NETGEAR®
User Manual

Insight Instant VPN Router

BR500

Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.

See the regulatory compliance document before connecting the power supply.

For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.

By using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions. If you do not agree, return the device to your place of purchase within your return period.

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-11903-04	March 2020	Revised Limitation for a Mac VPN client on page 9. Revised About Instant VPN connections on page 127.
202-11903-03	March 2020	Added Limitation for a Mac VPN client on page 9. Revised About Instant VPN connections on page 127.
202-11903-02	April 2019	Added IPSec VPN options to the chapter Set Up VPN Connections on page 126.
202-11903-01	October 2018	First publication.

Contents

Chapter 3 Manage the Firewall and Security

Chapter 4 Manage the LAN and VLAN Settings

Chapter 5 Optimize Performance

Chapter 6 Maintain the Router

Chapter 7 Monitor the router and the router network

Chapter 8 Set Up VPN Connections

Chapter 9 Manage Port Forwarding and Port Triggering Traffic Rules

Chapter 10 Troubleshooting

Appendix A Supplemental information

1
Set Up and Access the Router

This user manual is for the NETGEAR Insight Instant VPN Router BR500, in this manual referred to as the router.

The router is designed to provide firewall and VPN gateway functionality for small business environments with up to 50 users. A pair of routers can provide VPN functionality to users between remote sites. A VPN group with up to three routers can provide a complete meshed network between three locations.

The router functionality includes Network Address Translation (NAT) routing and classical routing, a configurable firewall, VLANs for guest networks and better network segmentation, and IPv6.

This chapter describes how you can connect the router to the Internet and how you can access and log in to the router.

The chapter contains the following sections:

- About this user manual and NETGEAR Insight
- Limitation for a Mac VPN client
- Set up the BR500 router with an Internet connection
- Router management options
- Log in to the local browser interface
- Change the language of the local browser interface
- Add the router to an Insight managed network
- Access Insight to manage the router

Note: This user manual complements the installation guide and hardware installation guide that you can download by visiting netgear.com/support/download/.

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

Note: Firmware updates with new features and bug fixes are made available from time to time at netgear.com/support/download/. You can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this manual, see the latest firmware release notes for your switch model.

About this user manual and NETGEAR Insight

This user manual describes the router's local browser–based management interface, in this manual referred to as the local browser interface. That is, this manual describes the tasks that you can perform using the local browser interface. However, the router is designed to function with NETGEAR Insight as an Insight managed device and to provide virtual private networking (VPN) using the NETGEAR Insight mobile app and Cloud Portal.

For information about NETGEAR Insight and how you can use the NETGEAR Insight mobile app and Cloud Portal to discover the router, add it to an Insight network, and use Insight and the router to set up VPN connections, see the NETGEAR knowledge base articles at netgear.com/support/ and the Insight user manual at downloads.netgear.com/files/GDC/Insight/Insight_UM_EN.pdf.

For general information about NETGEAR Insight, visit netgear.com/insight.

Limitation for a Mac VPN client

If you use a NETGEAR Insight Instant VPN configuration, the Mac VPN client does not function in a client-to-gateway VPN connection.

Set up the BR500 router with an Internet connection

You can set up the router in two ways:

- **Single router providing Internet access**. If the BR500 router is the single router in your network, connect the router directly to a modem, such as a DSL or cable modem that is connected to the Internet, and set up the Internet connection. See Set up the BR500 router to connect to a modem on page 10.

- **Secondary router connected to an existing LAN**. If another router provides the Internet connection, connect the BR500 router to the LAN that is broadcast by the other router and set up the Internet connection of the BR500 router. See Set up the BR500 router to connect to the LAN of an existing router on page 13.

Set up the BR500 router to connect to a modem

If the BR500 router is the single router in your network, connect the router directly to a modem, such as a DSL or cable modem that is connected to the Internet, and set up the Internet connection. Before you start, locate your Internet service provider (ISP) configuration information.

After you physically connect the router, you can let the NETGEAR installation assistant set up your router automatically. For DSL service, you might need the following information to set up the Internet connection for your router:

- The ISP configuration information for your DSL account.

- The ISP login name and password.

- Fixed or static IP address setting (special deployment by the ISP; this setting is rare).

The NETGEAR installation assistant runs on any device with a web browser. Installation and basic setup takes about 15 minutes to complete.

To connect the BR500 router to a modem and use the NETGEAR installation assistant to automatically get an Internet connection:

1. Unplug the modem's power, leaving the modem connected to the wall jack for your Internet service.

   If the modem uses a battery backup, remove the battery.

2. Using an Ethernet cable, connect the modem to the Internet WAN port on the router.

3. Plug in and turn on the modem.

   If the modem uses a battery backup, put the battery back in before you turn on the modem.

4. Connect the router to power.

   After you connect the router to power, the Power LED on the front panel blinks green and then lights solid green.

   If the Power LED does not light at all, press the Power **On/Off** button.

5. Use a computer or mobile device to connect to the local browser interface of the router by doing one of the following:

   - **Use a computer with a wired Ethernet connection**. Do the following:
     a. Configure a computer to obtain an IP address automatically using DHCP.

     b. Connect the computer with an Ethernet cable to a LAN port on the router. You can use LAN port 1, 2, 3, or 4. The conmputer receives an IP address from the router.

- **Use a mobile device to connect to the router over WiFi**. Do the following:

  a. Configure a WiFi access point to obtain an IP address automatically using DHCP.

  b. Connect the access point with an Ethernet cable to a LAN port on the router. You can use LAN port 1, 2, 3, or 4. The access point receives an IP address from the router.

  c. Connect your mobile device to the access point.

6. From the computer or mobile device, launch a web browser and enter **https://www.routerlogin.net** in the address field.

   You can also enter **https://www.routerlogin.com** or enter the IP address in this format: **https://192.168.1.1**. The default IP address for the router is 192.168.1.1.

   For security, we recommend that you enter **https** rather than http. However, if you enter http, the browser automatically redirects your request to https. Your browser might display a security message, which you can ignore (also see the following step).

7. If the browser does not display the login window, do the following:

   - Your browser displays a security message and does not let you proceed. Consider the following examples:

     - **Google Chrome**. If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to 192.168.1.1 (unsafe)** link, in which x.x.x.x represents the IP address of the switch, and install a security certificate.

     - **Apple Safari**. If Apple Safari displays a *This connection is not private* message, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window opens, click the **Visit Website** button. If another pop-up window opens to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.

     - **Mozilla Firefox**. If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that opens, click the **Confirm Security Exception** button and install a security certificate

     - **Microsoft Internet Explore**. If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link and install a security certificate.

     - **Microsoft Edge**. If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage** and install a security certificate.

- If you use a wired Ethernet connection, make sure that the computer is connected to one of the LAN Ethernet ports of the router.
- If you use a mobile device, make sure that mobile device is connected to the access point and that the access point is connected to one of the LAN Ethernet ports of the router.
- Make sure that the router is receiving power and that its Power LED is lit.
- Close and reopen the browser or clear the browser cache.
- If you use a wired Ethernet connection, if the computer is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.
- If you use a mobile device, if the access point to which your device is connected is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.

8. In the login window, enter **admin** for the user name and **password** for the password.

    The NETGEAR installation assistant starts and searches your Internet connection for servers and protocols to determine your Internet configuration. NETGEAR installation assistant guides you through connecting the router to the Internet and setting up a new admin password for the router.

    Note: If you prefer to set up the Internet connection of your router manually, see Manually set up the router Internet connection on page 22.

    When the router connects to the Internet, the Internet WAN LED lights solid green.

9. If the router does not connect to the Internet, do the following:

    a. Review your settings. Make sure that you selected the correct options and typed everything correctly.

    b. Contact your ISP to verify that you are using the correct configuration information.

    c. Read You cannot access the Internet on page 161. If problems persist, register your product and contact NETGEAR technical support.

    Note: The NETGEAR installation assistant runs only the first time that you set up the router.

    Note: The Setup Wizard is a tool with a similar function. For information on running the Setup Wizard, see Use the Internet Setup Wizard on page 21.

Set up the BR500 router to connect to the LAN of an existing router

If another router provides the Internet connection, connect the BR500 router to the LAN that is broadcast by the other router and set up the Internet connection for the BR500 router.

