

NETGEAR®

Dual Band Wireless VDSL2 + Ethernet Gateway

Model VEGN2610-1FXAUS
User Manual



February 2016
202-11408-02

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

© NETGEAR, Inc., NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Contents

Chapter 1 Hardware Setup

Unpack Your Gateway.....	8
Front Panel	8
Rear Panel.....	10
Position Your Gateway	10
Cable Your Gateway	11

Chapter 2 Connect to the Network and Access the Gateway

Connect to the Network.....	14
Wired Connection	14
WiFi Connection	14
Types of Logins	15
Log In to the Gateway	15

Chapter 3 Internet Setup

Use the Internet Setup Wizard	17
Manually Specify an Internet Connection Without a Login	18
Manually Specify an Internet Connection with a Login.....	19
Manually Specify ADSL Settings.....	20
Specify IPv6 Internet Connections.....	21
Requirements for Entering IPv6 Addresses	22
Use Auto Detect for an IPv6 Internet Connection.....	22
Use Auto Config for an IPv6 Internet Connection.....	23
Set Up an IPv6 6to4 Tunnel Internet Connection	24
Set Up an IPv6 Pass Through Internet Connection	26
Set Up an IPv6 Fixed Internet Connection	26
Set Up an IPv6 DHCP Internet Connection.....	28
Set Up an IPv6 PPPoE Internet Connection	29
Change the MTU Size	31

Chapter 4 Control Internet Access

Use Keywords to Block Internet Sites	35
Delete Keywords from the List to Be Blocked	36
Schedule When to Block Internet Sites	36
Avoid Blocking on a Trusted Computer	38
Set Up Security Event Email Notifications.....	38
Outbound Firewall Rules.....	40
Add a Custom Service	40

Add Outbound Firewall Rules	41
Edit an Outbound Firewall Rule	43
Delete an Outbound Firewall Rule	43
Set Up Port Forwarding to a Local Server	44
Add a Custom Port Forwarding Service	45
Edit a Port Forwarding Service	46
Delete a Port Forwarding Entry	47
Application Example: Make a Local Web Server Public	47
How the Gateway Implements the Port Forwarding Rule	48
Port Triggering	48
Add a Port Triggering Service	49
Set the Port Triggering Timeout	50
Application Example: Port Triggering for Internet Relay Chat	51

Chapter 5 Share a USB Drive Attached to the Gateway

USB Drive Requirements	54
Access a USB Drive on the Network	54
Map the USB Device to a Windows Network Drive	55
Control Access to the USB Drive	56
Use FTP Within the Network	57
View or Change Network Folders on a USB Drive	58
Add a Network Folder on a USB Drive	59
Edit a Network Folder on a USB Drive	60
Approve USB Devices	61
Safely Remove a USB Drive	62
Change the Media Server Settings	63
Enable Printer Sharing on a USB Device	64

Chapter 6 Specify Network Settings

View or Change the WAN Settings	67
Default DMZ Server	68
Set Up a Default DMZ Server	69
Change the Gateway's Device Name	69
Change the LAN TCP/IP Settings	70
Specify the IP Addresses That the Gateway Assigns	71
Reserved LAN IP Addresses	73
Reserve an IP Address	73
Edit a Reserved LAN IP Address	73
Delete a Reserved LAN IP Address	74
Allow or Block Access to Your Network	75
Use the WPS Wizard for WiFi Connections	76
Specify Basic WiFi Settings	76
Change the WiFi Mbps Settings	78
Change the WiFi Password or Security Level	79
Set Up a WiFi Guest Network	80
Control the WiFi Radios	82

- Enable or Disable the WiFi Radios 82
- Set Up a Wireless Schedule 83
- Beamforming 84
 - Implicit Beamforming 84
- Specify WPS Settings 85
- Dynamic DNS 85
- Set Up Dynamic DNS 86
- View Devices Currently on the Network 87
- Custom Static Routes 88
 - Set Up a Static Route 88
 - Edit a Static Route 90
 - Delete a Static Route 90
- Improve Network Connections with Universal Plug and Play 91

Chapter 7 Manage Your Network

- View Gateway Status 94
 - View WAN Information 94
 - View WAN Statistics 95
 - View the Internet Connection Status 96
- Update the Firmware 97
- Reboot the Gateway 98
- View Logs of Gateway Activity 98
- Manage the Gateway Configuration File 99
 - Back Up the Gateway’s Configuration Settings 100
 - Restore Configuration Settings 100
 - Erase the Current Configuration Settings 101
- Change the admin Password 101
- Set Up Password Recovery for admin 102
- Recover the admin Password 103
- Look Up the IP Address for a DNS URL 104
- Display the Gateway’s Routing Table 105
- Run the Ping Utility 105
- Set Up Remote Management 106
 - Use Remote Access 108
- Monitor Internet Traffic 108

Chapter 8 Troubleshooting

- Access a Forgotten WiFi Password 112
- WiFi Connections 112
- Changes Not Saved 113
- Troubleshoot with the LEDs 113
 - Apply Power to the Gateway and Check the LEDs 113
 - All LEDs Remain Lit 114
 - WiFi LED Is Off 114
- Cannot Log In to the Gateway 114
- The Gateway Cannot Access the Internet 115
 - Troubleshoot Internet Browsing 116

Troubleshoot a PPPoE Internet Connection	117
Troubleshoot Your Network Using the Ping Utility	117
Test the LAN Path to Your Gateway	117
Test the Path from Your Computer to a Remote Device	118
Troubleshoot IP Addresses	119
Problems with Date and Time	120

Appendix A Supplemental Information

Factory Settings	122
Technical Specifications	123

Hardware Setup

1

If you have did not already set up your gateway 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.



Figure 1. Package contents

Front Panel

Status LEDs and buttons are located on the front of the gateway.

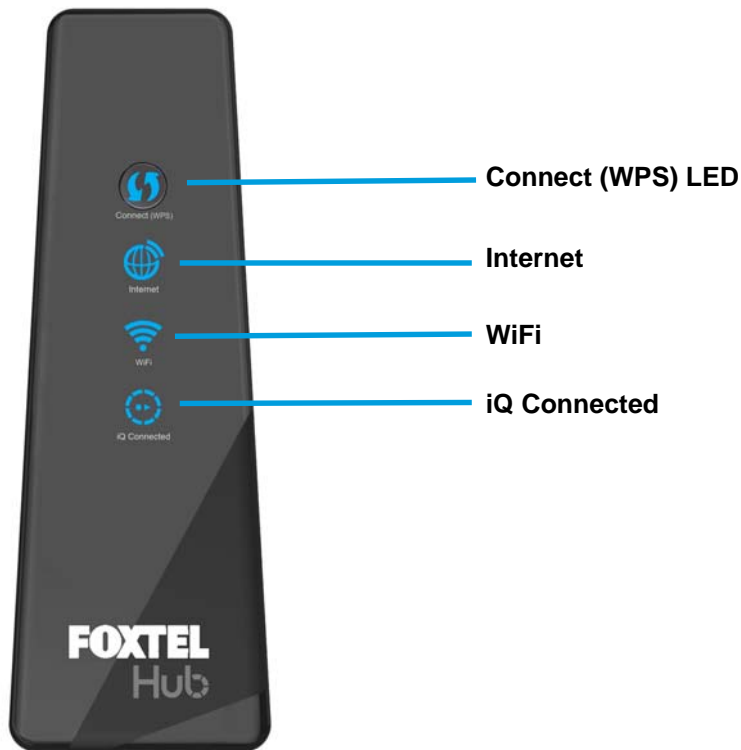






Figure 2. Gateway front view

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.

Table 1. LED and button descriptions

LEDs and Buttons	Description
Connect (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.
Internet 	<ul style="list-style-type: none"> • Solid blue. The gateway is connected to the Internet. • Solid red. PPP is in progress. • Blinking red. DSL synch is in process.
WiFi 	<ul style="list-style-type: none"> • Solid blue. The WiFi radio is on. • Off. The wireless radio is turned off and you cannot connect to the gateway with WiFi.
iQ Connected 	<ul style="list-style-type: none"> • Solid blue. STB is connected with WiFi or Ethernet. • Off. STB is not connected.

Rear Panel

The connections and button shown the following figure are located on the rear panel.

