NETGEAR®

VDSL Voice Gateway

Model VEVG2660-1TKSAS
User Manual

October 2014
202-11428-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Contact your Internet service provider for technical support.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

Contents

Chapter 5   Share a USB Drive Attached to the Gateway

Chapter 6   Specify Network Settings

Appendix A   Supplemental Information

Hardware Setup

1

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup.

This chapter covers the following topics:

- *Unpack Your Gateway*
- *Front Panel*
- *Rear Panel*
- *Position Your Gateway*
- *Cable Your Gateway*

Unpack Your Gateway

Your package contains the following items.

You can use the phone-only filter for any other phone plugged into the same line as the DSL modem.

Phone-only filter (green port)

Splitter/filter (red and green ports)

Surge protected power adapter

Ethernet cable

Gateway

Phone cable (white)

Phone cable (grey)
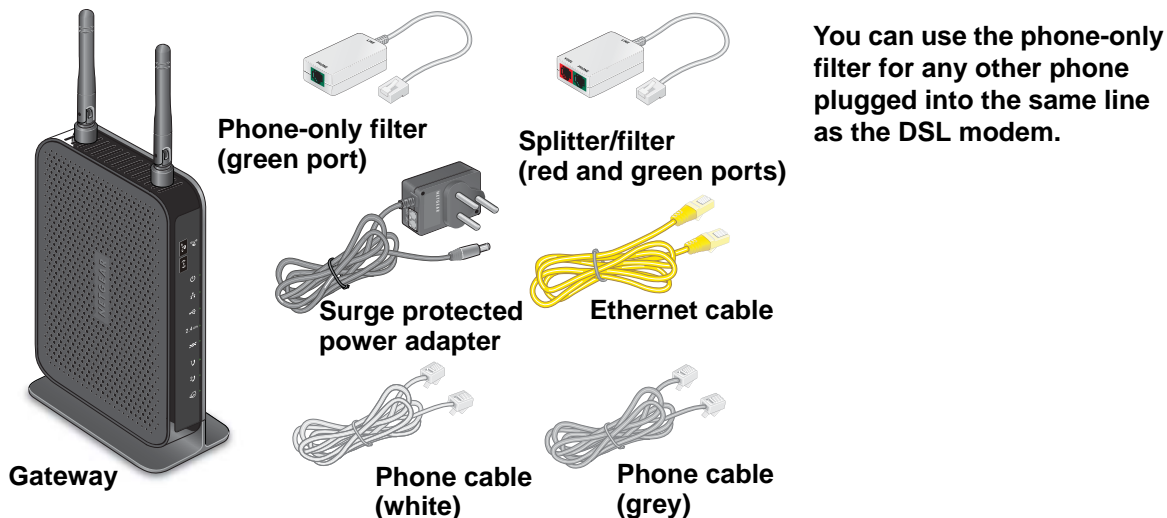
Figure 1. Package contents

Front Panel

The gateway has status LEDs and buttons on the front.

WPS button

WiFi On/Off button

WPS LED

Power LED

Ethernet LAN LED

USB LED

2.4 GHz WiFi LED

DSL LED

Voice LEDs (2)

Internet LED
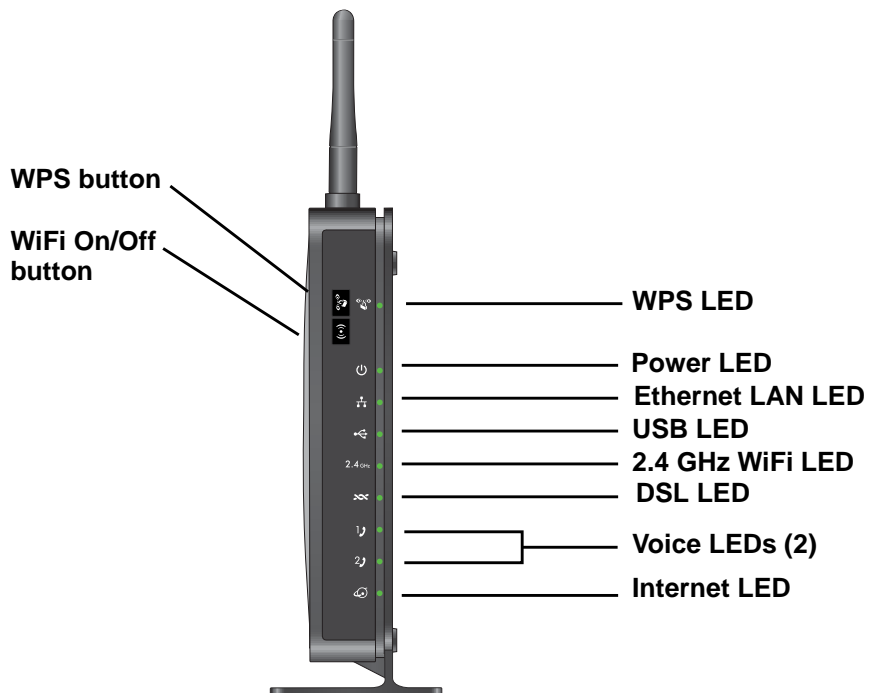
Figure 2. Gateway front view

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

LEDs and Buttons	Description
Power	• **Solid green**. The gateway has power. • **Blinking green**. The gateway is powering on. • **Solid red**. The gateway is performing a self-test or the thermal cutoff circuit has been triggered. • **Off**. The gateway is not receiving power or is powered off.
LAN ports	• **Solid green**. The gateway detects an Ethernet connection on one or more LAN ports. • **Blinking green**. The gateway is sending data over one or more LAN ports. • **Off**. The gateway does not detect Ethernet links on the LAN ports.
USB port	• **Solid green**. The gateway detects an active link on the USB port. • **Blinking green**. The gateway is sending or receiving data over the USB port. • **Off**. The gateway does not detect a USB device connected to the USB port.
2.4 GHz	• **Solid green**. The gateway detects a 2.4 GHz WiFi connection. • **Blinking green**. The gateway is sending data over the WiFi link. • **Off**. The wireless radio is turned off and you cannot connect to the gateway with WiFi.
DSL	• **Solid green**. The gateway detects an active link on this port. • **Blinking green**. The DSL WAN port is synchronizing with the DSL line. • **Off**. The gateway does not detect a link on this port.
Voice 1 and 2	• **Solid green**. The gateway detects links with telephones on this port. • **Blinking green**. At least one telephone is off the hook. • **Off**. The gateway does not detect a link on this port.
Internet	• **Solid green**. The gateway is connected to the Internet. • **Blinking green**. The gateway is sending or receiving data from the Internet. • **Off.** The gateway is not connected to the Internet.
WiFi button	Pressing and holding this button for two seconds turns the wireless radio on and off.
WPS button	Pressing this button opens a two-minute window when you can use WPS on computers or wireless devices to connect to the gateway's WiFi network without typing the WiFi password. The LED blinks during the two-minute window.

Rear Panel

The rear panel has the connections and button shown the following figure.

DSL port

Voice ports (2)

Ethernet WAN port

USB port

Ethernet LAN ports

Power On/Off button
Power adapter input
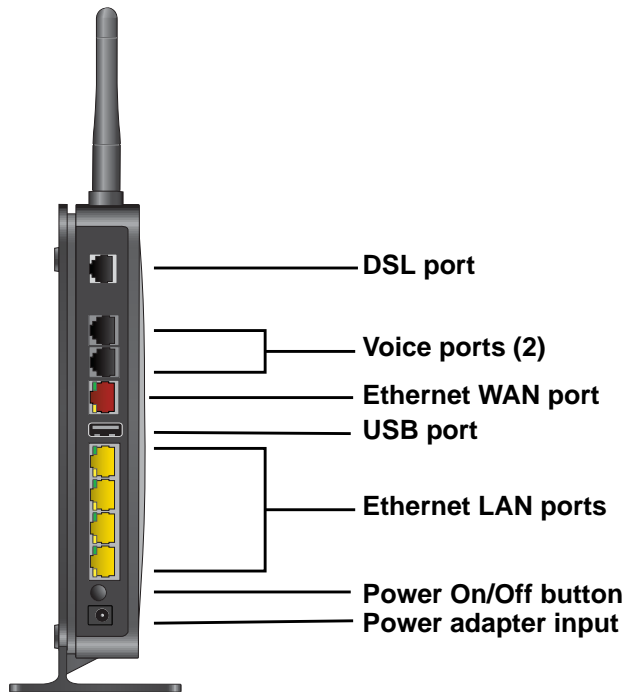
Figure 3. Gateway rear view

Position Your Gateway

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

Additionally, other wireless access points in and around your home might affect your gateway's signal. Wireless access points are gateways, repeaters, WiFi range extenders, and any other device that emits a wireless signal for network access.

Position your gateway according to the following guidelines:

• Place your gateway near the center of the area where your computers and other devices operate, and within line of sight to your wireless devices.

• Make sure that the gateway is within reach of an AC power outlet and near Ethernet cables for wired computers.

• Place the gateway in an elevated location, minimizing the number walls and ceilings between the gateway and your other devices.

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

Cable Your Gateway

You can cable the gateway to a DSL line or to a cable modem.
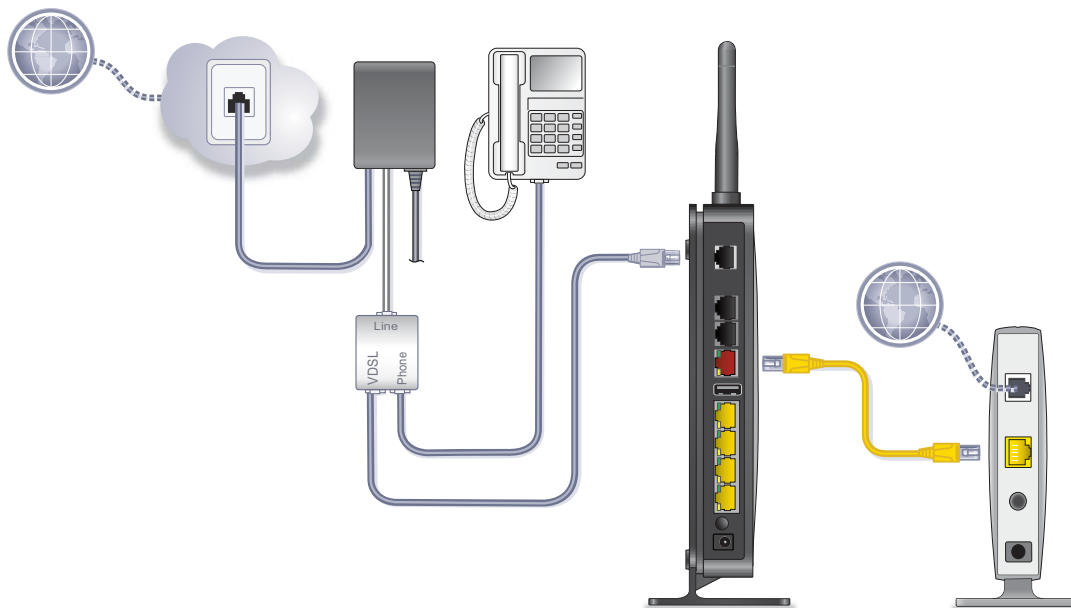
Figure 4. Gateway cabling diagram

For information about installation, see the installation guide that came in the package with the product.