After you physically connect the router, you can let the NETGEAR installation assistant set up your router automatically. By default, the DHCP client of the BR500 router is enabled so that the BR500 router receives an IP address from the other router in your network.

The NETGEAR installation assistant runs on any device with a web browser. Installation and basic setup takes about 15 minutes to complete.

To set up the BR500 router to connect to the LAN of another router and get an Internet connection:

1. Connect an Ethernet cable from the Internet WAN port on the BR500 router to a LAN port on a switch or hub that is connected to the LAN of the other router.

    You can also connect the Ethernet cable directly to a LAN port on the other router.

2. Connect the router to power.

    After you connect the router to power, the Power LED on the front panel first blinks green and then lights solid green.

    If the Power LED does not light at all, press the Power **On/Off** button.

3. Use a computer or mobile device to access the local browser interface of the router by doing one of the following:

    - **Use a computer with a wired Ethernet connection**. Do the following:
        a. Configure a computer to obtain an IP address automatically using DHCP.

        b. Connect the computer with an Ethernet cable to a LAN port on the router. You can use LAN port 1, 2, 3, or 4. The computer receives an IP address from the router.

    - **Use a mobile device to connect to the router over WiFi**. Do the following:
        a. Configure a WiFi access point to obtain an IP address automatically using DHCP.

        b. Connect the access point with an Ethernet cable to a LAN port on the router. You can use LAN port 1, 2, 3, or 4. The access point receives an IP address from the router.

        c. Connect your mobile device to the access point's WiFi network.

4. From the computer or mobile device, launch a web browser and enter
    https://www.routerlogin.net in the address field.

    You can also enter **https://www.routerlogin.com** or enter the IP address in this
    format: **https://192.168.1.1**. The default IP address for the router is 192.168.1.1.

    For security, we recommend that you enter **https** rather than http. However, if you
    enter http, the browser automatically redirects your request to https. Your browser
    might display a security message, which you can ignore (also see the following step).

5. If the browser does not display the login window, do the following:

    - Your browser displays a security message and does not let you proceed. Consider
      the following examples:

        - **Google Chrome**. If Google Chrome displays a *Your connection is not private*
          message, click the **ADVANCED** link. Then, click the **Proceed to 192.168.1.1
          (unsafe)** link, in which x.x.x.x represents the IP address of the switch, and install
          a security certificate.

        - **Apple Safari**. If Apple Safari displays a *This connection is not private* message,
          click the **Show Details** button. Then, click the **visit this website** link. If a
          warning pop-up window opens, click the **Visit Website** button. If another
          pop-up window opens to let you confirm changes to your certificate trust
          settings, enter your Mac user name and password and click the **Update Setting**
          button.

        - **Mozilla Firefox**. If Mozilla Firefox displays a *Your connection is not secure*
          message, click the **ADVANCED** button. Then, click the **Add Exception** button.
          In the pop-up window that opens, click the **Confirm Security Exception** button
          and install a security certificate

        - **Microsoft Internet Explore**. If Microsoft Internet Explorer displays a *There is
          a problem with this website's security certificate* message, click the **Continue
          to this website (not recommended)** link and install a security certificate.

        - **Microsoft Edge**. If Microsoft Edge displays a *There is a problem with this
          website's security certificate* message or a similar warning, select **Details > Go
          on to the webpage** and install a security certificate.

    - If you use a wired Ethernet connection, make sure that the computer is connected
      to one of the LAN Ethernet ports of the router.
    - If you use a mobile device, make sure that mobile device is connected to the
      access point and that the access point is connected to one of the LAN Ethernet
      ports of the router.
    - Make sure that the router is receiving power and that its Power LED is lit.
    - Close and reopen the browser or clear the browser cache.

- If you use a wired Ethernet connection, if the computer is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.
- If you use a mobile device, if the access point to which your device is connected is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.

6. In the login window, enter **admin** for the user name and **password** for the password.

   The NETGEAR installation assistant starts and searches your Internet connection for servers and protocols to determine your Internet configuration. NETGEAR installation assistant guides you through connecting the router to the Internet and setting up a new admin password for the router.

   Note: If you prefer to set up the Internet connection of your router manually, see Manually set up the router Internet connection on page 22.

   When the router connects to the Internet, the Internet WAN LED lights solid green.

7. If the router does not connect to the Internet, do the following:

   a. Review your settings. Make sure that you selected the correct options and typed everything correctly.

   b. Make sure that the other router is connected to the Internet.

   c. Read You cannot access the Internet on page 161. If problems persist, register your product and contact NETGEAR technical support.

   Note: The NETGEAR installation assistant runs only the first time that you set up the router.

   Note: The Setup Wizard is a tool with a similar function. For information on running the Setup Wizard, see Use the Internet Setup Wizard on page 21.

Router management options

The router provides management options (which are not mutually exclusive) that let you discover the router on the network and configure, monitor, and control the router:

- **Local browser–based management interface**. You must access the local browser–based management interface, in this manual referred to as the local browser interface, to set up the WAN (Internet) connection and other settings of the router.

- **NETGEAR Insight mobile app**. After you set up the WAN connection of the router using the local browser interface, you can use the NETGEAR Insight mobile app to discover the router on the network and add the router to the NETGEAR Insight app. Doing so allows you to set up the router in the network and manage and monitor the router remotely from your smartphone. You can choose from four methods to add the router to the NETGEAR Insight app: You can scan your network for the router, scan the QR code or the barcode of the router, or add the serial number of the router (see Add the router to an Insight managed network on page 18).

- **Insight Cloud portal**. As an Insight Premium or Pro user, after you set up the WAN connection of the router using the local browser interface, you can use the NETGEAR Insight Cloud portal to set up the router in the network, perform advanced remote management, monitor the router, analyze the router and network usage, and, if necessary, troubleshoot the router and the network.

Note: For more information about NETGEAR Insight, visit netgear.com/insight, see the NETGEAR knowledge base articles at netgear.com/support/, and see the Insight user manual at downloads.netgear.com/files/GDC/Insight/Insight_UM_EN.pdf.

Log in to the local browser interface

After you set up the router and the router is connected to the Internet, you can view and change the router settings by connecting to the local browser–based management interface, in this manual referred to as the local browser interface.

To access the local browser interface, the procedures in this manual use **https://www.routerlogin.net**. You can also enter **https://www.routerlogin.com** or enter the IP address in this format: **https://192.168.1.1**. The default IP address for the router is 192.168.1.1.

For security, we recommend that you enter **https** rather than http. However, if you enter http, the browser automatically redirects your request to https.

Your browser might display a security message, which you can ignore. Consider the following examples:

- **Google Chrome**. If Google Chrome displays a *Your connection is not private* message, click the **ADVANCED** link. Then, click the **Proceed to 192.168.1.1 (unsafe)** link, in which x.x.x.x represents the IP address of the switch, and install a security certificate.

- **Apple Safari**. If Apple Safari displays a *This connection is not private* message, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window opens, click the **Visit Website** button. If another pop-up window opens to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.

- **Mozilla Firefox**. If Mozilla Firefox displays a *Your connection is not secure* message, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that opens, click the **Confirm Security Exception** button and install a security certificate

- **Microsoft Internet Explore**. If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message, click the **Continue to this website (not recommended)** link and install a security certificate.

- **Microsoft Edge**. If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage** and install a security certificate.

Note: If the router detects a conflict with a WAN IP address, it changes its IP address to 10.0.0.1 or 172.16.5.1.

To log in to the local browser interface:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays. You can now monitor and change the settings of the router.

Change the language of the local browser interface

By default, the language of the local browser interface is set to English. However, you can set the language to a specific one.

To change the language of the local browser interface:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. At the top of the page, from the **Language** menu, select a language.

The language changes.

Add the router to an Insight managed network

When the router is connected to the Internet, the router can communicate with the Insight cloud and you can add the router to an Insight managed network.

To use the NETGEAR Insight mobile app to add the router to an Insight managed network:

1. On your iOS or Android mobile device, visit the app store, search for NETGEAR Insight, and download the app.

2. Open the NETGEAR Insight app on your mobile device.

3. If you did not set up a NETGEAR account yet, tap **Create NETGEAR Account** and follow the onscreen instructions.

4. To log in to your NETGEAR account, enter your credentials and tap **LOG IN**.

5. Name your network and specify a device admin password that applies to all devices that you add to this network.

6. Tap the **Next** button.

7. To add the router to your account, use one of the following options:

- If the router is connected through a WiFi access point to the same WiFi network as the NETGEAR Insight app, scan the network so that Insight can find the router and you can add it to your Insight account.