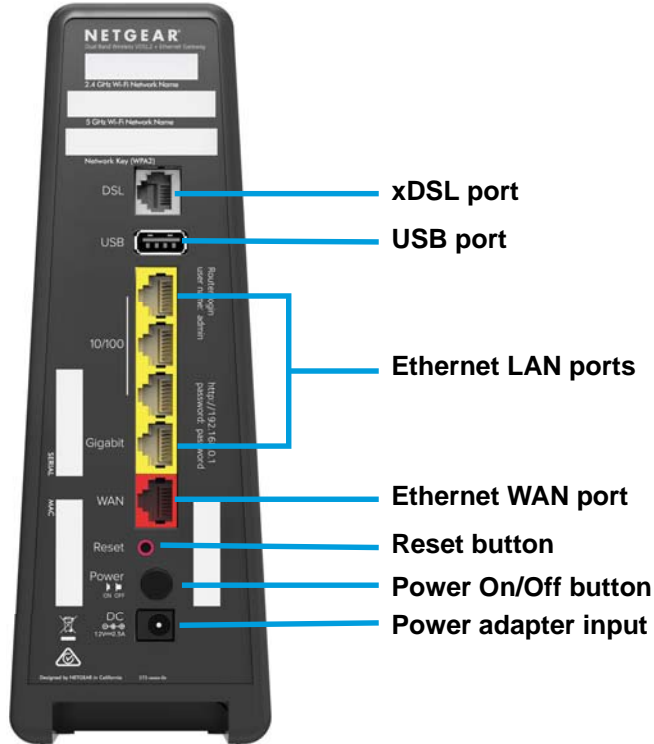


Figure 3. Gateway rear view

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, insulated walls, and items such as these:
 - Solid metal doors
 - Aluminum studs
 - Fish tanks
 - Mirrors
 - Brick
 - Concrete

Cable Your Gateway

You can use the gateway with a DSL line or an Ethernet WAN connection.

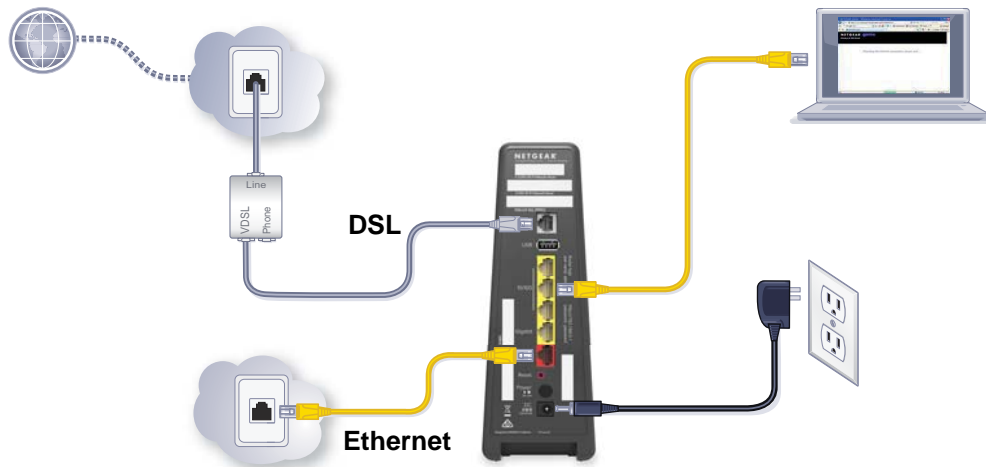


Figure 4. Gateway cabling diagram

➤ To cable your gateway:

1. Connect DSL or a cable modem.
 - For DSL, use phone cable to connect the DSL line to the gateway's xDSL port.
 - For a cable modem, unplug the modem's power. Remove the battery, if present. Then plug in the modem and put the battery back in.

Dual Band Wireless VDSL2 + Ethernet Gateway

Use an Ethernet cable to connect the modem to the gateway's red Ethernet WAN port.

2. Connect the power adapter to the gateway and plug it into an electrical outlet.
The LEDs light. If the LEDs do not light, press the **Power On/Off** button on the gateway.
3. Connect a computer to your gateway.
 - Use an Ethernet cable to connect your computer to a yellow Ethernet LAN port on the gateway.
 - For a WiFi connection, use the WiFi network name and password on the product label.

You can log in to the gateway to view or change its settings. For information about installation, see the installation guide that came in the package with the product.

2

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 power is supplied to the gateway and the WiFi 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.

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 power is supplied to the gateway and the WiFi 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 power is supplied to the gateway and the WiFi 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 serve 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 **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.

3

3. Internet Setup

Usually, the quickest way to set up the router to use your Internet connection is to allow 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*
- *Manually Specify an Internet Connection Without a Login*
- *Manually Specify an Internet Connection with a Login*
- *Manually Specify ADSL Settings*
- *Specify IPv6 Internet Connections*
- *Change the MTU Size*

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 *Manually Specify an Internet Connection Without a Login* on page 18.

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

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

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

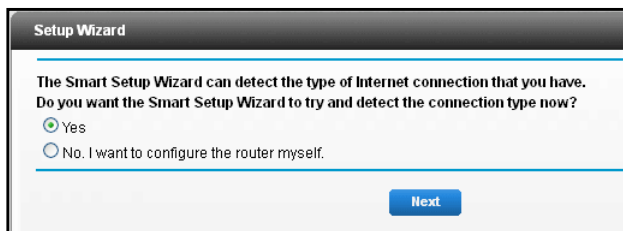
A login screen displays.

3. Enter the 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 > Setup Wizard**.



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

6. When prompted, in the **Select Country** list, select your country.

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

7. Click the **Test** button.

The Setup Wizard checks your Internet connection.

Note: If the gateway does not connect to the Internet, see *Chapter 8, Troubleshooting*, for help.

8. After the test succeeds, 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 an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

A login screen displays.

3. Enter the 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 **Internet Setup**.

5. For the Does your Internet connection require a login? setting, select the **No** radio button.
6. If your Internet connection requires an account name or host name, type it in the **Account Name (If Required)** field.
7. 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.

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

9. 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 an Internet Connection with a Login

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

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

A login screen displays.

3. Enter the 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 **Internet Setup**.

Internet Setup

Apply Cancel

Does your Internet connection require a login?

Yes
 No

Internet Service Provider: PPPoE

Login: @foxtel.net.au
Password:
Service Name (If Required):
Connection Mode: Dial on Demand
Idle Timeout (In Minutes): 0

Internet IP Address
 Get Dynamically from ISP
 Use Static IP Address:

Domain Name Server (DNS) Address
 Get Automatically from ISP
 Use These DNS Servers
Primary DNS:

Help Center Show/Hide Help Center

5. For the Does your Internet connection require a login? setting, leave the **Yes** radio button selected.
6. Complete the fields to specify your Internet connection.
For more information about the settings, see the online help.
7. Click the **Apply** button.
Your settings are saved.

Manually Specify ADSL Settings

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

➤ To specify the ADSL settings:

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

A login screen displays.

3. Enter the 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 > Setup > ADSL 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** 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 IPv6 Internet Connections

You can set up an IPv6 Internet connection if genie does not detect it automatically.

➤ To set up an IPv6 Internet connection:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
3. Enter the 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 > IPv6**.
The Basic Settings screen displays.
5. In the **Internet Connection Type** list, select the IPv6 connection type:
 - If your ISP did not provide details, select **IPv6 Tunnel**.
 - If you are not sure, select **Auto Detect** so that the gateway detects the IPv6 type that is in use.
 - If your Internet connection does not use PPPoE or DHCP, or not fixed, but is IPv6, select **Auto Config**.

Your Internet service provider (ISP) can provide this information.
6. Click the **Apply** button.
Your changes take effect.

Requirements for Entering IPv6 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. You can reduce any four-digit group of zeros within an IPv6 address to a single zero or omit it. The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Use Auto Detect for an IPv6 Internet Connection

➤ **To set up an IPv6 Internet connection through auto detection:**

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

A login screen displays.

3. Enter the 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 > IPv6**.

The IPv6 screen displays.

5. In the **Internet Connection Type** list, select **Auto Detect**.

6. Click the **Apply** button.

The screen adjusts.

The gateway automatically detects the information in the following fields:

- **Connection Type.** This field indicates the connection type that is detected.
 - **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the gateway's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the gateway's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
7. Select an IP Address Assignment radio button.
 - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.

- **Auto Config.** This is the default setting.

This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).

8. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the gateway's LAN interface.

If you do not specify an ID here, the gateway generates one automatically from its MAC address.

9. Click the **Apply** button.

Your settings are saved.

Use Auto Config for an IPv6 Internet Connection

- **To set up an IPv6 Internet connection through auto configuration:**

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

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

A login screen displays.

