label of the N450

Position Your WiFi Cable Data Gateway

The cable data gateway lets you access your network from anywhere within the operating range of your WiFi network. However, the operating distance or range of your WiFi connection can vary significantly depending on the physical placement of your cable data gateway. For example, the thickness and number of walls the WiFi signal passes through can limit the range.

For best results, place your cable data gateway according to the following guidelines:

- Place your cable data gateway on an upper floor of a multifloor home or office.
- Place your cable data gateway near the center of the area where your computers and other devices operate, and within line of sight to your WiFi devices.
- Make sure that the cable data gateway is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the cable data gateway in an elevated location, minimizing the number walls and ceilings between the cable data gateway and your other devices.
- Place the cable data gateway away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz cordless phone

- Place the cable data gateway away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal doors
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete

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).

2. Connect and Get Started

This chapter describes how to use NETGEAR genie to connect to the cable data gateway and get started.

This chapter contains the following sections:

WiFi Cable Data Gateway Setup Requirements

The cable data gateway comes with a default configuration. If you want to change from the default configuration, you can use the NETGEAR genie menus and screens to set up your cable data gateway manually. However, before you start the setup process, you need your cable service provider information available.

Use Standard TCP/IP Properties for DHCP

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

WiFi Devices and Security Settings

Make sure that the WiFi device or computer that you are using supports WPA or WPA2 WiFi security, which is the WiFi security supported by the cable data gateway. Best practice is to use WPA2-AES security for your network.

Types of Logins and Access

The cable data gateway supports separate types of logins that serve different purposes. It is important that you understand the difference so that you know which of the following logins to use when:

- **Cable modem router login**. This login logs you in to the cable data gateway interface from NETGEAR genie. For more information, see *Access NETGEAR genie* on page 23.
- **WiFi network key or password**. Your cable data gateway is preset with a unique WiFi network name (SSID) and password for WiFi access. This information is on the product label. For more information, see *Join the WiFi Network of the WiFi Cable Data Gateway* on page 26.

Access NETGEAR genie

NETGEAR genie runs on any device with a web browser.

Note: For information about installing the cable data gateway, see the installation guide that came in the product package. You can also download the installation guide from *downloadcenter.netgear.com*.

The following procedure assumes that you installed the cable data gateway and that your computer or another device is connected with an Ethernet cable or over WiFi with the preset security settings that are listed on the product label.

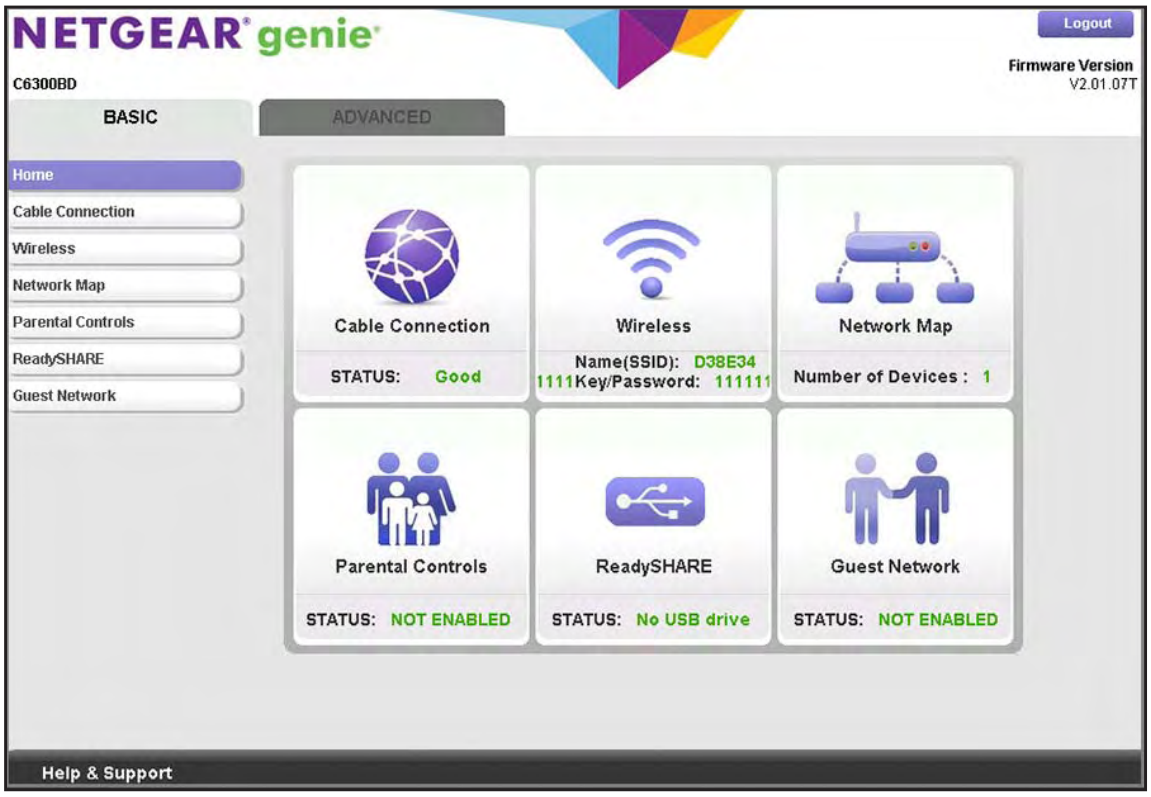
➢ **To access NETGEAR genie to set up your cable data gateway:**

1. Apply power to the cable data gateway.
2. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
3. In the address field of your browser, type **http://routerlogin.net** (or **http://192.168.0.1**).

   The login screen displays. You are prompted to enter a user name and password.

4. Type **admin** for the user name and **password** for the password.
5. Click the **OK** button.

   The NETGEAR genie BASIC Home screen displays. The following figure shows the screen for the AC1900 WiFi Cable Data Gateway, Model C6300BD.



The cable data gateway BASIC Home screen provides a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the sections of the dashboard to view more detailed information. The left column provides the menus, and at the top is an ADVANCED tab that you can use to access more menus and screens.

If you cannot log in to the cable data gateway or your browser does not display the NETGEAR genie screen, check the following:

- Make sure that the computer is connected to one of the four LAN Ethernet ports or over WiFi to the cable data gateway.
- Make sure that your browser does not cache the previous page by closing and reopening the browser.
- If your computer is set to a static or fixed IP address (this type of setting is uncommon), change the setting to obtain an IP address automatically from the cable data gateway (see *Manage the Internet Setup* on page 42).

For more troubleshooting information, see *Cannot Log In to the Cable Data Gateway* on page 157.

Change the Password

The user name to access the cable data gateway is admin, and its default password is password. Best practise is that you set a more secure password.

A secure password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. The password must contain at least 4 characters and can contain a maximum of 15 characters.

Note: This change of password is not the same as changing the password (key) for WiFi access. The product label shows your unique WiFi network name (SSID) and password for WiFi access.

➢ **To change the password for the cable data gateway:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

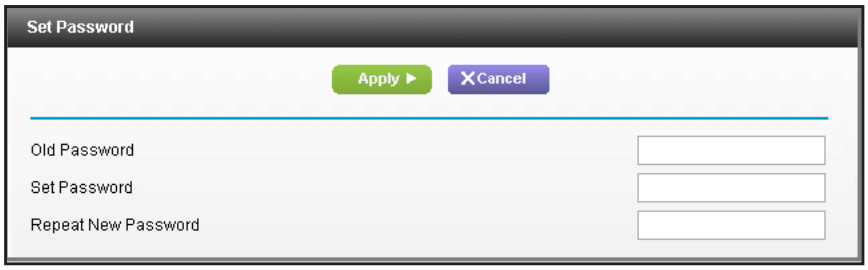
   You are prompted to enter a user name and password.
3. Type **admin** for the user name and **password** for the password.

   If you already changed the password and want to change it again, type your personalized password.
4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Set Password screen displays.



6. Type the old password.
7. Type the new password twice.
8. Click the **Apply** button.

   Your settings are saved.

Join the WiFi Network of the WiFi Cable Data Gateway

Choose either the manual or the WPS method to add a WiFi device such as a computer, iPhone, iPad, or gaming device to the WiFi network of the cable data gateway.

Manual Method

➢ **To connect a device manually to the WiFi network of the cable data gateway:**

1. On the WiFi device that you want to connect to your cable data gateway, open the software application that manages your WiFi connections.

   This software scans for all WiFi 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 on the product label.

3. Enter the cable data gateway password.

   The default WiFi password (also referred to as passphrase or key) is on the product label.

4. Click the **Connect** button.

   The device connects to the WiFi network of the cable data gateway.

Wi-Fi Protected Setup 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 (Push 'N' Connect), make sure that all WiFi 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 cable data gateway so that every device in the network supports the same security settings.

➢ **To use WPS to connect a device to the WiFi network of the cable data gateway:**

1. Press the **WPS** button on the front panel of the cable data gateway.
2. Within two minutes, press the **WPS** button on your WiFi device, or follow the WPS instructions that came with the device.

   The WPS process automatically sets up the device with the network password and connects the device to the WiFi network of the cable data gateway.

   For more information, see *Use the WPS Wizard to Add a Device to the WiFi Network* on page 52.

Configure Parental Controls and Basic WiFi Settings

3

This chapter describes how to configure the basic settings such as parental controls, the basic WiFi network, and the guest WiFi network.

This chapter contains the following sections:

- *Set Up Parental Controls*
- *View or Change the Basic Settings for the Main WiFi Network*
- *Enable and Configure the Guest WiFi Network*

For information about other settings that display on the BASIC menu of the web management interface, see the following sections or chapters:

- For information about viewing the cable initiation, see *View the WiFi Cable Data Gateway Cable Initialization* on page 86.
- For information about changing the cable connection starting frequency, see *Port Forwarding and Port Triggering Concepts* on page 117.
- For information about viewing the network map, see *View the Network Map* on page 87.
- For information about using ReadySHARE, see *Chapter 7, Share USB Drives Attached to the Cable Data Gateway*.

Set Up Parental Controls

The first time that you select **Parental Controls** from the BASIC Home screen, your browser goes to the *Parental Controls* website. You can learn more about Parental Controls or download the application.

Figure 10. Parental Controls website

➢ **To set up parental controls:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

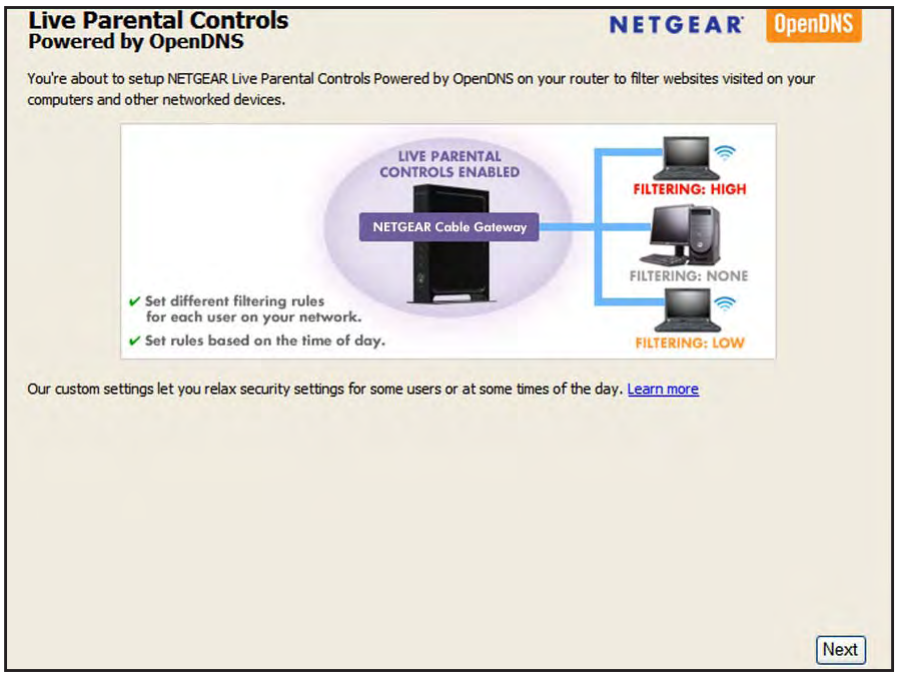
   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **BASIC > Parental Controls**.

   The *Parental Controls* website opens.
6. Click the button for the app or version that you want to download and use.

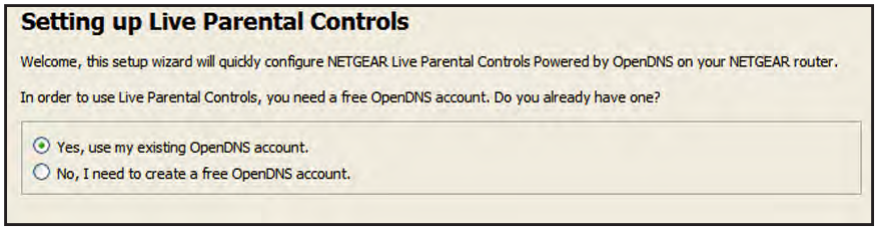
7. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management utility.

   After installation, Live Parental Controls automatically starts.



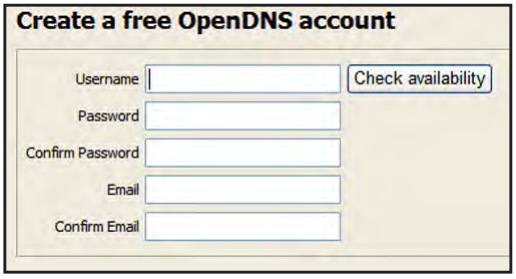
8. Click the **Next** button, read the note, and click the **Next** button again.

   Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.



9. Select a radio button as follows:
   - If you already own an OpenDNS account, leave the **Yes** radio button selected.
   - If you do not own an OpenDNS account, select the **No** radio button.

     If you are creating an account, the following screen displays:



a. Complete the fields.
b. Click the **Next** button.

After you log on or create your account, the filtering level screen displays:

10. Select the radio button for the filtering level that you want and click the **Next** button.

    The Setup is complete screen displays.

11. Click the **Take me to the status screen** button.

    Parental controls are now set up for the cable data gateway. The dashboard shows Parental Controls as Enabled.

View or Change the Basic Settings for the Main WiFi Network

You can view or configure the WiFi network setup.

The cable data gateway 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 product label (see *Chapter 1, Hardware Overview*).

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

Note: Best practice is not to change your preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store the note in a safe place where you can easily find it.

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

➢ **To view or change basic WiFi settings for main WiFi network:**

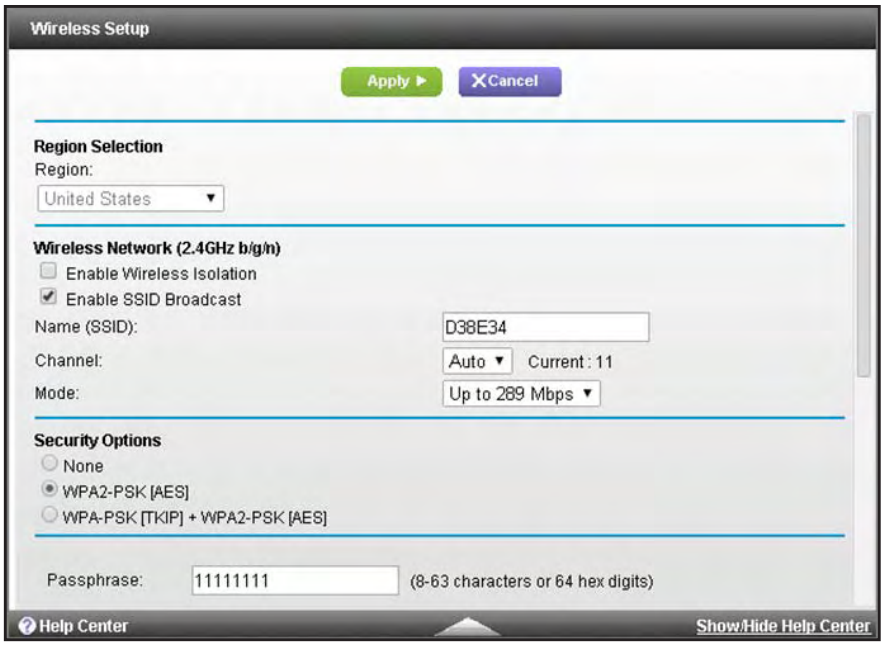
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **BASIC > Wireless**.

   The Wireless Setup screen displays.



6. View or change the basic WiFi settings.

   The following table describes the fields on the basic Wireless Setup screen.

Field	Description
Region Selection	
Region	The selection from the **Region** menu is **United States**. You cannot change this selection.
Wireless Network (2.4GHz b/g/n)	
Enable Wireless Isolation	By default, WiFi clients that are connected to the 2.4 GHz WiFi band of the main WiFi network can access each other and Ethernet devices that are connected to the main WiFi network. As an additional security measure, you can prevent WiFi devices from doing so by selecting the **Enable Wireless Isolation** check box.
Enable SSID Broadcast	By default, the cable data gateway broadcasts its SSID of the 2.4 GHz WiFi band so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 2.4 GHz WiFi band, clear the **Enable SSID Broadcast** check box.
Name (SSID)	The SSID is the 2.4 GHz WiFi band name. If you did not change the SSID, the default SSID displays. The default SSID for the 2.4 GHz WiFi band is also printed on the product label. Best practise is not to change the default SSID. If you must change the SSID, enter a 32-character (maximum), case-sensitive name in this field.
Channel	From the **Channel** menu, select **Auto** for automatic channel selection for the 2.4 GHz WiFi band, or select an individual channel. The default selection is **Auto**. **Note:** 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.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Mode</td><td>From the Mode menu, select one of the following modes for the 2.4 GHz WiFi band:
Up to 54 Mbps. Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to function at up to 54 Mbps.
Up to 289 Mbps. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to function at up to 289 Mbps. This mode is the default mode.
The available performance mode (that is, the highest possible mode on the cable data gateway) depends on the model:
Models N900 and N450:
Up to 450 Mbps. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11n devices to function at up to 450 Mbps.
Model AC1900:
Up to 600 Mbps. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11n devices to function at up to 600 Mbps.</td></tr>
<tr><td colspan="2">Security Options</td></tr>
<tr><td colspan="2">Note: Best practise is not to change your preset security settings (WPA-PSK [TKIP] + WPA2-PASK [AES]).

If you must change the WiFi security, select one of the following WiFi security options for the 2.4 GHz band of the main WiFi network:
None. An open WiFi network that does not provide any security. Any WiFi device can join the 2.4 GHz band of the main WiFi network. Because of complete lack of security, best practise is not to use an open main WiFi network.
WPA2-PSK [AES]. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select this mode to allow 802.11n devices to connect to the 2.4 GHz band of the main WiFi network at the fastest speed.
To use this type of security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the main WiFi network, a user must enter this passphrase.
WPA-PSK [TKIP] + WPA2-PASK [AES]. This type of security is the default setting and enables WiFi devices that support either WPA or WPA2 to join the cable data gateway's WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is also printed on the product label.
Best practise is not to change the default passphrase. If you must change the passphrase, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the main WiFi network, a user must enter this passphrase.</td></tr>
<tr><td>Passphrase</td><td>The passphrase that provides users access to the main WiFi network in the 2.4 GHZ band. The passphrase is also referred to as password or key.</td></tr>
</table>

Field	Description
Wireless Network (5GHz a/n/ac) **Note:** Models AC1900 and N900 support the 5 Ghz band. Model N450 does not.	
Enable Wireless Isolation	By default, WiFi clients that are connected to the 5 GHz WiFi band of the cable data gateway can access each other and Ethernet devices that are connected to the cable data gateway. As an additional security measure, you can prevent WiFi from doing so by selecting the **Enable Wireless Isolation** check box.
Enable SSID Broadcast	By default, the cable data gateway broadcasts its SSID of the 5 GHz WiFi band so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 5 GHz WiFi band, clear the **Enable SSID Broadcast** check box.
Name (SSID)	The SSID is the 5 GHz WiFi band name. If you did not change the SSID, the default SSID displays. The default SSID for the 5 GHz WiFi band is also printed on the product label. Best practise is not to change the default SSID. If you must change the SSID, enter a 32-character (maximum), case-sensitive name in this field.
Channel	From the **Channel** menu, select **Auto** for automatic channel selection for the 5 GHz WiFi band, or select an individual channel. The default selection is **Auto**. **Note:** 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	From the **Mode** menu, select one of the following modes for the 5 GHz WiFi band. The available mode depends on the model: • **Model N900**: - **Up to 289 Mbps**. Legacy mode. This mode allows 802.11na and 802.11a devices to join the network but limits 802.11na devices to function at up to 289 Mbps. - **Up to 450 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11naand 802.11a devices to join the network but limits 802.11na devices to function at up to 450 Mbps. - **Up to 600 Mbps**. Performance mode. This mode allows 802.11na and 802.11a devices to join the network and allows 802.11na devices to function at up to 600 Mbps. This mode is the default mode. • **Model AC1900**: - **Up to 289 Mbps**. Legacy mode. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network but limits 802.11ac and 802.11na devices to function at up to 289 Mbps. - **Up to 600 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network, allows 802.11na devices to function at up to 600 Mbps, but limits 802.11ac devices to function at up to 600 Mbps. - **Up to 1300 Mbps**. Performance mode. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network and allows 802.11ac devices to function at up to 1300 Mbps. This mode is the default mode.

Field	Description
Security Options	
Note: Best practise is not to change your preset security settings (WPA-PSK [TKIP] + WPA2-PASK [AES]). If you must change the WiFi security, select one of the following WiFi security options for the 5 GHz band of the main WiFi network: • **None**. An open WiFi network that does not provide any security. Any WiFi device can join the 5 GHz band of the main WiFi network. Because of complete lack of security, best practise is not to use an open main WiFi network. • **WPA2-PSK [AES]**. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select this mode to allow 802.11n devices to connect to the 5 GHz band of the main WiFi network at the fastest speed. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the main WiFi network, a user must enter this passphrase. • **WPA-PSK [TKIP] + WPA2-PASK [AES]**. This type of security is the default setting and enables WiFi devices that support either WPA or WPA2 to join the 5 GHz band of the main WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is also printed on the product label. Best practise is not to change the default passphrase. If you must change the passphrase, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the main WiFi network, a user must enter this passphrase.	
Passphrase	The passphrase that provides users access to the main WiFi network in the 5 GHZ band. The passphrase is also referred to as password or key.

7. If you changed the settings, click the **Apply** button.

   Your settings are saved.

8. Set up and test your WiFi devices and computers to make sure that they can connect over WiFi.

   If they do not, check the following:

   - Is your WiFi device connected to your network or another WiFi network in your area? Some WiFi devices automatically connect to the first open network (without WiFi security) that they discover.
   - Does your WiFi device display in the network map? (See *View the Network Map* on page 87.) If it does, it is connected to the network.
   - Do you use the correct network name (SSID) and password? The default SSID and default password are on the product label.

Enable and Configure the Guest WiFi Network

By default, the guest WiFi network is disabled. You can enable and configure the guest WiFi network.

The WiFi mode of the guest WiFi network depends on the WiFi mode of the main WiFi network. For example, if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band, the guest WiFi network also functions in the Up to 54 Mbps

mode in the 2.4 GHz band. For information about configuring the WiFi mode, see *View or Change the Basic Settings for the Main WiFi Network* on page 31.

➢ **To enable and configure the settings for the guest WiFi network:**

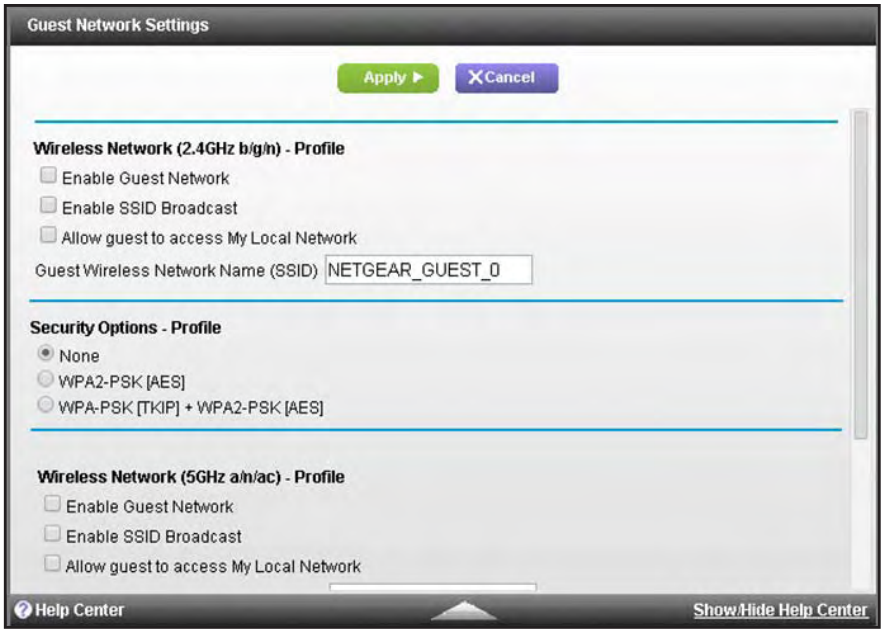
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **BASIC > Guest Network**.

   The Guest Network Settings screen displays.



6. Enable the guest network and configure its WiFi settings.

   The following table describes the fields on the Guest Network Settings screen.

Field	Description
Wireless Network (2.4GHz b/g/n)	
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 2.4 GHz WiFi band, select the **Enable Guest Network** check box.

Field	Description
Enable SSID Broadcast	By default, the cable data gateway broadcasts its SSID of the 2.4 GHz WiFi band so WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 2.4 GHz WiFi band for the guest WiFi network, clear the **Enable SSID Broadcast** check box.
Allow guest to access My Local Network	By default, WiFi clients that are connected to the 2.4 GHz WiFi band of guest WiFi network cannot access WiFi devices and Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the **Allow guest to access My Local Network** check box.
Guest Wireless Network Name (SSID)	The SSID is the 2.4 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR_GUEST_0. (This name is same as the default SSID for the 5 GHz band of the guest WiFi network.) If you want to change the SSID in the 2.4 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
Security Options Profile	
If you want to change the WiFi security, select one of the following WiFi security options for the 2.4 GHz band of the guest WiFi network: • **None**. An open WiFi network that does not provide any security. Any WiFi device can join the 2.4 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network. • **WPA2-PSK [AES]**. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select this mode to allow 802.11n devices to connect to the 2.4 GHz band of the guest WiFi network at the fastest speed. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase. • **WPA-PSK [TKIP] + WPA2-PASK [AES]**. This type of security is the default setting and enables WiFi devices that support either WPA or WPA2 to join the 2.4 GHz band of the guest WiFi network. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase.	
Security Options	
Passphrase	The passphrase that provides users access to the guest WiFi network in the 2.4 GHZ band. The passphrase is also referred to as password or key.