- If the router is not connected to the same WiFi network as the NETGEAR Insight app, do one of the following, using the information that is on the router label:

  - Scan the serial number bar code.

  - Scan the QR code. (The QR code is located on the router label and is displayed at the upper right corner of the Dashboard in the local browser interface.)

  - Enter the serial number manually.

Note: You might be prompted to connect the router to power and to an uplink. Since you already did this, tap the **Next** button.

The NETGEAR Insight app discovers the router and registers it on the network that you named earlier in this procedure. When the router is connected to the Insight cloud and registered, the Cloud LED lights solid blue.

You can now select the router to configure and manage it or you can use the NETGEAR Insight app to access the router later to view or change the configuration settings.

For more information about how to connect a NETGEAR Insight managed device to an existing network, visit https://kb.netgear.com/000044341.

For more information about NETGEAR Insight, visit netgear.com/insight, see the NETGEAR knowledge base articles at netgear.com/support/, and see the Insight user manual at downloads.netgear.com/files/GDC/Insight/Insight_UM_EN.pdf.

Access Insight to manage the router

After you add the router to an Insight managed network (see Add the router to an Insight managed network on page 18), you can manage the router through one of the following methods:

- **Cloud access from a mobile device**. After initial configuration, as long as your router is on a network with an Internet connection, you can access the router through the cloud using the Insight mobile app.

- **Insight Cloud Portal**. The Insight Cloud Portal is available for Insight Premium and Insight Pro subscribers to set up, manage, and monitor their Insight network and devices. Visit insight.netgear.com/#/login.

2
Specify Your Internet Settings Manually

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

This chapter contains the following sections:

- Use the Internet Setup Wizard
- Manually set up the router Internet connection
- Specify IPv6 Internet connections
- Change the MTU size
- Set Up and Manage Dynamic DNS

Use the Internet Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your router. Although the functionality is similar, the Setup Wizard is not the same as the NETGEAR installation assistant that runs the first time that you connect to your router to set it up.

To use the Setup Wizard:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup Wizard**.

    The Setup Wizard page displays.

5. Select the **Yes** radio button.

    If you select the **No** radio button, you are taken to the WAN Setup page (see Manually set up the router Internet connection on page 22) when you click the **Next** button.

6. Click the **Next** button.

    The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration. When the router connects to the Internet, you are prompted to change the admin password.

Manually set up the router Internet connection

You can view or change the router's Internet connection settings.

Specify a dynamic or fixed IP address Internet connection without a login

To specify or view the settings for an ISP or LAN Internet connection that uses a dynamic or fixed IP address and that does not require a login:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > WAN Setup**.

   The WAN Setup page displays.

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

   This is the default setting.

6. If your Internet connection requires an account name (or host name), do the following:

   a. Click the **Edit** button.
      The Edit Device Name slide-out panel opens.

   b. In the **Device Name** field, enter the account name.
      The account name is the same as the device name, which, by default, is BR500.

   c. Click the **Apply** button.
      Your settings are saved.

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

    For the other sections on this page, the default settings usually work, but you can change them.

8. Select an Internet IP Address radio button:

    - **Get Dynamically**. Depending on your router connection, your ISP uses DHCP to automatically assign your IP address, or another router on the LAN does so.
    - **Use Static IP Address**. Depending on your router connection, do one of the following:

        - **Your router connects to a modem**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.

        - **Your router connects to another router in your network**. Enter the IP address and IP subnet mask for the LAN subnet of the other router. The gateway is the same gateway that the other router is using for its LAN subnet.

9. Select a Domain Name Server (DNS) Address radio button:

    - **Get Automatically from ISP**. Depending on your router connection, your ISP uses DHCP to assign your DNS servers, or another router on the LAN does so. Your ISP or the other router on the LAN automatically assigns these addresses.
    - **Use These DNS Servers**. Depending on your router connection, do one of the following:

        - **Your router connects to a modem**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

        - **Your router connects to another router in your network**. Enter the same DNS servers that the other router is using for its LAN subnet.

10. Select a Router MAC Address radio button:

    - **Use Default Address**. Use the default router MAC address that displays on the Dashboard page and the router label.
    - **Use Computer MAC Address**. If your router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.

11. Click the **Apply** button.

    Your settings are saved.

12. Click the **Test** button to test your Internet connection.

    If the NETGEAR website does not display within one minute, see <u>You cannot access the Internet</u> on page 161.

Specify a PPPoE Internet connection that uses a login

To specify or view the settings for an ISP Internet connection that uses PPPoE and that requires a login:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup > WAN Setup**.

    The WAN Setup page displays.

5. Select the **Yes** radio button.

    The settings on the page change.

6. From the **Internet Service Provider** menu, select **PPPoE** as the encapsulation method.

7. In the **Login** field, enter the login name that your ISP gave you.

    This login name is often an email address.

8. In the **Password** field, enter the password that you use to log in to your Internet service.

9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.

10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.

11. If you select **Dial on Demand** from the **Connection Mode** menu, in the **Idle Timeout (In minutes)** field, enter the number of minutes until the Internet login times out

This is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out. The default is 5 minutes.

12. Select an Internet IP Address radio button:

- **Get Dynamically**. Your ISP uses DHCP to automatically assign your IP address.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.

13. Select a Domain Name Server (DNS) Address radio button:

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
- **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

14. Select a Router MAC Address radio button:

- **Use Default Address**. Use the default router MAC address that displays on the Dashboard page and the router label.
- **Use Computer MAC Address**. If your router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.

15. Click the **Apply** button.

Your settings are saved.

16. Click the **Test** button to test your Internet connection.

If the NETGEAR website does not display within one minute, see <u>You cannot access the Internet</u> on page 161.

Specify a PPTP or L2TP Internet connection that uses a login

To specify or view the settings for an ISP Internet connection that uses PPTP or L2TP and that requires a login:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > WAN Setup**.

   The WAN Setup page displays.

5. Select the **Yes** radio button.

   The settings on the page change.

6. From the **Internet Service Provider** menu, select **PPTP** or **L2TP** as the encapsulation method.

7. In the **Login** field, enter the login name that your ISP gave you.

   This login name is often an email address.

8. In the **Password** field, enter the password that you use to log in to your Internet service.

9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.

10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.

11. If you select **Dial on Demand** from the **Connection Mode** menu, in the **Idle Timeout (In minutes)** field, enter the number of minutes until the Internet login times out

    This is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out. The default is 5 minutes.

12. If your ISP gave you fixed IP addresses and a connection ID or name, enter them in the **My IP Address**, **Subnet Mask**, **Server Address**, **Gateway IP Address**, and **Connection ID/Name** fields.

    If your ISP did not give you an IP addresses, connection ID, or name, leave these fields blank. The connection ID or name applies to a PPTP service only.

13. Select a Domain Name Server (DNS) Address radio button:

    - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
    - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

14. Select a Router MAC Address radio button:

    • **Use Default Address**. Use the default router MAC address that displays on the Dashboard page and the router label.
    • **Use Computer MAC Address**. If your router connects to a modem, the router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.

15. Click the **Apply** button.
    Your settings are saved.

16. Click the **Test** button to test your Internet connection.
    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 161.

Specify IPv6 Internet connections

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

To set up an IPv6 Internet connection:

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

2. Enter **https://www.routerlogin.net**.
    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.
    A login window opens.

3. Enter the router user name and password.
    The default user name is **admin**. The password is the one that you specified when you set up your router. If you skipped specifying a new password, the default password is **password**. The user name and password are case-sensitive.
    The Dashboard displays.

4. Select **ADVANCED > IPv6**.
    The IPv6 page displays.

5. From the **Internet Connection Type** menu, select the IPv6 connection type:

    •   If your ISP did not provide details, select **6to4 Tunnel**.

    •   If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.

    •   If your Internet connection does not use PPPoE or DHCP, or is not fixed, but is IPv6, select **Auto Config**.