2
Connect to the Network and Access the Gateway

You can connect to the gateway's WiFi network or LAN and you can use a web browser to log in to the gateway to view or change its settings.

This chapter contains the following sections:

- *Connect to the Network*
- *Types of Logins*
- *Log In to the Gateway*

Connect to the Network

You can connect to the gateway's network through a wired or WiFi connection. If you set up your computer to use a static IP address, change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Wired Connection

You can connect your computer to the gateway using an Ethernet cable and join the gateway's local area network (LAN).

➢ **To connect your computer to the gateway with an Ethernet cable:**

1. Make sure that the gateway has power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports on the rear panel of the gateway.

   Your computer connects to the local area network (LAN). A message might display on your computer screen to notify you that an Ethernet cable is connected.

WiFi Connection

You can connect to the gateway's WiFi network with Wi-Fi Protected Setup (WPS) or you can find and select the WiFi network.

➢ **To use WPS to connect to the WiFi network:**

1. Make sure that the gateway has power (its Power LED is lit).
2. Check the WPS instructions for your computer or wireless device.
3. Press the **WPS** button on the gateway.
4. Within two minutes, on your computer or WiFi device, press its **WPS** button or follow its instructions for WPS connections.

   Your computer or wireless device connects to the WiFi network.

➢ **To find and select the WiFi network:**

1. Make sure that the gateway has power (its Power LED is lit).
2. On your computer or wireless device, find and select the WiFi network.

   The WiFi network name is on the product label.

3. Join the WiFi network and enter the WiFi password.

   The password is on the product label.

   Your wireless device connects to the WiFi network.

Types of Logins

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

These types of logins are associated with the gateway:

- **Internet service login**. The login that your Internet service provider gave you logs you in to your Internet service. Your service provider gave you this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

- **WiFi network key or password**. Your gateway is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the gateway label.

- **Gateway login**. This logs you in to the gateway interface from a web browser as admin.

Log In to the Gateway

When you connect to the network (either with WiFi or with an Ethernet cable), you can use a web browser to access the gateway to view or change its settings. The first time you access the gateway, NETGEAR genie automatically checks to see if your gateway can connect to your Internet service. The next time you access the gateway with a browser, you are prompted to log in.

➢ **To log in to the gateway:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

Internet Setup 3

Usually, the quickest way to set up the router to use your Internet connection is to allow the genie to detect the Internet connection when you first access the router with a web browser. You can also customize or specify your Internet settings.

This chapter covers the following topics:

- *Use the Internet Setup Wizard*
- *Static IP Address*
- *Manually Specify an Internet Connection with a Login*
- *Manually Specify DSL Settings*
- *Manually Specify DSL Settings*
- *Specify When to Use DSL and Mobile Broadband Internet Connections*
- *Change to 3G Broadband Connection Mode*
- *Specify Mobile Broadband Connection Settings*
- *Specify IPv6 Settings*

Use the Internet Setup Wizard

The Internet Setup Wizard detects the type of Internet connection and helps you configure the gateway.

Note: If your Internet service provider assigned you a static IP address (this is uncommon), see *Static IP Address* on page 18.

➢ **To use the Internet Setup Wizard:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Setup Wizard**.

5. Click the **Next** button.

Broadband Connection Settings

Internet Connection Mode

Always use DSL connection ▾

Cancel   Next

6. In the **Internet Connection Mode** drop-down list, select one of the following:
   - Use DSL connection first and if fail 3G Mobile Broadband connection
   - Always use Mobile Broadband connection
   - Always use DSL connection

7. Click the **Next** button.

8. In the **Select Country** list, select your country.

9. Leave the **Yes** radio button selected and click the **Next** button.

   A connection detection progress screen displays. When the gateway detects the connection, more screens display.

10. When prompted, select your Internet service provider.

11. If your ISP requires login credentials, enter your user name and password and click the **Next** button.

   The Setup Wizard detects the connection type and displays relevant prompts.

12. Complete the fields for your connection type:
   - For a PPPoE or PPoA connection, type the user name and password.

     Both are case-sensitive.

   - For IP over ATM Classical IP assignment (RFC1577), **e**nter the assigned IP address, the subnet mask, and the IP address of the primary DNS server for your ISP.

     DNS servers translate an Internet name such as www.netgear.com to a numeric IP address.

13. Click the **Test** button.

   The Setup Wizard checks your Internet connection.

   Note: If you have trouble connecting to the Internet, see *Chapter 10, Troubleshooting*, for help.

14. After the test succeeds, click the **Apply** button.

   Your settings are saved.

Static IP Address

Internet service with a static IP address is uncommon. If the Setup Wizard detects this type of Internet connection, you are prompted to enter the following information:

- The Internet service provider's recommendation for one of these settings:
  - **Use Static IP Address**
  - **Use IP Over ATM** (IPoA — RFC1483 Routed)
- Your assigned IP address, subnet mask, and the IP address of your ISP gateway
- The IP address of your ISP primary DNS server and a secondary DNS server address if one is available

Your Internet service provider can provide this information to you.

Manually Specify an Internet Connection with a Login

➢ **To configure an Internet connection with a login:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **Internet Setup**.

5. In the WAN drop-down list, select a WAN.

6. For the Does your Internet connection require a login? setting, leave the **Yes** radio button selected.

7. Complete the fields to specify your Internet connection.

   For more information about the settings, see the online help.

8. Click the **Apply** button.

   Your settings are saved.

Manually Specify an Internet Connection Without a Login

➢ **To configure an Internet connection without a login:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **Internet**.

5. In the WAN drop-down list, select a WAN.

6. For the Does your Internet connection require a login? setting, select the **No** radio button.

7. If your Internet connection requires an account name or host name, type it in the **Account Name (If Required)** field.

8. If your Internet connection requires a domain name, type it in the **Domain Name (If Required)** field.

For the other sections in this screen, the default settings usually work, but you can change them. For more information about the settings, see the online help.

9. Complete the fields to specify your Internet connection settings.

10. Click the **Apply** button.

Your settings are saved.

Note: If you can access websites, but you get errors, it is likely that your DNS servers are not set up correctly. Contact your Internet service provider to get the DNS server addresses.

Manually Specify DSL Settings

You can view or change the gateway's DSL settings.

➢ **To specify the DSL settings:**

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

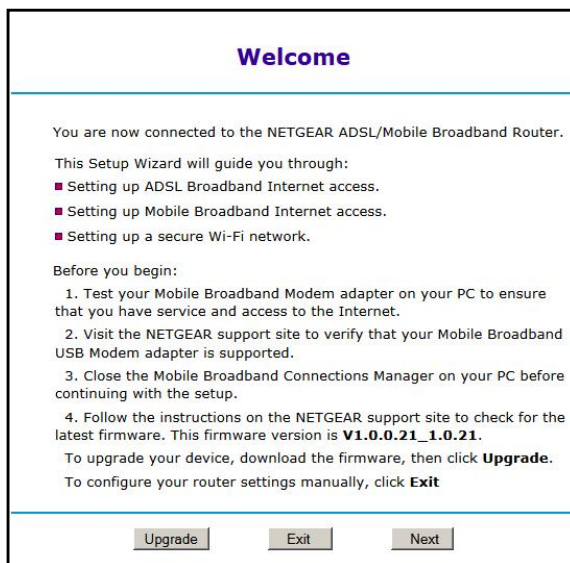2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Setup > DSL Settings**.

5. If your ISP provided you with a modulation, multiplexing method, or VPI and VCI numbers, enter the settings.

   Otherwise, the default settings are adequate.

6. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.

7. In the **VPI** field, type a number from 0 through 255.

   The default is 8.

8. In the **VCI** field, type a number from 32 through 65535.

   The default is 35.

9. Click the **Apply** button.

   Your settings are saved.

Specify When to Use DSL and Mobile Broadband Internet Connections

The gateway supports DSL and mobile broadband connections. You can specify the Internet connection mode that the gateway uses by default and in a failover situation.

➢ **To specify when to use DSL and mobile broadband:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Setup > Broadband Settings**.

5. In the **Internet Connection Mode** drop-down list, select one of the following:
   - Use DSL first and if fail use Mobile Broadband connection
   - Always use Mobile Broadband connection
   - Always use DSL connection

6. In the Failover Detection Method section, select one of the following radio buttons:
   - **DNS lookup using WAN DNS Server**.
   - **Perform a DNS lookup by a hostname**. If you select this option, you must enter the DNS lookup host name in the field to the right of this option.
   - **Ping this IP address**. If you select this option, you must enter the IP address to the right of this option.

7. (Optional) Customize the retry and failover settings.

8. Click the **Apply** button.

   Your settings are saved.

Change to 3G Broadband Connection Mode

By default, the gateway is set up to allow DSL connections. To use a 3G broadband connection, you must change this setting. Changing to a 3G broadband connection causes the gateway to reboot.

➢ **To change to 3G broadband connection mode:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Setup > Broadband Settings**.

5. In the **Internet Connection Mode** field, select **Always use 3G Mobile Broadband connection**.

6. Click the **Apply** button.

   The gateway reboots.

   ⚠️ **WARNING:**

   Do not interrupt the reboot process.

Specify Mobile Broadband Connection Settings

Before you can specify these settings, you must set the gateway's Internet connection mode to **Always use 3G Mobile Broadband connection**. See *Change to 3G Broadband Connection Mode* on page 23.

Note: To connect to the 3G network, you must have an active broadband service account. Contact your service provider for your user name, password, and the 3G network name.

➢ **To specify mobile broadband connection settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Setup > Mobile Broadband Settings**.

5. Enter the user name and password for your broadband service account.

6. (Optional) Select or clear the check boxes to customize the connection and roaming settings.

7. Click the **Apply** button.

   Your settings are saved.

Specify IPv6 Settings

➢ **To specify IPv6 settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > IPv6**.

5. In the **Internet Connection Type** drop-down list, select **6RD**.

   The screen adjusts.

6. Complete the fields based on the settings the information that your Internet service provider gave you.

7. Click the **Apply** button.

   Your settings are saved.

Control Access to the Internet

4

This chapter explains how to prevent objectionable content from reaching the computers and other devices that are connected to your network. It also explains how to customize firewall rules to specify exceptions to how network traffic to and from the Internet is handled.

This chapter includes the following sections:

- *Use Keywords to Block Internet Sites*
- *Schedule When to Block Internet Sites*
- *Avoid Blocking on a Trusted Computer*
- *Set Up Security Event Email Notifications*
- *Outbound Firewall Rules*
- *Set Up a Custom Port Forwarding Service*
- *How the Gateway Implements the Port Forwarding Rule*
- *Port Triggering*

Use Keywords to Block Internet Sites

You can use keywords to block certain Internet sites from your network. You can use blocking all the time or based on a schedule.