Field	Description
Wireless Network (5GHz a/n/ac)	
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 5 GHz WiFi band, select the **Enable Guest Network** check box.
Enable SSID Broadcast	By default, the cable data gateway broadcasts its SSID of the 5 GHz WiFi band so WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 5 GHz WiFi band for the guest WiFi network, clear the **Enable SSID Broadcast** check box.
Allow guest to access My Local Network	By default, WiFi clients that are connected to the 5 GHz WiFi band of guest WiFi network cannot access WiFi devices and Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the **Allow guest to access My Local Network** check box.
Guest Wireless Network Name (SSID)	The SSID is the 5 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR_GUEST_0. (This name is same as the default SSID for the 2.4 GHz band of the guest WiFi network.) If you want to change the SSID in the 5 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
If you want to change the WiFi security, select one of the following WiFi security options for the 5 GHz band of the guest WiFi network: • **None**. An open WiFi network that does not provide any security. Any WiFi device can join the 5 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network. • **WPA2-PSK [AES]**. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select this mode to allow 802.11n devices to connect to the 5 GHz band of the guest WiFi network at the fastest speed. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the guest WiFi network, a user must enter this passphrase. • **WPA-PSK [TKIP] + WPA2-PASK [AES]**. This type of security is the default setting and enables WiFi devices that support either WPA or WPA2 to join the cable data gateway's WiFi network. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the guest WiFi network, a user must enter this passphrase.	
Security Options	
Passphrase	The passphrase that provides users access to the guest WiFi network in the 5 GHZ band. The passphrase is also referred to as password or key.

7. If you changed the settings, click the **Apply** button.

   Your settings are saved.

8. Set up and test your WiFi devices and computers to make sure that they can connect over WiFi.

   If they do not, check the following:

   - Is your WiFi device connected to your network or another WiFi network in your area? Some WiFi devices automatically connect to the first open network (without WiFi security) that they discover.
   - Does your WiFi device display in the network map? (See *View the Network Map* on page 87.) If it does, it is connected to the network.

- Do you use the correct network name (SSID) and password?

Manage Internet, WAN, and LAN Settings and Use the WPS Wizard

4

This chapter describes how to manage the Internet, WAN, and LAN settings and how to use the WPS wizard.

This chapter contains the following sections:

Manage the Internet Setup

In general, the cable data gateway receives the Internet settings dynamically from the cable service provider. However, you can view or change the Internet settings.

The main Internet settings that you can configure are the IP address of the cable data gateway (dynamic or static) and the Domain Name System (DNS) server (dynamic or static).

➢ **To view or change the Internet settings:**

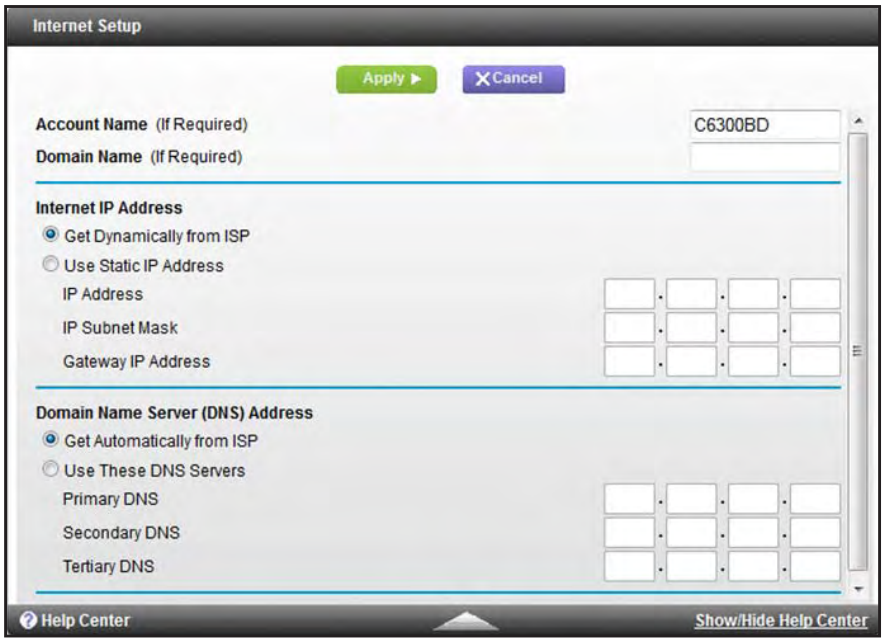
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > Internet Setup**.

   The Internet Setup screen displays.



6. View or change the settings for the IP address and DNS server.

   The default settings usually work fine. If problems occur with the connection, check the settings that your cable service provider gave you.

The following table describes the fields on the Internet Setup screen.

Field	Description
Account Name (If Required)	Enter the account name provided by your cable service provider. This name might also be called the host name. If you do not know or did not receive an account name, leave the default name, which is the model number of the cable data gateway.
Domain Name (If Required)	Enter the domain name provided by your cable service provider. If you do not know the domain name, leave this field blank.
Internet IP Address	
Get Dynamically from ISP	Your cable service provider uses DHCP to assign your IP address. Your cable service provider automatically assigns these addresses.
Use Static IP Address	Enter the IP address, IP subnet mask, and gateway IP address that your cable service provider assigned to you. The gateway is the provider gateway to which your cable data gateway connects.
Domain Name Server (DNS) Address The DNS server is used to look up site addresses based on their names.	
Get Dynamically from ISP	Your cable service provider uses DHCP to assign your DNS servers. Your cable service provider automatically assigns this address.
Use These DNS Servers	If you know that your cable service provider does not automatically transmit DNS addresses to the cable data gateway during login, select this option, and enter the IP address of your cable service provider primary DNS server. If secondary and tertiary DNS server addresses are available, enter these also.

7. If you changed the settings, click the **Apply** button.

   Your settings are saved.

Manage the WAN Settings

You can configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the cable data gateway to respond to a ping on the WAN (Internet) port.

View or Change the WAN Settings

➢ **To view or change the WAN settings:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup screen displays.

6. View or change the WAN settings.

   The following table describes the fields on the WAN Setup screen.

Field	Description
Disable Port Scan Protection	If you want the cable data gateway to respond to a ping from the Internet, select the **Disable Port Scan Protection** check box. However, use this feature only as a diagnostic tool because your cable data gateway can be discovered and in that way become vulnerable to attacks. Do not select this check box unless a specific reason exists.
Disable 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. Select the **Disable DoS Protection** check box to disable protection only in special circumstances.
Default DMZ Server	Setting up a default DMZ server might be helpful when you are playing online games or videoconferencing. However, a DMZ server can make the cable data gateway security less effective. For more information, see *Configure a Default DMZ Server* on page 45.

Field	Description
Respond to Ping on Internet Port	By default, this check box is selected to enable the cable data gateway to respond to a ping from the Internet. **Note:** When you allow the cable data gateway to respond to a ping from the Internet, the cable data gateway could be discovered by anyone and in that way become vulnerable to attacks. For optimum security, clear this check box to prevent the cable data gateway from responding to a ping from the Internet.
MTU Size (in bytes)	The default MTU setting is 0 (zero), which specifies that the cable data gateway must use the maximum transmit unit (MTU) value for best throughput. However, if you use a VPN connection, you might need to adjust the MTU to prevent packet fragmentation and packet drops. **Note:** An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.
Disable SIP ALG	The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. Disabling the SIP ALG might be useful when you are running certain applications. Select the **Disable SIP ALG** check box to disable the SIP ALG.

7. If you changed the settings, click the **Apply** button.

   Your settings are saved and the cable data gateway might restart.

Configure a Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The cable data gateway can detect some of these applications and function correctly with them but other applications 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 that is designated as the default DMZ server loses firewall protection from exploits on the Internet. Once compromised, the DMZ server computer attacks other computers on your network.

The cable data gateway discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you specially set up for this purpose (see *Set Up Port Forwarding to Local Computers* on page 121). Instead of discarding this traffic, you can let the cable data gateway forward the traffic to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup screen displays.
6. Select the **Default DMZ Server** check box.
7. Type the IP address for the DMZ server.
8. Click the **Apply** button.

   Your settings are saved and the cable data gateway might restart.

Manage the LAN Settings

You can change the LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

By default, the cable data gateway uses private IP addresses on the LAN side and functions as a DHCP server. The cable data gateway's default LAN IP configuration is as follows:

- LAN IP address. **192.168.0.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network uses a different IP addressing scheme, then make those changes in the LAN Setup screen.

Note: If you change the LAN IP address of the cable data gateway while you are connected through the browser, you are disconnected. To continue to use the genie menus, open a new connection to the new IP address and log in again.

View or Change the LAN Settings

You can view or change the LAN settings.

➢ **To view or change the LAN settings:**

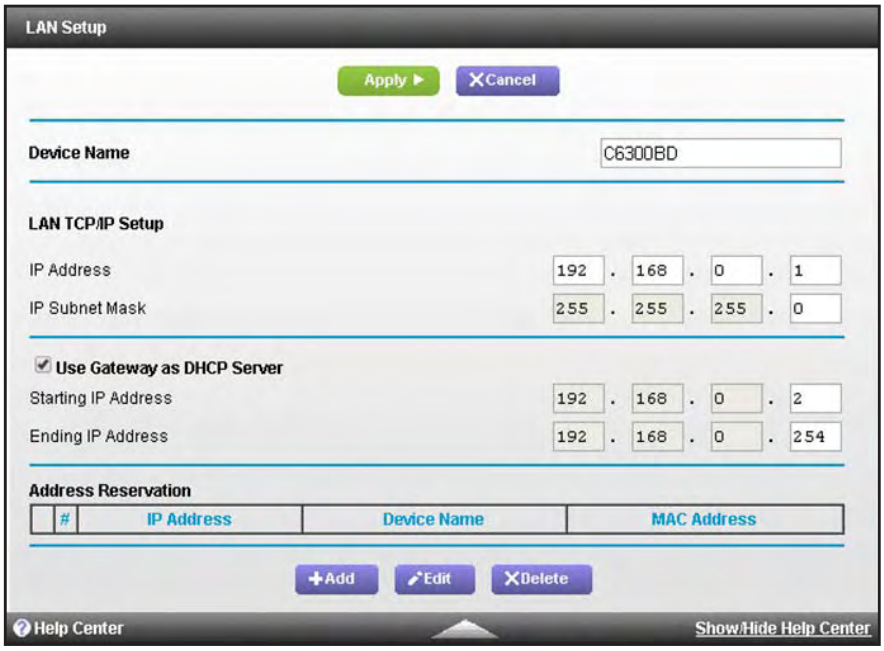
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays.



6. View or change the LAN settings.

The following table describes the fields on the LAN Setup screen.

Field	Description
Device Name	By default, the device name is the cable data gateway model. You can change the device name to another name.
LAN TCP/IP Setup	
IP Address	The LAN IP address of the cable data gateway. The default LAN IP address is 192.168.0.1. **Note:** If you change the IP address, you first might need to disable the DHCP server. After you change the IP address, you can reenable the DHCP server.
IP Subnet Mask	The LAN subnet mask of the cable data gateway. Combined with the IP address, the IP subnet mask allows a device to detect which other addresses are local to it and which must be reached through a gateway or cable data gateway. The default IP subnet mask is 255.255.255.0.
Use Gateway as DHCP Server	By default, the **Use Router as DHCP Server** check box is selected so that the cable data gateway functions as a Dynamic Host Configuration Protocol (DHCP) server. For more information, see *Use the WiFi Cable Data Gateway as a DHCP Server* on page 48.
Starting IP Address	Specify the start of the range for the DHCP pool of IP addresses in the same subnet as the cable data gateway. By default, the starting IP address is 192.168.0.2.
Ending IP Address	Specify the end of the range for the DHCP pool of IP addresses in the same subnet as the cable data gateway. By default, the ending IP address is 192.168.0.254.
Address Reservation	A device with a reserved IP address on the LAN always receives the same IP address when it accesses the cable data gateway's DHCP server. Assign reserved IP addresses to devices that require permanent IP settings. For more information, see *Manage IP Address Reservation* on page 49.

7. If you changed the settings, click the **Apply** button.

   Your settings are saved and the cable data gateway might restart.

Use the WiFi Cable Data Gateway as a DHCP Server

By default, the cable data gateway functions as a DHCP server. The cable data gateway assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the cable data gateway. The cable data gateway assigns IP addresses to the attached computers from a pool of addresses specified on the LAN Setup 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 cable data gateway work well.

The cable data gateway delivers the following parameters to any LAN device that requests DHCP:

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

You can specify the pool of IP addresses that the cable data gateway assigns by setting the starting IP address and ending IP address. These addresses must be part of the same IP address subnet as the cable data gateway's LAN IP address. Using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

➢ **To specify the pool of IP addresses that the cable data gateway assigns:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays.
6. Make sure that the **Use Gateway as a DHCP Server** check box is selected.
7. Specify the range of IP addresses:
   - **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the cable data gateway.
   - **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the cable data gateway.

   For example, using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.
8. Click the **Apply** button.

   Your settings are saved and the cable data gateway might restart.

Manage IP Address Reservation

When you specify a reserved IP address for a device on the LAN, that computer always receives the same IP address each time it accesses the cable data gateway's DHCP server.

Best practise is to assign a reserved IP address to a computer or server that requires permanent IP settings.

Reserve an IP Address

You must know the IP address and MAC address of a device for which you want to reserve an IP address.

➢ **To reserve an IP address:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

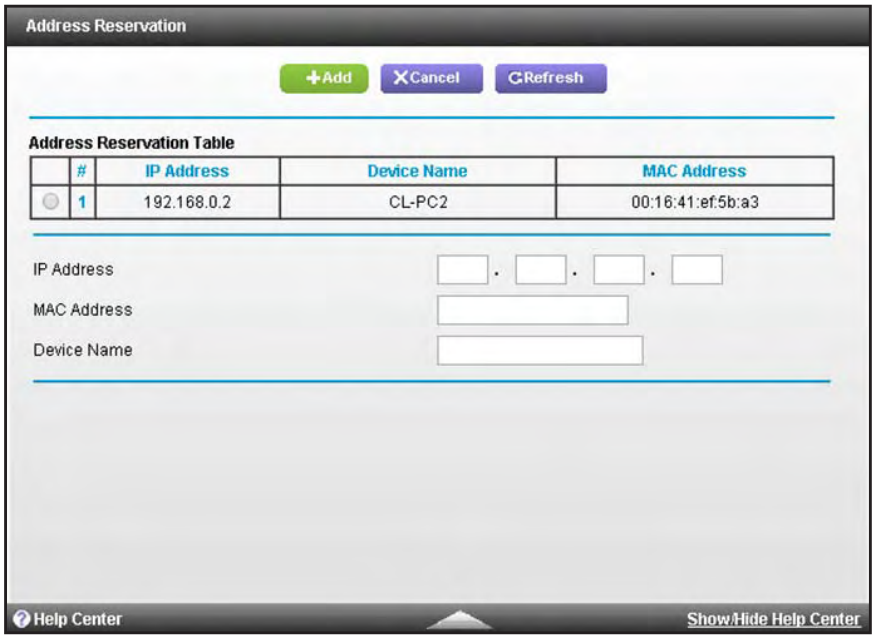
   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays.
6. In the Address Reservation section, click the **Add** button.

   The Address Reservation screen displays.



7. In the **IP Address** field, type the IP address to assign to the device.

   Choose an IP address from the cable data gateway's LAN subnet, such as 192.168.0.x.

Tip: If the computer is already on your network, you can select the corresponding radio button from the Address Reservation Table. The computer's information is automatically copied into the **IP Address**, **MAC Address**, and **Device Name** fields.

8. Type the MAC address of the device.
9. Type a name for the device.
10. Click the **Add** button.

    The reserved address is entered into the Address Reservation Table on the LAN Setup screen.

11. On the LAN Setup screen, click the **Apply** button.

    Your settings are saved.

    The reserved address is not assigned until the next time the device contacts the cable data gateway's DHCP server. Reboot the device or access its IP configuration and force a DHCP release and renew.

Change a Reserved IP Address

You can change the settings for a reserved IP address.

➢ **To change a reserved IP address:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays.

6. In the Address Reservation Table, select the radio button next to the reserved address that you want to change.
7. Click the **Edit** button.
8. Change the settings.
9. Click the **Accept** button.

   The changes are entered into the Address Reservation Table on the LAN Setup screen.

10. On the LAN Setup screen, click the **Apply** button.

    Your settings are saved.

Remove an IP Address Reservation

You can remove an IP address reservation that you no longer need.

➢ **To remove an IP address reservation:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup screen displays.
6. In the Address Reservation Table, select the radio button next to the reserved address that you want to remove.
7. Click the **Delete** button.

   The reserved address is removed from the Address Reservation Table.
8. Click the **Apply** button.

   Your settings are saved.

Use the WPS Wizard to Add a Device to the WiFi Network

WPS (Wi-Fi Protected Setup) lets you connect a computer or WiFi device to the cable data gateway's network without entering the WiFi network passphrase or key. Instead, you use a **WPS** button or enter a PIN to connect.

If you use the push button method, the WiFi device that you are trying to connect must provide either a physical button or a software button. If you use the PIN method, you must know the PIN of the WiFi device that you are trying to connect.

WPS supports WPA and WPA2 WiFi security. If your cable data gateway network is open (no WiFi security is set, which is not the default setting for the cable data gateway), connecting with WPS automatically sets WPA + WPA2 WiFi security on the cable data gateway network and generates a random passphrase. You can view this passphrase (see *View or Change the Basic Settings for the Main WiFi Network* on page 31).

Use WPS with the Push Button Method

For you to use the push button method to connect a WiFi device to the cable data gateway's WiFi network, the WiFi device that you are trying to connect must provide either a physical button or a software button. You can use the physical button and software button only to let a WiFi device join the main WiFi network, not the guest WiFi network.

➢ **To let a WiFi device join the cable data gateway's main WiFi network using WPS with the push button method:**

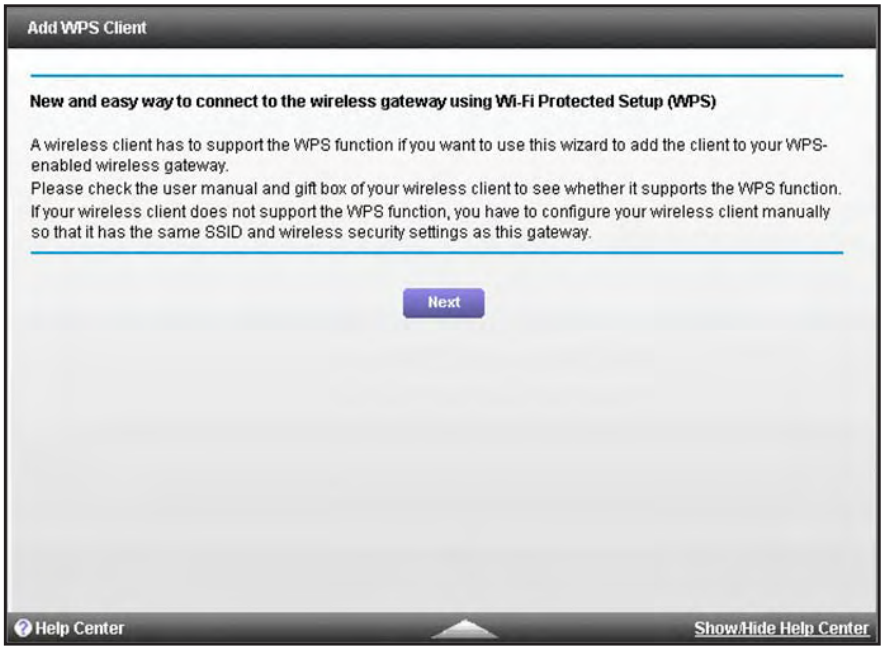
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

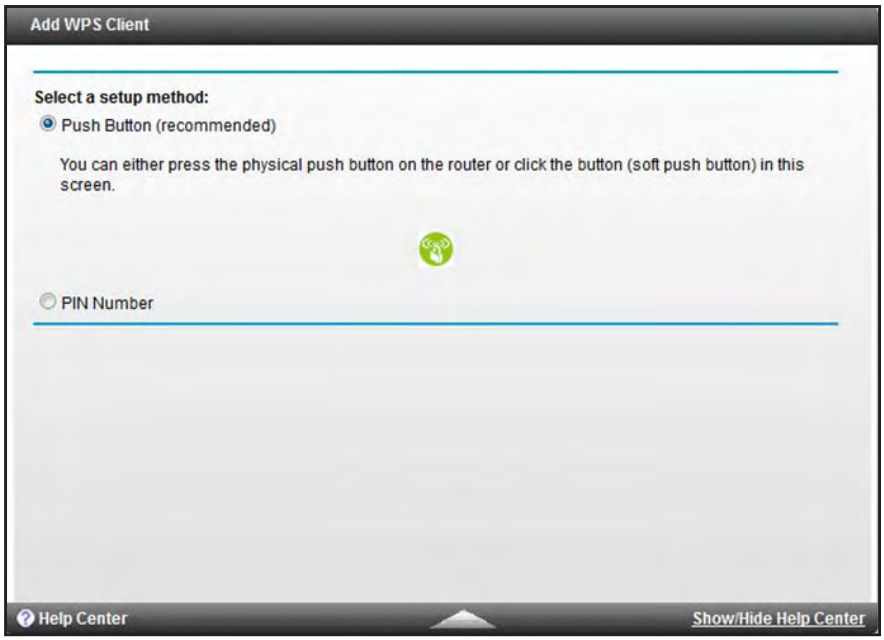
   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > WPS Wizard**.

   The screen displays a description of the WPS method.



6. Click the **Next** button.
7. The Add WPS Client screen adjusts.



By default, the **Push Button (recommended)** radio button is selected.

8. Either click the button onscreen or press the **WPS** button on the front panel of the cable data gateway.

   For two minutes, the cable data gateway attempts to find the WiFi device (that is, the client) that you want to join the cable data gateway's main WiFi network.

   During this time, the WPS LED on the front panel of the cable data gateway blinks green.

9. Within two minutes, go to the WiFi device and press its **WPS** button to join the cable data gateway's main WiFi network without entering a password.

   After the cable data gateway establishes a WPS connection, the LED lights solid green and the Add WPS Client screen displays a confirmation message.

10. To verify that the WiFi device is connected to the cable data gateway's main WiFi network, select **BASIC > Network Map**.

    The WiFi device displays onscreen.

Use WPS with the PIN Method

To use the PIN method to connect a WiFi device to the cable data gateway's WiFi network, you must know the PIN of the WiFi device that you are trying to connect.

➢ **To let a WiFi device join the cable data gateway's WiFi network using WPS with the PIN method:**

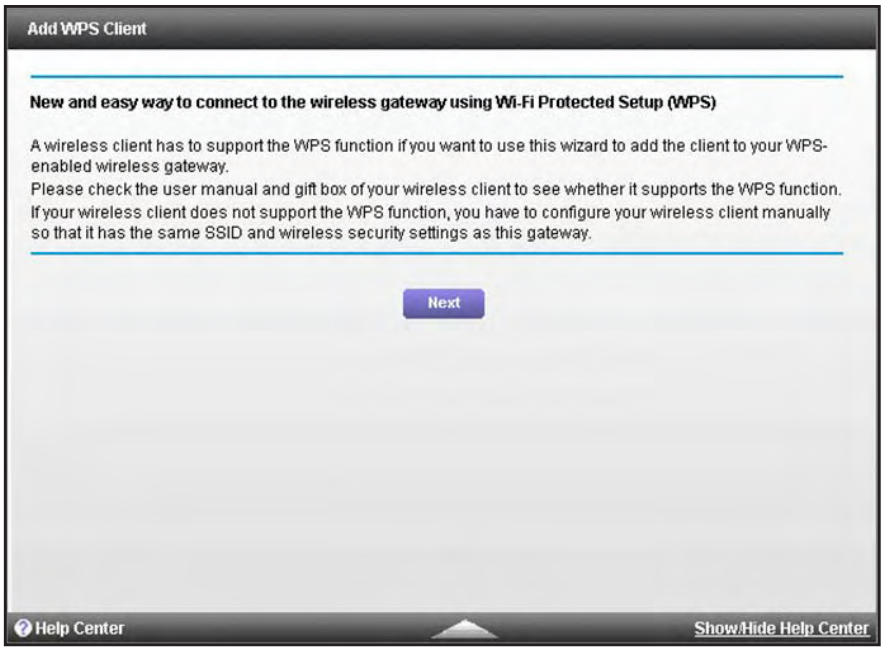
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

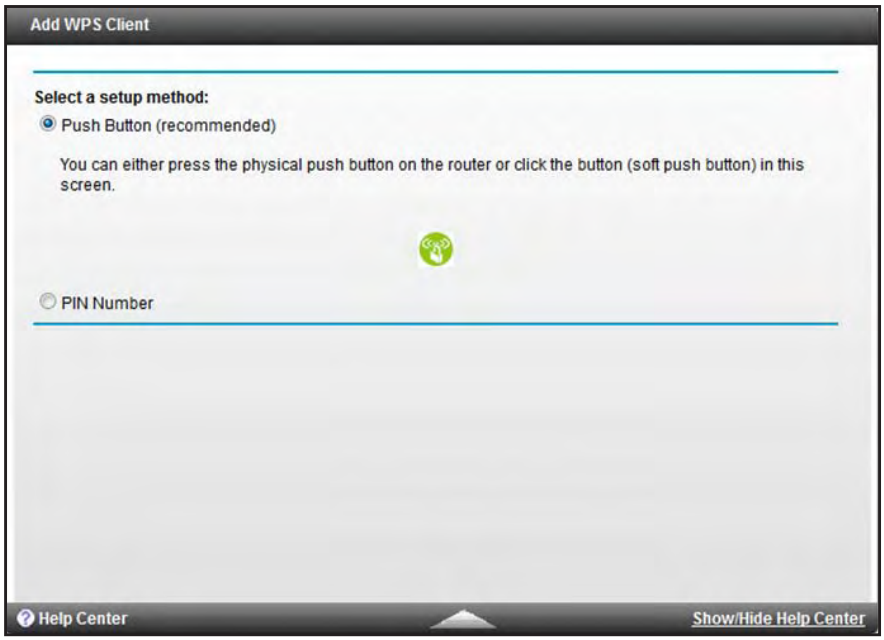
   The BASIC Home screen displays.
5. Select **ADVANCED > WPS Wizard**.

   The screen displays a description of the WPS method.