Your Internet service provider (ISP) can provide this information. For more information about IPv6 Internet connection, see the following sections:

- Use Auto Detect for an IPv6 Internet connection on page 28

- Use Auto Detect for an IPv6 Internet connection on page 28

- Set up an IPv6 6to4 tunnel Internet connection on page 31

- Set up an IPv6 6rd Internet connection on page 33

- Set up an IPv6 passthrough Internet connection on page 35

- Set up an IPv6 fixed Internet connection on page 35

- Set up an IPv6 DHCP Internet connection on page 37

- Set up an IPv6 PPPoE Internet connection on page 38

6. Click the **Apply** button.
   Your settings are saved.

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 autodetection:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > IPv6**.

 The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Auto Detect**.

 The page adjusts. The router 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 router'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 router'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. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

7. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

8. Select an IPv6 Filtering radio button:

 - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
 - **Open**. In open mode, the router inspects UDP packets only.

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 autoconfiguration:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPv6**.

   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Auto Config**.

   The page adjusts. The router 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 router'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 router'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 gave 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 IPv6 Domain Name Server (DNS) Address radio button:

    - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
    - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IPv6 address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

9. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on the LAN of the router.

10. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

11. Select an IPv6 Filtering radio button:

    - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
    - **Open**. In open mode, the router inspects UDP packets only.

12. Click the **Apply** button.

    Your settings are saved.

Set up an IPv6 6to4 tunnel Internet connection

The remote relay router is the router to which your router 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 a web browser from a computer or mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > IPv6**.

    The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.

    The page adjusts. The router automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the router'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 router uses any remote relay router that is available on the Internet. This is the default setting.
    *   **Static IP Address**. Enter the static IPv4 address of the remote relay router. Your IPv6 ISP usually provides this address.

7. Select an IPv6 Domain Name Server (DNS) Address radio button:

    *   **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
    *   **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

8. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

9. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

10. Select an IPv6 Filtering radio button:

- **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open**. In open mode, the router inspects UDP packets only.

11. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 6rd Internet connection

The 6rd protocol makes it possible to deploy IPv6 to sites using a service provider's IPv4 network. 6rd (also referred to as IPv6 rapid deployment) uses the service provider's own IPv6 address prefix. This limits the operational domain of 6rd to the service provider's network and is under direct control of the service provider. The IPv6 service provided is equivalent to native IPv6. The 6rd mechanism relies on an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider's network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

With a 6rd tunnel configuration, the router follows the RFC5969 standard, supporting two ways to establish a 6rd tunnel IPv6 WAN connection:

- **Auto Detect mode**. In IPv6 Auto Detect mode, when the router receives option 212 from the DHCPv4 option, autodetect selects the IPv6 as 6rd tunnel setting. The router uses the 6rd option information to establish the 6rd connection.

- **Manual mode**. Select **6rd Tunnel**. If the router receives option 212, the fields are automatically completed. Otherwise, you must enter the 6rd settings.

To set up an IPv6 6rd Internet connection:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > IPv6**.

   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **6rd Tunnel**.

   The page adjusts. The router automatically detects the information in the following sections:

   - **6rd (IPv6 Rapid Development) Configuration**. The router detects the service provider's IPv4 network and attempts to establish an IPv6 6rd tunnel connection. If the IPv4 network returns 6rd parameters to the router, the page adjusts to display the correct settings in this section.
   - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router'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 an IPv6 Domain Name Server (DNS) Address radio button:

   - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
   - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

7. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

8. (Optional) In the LAN Setup section, 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 router's LAN interface.

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

9. Select an IPv6 Filtering radio button:

   - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
   - **Open**. In open mode, the router inspects UDP packets only.

10. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 passthrough Internet connection

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

To set up a pass-through IPv6 Internet connection:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPv6**.

   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Pass Through**.

   The page 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 a web browser from a computer or mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPv6**.

   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Fixed**.

   The page adjusts.

6. In the WAN Setup section, specify the fixed IPv6 addresses for the WAN connection:

   - **IPv6 Address/Prefix Length**. The IPv6 address and prefix length of the router WAN interface.

   - **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway for the router's WAN interface.

   - **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the router.

   - **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the router.

   Note: If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the WAN Setup page. (See Manually set up the router Internet connection on page 22.)

7. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

8. In the LAN Setup section, in the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the router's LAN interface.

9. Select an IPv6 Filtering radio button:

   - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
   - **Open**. In open mode, the router inspects UDP packets only.

10. 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 a web browser from a computer or mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > IPv6**.

    The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **DHCP**.

    The page adjusts. The router 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 router'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 router'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 IPv6 Domain Name Server (DNS) Address radio button:

   • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.
   • **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

9. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

10. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

11. Select an IPv6 Filtering radio button:

    • **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
    • **Open**. In open mode, the router inspects UDP packets only.

12. 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 a web browser from a computer or mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.
   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPv6**.

   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **PPPoE**.

   The page adjusts. The router 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 router'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 router'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. Either select the **Use the same Login information as IPv4 PPPoE** check box, or specify the PPPoE settings for IPv6:

   - **Login**. Enter the login name that your ISP gave you.

   - **Password**. Enter the password for the ISP connection.

   - **Service Name (If Required)**. 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** menu is **Always On** to provide a steady IPv6 connection. The router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

7. Select an IPv6 Domain Name Server (DNS) Address radio button:

   - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns these addresses.

- **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

8. In the LAN Setup section, 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

9. (Optional) In the LAN Setup section, select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

10. Select an IPv6 Filtering radio button:

- **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
- **Open**. In open mode, the router inspects UDP packets only.

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 uses 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 router 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 router 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

- You use VPN and experience 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 a web browser from a computer or mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

   The firewall Basic Setup page displays.

5. In the **MTU Size** field, enter a value from 616 to 1500.

   The default size is 1500 bytes.

6. Click the **Apply** button.

   Your settings are 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 1. 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 routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1436	Used in PPTP environments or with VPN.

Set Up and Manage Dynamic DNS

Internet service providers (ISPs) assign IP addresses to identify each Internet account. Most ISPs use dynamically assigned IP addresses. This means that the IP address can change at any time. You can use the IP address to access your network remotely, but most people do not know what their IP address is or when this address changes.

To make it easier to connect when you use OpenVPN, you can get a free account with a Dynamic DNS service that lets you use a domain name to access your home network. To use this account, you must set up the router to use Dynamic DNS. Then the router notifies the Dynamic DNS service provider whenever its IP address changes. When you access your Dynamic DNS account, the service finds the current IP address of your home network and automatically connects you.

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

Note: If you use the router for VPN connections in an Insight managed network with the NETGEAR Insight mobile app or Cloud Portal, the router doesn't require a static IP address and doesn't need to use Dynamic DNS.

Set up a new Dynamic DNS account

NETGEAR offers you the opportunity to set up and register for a free Dynamic DNS account.

To set up Dynamic DNS and register for a free NETGEAR account:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Dynamic DNS page displays.

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

6. From the **Service Provider** menu, select **NETGEAR**.

7. Select the **No** radio button.

8. In the **Host Name** field, enter the name that you want to use for your URL.

    The host name is sometimes called the domain name. Your free URL includes the host name that you specify and ends with mynetgear.com. For example, enter *MyName***.mynetgear.com**.

9. In the **Email** field, enter the email address that you want to use for your account.

10. In the **Password (6-32 characters)** field, enter the password that you want to use for your account.

11. Click the **Register** button.

12. Follow the onscreen instructions to register for your NETGEAR Dynamic DNS service.

Specify a DNS account that you already created

If you already created a Dynamic DNS account with NETGEAR, No-IP, or Dyn, you can set up the router to use your account.

To set up Dynamic DNS if you already created an account:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Dynamic DNS page displays.

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

6. From the **Service Provider** menu, select your provider.

7. Select the **Yes** radio button.

8. In the **Host Name** field, enter the host name (sometimes called the domain name) for your account.

9. Depending on the type of account, specify your user name or email address:

    *   For a No-IP or Dyn account, in the **User Name** field, enter the user name for your account.
    *   For a NETGEAR account, in the **Email** field, enter the email address for your account.

10. In the **Password** field, enter the password for your Dynamic DNS account.

11. Click the **Apply** button.

    Your settings are saved.