➢ **To block Internet sites:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select a keyword blocking option:
   - **Per Schedule**. Use keyword blocking according to a schedule you set. (See *Schedule When to Block Internet Sites* on page 28.)
   - **Always**. Use keyword blocking continuously.

6. In the **keyword** field, enter a keyword or domain that you want to block.
   - 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.

7. Click the **Add Keyword button.**

The keyword is added to the keyword list. The keyword list supports up to 32 entries.

8. **C**lick the **Apply** button.

   Keyword blocking takes effect.

Delete Keywords from the List to Be Blocked

➢ **To delete keywords from the list:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Do one of the following:

   - To delete a single word, select it and click the **Delete Keyword button.**

     The keyword is removed from the list.

   - **To delete all keywords on the list, click the Clear List button.**

     All keywords are removed from the list.

6. **Click t**he **Apply** button**.**

   Your changes are saved.

Schedule When to Block Internet Sites

When you schedule blocking, the same schedule is used to block sites and to block services. For information about how to specify what you want the gateway to block, see *Use Keywords to Block Internet Sites* on page 27.

➢ **To schedule blocking:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Select **ADVANCED > Security > Schedule**.

5. Specify when to block keywords and services:

    • **Days to Block**. Select the check box for each day that you want to block the keywords or select the **Every Day** check box, which automatically selects the check boxes for all days.

    • **Time of Day to Block**. Select a start time and end time in 24-hour format, or select **All Day** for 24-hour blocking.

6. Select your time zone from the list.

7. If you live in an area that observes daylight saving time, select the **Automatically adjust for daylight savings time** check box.

8. Click the **Apply** button.

    Your settings are saved.

Avoid Blocking on a Trusted Computer

You can exempt one trusted computer from blocking. The computer you exempt must have a fixed IP address. You can use the reserved IP address feature to specify the IP address. See *Reserved LAN IP Addresses* on page 59.

➢ **To specify a trusted computer:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

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

5. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.

6. In the **Trusted IP Address** fields, enter the IP address of the trusted computer.

7. Click the **Apply** button.

Your changes are saved.

Set Up Security Event Email Notifications

The gateway can email you its logs. The log records gateway activity and security events such as attempts to access blocked sites or services.

➢ **To set up email notifications:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Security > E-mail**.

5. Select the **Turn E-mail Notification On** check box.

6. In the **Your Outgoing Mail Server** field, enter the name of your Internet service provider's outgoing (SMTP) mail server (such as mail.myISP.com).

   You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent.

7. Enter the email address to which logs and alerts are sent in the **Send to This E-mail Address** field.

   This email address is also used for the From address. If this field is blank, log and alert messages are not sent.

8. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box.

    a. In the **User Name** field, type the user name for the outgoing email server.

    b. In the **Password** field, type the password for the outgoing email server.

9. To send alerts when someone attempts to visit a blocked site, select the **Send Alerts Immediately** check box.

10. To send logs based on a schedule, specify these settings:

    • From **Send logs according to this schedule** drop-down list, select the schedule type.

    • From the **Day** drop-down list, select the day.

    • From the **Time** drop-down list, select the time and select the **am** or **pm** radio button.

11. Click the **Apply** button.

    Your settings are saved.

    Logs are sent according to the schedule that you set. If the log fills up before the specified time, it is sent. After the log is sent, it is cleared from the gateway memory. If the gateway cannot email the log and the log buffer fills up, the gateway overwrites the log.

Outbound Firewall Rules

You can add firewall rules to block or allow specific traffic. For information about inbound rules, see *Set Up a Custom Port Forwarding Service* on page 35.

Note: This feature is for advanced administrators only. Incorrect configuration causes serious problems.

By default your gateway blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. You might need to create exceptions to this rule to allow remote computers to access a server on your local network or to allow certain applications and games to work correctly. Your gateway provides firewall rules for creating these exceptions.

Authorized communications are established according to inbound and outbound rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications.

Add a Custom Service

➢ **To add a custom service:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Security > Firewall Rules**.

5. Click the **Add a Custom Service** button.

6. In the **Name** field, type the name of the service.

7. In the **Type** list, select **TCP**, **UDP** or **TCP/UDP**.

   If you are not sure, select **TCP/UDP**.

8. Specify the range of ports in the **Start Port** and **Finish Port** fields.

9. Click the **Apply** button.

   The service is added.

Add Outbound Firewall Rules

By default, the gateway allows all communication from your network out to the Internet. You can add rules to restrict outbound Internet traffic.

Note: This feature is for advanced administrators only. Incorrect configuration causes serious problems.

➢ **To add firewall rules for an outbound service:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Select **ADVANCED > Security > Firewall Rules**.
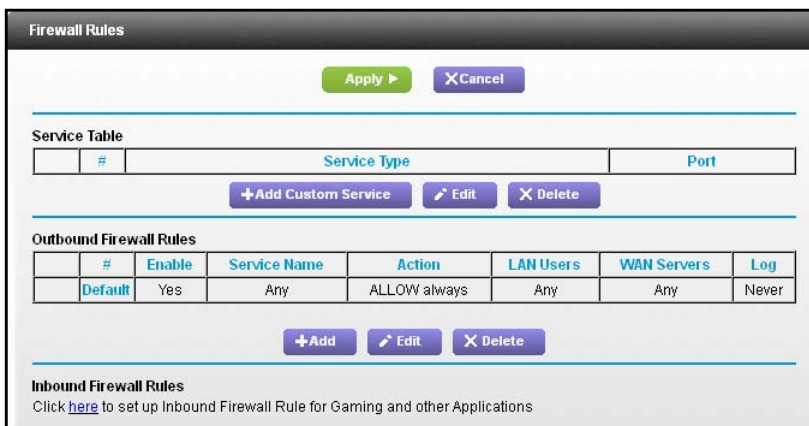
If you have not defined any outbound rules, only the default rule is listed in the Outbound Firewall Rules table. The default rule allows all outgoing traffic.

5. Click the **Add** button.
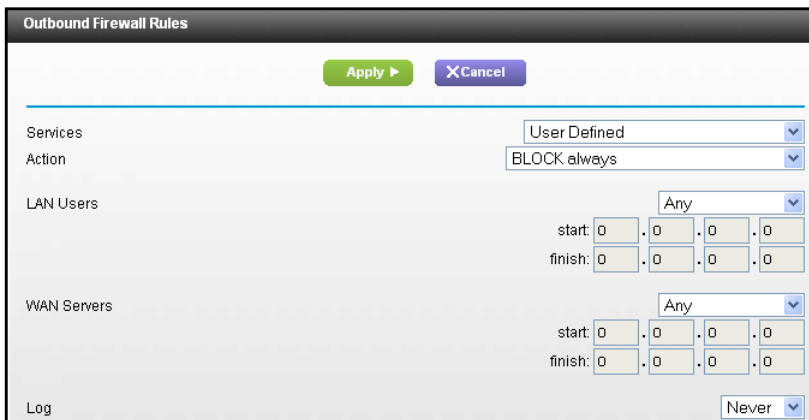
6. In the **Services** list, select the service.

If the service is not in the list, select **User Defined**. If you select User Defined, you must select the protocol and enter the name and the range of port numbers used by the service. For services on the list, these fields are filled in automatically.

7. In the **Action** list, select a block or allow setting.

8. To block specific LAN users, in the **LAN Users** list, select **Single Address** or **Address Range** and type the IP addresses.

9. To block specific WAN servers, in the **WAN Services** list, select **Single Address** or A**ddress Range** and type the IP addresses.

10. To log instances of when this rule is used, in the **Log** field, select **Always**.

11. Click the **Apply** button.

Your settings are saved. The Firewall Rules screen displays the new rule.

Edit an Outbound Firewall Rule

This feature is for advanced administrators only. Incorrect configuration causes serious problems.

➢ **To edit an outbound rule:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Security > Firewall Rules**.

   The table under Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule is listed. The default rule allows all outgoing traffic.

5. Select the radio button for the rule.

6. Click the **Edit** button.

7. Change the settings.

8. Click the **Apply** button.

   Your settings are saved.

Delete an Outbound Firewall Rule

➢ **To delete an outbound rule:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Security > Firewall Rules**.

The table under Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule is listed. The default rule allows all outgoing traffic.

5. Select the radio button for the rule.

6. Click the **Delete** button.

The rule is deleted.

Set Up a Custom Port Forwarding Service

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

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

➢ **To forward specific incoming protocols:**

1. Decide which type of service, application, or game you want to provide.

2. Find the local IP address of the computer on your network that will provide the service.

The server computer must always have the same IP address. Assign a reserved IP address to the server computer. See *Reserved LAN IP Addresses* on page 59.

3. Launch a web browser from a computer or wireless device that is connected to the network.

4. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

5. Enter the gateway user name and password.

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

The BASIC Home screen displays.

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

7. Leave the **Port Forwarding** radio button selected as the service type.
8. Click the **Add Custom Service** button.

9. In the **Service Name** field, enter a descriptive name.
10. In the **Service Type** field, select the protocol. If you are unsure, select **TCP/UDP**.
11. In the **External Starting Port** field, enter the beginning port number.

    If the application uses a single port, enter the same port number in the **Ending Port** field.

    If the application uses a range of ports, enter the ending port number of the range in the **External Ending Port** field.

12. Use one of the following methods to specify the internal port numbers:
    - Leave the **Use the same port range for internal port** check box selected.
    - Type the port numbers in the **Internal Starting Port** and **Internal Ending Port** fields.

13. Type the IP address in the **Internal IP address** field or select the radio button for an attached device listed in the table.
14. Click the **Apply** button.

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

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 gateway always gives your web server an IP address of 10.0.0.33.

2. In the Port Forwarding/Port Triggering screen, configure the gateway to forward the HTTP service to the local address of your web server at **10.0.0.33**.

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

3. (Optional) Register a host name with a Dynamic DNS service and specify that name in the Dynamic DNS screen of the gateway.

   For more information, see *Dynamic DNS* on page 70.

   Dynamic DNS makes it much easier to access a server from the Internet because you can type the name in the Internet browser. Otherwise, you must know the IP address that the Internet service provider assigned, which typically changes.

How the Gateway Implements the Port Forwarding Rule

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

1. When you type the URL www.example.com in your browser, the browser sends a web page request message with the following destination information:
   - **Destination address**. The IP address of www.example.com, which is the address of your gateway.
   - **Destination port number**. 80, which is the standard port number for a web server process.
2. Your gateway receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The gateway changes the destination in the message to IP address 10.0.0.223 and sends the message to that computer.
4. Your web server at IP address 10.0.0.223 receives the request and sends a reply message to your gateway.
5. Your gateway performs Network Address Translation (NAT) on the source IP address and sends the reply through the Internet to the computer or wireless device that sent the web page request.