6. Click the **Next** button.

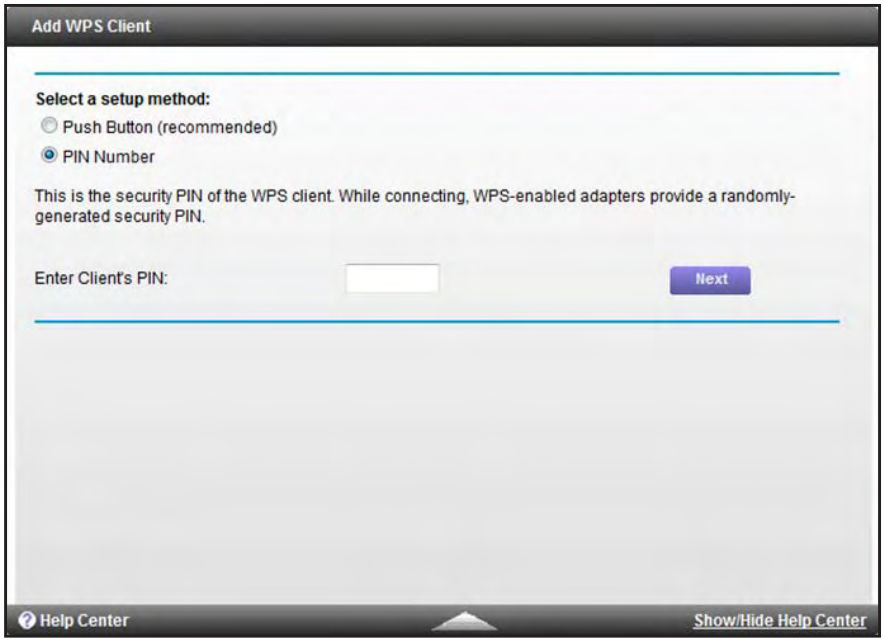
   The Add WPS Client screen adjusts.



On the screen that displays, the **Push Button (recommended)** radio button is selected by default.

7. Select the **PIN Number** radio button.

   The Add WPS Client screen displays.



8. In the **Enter Client's PIN** field, enter the PIN number of the WiFi device.
9. Click the **Next** button.

For four minutes, the cable data gateway attempts to find the WiFi device (that is, the client) that you want to join the cable data gateway's main WiFi network.

During this time, the WPS LED on the front panel of the cable data gateway blinks green.

10. Within four minutes, go to the WiFi device and use its WPS software to join the network without entering a password.

    When the cable data gateway establishes a WPS connection, the LED lights solid green and the Add WPS Client screen displays a confirmation message.

11. To verify that the WiFi device is connected to the cable data gateway's main WiFi network, select **BASIC > Network Map**.

    The WiFi device displays onscreen.

Manage the Firewall and Secure Your Network

5

This chapter describes how to use the basic firewall features of the cable data gateway to prevent objectionable content from reaching the computers and other devices connected to your network.

This chapter includes the following sections:

Note: For information about parental controls, which is another security feature, see *Set Up Parental Controls* on page 29.

Block Keywords and Domains for HTTP Traffic

You can block keywords and domains (websites) to prevent certain types of HTTP traffic from accessing your network. By default, keyword blocking is disabled and no domains are blocked.

Set Up Blocking

You can set up blocking of specific keywords and domains to occur continuously or according to a schedule.

➢ **To set up keyword and domain blocking:**

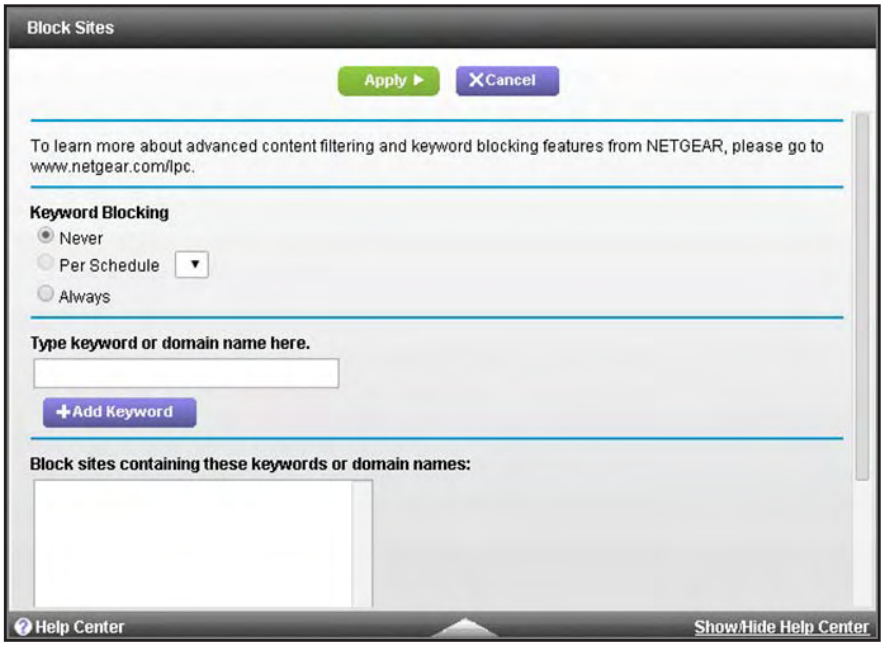
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Sites**.

   The Block Sites screen displays.



6. Specify a keyword blocking option:
   - **Per Schedule**. Use keyword blocking according to a schedule that you set.

     For more information, see *Schedule When Features Are Active* on page 68.
   - **Always**. Use keyword blocking continuously.
7. In the **Type keyword or domain name here** field, enter a keyword or domain.

   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.
8. Click the **Add Keyword** button.

   The keyword or domain is added to the **Block sites containing these keywords or domain names** field (which is also referred to as the blocked list).
9. To add more keywords or domains, repeat *Step 7* and *Step 8*.

   The keyword list supports up to 32 entries.
10. Click the **Apply** button.

    Your settings are saved.

Remove a Keyword or Domain from the Blocked List

If you no longer need a keyword or domain on the blocked list, you can remove the keyword or domain.

➢ **To remove a keyword or domain from the blocked list:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Sites**.

   The Block Sites screen displays.
6. In the **Block sites containing these keywords or domain names** field, select the keyword or domain that you want to remove.
7. Click the **Delete Keyword** button.

The keyword or domain is removed from the blocked list.

8. Click the **Apply** button.

   Your settings are saved.

Remove All Keywords and Domains from the Blocked List

You can simultaneously remove all keywords and domains from the blocked list.

➢ **To remove all keywords and domains from the blocked list:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Sites**.

   The Block Sites screen displays.
6. Click the **Clear List** button.

   All keywords and domains are removed from the blocked list.
7. Click the **Apply** button.

   Your settings are saved.

Specify a Trusted Computer

You can exempt one trusted device from blocking and logging. The device that you exempt must be assigned a fixed (static) IP address.

➢ **To specify a trusted device:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

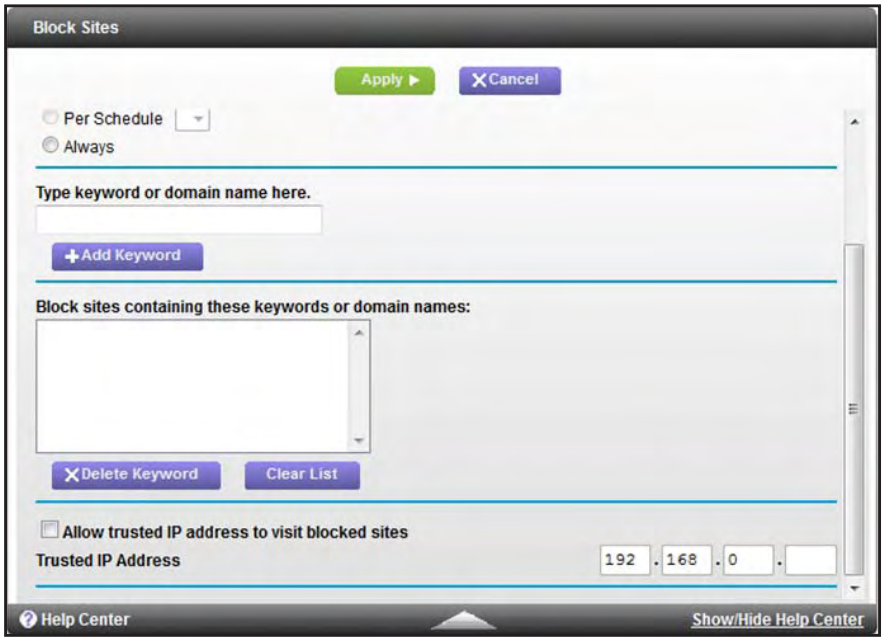
   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

The BASIC Home screen displays.

5. Select **ADVANCED > Security > Block Sites**.

   The Block Sites screen displays.



6. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.
7. In the **Trusted IP Address** field, enter the IP address of the trusted device.

   The first three octets of the IP address are automatically populated and depend on the IP address that is assigned to the cable data gateway on the LAN Setup screen.

8. Click the **Apply** button.

   Your settings are saved.

Block Access to Services and Applications

Services are functions that servers perform at the request of client devices. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about the moves of the players.

When a device on the Internet sends a request for service to a server, the requested service is identified by a service or port number. (For this reason, service blocking is also referred to as port filtering.) The service or port 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 1024–65535 by

the authors of the application. Although the cable data gateway already holds a list of many service port numbers, you are not limited to these choices.

You can block access to specific Internet services by devices on your network. This feature is called service blocking or port filtering. The cable data gateway provides default (predefined) services that you can select to block. You can also add a new service for blocking, but you first must find out which port number or range of numbers the application uses. You can find port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching the Internet.

Block a Default Service

You can set up blocking of specific services to occur continuously or according to a schedule.

➢ **To block a default service:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

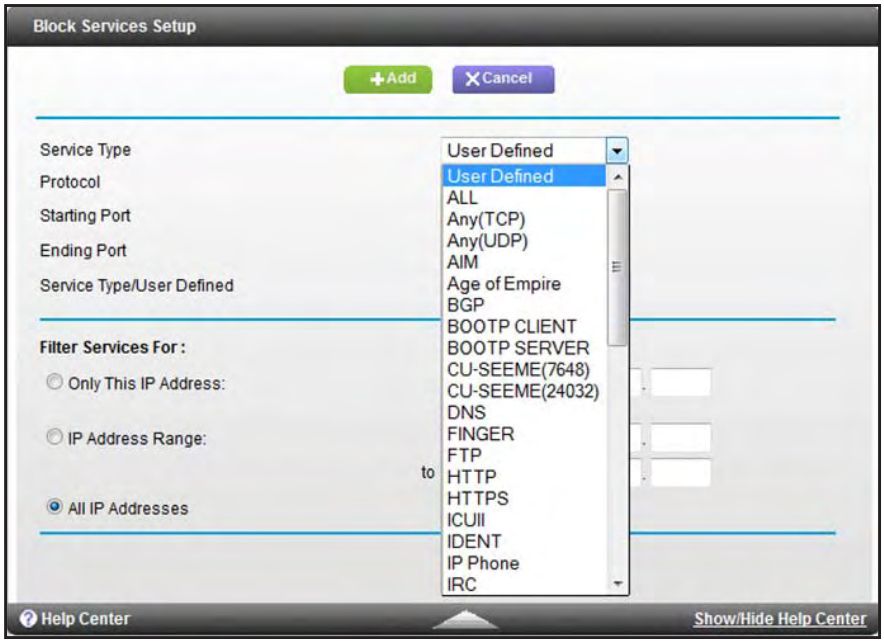
   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Services**.

   The Block Services screen displays.

6. Specify a keyword blocking option:
   - **Per Schedule**. Use service blocking according to a schedule that you set.

     For more information, see *Schedule When Features Are Active* on page 68.
   - **Always**. Use service blocking continuously.
7. Click the **Add** button.

   The Block Services Setup screen displays.



8. From the **Service Type** menu, select the default application or service to block.

   The menu displays several common services, but you are not limited to these choices. For information about how to add any additional services or applications, see *Add and Block a Custom Service* on page 65.
9. Under Filter Services For, select an IP address configuration:
   - **Only This IP Address**. Complete the IP address for the device for which the application or service must be blocked.
   - **IP Address Range**. Complete the IP address range for the devices for which the application or service must be blocked.
   - **All IP Addresses**. The application or service is blocked for all IP addresses on your network.
10. Click the **Add** button.

    Your changes are saved in the table on the Block Services screen. However, if you restart the cable data gateway, the changes are lost. You also must apply the changes on the Block Services screen.
11. On the Block Services screen, click the **Apply** button.

Your settings are saved.

Add and Block a Custom Service

If the service that you want to block is not on the default service list, you can define a custom service.

➢ **To add and block a custom service:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Services**.

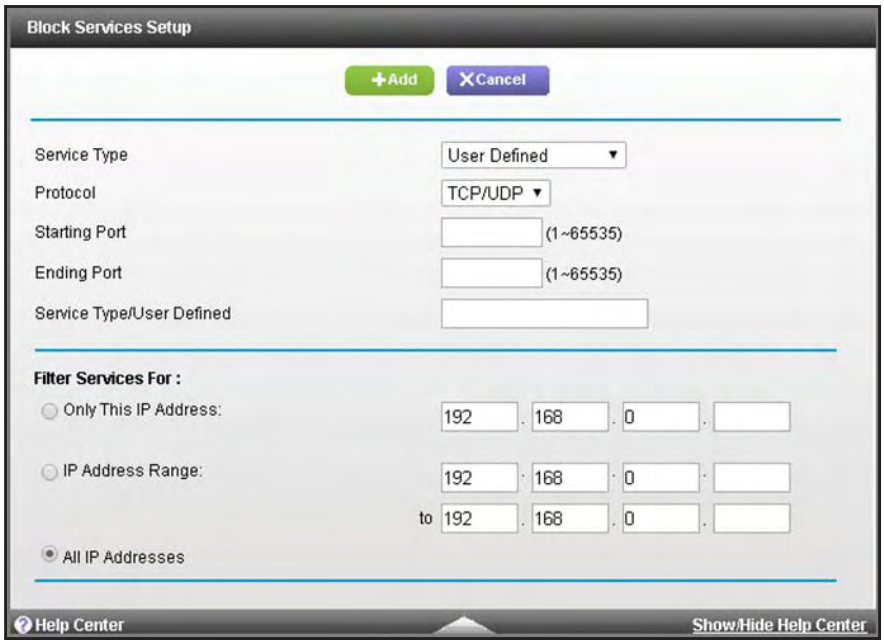
   The Block Services screen displays.

6. Specify a keyword blocking option:
   - **Per Schedule**. Use service blocking according to a schedule that you set.

     For more information, see *Schedule When Features Are Active* on page 68.
   - **Always**. Use service blocking continuously.

7. Click the **Add** button.

   The Block Services Setup screen displays.



8. From the **Service Type** menu, select **User Defined**.
9. Configure the settings for the custom service or application:
   - **Protocol**. Select a protocol. If you are not sure what protocol the service or application uses, select **TCP/UDP**.
   - **Starting Port** and **Ending Port**. Enter the starting and ending port numbers. If the service or application uses a single port number, enter that number in both fields.
   - **Service Type/User Defined**. Enter a name for the service or application.
10. Under Filter Services For, select an IP address configuration:
    - **Only This IP Address**. Complete the IP address for the device for which the application or service must be blocked.
    - **IP Address Range**. Complete the IP address range for the devices for which the application or service must be blocked.
    - **All IP Addresses**. The application or service is blocked for all IP addresses on your network.
11. Click the **Add** button.

    Your changes are saved in the table on the Block Services screen. However, if you restart the cable data gateway, the changes are lost. You also must apply the changes on the Block Services screen.

12. On the Block Services screen, click the **Apply** button.

    Your settings are saved.

Change the Settings for a Blocked Service

You can change the settings for a specific service that is being blocked.

➢ **To change the settings for a service on the Block Services screen:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Services**.

   The Block Services screen displays.
6. Select the radio button next to the service or application that you want to change.
7. Click the **Edit** button.

   The Block Services Setup screen displays.
8. Change the settings for the service or application.

   For information about the settings, see *Add and Block a Custom Service* on page 65.
9. Click the **Add** button.

   Your changes are saved in the table on the Block Services screen. However, if you restart the cable data gateway, the changes are lost. You also must apply the changes on the Block Services screen.
10. To enable or disable blocking of the service, select or clear the **Enable** check box.
11. On the Block Services screen, click the **Apply** button.

    Your settings are saved.

Remove a Blocked Service

If you no longer need a service on the blocked list, you can remove the service.

➢ **To remove a service from the table on the Block Services screen:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Block Services**.

   The Block Services screen displays.
6. Select the radio button next to the service or application that you want to remove from the table.
7. Click the **Delete** button.

   The service or application is removed from the table. A default service or application is not removed from the **Service Type** menu on the Block Services Setup screen. However, a custom service or application that you added *is* deleted. If you want to use the same custom service or application again, you must redefine it (see *Add and Block a Custom Service* on page 65).
8. Click the **Apply** button.

   Your settings are saved.

Schedule When Features Are Active

You can specify the days and time that you want a feature to be active. You can set up multiple schedules, for example, one for each feature, or you can use the same schedule for a combination of different features.

You can apply schedules to the following features:

- Keyword blocking (see *Block Keywords and Domains for HTTP Traffic* on page 59)
- Service blocking (see *Block Access to Services and Applications* on page 62)
- Port forwarding (see *Set Up Port Forwarding to Local Computers* on page 121)
- Port triggering (see *Set Up and Manage Port Triggering* on page 127)
- IP Address filtering (see *Set Up and Manage IP Address Filtering* on page 134)
- MAC address filtering (see *Set Up and Manage MAC Address Filtering* on page 137)

By default, no schedules are set and you can either enable or disable these features.

Set Up a Schedule

The cable data gateway does not provide a default schedule but you can add up to 16 custom schedules.

➢ **To set up a schedule for blocking:**

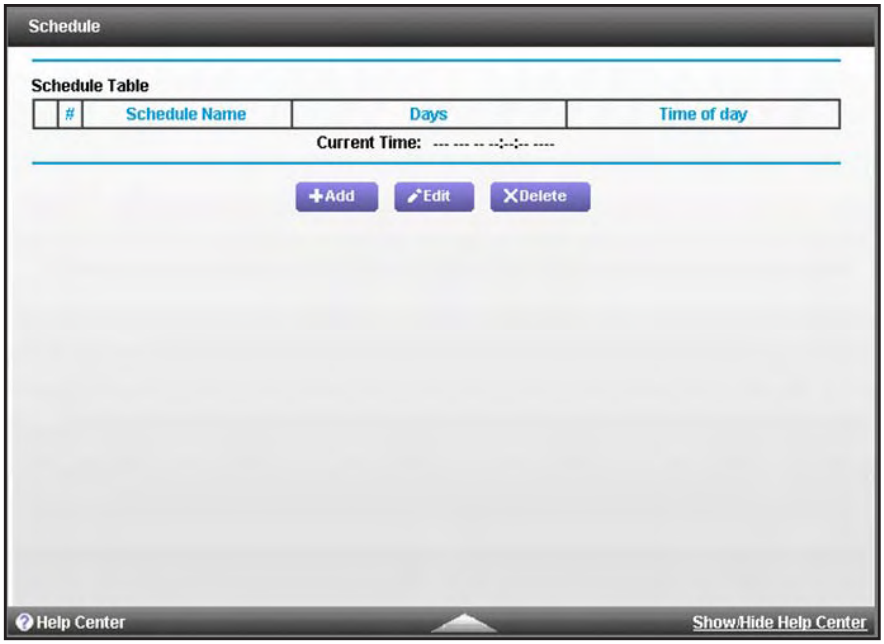
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

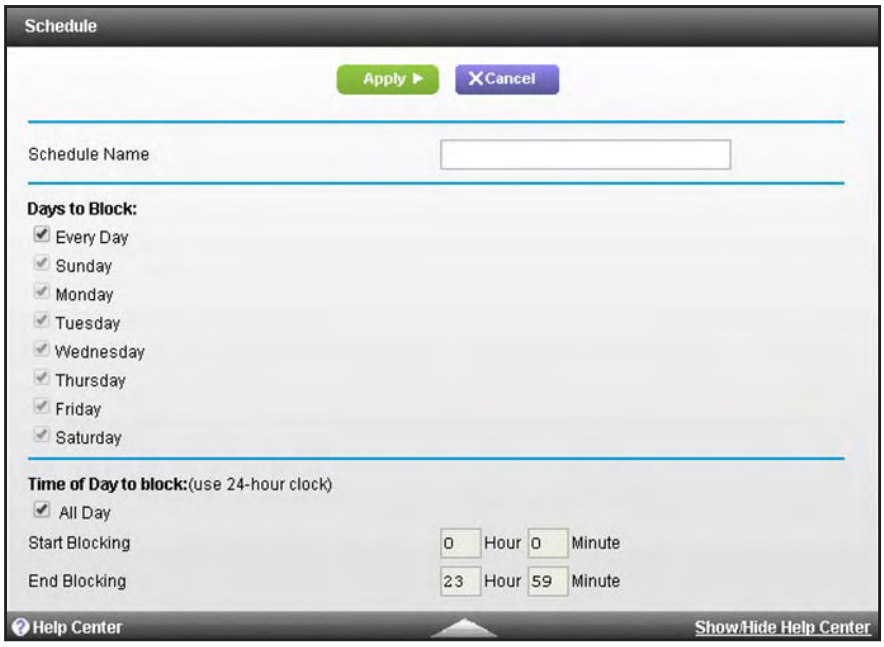
   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Schedule**.

   The Schedule screen displays.



6. Click the **Add** button.

   The screen adjusts.



7. In the **Schedule Name** filed, enter a name for the schedule.

   For example, if you are setting up a schedule for keyword blocking during business hours, you could enter a name that lets you easily identify such a schedule.

8. Set up the schedule for blocking:
   - **Days to Block**. Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
   - **Time of Day to Block**. Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.

     The start time must be earlier than the end time. For example, you cannot block overnight by specifying 20:00 in the start field and 07:00 in the end field. In such a situation, you need to set up two schedules.

9. Click the **Apply** button.

   Your settings are saved and the schedule is added to the Schedule Table.

10. To display the Schedule Table, click the **Cancel** button.

Change a Schedule

You can change the settings for a schedule.

➢ **To change the settings for a schedule:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Schedule**.

   The Schedule screen displays.
6. Select the radio button next to the schedule that you want to change.
7. Click the **Edit** button.

   The Schedule screen adjusts.
8. Change the settings for the schedule.
9. Click the **Apply** button.

   Your changes are saved and the schedule is added to the Schedule Table.
10. To display the Schedule Table, click the **Cancel** button.

Remove a Schedule

If you no longer need a schedule, you can remove it.

➢ **To remove a schedule:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Schedule**.

The Schedule screen displays.

6. Select the radio button next to the schedule that you want to remove.
7. Click the **Delete** button.

   The schedule is removed from the table.

Set Up Security Event Email Notification

To receive logs and alerts by email about websites that users accessed, attempts to access blocked sites, cable data gateway operation, DoS attacks and port scans, WiFi access, and other information, provide your email information on the E-mail screen, and specify how often you want to receive logs and alerts.

➢ **To set up email notifications:**

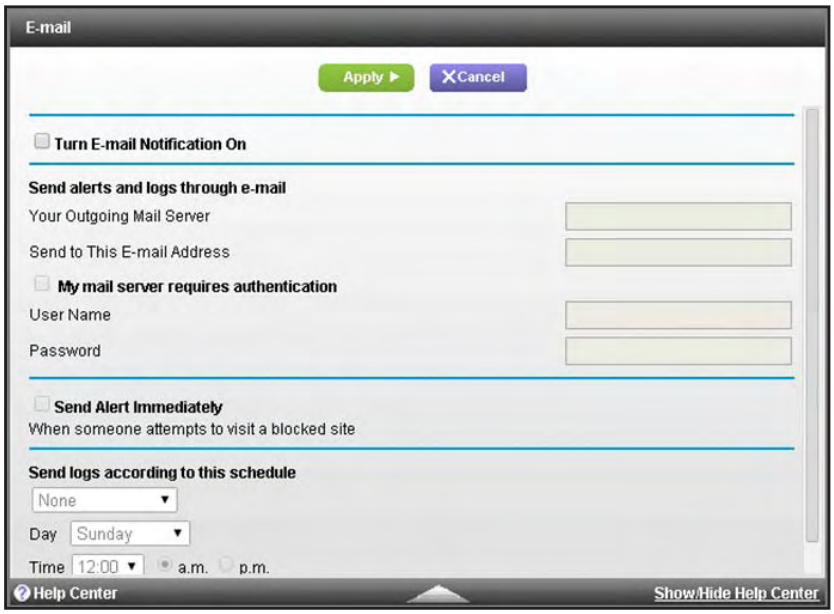
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > E-mail**.

   The E-mail screen displays.



6. Select the **Turn E-mail Notification On** check box.
7. In the **Your Outgoing Mail Server** field, enter the name of your cable service provider's outgoing (SMTP) mail server (such as mail.myISP.com).

   You might be able to find this information on the configuration screen of your email program or by contacting your cable service provider. If you leave this field blank, log and alert messages are not sent.
8. In the **Send to This E-mail 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.
9. If your outgoing email server requires authentication, set up the authentication:
   a. Select the **My Mail Server requires authentication** check box.
   b. Complete the **User Name** and **Password** fields for the outgoing email server.
10. If you want alerts to be sent immediately, select the **Send Alerts Immediately** check box.

    Email alerts are sent immediately when someone attempts to visit a blocked site.
11. To set up a schedule for logs to be sent, specify the following settings:
    a. Select an option from the **Send logs according to this schedule** menu:
       - **When log is full**
       - **Hourly**
       - **Daily**
       - **Weekly**
       - **None**
    b. If you select **Daily** or **Weekly**, select the time from the **Day** menu and select the **a.m.** or **p.m.** radio button.
    c. If you select **Weekly**, also select the day from the **Day** menu.

    Logs are sent automatically. If the log fills before the specified time, the log is emailed. After the log is sent, the log is cleared from the memory of the cable data gateway. If the cable data gateway cannot email the log file, the log buffer might fill. In this case, the cable data gateway overwrites the log and discards its contents.
12. Click the **Apply** button.

    Your settings are saved.

Manage Firewall, Web, and NAT ALG Security

The built-in firewall of the cable data gateway supports multiple features, all of which are enabled by default. You can disable some or all of these firewall features. As an option, you can also enable web features, which are disabled by default. The Application Level Gateway (ALG) is enabled by default to optimize Network Address Translation (NAT). You can disable some or all of the ALG NAT traversal filters.

➢ **To manage firewall, web, and NAT ALG features:**

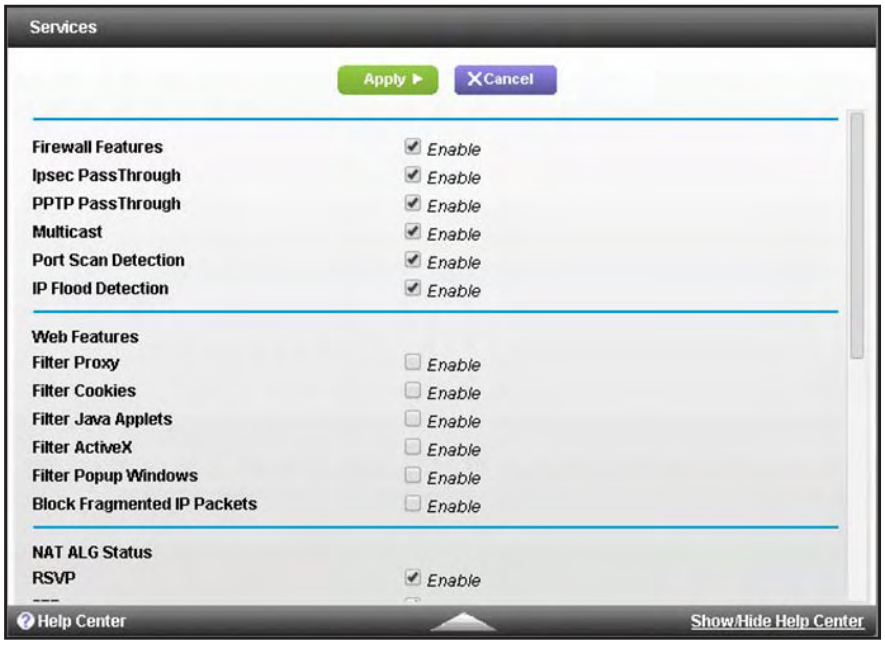
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Security > Services**.