12. To verify that your Dynamic DNS service is enabled in the router, click the **Show Status** button.

    A message displays the Dynamic DNS status.

Change the Dynamic DNS settings

You can change the settings for your Dynamic DNS account.

To change your settings:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Dynamic DNS page displays.

5. Change your DDNS account settings as necessary.

6. Click the **Apply** button.

   Your settings are saved.

3

Manage the Firewall and Security

The router comes with a built-in firewall that helps to protect your network from unwanted intrusions *from* the Internet and lets you control access *to* the Internet.

This chapter includes the following sections:

- Manage the basic firewall settings
- Allow or block device access to your network
- Specify keywords and domains to block Internet sites
- Block specific services and applications from the Internet
- Set up a schedule for blocking
- Manage custom firewall traffic rules

Manage the basic firewall settings

The basic firewall settings let you manage port scan protection and denial of service (DoS) protection, specify whether the router can respond to a ping from the WAN port, set up a DMZ server, and manage IGMP proxying, NAT filtering, and the application-level gateway (ALG) for the Session Initiation Protocol (SIP).

For information about the MTU size, which is another basic firewall setting, see Change the MTU size on page 40.

Manage port scan protection and denial of service protection

Port scan protection and denial of service (DoS) protection can protect your LAN against attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. By default, DoS protection is enabled and a port scan is rejected.

You can also enable the router to respond to a ping to its WAN (Internet) port. This feature allows your router to be discovered. Enable this feature only as a diagnostic tool or if a specific reason exists.

To change the default WAN security settings:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

   The Basic Setup page displays.

5. To enable a port scan and disable DoS protection, select the **Disable Port Scan and DoS Protection** check box.

6. To enable the router to respond to a ping on its WAN port, select the **Respond to Ping on Internet Port** check box.

7. Click the **Apply** button.

   Your settings are saved.

Set up a default DMZ server

A default DMZ server is helpful when you are using some Internet services and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router 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 router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service or application for which you set up a port forwarding or port triggering rule (see <u>Manage Port Forwarding and Port Triggering Traffic Rules</u> on page 143). Instead of discarding this traffic, you can direct the router to forward the traffic to one computer on your network. This computer is called the default DMZ server.

To set up a default DMZ server:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

   The Basic Setup page displays.

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

6. Enter the LAN IP address of the computer that must function as the DMZ server.

7. Click the **Apply** button.

   Your settings are saved.

Manage IGMP proxying

IGMP proxying allows a computer or mobile device on the LAN to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, leave it disabled, which is the default setting.

To enable IGMP proxying:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

   The Basic Setup page displays.

5. Clear the **Disable IGMP Proxying** check box.

   By default, this check box is selected and IGMP proxying is disabled.

6. Click the **Apply** button.

   Your settings are saved.

Manage NAT filtering

Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet but might prevent some Internet services, point-to-point applications, or multimedia

applications from working. Open NAT provides a much less secured firewall but allows almost all Internet applications to work. Secured NAT is the default setting.

To change the default NAT filtering settings:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

   The Basic Setup page displays.

5. Select a NAT Filtering radio button:

   • **Secured**. Provides a secured firewall to protect the computers on the LAN from attacks from the Internet but might prevent some Internet services, point-to-point applications, or multimedia applications from functioning. By default, the Secured radio button is selected.

   • **Open**. Provides a much less secured firewall but allows almost all Internet applications to function.

6. Click the **Apply** button.

   Your settings are saved.

Manage the SIP application-level gateway

The application-level gateway (ALG) for the Session Initiation Protocol (SIP) is enabled by default for enhanced address and port translation. However, some types of VoIP and video traffic might not work well when the SIP ALG is enabled. For this reason, the router provides the option to disable the SIP ALG.

To change the default SIP ALG setting:

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

2. Enter **https://www.routerlogin.net**.

>   Your browser might display a security message, which you can ignore. For more
>   information, see Log in to the local browser interface on page 16.
>
>   A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set
    up your router. If you didn't change the password, enter **password**. The user name
    and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > Firewall > Basic Setup**.

    The Basic Setup page displays.

5. To disable the SIP ALG, select the **Disable SIP ALG** check box.

    The SIP ALG is enabled by default.

6. Click the **Apply** button.

    Your settings are saved.

Allow or block device access to your network

You can use device access control to block or allow access to your network. You define
access by selecting or specifying the MAC addresses of the wired devices that either
can access your entire network or are blocked from accessing your entire network.

Enable and manage network access control

When you enable access control, you must select whether new devices are allowed to
access the network or are blocked from accessing the network. By default, currently
connected devices are allowed to access the network, but you can also block these
devices from accessing the network.

To set up network access control:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more
    information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Access Control**.

   The Access Control page 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 the **Turn on Access Control** check box is cleared, all devices are allowed to connect, even if a device is in the list of blocked devices.

6. Click the **Apply** button.

   Your settings are saved.

7. Select an access rule for new devices:

   - **Allow all new devices to connect**. With this setting, if you add a new device, it can access your network. You do not need to enter its MAC address on this page. We recommend that you leave this radio button selected.
   - **Block all new devices from connecting**. With this setting, if you add a new device, before it can access your network, you must enter its MAC address in the allowed list. For more information, see <u>Manage network access control lists</u> on page 53.

   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.

8. To manage access for currently connected computers and devices, do the following:

   a. If you blocked all new devices, you can allow the computer or device that you are currently using to continue to access the network. Select the check box next to your computer or device in the table, and click the **Allow** button.

   b. To change the allow or block settings for other computers and devices, select the check box next to the computer or device in the table, and click either the **Allow** button or the **Block** button.

9. Click the **Apply** button.

   Your settings are saved.

Manage network access control lists

You can use access control to block or allow device access to your network. An access control list (ACL) functions with the MAC addresses of wired and mobile devices that can either access your entire network or are blocked from accessing your entire network.

The router can detect the MAC addresses of devices that are connected to the network and list the MAC addresses of devices that were connected to the network.

Each network device owns a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of a device. If you cannot see the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses of devices that are connected to the router on the Access Control page of the local browser interface (see Add a device to or remove it from the allowed list on page 53 and Add a device to or remove it from the blocked list on page 54).

Add a device to or remove it from the allowed list

If you set up an access list that blocks all new devices from accessing your network, you must specify which devices are allowed to access your network.

To add or remove a device that is allowed:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Access Control**.

   The Access Control page displays.

5. Click the **View list of allowed devices not currently connected to the network** link.

   A table displays the detected device name, MAC address, and connection type of the devices that are not connected but allowed to access the network.

6. To add a device to the allowed list, do the following:

    a. Click the **Add** button.

    The Add Allowed Device slide-out panel opens.

    b. Enter the MAC address and device name for the device that you want to allow.

    c. In the Add Allowed Device slide-out panel, click the **Apply** button.

    The device is added to the allowed list on the Access Control page.

7. To remove a device from the allowed list, do the following:

    a. Select the check box for the device.

    b. Click the **Delete** button.

    The device is removed from the allowed list.

8. Click the **Apply** button.

    Your settings are saved.

Add a device to or remove it from the blocked list

If you set up an access list that allows all new devices to access your network but you want to block some devices, you must specify the devices that you want to block.

To add or remove a device that is blocked:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > Firewall > Access Control**.

    The Access Control page displays.

5. Click the **View list of blocked devices not currently connected to the network** link.

A table displays the detected device name, MAC address, and connection type of the devices that are not connected and are blocked from accessing the network.

6. To add a device to the blocked list, do the following:

    a. Click the **Add** button.

        The Add Blocked Device slide-out panel opens.

    b. Enter the MAC address and device name for the device that you want to block.

    c. In the Add Blocked Device slide-out panel, click the **Apply** button.

        The device is added to the blocked list on the Access Control page.

7. To remove a device from the blocked list, do the following:

    a. Select the check box for the device.

    b. Click the **Delete** button.

        The device is removed from the blocked list.

8. Click the **Apply** button.

    Your settings are saved.

Specify keywords and domains to block Internet sites

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

Set up keyword and domain blocking

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

To set up keyword and domain blocking:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

---

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Block Sites page displays.

5. Specify a keyword blocking option:

   - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Set up a schedule for blocking on page 63.
   - **Always**. Use keyword blocking continuously.