Port Triggering

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

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

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

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

Note: If you enabled port triggering because you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), enable Universal Plug and Play (UPnP). See *Improve Network Connections with Universal Plug and Play* on page 75.

Add a Port Triggering Service

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

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

6. Click the **Add Service** button.

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

8. From the **Service User** list, select a user option:

- **Any** (the default) allows any computer on the Internet to use this service.

- **Single address** restricts the service to a particular computer. You must enter the IP address of the computer to which you want to grant access.

9. From the **Service Type** list, select a service.

If you are not sure, select **TCP/UDP**.

10. In the **Triggering Port** field, enter the number of the outbound traffic port that will open the inbound ports.

11. In the **Connection Type**, **Starting Port**, and **Ending Port** fields, enter the inbound connection port information.

12. Click the **Apply button**.

The service is added. You must enable port triggering before the gateway uses port triggering. For information about port triggering, see *Specify the Port Triggering Time-out* on page 39.

Specify the Port Triggering Time-out

➢ **To specify the port triggering time-out:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

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

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

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

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

Application Example: Port Triggering for Internet Relay Chat

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

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the 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 gateway.

3. Your gateway creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your 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. Noting your port triggering rule and observing the destination port number of 6667, your gateway creates another session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your gateway using the NAT-assigned source port (for example, port 33333) as the destination port and sends an "identify" message to your gateway with destination port 113.

6. When your gateway receives the incoming message to destination port 33333, it checks its session table to see if a session is active for port number 33333. Finding an active session, the gateway restores the original address information replaced by NAT and sends this reply message to your computer.

7. When your gateway receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The gateway replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

When you finish your chat session, your gateway eventually senses a period of inactivity in the communications and removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

Share a USB Drive Attached to the Gateway

5

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

This chapter contains the following sections:

- *USB Drive Requirements*
- *Access a USB Drive on the Network*
- *Control Access to the USB Drive*
- *Use FTP Within the Network*
- *View or Change Network Folders on a USB Drive*
- *Add a Network Folder on a USB Drive*
- *Edit a Network Folder on a USB Drive*
- *Approve USB Devices*
- *Safely Remove a USB Drive*
- *Change the Media Server Settings*

USB Drive Requirements

The gateway works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives that the 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 gateway.

The gateway supports the following file system types for full read/write access:

- FAT16, FAT32
- NTFS
- NTFS with compression format enabled
- Ext2, Ext3, Ext4
- XFS
- HFS
- HFS+

Access a USB Drive on the Network

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

➢ **To connect a USB drive:**

Insert your USB storage drive into the USB port on the rear panel of the gateway.

If your USB drive has a power supply, you must use it when you connect the USB drive to the gateway.

When you connect the USB drive to the 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.

Map the USB Device to a Windows Network Drive

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

1. Visit *http://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`.
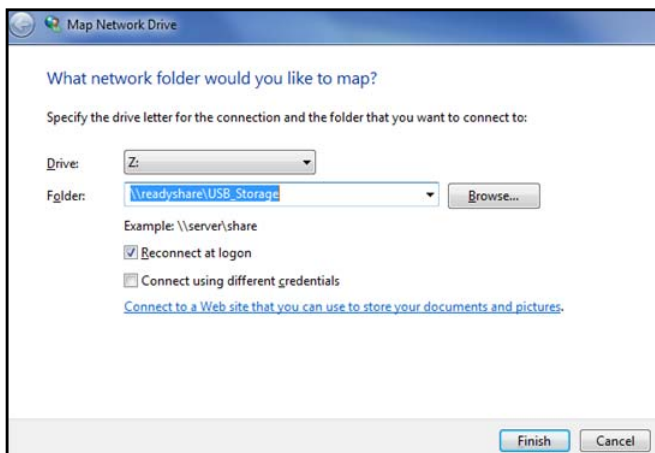
4. Select the drive letter to map to the network folder.

5. To connect to the USB drive as a different user, select the **Connect using different credentials** check box.

   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.

Control Access to the USB Drive

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

➢ **To specify the USB access settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Select **ADVANCED > USB Storage > Advanced Settings**.

5. Specify access to the USB storage device:

   • **Network Device Name**. This is the name used to access the USB device connected to the gateway. The default 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.

   • **Access Method**. Select the access methods:

     - **Network Neighborhood/MacShare. Enabled by default.**

     - **HTTP**. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.

     - **HTTP (via Internet)**. Disabled by default. If you enable this feature, remote users can type **http://**<public IP address/shares> (for example, http://1.1.10.102/shares) or a URL domain name to access the USB drive over the Internet. This feature supports file uploading only.

     - **FTP**. Disabled by default.

     - **FTP (via Internet)**. Disabled by default. If you select this check box, remote users can access the USB drive through FTP over the Internet. This feature supports both downloading and uploading of files.

6. Click the **Apply** button.

   Your changes are saved.

Use FTP Within the Network

File Transfer Protocol (FTP) lets you send and receive large files faster.

➢ **To allow FTP access:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > USB Storage > Advanced Settings**.

5. Select the **FTP** check box.

6. Click the **Apply** button.

   Your changes are saved.

View or Change Network Folders on a USB Drive

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

➢ **To view or change network folders:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > USB Storage > Advanced Settings**.

5. Scroll down to the Available Networks Folder section and view or adjust the following settings:

   • **Share Name**. If only one device is connected, the default share name is USB_Storage. (Some gateway models have more than one USB port.)

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

   • **Read Access and Write Access**. Show the permissions and access controls on the network folder. All – no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the gateway.

   • **Folder Name**. Full path of the network folder.

- • **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- • **Total Space and Free Space**. Show the current utilization of the storage device.

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

   Your changes are saved.

Add a Network Folder on a USB Drive

You can add network folders on the USB storage device.

➢ **To add a network folder:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > ReadySHARE**.

   The Advanced ReadySHARE screen displays.

5. Click the **Create Network Folder** button.

   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.

6. In the **USB Device list**, select the USB drive.

7. Click the **Browse** button and in the **Folder** field, select the folder.

8. In the **Share Name** field, type the name of the share.

9. In the **Read Access** list and the **Write Access** list, select the settings that you want.

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

10. Click the **Apply** button.

The folder is added on the USB device.

Edit a Network Folder on a USB Drive

You can edit network folders on the USB storage device.

➢ **To edit a network folder:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Select **ADVANCED > ReadySHARE**.

The Available Network Folders list displays.

5. Click the **Edit** button.

The Edit Network Folder screen displays.

6. Change the settings as needed:
   - In the **Share Name** field, edit the name of the share.
   - In the **Read Access** list and the **Write Access** list, select the settings that you want.

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

7. Click the **Apply** button.

Your changes are saved.

Approve USB Devices

For more security, you can set up the gateway to share only USB devices that you approve.

➢ **To approve USB devices:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > USB Settings.**
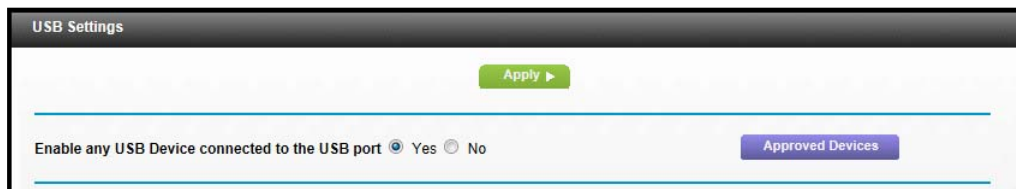
   By default the Enable any USB Device connection to the USB port **Yes** radio button is selected. This setting lets you connect and access all your USB drives.

5. Select the **No** radio button.

6. **Click the Approved Devices** button.

   The approved and available USB devices display.
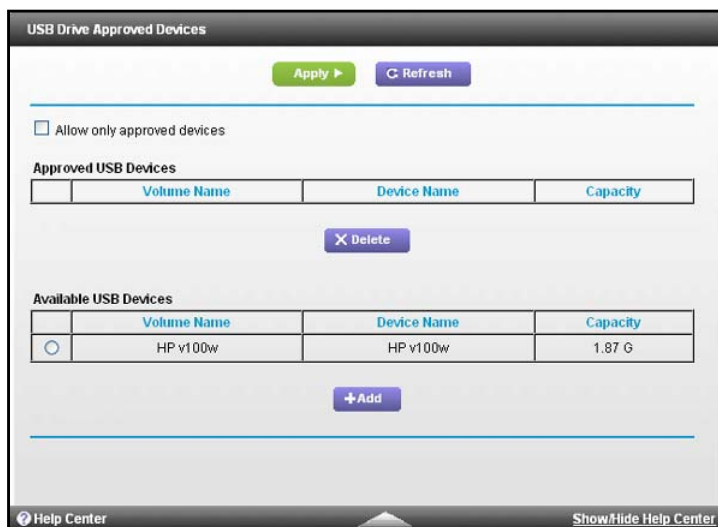
7. In the Available USB Devices list, select the drive that you want to approve.

8. Click the **Add** button.

9. Select the **Allow only approved devices** check box.

10. Click the **Apply** button.

    Your change takes effect.

11. To work with another USB device, first click the **Safely Remove USB Device** button for the currently connected USB device. Connect the other USB device, and repeat this process.

Safely Remove a USB Drive

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

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **USB Storage > Basic Settings**.

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

   This takes the drive offline.

6. Physically disconnect the USB drive.

Change the Media Server Settings

By default, the gateway is set up to act as a ReadyDLNA media server. This enables playback of videos, movies, and pictures on DLNA or UPnP AV compliant media players like Xbox360, Playstation, and NETGEAR media players.

➢ **To change the media server settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. To disable the media server, clear the **Enable Media Server** check box.
6. To change the media server name, type a name in the **Media Server Name** field.

   This is the name that displays on media players.

7. To stop automatic scanning, clear the **Automatic (when new files added)** check box.

   Automatic scanning scans for media files whenever new files are added to ReadySHARE USB storage (the USB device connected to the gateway's USB port). Only shared folders with the Read Access setting of All/no password can be scanned for media files.

8. Click the **Apply** button.

   Your settings are saved.

Specify Network Settings

6

This chapter includes the following sections:

View or Change the WAN Settings

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

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. View or change the following settings:

   • Enable PPPoE Relay. Allow a PPPoE client on a local computer to connect to a remote PPPoE server with the gateway acting as a relay agent.

   • **WAN Preference**. By default, this is set to **Auto-Detect**, but you can specify **Must use DSL WAN** or **Must use Ethernet WAN**.

   • **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. Select this check box only in special circumstances.

- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing but it makes the firewall security less effective. See *Default DMZ Server* on page 55.

- **Respond to Ping on Internet Port**. This feature allows your gateway to be discovered. Use this feature only as a diagnostic tool or if you have a specific reason.

- **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive multicast traffic from the Internet. If you do not need this feature, you can select this check box to disable it.

- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. Change the MTU only if you are sure that it is necessary for your Internet connection. See *Default DMZ Server* on page 55.