   The Services screen displays.



6. Customize the settings as described in the following table.

Feature	Description
Firewall Features These features are enabled by default. To disable a feature, clear the associated **Enable** check box.	
Firewall Features	If firewall features are enabled, the cable data gateway performs stateful packet inspection (SPI) and protects against denial of service (DoS) attacks. If firewall features are disabled, the cable data gateway does not perform SPI and does not provide DoS protection. **Note:** Best practise is to keep firewall features enabled.

Feature	Description
Ipsec PassThrough	If IPSec pass-through is enabled, IPSec traffic is forwarded. If it is disabled, IPSec traffic is blocked.
PPTP PassThrough	If PPTP pass-through is enabled, PPTP traffic is forwarded. If it is disabled, PPTP traffic is blocked.
Multicast	If multicast is enabled, the cable data gateway passes multicasting streams through the firewall. If it is disabled, multicast streams are blocked.
Port Scan Detection	If port scan detection is enabled, the cable data gateway responds to Internet-based port scans. If it is disabled, the cable data gateway blocks port scans. **Note:** Best practise is to keep port scan detection enabled.
IP Flood Detection	If IP flood detection is enabled, the cable data gateway blocks devices (usually malicious devices) that are attempting to flood devices. If it is disabled, flooding is not blocked. **Note:** Best practise is to keep IP flood detection enabled.
Web Features These features are disabled by default. To enable a feature, select the associated **Enable** check box.	
Filter Proxy	If the proxy filter is enabled, the HTTP proxy is blocked and you can connect to the web only directly. That is, you cannot connect to the web through a proxy server. If the proxy filter is disabled, you can connect to the web through a proxy server.
Filter Cookies	If the cookie filter is enabled, websites cannot deposit cookies. If it is disabled, websites can deposit cookies.
Filter Java Applets	If the Java applets filter is enabled, websites cannot use Java applets. If it is disabled, websites can use Java applets.
Filter ActiveX	If the ActiveX filter is enabled, websites cannot use ActiveX. If it is disabled, websites can use ActiveX.
Filter Popup Windows	If the pop-up filter is enabled, websites cannot use pop-up screens. If it is disabled, websites can use pop-up screens.
Block Fragmented IP Packets	If the fragmented IP packet filter is enabled, you can download only complete (unfragmented) IP packets. If it is disabled, you can download fragmented IP packets.

Feature	Description
NAT ALG Status These features are enabled by default. To disable a feature, clear the associated **Enable** check box.	
RSVP	By default, each application and protocol that is listed here can pass through NAT, which means that it is not obstructed by NAT. These applications and protocols are self-explanatory.
FTP	
TFTP	
Kerb88	
NetBios	
IKE	
Kerb1293	
H225	
PPTP	
MSN	
SIP	
ICQ	
IRC666x	
ICQTalk	
Net2Phone	
IRC7000	

7. Click the **Apply** button.

   Your settings are saved and take effect immediately.

Manage and Monitor Your Network

6

This chapter describes the cable data gateway settings and options for administering, maintaining, and monitoring your cable data gateway and network.

This chapter includes the following sections:

- *View the Status and Statistics of the WiFi Cable Data Gateway*
- *View the WiFi Cable Data Gateway Cable Initialization*
- *View the Network Map*
- *View WiFi Channels in Your Environment*
- *View WiFi Access Points in Your Environment*
- *View and Manage the Log*
- *Manage the WiFi Cable Gateway Settings*
- *Return the WiFi Cable Data Gateway to Its Factory Default Settings*
- *Reboot the Cable Data Gateway*

For additional management information, see the following sections:

- For information about changing the password of the cable data gateway, see *Change the Password* on page 25.
- For information about managing the cable data gateway over the Internet, see *Manage the Cable Data Gateway Remotely* on page 141.
- For information about diagnostic tools, see *Perform Diagnostics* on page 151.
- For information about the event log, see *View and Manage the Event Log* on page 157.

View the Status and Statistics of the WiFi Cable Data Gateway

You can view status information about the cable data gateway and its cable connection, Internet connection, and WiFi networks. In addition, you can view traffic statistics for the various ports.

View the Cable Information, Internet Port Status, and WiFi Status

The ADVANCED Home screen displays cable information, the Internet port status, and WiFi settings for both radios of the main and guest networks.

➢ **To view information about the cable data gateway, Internet port, and WiFi settings:**

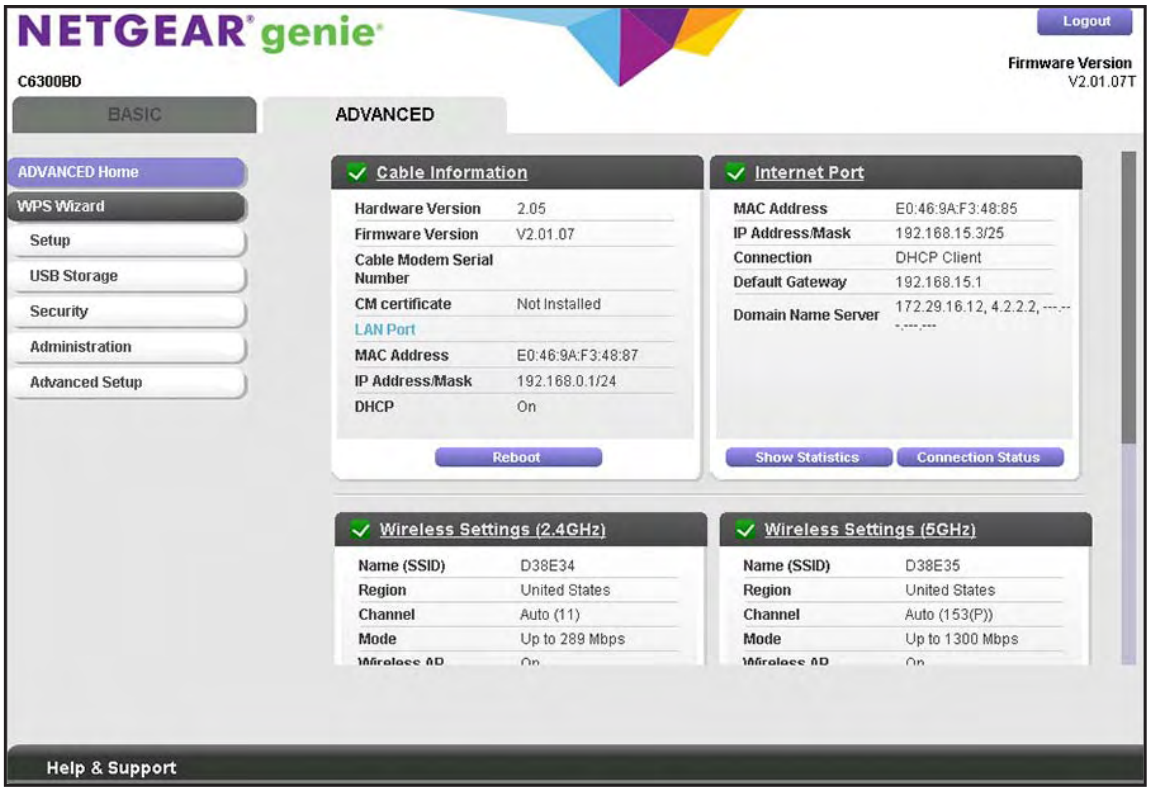
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays. The following figure shows the screen for the AC1900 WiFi Cable Data Gateway, Model C6300BD. Other models might not show the same panes.



The color of the Flag icon indicates the following status:

- **Green Flag icon**. The cable connection or Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
- **Red Flag icon**. Configuration problems exist for the cable connection or Internet connection or the connection is down. For a WiFi network, the network is disabled or down.
- **Amber Flag icon**. For a WiFi network, the network is enabled but unsecured.

The following table describes the panes on the ADVANCED Home screen.

Field	Description
Cable Information	
Hardware Version	The cable data gateway hardware version.
Firmware Version	The version of the router firmware. If you upgrade the router firmware on the cable data gateway, the version changes.
Cable Modem Serial Number	The cable data gateway serial number.
CM certificate	The cable data gateway digital certificate.

Field	Description
LAN Port The settings of the LAN port. For information about how to configure the LAN settings, see *Manage the LAN Settings* on page 46.	
MAC Address	The Media Access Control (MAC) address. This address is the unique physical address that is assigned to the Ethernet LAN port.
IP Address	The IP address that the Ethernet LAN port uses. The default IP address is 192.168.0.1.
DHCP	Displays whether the DHCP server of the cable data gateway is enabled for devices that are attached to the LAN.
Internet Port The settings of cable Internet port. You cannot change these settings. Other than the MAC address, these settings are assigned by the cable service provider.	
MAC Address	The Media Access Control (MAC) address. This address is the unique physical address that is assigned to the cable Internet port.
IP Address/Mask	The IP address and subnet mask (in the /xx format) that the cable Internet port uses. If this field does not display an address or displays 0.0.0.0 as the address, the cable data gateway cannot provide an Internet connection over the cable Internet port.
Connection	The type of network address, which is either a fixed IP address or an IP address that the cable data gateway obtains dynamically from the DHCP server of the cable service provider. In the latter case, the field displays DHCP Client.
Default Gateway	The IP address of the cable service provider's gateway that the cable Internet port uses.
Domain Name Server	The IP addresses of the Domain Name System (DNS) servers that the cable Internet port uses.
Wireless Settings (2.4GHz) The settings of the 2.4 GHz band of the main WiFi network. For information about how to configure the WiFi settings, see *View or Change the Basic Settings for the Main WiFi Network* on page 31 and *Manage Advanced WiFi Settings* on page 109.	
Name (SSID)	The network name of the 2.4 GHz band of the main WiFi network.
Region	The location (country). By default, the region is the United States.
Channel	The channel that the 2.4 GHz band of the main WiFi network uses.
Mode	The WiFi mode that the 2.4 GHz band of the main WiFi network uses. By default, the mode is Up to 289 Mbps. **Note:** The selected mode also applies to the 2.4 GHz band of the guest WiFi network.
Wireless AP	Displays whether the 2.4 GHz band of the main WiFi network is enabled. If the 2.4 GHz band is disabled, the 2.4 GHz WiFi LED on the front panel of the cable data gateway is off.

Field	Description
Broadcast Name	Displays whether the 2.4 GHz band of the main WiFi network broadcasts its SSID.
Wireless isolation	Displays whether WiFi isolation is enabled for the 2.4 GHz band of the main WiFi network.
Wi-Fi Protected Setup	By default, the Wi-Fi Protected Setup (WPS) function is configured.
Wireless Settings (5GHz) The settings of the 5 GHz band of the main WiFi network. For information about how to configure the WiFi settings, see *View or Change the Basic Settings for the Main WiFi Network* on page 31 and *Manage Advanced WiFi Settings* on page 109.	
Name (SSID)	The network name of the 5 GHz band of the main WiFi network.
Region	The location (country). By default, the region is the United States.
Channel	The channel that the 5 GHz band of the main WiFi network uses.
Mode	The WiFi mode that the 5 GHz band of the main WiFi network uses. For model N900, the mode is Up to 450 Mbps by default. For model AC1900, the mode is Up to 600 Mbps by default. Model N450 does not support the 5 GHz band. **Note:** The selected mode also applies to the 5 GHz band of the guest WiFi network.
Wireless AP	Displays whether the 5 GHz band of the main WiFi network is enabled. If the 5 GHz band is disabled, the 5GHz WiFi LED on the front panel of the cable data gateway is off.
Broadcast Name	Displays whether the 5 GHz band of the main WiFi network broadcasts its SSID.
Wireless isolation	Displays whether WiFi isolation is enabled for the 5 GHz band of the main WiFi network.
Wi-Fi Protected Setup	By default, the Wi-Fi Protected Setup (WPS) function is configured.
Guest Network (2.4GHz) The settings of the 2.4 GHz band of the guest WiFi network. For information about how to configure the WiFi settings, see *Enable and Configure the Guest WiFi Network* on page 36.	
Name (SSID)	The network name of the 2.4 GHz band of the guest WiFi network. By default, the name is NETGEAR_GUEST_0.
Wireless AP	Displays whether the 2.4 GHz band of the guest WiFi network is enabled. **Note:** The 2.4 GHz band for the main WiFi network can override the 2.4 GHz band for the guest WiFi network. That is, if you disable the 2.4 GHz band for the main network, the entire 2.4 GHz radio is disabled, which also disables the 2.4 GHz band for the guest network.
Broadcast Name	Displays whether the 2.4 GHz band of the guest WiFi network broadcasts its SSID.

Field	Description
Wireless isolation	By default, WiFi isolation is off. You cannot enable WiFi isolation for the guest WiFi network.
Allow guest to access My Local Network	Displays whether guests that connect to the 2.4 GHz band of the guest WiFi network are allowed access to devices on the main WiFi network and devices that are attached through the LAN ports.
Guest Network (5GHz) The settings of the 5 GHz band of the guest WiFi network. For information about how to configure the WiFi settings, see *Enable and Configure the Guest WiFi Network* on page 36.	
Name (SSID)	The network name of the 5 GHz band of the guest WiFi network. By default, the name is NETGEAR_GUEST_0.
Wireless AP	Displays whether the 5 GHz band of the guest WiFi network is enabled. **Note:** The 5 GHz band for the main WiFi network can override the 5 GHz band for the guest WiFi network. That is, if you disable the 5 GHz band for the main network, the entire 5 GHz radio is disabled, which also disables the 5 GHz band for the guest network.
Broadcast Name	Displays whether the 5 GHz band of the guest WiFi network broadcasts its SSID.
Wireless isolation	By default, WiFi isolation is off. You cannot enable WiFi isolation for the guest WiFi network.
Allow guest to access My Local Network	Displays whether guests that connect to the 5 GHz band of the guest WiFi network are allowed access to devices on the main WiFi network and devices that are attached through the LAN ports.

View the Traffic Statistics

You can view the traffic statistics for the ports of the cable data gateway, change the polling frequency, and stop traffic polling.

➢ **To view the traffic statistics for the ports of the cable data gateway:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

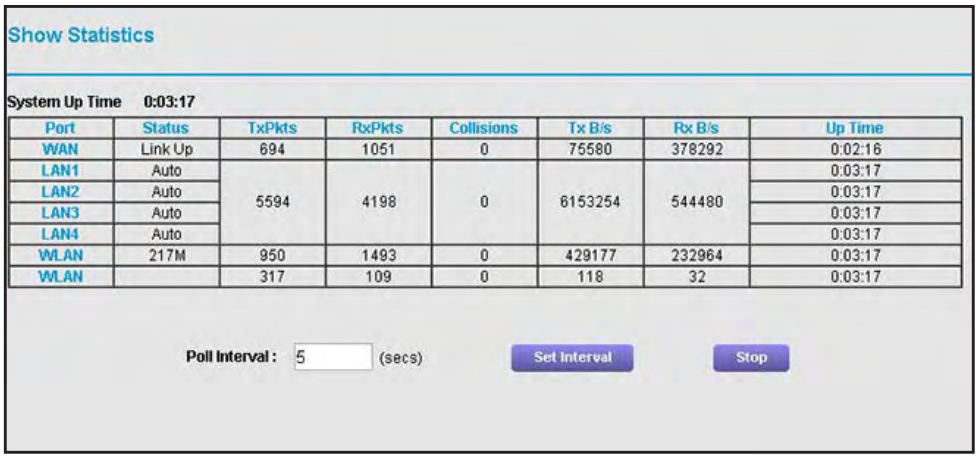
   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays.

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

   The Show Statistics pop-up screen displays.



If this screen does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups. The cable data gateway could also block pop-ups. For information about allowing pop-ups on the cable data gateway, see *Manage Firewall, Web, and NAT ALG Security* on page 73.

The following table describes the fields and columns of the Show Statistics pop-up screen.

Field or Column	Description
System Up Time	The time elapsed since the cable data gateway was last restarted.
Port	The statistics for the WAN port (that is, the cable Internet port that connects to the Internet), LAN (Ethernet) ports, and WLAN (WiFi) ports. For each port, the screen displays the information that is described in this table.
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 traffic statistics polling frequency or stop polling:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays.
6. In the Internet Port pane, click the **Show Statistics** button.

   The Show Statistics pop-up screen displays.

   If this screen does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups. The cable data gateway could also block pop-ups. For information about allowing pop-ups on the cable data gateway, see *Manage Firewall, Web, and NAT ALG Security* on page 73.
7. Change the polling frequency or stop polling:
   - To change the polling frequency:
     a. In the **Poll Interval** field, enter a time in seconds.
     b. Click the **Set Interval** button.
   - To stop polling, click the **Stop** button.

View the Internet Port Connection Status and Release and Renew the Connection

You can view information about the cable Internet connection of the cable data gateway. You can also release and renew the connection.

➢ **To view the status of the cable Internet connection of the cable data gateway and release the connection and renew the connection:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

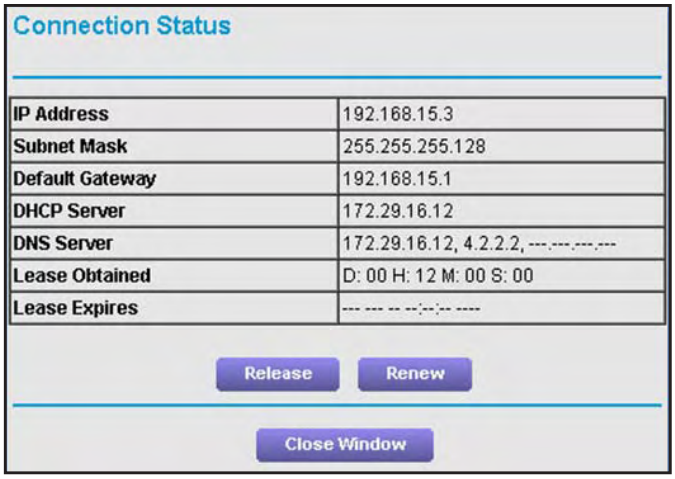
   The BASIC Home screen displays.

5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays.

6. In the Internet Port pane, click the **Connection Status** button.

   The Connection Status pop-up screen displays.



If this screen does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups. The cable data gateway could also block pop-ups. For information about allowing pop-ups on the cable data gateway, see *Manage Firewall, Web, and NAT ALG Security* on page 73.

The following table describes the fields of the Connection Status pop-up screen.

Field	Description
IP Address	The IP address that is assigned by the cable service provider to the cable data gateway.
Subnet Mask	The subnet mask that is assigned by the cable service provider to the cable data gateway.
Default Gateway	The IP address of the default gateway of the cable service provider that the cable data gateway communicates with.
DHCP Server	The IP address of the Dynamic Host Configuration Protocol (DHCP) server of the cable service provider that provides translation of network names to IP addresses.
DNS Server	The IP address of the Domain Name Service (DNS) server of the cable service provider that provides translation of network names to IP addresses.
Lease Obtained	The day and time that the lease was obtained.
Lease Expires	The day and time that the lease expires.

7. To release the connection, click the **Release** button.

   The connection with your cable service provider is shut down, as is your Internet connection.

8. To renew the connection, click the **Renew** button.

   The connection with your cable service provider is reestablished, as is your Internet connection. If a DHCP connection with your cable service provider exists, the cable data gateway receives a new DHCP lease and might receive a new IP address.

9. Click the **Close Window** button.

   The pop-up screen closes.

View the WiFi Cable Data Gateway Cable Initialization

You can track the initialization procedure of the cable data gateway and get details about the downstream and upstream cable channels. The time is displayed after the cable data gateway is initialized.

The cable data gateway automatically goes through the following steps in the provisioning process:

1. Scans and locks the downstream frequency and then ranges the upstream channels.
2. Obtains a WAN IP address for the cable data gateway.
3. Connects to the Internet.

➢ **To view the status of the cable data gateway initialization:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

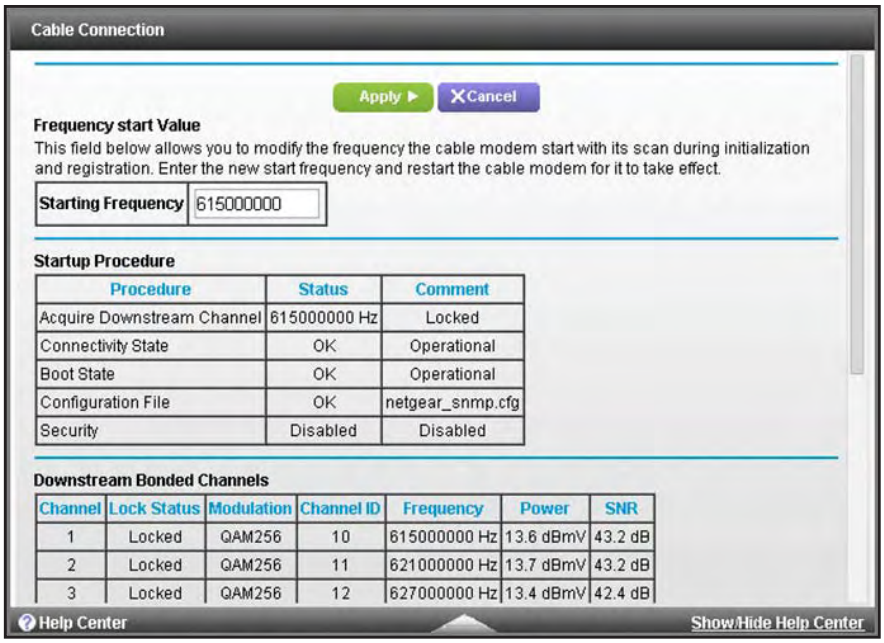
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **Cable Connection**.

   The Cable Connection screen displays.



The Startup Procedure section displays the initialization progress.

The Downstream Bonded Channels section displays the status of each channel.

6. To see the Upstream Bonded Channels section and system time, scroll down.

View the Network Map

You can view the active wired and WiFi devices in both the network to which the cable data gateway is connected and the cable data gateway network. If you do not recognize a WiFi device, it might be an intruder.

➢ **To display the wired and WiFi devices:**

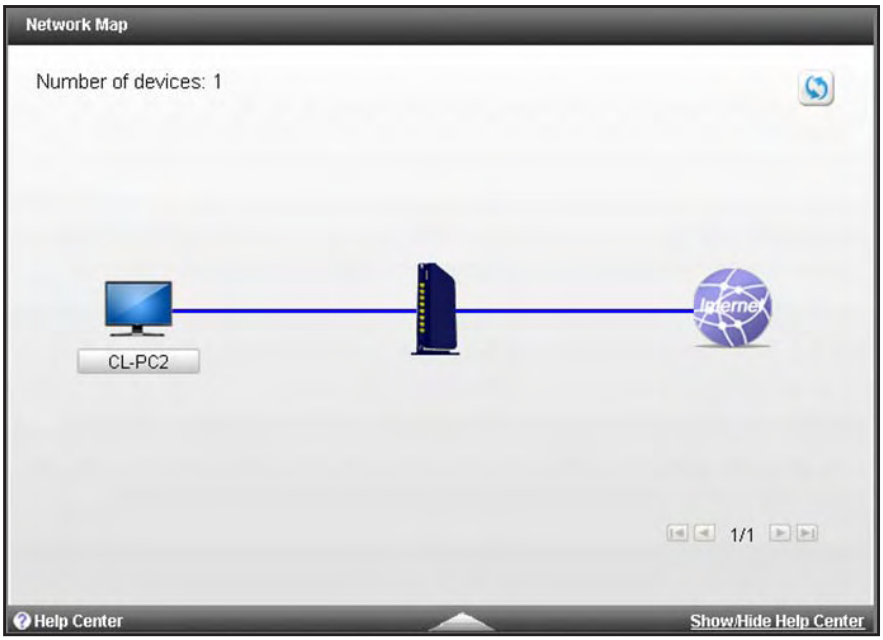
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **Network Map**.

   The Network Map screen displays.



If a connection is broken, no blue line displays between the device and the cable data gateway, between the cable data gateway and the Internet, or both. If a connection is over WiFi rather than an Ethernet cable, a WiFi icon displays on the blue line.

6. If more than one device is connected to the cable data gateway, use the arrow icons in the lower right to scroll through the screens.
7. To refresh the screen, click the refresh icon in the upper right.

   The information onscreen is updated.

View WiFi Channels in Your Environment

You can view the active WiFi channels in your environment, including the channels that the cable data gateway is broadcasting on. If several WiFi networks in your environment are using the same channel as the one that the cable data gateway is using, interference might occur. In that situation, you might want to change the channel that the cable data gateway is using.

Note: Many countries and geographic locations implement laws or guidelines about which channels can be used. Depending on your location, some channels might not be available.

➢ **To view the WiFi channels in your environment:**

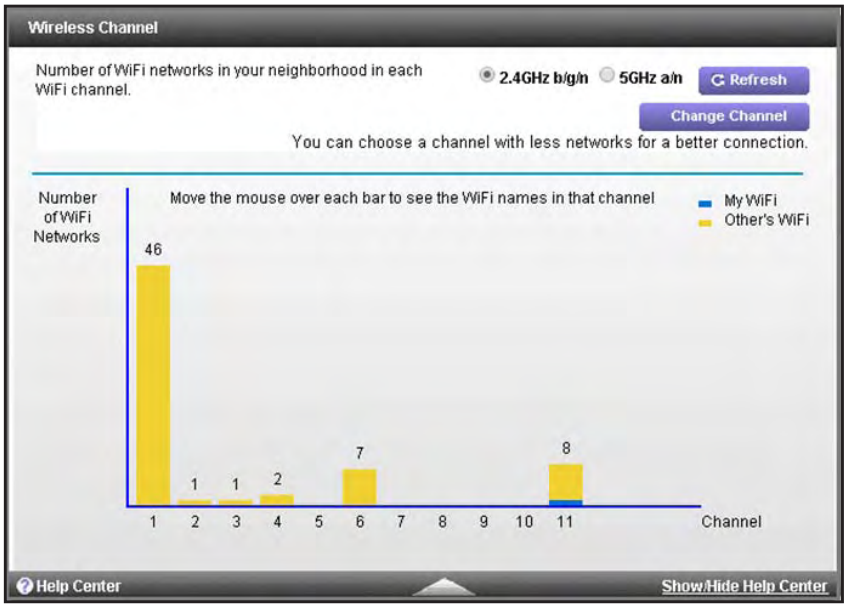
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Wireless Channel**.

   The Wireless Channel screen displays.