3. Enter the gateway user name and password.

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

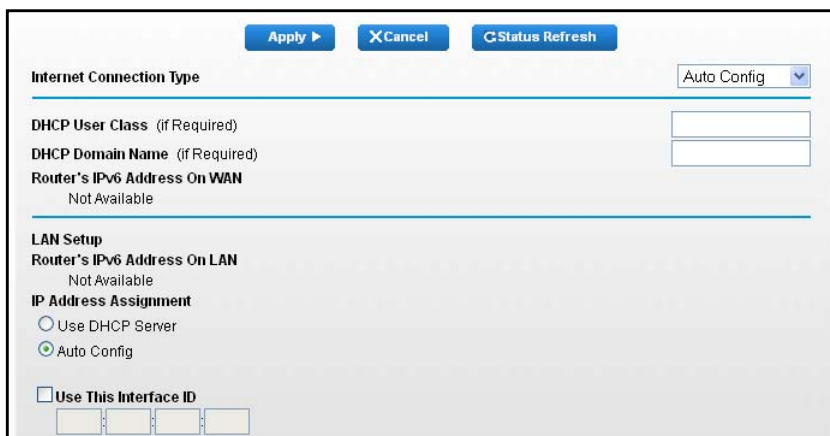
The BASIC Home screen displays.

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

The IPv6 screen displays.

5. In the **Internet Connection Type** list, select **Auto Config**.

The screen adjusts:



The screenshot shows a web interface for IPv6 configuration. At the top, there are three buttons: 'Apply' (with a right arrow), 'Cancel' (with an X), and 'Status Refresh' (with a circular arrow). Below these is a section titled 'Internet Connection Type' with a dropdown menu set to 'Auto Config'. Underneath are three input fields: 'DHCP User Class (if Required)', 'DHCP Domain Name (if Required)', and 'Router's IPv6 Address On WAN' (with the text 'Not Available' below it). A horizontal line separates this from the 'LAN Setup' section. Under 'LAN Setup', there are two more input fields: 'Router's IPv6 Address On LAN' (with 'Not Available' below it) and 'IP Address Assignment'. The 'IP Address Assignment' section has two radio buttons: 'Use DHCP Server' (unselected) and 'Auto Config' (selected). At the bottom, there is a checkbox labeled 'Use This Interface ID' which is unchecked, followed by four small input boxes for an interface ID.

The gateway automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the gateway's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the gateway's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
6. (Optional) In the **DHCP User Class (If Required)** field, enter a host name.
- Most people can leave this field blank, but if your ISP has given you a specific host name, enter it here.
7. (Optional) In the **DHCP Domain Name (If Required)** field, enter a domain name.
- You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.
8. Select an IP Address Assignment radio button.
- **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** This is the default setting.
- This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).
9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the gateway's LAN interface.
- If you do not specify an ID here, the gateway generates one automatically from its MAC address.
10. Click the **Apply** button.
- Your settings are saved.

Set Up an IPv6 6to4 Tunnel Internet Connection

The remote relay gateway is the gateway to which your gateway creates a 6to4 tunnel. Make sure that the IPv4 Internet connection is working before you apply the 6to4 tunnel settings for the IPv6 connection.

- **To set up an IPv6 Internet connection by using a 6to4 tunnel:**
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
 2. Type <http://www.routerlogin.net> or <http://www.routerlogin.com>.
- A login screen displays.

3. Enter the 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 > IPv6**.

The IPv6 screen displays.

5. In the **Internet Connection Type** list, select **6to4 Tunnel**.

The screen adjusts:

The screenshot shows the IPv6 configuration interface. At the top, there are three buttons: 'Apply', 'Cancel', and 'Status Refresh'. Below them, the 'Internet Connection Type' is set to '6to4 Tunnel'. The 'Remote 6to4 Relay Router' section has two radio buttons: 'Auto' (selected) and 'Static IP Address' (with an empty IP address field). The 'LAN Setup' section includes 'Router's IPv6 Address On LAN' (displaying 'Not Available'), 'IP Address Assignment' with 'Auto Config' selected, and a 'Use This Interface ID' checkbox (unchecked) with an empty field.

The gateway automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the gateway's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select a Remote 6to4 Relay Router radio button:
 - **Auto**. Your gateway uses any remote relay gateway that is available on the Internet. This is the default setting.
 - **Static IP Address**. Enter the static IPv4 address of the remote relay gateway. Your IPv6 ISP usually provides this address.
7. Select an IP Address Assignment radio button.
 - **Use DHCP Server**. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config**. This is the default setting.

This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).

8. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the gateway's LAN interface.

If you do not specify an ID here, the gateway generates one automatically from its MAC address.

9. Click the **Apply** button.

Your settings are saved.

Set Up an IPv6 Pass Through Internet Connection

In pass-through mode, the gateway works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The gateway does not process any IPv6 header packets.

➤ **To set up a pass-through IPv6 Internet connection:**

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

A login screen displays.

3. Enter the 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 > IPv6**.

The IPv6 screen displays.

5. In the **Internet Connection Type** list, select **Pass Through**.

The screen adjusts, but no additional fields display.

6. Click the **Apply** button.

Your settings are saved.

Set Up an IPv6 Fixed Internet Connection

➤ **To set up a fixed IPv6 Internet connection:**

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

A login screen displays.

3. Enter the 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 > IPv6**.

The IPv6 screen displays.

- In the **Internet Connection Type** list, select **Fixed**.

The screen adjusts:

The screenshot shows the 'Basic Settings' window for IPv6 configuration. At the top, there are 'Apply' and 'Cancel' buttons. The 'Internet Connection Type' is set to 'Fixed'. Below this, the 'WAN Setup' section contains four rows of input fields: 'IPv6 Address:Prefix Length', 'Default IPv6 Gateway', 'Primary DNS', and 'Secondary DNS'. Each row has eight input boxes. The 'LAN Setup' section is below, with 'IP Address Assignment' options: 'Use DHCP Server' (unselected) and 'Auto Config' (selected). Below that is another 'IPv6 Address:Prefix Length' row with eight input boxes.

- Configure the fixed IPv6 addresses for the WAN connection:
 - IPv6 Address/Prefix Length.** The IPv6 address and prefix length of the gateway WAN interface.
 - Default IPv6 Gateway.** The IPv6 address of the default IPv6 gateway for the gateway's WAN interface.
 - Primary DNS Server.** The primary DNS server that resolves IPv6 domain name records for the gateway.
 - Secondary DNS Server.** The secondary DNS server that resolves IPv6 domain name records for the gateway.

Note: If you do not specify the DNS servers, the gateway uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup screen. (See *Manually Specify an Internet Connection Without a Login* on page 18.)

- Select an IP Address Assignment radio button.
 - Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
 - Auto Config.** This is the default setting.

This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).

- In the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the gateway's LAN interface.

If you do not specify an ID here, the gateway generates one automatically from its MAC address.

9. Click the **Apply** button.

Your settings are saved.

Set Up an IPv6 DHCP Internet Connection

- **To set up an IPv6 Internet connection with a DHCP server:**

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

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

A login screen displays.

3. Enter the 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 > IPv6**.

The IPv6 screen displays.

5. In the **Internet Connection Type** list, select **DHCP**.

The screen adjusts:

The screenshot shows the 'Basic Settings' window for IPv6 configuration. At the top, there are three buttons: 'Apply', 'Cancel', and 'Status Refresh'. Below these, the 'Internet Connection Type' is set to 'DHCP' in a dropdown menu. There are two empty input fields for 'User Class (if Required)' and 'Domain Name (if Required)'. The 'Router's IPv6 Address On WAN' field displays 'Not Available'. The 'LAN Setup' section shows 'Router's IPv6 Address On LAN' as 'Not Available'. Under 'IP Address Assignment', the 'Auto Config' radio button is selected, while 'Use DHCP Server' is unselected. At the bottom, there is a checkbox for 'Use This Interface ID' which is also unselected, followed by four empty input boxes for the interface ID.

The gateway automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the gateway's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the gateway's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
6. (Optional) In the **User Class (If Required)** field, enter a host name.
Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.
 7. (Optional) In the **Domain Name (If Required)** field, enter a domain name.
You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.
 8. Select an IP Address Assignment radio button.
 - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** This is the default setting.This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).
 9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the gateway's LAN interface.
If you do not specify an ID here, the gateway generates one automatically from its MAC address.
 10. Click the **Apply** button.
Your settings are saved.

Set Up an IPv6 PPPoE Internet Connection

- **To set up a PPPoE IPv6 Internet connection:**
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
 2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.
A login screen displays.
 3. Enter the 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 > IPv6**.

The IPv6 screen displays.

- In the **Internet Connection Type** list, select **PPPoE**.