- **Disable SIP ALG**. Some VoIP applications do not work well with the SIP ALG. Selecting this check box to turn off the SIP ALG might help your VoIP devices to create or accept a call through the gateway.

- **NAT Filtering**. Network Address Translation (NAT) determines how the gateway processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall but allows almost all Internet applications to work.

6. Click the **Apply** button.

   Your changes are saved.

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

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

The gateway usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have the

gateway forward the traffic to one computer on your network. This computer is called the default DMZ server.

Set Up a Default DMZ Server

➢ **To set up a default DMZ server:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select the **Default DMZ Server** check box.

6. Type the IP address.

7. Click the **Apply** button.

   Your change takes effect.

Change the Gateway's Device Name

The gateway's device name is VEVG2660-1TKSAS. This device name displays in a file manager when you browse your network.

➢ **To change the gateway's device name:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. In the **Device Name** field, type a new name.

6. Click the **Apply** button.

Your change is saved.

Change the LAN TCP/IP Settings

The gateway is preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The gateway's default LAN IP configuration is as follows:

• **LAN IP address**. 10.0.0.2

• **Subnet mask**. 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings.

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

➢ **To change the LAN TCP/IP settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

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

5. In the **IP Address** field, type the IP address.
6. In the **IP Subnet Mask** field, type the subnet mask of the gateway.

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

7. Click the **Apply** button.

    Your changes are saved.

    If you changed the LAN IP address of the gateway, you are disconnected when this change takes effect.

To reconnect, close your browser, relaunch it, and log in to the gateway.

Specify the IP Addresses That the Gateway Assigns

By default, the gateway acts as a Dynamic Host Configuration Protocol (DHCP) server. The 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 gateway.

These addresses must be part of the same IP address subnet as the gateway's LAN IP address. Using the default addressing scheme, define a range between 10.0.0.3 and 10.0.0.254, although you can save part of the range for devices with fixed addresses.

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

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

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Specify the range of IP addresses that the gateway assigns:

   a. In the **Starting IP Address** field, type the lowest number in the range.

      This IP address must be in the same subnet as the gateway.

   b. In the **Ending IP Address** field, type the number at the end of the range of IP addresses.

      This IP address must be in the same subnet as the gateway.

6. Click the **Apply** button.

   Your settings are saved.

Reserved LAN IP Addresses

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

Reserve an IP Address

➢ **To reserve an IP address:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. In the Address Reservation section of the screen, click the **Add** button.

6. In the **IP Address** field, type the IP address to assign to the computer or server.

   Choose an IP address from the gateway's LAN subnet, such as 10.0.0.x.

7. Type the MAC address of the computer or server.

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

8. Type a name for the device.

9. Click the **Add** button**.**

   The reserved address is entered into the table.

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

Edit a Reserved LAN IP Address

➢ **To edit a reserved address:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select the radio button next to the reserved address.

6. Click the **Edit** button.

7. Change the settings.

8. Click the **Apply** button.

   Your changes are saved.

Delete a Reserved LAN IP Address

➢ **To delete a reserved address:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select the radio button next to the reserved address.

6. Click the **Delete** button.

   The address is removed.

Use the WPS Wizard for WiFi Connections

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

➢ **To use the WPS Wizard:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Click the **Next** button.

6. Select a setup method:

   - **Push button**. Click the **WPS** button on this screen.

   - **PIN Number**. The screen adjusts. Enter the client security PIN and click the **Next** button.

7. Within two minutes, go to the client device and use its WPS software to connect to the WiFi network.

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

Specify Basic WiFi Settings

The 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 gateway label. The preset SSID and password are uniquely generated for every device to maximize your wireless security.

You do not need to change the security settings. If you change the 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 wireless computer to change the SSID or other wireless security settings, you are disconnected when you click the **Apply** button. To avoid this problem, use a computer with a wired connection to access the gateway.

➢ **To specify basic wireless settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **Wireless**.

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

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

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

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

7. In the **Region** list, select your region.

   In some locations, you cannot change this setting.

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

   In some regions, not all channels are available. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

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

9. To change the mode, select it from the **Mode** list.
   - **Up to 145 Mbps**. This is the default setting, which allows 802.11n and 802.11g wireless devices to join the network.
   - **g & b. This** supports up to 54 Mbps.
   - **300-Mbps**.802.11n devices can connect at this speed.

10. Click the **Apply** button.

    Your settings are saved.

If you used WiFi to connect to the network and you changed the SSID, you are disconnected from the network.

11. Make sure that you can connect with WiFi to the network with its new settings.

If you cannot connect, check the following:

- Is your computer or wireless device connected to another WiFi network in your area? Some wireless devices automatically connect to the first open network without wireless security that they discover.

- Is your computer or wireless device trying to connect to your network with its old settings (before you changed the settings)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

Change the WiFi Security Option

Your gateway comes with preset WPA2 or WPA security. The password that you enter to connect to your network is unique to your gateway and is on the gateway label. You don't need to change these settings, but you can. Best practice is to avoid disabling security.

➢ **To change the WPA settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **Wireless**.

5. Under Security Options, select a WPA option:
   - WPA2-PSK [AES]
   - WPA-PSK [TKIP] + WPA2-PSK [AES]

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

   The **Passphrase** field displays.

6. In the **Passphrase** field, enter the network key (password) that you want to use.

   It is a text string from 8 to 63 characters.

7. Write down the new password and keep it in a secure place for future reference.

8. Click the **Apply** button.

   Your changes are saved.

Set Up a WiFi Guest Network

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

➢ **To set up a guest network:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **Guest Network**.

5. Select any of the following wireless settings:

   • **Enable Guest Network**. When this check box is selected, the guest network is enabled and guests can connect to your network using the SSID of this profile.

   • **Enable SSID Broadcast**. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.

- **Allow guest to see each other and access my local network**. If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.

- **Enable Wireless Isolation**. If this check box is selected, wireless clients (computers or devices that connect to the WiFi network) can access the Internet, but cannot access other clients.

6. Give the guest network a name.

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

7. Select a security option.

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

8. Click the **Apply** button.

   Your settings are saved.

Control the WiFi Radio

The gateway has an internal wireless radio that broadcast signals in the 2.4 GHz range. By default, this radio is on so that you can connect wirelessly to the gateway. When the wireless radio is off, you can still use an Ethernet cable for a LAN connection to the gateway.

You can turn the wireless radio on and off with the WiFi On/Off button on the gateway, or you can log in to the gateway and enable or disable the wireless radio. If you are close to the gateway, it might be easier to press its **WiFi On/Off** button. If you are away from the gateway or have already logged in, it might be easier to enable or disable the radio.

Use the WiFi On/Off Button

➢ **To turn the wireless radio off and on with the WiFi On/Off button:**

   Press the **WiFi On/Off** button on the gateway for two seconds.

   If you turn off the wireless radio, the 2.4 GHz LED and the WPS LED turn off. If you turn on the wireless radio, the 2.4 GHz LED and the WPS LED light.

Enable or Disable the Wireless Radio

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

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select or clear the **Enable Wireless Router Radio** check box.

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

6. Click the **Apply** button.

   If you disabled the wireless radio, the 2.4 GHz LED and the WPS LED turn off. If you enabled the wireless radio, the 2.4 GHz LED and the WPS LED light.

Specify WPS Settings

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

➢ **To specify WPS settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

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

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

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

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

   By default, the **Keep Existing Wireless Settings** check box is selected. Leave this check box selected.

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

7. Click the **Apply** button.

   Your changes are saved.

Set Up a Wireless Card Access List

By default, any wireless computer or device that is configured with the correct SSID is allowed access to your wireless network. For increased security, allow only specific wireless computers and devices to access the wireless network based on their MAC addresses.

➢ **To set up wireless card access:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

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

6. Click the **Add** button.

   The screen displays a list of available wireless cards.

7. To add a device from the Available Wireless Cards list, do the following:

   a. Select the device.

   b. Click the **Add** button.

   The device displays in the Wireless Card Access List.

8. To add a computer or device that is not in the list, do the following:

   a. Type a name in the **Device Name** field.

   b. Type the MAC address in the **MAC Address** field.

      The MAC address is found on the computer or device.

   c. Click the **Add** button.

The device displays in the Wireless Card Access List.

9. Select the **Turn Access Control On** check box.

10. Click the **Apply** button.

Your settings are saved.

Dynamic DNS

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

If your Internet service provider assigns a private WAN IP address (such as10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

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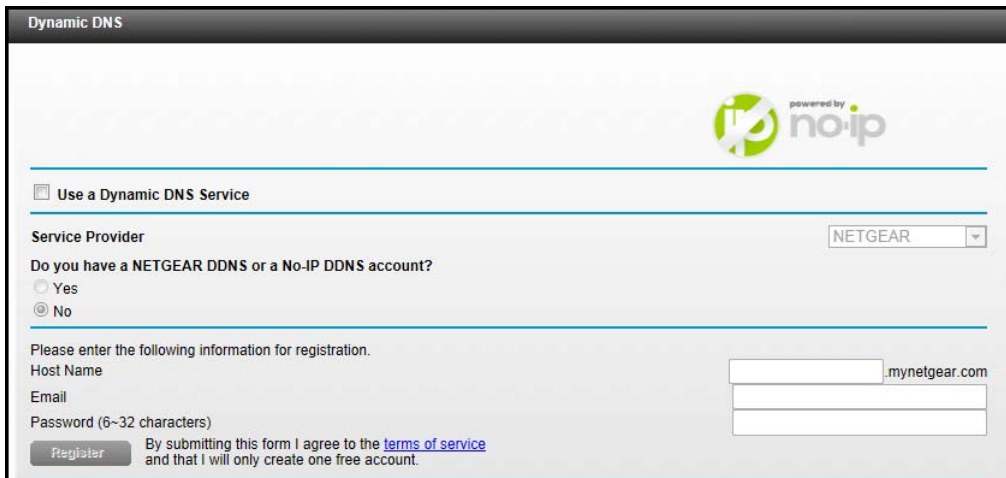
Set up Dynamic DNS

➢ **To set up Dynamic DNS:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

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

5. Register for an account with one of the Dynamic DNS service providers whose URLs display in the **Service Provider** list.

6. Select the **Use a Dynamic DNS Service** check box.

7. In the **Service Provider** list, select the URL for your Dynamic DNS service provider.

8. IN the **Host Name** field, type the host name (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 name 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 configuration is saved.

View Devices Currently on the Network

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

➢ **To view devices on the network:**

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

2. Type **http://www.routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **Attached Devices**.

Attached Devices			
		Refresh	
Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.1.2	F0:DE:F1:0F:35:FE	MPAWLAN
Wireless Devices (Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name

The Wired Devices section lists devices that are connected to the gateway with Ethernet cables. The Wireless Devices section lists devices that are connected to the wireless network.

The following information is displayed:

- **IP Address**. The IP address that the gateway assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.

- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

- **Device Name**. If the device name is known, it is shown here.

To update this screen, click the **Refresh** button.