   By default, the screen displays the active channels in the 2.4 GHz band.

   The channel that the WiFi network of the cable data gateway is using displays in blue. The channels that other WiFi network in your environment are using display in yellow.
6. To display the active channels in the 5 GHz band, select the **5GHz a/n** radio button.

   The screen displays the active channels in the 5 GHz band.
7. To refresh the screen, click the **Refresh** button.

   The information onscreen is updated.

   To change the channel that a radio of the cable data gateway is using, click the **Change Channel** button. The Wireless Setup screen displays. For information about changing the WiFi settings for the main WiFi network, including the channel, see *View or Change the Basic Settings for the Main WiFi Network* on page 31.

View WiFi Access Points in Your Environment

You can view the WiFi access points (APs) that are broadcasting WiFi networks in your environment. These are APs other than the cable data gateway. For each WiFi network, the security level and the signal strength are displayed.

➢ **To view the WiFi APs in your environment:**

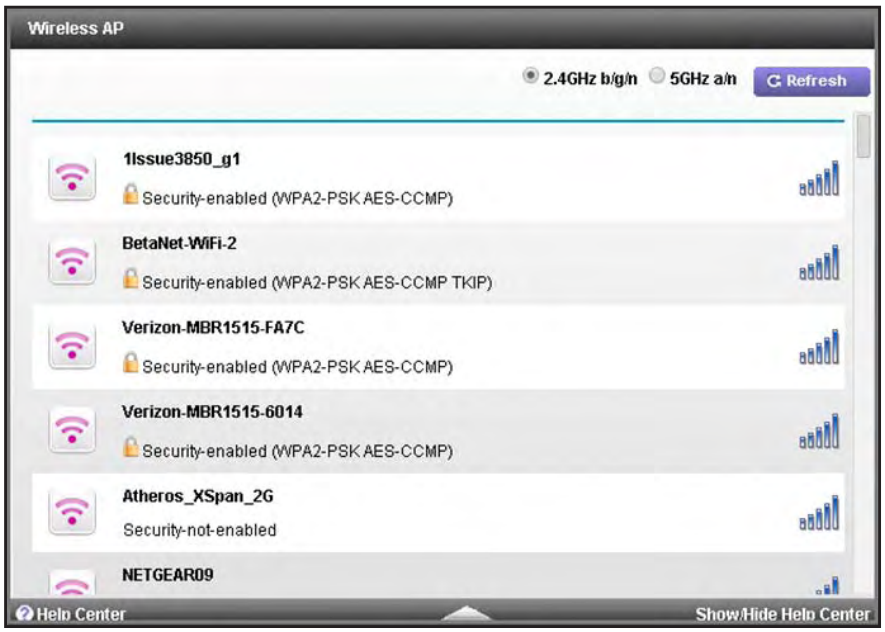
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Wireless AP**.

   The Wireless AP screen displays.



   By default, the screen displays the APs in the 2.4 GHz band.
6. To display the APs in the 5 GHz band, select the **5GHz a/n** radio button.

   The screen displays the APs in the 5 GHz band.
7. To refresh the screen, click the **Refresh** button.

   The information onscreen is updated.

View and Manage the Log

The log is a detailed record of websites that users accessed, attempts to access blocked sites, cable data gateway operation, DoS attacks and port scans, WiFi access, and other information. Up to 256 entries can be stored in the log.

If you enabled email notification, you receive these logs in an email message. For more information, see *Set Up Security Event Email Notification* on page 72.

Note: For information about the event log, which is a log that records events that occur between the cable data gateway and the cable service provider's cable modem termination system (CMTS), see *View and Manage the Event Log* on page 157.

➢ **To view, clear, or send the log and specify what is included in the log:**

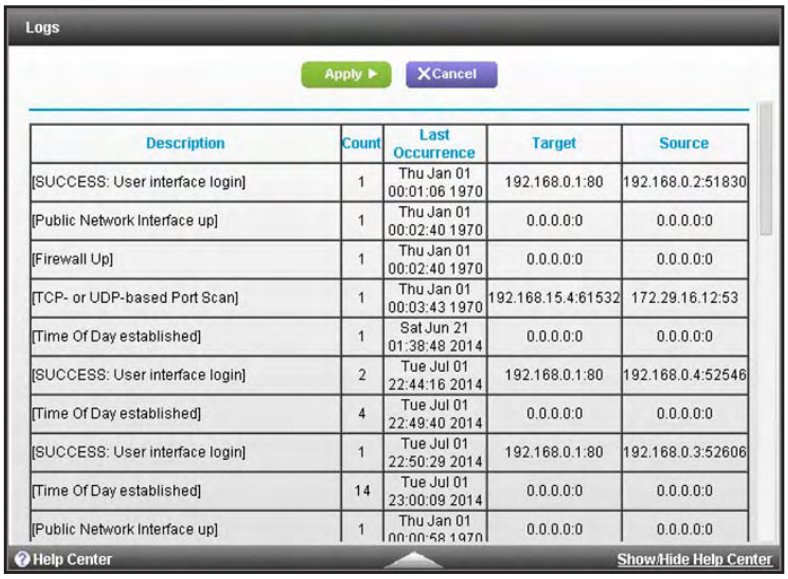
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Administration > Logs**.

   The Logs screen displays.



The Logs screen displays a table that shows for each event a description, the number of times the events occurred, the date and time of the last occurrence, the target IP address and port, and the source IP address and port.

6. Scroll down.

   The bottom of the screens shows check boxes and buttons.

7. To specify which types of events are logged, scroll down and select or clear the check boxes.

   By default, all the check boxes are selected and the associated events are logged.

8. If you make any changes, click the **Apply** button at the top of the screen.

   Your settings are saved.

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

   The information onscreen is updated.

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

    This feature can be useful for testing your email settings. For this feature to function, you first must enable email notification. For more information, see *Set Up Security Event Email Notification* on page 72.

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

    All entries are removed from the table.

Manage the WiFi Cable Gateway Settings

The configuration settings of the cable data gateway are stored within the cable data gateway in a configuration file. You can back up (save) this file to your computer or restore it.

Back Up the Settings

You can save a copy of the current configuration settings.

➢ **To back up the cable data gateway's configuration settings:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

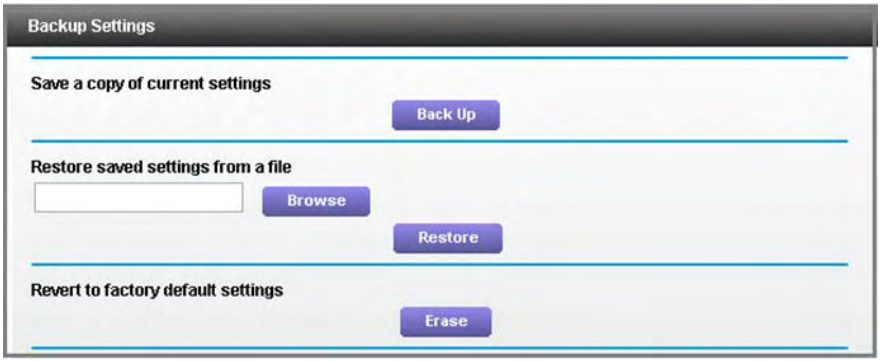
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Backup Setting screen displays.



6. Click the **Back Up** button.
7. Choose a location to store the file on a device on your network.

   The name of the backup file is `NETGEAR_<model number>.cfg`. in which `<model number>` is the model number of your cable data gateway.

8. Follow the directions of your browser to save the file.

Restore the Settings

If you backed up the configuration file, you can restore the configuration from this file.

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

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

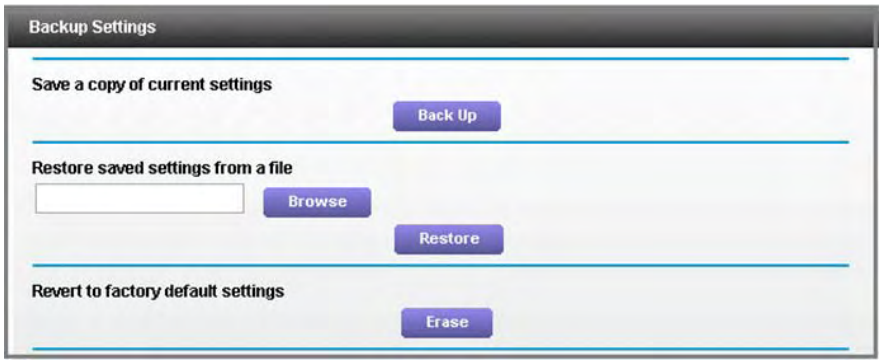
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

The Backup Setting screen displays.



6. Enter the full path to the file on your network or click the **Browse** button to find the file.

   The name of the backup file from which you can restore the configuration is `NETGEAR_<model number>.cfg`. in which `<model number>` is the model number of your cable data gateway.

7. Follow the directions of your browser to locate the file, and select it.
8. Click the **Restore** button.

   The configuration is uploaded to the cable data gateway. When the restoration is complete, the cable data gateway reboots.

WARNING:

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

Return the WiFi Cable Data Gateway to Its Factory Default Settings

Under some circumstances (for example, if you lost track of the changes that you made to the cable data gateway settings or you move the cable data gateway to a different network), you might want to erase the configuration and reset it to factory default settings.

If you do not know the current LAN IP address of the cable data gateway, first try to use an IP scanner application to detect the IP address before you reset the cable data gateway to factory default settings.

To reset the cable data gateway to factory default settings, you can use either the **Reset** button on the side of the cable data gateway or the Erase function in the web management interface. However, if you cannot find the LAN IP address or lost the password to access the cable data gateway, you must use the **Reset** button.

After you reset the cable data gateway to factory default settings, the user name is admin, the password is password, the LAN IP address is 192.168.0.1 (which is the same as www.routerlogin.net), and the DHCP server is enabled. For a list of factory default settings, see *Factory Default Settings* on page 164.

Use the Reset Button

CAUTION:

This process erases all settings that you configured in the cable data gateway.

➢ **To reset the cable data gateway to factory default settings:**

1. On the back panel of the cable data gateway, look for the small hole in which the **Reset** button is located.

   For more information about the location of the **Reset** button, see the Back Panel sections in *Chapter 1, Hardware Overview*.

2. Insert a straightened paper clip into the hole and press for at least seven seconds.

   The Power LED blinks amber.

3. Release the button.

   The cable data gateway resets and restarts. This process takes about one minute.

WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not turn off the cable data gateway.

Erase the Settings

CAUTION:

This process erases all settings that you configured in the cable data gateway.

➢ **To erase the settings:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

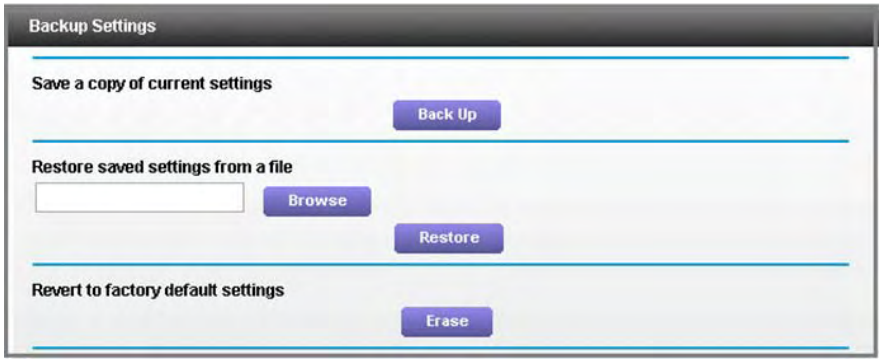
If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Backup Setting screen displays.



6. Click the **Erase** button.

   The configuration is reset to factory default settings. When the restoration is complete, the cable data gateway reboots.

WARNING:

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

Reboot the Cable Data Gateway

You can reboot the cable data gateway from the web management interface.

➢ **To reboot the cable data gateway from the web management interface:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays.

6. In the Cable Information pane, click the **Reboot** button.

   A warning message displays.

7. To confirm the reboot, click the **OK** button.

   The cable data gateway reboots.

WARNING:

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

7. Share USB Drives Attached to the Cable Data Gateway

This chapter describes how to access and configure a USB storage drive attached to your cable data gateway. The USB port on the cable data gateway can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, CD drives, or DVD drives to the cable data gateway USB port.

This chapter contains the following sections:

Note: For more information about ReadySHARE features, visit *www.netgear.com/readyshare*.

USB Drive Requirements

The cable data gateway works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives that the cable data gateway supports, visit *http://kbserver.netgear.com/readyshare*.

Some USB external hard drives and flash drives require you to load the drivers onto the computer before the computer can access the USB device. Such USB devices do not work with the cable data gateway.

The cable data gateway supports the following file system types:

- FAT (read/write)
- NTFS (read)
- EXT2 (read/write)
- EXT3 (read/write)
- EXT4 (read/write)
- HFS (read)
- HFS+ (read)

Access a USB Drive on the Network

ReadySHARE lets you access and share a USB drive that is connected to the cable data gateway USB port. (If your USB drive requires special drivers, it is not compatible.)

➢ **To connect a USB drive:**

1. Insert your USB storage drive into the USB port on the back panel of the cable data gateway.
2. If your USB drive requires a power supply, you must use it when you connect the USB drive to the cable data gateway.

   When you connect the USB drive to the cable data gateway USB port, it might take up to two minutes before it is ready for sharing. By default, the USB drive is available to all computers on your local area network (LAN).

➢ **To access the USB drive from a Mac:**

1. Select **Go > Connect to Server**.
2. Enter **smb://readyshare** as the server address.
3. Click the **Connect** button.

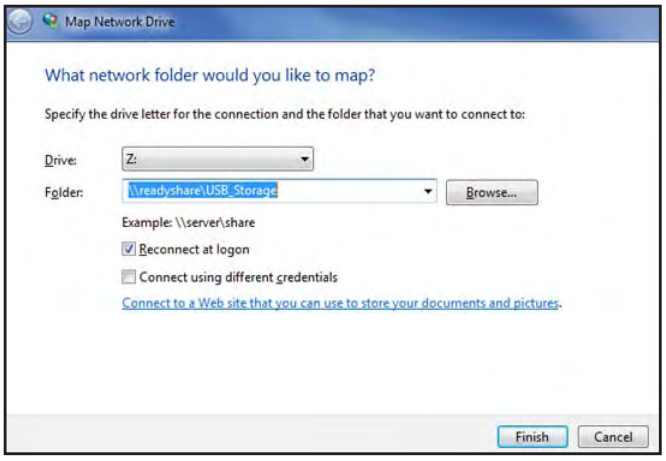
➢ **To access the USB drive from a Windows computer:**

1. Select **Start > Run**.
2. Enter **\\readyshare** in the dialog box and click the **OK** button.

➢ **To map the USB device to a Windows network drive:**

1. Visit *www.netgear.com/readyshare*.
2. In the ReadySHARE USB Storage Access pane, click the **PC Utility** link.

   The `readyshareconnect.exe` file is downloaded to your computer.
3. Launch `readyshareconnect.exe`.



4. Select the drive letter to map to the network folder.
5. To connect to the USB drive as a different user, select the **Connect using different credentials** check box and do the following:
   a. Type the user name and password.
   b. Click the **OK** button.
6. Click the **Finish** button.

   The USB drive is mapped to the drive letter that you specified.

Back Up Windows Computers with ReadySHARE Vault

Your cable data gateway comes with free backup software for all the Windows computers in your home. Connect a USB hard disk drive (HDD) to the USB port on your cable data gateway for centralized, continuous, and automatic backup.

➢ **To back up your Windows computer:**

1. Connect a USB HDD to a USB port on the cable data gateway.
2. Install the genie app on each Windows computer.

   To download the genie app, visit *www.netgear.com/genie*.
3. Download ReadySHARE Vault from *www.netgear.com/readyshare* and install it on each Windows computer.
4. Launch ReadySHARE Vault.
5. Use the dashboard or the **Backup** tab to set up and run your backup.

Specify the Method for Accessing the USB Drive

You can specify the device name, workgroups, and method for accessing network folders for your USB device.

➢ **To specify the method for accessing the USB drive:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.

   The USB Storage (Advanced Settings) screen displays.

6. Specify access to the USB storage device:
   - **Network Device Name**. This is the name used to access the USB device connected to the cable data gateway. The default name is readyshare.
   - **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. The default name is WORKGROUP.

- **Access Method**. By default USB access to the network, HTTP, and FTP are enabled. (File Transfer Protocol [FTP] lets you send and receive large files fast.) You can disable access by clearing the **Enable** check boxes to the left of the Network Neighborhood, HTTP, and FTP entries in the table.

7. If you changed the settings, click the **Apply** button.

   Your changes are saved.

View Network Folders on a USB Drive

You can view the network folders on the USB storage device.

➢ **To view network folders:**

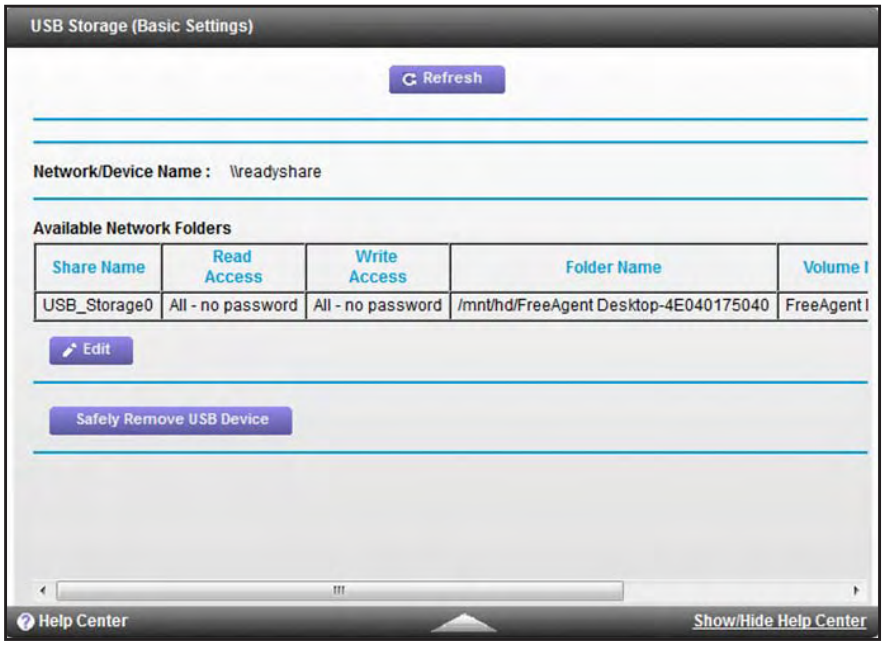
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ReadyShare**.

   The USB Storage (Basic Settings) screen displays.



The table in the Available Networks Folder section shows the following settings:

- **Share Name**. The default share name is USB_Storage0.

  If Not Shared displays, the default share is deleted, and no other share for the root folder exists. For information about how to change this situation, see *Add a Network Folder on a USB Drive* on page 103.

- **Read Access and Write Access**. The permissions and access controls on the network folder.

  All–no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same one that you use to log in to the cable data gateway. For information about changing read and write access, see *Change a Network Folder, Including Read and Write Access, on a USB Drive* on page 104.

- **Folder Name**. The full path of the network folder.
- **Volume Name**. The volume name from the storage device (either USB drive or HDD).
- **Total Space and Free Space**. The current utilization of the storage device.

Add a Network Folder on a USB Drive

You can add network folders on the USB storage device.

➢ **To add a network folder:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

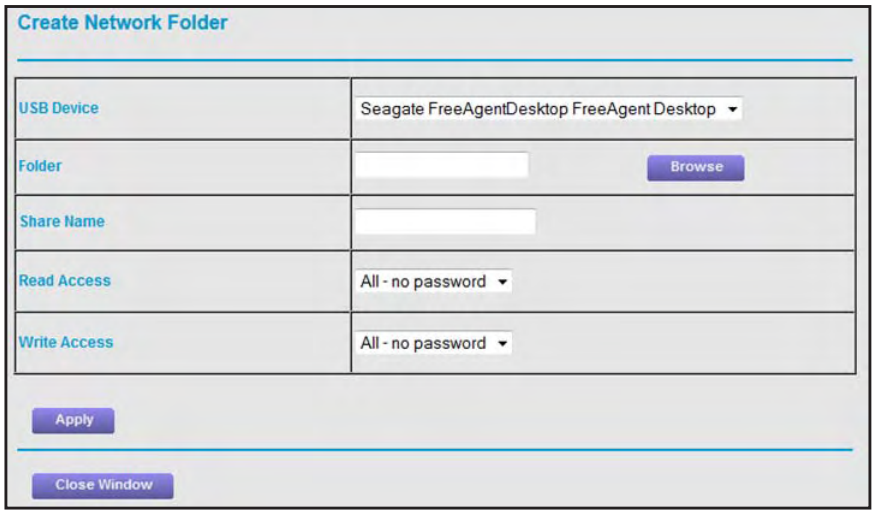
   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.

   The USB Storage (Advanced Settings) screen displays.
6. Click the **Create Network Folder** button.

   The Create Network Folder screen displays.



7. In the **USB Device** menu, select the USB drive.

   Note: Best practise is not to attach more than one drive to the USB port (for example, through a USB hub).

8. Click the **Browse** button and in the **Folder** field, select the folder.
9. In the **Share Name** field, type the name of the share.
10. From the **Read Access** menu and the **Write Access** menu, select the settings that you want.

    All–no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same one that you use to log in to the cable data gateway.

11. Click the **Apply** button.

    The folder is added on the USB device.

Change a Network Folder, Including Read and Write Access, on a USB Drive

You can change the settings for a network folder on a USB drive.

➢ **To change a network folder:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

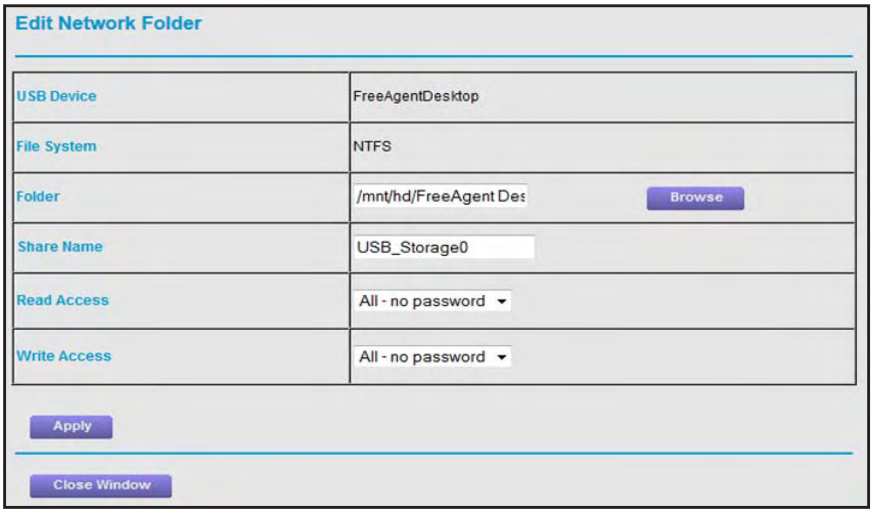
If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Click the **Edit** button.

   The Edit Network Folder screen displays.



6. Change the settings in the fields as needed.

   For more information about the settings, see *Add a Network Folder on a USB Drive* on page 103.

7. Click the **Apply** button.

   Your changes are saved.

Safely Remove a USB Drive

Before you physically disconnect a USB drive from the cable data gateway USB port, log in to the cable data gateway and take the drive offline.

➢ **To remove a USB disk drive safely:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ReadyShare**.

   The USB Storage (Basic Settings) screen displays.

6. Click the **Safely Remove USB Device** button.

   The drive goes offline.

7. Physically disconnect the USB drive.

Enable the Media Server

The cable data gateway can function as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV-compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

➢ **To enable the media server, specify its settings, and scan for media content:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

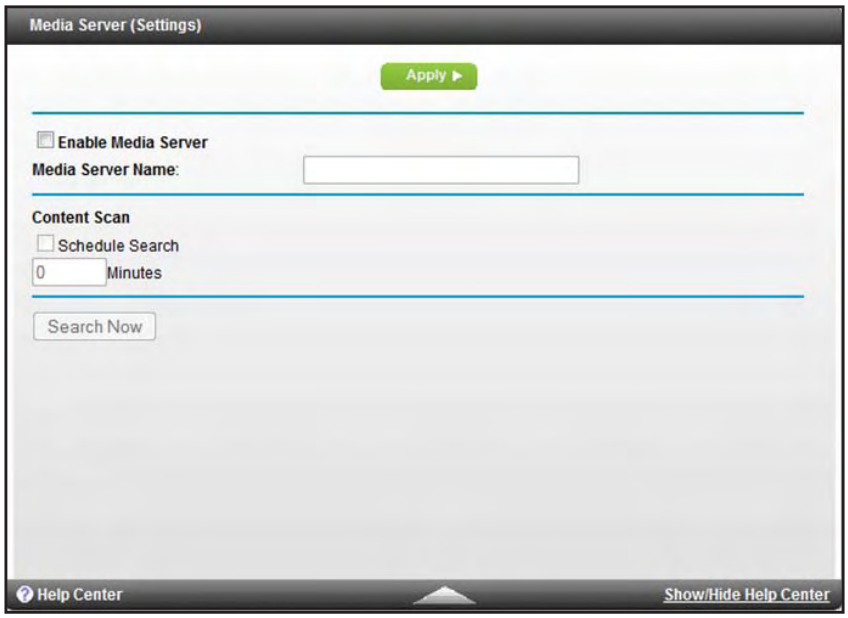
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > USB Storage > Media Server**.

   The Media Server (Settings) screen displays.



6. To enable the cable data gateway to function as a media server, select the **Enable Media Server** check box.
7. In the **Media Server Device Name** field, specify the name of the media server.
8. Click the **Apply** button.

   Your changes are saved.
9. To schedule a content scan or scan for content immediately, take one of the following actions:
   - Select the **Schedule Search** check box and enter a period in the **Minutes** field to specify the interval at which the cable data gateway must search for (updated) content.
   - Click the **Search Now** button.

     The cable data gateway searches for content immediately.

Configure Advanced Features

8

This chapter describes the advanced features of your cable data gateway. Networking knowledge is needed to implement some of these features.

This chapter includes the following sections:

Manage Advanced WiFi Settings

You can turn the WiFi radio on and off, configure advanced WiFi settings, specify WPS settings, and set up a WiFi access list.

Note: The cable data gateway is already configured with the optimum settings. Do not alter these settings unless directed by Cox Support. Incorrect settings might disable the WiFi radio.

Control the WiFi Radios

By default, the 2.4 GHz and 5 GHz WiFi radios are enabled so that you can connect over WiFi to the cable data gateway. You can turn the WiFi radio on or off. When the WiFi radio is off, you can still use an Ethernet cable for a LAN connection to the cable data gateway.

Note: The WiFi **On/Off** button on the front panel is disabled.