The screen adjusts:

The gateway automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the gateway's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the gateway's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
- In the **Login** field, enter the login information for the ISP connection.

This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

- In the **Password** field, enter the password for the ISP connection.
- In the **Service Name** field, enter a service name.

If your ISP did not provide a service name, leave this field blank.

Note: The default setting of the **Connection Mode** list is **Always On** to provide a steady IPv6 connection. The gateway never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the gateway attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

9. Select an IP Address Assignment radio button.
 - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
 - **Auto Config.** This is the default setting.

This setting specifies how the gateway assigns IPv6 addresses to the devices on your home network (the LAN).

10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the gateway's LAN interface.

If you do not specify an ID here, the gateway generates one automatically from its MAC address.

11. Click the **Apply** button.

Your settings are saved.

Change the MTU Size

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

The best MTU setting for NETGEAR equipment is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You experience problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
 - A secure website that does not open, or displays only part of a web page
 - Yahoo email
 - MSN portal
 - America Online's DSL service
- You use VPN and are experiencing severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you are experiencing connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

➤ **To change the MTU size:**

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

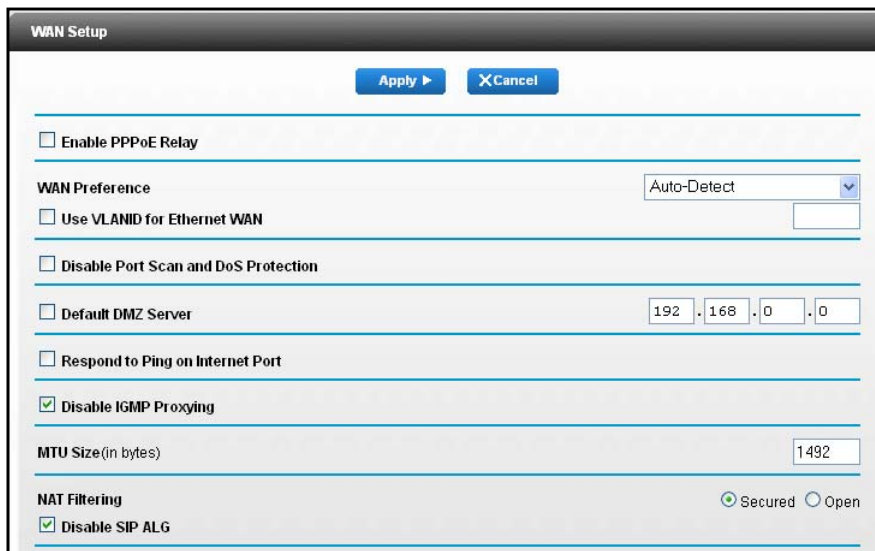
A login screen displays.

3. Enter the 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 > Setup > WAN Setup**.



5. In the **MTU Size** field, enter a value from 64 to 1500.
6. Click the **Apply** button.

Your change is saved.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR gateways, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)

Table 2. Common MTU sizes (continued)

MTU	Application
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not send or receive large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

4 Control Internet Access

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 Port Forwarding to a Local Server*
- *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 **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 > Security > Block Sites**.

5. Select a keyword blocking option:

- **Per Schedule.** Use keyword blocking according to a schedule that you set. (See [Schedule When to Block Internet Sites](#) on page 36.)
- **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. Click 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 **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 > Security > Block Sites**.
The Block Sites screen displays.
 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 the **Apply** button.
Your changes are saved.

Schedule When to Block Internet Sites

For information about how to specify what you want the gateway to block, see [Use Keywords to Block Internet Sites](#) on page 35.

- **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 **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 > Security > Schedule**.

The screenshot shows the 'Schedule' configuration page. At the top, there are 'Apply' and 'Cancel' buttons. Below them, the 'Days to Block' section has a list of days with checkboxes: 'Every Day' (checked), 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday'. The 'Time of day to block' section has a sub-section 'Time of day to block:(use 24-hour clock)' with an 'All Day' checkbox (checked). Below this are 'Start Blocking' and 'End Blocking' fields, each with 'Hour' and 'Minute' spinners. The 'Start Blocking' field shows '0' for hours and '0' for minutes. The 'End Blocking' field shows '24' for hours and '0' for minutes. The 'Time Zone' section has a dropdown menu showing '(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London' and a checked 'Automatically adjust for daylight savings time' checkbox. At the bottom, it displays 'Current Time: Wednesday, 01 Jan 2003 00:21:15'.

5. Specify when to block keywords:
 - **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 73.

➤ **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 **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 > Security > Block Sites**.

The Block Sites screen displays.

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

The screenshot shows a configuration section with a checkbox labeled "Allow trusted IP address to visit blocked sites" which is currently unchecked. Below the checkbox is a label "Trusted IP Address" followed by four input fields containing the IP address "10.0.0.0".

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 **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 > 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. In the **Send to This E-mail Address** field, enter the email address to which logs and alerts are sent.

This email address is also used for the From address. If 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** list, select the schedule type.
 - From the **Day** list, select the day.
 - From the **Time** 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, 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 Port Forwarding to a Local Server* on page 44.

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 **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 > Security > Firewall Rules**.

The Firewall Rules screen displays.

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

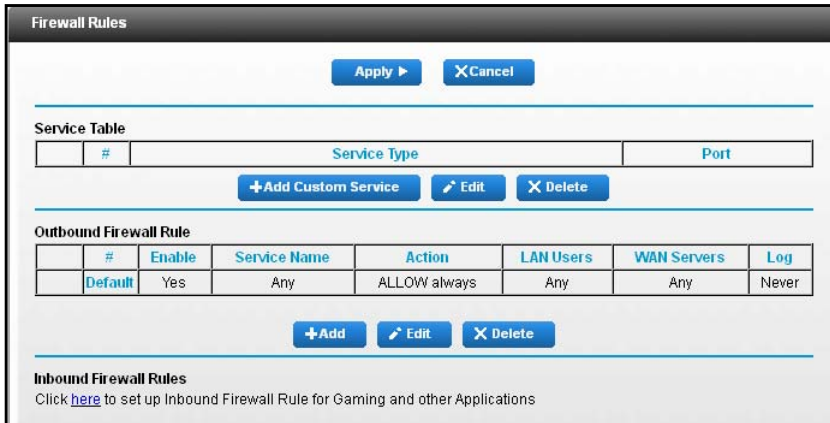
By default, the gateway allows all communication from your network out to the Internet. You can add rules to restrict outbound Internet traffic.

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 **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 > Security > Firewall Rules**.



If you did not define 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 address or addresses.

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

10. To log instances of when this rule is used, in the **Log** list, 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 **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 > Security > Firewall Rules**.
The Firewall Rules screen displays.
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 **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 > Security > Firewall Rules**.
The Firewall Rules screen displays.

The table under Outbound Services lists all existing rules for outbound traffic. If you did not define 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 Port Forwarding to a Local Server

If your home network includes a server, 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 73.

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

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**.

Port Forwarding / Port Triggering

+Add Custom Service Apply Cancel

Please select the service type.

Port Forwarding
 Port Triggering

Inbound Firewall Rules

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

+Add Edit Delete

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

8. In the **Service Name** list, select the service name.

If the service that you want to add is not in the list, create a custom service. See [Add a Custom Port Forwarding Service](#) on page 45.

9. Click the **Add** button.

The service displays in the list.

Add a Custom Port Forwarding Service

➤ To add a custom service:

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

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

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

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

A login screen displays.

4. 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.

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

The Port Forwarding/Port Triggering screen displays.

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

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

- In the **Name** field, enter a descriptive name.
- In the **Type** field, select the protocol.
If you are unsure, select **TCP/UDP**.
- In the **Start Port** field, enter the beginning port number.
If the application uses a single port, enter the same port number in the **End Port** field.
If the application uses a range of ports, enter the ending port number of the range in the **Finish Port** field.
- Type the IP address in the **Internal IP address** field or select the radio button for an attached device listed in the table.
- Click the **Apply** button.
The service is now in the list on the Port Forwarding/Port Triggering screen.

Edit a Port Forwarding Service

➤ To edit a port forwarding entry:

- Launch a web browser from a computer or wireless device that is connected to the network.
- Type **http://routerlogin.net** or **www.routerlogin.com**.
A login screen displays.
- 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.
- Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
The Port Forwarding/Port Triggering screen displays.
- Leave the **Port Forwarding** radio button selected as the service type.
- In the table, select the radio button next to the service name.
- Click the **Edit Service** button.

The Ports - Custom Services screen displays.

8. Specify changes as needed.
9. Click the **Apply** button.

Your changes are saved.