Custom Static Routes

Static routes provide routing information to your gateway. Under usual circumstances, the gateway has adequate routing information after it has been configured for Internet access, and you do not need to configure more static routes. You must configure static routes only for unusual cases such as multiple gateways or multiple IP subnets on your network.

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

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN gateway on your home network for connecting to the company where you are employed. This gateway's address on your LAN is 192.168.1.100.

- Your company's network address is 134.177.0.0.

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

In this case you must define a static route, telling your gateway that 134.177.0.0 should be accessed through the ISDN gateway at 192.168.1.100. This example assumes the following settings:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.

- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN gateway at 192.168.1.100.

- A metric value of **1** works because the ISDN gateway is on the LAN.

- **Private** is selected only as a precautionary security measure in case RIP is activated.

Set Up a Static Route

➢ **To set up a static route:**

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

2. Type **http://www.routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Static Routes**.

5. Click the **Add** button.

   The screen adjusts:

6. In the **Route Name** field, type a name for this static route (for identification purposes only).

7. To limit access to the LAN only, select the **Private** check box.

   If you select **Private**, the static route is not reported in RIP.

8. To make this route effective, select the **Active** check box.

   By default, the **Active** check box is selected.

9. Type the IP address of the final destination.

10. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.

11. Type the gateway IP address, which must be a gateway on the same LAN segment as the gateway.

12. Type a number from 1 through 15 as the metric value.

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

13. Click the **Apply** button.

    The route is added to the table on the Static Routes screen.

Edit a Static Route

➢ **To edit a static route:**

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

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

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Static Routes**.

    The Static Routes screen displays.

5. In the table, select the radio button next to the route that you want to edit.

6. Click the **Edit** button.

    The Static Routes screen adjusts.

7. Edit the route information.

8. Click the **Apply** button.

    Your changes are saved.

Delete a Static Route

➢ **To delete a static route:**

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

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

    A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > Static Routes**.

    The Static Routes screen displays.

5. In the table, select the radio button next to the route that you want to delete.

6. Click the **Delete** button.

    The route is removed from the table.

Improve Network Connections with Universal Plug and Play

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

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

➢ **To enable Universal Plug and Play:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Advanced Setup > UPnP**.

5. Select the **Turn UPnP On** check box.

By default, this check box is selected. If the **Turn UPnP On** check box is cleared, the gateway does not allow any device to automatically control router resources, such as port forwarding.

6. Type the advertisement period in minutes.

   The advertisement period specifies how often the 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 have current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

7. Type the advertisement time to live 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 should be 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.

8. Click the **Apply** button.

   The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the gateway and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

   To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

Voice Settings

7

This chapter covers the following topics:

- *Specify VoIP Settings*
- *View the VoIP Status*
- *View the Call Log*

Specify VoIP Settings

➢ **To specify VoIP settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Telephony Setting > VoIP Settings**.

5. Specify the settings.

   For information about the settings, see the online help.

6. Click the **Apply** button.

   Your settings are saved.

View the VoIP Status

➢ **To view the VoIP status:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Telephony > VoIP Status**.

View the Call Log

The call log displays recent call activities including missed calls, successful calls, and incoming calls.

➢ **To view or change the call log:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Telephony > Call Log**.
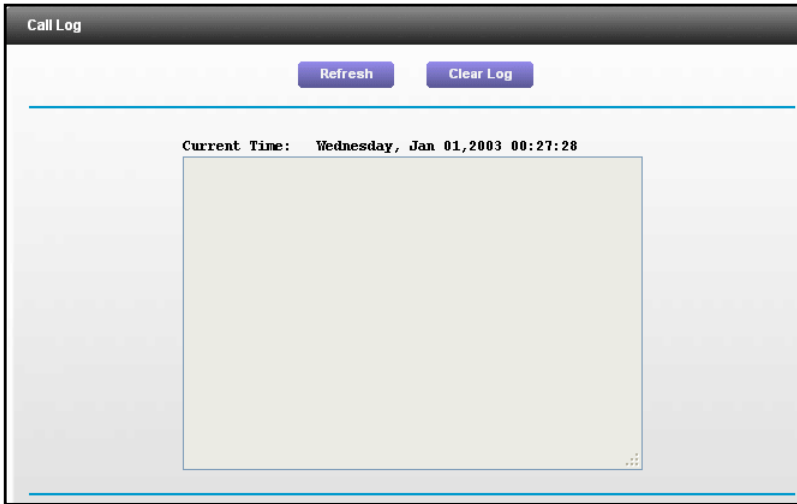
Manage Your Network

8

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

This chapter includes the following sections:

- *View Gateway Status*
- *Update the Firmware*
- *Reboot the Gateway*
- *View Logs of Gateway Activity*
- *Manage the Gateway Configuration File*
- *Change the admin Password*
- *Set Up Password Recovery for admin*
- *Recover the admin Password*
- *Look Up the IP Address for a DNS URL*
- *Display the Gateway's Routing Table*
- *Run the Ping Utility*
- *Set Up Remote Management*
- *Monitor Internet Traffic*

View Gateway Status

➢ **To view gateway status and usage information:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

   The following screen displays.

Scroll to view more

View WAN Information

➢ **To view gateway Internet port information:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

The WAN1 through WAN5 panes display these WAN Internet port settings:

- **MAC Address**. The MAC address of the WAN Internet port.
- **IP Address/Mask**. The IP address of the WAN Internet port.
- **Connection**. The type of WAN Internet port connection.
- **IP Subnet Mask**. The subnet mask.
- **Domain Name Server**. The IP address of the Domain Name Server.

View WAN Statistics

➢ **To view the WAN statistics:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.
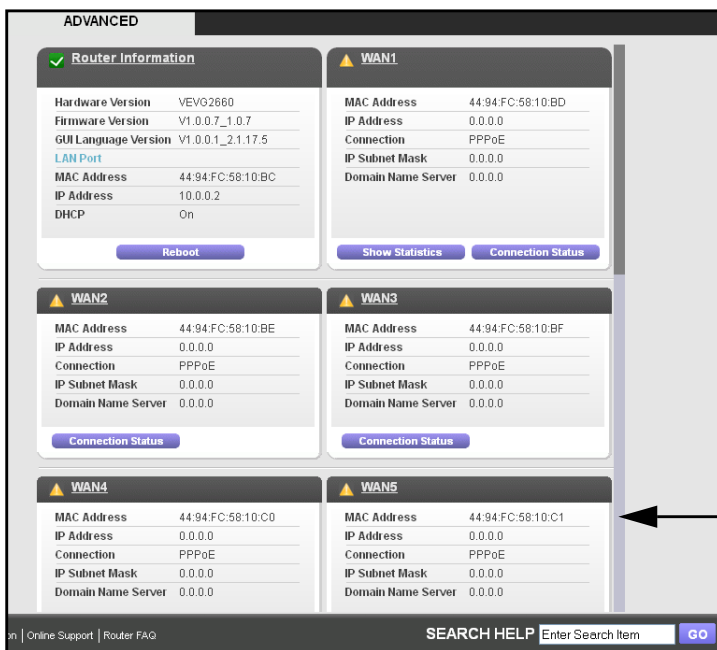
A login screen displays.

3. Enter the gateway user name and password.

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

The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

5. In the WAN1 pane, click **the Show Statistics** button.

Show Statistics

System Up Time 00:24:30

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link Down	0	0	0	0	0	00:00:00
LAN1	Link Down						--
LAN2	Link Down						--
LAN3	Link Down	9776	15417	0	6346	1090	--
LAN4	Link Down						--
2.4G WLAN b/g/n							

ADSL Link	Downstream	Upstream
Connection Speed		
Line Attenuation		
Noise Margin		

Poll Interval : 5 (secs)   [Set Interval]   [Stop]

The following information displays:

- **System Up Time**. The time elapsed since the gateway was last restarted.

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

  - **Status**. The link status of the port.

  - **TxPkts**. The number of packets transmitted on this port since reset or manual clear.

  - **RxPkts**. The number of packets received on this port since reset or manual clear.

  - **Collisions**. The number of collisions on this port since reset or manual clear.

  - **Up Time**. The time elapsed since this port acquired the link.

  - **Poll Interval**. The interval at which the statistics are updated in this screen.

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

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

View WAN Connection Status

➢ **To view the WAN connection status:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

5. In a WAN pane, click **the Connection Status** button.

The following information displays:

- **Connection Time**. The time that elapsed since the connection was established.

- **Connection Status**. The status of the connection: Connected, Disconnected, Negotiation (---, Success), or Authentication (---, Success). --- indicates failure.
- **Negotiation**.
- **Authentication**.
- **IP Address**. The IP address that is assigned to the gateway.
- **Subnet Mask**. The subnet mask that is assigned to the gateway.

Update the Firmware

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

➢ **To manually update your gateway with firmware that you downloaded:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.
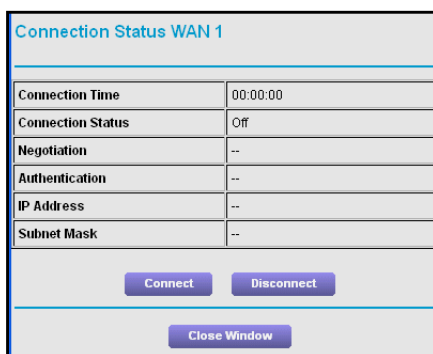
   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Click **Browse**, navigate to the firmware file (the file ends in `.img`), and select the firmware file.

6. Click the **Upload** button.

> ⚠️ **WARNING:**
>
> **To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the gateway.**

A progress bar shows the progress of the firmware upload process.

When the upload is complete, your gateway restarts. The upload process can take up to three minutes and the upgrade process typically takes about one minute. To determine whether you need to reconfigure the gateway after upgrading, read the new firmware release notes.

Reboot the Gateway

Rebooting the gateway disconnects all computers and mobile devices from the gateway's network.

➢ **To reboot the gateway:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

5. In the Router Information pane, click the **Reboot** button.

    A confirmation message displays.

6. Click the **OK** button.

    The gateway reboots.

View Logs of Gateway Activity

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

➢ **To view and customize logs:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Logs**.
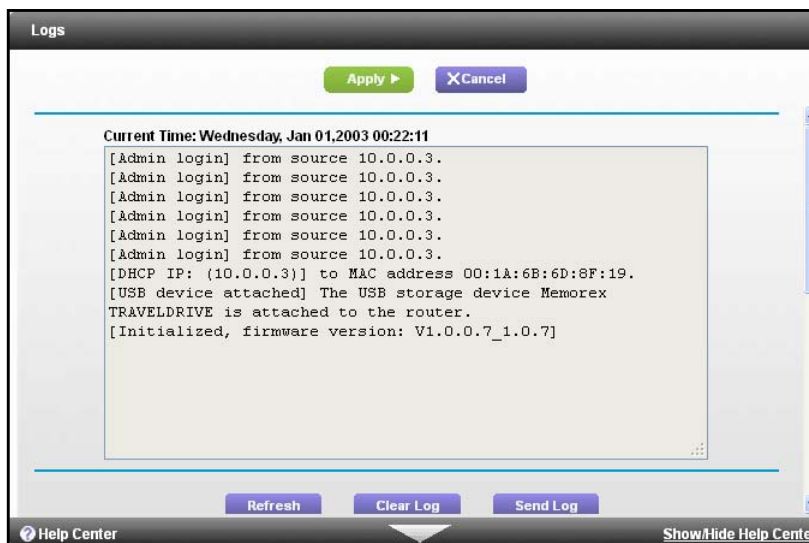
    The log screen shows the following information:

    - **Description**. The action that occurred.
    - **Count**. The number of occurrences.
    - **Last Occurrence**. The date and time the log entry was recorded.
    - **Target**. The name or IP address of the website or news group visited or to which access was attempted.
    - **Source**. The source IP address of the initiating device for this log entry.