➢ **To turn the radio on or off or change advanced settings for your WiFi network:**

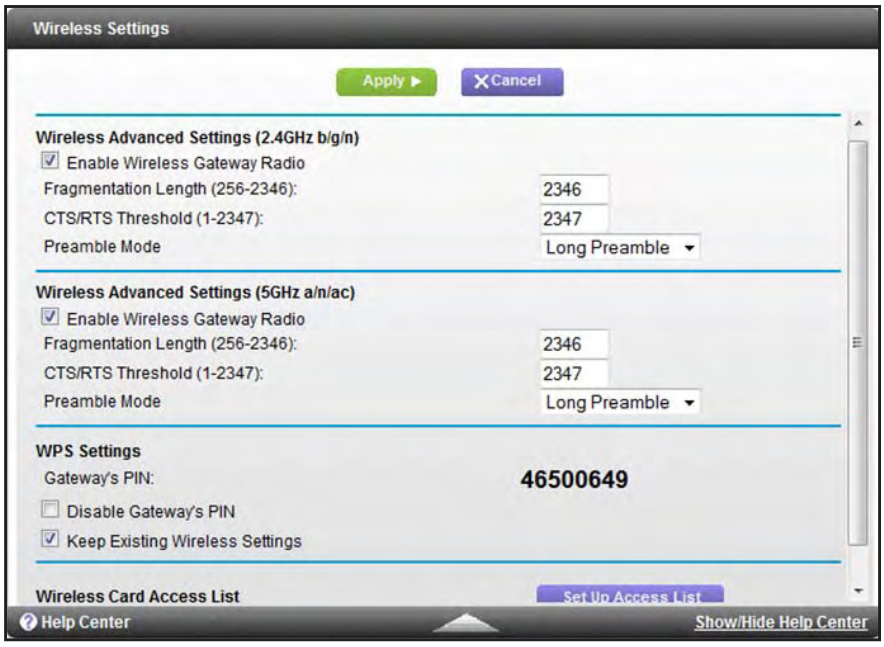
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings screen displays (that is, the screen to configure advanced settings).



6. Change the advanced WiFi settings for the 2.4 GHz and 5 GHz radios:
   - **Enable Wireless Router Radio**. By default, the **Enable Wireless Router Radio** check box is selected and the WiFi radio is enabled.

     Clearing this check box turns off the WiFi radio of the cable data gateway. When the WiFi radio is disabled, you can still use the cable data gateway by connecting devices with an Ethernet cable.
   - **Fragmentation Length (256-2346)**, **CTS/RTS Threshold (1-2347)**, and **Preamble Mode**. These settings are reserved for WiFi testing and advanced configuration only. Do not change these settings unless directed by Cox Support. Incorrect settings might disable the WiFi function of the cable data gateway unexpectedly.

     The following settings are the default settings:
     - **Fragmentation Length**. 2346
     - **CTS/RTS Threshold**. 2347
     - **Preamble Mode**. Long Preamble
7. Click the **Apply** button.

   Your settings are saved.

View or Change WPS Settings

You can control how WPS functions on the cable data gateway. Use caution if you change the WPS settings.

Note: For information about how to use WPS to add WiFi devices and other equipment to your WiFi network, see *Join the WiFi Network of the WiFi Cable Data Gateway* on page 26 and *Use the WPS Wizard to Add a Device to the WiFi Network* on page 52.

➢ **To specify WPS settings:**

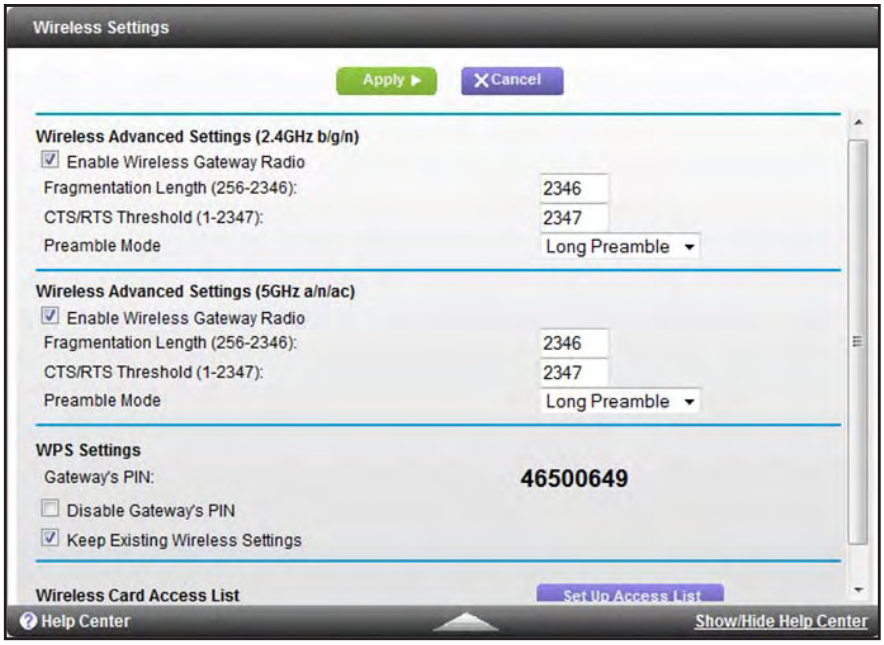
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings screen displays (that is, the screen to configure advanced settings).



The **Gateway's PIN** field displays the PIN that you can enter on a registrar (for example, Windows Connect Now in Microsoft Windows 7) to configure the cable data gateway's WiFi settings through WPS.

6. Specify the WPS settings:
   - **Disable Gateway's PIN**. By default, the PIN is enabled, but situations might occur in which you want to disable the PIN. The PIN function might temporarily be disabled when the cable data gateway detects suspicious attempts to break into the cable data gateway's WiFi settings through use of the cable data gateway's PIN and WPS. You can manually disable the PIN function by selecting the **Disable Router's PIN** check box.
   - **Keep Existing Wireless Settings**. By default, the **Keep Existing Wireless Settings** check box is selected. Best practise is to leave this check box selected. However, when the check box is selected, some applications might not detect the cable data gateway.

CAUTION:

When you clear the **Keep Existing Wireless Settings** check box and you add a new WiFi client through WPS, the cable data gateway's WiFi settings change to an automatically generated SSID and passphrase (also referred to as the WiFi network password or network key).

7. Click the **Apply** button.

   Your settings are saved.

Set Up a WiFi Access List by MAC Address

By default, any WiFi device that is configured with the correct SSID is allowed access to your main and guest WiFi networks. For increased security, you can restrict access to the WiFi networks to allow only specific WiFi devices based on their MAC addresses. You can restrict access to the main WiFi network separately from the guest WiFi network.

Each network device uses a MAC address, which is a unique 12-character physical address containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the WiFi card or network interface device. Or you can display the MAC address using the network configuration utilities of the computer through the web management interface of the cable data gateway. For more information, see *Set Up and Enable a WiFi Access List* on page 113.

Note: If you use a WiFi computer to set up a WiFi access list, add your WiFi computer to the access list; otherwise, you are disconnected when you click the **Apply** button. To avoid this situation, use a computer with a wired connection to access the cable data gateway.

Set Up and Enable a WiFi Access List

You can add one or more devices to the WiFi access list for the main WiFi network and the guest WiFi network. The cable data gateway supports two access lists: one for the main WiFi network and one for the guest WiFi network.

➢ **To restrict WiFi access based on MAC addresses:**

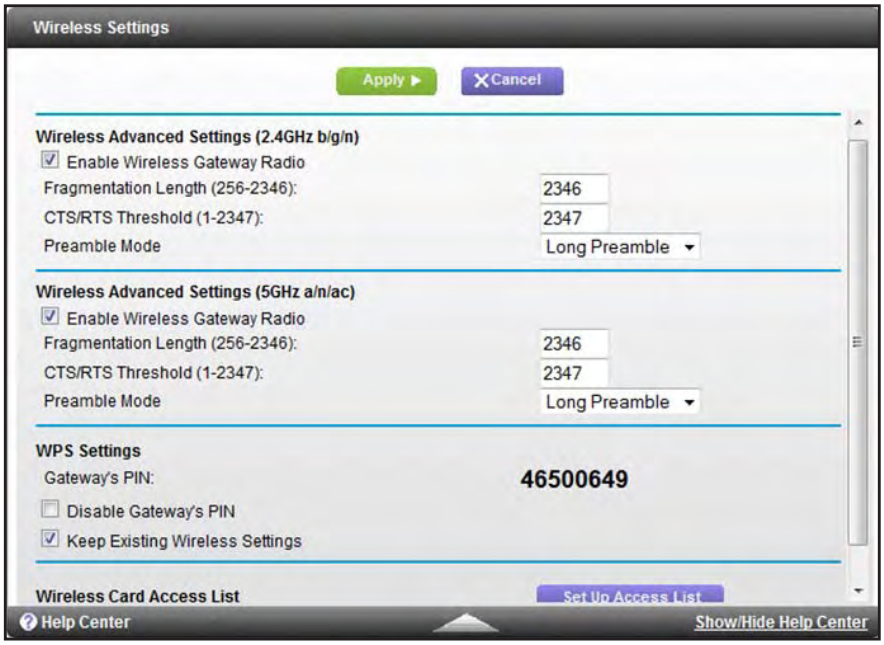
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.

   The Wireless Settings screen displays (that is, the screen to configure advanced settings).

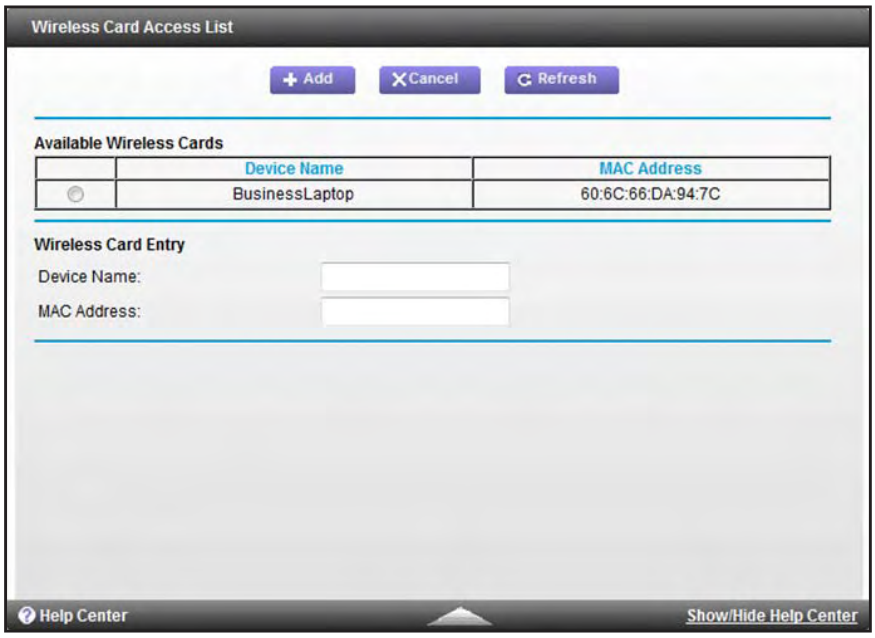


6. Click the **Set Up Access List** button.

   The Wireless Card Access List screen displays.

7. Select the network that the device that you are adding must be allowed or denied access to:
   - **Primary SSID**. The device is allowed or denied access to the main WiFi network.
   - **Guest Network SSID**. The device is allowed or denied access to the guest WiFi network.
8. Click the **Add** button.

   The screen adjusts.



9. In the **Device Name** field, type a name for the WiFi device.
10. In the **MAC Address** field, type the MAC address of the WiFi device.

    Tip: You can also select a device from the Available Wireless Cards table by selecting the corresponding radio button. If the device that you want to add is not listed, click the **Refresh** button to update the Available Wireless Cards table.

11. Click the **Add** button.

    The WiFi device is added to the table on the Wireless Card Access List screen.

12. To add another WiFi device, repeat *Step 8* through *Step 11*.

    Note: If you are connected to the cable data gateway over WiFi, make sure that you add your own device to an access list that allows access. If you do not, your device is denied access when you enable the access list and you must reconnect to the cable data gateway over an Ethernet cable.

13. Select the **Turn Access Control On** check box.
14. Select whether access is allowed or denied for this access list:
    - **Allows List**. All devices on the access list are allowed access to the network (either the main or the guest WiFi network).
    - **Deny List**. All devices on the access list are denied access to the network (either the main or the guest WiFi network).
15. Click the **Apply** button.

    Your settings are saved. Now only WiFi devices that are in the table on the Wireless Card Access List screen are allowed or denied access to the cable data gateway.

Change the Settings for a Device on the WiFi Access List

You can change the name or MAC address for a device on a WiFi access list.

➢ **To change the settings for a device on a WiFi access list:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

The Wireless Settings screen displays (that is, the screen to configure advanced settings).

6. Click the **Set Up Access List** button.

   The Wireless Card Access List screen displays.

7. Select the access list for which you are changing the settings of a device:
   - **Primary SSID**. The access list for the main WiFi network.
   - **Guest Network SSID**. The access list for the guest WiFi network.
8. In the table, select the radio button next to the device that you want to change.
9. Click the **Edit** button.

   The Edit Wireless Card screen displays.

10. Change the device name or MAC address.
11. Click the **Apply** button.

    The settings are saved and display in the table on the Wireless Card Access List screen. However, if you restart the cable data gateway, the changes are lost. You also must apply the changes on the Wireless Card Access List screen.

12. On the Wireless Card Access List screen, click the **Apply** button.

    Your settings are saved.

Remove a Device From the WiFi Access List

You can remove a device from a WiFi access list if you no longer want to allow or deny access to the device.

➢ **To remove a WiFi device from an access list:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Wireless Settings screen displays (that is, the screen to configure advanced settings).

6. Click the **Set Up Access List** button.

   The Wireless Card Access List screen displays.

7. Select the access list from which you are removing a device:
   - **Primary SSID**. The access list for the main WiFi network.
   - **Guest Network SSID**. The access list for the guest WiFi network.
8. In the table, select the radio button next to the device that you want to remove.

   Note: If you are connected to the cable data gateway over WiFi, make sure that you do not remove your own device from an access list that allows access. If you do, your device is denied access and you must reconnect to the cable data gateway over an Ethernet cable.

9. Click the **Delete** button.

   The device is removed from the table on the Wireless Card Access List screen.
10. Click the **Apply** button.

    Your settings are saved.

Port Forwarding and Port Triggering Concepts

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

- To enable remote computers on the Internet to access a server on your local network
- To enable certain applications and games to work correctly if the cable data gateway does not recognize their replies

Your cable data gateway provides two features for creating these exceptions: port forwarding and port triggering. For more information, see the following sections:

- *Remote Computer Access Basics* on page 117
- *Port Triggering to Open Incoming Ports* on page 119
- *Port Forwarding to Permit External Host Communications* on page 120
- *How Port Forwarding Differs from Port Triggering* on page 121

For information about how to configure port forwarding, see *Set Up Port Forwarding to Local Computers* on page 121.

For information about how to configure port triggering, see *Set Up and Manage Port Triggering* on page 127.

Remote Computer Access Basics

When a computer on your network must access a computer on the Internet, your computer sends your cable data gateway a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your cable data gateway must 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 in the URL field, and your computer creates a web page request message that it sends to your cable data gateway. The message contains the following information:
   - **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 cable data gateway 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 cable data gateway 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 cable data gateway's public IP address. This requirement 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 cable data gateway, such as 33333. This requirement is necessary because two computers might independently be using the same port number.

   Your cable data gateway 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 web server then sends this reply message to your cable data gateway. The return message 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**. The public IP address of your cable data gateway
   - **Destination port number**. 33333
5. When your cable data gateway receives the incoming message, it checks its session table for an active session for port number 33333. Finding an active session, the cable data gateway then modifies the message to restore the original address information replaced by NAT. Your cable data gateway 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 cable data gateway eventually detects a period of inactivity in the communications and removes the session information from its session table. Incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

Some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your cable data gateway, you can tell the cable data gateway to open more 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 cable data gateway, “When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer.” The following sequence shows the effects of this port triggering rule:

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 cable data gateway.
3. Your cable data gateway creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your cable data gateway 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. When the cable data gateway detects the port triggering rule and the destination port number of 6667, it 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 cable data gateway using the NAT-assigned source port (for example, port 33333) as the destination port and sends an “identify” message to your cable data gateway with destination port 113.
6. When your cable data gateway detects the incoming message to destination port 33333, it checks its session table for an active session for port number 33333. Finding an active session, the cable data gateway restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your cable data gateway detects the incoming message to destination port 113, it checks its session table and learns that an active session for port 113 is associated with your computer. The cable data gateway 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 cable data gateway eventually detects a period of inactivity in the communications. The cable data gateway 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 must know which inbound ports the application needs. Also, you must know the number of the outbound port that will trigger the opening of the inbound ports. You can usually find this information by contacting the publisher of the application or the user groups or news groups.

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

Port Forwarding to Permit External Host Communications

In the examples in *Remote Computer Access Basics* on page 117 and *Port Triggering to Open Incoming Ports* on page 119, 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 cable data gateway 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 web server example in *Port Triggering to Open Incoming Ports* on page 119. In this case, a remote computer's browser must access a web server running on a computer in your local network. Using port forwarding, you can tell the cable data gateway, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.0.123."

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

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 cable data gateway. 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 cable data gateway
   - **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 cable data gateway.
2. Your cable data gateway 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 must be forwarded to local IP address 192.168.0.123. Therefore, your cable data gateway modifies the destination information in the request message.

   The destination address is replaced with 192.168.0.123.

   Your cable data gateway then sends this request message to your local network.
3. Your web server at 192.168.0.123 receives the request and composes a return message with the requested web page data and sends this reply message to your cable data gateway.

4. Your cable data gateway 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 must know which inbound ports the application needs. You usually can find this information by contacting the publisher of the application or the relevant user groups or news groups.

How Port Forwarding Differs from Port Triggering

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

- Any computer on your network can use port triggering, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- With port triggering, the cable data gateway does not need to 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 Computers

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.

You can configure the cable data gateway 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 you start, 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 must always receive the same IP address.

To ensure that your server computer always receives the same IP address, use the reserved IP address feature of your product. For more information, see *Manage IP Address Reservation* on page 49.

➢ **To forward specific incoming protocols and enable or schedule port forwarding:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Port Forwarding / Port Triggering screen displays.

6. Leave the **Port Forwarding** radio button selected as the service type.
7. From the **Service Name** menu, select the service or game that you plan to host on your network.

   If the service does not display in the menu, see *Manage Services or Applications for Port Forwarding* on page 123.

8. In the **Server IP Address** field, complete the IP address of your local device that must receive the inbound traffic that is covered by this service.
9. Click the **Apply** button.

   The service or application is added to the Port Forwarding Portmap Table. The **Enable** check box is selected automatically.

10. In the Port Forwarding section, selects how the cable data gateway applies port forwarding:
    - **Per Schedule**. Port forwarding is enabled according the schedule that you must select from the menu.

      For more information, see *Schedule When Features Are Active* on page 68.
    - **Always**. Port forwarding is always enabled.

Note: By default, the **Never** radio button is selected and port forwarding is disabled, even if you specified services and applications in the table.

11. Click the **Apply** button.

    Your settings are saved.

Manage Services or Applications for Port Forwarding

Before you define a service, game, or application that does not display in the **Service Name** menu on the Port Forwarding / Port Triggering screen, first determine which port number or range of numbers the application uses. You can usually find this information by contacting the publisher of the application or user groups or news groups.

Add a Service or Application for Port Forwarding

If the service or application that you want to use for port forwarding is not a default service that is already included in the menu, you can add it as a custom service.

➢ **To add a custom service for port forwarding:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Leave the **Port Forwarding** radio button selected as the service type.
7. Click the **Add Custom Service** button.

   The Ports - Custom Service screen displays.

8. Specify the custom service or application.

   The following table describes the fields on the Ports - Custom Service screen.

Field	Description
Service Name	Enter a descriptive name.
Service Type	From the menu, select the correct type of protocol for the service or application (**TCP**, **UDP**, or **TCP/UDP**). **Note:** If you are not sure which protocol to select, select **TCP/UDP**.
External Starting Port	Enter the external starting port number for the service or application.
External Ending Port	If the service or application uses a single port, enter the same port number that you enter in the **External Starting Port** field. If the service or application uses a range of ports, enter the ending port number of the range.
Use the same port range for Internal port	If the service or application uses the same internal ports port numbers that you specify for the external ports, select the check box.
Internal Starting Port	If the service or application does not use the same internal ports port numbers that you specify for the external ports, enter the internal starting port number for the service or application.
Internal Ending Port	This field is automatically completed when you enter a port number in the **Internal Starting Port** field.

Field	Description
Internal IP address	Complete the IP address of your local device that must receive the inbound traffic that is covered by this service or application.
External IP address	From the menu, select if either any external IP address can connect to the service or application or a single IP address only. If you select a single IP address, enter the IP address.

9. Click the **Apply** button.

   The custom service or application is added to the Port Forwarding Portmap Table. The **Enable** check box is selected automatically.

Change a Service or Application for Port Forwarding

You can change the settings for a default or custom service or application that you use for port forwarding.

➢ **To change the port forwarding settings for a default or custom service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Leave the **Port Forwarding** radio button selected as the service type.
7. In the table, select the radio button next to the service that you want to change.
8. Click the **Edit Service** button.

   The Ports - Custom Services screen displays.
9. Change the settings for the service.

   For information about the settings, see *Add a Service or Application for Port Forwarding* on page 123.
10. Click the **Apply** button.

    Your settings are saved. The changed settings for the service or application are shown in the Port Forwarding Portmap Table.

Disable a Service or Application for Port Forwarding

You can disable a port forwarding service or application without removing it from the Port Forwarding Portmap Table.

➢ **To disable a port forwarding service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Leave the **Port Forwarding** radio button selected as the service type.
7. In the table, clear the **Enable** check box for the service or application that you want to disable.
8. Click the **Apply** button.

   The service or application remains in the Port Forwarding Portmap Table but is disabled.

Remove a Service for Port Forwarding

You can remove a service or application that you no longer need for port forwarding.

➢ **To remove a port forwarding service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Leave the **Port Forwarding** radio button selected as the service type.

7. In the table, select the radio button to the left of the service that you want to remove.
8. Click the **Delete Service** button.

   The service or application is removed from the Port Forwarding Portmap Table.

   Note: A default service or application is not removed from the **Service Name** menu.

Application Example: Make a Local Web Server Public

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

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

   In this example, your cable data gateway always gives your web server an IP address of 192.168.0.33.

2. On the Port Forwarding / Port Triggering screen, configure the cable data gateway to forward the HTTP service to the local address of your web server at 192.168.0.33.

   HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your cable data gateway to use the name.

   To access your web server from the Internet, a remote user must know the IP address that your cable service provider assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dns.com.

Set Up and Manage 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 must open incoming ports that are different from the outgoing port.

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

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, keep Universal Plug and Play (UPnP) enabled for ease of configuration. For more information, see *Manage Universal Plug and Play* on page 143.

Manage Port Triggering Services and Applications

To configure port triggering services, you must know which inbound ports the service or application uses and the number of the outbound port that triggers the opening of the inbound ports. You can usually find this information by contacting the publisher of the service or application or through user groups or news groups on the Internet.

Add a Service or Application for Port Triggering

The cable data gateway does not provide default services or applications for port triggering. You must add each service and application for which you want to set up port triggering.

➢ **To add a port triggering service or application and enable or schedule port triggering:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

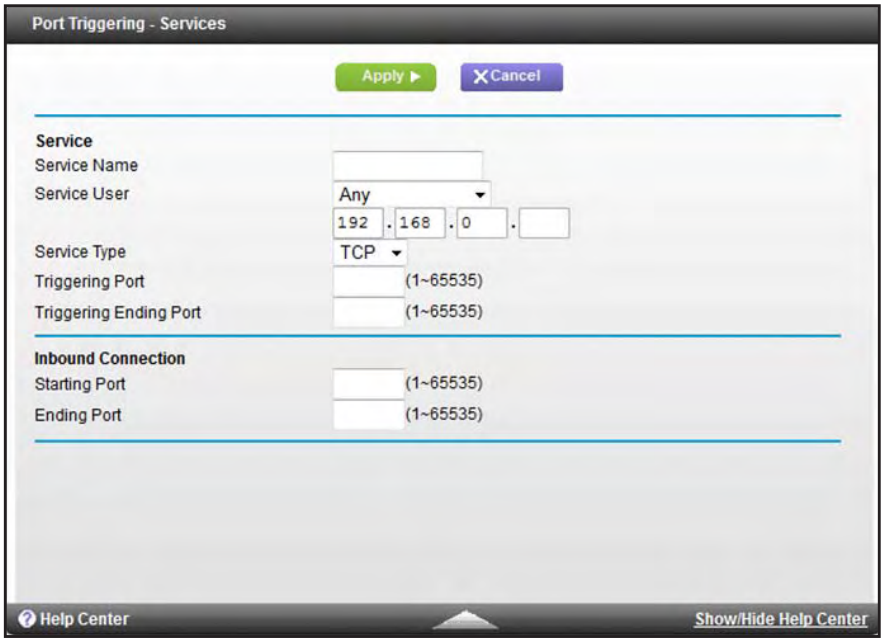
   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Select the **Port Triggering** radio button.

   The screen adjusts.

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

   The Port Triggering - Services screen displays.



8. Specify the custom service or application.

The following table describes the fields on the Port Triggering - Services screen.

Field	Description
Service	
Service Name	Enter a descriptive name.
Service User	From the menu, select if any internal IP address can connect to the service or application or only a single IP address can connect. If you select **Single address** from the menu, enter the IP address.
Service Type	From the menu, select the correct type of protocol for the service or application (**TCP** or **UDP**).
Triggering Port	Enter the internal starting port number for the service or application. This number represents the outbound traffic port that must cause the inbound ports (see Inbound Connection later in this table) to be opened.
Triggering Ending Port	If the service or application uses a single triggering port, enter the same port number that you enter in the **Triggering Port** field. If the service or application uses a range of triggering ports, enter the ending port number of the range.
Inbound Connection	
Starting Port	Enter the starting port number for the inbound connection. This number represents the inbound traffic port that is triggered open by the triggering port.
Ending Port	If the service or application uses a single ending port for the inbound connection, enter the same port number that you enter in the **Starting Port** field. If the service or application uses a range of ports for the inbound connection, enter the ending port number of the range.

9. Click the **Apply** button.

   The service or application is added to the Port Triggering Portmap Table. The **Enable** check box is selected automatically.

10. In the Port Triggering section, select how the cable data gateway applies port triggering:
    - **Per Schedule**. Port triggering is enabled according the schedule that you must select from the menu.

      For more information, see *Schedule When Features Are Active* on page 68.
    - **Always**. Port triggering is always enabled.

    Note: By default, the **Never** radio button is selected and port triggering is disabled, even if you specified services and applications in the table.

11. Click the **Apply** button.

    Your settings are saved.

Change a Service or Application for Port Triggering

You can change the settings for a service or application that you use for port triggering.

➢ **To change the port triggering settings for a service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Select the **Port Triggering** radio button.