Delete a Port Forwarding Entry

➤ To delete a port forwarding entry:

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

The Port Forwarding/Port Triggering screen displays.

5. Select the **Port Forwarding** radio button as the service type.
6. In the table, select the radio button next to the service name.
7. Click the **Delete Service** button.

The service is deleted.

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 192.168.0.33.

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 **192.168.0.33**.

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

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

For more information, see *Dynamic DNS* on page 85.

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 `192.168.0.223` and sends the message to that computer.
4. Your web server at IP address `192.168.0.223` 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 91.

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 **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 > Port Forwarding/Port Triggering**.

The Port Forwarding/Port Triggering screen displays.

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

Port Forwarding / Port Triggering

Apply Cancel

Please select the service type.

Port Forwarding

Port Triggering

Disable Port Triggering

Port Triggering Time-out (in minutes) 20

Port Triggering Portmap Table

#	Enable	Service Name	Service Type	Inbound Connection	Service User

+Add Service Edit Service X Delete Service

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 [Set the Port Triggering Timeout](#) on page 50.

Set the Port Triggering Timeout

➤ To enable port triggering:

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

The Port Forwarding/Port Triggering screen displays.

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.
8. 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.

5 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*
- *Enable Printer Sharing on a USB Device*

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:

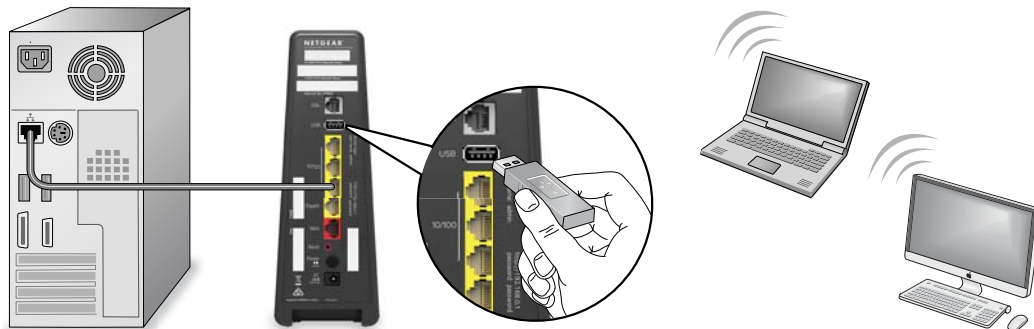
- FAT16
- FAT32
- NTFS
- NTFS with compression format enabled
- Ext2
- Ext3
- Ext4
- XFS
- HFS
- HFS+

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 uses 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.



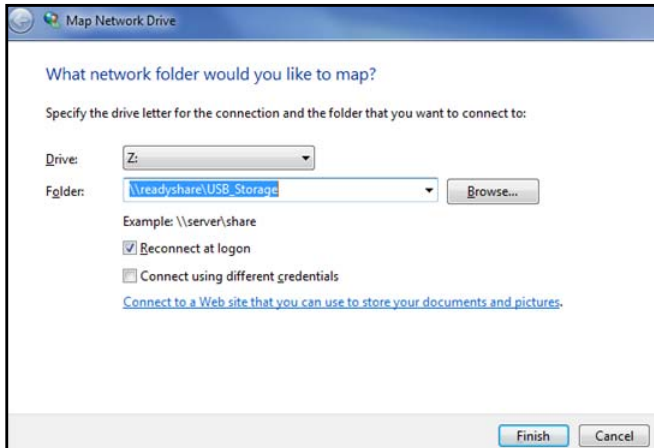
If your USB drive uses a power supply, you must use it when you connect the USB drive to the gateway.

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 and do the following:
 - a. Type the user name and password.
 - b. Click the **OK** button.
6. Click the **Finish** button.
The USB drive is mapped to the drive letter that you specified.

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 **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 > USB Storage > Advanced Settings**.

The screenshot shows the 'USB Storage (Advanced Settings)' page. At the top, there are 'Apply' and 'Refresh' buttons. Below are input fields for 'Network Device Name' (containing 'readyshare') and 'Workgroup' (containing 'Workgroup').

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readyshare	-
<input checked="" type="checkbox"/>	HTTP	http://readyshare.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readyshare.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via internet)	ftp://0.0.0.0/shares	21

Below the table is the 'Available Network Folders' section:

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input checked="" type="radio"/>	\\readyshare\	All - no password	All - no password		TRAVELDRIVE	978.8M	172.8M

At the bottom of the folder list are buttons for 'Edit', 'Create Network Folder', and 'Delete'. Below that is a 'Safely Remove USB Device' button. The footer contains 'Help Center' and 'Show/Hide Help Center'.

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 **www.routerlogin.com**.
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 > USB Storage > Advanced Settings**.

USB Storage (Advanced Settings)

Apply Refresh

Network Device Name : readyshare

Workgroup : Workgroup

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readyshare	-
<input checked="" type="checkbox"/>	HTTP	http://readyshare.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via Internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readyshare.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via Internet)	ftp://0.0.0.0/shares	21

Available Network Folders

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input checked="" type="checkbox"/>	\\readyshare\	All - no password	All - no password		TRAVELDRIVE	978.8M	172.8M

Edit Create Network Folder Delete

Safely Remove USB Device

Help Center Show/Hide Help Center

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 **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 > USB Storage > Advanced Settings**.

USB Storage (Advanced Settings)

Apply Refresh

Network/Device Name : readyshare

Workgroup : Workgroup

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readyshare	-
<input checked="" type="checkbox"/>	HTTP	http://readyshare.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readyshare.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via internet)	ftp://0.0.0.0/shares	21

Available Network Folders

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input checked="" type="checkbox"/>	\\readyshare\	All - no password	All - no password		TRAVELDRIVE	978.8M	172.8M

Edit Create Network Folder Delete

Safely Remove USB Device

Help Center Show/Hide Help Center

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 include 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, someone deleted the default share, 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 **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 > ReadySHARE**.
The Advanced ReadySHARE screen displays.
5. Click the **Create Network Folder** button.

Create Network Folder	
USB Device	<input type="button" value="v"/>
Folder	<input type="text"/> <input type="button" value="Browse"/>
Share Name	<input type="text"/>
Read Access	<input type="button" value="All - no password v"/>
Write Access	<input type="button" value="All - no password v"/>
<input type="button" value="Apply"/>	
<input type="button" value="Close Window"/>	

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 **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 > ReadySHARE**.
The Advanced ReadySHARE screen 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 **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 > 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.

Approved USB Devices			
	Volume Name	Device Name	Capacity

Available USB Devices			
	Volume Name	Device Name	Capacity
<input checked="" type="radio"/>	TRAVELDRIVE	Memorex TRAVELDRIVE 005B	978MB

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 **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 **USB Storage > Basic Settings**.
The USB Basic Settings screen displays.
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 **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 > 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.

Enable Printer Sharing on a USB Device

➤ To enable printer sharing:

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

5. Select the Enable the USB port **Yes** radio button to share a compatible printer on the Network.

6. Click the **Configure** button.

The gateway checks to see if a compatible USB printer is connected and displays its status (Online or Offline).

7. Click the **Apply** button.

Your settings are saved.

6 Specify Network Settings

This chapter includes the following sections:

- *View or Change the WAN Settings*
- *Default DMZ Server*
- *Change the Gateway's Device Name*
- *Change the LAN TCP/IP Settings*
- *Specify the IP Addresses That the Gateway Assigns*
- *Reserved LAN IP Addresses*
- *Allow or Block Access to Your Network*
- *Use the WPS Wizard for WiFi Connections*
- *Specify Basic WiFi Settings*
- *Beamforming*
- *Change the WiFi Password or Security Level*
- *Set Up a WiFi Guest Network*
- *Control the WiFi Radios*
- *Set Up a Wireless Schedule*
- *Specify WPS Settings*
- *Dynamic DNS*
- *Set Up Dynamic DNS*
- *View Devices Currently on the Network*
- *Custom Static Routes*
- *Improve Network Connections with Universal Plug and Play*

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 www.routerlogin.com.