6. In the **Type keyword or domain name here** field, enter a keyword or domain.

   Here are some sample entries:

   - Specify XXX to block http://www.badstuff.com/xxx.html.

   - Specify the domain suffix (for example, .edu or .gov) 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 or domain is added to the **Block sites containing these keywords or domain names** field (which is also referred to as the blocked list).

8. To add more keywords or domains, repeat the previous two steps.

   The keyword list supports up to 32 entries.

9. Click the **Apply** button.

   Your settings are saved.

Specify a trusted device

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

To specify a trusted device:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

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

The Block Sites page displays.

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

6. In the **Trusted IP Address** field, enter the IP address of the trusted device.

The first three octets of the IP address are automatically populated and depend on the IP address that is assigned to the DHCP server of the router (see Manage the DHCP server address pool for a LAN subnet on page 73).

7. Click the **Apply** button.

Your settings are saved.

Remove a keyword or domain from the blocked list

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

To remove a keyword or domain from the blocked list:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

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

    The Block Sites page displays.

5. In the **Block sites containing these keywords or domain names** field, select the keyword or domain.

6. Click the **Delete keyword** button.

    The keyword or domain is removed from the blocked list.

7. Click the **Apply** button.

    Your settings are saved.

Remove all keywords and domains from the blocked list

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

To remove all keywords and domains from the blocked list:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Block Sites page displays.

5. Click the **Clear List** button.

    All keywords and domains are removed from the blocked list.

6. Click the **Apply** button.

    Your settings are saved.

Block specific services and applications from the Internet

You can add service blocking rules to prevent access from your LAN to specific services and applications on the Internet. In addition, you can specify if a blocking rule applies to one user, a range of users, or all users on your LAN. The router lists many default services and applications that you can use in blocking rules. You can also add a service blocking rule for a custom service or application.

Add a service blocking rule for a predefined service or application

The router lists many predefined services and applications that you can use in outbound rules.

You can add a service blocking rule to prevent access to a specific service or application on the Internet.

To add a service blocking rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Block Services page displays.

5. In the Services Blocking section, specify how the router applies outbound rules:

   - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Set up a schedule for blocking on page 63.
   - **Always**. Use keyword blocking continuously.

6. Click the **Add** button.

   The Add Services Blocking slide-out panel opens.

7. From the **Service Type** menu, select the service or application to be covered by this rule.

   The **Protocol**, **Starting Port**, and **Ending Port** fields are automatically populated when you select the service or application.

   Note: If the service or application does not display in the list, you can add it by selecting **User Defined** from the **Service Type** menu (see Add a service blocking rule for a custom service or application on page 60).

8. Specify which devices on your LAN are affected by the rule, based on their IP addresses:

   • **Only This IP Address**. Enter the required IP address in the fields to apply the rule to a single device on your LAN.
   • **IP Address Range**. Enter the required start and end IP addresses in the fields to apply the rule to a range of devices.
   • **All IP Addresses**. All computers and devices on your LAN are covered by this rule.
     By default, the All IP Addresses radio button is selected.

9. Click the **Add** button.

   The new rule is added to the Service Table on the Block Services page.

Add a service blocking rule for a custom service or application

If the service or application is not predefined, you can add a service blocking rule for a custom service or application.

To add service blocking rule for a custom service or application:

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

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

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

3. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

4. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

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

The Block Services page displays.

6. The first time that you add an outbound firewall rule, in the Services Blocking section, specify how the router applies outbound rules:

- **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see <u>Set up a schedule for blocking</u> on page 63.
- **Always**. Use keyword blocking continuously.

7. Click the **Add** button.

The Add Services Blocking slide-out panel opens.

8. From the **Service Type** menu, select **User Defined**.

9. Specify a new service blocking rule by selecting a protocol, defining the ports, and defining a name:

- **Protocol**. From the menu, select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.

- **Starting Port**. In the field, enter the start port for the service or application.

- **Ending Port**. In the field, enter one of the following:

  - If the service or application uses a range of ports, enter the end port for the range.

  - If the service or application uses a single port, repeat the port number that you entered in the **Starting Port** field.

- **Service Type/User Defined**. In the field, enter the name of the custom service or application.

10. Specify which devices on your LAN are affected by the rule, based on their IP addresses:

- **Only This IP Address**. Enter the required address in the fields to apply the rule to a single device on your LAN.
- **IP Address Range**. Enter the required addresses in the start and end fields to apply the rule to a range of devices.
- **All IP Addresses**. All computers and devices on your LAN are covered by this rule.
  By default, the **All IP Addresses** radio button is selected.

11. Click the **Add** button.

    The new rule is added to the Service Table on the Block Services page.

Change a service blocking rule

You can change an existing service blocking rule.

To change a service blocking rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Block Services page displays.

5. In the Service Table, select the radio button for the rule.

6. Click the **Edit** button.

   The Edit Services Blocking slide-out panel opens.

7. Change the settings.

   For more information about the settings, see Add a service blocking rule for a custom service or application on page 60.

8. Click the **Apply** button.

Your settings are saved. The modified rule displays in the Service Table on the Block Services page and the changes go into effect immediately.

Remove a service blocking rule

You can remove a service blocking rule that you no longer need.

To remove a service blocking rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Block Services page displays.

5. In the Service Table, select the radio button for the rule.

6. Click the **Delete** button.

   A warning pop-up window opens.

7. Click the **OK** button.

   The rule is removed from the Service Table. Custom rules are deleted.

Set up a schedule for blocking

You can set up a schedule that you can apply to keyword and domain blocking, Internet service and application blocking, or both.

The schedule can specify the days and times that these features are active. After you set up the schedule, if you want it to become active, you must apply it to keyword and domain blocking (see Set up keyword and domain blocking on page 55), Internet service and application blocking (see Block specific services and applications from the Internet

on page 59), or both. Without a schedule, you can only enable or disable these features. By default, no schedule is set.

To set up a schedule:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Schedule page displays.

5. Set up the schedule for blocking:

    *   **Days to Block**. Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
        By default, the **Every Day** check box is selected.

    *   **Time of Day to Block**. Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.
        By default, the **All Day** check box is selected.

6. From the **Time Zone** menu, select your time zone.

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

    Note: If the router synchronized its internal clock with a time server on the Internet and you selected the correct time zone, the Current Time field displays the correct date and time.

8. Click the **Apply** button.

    Your settings are saved.

Manage custom firewall traffic rules

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

The router provides one default outbound traffic rule: It allows all access to the Internet (that is, the WAN). You can add rules to allow access to or prevent access from specific protocols, IP addresses, and MAC addresses on the Internet. For example, you can specify if a traffic rule applies to one user, a range of users, all users on a LAN, or to the WAN. You need networking knowledge to set up traffic rules.

For information about blocking specific keywords, URLs, or sites, see Specify keywords and domains to block Internet sites on page 55. For information about blocking services or applications from the Internet, see Block specific services and applications from the Internet on page 59. These types of blocking are other components of the firewall.

For information about an advanced component of the firewall, see Manage Port Forwarding and Port Triggering Traffic Rules on page 143.

Add a firewall traffic rule

You can add a traffic rule to the firewall to prevent or allow traffic based on its protocol, source, destination, and other criteria.

To add a firewall traffic rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Traffic Rules page displays.

5. Click the **Add** button.

    The Add Traffic Rule slide-out panel opens.

6. In the **Name** field, enter a name for the traffic rule.

    The name is for identification purposes.

7. From the **Protocol** menu, select the protocol to which the rule must apply.

    By default, the selection is ALL and the rule applies to the ICMP, UDP, and TCP protocols.

8. Specify the source or sources from which the traffic originates by doing the following:

    a. Select a Source Zone radio button:

        •   **LAN**. The traffic originates from the LAN. If you set up more than one LAN subnet, select the check box for the LAN. By default, the selection is LAN1.

        •   **WAN**. The traffic originates from the WAN.

    b. If the traffic for the rule must originate from a specific IP address, enter the IP address. Otherwise, leave the default setting of any.

    c. If the traffic for the rule must originate from a specific port, enter the port number. Otherwise, leave the default setting of any.

    d. If the traffic for the rule must originate from a MAC address, enter the MAC address. Otherwise, leave the default setting of any.