   The screen adjusts.
7. In the table, select the radio button next to the service that you want to change.
8. Click the **Edit Service** button.

   The Ports Triggering - Services screen displays.
9. Change the settings for the service.

   For information about the settings, see *Add a Service or Application for Port Triggering* on page 128.
10. Click the **Apply** button.

    Your settings are saved. The changed settings for the service or application are shown in the Port Triggering Portmap Table.

Disable a Service or Application for Port Triggering

You can disable a port triggering service or application without removing it from the Port Triggering Portmap Table.

➢ **To disable a port triggering service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Port Forwarding / Port Triggering screen displays.

6. Select the **Port Triggering** radio button.

   The screen adjusts.

7. In the table, clear the **Enable** check box for the service or application that you want to disable.
8. Click the **Apply** button.

   The service or application remains in the Port Triggering Portmap Table but is disabled.

Remove a Service for Port Triggering

You can remove a service or application that you no longer need for port triggering.

➢ **To remove a port triggering service or application:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

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

   The Port Forwarding / Port Triggering screen displays.

6. Select the **Port Triggering** radio button.

   The screen adjusts.

7. In the table, select the radio button to the left of the service that you want to remove.
8. Click the **Delete Service** button.

   The service or application is removed from the Port Triggering Portmap Table.

Manage the Port Triggering Time-Out Period

By default, port triggering is enabled with a time-out period of 10 minutes.

The time-out value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This closure is required because the cable data gateway cannot detect when the application terminates.

If you disable port triggering after you configured port triggering services, the services are retained even though they are not used.

➢ **To change the port triggering time-out period:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering screen displays.
6. Select the **Port Triggering** radio button.

   The screen adjusts.

7. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.

   By default, the port triggering time-out is 10 minutes.

8. Click the **Apply** button.

   Your settings are saved.

Set Up and Manage IP Address Filtering

By default, the cable data gateway allows any connected device access to the Internet. As an added security measure, you can use IP filtering to block specific devices based on their IP addresses from accessing the Internet.

Block or Schedule Blocking for Devices Based on IP Address

You must add each device for which you want to block Internet access based on IP address.

➢ **To block or schedule blocking for devices based on IP address:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

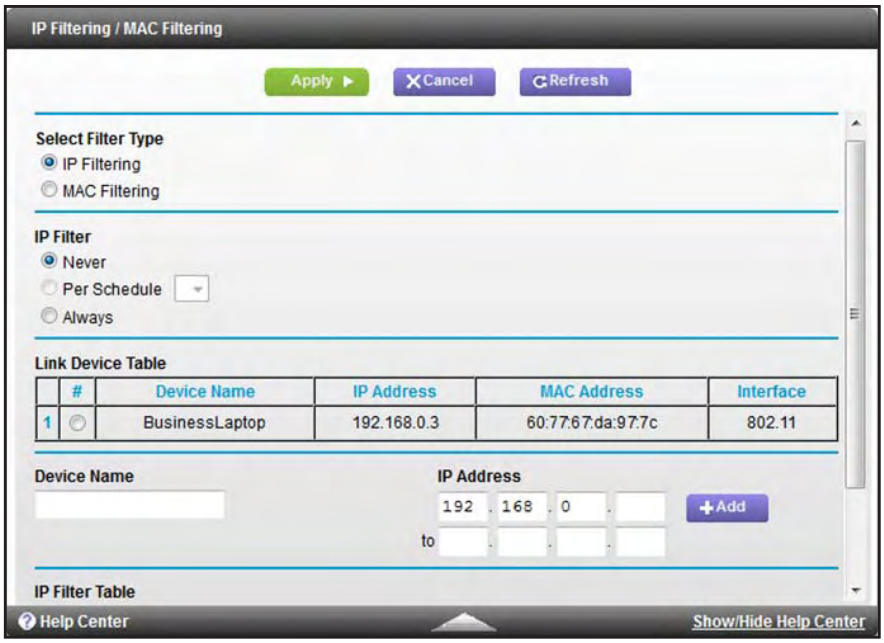
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

   The IP Filtering / MAC Filtering screen displays.



6. Leave the **IP Filtering** radio button selected as the filter type.
7. Add a device to the IP Filter Table:
   a. **Device Name**. Enter a descriptive name.
   b. **IP Address**. Complete the IP address. If the device covers a range of IP addresses, complete the ending IP address for the range in the lower field.

   Tip: You can also select a device from the Link Device Table by selecting the corresponding radio button. If the device that you want to add is not listed, click the **Refresh** button to update the Link Device Table.

8. Click the **Add** button.

   The device is added to the IP Filter Table. The **Enable** check box is selected automatically.
9. To add more devices to the table, repeat *Step 7* and *Step 8*.
10. In the IP Filter section, select how the cable data gateway applies IP address filtering:
    - **Per Schedule**. IP address filtering is enabled according the schedule that you must select from the menu.

      For more information, see *Schedule When Features Are Active* on page 68.
    - **Always**. IP address filtering is always enabled.

    Note: By default, the **Never** radio button is selected and IP address filtering is disabled, even if you specified devices in the table.

11. Click the **Apply** button.

    Your settings are saved.

Unblock a Device for IP Address Filtering

You can unblock a device for IP address filtering so the device can access the Internet access.

➢ **To unblock a device for IP address filtering:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

   The IP Filtering / MAC Filtering screen displays.
6. Leave the **IP Filtering** radio button selected as the filter type.
7. In the IP Filter Table, clear the **Enable** check box for the device that you want to unblock.
8. Click the **Apply** button.

   The device remains in the IP Filter Table but is unblocked and can access the Internet.

Remove a Device for IP Address Filtering

You can remove a device that you no longer need for IP address filtering.

➢ **To remove a device for IP address filtering:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

   The IP Filtering / MAC Filtering screen displays.
6. Leave the **IP Filtering** radio button selected as the filter type.
7. In the IP Filter Table, select the radio button to the left of the device that you want to remove.

8. Click the **Delete** button.

   The device is removed from the IP Filter Table.

Set Up and Manage MAC Address Filtering

By default, the cable data gateway allows any connected device access to the Internet. As an added security measure, you can use MAC filtering to block specific devices based on their MAC addresses from accessing the Internet. MAC address filtering is a more stable blocking method than IP address filtering because IP addresses can change but MAC addresses do not.

Block or Schedule Blocking for Devices Based on MAC Address

You must add each device for which you want to block Internet access based on MAC address.

➢ **To block or schedule blocking for devices based on MAC address:**

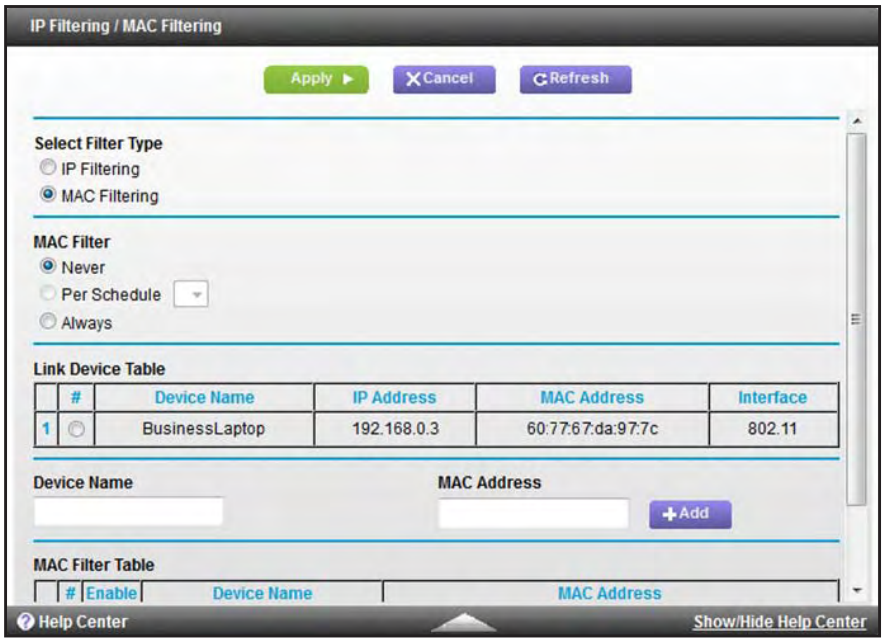
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

   The IP Filtering / MAC Filtering screen displays.



6. Select the **MAC Filtering** radio button.

   The screen adjusts.

7. Add a device to the MAC Filter Table:
   a. **Device Name**. Enter a descriptive name.
   b. **MAC Address**. Enter the MAC address.

   Tip: You can also select a device from the Link Device Table by selecting the corresponding radio button. If the device that you want to add is not listed, click the **Refresh** button to update the Link Device Table.

8. Click the **Add** button.

   The device is added to the MAC Filter Table. The **Enable** check box is selected automatically.

9. To add more devices to the table, repeat *Step 7* and *Step 8*.
10. In the MAC Filter section, select how the cable data gateway applies MAC address filtering:
    - **Per Schedule**. MAC address filtering is enabled according the schedule that you must select from the menu.

      For more information, see *Schedule When Features Are Active* on page 68.
    - **Always**. MAC address filtering is always enabled.

    Note: By default, the **Never** radio button is selected and MAC address filtering is disabled, even if you specified devices in the table.

11. Click the **Apply** button.

Your settings are saved.

Unblock a Device for MAC Address Filtering

You can unblock a device for MAC address filtering so that the device can access the Internet.

➢ **To unblock a device for MAC address filtering:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

   The IP Filtering / MAC Filtering screen displays.
6. Select the **MAC Filtering** radio button.

   The screen adjusts.
7. In the MAC Filter Table, clear the **Enable** check box for the device that you want to unblock.
8. Click the **Apply** button.

   The device remains in the MAC Filter Table but is unblocked and can access the Internet.

Remove a Device for MAC Address Filtering

You can remove a device that you no longer need for MAC address filtering.

➢ **To remove a device for MAC address filtering:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > IP Filtering/MAC Filtering**.

The IP Filtering / MAC Filtering screen displays.

6. Select the **MAC Filtering** radio button.

   The screen adjusts.

7. In the MAC Filter Table, select the radio button to the left of the device that you want to remove.
8. Click the **Delete** button.

   The device is removed from the MAC Filter Table.

Configure Dynamic DNS

If your cable service provider gave you a permanently assigned (fixed) IP address, you can register a domain name and link that name with your IP address by a public Domain Name Server (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know your IP address in advance and the address can change frequently. In this case, you can use a commercial Dynamic DNS (DDNS) 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 cable service provider assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the DDNS service does not work because private addresses are not routed on the Internet.

Your cable data gateway contains a client that can connect to the DDNS service provided by *Dyn*. First, visit their website and obtain an account and host name that you configure in the cable data gateway. Then, whenever your cable service provider–assigned IP address changes, your cable data gateway automatically contacts the DDNS 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 cable data gateway at http://hostname.dyn.com.

➢ **To set up Dynamic DNS:**

1. Register for an account with a DDNS service providers whose URL is listed in the **Service Provider** menu.
2. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
3. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

4. Type **admin** for the user name and type your password.

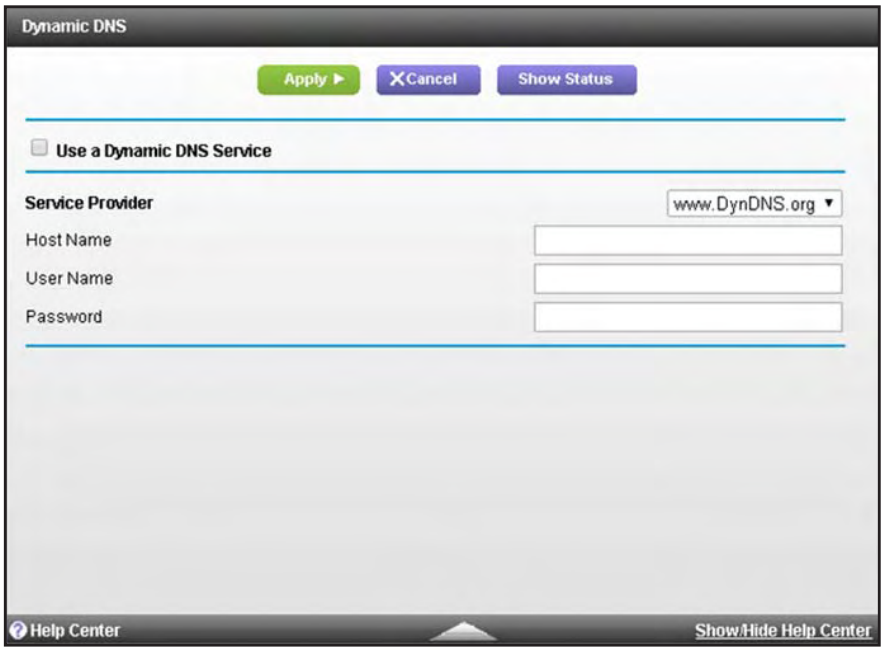
   If you did not yet personalize your password, type **password** for the password.

5. Click the **OK** button.

   The BASIC Home screen displays.

6. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

The Dynamic DNS screen displays.



7. Select the **Use a Dynamic DNS Service** check box.

   The selection from the **Service Provider** menu is fixed at **www.DynDNS.org**.

8. In the **Host Name** field, type the host or domain name that your Dynamic DNS service provider gave you.
9. In the **User Name** field, 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.

10. In the **Password** field, type the password or key for your Dynamic DNS account.
11. Click the **Apply** button.

    Your settings are saved.

12. To see the connection status with the DDNS server, click the **Show Status** button.

    A pop-up window displays.

Manage the Cable Data Gateway Remotely

The remote management feature lets you update or check the status of your cable data gateway over the Internet. For enhanced security, restrict access to as few external IP addresses as practical.

Note: Be sure to change the cable data gateway default login password to a secure password. For more information, see *Change the Password* on page 25.

➢ **To set up remote management:**

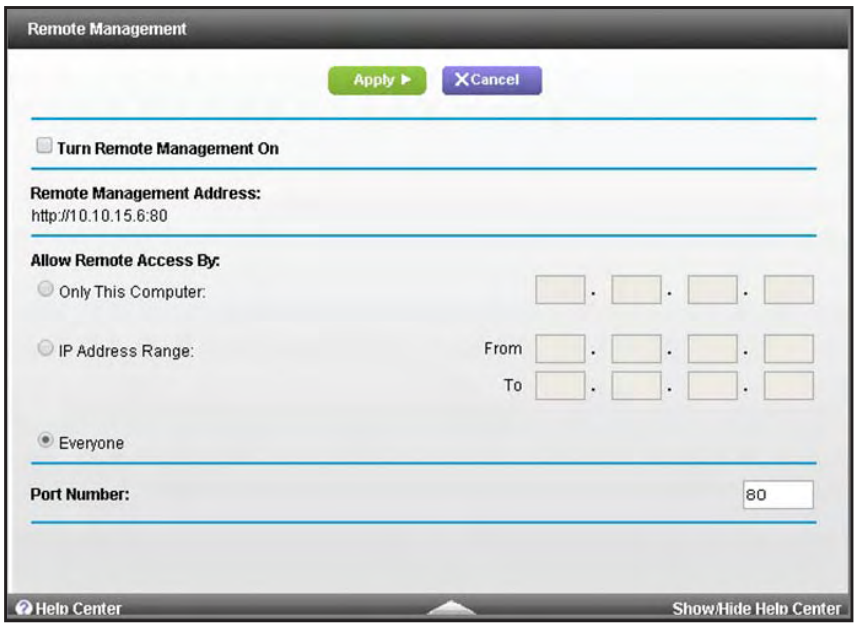
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > Remote Management**.

   The Remote Management screen displays.



6. Select the **Turn Remote Management On** check box.
7. Specify the external IP address or addresses from which the cable data gateway can be managed remotely:
   - To specify access for a single IP address on the Internet:
     a. Select the **Only This Computer** radio button.
     b. Enter the IP address from which access is allowed.

- To specify access for a range of IP addresses on the Internet:
  a. Select **IP Address Range** radio button.
  b. In the **From** field, enter the start IP address of the range from which access is allowed.
  c. In the **To** field, enter the end IP address of the range from which access is allowed.
- To specify access for all IP addresses on the Internet, keep the **Everyone** radio button selected.

  This is the default setting.

8. In the **Port Number** field, specify the port number for accessing the web management interface.

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

9. Click the **Apply** button.

   Your changes are saved. After a while, the external IP address and port number display in the **Remote Management Address** field.

When you access your cable data gateway from the Internet, type your cable data gateway's external (WAN) IP address in your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 203.0.113.123 and you use port number 8080, enter **http://203.0.113.123:8080** in your browser.

Manage Universal Plug and Play

Universal Plug and Play (UPnP) enables devices, such as Internet devices 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.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, best practise is to keep UPnP enabled, which is the default setting.

➢ **To manage Universal Plug and Play:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

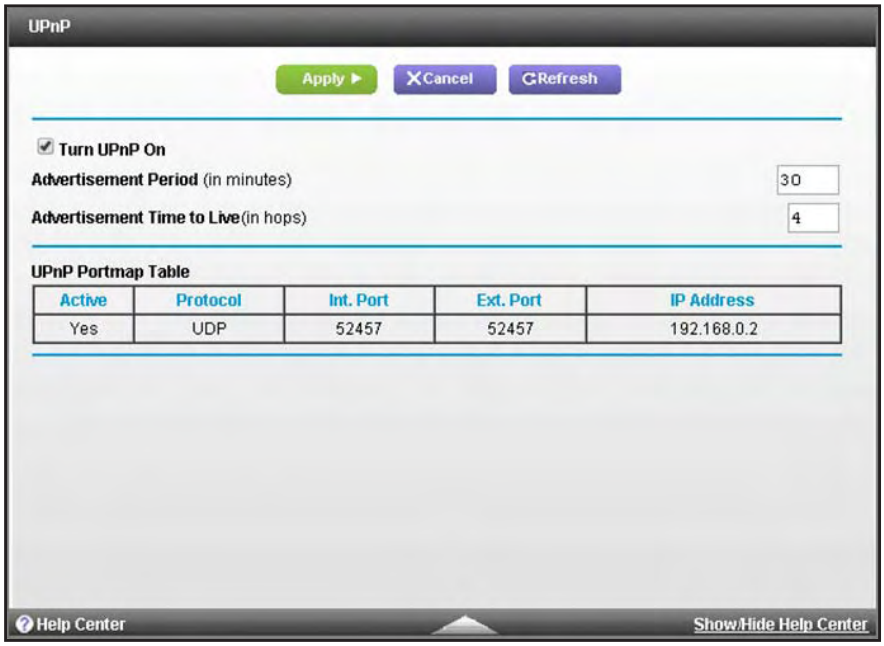
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > UPnP**.

   The UPnP screen displays.



   The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the cable data gateway and which internal and external ports that device opened. The UPnP Portmap Table also displays what type of port (that is, the protocol that is associated with port) is open and whether that port is still active for each IP address.

6. To turn off UPnP, clear the **Turn UPnP On** check box.

   By default, this check box is selected. If you clear the **Turn UPnP On** check box, the cable data gateway does not allow any device to automatically control the resources, such as port forwarding (mapping), of the cable data gateway.

7. To change the advertisement period, in the **Advertisement Period** field, enter a new period in minutes.

   The advertisement period specifies how often the cable data gateway 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 can obtain 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.

8. To change the advertisement time to live value, in the **Advertisement Time to Live** field, enter a new value in hops.

   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which is fine

for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

9. Click the **Apply** button.

   Your settings are saved.

10. To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

    The information onscreen is updated.

Manage the Network Address Translation

Network Address Translation (NAT) determines how the cable data gateway processes inbound traffic. NAT provides one-to-many translation of IP addresses between devices. This means that your network presents only one IP address to the Internet, and outside users cannot directly address any of your local devices on your LAN. Leave NAT enabled to allow multiple devices on your network to access the Internet using a single public IP address. NAT is enabled by default.

Situations might occur in which you want to disable NAT.

➢ **To manage NAT:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

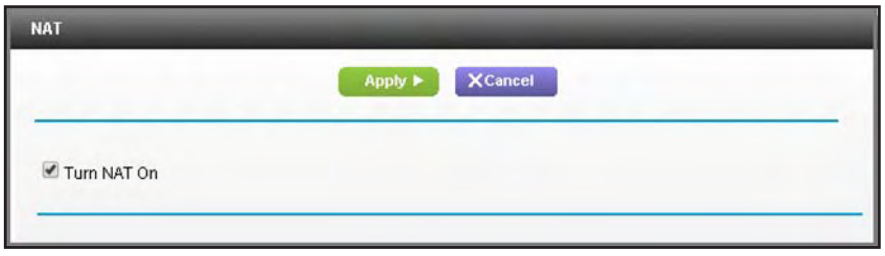
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > NAT Mode**.

   The NAT screen displays.



   By default, the **Turn NAT On** check box is selected.

6. To disable NAT, clear the **Turn NAT On** check box.

7. Click the **Apply** button.

   Your settings are saved.

Manage the Ethernet Ports of the LAN Switch

For devices that connect to the cable data gateway over an Ethernet cable, the cable data gateway provides access to the LAN through a built-in 10/100/1000BASE-T Ethernet switch. The switch ports automatically negotiate speed and duplex communication with any connected device.

Change the Default Settings of the Ethernet Ports

If a connected LAN device does not autonegotiate correctly, you can change the default setting for the Ethernet port. For information about port numbering, see the Back Panel sections in *Chapter 1, Hardware Overview*.

➢ **To change the default settings of an Ethernet port:**

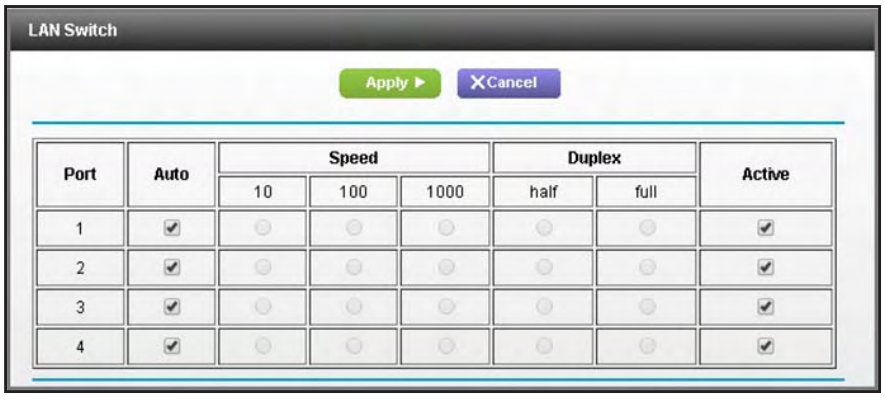
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > LAN Switch**.

   The LAN Switch screen displays.



By default, the **Auto** check box is selected for all Ethernet ports.

6. Clear the **Auto** check for the port for which you want to change the settings.
7. Specify the speed in Mbps by selecting a radio button (**10**, **100**, or **1000**).
8. Specify the duplex mode by selecting a radio button (**half** or **full**).
9. Click the **Apply** button.

   Your changes are saved.

Disable Access to an Ethernet Port

A situation might occur in which you want to disable access to an Ethernet port. For example, you can disconnect a computer from the network without unplugging the cable. For information about port numbering, see the Back Panel sections in *Chapter 1, Hardware Overview*.

➢ **To disable access to an Ethernet port:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Advanced Setup > LAN Switch**.

   The LAN Switch screen displays.
6. Clear the **Active** check for the port for which you want to disable access.
7. Click the **Apply** button.

   Your changes are saved.

Manage Network Time Protocol

Network Time Protocol (NTP) is a networking protocol that synchronizes clocks between computer systems over data networks. The cable data gateway includes a real-time clock (RTC), which it uses for scheduling. The cable data gateway regularly updates its RTC by contacting one of the three NTP servers.

➢ **To manage NTP and NTP servers:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

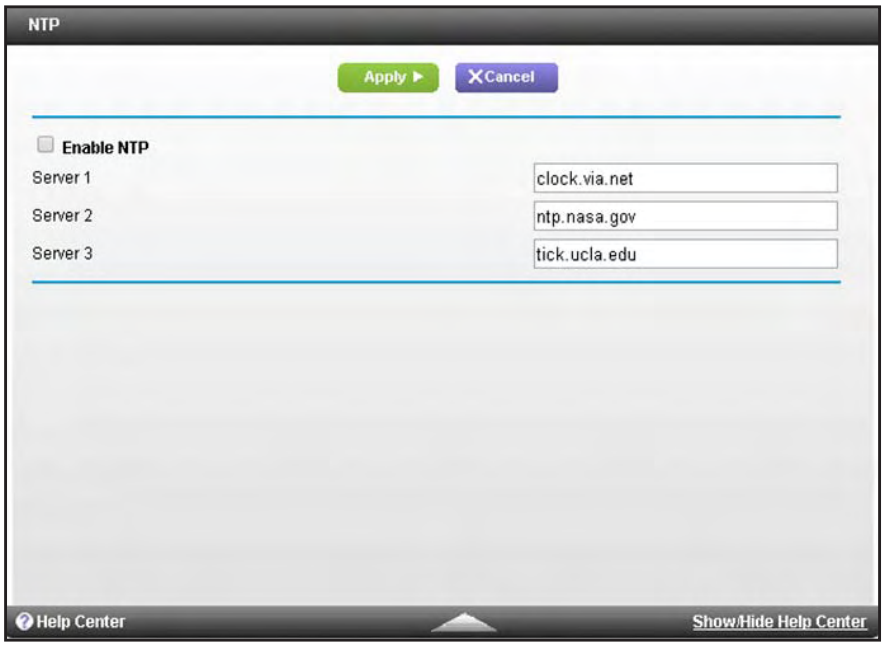
   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Advanced Setup > NTP**.

   The NTP screen displays.



   By default, the **Enable NTP** check box is cleared and NTP is disabled.

6. Select the **Enable NTP** check box.

   You can either keep the default NTP servers or configure one or more custom NTP servers.

7. To configure custom NTP servers:

   - In the **Server 1** field, enter the IP address or Dynamic DNS name for the first NTP server.

     The first default NTP server is clock.via.net.

   - In the **Server 2** field, enter the IP address or Dynamic DNS name for the second NTP server.

     The second default NTP server is ntp.nasa.org.

   - In the **Server 3** field, enter the IP address or Dynamic DNS name for the third NTP server.

     The third default NTP server is tick.ucla.edu.

8. Click the **Apply** button.

   Your settings are saved.

Diagnostics and Troubleshooting

9

This chapter provides information to help you diagnose and solve problems that might occur with the cable data gateway. If you do not find the solution here, contact Cox Support.

This chapter contains the following sections:

Perform Diagnostics

The cable data gateway lets you perform various diagnostic tasks. For normal operation, these tasks are not required.

Ping an IP Address

Use this test to send a ping packet request to an IP address to test the connection. If the request times out because no reply is received, the destination might be unreachable. However, some network devices can be configured not to respond to a ping.