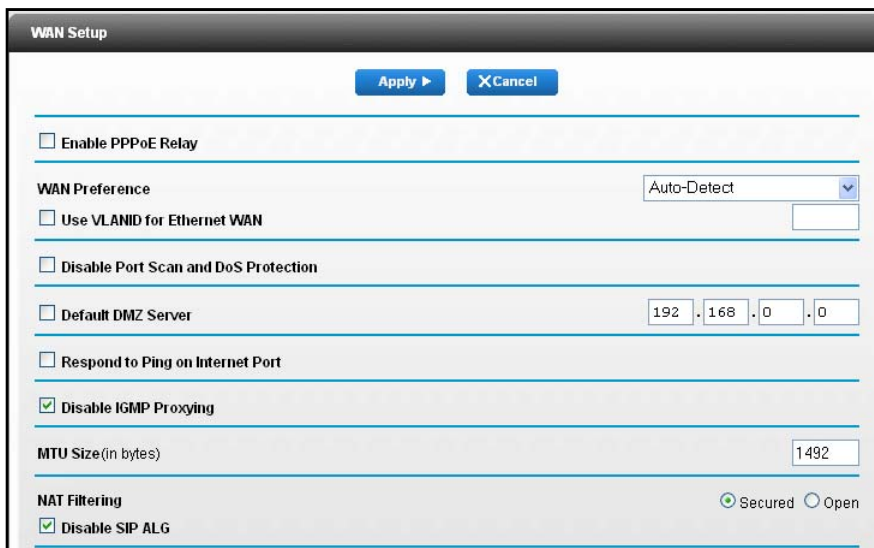
A login screen displays.

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 > Setup > WAN Setup**.



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

- Enable PPPoE Relay
- WAN Preference**: Auto-Detect (dropdown menu)
- Use VLANID for Ethernet WAN
- Disable Port Scan and DoS Protection
- Default DMZ Server: 192 . 168 . 0 . 0
- Respond to Ping on Internet Port
- Disable IGMP Proxying
- MTU Size (in bytes)**: 1492
- NAT Filtering**: Secured Open
- Disable SIP ALG

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 select **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 68.
 - **Respond to Ping on Internet Port.** This feature allows your gateway to be discovered. Use this feature only as a diagnostic tool or for 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 68.
 - **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.
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 configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can specify that the gateway forwards 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 **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 > Setup > WAN Setup**.
The WAN Setup screen displays.
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 VEGN2610-1FXAUS. 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 **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 > Setup > LAN Setup**.

LAN Setup

Apply Cancel

Device Name VEGN2610

LAN TCP/IP Setup

IP Address 192 . 168 . 0 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction Both

RIP Version Disabled

Use Router as DHCP Server

Starting IP Address 192 . 168 . 0 . 2

Ending IP Address 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

+Add Edit Delete

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.** 192.168.0.1
- **Subnet mask.** 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network 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 competing subnets use 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 **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 > Setup > LAN Setup**.

The screenshot shows the LAN Setup configuration interface. At the top, there are 'Apply' and 'Cancel' buttons. Below that is a 'Device Name' field with the value 'VEGN2610'. The 'LAN TCP/IP Setup' section contains several fields: 'IP Address' (192.168.0.1), 'IP Subnet Mask' (255.255.255.0), 'RIP Direction' (Both), and 'RIP Version' (Disabled). There is a checked box for 'Use Router as DHCP Server'. Below this, 'Starting IP Address' is set to 192.168.0.2 and 'Ending IP Address' is set to 192.168.0.254. At the bottom, there is an 'Address Reservation' table with columns for '#', 'IP Address', 'Device Name', and 'MAC Address', and buttons for '+Add', 'Edit', and 'Delete'.

5. 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 198.168.0.2 and 192.168.0.254, 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 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 **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 > 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 **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 > Setup > LAN Setup**.

The LAN Setup screen displays.

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 192.068.0.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. Click the **Apply** button.

The reserved address is entered into the table.

The reserved address is not assigned until the next time the computer contacts the 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 **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 > Setup > LAN Setup**.

The LAN Setup screen displays.

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 **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 > Setup > LAN Setup**.

The LAN Setup screen displays.

5. Select the radio button next to the reserved address.
6. Click the **Delete** button.

The address is removed.

Allow or Block Access to Your Network

You can use access control to block access to your network.

➤ **To set up access control:**

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

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

A login screen displays.

3. Enter the router user name and password.

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

The BASIC Home screen displays.

4. Select **Advanced > Security > Access Control**.

The Access Control screen displays.

5. Select the **Turn on Access Control** check box.

You must select this check box before you can specify an access rule and use the **Allow** and **Block** buttons. When this check box is cleared, all devices are allowed to connect, even if the device is in the blocked list.

6. Select an access rule:

- **Allow all new devices to connect.** With this setting, if you buy a new device, it can access your network. You don't need to enter its MAC address in this screen. Best practice is to leave this radio button selected.
- **Block all new devices from connecting.** With this setting, if you buy a new device, before it can access your network, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list.

The access rule does not affect previously blocked or allowed devices. It applies only to devices joining your network in the future after you apply these settings.

7. To allow the computer or device you're currently using to continue to access the network, select the check box next to your computer or device, and click the **Allow** button.

8. Click the **Apply** button.

Your changes take effect.

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 **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 > WPS Wizard**.

A note displays that explains WPS.

5. Click the **Next** button.

The WPS screen displays.

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 **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 **Wireless**.

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

In some locations, you cannot change this setting.

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

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

7. 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 label. If you change the name, make sure to write down the new name and keep it in a safe place.

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. Best practice is to use channel spacing between adjacent access points of four channels (for example, use Channels 1 and 5, or 6 and 10).

Change the WiFi Mbps Settings

The data rate for high-speed transmissions is commonly identified as megabits per second (Mbps). By default, the router is set to operate with up to 600 Mbps in the 2.4 GHz WiFi band and up to 1,300 Mbps in the two 5 GHz WiFi bands. You can select slower settings if you want.

9. 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.

➤ To change the WiFi Mbps settings:

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

A login screen displays.

3. Enter the router user name and password.

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

The BASIC Home screen displays.

4. Select **Wireless**.

5. For the 2.4 GHz WiFi band, in the Wireless Network (2.4 GHz b/gn/n) section of the screen, select a setting in the **Mode** list.

- **300-Mbps.** 802.11n devices can connect at this speed. This is the default setting.
- **Up to 145 Mbps.** 802.11n and 802.11g wireless devices can join the network.
- **g & b.** This supports up to 54 Mbps.

6. 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.

Change the WiFi Password or Security Level

Your router comes with preset WPA2 or WPA security. The password that you enter to connect to your network is unique to your router and is on the router label. To protect your network from unwanted access, do not to disable security.

➤ **To change the WPA settings:**

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

A login screen displays.

3. Enter the router user name and password.

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

The BASIC Home screen displays.

4. Select **Wireless**.

The Wireless Settings screen displays.

5. Under **Security Options**, select a radio button for one of the following WPA options:

- **WPA2-PSK [AES]**
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**
- **WPA/WPA2 Enterprise**

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

The **Passphrase** field displays.

6. In the **Passphrase** field, enter the network key (password).

It is a text string from 8 to 63 characters.

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

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 **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 **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 can access your local network, not just the Internet.
- **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 Radios

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

You can enable or disable the wireless radios and you can set up a WiFi schedule.

Enable or Disable the WiFi Radios

➤ **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 **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 > Wireless Settings**.

Wireless Settings

Apply Cancel

Advanced Wireless Settings (2.4GHz b/g/n)

Enable Wireless Router Radio

Enable 20/40 MHz Coexistence

Fragmentation Length (256-2346): 2346

CTS/RTS Threshold (1-2347): 2347

Preamble Mode: Long Preamble

Turn off wireless signal by schedule

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

Period	Start	End	Recurrence Pattern
+ Add a new period Edit Delete			

Advanced Wireless Settings (5GHz a/n/ac)

Enable Wireless Router Radio

Enable 20/40 MHz Coexistence

Fragmentation Length (256-2346): 2346

CTS/RTS Threshold (1-2347): 2347

Preamble Mode: Long Preamble

Turn off wireless signal by schedule

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

Period	Start	End	Recurrence Pattern
+ Add a new period Edit Delete			

Help Center Show/Hide Help Center

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 WiFi LED turns off. If you enabled the wireless radio, the WiFi LED lights.

Set Up a Wireless Schedule

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

➤ To set up the wireless schedule:

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

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

A login screen displays.

3. Enter the router user name and password.

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

The BASIC Home screen displays.

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

The Advanced Wireless Settings screen displays.

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

6. Use the lists, radio buttons, and check boxes to set up a period during which you want to turn off the wireless signal.

7. Click the **Apply** button.

The Advanced Wireless Settings screen displays.

8. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
9. Click the **Apply** button.

Your settings are saved.

Beamforming

Beamforming means that your gateway actively tracks clients and directs WiFi to the client, rather than just blasting it out in all directions. This means better WiFi range and performance for your WiFi devices.