9. Specify the destination or destinations to which the traffic must be sent by doing the following:

    a. Select a Destination Zone radio button:

        •   **Device (input)**. The traffic must be sent to the computer or mobile device that you are currently using.

        •   **LAN**. The traffic must be sent to the LAN. If you set up more than one LAN subnet, select the check box for the LAN. By default, the selection is LAN1.

        •   **WAN**. The traffic must be sent to the WAN.

    b. If the traffic for the rule must be sent to a specific IP address, enter the IP address. Otherwise, leave the default setting of any.

    c. If the traffic for the rule must be sent to a specific port, enter the port number. Otherwise, leave the default setting of any.

10. Specify the action for the rule by making a selection from the **Action** menu:

    • **ACCEPT**. Traffic that conforms to the rule is accepted from its origination and sent to its destination.

    • **DROP**. Traffic that conforms to the rule is dropped.

11. (Optional). In the **Extra arguments** field, enter arguments that are added to the iptables for the rule.

    This is an advanced option and we recommend that you use care adding arguments to this field. Incorrect configuration might cause your Internet connection to go down or to be negatively affected.

12. Click the **Apply** button.

    The new rule is added to the table on the Traffic Rules page and goes into effect immediately.

Change a firewall traffic rule

You can change an existing firewall traffic rule.

To change a firewall traffic rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Traffic Rules page displays.

5. In the table, click the blue **pencil** icon for the rule.

   The Edit Traffic Rule slide-out panel opens.

6. Change the settings for the rule.

   For more information about the settings, see <u>Add a firewall traffic rule</u> on page 65.

7. Click the **Apply** button.

The modified rule displays in the table on the Traffic Rules page and the changes go into effect immediately.

Remove a traffic rule

If you no longer need a traffic rule, you can remove it from the firewall.

To remove a traffic rule from the firewall:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Traffic Rules page displays.

5. In the table, click the red **trash can** icon for the rule.

   A warning pop-up window opens.

6. Click the **OK** button.

   The rule is removed from the table.

Remove several or all traffic rules from the firewall

You can simultaneously remove several or all traffic rules from the firewall.

To remove several or all traffic rules from the firewall:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Traffic Rules page displays.

5. Do one of the following:

    • **Remove several rules**. Select the check boxes to the left of the rules.

    • **Remove all rules**. Select the check box in the table heading.

6. Click the **Delete** button.

    A warning pop-up window opens.

7. Click the **OK** button.

    The rules are removed from the table.

4

Manage the LAN and VLAN Settings

This chapter describes how you can manage the local area network (LAN) and virtual LAN (VLAN) settings of the router.

The chapter includes the following sections:

- Change the router network device name
- Manage the default IP address settings and LAN subnets
- Manage VLANs
- Manage reserved LAN IP addresses
- Add and manage IPv4 static routes
- Enable an IPTV bridge for a port group or VLAN tag group

Change the router network device name

The router's default network device name is the router model number (BR500).

This device name displays in, for example, a file manager when you browse your network.

To change the router network device name:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. Click the Device Name **Edit** button.

   The Edit Device Name slide-out panel opens.

6. Enter a new name in the **Device Name** field.

7. Click the **Apply** button.

   Your settings are saved.

Manage the default IP address settings and LAN subnets

The default LAN subnet (LAN1) defines the default LAN IP address settings for the router, including the IP address at which you can access the router over the local browser interface. However, the router can support multiple LAN subnets.

Change the LAN IP address settings for a LAN subnet

The router is preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The router's LAN IP configuration for the default LAN subnet (LAN1) is as follows:

- **LAN IP address**. 192.168.1.1 (this is the same as www.routerlogin.net)
- **Subnet mask**. 255.255.255.0
- **VLAN ID**. 1

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. The IP address and subnet mask identify which addresses are local to a specific device and which must be reached through a gateway or router. 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, you can change the LAN IP address settings for the default LAN subnet or add another LAN subnet (see Add a LAN subnet on page 76). If you add another LAN subnet, you must use unique LAN IP address settings and a unique VLAN ID for that subnet.

Note: If you change the default LAN IP address settings, the IP address range for the default DHCP server also changes (see Manage the DHCP server address pool for a LAN subnet on page 73).

To change the LAN IP address settings for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

    The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see Add a LAN subnet on page 76) and want to change the IP address settings for that LAN subnet, click the tab for that LAN subnet.

6. In the **IP Address** fields, enter the LAN IP address.

    If you change the IP address for the default LAN subnet (LAN1), the LAN IP address for the router changes.

7. In the **IP Subnet Mask** fields, enter the LAN subnet mask.

    If you change the IP subnet mask for the default LAN subnet, the LAN IP subnet mask for the router changes.

8. Click the **Apply** button.

    Your settings are saved.

    If you changed the LAN IP address settings of the default LAN subnet, you are disconnected from the local browser interface.

    To reconnect, close your browser, relaunch it, and log in to the router at its new LAN IP address.

Manage the DHCP server address pool for a LAN subnet

By default, the router acts as a Dynamic Host Configuration Protocol (DHCP) server. For each LAN subnet, the router assigns IP, DNS server, and default gateway addresses to all computers that are connected to its LAN subnet.

For a LAN subnet, these addresses must be part of the same IP address subnet as the router's LAN IP address for that LAN subnet. The DHCP address pool for the default LAN subnet is 192.168.1.2 through 192.168.1.254.

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

*   An IP address from the range that you define
*   Subnet mask
*   Gateway IP address
*   DNS server IP address

To specify the DHCP pool of IP addresses that the router assigns for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see <u>Add a LAN subnet</u> on page 76) and want to change the DHCP pool for that LAN subnet, click the tab for that LAN subnet.

6. Make sure that the **Use Router as DHCP Server** check box is selected.

   This check box is selected by default.

7. Specify the range of IP addresses that the router assigns for the LAN subnet:

   • In the **Starting IP Address** field, enter the lowest number in the range.
     This IP address must be in the same LAN subnet.

   • In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.
     This IP address must be in the same LAN subnet.

8. Click the **Apply** button.

   Your settings are saved.

Disable the DHCP server for a LAN subnet

By default, the router functions as a DHCP server for the default LAN subnet (LAN1). The router assigns IP, DNS server, and default gateway addresses to all devices connected to the LAN. The assigned default gateway address is the LAN address of the router.

You can use another device on your network as the DHCP server or specify the network settings of all your computers.

Note: If you disable the DHCP server for the default LAN subnet and do not specify another DHCP server in another LAN subnet or no other DHCP server is available on your network, you must set your computer IP addresses manually so that they can access the router.

To disable the DHCP server for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

    The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see <u>Add a LAN subnet</u> on page 76) and want to change the DHCP pool for that LAN subnet, click the tab for that LAN subnet.

6. Clear the **Use Router as DHCP Server** check box.

7. Click the **Apply** button.

    Your settings are saved.

Manage the Router Information Protocol settings

Router Information Protocol (RIP) lets the router exchange routing information with other routers. By default, RIP is enabled for the default LAN subnet (LAN1) in both directions (in and out) without a particular RIP version. You cannot configure RIP for any other LAN subnets.

To manage the RIP settings:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

    The LAN Setup page displays for the default LAN subnet (LAN1).

5. From the **RIP Direction** menu, select the RIP direction:

    - **Both**. The router broadcasts its routing table periodically and incorporates information that it receives. This is the default setting.
    - **Out Only**. The router broadcasts its routing table periodically but does not incorporate the RIP information that it receives.
    - **In Only**. The router incorporates the RIP information that it receives but does not broadcast its routing table.

6. From the **RIP Version** menu, select the RIP version:

    - **Disabled**. The RIP version is disabled. This is the default setting.
    - **RIP-1**. This format is universally supported. It is adequate for most networks, unless you are using an unusual network setup.
    - **RIP-2**. This format carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

7. Click the **Apply** button.

    Your settings are saved.

Add a LAN subnet

The router includes one default LAN subnet (LAN1), but you can add multiple LAN subnets. Each LAN subnet requires unique LAN IP address settings and a unique VLAN ID (see Add a VLAN on page 81).

To add a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

    The LAN Setup page displays for the default LAN subnet (LAN1).

5. Click the **Add Subnet** button.

    The Add New Subnet slide-out panel opens.