5. To customize the log, clear or select the check boxes.

6. Click the **Apply** button.

    Your settings are saved.

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

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

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

Control the Syslog

➢ **To control the syslog:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.
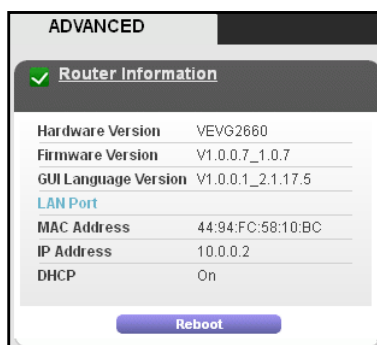
   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Scroll down to the Syslog section of the screen.

6. To disable the syslog, select the **Disable** radio button.

7. To broadcast the syslog, select the **Broadcast on LAN** radio button.

8. To send the syslog to a syslog server, select the **Send to this Syslog server IP address** and type the IP address in the corresponding field.

9. Click the **Apply** button.

   Your settings are saved.

Manage the Gateway Configuration File

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

Back Up the Gateway's Configuration Settings

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

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

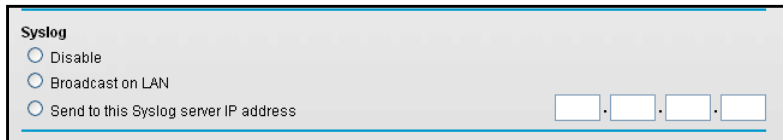2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Click the **Back Up** button.

6. When prompted, specify a location on your network and click the **OK** button.

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

Restore Configuration Settings

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

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Click the **Browse** button to find and select the `.cfg` file.

6. Click the **Restore** button.

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

WARNING:

Do not interrupt the reboot process.

Erase the Current Configuration Settings

You can erase the current configuration and restore the factory default settings. You might want to do this if you move the gateway to a different network. (For more information, see *Factory Settings* on page 114.)

➢ **To erase the configuration settings:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Click the **Erase** button.

The factory default settings are restored. The user name is admin, the password is password, and the LAN IP address is 10.0.0.2. DHCP is enabled.

Change the admin Password

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

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

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

2. Type **http://www.routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Type the old password, and type the new password twice.

6. To be able to recover the password, select the **Enable Password Recovery** check box.

   NETGEAR recommends that you enable password recovery.

7. Click the **Apply** button.

   Your changes are saved.

Set Up Password Recovery for admin

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

➢ **To set up password recovery:**

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

2. Type **http://www.routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

   The Set Password screen displays.

5. Select the **Enable Password Recovery** check box.

6. Select two security questions and provide answers to them.

7. Click the **Apply** button.

   Your changes are saved.

Recover the admin Password

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

➢ **To recover the admin password:**

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

   A login screen displays.

2. Click the **Cancel** button.

   If password recovery is enabled, you are prompted to enter the serial number of the gateway.

   The serial number is on the product label.

3. Enter the serial number of the gateway.

4. Click the **Continue** button.

   A screen displays requesting the answers to your security questions.

5. Enter the saved answers to your security questions.

6. Click the **Continue** button.

   A screen displays your recovered password.

7. Click the **Login again** button.

   A login screen displays.

8. With your recovered password, log in to the gateway.

Look Up the IP Address for a DNS URL

➢ **To perform a DNS lookup:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Diagnostics**.

5. In the **Internet Name** field, type the DNS URL.

6. Click the **Lookup** button.

   The IP address for the DNS server displays.

Display the Gateway's Routing Table

➢ **To display the routing table:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Diagnostics**.

5. Click the **Display** button.

The routing table displays.

Run the Ping Utility

Ping is an administration utility that tests whether a computer on the network is reachable and measures the time it takes messages sent from the originating device to reach a destination computer and return.

➢ **To run a ping test:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

    A login screen displays.

3. Enter the gateway user name and password.

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

    The BASIC Home screen displays.

4. Select **ADVANCED > Administration > Diagnostics**.

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

6. Click the **Ping** button.

    The ping results display.

    To stop a ping test, click the **Abort Test button.**

To clear the results from the display, click the **Clear Results button.**

Set Up Remote Management

You can access your gateway over the Internet to view or change its settings.

Note: Be sure to change the gateway login password to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See *Change the admin Password* on page 90.

➢ **To set up remote management:**

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

2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

5. Select the **Turn Remote Management On** check box.

6. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the gateway's remote management.

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

   Select one of the following:

   • **Only This Computer**. Enter the IP address that will be allowed access.

- **IP Address Range**. Enter a beginning IP address and an ending IP address.
- **Everyone**. Allows access from any IP address on the Internet.

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

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

8. Click the **Apply button**.

   Your changes are saved.

Use Remote Access

Before you can access the gateway remotely, you must log in to the gateway and set up remote management. See *Set Up Remote Management* on page 95.

➢ **To use remote access:**

1. Launch a web browser on a computer that is not on your home network.
2. Type your gateway's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

   For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

Monitor Internet Traffic

➢ **To monitor Internet traffic:**

1. Launch a web browser from a computer or wireless device that is connected to the network.
2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

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

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

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

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

    -   Select the **Traffic volume control by** radio button and then select one of the following options:
        -   **No Limit**. No restriction is applied when the traffic limit is reached.
        -   **Download only**. The restriction is applied to incoming traffic only.
        -   **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
    -   Select the Connection time control radio button and enter the allowed hours in the Monthly limit field.

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

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

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

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

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

    -   The Internet LED blinks green or amber.

- The Internet connection is disconnected and disabled.

10. Click the **Apply** button.

Your settings are saved.

11. In the Internet Traffic Statistics section, monitor the data traffic:

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

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

VPN Lite

9

This chapter includes the following sections:

- *VPN Lite Overview*
- *Configure VPN Lite Sites*

VPN Lite Overview

VPN Lite is a secure, easy-to-use, and cost-effective virtual private network (VPN). With VPN Lite, you can configure the network that is right for you with the flexibility to adjust the configuration as your business needs change. A VPN Lite configuration consists of sites and individual connections. A site is a device within your VPN network that has a private static IP address. Each site within the network has a private VPN connection with any other site in the network. You can connect up to 50 sites on a VPN Lite network without affecting your monthly DSL ISP bill.

Note: To learn more about the Telkom VPN Lite service offering, log in to the Telkom VPN Lite web portal at *http://www.telkom.co.za/*.

Note: The VPN Lite connection cannot be established over 3G mobile broadband. When the DSL connection fails, the gateway fails over to 3G mobile broadband when the unit is configured to do so, but the VPN Lite connection remains unavailable until the DSL connection is restored.

Configure VPN Lite Sites

The VPN Lite Setup Wizard lets you configure your VPN Lite network connections one by one.

➢ **To use the VPN Lite Wizard:**

1. Launch a web browser from a computer or wireless device that is connected to the network.
2. Type **http://routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.
3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.
4. **Select ADVANCED > VPN Lite Wizard.**
5. Read the notice on the VPN Lite setup screen and click the **Next** button.

The VPN lite Configuration screen displays:

6. Enter the information for one of the sites that you configured on the Telkom VPN Lite web portal and the click **Next** button

   Note: .The ampersand (&) character is not supported.

   For the site that you are adding to your network, complete the following fields:

   • **Username**. Enter the user name that you configured.
   • **Password**. Enter the password that you configured.
   • **LAN IP/netmask**. Enter the private and static IP address that you configured.

   Note: The IP address for each site configured must be different and fall within a different IP subnet range. For example, site1@evpn.lite.0001 can be 10.0.1.0/24. Then the IP subnet for site2@evpn.lite.0002 must be a different subnet, like 10.0.2.0/24. The IP address must correspond exactly to the one configured on the VPN Lite web page.

7. Review the configuration details and click the **Finish** button.

   Your settings are saved.

   Note: After clicking the **Finish** button, you might need to connect to your gateway with the new LAN IP address entered when you configured VPN Lite. Wait until the progress bar on the screen has completed before attempting to reconnect.

8. Repeat this process for every VPN Lite site that you want to add to your network.

Troubleshooting 10

This chapter provides information to help you diagnose and solve problems you might have with your router.

This chapter includes the following sections:

- *Access a Forgotten WiFi Password*
- *WiFi Connections*
- *Changes Not Saved*
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Gateway*
- *The Gateway Cannot Access the Internet*
- *Troubleshoot Your Network Using the Ping Utility*
- *Troubleshoot IP Addresses*
- *Problems with Date and Time*

Access a Forgotten WiFi Password

The gateway comes preset with a unique WiFi network name and WiFi password. This information is on the product label. You can also set up a guest network to allow visitors to access your Internet connection.

If you changed the WiFi settings and do not remember what they are, you can use a wired Ethernet connection to log in to the gateway to view the WiFi settings.

➢ **To use a wired connection to view WiFi settings:**

1. Use an Ethernet cable to connect your computer to an Ethernet LAN port on the gateway.

   The LAN LED [ ] lights.

2. Launch a web browser from the connected computer.

3. Type **http://www.routerlogin.net** or **http://10.0.0.2**.

   A login screen displays.

4. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

5. To view the WiFi settings, select **Wireless**.

   The Wireless Network screen displays.

6. To view guest network settings, select **Guest**.

   The Guest Network Settings screen displays.

WiFi Connections

If you are having trouble connecting with WiFi, try to isolate the problem, it might be due to one of the following reasons.

• The WiFi signal strength is weak.

   Check these conditions:

   - Is your gateway too far from your computer, or too close? Move your computer near the gateway, but at least 6 feet (2 meters) away, and see if the signal strength improves.

   - Is your WiFi signal blocked by objects between the gateway and your computer?

• Your computer or wireless devices does not find your WiFi network.

   Check the following:

   - Is the 2.4 GHz LED on the gateway lit?

If this LED is off, someone might have disabled the wireless radio or set up a wireless schedule. For more information about these settings, see *Control the WiFi Radio* on page 66.

- Did you disable the gateway's SSID broadcast?

    If you cleared the **Enable SSID Broadcast** check box in the Wireless Settings screen, your wireless network is hidden and does not display in your wireless client'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 *Specify Basic WiFi Settings* on page 62.