The gateway uses explicit and implicit beamforming to improve WiFi performance. Explicit beamforming requires the client to support beamforming. Typically 802.11ac clients support beamforming. Implicit beamforming means that the gateway can support beamforming even with clients that do not support beamforming. This gateway supports implicit beamforming for both 2.4 and 5 GHz clients, which means that it will provide beamforming benefits of better range and performance for all WiFi devices, even older 802.11a/b/g/n, not just the latest WiFi clients.

Implicit Beamforming

Implicit beamforming means that the router can use information from client devices that support beamforming to improve the WiFi signal. This feature is enabled by default, but you can disable it.

➤ To disable implicit beamforming:

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 router user name and password.

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

The BASIC Home screen displays.

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

The Advanced Wireless Settings screen displays.

5. Scroll down below the WPS Settings section and clear the **Enable Implicit BEAMFORMING** check box.

6. Click the **Apply** button.

Your settings are saved.

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 **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 > Wireless Settings**.

The Advanced Wireless Settings screen displays.

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.

Dynamic DNS

If your Internet service provider gave you a permanently assigned IP address, you can register a domain name and use a public Domain Name Service (DNS) that links that name with your IP address. 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 as 10.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 www.routerlogin.com.

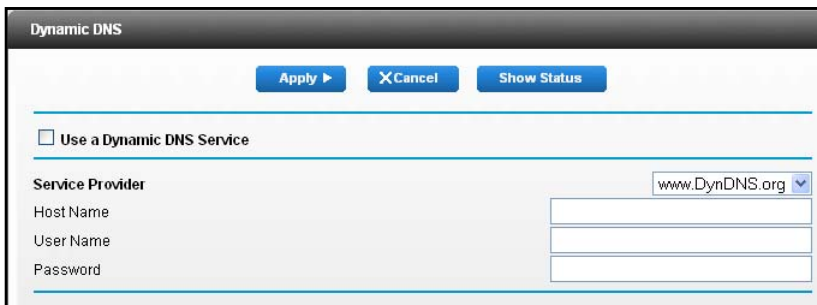
A login screen displays.

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 > 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.

For example, if your Dynamic DNS service provider is DynDNS.org, select **www.DynDNS.org**.

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 **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 **Attached Devices**.

Attached Devices			
Go to Access Control to allow or block devices.			
Access Control: Turned Off Refresh			
Wired Devices			
Device Name	IP Address	MAC Address	Connection Type
TECHPUBS	192.168.0.2	00:1A:6B:8D:8F:19	Wired
Wireless Devices (Wireless intruders also show up here)			
Device Name	IP Address	MAC Address	Connection Type

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:

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

- **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.
- **Connection Type.** The method used to access to the gateway, wired or wireless.

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

Custom Static Routes

Static routes provide routing information to your gateway. In most situations, you don't need to create custom 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.
- Your home network includes an ISDN gateway for connecting to the company where you are employed. This gateway's address on your LAN is 192.168.0.100.
- 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 192.168.0.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 192.168.0.100. 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 is forwarded to the ISDN gateway at 192.168.0.100.
- 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 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. 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** check box, 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 **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 > UPnP**.

Active	Protocol	Int. Port	Ext. Port	IP Address

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 receive 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 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.

7 Manage Your Network

7

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 **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. Click the **Advanced** tab.

The screenshot shows the 'Advanced' tab of the gateway status page. It is divided into four sections:

- Router Information:** Hardware Version (VEGN2610), Firmware Version (V1.0.0.8_1.0.8_Test), GUI Language Version (V1.0.0.7_3.1.2.5), LAN Port, MAC Address (00:00:00:00:00:01), IP Address (192.168.0.1), DHCP (On), and a Reboot button.
- WAN:** MAC Address (00:00:00:00:00:02), IP Address (172.16.2.5), Connection (PPPoE), IP Subnet Mask (255.255.255.255), and Domain Name Server (172.16.2.3, 172.16.2.4). It includes Show Statistics and Connection Status buttons.
- Wireless Settings (2.4GHz):** Name (SSID) (FoxtelHub0001), Region (Australia), Channel (Auto (1)), Mode (Up to 300 Mbps), Wireless AP (On), Broadcast Name (On), Wireless isolation, and Wi-Fi Protected Setup (Configured).
- Wireless Settings (5GHz):** Name (SSID) (FoxtelHubMedia0001), Region (Australia), Channel (36 + 40 + 44(P) + 48), Mode (Up to 1200 Mbps), Wireless AP (On), Broadcast Name (On), Wireless isolation, and Wi-Fi Protected Setup (Configured).

Scroll to view more

View WAN Information

➤ To view gateway WAN information:

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

The WAN pane displays 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 **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. Click the **Advanced** tab.
5. In the WAN pane, click the **Show Statistics** button.

Show Statistics							
System Up Time 00:02:11							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	1000M/Half	13	17	0	7	13	00:01:12
LAN1	Link Down						--
LAN2	Link Down						--
LAN3	1000M/Half	1692	3779	0	28368	3232	00:02:11
LAN4	Link Down						--
2.4G WLAN b/g/n	300M	0	0	0	0	0	00:02:10
5G WLAN a/n/ac	1300M	0	0	0	0	0	00:02:10
ADSL Link				Downstream		Upstream	
Connection Speed							
Line Attenuation							
Noise Margin							
Poll Interval : <input type="text" value="5"/> (secs) <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>							

The following information displays:

- **System Up Time.** The time that elapsed since the gateway was last restarted.
- **Port.** The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays the following information:
 - **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 the Internet Connection Status

➤ To view the Internet 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 **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. Click the **Advanced** tab.
5. In a WAN pane, click the **Connection Status** button.

Connection Status WAN 1	
Connection Time	00:01:27
Connection Status	On
Negotiation	On
Authentication	On
IP Address	172.16.2.6
Subnet Mask	255.255.255.255

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 **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 > Administration > Router Update**.
The Firmware Update screen displays.
5. Click **Browse**, navigate to the firmware file (the file ends in **.chk**), and select the firmware file.
6. Click the **Upload** button.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the update. 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 update 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 updating, 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 **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. Click the **Advanced** tab.
The Advanced Home screen displays.
5. In the Router Information pane, click the **Reboot** button.
A confirmation message displays.
6. Click the **OK** button.
The gateway reboots.

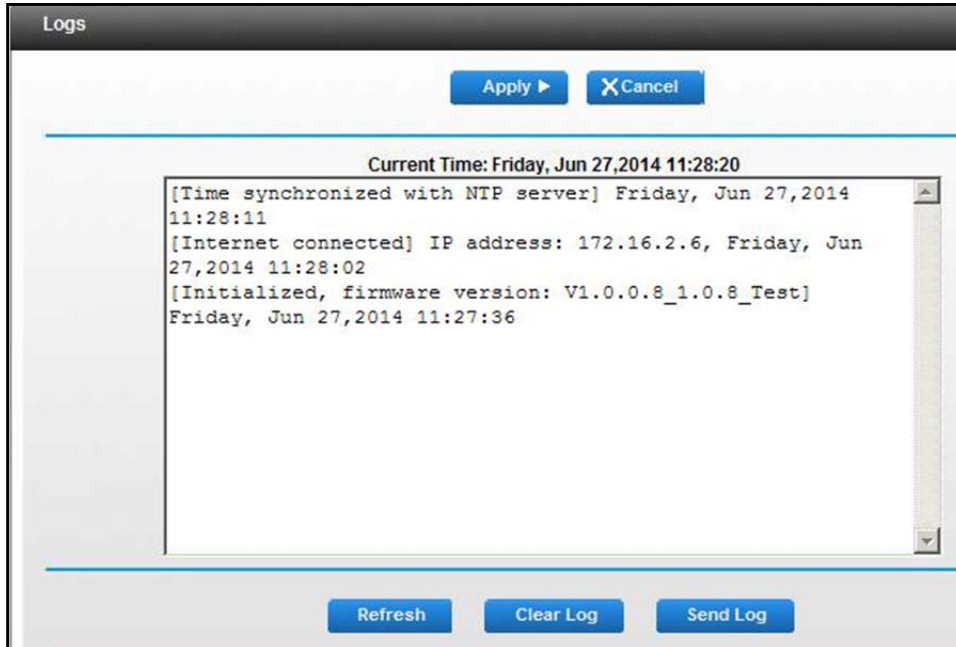
View Logs of Gateway Activity

The log is a detailed record of the websites that you 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 **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 > Administration > Logs**.



The Logs 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.

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

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

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 **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 > Administration > Backup Settings**.