➢ **To ping an IP address:**

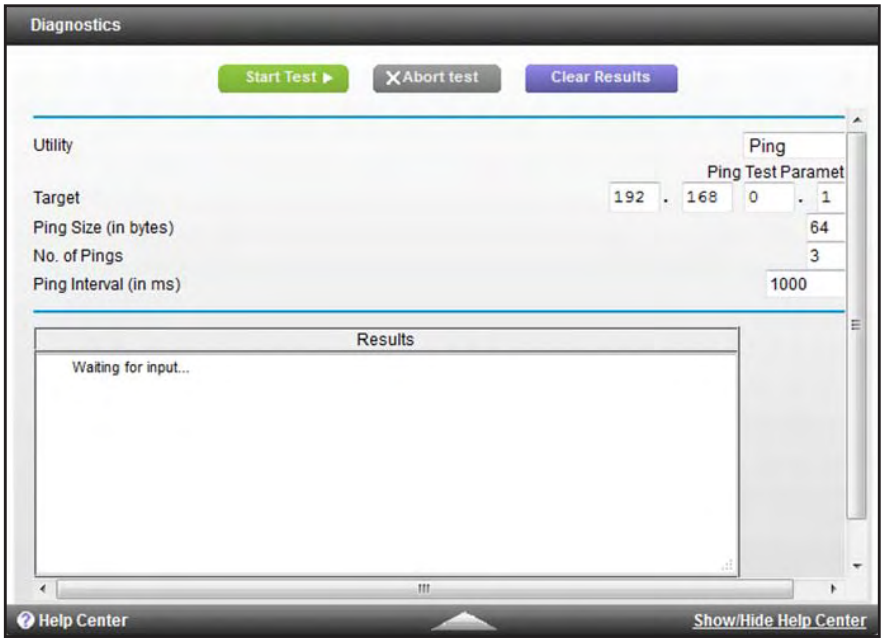
1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > Administration > Diagnostics**.

   The Diagnostics screen displays.



By default, **Ping** is selected from the **Utility** menu.

6. Enter the ping settings.

   The following table describes the fields for the ping settings on the Diagnostics screen.

Field	Description
Target	Enter the IP address of the device that you want to ping.
Ping Size (in bytes)	Enter the size of the ping packet. By default, the packet size is 64 bytes.
No. of Pings	Enter the number of times that the IP address is pinged. By default, the ping is sent three times.
Ping Interval (in ms)	Enter the interval between the consecutive pings. By default, the interval is 1000 ms.

7. Click the **Start Test** button.

   The Results field displays the results of the ping test.

8. If the test does not complete, click the **Abort Test** button and try again.
9. To refresh the results in the Results field, click the **Refresh** button at the bottom of the field.
10. To remove all information from the Results field, click the **Clear Results** button.

Trace a Route

Use this test to trace a route to an IP address or host name to test the connection. If you use a host name, you can also use this test to resolve the name to an IP address. If the request times out because no reply is received, the destination might be unreachable. However, some network devices can be configured not to respond to a traceroute request.

➢ **To trace a route:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.

3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

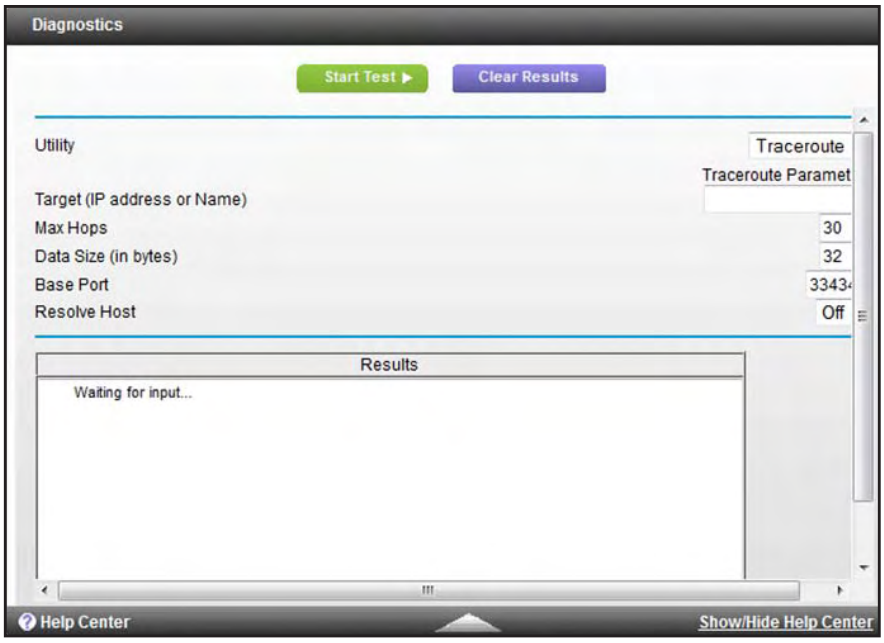
   The BASIC Home screen displays.

5. Select **ADVANCED > Administration > Diagnostics**.

   The Diagnostics screen displays.

6. From the **Utility** menu, select **Traceroute**.

   The screen adjusts.



7. Enter the traceroute settings.

   The following table describes the fields for the traceroute settings on the Diagnostics screen.

Field	Description
Target (IP address or Name)	Enter the IP address or host name of the device that you want to trace.
Max Hops	Enter the maximum number of hops for the trace. By default, the maximum number of hops is 30.
Data Size (in bytes)	Enter the size of the probe packet. By default, the probe packet size is 32 bytes.
Base Port	Enter the port from which the probe packet is sent. By default, the port number is 33434.
Resolve Host	If you enter a host name, specify whether the name is resolved to an IP address by selecting one of the following options from the **Resolve Host** menu: • **Off**. The name is not resolved to an IP address. • **On**. The name is resolved to an IP address.

8. Click the **Start Test** button.

   The Results field displays the results of the ping test.

   Note: After 30 hops, a traceroute times out.

9. To refresh the results in the Results field, click the **Refresh** button at the bottom of the field.
10. To remove all information from the Results field, click the **Clear Results** button.

Quick Tips for Troubleshooting

The following table includes tips for troubleshooting some common problems.

Table 4. Quick tips for troubleshooting

Problem	Possible Solution
Your WiFi network is unresponsive or does not function normally.	Restart your WiFi network: 1. Turn off and unplug the cable data gateway. 2. Plug in the cable data gateway and turn it on. Wait two minutes.
You cannot connect over WiFi to the cable data gateway.	• Make sure that the WiFi settings in your WiFi device and cable data gateway match exactly. For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the cable data gateway and WiFi computer must match exactly. The default SSID and password are on the cable data gateway product label (see *Chapter 1, Hardware Overview*). • Make sure that your WiFi device supports the security that you are using for your WiFi network (WPA2-PSK [AES] or WPA-PSK [TKIP] + WPA2-PASK [AES]). For information about WiFi security settings, see *View or Change the Basic Settings for the Main WiFi Network* on page 31. • Make sure that the cable data gateway is not too far from your WiFi device or too close. - Move your WiFi device near the cable data gateway but at least 6 feet (about 2 meters) away and see if the signal strength improves. - Make sure that the WiFi signal is not blocked by objects between the cable data gateway and your WiFi device. • Make sure that the 2.4 GHz LED or 5 GHz LED (or, for model N450, the WiFi LED) on the cable data gateway is not off. If this LED is off, the WiFi radio might be disabled. For more information about the WiFi radio, see *Control the WiFi Radios* on page 109. • Make sure that the cable data gateway's SSID broadcast is not disabled. If the cable data gateway's SSID broadcast is disabled, the WiFi network name is hidden and does not display in your WiFi device's scanning list. To connect to a hidden network, you must type the network name and the WiFi password. For more information about the SSID broadcast, see *View or Change the Basic Settings for the Main WiFi Network* on page 31. • If you set up an access list on the advanced Wireless Settings screen (see *Set Up a WiFi Access List by MAC Address* on page 112), add the MAC address of each WiFi device to the cable data gateway's access list. • Make sure that your WiFi device is not configured with a static IP address but is configured to receive an IP address automatically with DHCP.
All LEDs are off when the cable data gateway is plugged in.	Make sure that the power cord is properly connected to your cable data gateway and that the power supply adapter is properly connected to a functioning power outlet. Check that you are using the power adapter that came in the product package and not any other power adapter. If the error persists, a hardware problem occurred. Contact Cox Support.

Table 4. Quick tips for troubleshooting

Problem	Possible Solution
All LEDs stay on.	• Clear the configuration of the cable data gateway to its factory defaults. This operation sets the IP address of the cable data gateway to 192.168.0.1. • If the error persists, it is possible that a hardware problem occurred. Contact Cox Support.
Ethernet LED is off for a port with an Ethernet connection.	• Make sure that the connected Ethernet device does not use a static IP address but is configured to receive an IP address automatically with DHCP. • Make sure that the Ethernet cable connections are secure at the cable data gateway and at the Ethernet device. • Make sure that power is turned on to the connected Ethernet device. • Be sure that you are using the correct cable.
Internet LED (or, for model AC1900, the Online LED) is off even though the cable data gateway is connected to the cable wall jack.	• Make sure that the coaxial cable connections are secure at the cable data gateway and at the wall jack. • Make sure that your cable service provider provisioned your cable Internet service. Your provider can verify that the signal quality is good enough for cable data gateway service. • Remove any excessive splitters that you installed on your cable line. Run a “home run” back to the point where the cable enters your home.

Troubleshoot with the LEDs

When you turn on the power, the LEDs light as described here.

1. When power is first applied, all LEDs light solid.

   Whether an Ethernet LED lights depends on whether an Ethernet device is connected to the cable data gateway.

2. After approximately 12 seconds, all LEDs start blinking green except for the Power LED, which blinks red.
3. After approximately one minute, the following LED behavior occurs:
   - The Power LED turns solid green, indicating that the boot process is complete.
   - The Downstream LED starts blinking green.
   - The 2.4 GHz and 5 GHz LEDs (or, for model N450, the WiFi LED) start blinking green or light solid green.
4. After the cable data gateway establishes a downstream connection, the following LED behavior occurs:
   - The Downstream LED lights solid blue or green.
   - The Upstream LED starts blinking green.
5. After the cable data gateway establishes an upstream connection, the Upstream LED lights solid blue or green.

Power LED Is Off

If the Power LED and other LEDs are off when your cable data gateway is turned on, do the following:

- Check that the power cord is correctly connected to your cable data gateway and that the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the power adapter that NETGEAR supplied for this product.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact Cox Support.

Power LED Is Red (Solid or Blinking) at Any Time Other Than While Booting

When the cable data gateway is turned on, it performs a power-on self-test, during which time the Power LED blinks red. If the Power LED does not turn green within a minute or so, or if it turns red (solid or blinking) at any other time during normal operation, a fault exists within the cable data gateway.

If the Power LED turns red to indicate a cable data gateway fault, turn the power off and on to see if the cable data gateway recovers. If the Power LED is still red one minute after power-up, do the following:

- Turn the power off and on one more time to see if the cable data gateway recovers.
- Clear the cable data gateway's configuration to factory defaults (see *Return the WiFi Cable Data Gateway to Its Factory Default Settings* on page 94). This sets the cable data gateway's IP address to 192.168.0.1.

If the error persists, an unrecoverable firmware or hardware problem occurred. For recovery instructions or help with a hardware problem, contact Cox Support.

2.4 GHz or 5 GHz LED or WiFi LED Is Off

If the 2.4 GHz or 5 GHz LED (or, for model N450, the WiFi LED) stays off, the WiFi radio in the cable data gateway is off. For information about turning on the WiFi radio, see *Control the WiFi Radios* on page 109. When the WiFi radio is turned on, the LED starts blinking green or lights solid green.

LAN LED Is Off

If the LAN LED for a port does not light when you connect a device, check the following:

- The Ethernet cable connections are secure at the cable data gateway and at the device.
- The power is turned on to the connected device.
- You are using the correct cable.

Cannot Log In to the Cable Data Gateway

If you are unable to log in to the cable data gateway from a device on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the cable data gateway (see *LAN LED Is Off* on page 156).
- Make sure that Java, JavaScript, or ActiveX is enabled in your web browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- Make sure that your computer's IP address is on the same subnet as the cable data gateway. If you are using the recommended addressing scheme, your computer's address is in the range of 192.168.0.2 to 192.168.0.254. For more information, see *Manage the Internet Setup* on page 42.
- If your computer's IP address is shown as 169.254.x.x: Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the cable data gateway and reboot your computer.
- If your cable data gateway's IP address was changed and you do not know the current IP address, use an IP scanner application to detect the IP address. If you still cannot find the IP address, clear the cable data gateway's configuration to factory defaults. This sets the cable data gateway's IP address to 192.168.0.1. For more information, see *Factory Default Settings* on page 164.

View and Manage the Event Log

The event log is a detailed record of events that occur between the cable data gateway and the cable service provider's cable modem termination system (CMTS). Such events include firmware downloads, DOCSIS time-outs, WiFi channel changes, and login authentications to the CMTS.

The event log might help your cable service provider to troubleshoot problems and isolate faults that might occur. Cox Support might ask about events that are listed in the event log.

➢ **To view or clear the event log:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

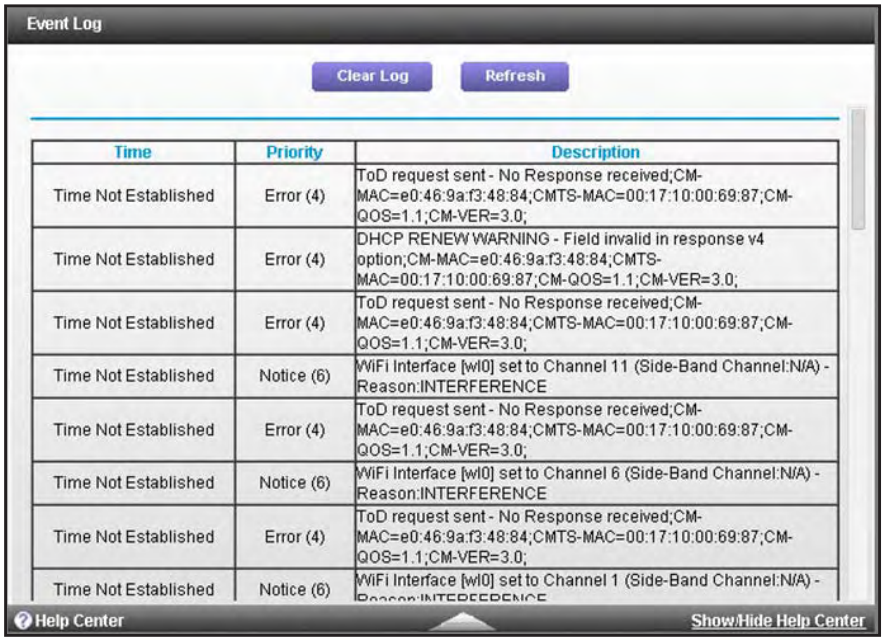
If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

   The BASIC Home screen displays.

5. Select **ADVANCED > Administration > Event Log**.

   The Event Log screen displays.



   The Event Log screen displays a table that shows, for each event, the time that the event occurred, the priority of the event (0 being the highest priority and 6 the lowest), and a detailed description.

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

   The information onscreen is updated.

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

   All entries are removed from the table.

Troubleshoot the Cable Internet Connection

If your cable data gateway cannot access the Internet but the Internet LED (or, for model AC1900, the Online LED) lights green, contact Cox Support.

For more information about Internet connection problems, see *TCP/IP Network Not Responding* on page 161.

Internet LED or Online LED Is Off

If the Internet LED (or, for model AC1900, the Online LED) is off, the cable data gateway was unable to connect to the Internet. Verify the following:

- Check that the Internet information is correct (see *Manage the Internet Setup* on page 42).
- Check to see if your cable service provider is experiencing a service problem. It might not be that the cable data gateway cannot connect to the Internet, but rather that your cable service provider cannot provide an Internet connection.

Obtain an Internet IP Address

If your cable data gateway cannot access the Internet and your Internet LED lights green, see if the cable data gateway can obtain an Internet IP address from the cable service provider. Unless you were assigned a static IP address, your cable data gateway requests an IP address from the cable service provider. You can determine whether the request was successful using the web management interface.

➢ **To check the Internet IP address:**

1. On your computer, launch an Internet browser such as Mozilla Firefox or Microsoft Internet Explorer.
2. In the address field of your browser, enter **http://routerlogin.net**.

   You are prompted to enter a user name and password.
3. Type **admin** for the user name and type your password.

   If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

   The BASIC Home screen displays.
5. Select **ADVANCED > ADVANCED Home**.

   The ADVANCED Home screen displays.
6. In the Internet Port pane, check that an IP address is shown in the IP address/Mask field.

   If 0.0.0.0 is shown, the cable data gateway did not obtain an IP address from the cable service provider.

If the cable data gateway cannot obtain an IP address from the cable service provider, the cable service provider might check for a host name, a domain name, or both.

Assign the host name, domain name, or both. For more information, see *Manage the Internet Setup* on page 42.

Troubleshoot Internet Browsing

If your cable data gateway can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for one of the following reasons:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your cable service provider provides the addresses of one, two, or three DNS servers for your use. If you entered a DNS address when you set up the cable data gateway, reboot your computer and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- The cable data gateway might not be configured as the computer's TCP/IP cable data gateway.

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

  For information about TCP/IP problems, see *TCP/IP Network Not Responding* on page 161.

Changes Not Saved

If the cable data gateway does not save the changes you make in the cable data gateway web management interface, do 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 occurred, but the old settings might be in the web browser's cache.

WiFi Connectivity

If you experience trouble connecting over WiFi to the cable data gateway, try to isolate the problem.

- Does the WiFi device that you are using find your WiFi network?

  If not, check the 2.4 GHz LED or 5 GHz LED (or, for model N450, the WiFi LED) on the front panel of the cable data gateway. If a LED is off, the corresponding WiFi radio in the cable data gateway is off. For information about turning on the WiFi radio, see *Control the WiFi Radios* on page 109. When the WiFi radio is turned on, the LED starts blinking green or lights solid green.

- If you disabled the cable data gateway's SSID broadcast, your WiFi network is hidden and does not display in your WiFi client's scanning list. (By default, SSID broadcast is

enabled.) For more information, see *View or Change the Basic Settings for the Main WiFi Network* on page 31.

- Does your WiFi device support the security that you are using for your WiFi network (WPA2-PSK [AES] or WPA-PSK [TKIP] + WPA2-PASK [AES])? For information about changing the WiFi security, see *View or Change the Basic Settings for the Main WiFi Network* on page 31.

Note: If you want to change the WiFi settings for the cable data gateway, use an Ethernet cable to connect a computer to a LAN port on the cable data gateway and then log in to the cable data gateway.

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

- Is your cable data gateway too far from your WiFi device or too close? Place your WiFi device near the cable data gateway but at least 6 feet (about 2 meters) away and see whether the signal strength improves.
- Are objects between the cable data gateway and your WiFi device blocking the WiFi signal?

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers provide a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your WiFi Cable Data Gateway

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

➢ **To ping the cable data gateway from a Windows computer:**

1. From the Windows taskbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the cable data gateway, as in this example:

   ping 192.168.0.1

3. Click the **OK** button.

   A message such as the following one displays:

   ```
   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, the network might not be configured correctly. Do the following:

- Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
- Verify that the IP address for your cable data gateway 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 you verify that the LAN path works correctly, test the path from your computer to a remote device:

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

   `ping -n 10` *`IP address`*

   where *IP address* is the IP address of a remote device such as your cable service provider's DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your WiFi Cable Data Gateway* on page 161 display. If you do not receive replies, do the following:

- Check that your computer uses the IP address of your cable data gateway as the default cable data gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the cable data gateway is listed as the default router.
- Check that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- If the cable data gateway cannot obtain an IP address from the cable service provider, the cable service provider might check for a host name, a domain name, or both. Assign the host name, domain name, or both. For more information, see *Manage the Internet Setup* on page 42.

Factory Default Settings and Specifications

A

This appendix includes the factory default settings and technical specifications for the cable data gateway.

This appendix contains the following sections:

Factory Default Settings

You can return the cable data gateway to its factory default settings (see *Return the WiFi Cable Data Gateway to Its Factory Default Settings* on page 94). The following table shows the factory default settings.

Table 5. Factory default settings

Feature		Default Settings
Router Login	User login URL	http://routerlogin.net or http://192.168.0.1
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Local area network (LAN)	LAN IP address	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.0.2 to 192.168.0.254
	DHCP start IP address	192.168.0.2
	DHCP end IP address	192.168.0.254
	UPnP	Enabled
Wide area network (WAN) and security	Port scan protection	Enabled
	DoS protection	Enabled
	Default DMZ server	Disabled
	Respond to ping on Internet port	Enabled
	MTU size	Uses the maximum MTU value for best throughput
	SIP ALG	Enabled
	NAT	Enabled
	Remote management over WAN	Disabled
	Inbound communication from the Internet	Disabled, except for traffic on port 80 (the HTTP port) in response to requests from the LAN
	Outbound communication to the Internet	Enabled
	Sites blocked	None
	Services blocked	None

Table 5. Factory default settings (continued)

Feature		Default Settings
Services, pass-through, and security	Firewall features	Enabled
	IPSec pass-through	Enabled
	PPTP pass-through	Enabled
	Multicast	Enabled
	Port scan detection	Enabled
	IP flood detection	Enabled
Web features	Filter proxy	Disabled (proxy allowed)
	Filter cookies	Disabled (cookies allowed)
	Filter Java Applets	Disabled (Java Applets allowed)
	Filter ActiveX	Disabled (ActiveX allowed)
	Filter pop-up windows	Disabled (pop-up windows allowed)
	Block fragmented IP packets	Disabled (fragmented IP packets allowed)
NAT ALG protocols and services	RSVP	Enabled
	FTP	Enabled
	TFTP	Enabled
	Kerb88	Enabled
	NetBios	Enabled
	IKE	Enabled
	RTSP	Enabled
	Kerb1293	Enabled
	H225	Enabled
	PPTP	Enabled
	MSN	Enabled
	SIP	Enabled
	ICQ	Enabled
	IRC666x	Enabled
	ICQTalk	Enabled
	Net2Phone	Enabled
	IRC7000	Enabled

Table 5. Factory default settings (continued)

Feature		Default Settings
Main WiFi network	WiFi radios[1]	Enabled
	WiFi network names (SSIDs)[1]	See the product label
	WiFi passphrase for both SSIDs[1]	See the product label
	Type of WiFi security	WPA-PSK [TKIP] + WPA2-PSK [AES]
	Wireless isolation	Disabled
	Broadcast SSID	Enabled
	Country/region	Varies by region
	RF channel	Auto
	Operating mode[2]	AC1900 WiFi Cable Data Gateway, Model C6300BD: • Default mode at 2.4 GHz: Up to 289 Mbps • Default mode at 5 GHz: Up to 1300 Mbps
		N900 WiFi Cable Data Gateway, Model CG4500BD: • Default mode at 2.4 GHz: Up to 289 Mbps • Default mode at 5 GHz: Up to 450 Mbps
		N450 WiFi Cable Data Gateway, Model CG3000Dv2: Default at 2.4 GHz: Up to 289 Mbps
	Radio transmission power	100 percent, nonconfigurable
	20/40 MHz coexistence	Enabled, nonconfigurable
	Fragmentation length	2346
	CTS/RTS threshold	2347
	Preamble mode	Long preamble
WPS	WPS capability	Enabled
	PIN	Enabled, see the web management interface (path **ADVANCED > Setup > Wireless Settings**)
	Keep Existing Wireless Settings	Enabled
Guest WiFi network	WiFi radios[1]	Disabled
	WiFi network names (SSIDs)[1]	See the product label
	Type of WiFi security	none (open network)
	Enable SSID broadcast	Disabled
	Allow guests to access local network	Disabled

1. The N450 WiFi Cable Data Gateway, Model CG3000Dv2, support a single radio and SSID only.

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

Technical and Environmental Specifications

Table 6. Cable data gateway specifications

Feature	Description
Data and routing protocols	TCP/IP, DHCP server and client, DNS relay, NAT (many-to-one), TFTP client, VPN pass-through (IPSec, PPTP), DNS, UPnP
Power adapter	AC1900 WiFi Cable Data Gateway, Model C6300BD: • North America (input): 120V, 60 Hz, input • North America (output): 12VDC @ 3.5A output 42W maximum
	N900 WiFi Cable Data Gateway, Model CG4500BD: • North America (input): 120V, 60 Hz, input • North America (output): 12VDC @ 2.5A output 30W maximum
	N450 WiFi Cable Data Gateway, Model CG3000Dv2: • North America (input): 120V, 60 Hz, input • North America (output): 12VDC @ 2.5A output 30W maximum
Dimensions and weight	AC1900 WiFi Cable Data Gateway, Model C6300BD: • 10.2 by 6.49 by 3.65 in. (259.17 by 164.77 by 92.72 mm) • 1.52 lb (0.69 kg)
	N900 WiFi Cable Data Gateway, Model CG4500BD: • 10.2 by 6.49 by 3.65 in. (259.17 by 164.77 by 92.72 mm) • 1.34 lb (0.61 kg)
	N450 WiFi Cable Data Gateway, Model CG3000Dv2: • 10.2 by 6.49 by 3.65 in. (259.17 by 164.77 by 92.72 mm) • 1.30 lb (0.59 kg)
WAN port	One coaxial cable connector DOCSIS 3.0. backward compatible with DOCSIS 2.0, 1.1, and 1.0
LAN ports	Four 10/100/1000BASE-T, RJ-45 autosensing ports
USB port or ports	AC1900 WiFi Cable Data Gateway, Model C6300BD: One USB 2.0 port
	N900 WiFi Cable Data Gateway, Model CG4500BD: One USB 2.0 port
	N450 WiFi Cable Data Gateway, Model CG3000Dv2: Two USB 2.0 ports

Table 6. Cable data gateway specifications (continued)

Feature	Description
WiFi	AC1900 WiFi Cable Data Gateway, Model C6300BD: • Up to 600 Mbps[1] at 2.4 GHz for 802.11n/g/b devices • Up to 1300 Mbps[1] at 5 GHz for 802.11ac/n/a devices
	N900 WiFi Cable Data Gateway, Model CG4500BD: • Up to 450 Mbps[1] at 2.4 GHz for 802.11n/g/b devices • Up to 450 Mbps[1] at 5 GHz for 802.11n/a devices
	N450 WiFi Cable Data Gateway, Model CG3000Dv2: Up to 450 Mbps[1] at 2.4 GHz for 802.11n/g/b devices
WiFi channels	• 2.4 GHz band: Auto or a single channel from 01–11 • 5 GHz band:[2] Auto or 36, 40, 44, 48, 149, 143, 157, or 161
Maximum computers per WiFi network	Limited by the amount of WiFi network traffic generated by each node
Operating frequency ranges	• 2.4 GHz band: 2.412–2.462 GHz • 5 GHz band: 5.180-5.835 GHz[2]
802.11 authorization and encryption	• WPA2-PSK [AES] • WPA-PSK [TKIP] + WPA2-PSK [AES]
Operating temperature	32° to 140°F (0° to 40°C)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC
Safety standards	UL 60950

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

2. Not applicable to the N450 WiFi Cable Data Gateway, Model CG3000Dv2.