- Does your computer or wireless device support the security that you are using for your WiFi network (WEP, WPA, or WPA2)?

    For information about wireless security settings, see *Specify Basic WiFi Settings* on page 62.

- Did you set up a wireless access list in the gateway?

    If you set up an access list, you must add the MAC address for each computer and wireless device to the list. For more information about access list settings, see *Set Up a Wireless Card Access List* on page 68.

Changes Not Saved

If the gateway does not save the changes you make through the NETGEAR genie screens, do the following:

- When you log in to the gateway and change the settings on a screen, always click the **Apply** button before you move to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Troubleshoot with the LEDs

The LEDs on the front panel of the gateway indicate its status.

Apply Power to the Gateway and Check the LEDs

➢ **To apply power to the gateway and check the LEDs:**

1. Connect the power adapter cord that came with the gateway and plug it in to a power outlet.

    The Power LED lights and turns amber within a few seconds. This indicates that the self-test is running.

2. After approximately 30 seconds, verify that the LEDS are lit as follows:

- The Power LED   is lit solid green.
- The DSL Link LED is lit, indicating that a link has been established to the connected device.
- The 2.4 GHz LED   is lit solid green.

If the LEDs do not light as expected, use the LED behavior to troubleshoot the problem.

All LEDs Remain Lit

When the gateway is turned on, the LEDs light for about 10 seconds and then turn off. If all the LEDs stay lit, a fault exists within the gateway.

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

- Unplug the gateway's power adapter cord. Plug it in again and see if the gateway recovers.
- To return the gateway to its factory settings, press and hold the **Reset** button.

  For more information, see *Factory Settings* on page 114.

If the error persists, you might have a hardware problem.

Power LED Is Off or Blinking

If the Power LED   is off or blinking, try the following:

- Make sure that the power adapter cord is securely connected to your gateway and securely connected to a functioning power outlet.
- Make sure that you are using the power adapter cord that came with your product.
- If the Power LED blinks slowly and continuously, the gateway firmware is corrupted. This situation can happen if a firmware upgrade is interrupted, or if the gateway detects a problem with the firmware. If the error persists, you have a hardware problem.

Power LED Stays Amber

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

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

- Unplug the gateway's power adapter cord. Plug it in again and see if the gateway recovers.
- To return the gateway to its factory settings, press and hold the **Reset** button.

  For more information, see *Factory Settings* on page 114.

If the error persists, you might have a hardware problem.

DSL LED Is Off

If the DSL LED [ ] does not light, check the following:

- Disconnect all telephones on the line. If this action solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.
- Check that the telephone company made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper when your ADSL signal is on pins 1 and 4 of the RJ-11 jack. The gateway uses pins 2 and 3.

2.4 GHz LED Is Off

If the 2.4 GHz LED [ ] stays off, check to see if someone disabled the wireless radio or set up a wireless schedule. For more information about these settings, see *Control the WiFi Radio* on page 66. The 2.4 GHz LED is lit when the wireless radio is turned on.

LAN LED Is Off and Ethernet Devices Are Connected

If the LAN LED [ ] does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the gateway and computer.
- Make sure that power is turned on to the connected modem or computer.

Cannot Log In to the Gateway

If you cannot log in to the gateway from a computer or wireless device on your local network, do the following:

1. Make sure that your computer or wireless device is connected to the gateway's network.
   - For a WiFi connection, select the network and entered its WiFi password.
   - For a wired connection, use an Ethernet cable to connect your computer to an Ethernet LAN port on the gateway (not the Ethernet Internet port).
2. Launch a web browser and enter **www.routerlogin.net**.
3. If a login prompt does not display, try the following:
   - Close the browser and launch it again.
   - Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.

- If you are using a wired connection, check the Ethernet connection between the computer and the gateway. The LAN LEDgateway lights to show that your computer is connected.

4. If the login prompt displays, but you cannot log in, try the following:
   - Make sure that you are using the correct login information.
   - The user name is **admin** and the default password is **admin**. Make sure that Caps Lock is off when you enter this information.
   - If you customized the IP address scheme that the gateway uses, see *Troubleshoot IP Addresses* on page 111.

The Gateway Cannot Access the Internet

If you can log in to your gateway, but it cannot access the Internet, see if the gateway can obtain an IP address from your Internet service provider (ISP). Unless your Internet service provider assigned you a fixed IP address, your gateway requests an IP address from the Internet service. You can see if the request was successful using the ADVANCED Home screen.

> **Note:** The Setup Wizard can detect your Internet connection during installation, but if the gateway cannot get a WAN IP address, the Setup Wizard cannot automatically resolve this issue.

If you are attempting to set up your NETGEAR gateway as a replacement for an ADSL gateway in your network, the gateway cannot perform many gateway services. For example, the gateway cannot convert ADSL or cable data into Ethernet networking information.

➢ **To check the WAN IP address:**

1. Launch a web browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **10.0.0.2**.

   A login screen displays.
3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.
4. Click the **ADVANCED** tab.
5. In the WAN pane, check that an IP address is shown for the Internet port.

   If 0.0.0.0 is shown, your gateway has not obtained an IP address from your ISP.

For more information about the Internet connection, see *View WAN Information* on page 82.

6. If your gateway cannot obtain an IP address from the ISP, try to force your cable or DSL broadband modem to recognize your new gateway by restarting your network in this order:

   a. Unplug *and* turn off the cable or DSL broadband modem.

   b. Unplug the gateway.

   c. Plug in the cable or DSL broadband modem and turn it on.

   d. Wait two minutes.

   e. Plug in the gateway and wait two minutes.

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

- Your Internet service provider (ISP) might require a login program.

  Ask your ISP if it requires PPP over Ethernet (PPPoE) or some other type of login. If your ISP requires a login, the login name and password might be set incorrectly.

- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet Setup screen.

- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:

  - Inform your ISP that you have bought a new network device, and ask them to use the gateway's MAC address.

  - Configure your gateway to clone your computer's MAC address.

Troubleshoot Internet Browsing

If your gateway can obtain an IP address, but your computer is unable to load any web pages from the Internet, it might be for any 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 ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the gateway's configuration, reboot your computer and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

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

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

If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your gateway. If you use Internet Explorer as your browser, you might need to select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection** check box. Other browsers have similar options.

Troubleshoot a PPPoE Internet Connection

➢ **To troubleshoot a PPPoE Internet connection:**

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

2. Type **http://www.routerlogin.net** or **10.0.0.2**.

   A login screen displays.

3. Enter the gateway user name and password.

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

   The BASIC Home screen displays.

4. Click the **ADVANCED** tab.

5. On the WAN pane, click the **Connection Status** button.

   For more information, see *View WAN Information* on page 82. If the fields show valid information, including valid IP addresses, your PPPoE connection is up and working.

   If any of the fields show incomplete information or no valid IP address you can attempt to reconnect by clicking the **Connect** button. The gateway continues to attempt to connect indefinitely.

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

> **Note:** Unless you connect manually, the gateway does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Your Network Using the Ping Utility

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

Test the LAN Path to Your Gateway

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

➢ **To ping the gateway from a computer running Windows:**

1. From the Windows toolbar, click the **Start** button and select **Run**.

2. In the field provided, type **ping** followed by the IP address of the gateway, as in this example:

   ping www.routerlogin.net

3. Click the **OK** button.

   A message similar to the following 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, you might have one of the following problems:

- Wrong physical connections

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

  Check that the appropriate LEDs are on for your network devices. If your gateway and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and gateway.

- Wrong network configuration

  Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

  Verify that the IP address for your 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 verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button and select **Run**.

2. In the field provided, type

   ping -n 10 *<IP address>*

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

If the path is functioning correctly, replies like these examples shown in *Test the LAN Path to Your Gateway* on page 110 are displayed.

If you do not receive replies, try the following:

- Check that your computer has the IP address of your gateway listed as the default gateway. If a DHCP server assigns the IP configuration of your computer, this information is not visible on your computer's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway.

- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

- Check that your cable or DSL broadband modem is connected and functioning.

- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.

- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

  Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your gateway to clone or spoof the MAC address from the authorized computer.

Troubleshoot IP Addresses

By default, the gateway is set up to automatically assign IP addresses to network clients. The gateway's IP address is 10.0.0.2 unless you changed it. Wired and wirelessly connected computers must have network IP addresses on the same network as the gateway. The simplest way to meet this requirement is to configure each computer to obtain an IP address automatically using DHCP.

If you customized the IP address settings of your gateway and you're having trouble with network connections, check the following:

- Make sure that your computer's IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your computer's address is in the range of 10.0.0.3 to 10.0.0.255.

  If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the gateway and reboot your computer.

- If your gateway's IP address was changed and you do not know the current IP address, clear the gateway's configuration to factory defaults. This sets the gateway's IP address to 10.0.0.2. This procedure is explained in *Factory Settings* on page 114.

Problems with Date and Time

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

- Date shown is January 1, 2000.
  Cause. The gateway has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have completed configuring the gateway, wait at least five minutes, and check the date and time again.

- Time is off by one hour.
  Cause. The gateway does not automatically detect daylight saving time. In the Schedule screen, select the **Automatically adjust for Daylight Savings Time** check box.

Supplemental Information

A

This appendix covers the following topics:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can restore the gateway to its factory settings.

➢ **To restore factory settings:**

Use a paperclip to press and hold the **Reset** button for over seven seconds.

The gateway resets and returns to the factory configuration settings shown in the following table.

Table 1. Gateway factory default settings

Feature		Default Behavior
Gateway login	User login URL	www.routerlogin.net or http://10.0.0.2
	User name (case-sensitive)	admin
	Login password (case-sensitive)	admin
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	AutoSensing

Table 1. Gateway factory default settings (continued)

Feature		Default Behavior
Local area network (LAN)	LAN IP	10.0.0.2
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	10.0.0.3 to 10.0.0.254
	Time zone	United States is Pacific Time; otherwise, varies by region
	Time adjusted for daylight saving time	Disabled
Wireless	Wireless communication	Enabled
	SSID name	Preset. For information, see the product label.
	Security	
	Broadcast SSID	Enabled
	Transmission speed	Auto **Note:** Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
	Country/region	United States in the US; otherwise, varies by region
	RF channel	Auto
	Operating mode	
	20/40 MHz coexistence	Enabled
	Data rate	Best
	Output power	Full

Technical Specifications

The following table describes the technical specifications for the gateway.

Table 2. Technical specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	Output: 12 V @ 2.5A
Dimensions	8.5 x 4.6 x1.7 in. (215.3 x116.1 x42.7 mm) excluding external antennas
Weight	0.79 lb (360 g)
Operating temperature	0° to 40°C (32º to 104ºF)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	For regulatory compliance information, visit *http://www.netgear.com/about/regulatory*.
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the entry for Transmission speed in *Table 1* on page 114.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes)
Operating frequency range	2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI)
802.11 security	WEP, WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK mixed mode, WPA/WPA2 Enterprise