The screenshot shows a web interface titled "Backup Settings". It is divided into three horizontal sections by thin blue lines. The first section is titled "Save a copy of current settings" and contains a blue button labeled "Back Up". The second section is titled "Restore saved settings from a file" and contains a text input field, a blue button labeled "Browse", and a blue button labeled "Restore". The third section is titled "Revert to factory default settings" and contains a blue button labeled "Erase".

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 **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 > Administration > Backup Settings**.

The Backup Settings screen displays.

5. Click the **Browse** button to find and select the `.cfg` file.
6. Click the **Restore** button.
7. When prompted, click the **Yes** button to confirm.

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 122.)

➤ **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 **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 > Administration > Backup Settings**.
5. Click the **Erase** button.
6. When prompted, click the **Yes** button to confirm.

The factory default settings are restored. The user name is admin, the password is password, and the LAN IP address is 192.168.0.1. 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.

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.

➤ **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 **www.routerlogin.com**.

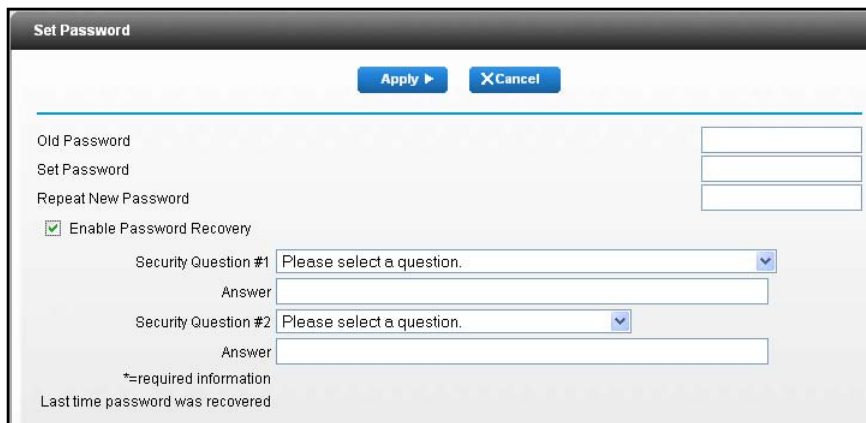
A login screen displays.

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 > 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.

Best practice is to 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 **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 > 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 **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 > Administration > Diagnostics**.

The screenshot shows the 'Diagnostics' page with the following sections:

- Ping an IP address:** IP Address: [] . [] . [] . [] [Ping]
- Perform a DNS Lookup:** Internet Name: [] [Lookup]
IP Address: 0.0.0.0
DNS Server: 0.0.0.0
- Display the Routing Table:** [Display]
- Reboot the Router:** [Reboot]

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 **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 > Administration > Diagnostics**.

The screenshot shows a web interface titled "Diagnostics". It contains four main sections, each with a corresponding button:

- Ping an IP address:** An input field for "IP Address" (divided into four boxes) and a "Ping" button.
- Perform a DNS Lookup:** An input field for "Internet Name", an "IP Address" field, a "DNS Server" field (pre-filled with "0.0.0.0"), and a "Lookup" button.
- Display the Routing Table:** A "Display" button.
- Reboot the Router:** A "Reboot" button.

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 **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 > 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 101.

➤ 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 **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 > 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 106.

➤ **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 **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 > 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 reached:

- 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.

8 Troubleshooting

8

This chapter provides information to help you diagnose and solve problems you might experience 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.
2. Launch a web browser from the connected computer.
3. Type **http://www.routerlogin.net** or **www.routerlogin.com**.

A login screen displays.

4. 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.

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

The Wireless Settings screen displays.

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

The Guest Network Settings screen displays.

WiFi Connections

If you are experiencing 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 WiFi LED on the gateway lit?

If this LED is off, it is possible that someone disabled the wireless radios. For more information about these settings, see [Enable or Disable the WiFi Radios](#) on page 82.

- Did you disable the gateway's SSID broadcast?

If you cleared the **Enable SSID Broadcast** check box in the Wireless Setup 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 76.

- 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 76.

- Did you block access to your network?

If you used access control and set up an access list, check to see if the computer or wireless device that cannot connect is in the list. For more information about access list settings, see [Allow or Block Access to Your Network](#) on page 75.

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. It is possible that the changes occurred but the old settings are 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 LEDs light within a few seconds. This indicates that the gateway has power.

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

- The Internet LED is lit solid blue, indicating that the gateway is connected to the Internet.

- The WiFi LED is lit solid blue, indicating that the WiFi radio is on.

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 122.

If the error persists, you might have a hardware problem.

WiFi LED Is Off

If the WiFi LED stays off, check to see if someone disabled the wireless radios or set up a wireless schedule. For more information about these settings, see *Enable or Disable the WiFi Radios* on page 82. The WiFi LED is lit when the wireless radios are turned on.

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 enter 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 WAN 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 Java, JavaScript, or ActiveX is enabled in your browser. 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 LED 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 **password**. 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 119.

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 ISP assigned you a fixed IP address, your gateway requests an IP address from the ISP. 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 **http://192.168.0.1**.

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. Click the **Advanced** tab.

The Advanced Home screen displays.

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 did not obtain an IP address from your ISP.

For more information about the Internet connection, see [View WAN Information](#) on page 94.

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 they require PPP over Ethernet (PPPoE) or some other type of login. If your ISP requires a login, the login name and password might be set incorrectly.

- Your ISP might check for your computer's host name.

Assign the computer host name of your ISP account as the account name in the Internet Setup screen.

- If your ISP allows only one Ethernet MAC address to connect to Internet and checks for your computer's MAC address, do one of the following:

- Inform your ISP that you 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.

- The gateway might not be configured as the TCP/IP gateway on your computer.

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 provide 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 **http://192.168.0.1**.

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. Click the **Advanced** tab.

The Advanced Home screen displays.

5. On the WAN pane, click the **Connection Status** button.

For more information, see [View WAN Information](#) on page 94. 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. Your ISP might also be experiencing a provisioning problem.

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 be experiencing 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 the examples shown in [Test the LAN Path to Your Gateway](#) on page 117 are displayed.

If you do not receive replies, try the following:

- Check that the IP address of your gateway listed as the default gateway on your computer. If a DHCP server assigns the IP configuration of your computer, this information is not visible on your computer's Network Control Panel.
- 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 192.168.0.1 unless you changed it. Wired and wirelessly connected computers must use 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 experiencing 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 192.168.0.x range.

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 192.168.0.1. This procedure is explained in *Factory Settings* on page 122.

Problems with Date and Time

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.

➤ **To view the gateway's date and time setting:**

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

2. Type **http://routerlogin.net** or **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 > Security > Schedule**.

The Schedule screen displays.

Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
Cause. The gateway did not yet reach a network time server. Check that your Internet access is configured correctly. If you just changed the gateway configuration, 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 and click the **Apply** button.

A 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 at least seven seconds.

The gateway resets and returns to the factory configuration settings shown in the following table.

Table 3. Gateway factory default settings

Feature		Default Behavior
Gateway login	User login URL	www.routerlogin.net or http://192.168.0.1
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address.
	WAN MTU size	1492
	Port speed	AutoSensing
Local area network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.0.2-192.168.0.254
	Time zone	Greenwich Mean Time (GMT) +10
	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	Australia

Table 3. Gateway factory default settings (continued)

Feature		Default Behavior
Wireless (continued)	RF channel	Auto
	Operating mode	<ul style="list-style-type: none"> 2.4 GHz is 11n, 300 Mbps 5 GHz is 11ac, 1300 Mbps
	20/40 MHz coexistence	Enabled
	Data rate	Best
	Output power	Full

Technical Specifications

The following table describes the technical specifications for the gateway.

Table 4. 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	240V, 50 Hz, input 12 VDC @ 2.5A output
Dimensions	73.20 x 122.5 x 209.95 mm (2.88 x 4.8 x 8.27 in.)
Weight	1.27 kg (2.8 lb)
Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	90% maximum relative humidity, noncondensing
LAN	10BASE-T or 100BASE-TX or 1000BASE-T, RJ-45
WAN	10BASE-T or 100BASE-TX or 1000BASE-T, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the entry for Transmission speed in Table 3 on page 122.
Radio data rates	Auto Rate Sensing
Data encoding standards	<ul style="list-style-type: none"> IEEE 802.11 b/g/n 2.4 GHz - 256 QAM support IEEE 802.11 a/n/ac 5.0 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes)
Operating frequency range	2.412–2.462 GHz 5.15 to 5.35 + 5.47 to 5.60 + 5.65 to 5.85 GHz
802.11 security	WPA-PSK, WPA2-PSK, WPA-PSK + WPA2-PSK mixed mode