    The LAN Name field and MAC Address field are automatically populated.

6. In the **IP Address** fields, enter the LAN IP address.

    By default, the third octet of the IP address increases by one for each LAN subnet that you add. For example, the default IP address for LAN2 is 192.168.2.1, the default IP address for LAN3 is, 192.168.3.1, and so on. However, you can use any LAN IP address, provided that the IP address differs from the one for the default LAN subnet (LAN1) or any other LAN subnet that you added.

7. In the **IP Subnet Mask** fields, enter the LAN subnet mask.

8. If you want to use the DHCP server for the LAN subnet, select the **Use Router as DHCP Server** check box and specify the range of IP addresses that the router assigns for the LAN subnet:

    *   In the **Starting IP Address** field, enter the lowest number in the range.
        This IP address must be in the same LAN subnet.

    *   In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.
        This IP address must be in the same LAN subnet.

9. In the **VLAN ID** field, enter a VLAN ID.

    The ID must be unique and cannot be used by any other LAN subnet (see <u>Add a VLAN</u> on page 81).

10. (Optional) In the **Description** field, enter a description for the LAN subnet.

    The description is for identification purposes.

11. Click the **Apply** button.

    The new LAN subnet is added.

Remove a LAN subnet

If you no longer need a LAN subnet, you can remove it. Before you remove it, make sure that no clients are connected to the LAN subnet. You cannot remove the default LAN subnet (LAN1).

Note: If you added two LAN subnets, LAN2 and LAN3, and you remove LAN2, the old LAN3 becomes the new LAN 2. That is, the name changes from LAN3 to LAN2.

To remove a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. Click the tab for that the LAN subnet that you want to remove.

6. Scroll to the bottom and click the **Delete** button.

   A warning pop-up window opens.

7. Click the **OK** button.

   The LAN subnet is removed.

Manage VLANs

The router supports virtual LANs (VLANs). This section describes how you can manage them.

VLAN concepts

You can define a local area network (LAN) as a broadcast domain. Hubs, bridges, switches, and WiFi access points in the same physical segment or segments connect all end nodes. End nodes can communicate with each other without a router. Routers connect LANs, routing the traffic to each appropriate port.

A virtual LAN (VLAN) is a local area network that maps devices on a basis other than geographic location, for example, by department, type of user, or primary application. Traffic that flows between different VLANs must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of network devices (computers, servers, and other resources) that behave as if they are connected to a single network segment, even though they might not be. For example, the marketing personnel might be located throughout a building, but if they are all assigned to a single VLAN, they can share resources and bandwidth as if they are connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specific individuals, depending on how you set up the VLAN.

VLANs provide a number of advantages:

- **VLANs let you easily segment your network**. You can group users who communicate most frequently with each other in a common VLAN, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.

- **VLANS are easy to manage**. You can quickly add or change network nodes and make other network changes through the Insight mobile app or Cloud Portal.

- **VLANs provide increased performance**. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.

- **VLANs enhance network security**. VLANs create virtual boundaries that can be crossed only through a router. Therefore, you can use standard, router-based security measures to restrict access to a VLAN.

Port-based VLAN concepts

The router supports port-based VLANs. Port-based VLANs help to confine broadcast traffic to the LAN ports. Even though a LAN port can be a member of more than one

VLAN, you can assign a single VLAN ID only as the port VLAN identifier (PVID). By default, all four LAN ports of the router are assigned to the default VLAN, or VLAN 1, and all untagged traffic is routed through the default VLAN. Therefore, by default, all four LAN ports are assigned the default PVID 1. However, you can change the configuration of VLAN 1 and you can assign another PVID to a LAN port. You cannot delete VLAN 1 because it is the management VLAN (see <u>Management VLAN concepts</u> on page 80).

Note: The WAN port is an untagged member of default VLAN 2. You cannot change or delete VLAN 2.

The following applies to VLANs on the router:

- A LAN port is assigned to at least one VLAN but you can assign it to multiple VLANs.
- When you assign a LAN port to multiple VLANs, you can use the port as a trunk port to connect the router to a switch, access point, or other router.
- You can assign a LAN port as a tagged member of multiple VLANs. However, a LAN port can be an untagged member of a single VLAN only. (By default, all LAN ports are untagged members of VLAN 1.)

The router treats incoming packets in the following ways:

- If an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID. Each port is assigned a default VLAN ID (the PVID) that you can configure. The default setting is 1.
- If a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID. The packet proceeds to the VLAN that is specified by the VLAN ID in the packet.
- If a packet enters through a port that is a member of the VLAN that is specified by the VLAN ID in the packet, the packet can be sent to other ports with the same VLAN ID.
- If a packet enters through a port that is not a member of the VLAN that is specified by the VLAN ID in the packet, the packet is dropped.
- Packets that leave the switch are either tagged or untagged, depending on the VLAN to which the port belongs.

Management VLAN concepts

A management VLAN is a much smaller network that is contained within your regular network. The primary benefit of using a management VLAN is improved network security. When all management traffic is on a separate VLAN, it is much harder for unauthorized users to make changes to your network or monitor network traffic.

Another potential benefit is that a management VLAN can help you minimize the impact of a broadcast storm on other VLANs by giving you a separate path to access your network.

On the router, the management VLAN (VLAN 1) is also the native or default VLAN. By default, all ports are members of the default VLAN. For the management VLAN to be secure, it must be used only for controlling and managing your network devices. We recommend that you restrict access to the management VLAN and configure other VLANs to carry all regular network traffic.

If you decide to restrict access to the management VLAN, especially with an access control list (ACL), make sure that you make your computer or device a member of the VLAN and add its MAC address to the ACL (if applicable). Otherwise, you must log in from an allowed device or lose access to the management functions of the switch. If you are unable to log in on an allowed device, you must reset the router to factory default settings to regain management access.

Add a VLAN

The router includes two default VLANs:

- **VLAN 1**. The default VLAN for the LAN, which includes all four LAN ports as untagged members. You can change this VLAN but you cannot remove it.

- **VLAN 2**. The default VLAN for the WAN, which includes the WAN port as an untagged member. You cannot change or remove this VLAN.

You can add more VLANs.

To add a VLAN:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > VLAN**.

   The VLAN page displays.

5. Click the **Add** button.

    The Add VLAN slide-out panel opens.

6. In the **VLAN ID** field, enter a VLAN ID.

    The ID must be in the range from 3 to 4094. (IDs 1 and 2 are already in use.)

7. In the **Name** field, enter a name for the VLAN.

    The name is for identification purposes.

8. Specify the port members of the VLAN by doing the following:

    a. Select the check boxes for the ports the must be members of the VLAN.

    b. From the menu for each port, select TAG or UNTAG.

        Note: By default, all ports are untagged members of VLAN 1. Before you can add a port as an untagged member to a VLAN, you must first make the port a tagged member of VLAN 1.

9. (Optional) In the **Description** field, enter a description for the VLAN.

    The description is for identification purposes.

10. Click the **Apply** button.

    The new VLAN is added to the table on the VLAN page.

Change a VLAN

You can change an existing VLAN, including VLAN 1 (the default VLAN for the LAN).

To change a VLAN:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > VLAN**.

    The VLAN page displays.

5. In the table, click the blue **pencil** icon for the VLAN.

    The Edit VLAN slide-out panel opens.

6. Change the settings for the VLAN.

    For more information about the settings, see Add a VLAN on page 81.

7. Click the **Apply** button.

    The modified VLAN displays in the table on the VLAN page.

Change the PVID for a LAN port

By default, all LAN ports are assigned a PVID of 1 because they are members of VLAN 1. (The WAN port is assigned a PVID of 2, and you cannot change that PVID.)

You can change the PVID for a LAN port only after you add the LAN port to a second VLAN, that is, a VLAN other than VLAN 1 (see Add a VLAN on page 81).

To change the PVID for a LAN port:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > VLAN**.

    The VLAN page displays.

5. Click the **Ports** tab.

    The Ports page displays.

6. From the menu for a LAN port, select another VLAN ID.

7. Click the **Apply** button.

Your settings are saved.

Remove a VLAN

If you no longer need a VLAN, you can remove it. You cannot remove VLAN 1 and VLAN 2.

To remove a VLAN:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > VLAN**.

   The VLAN page displays.

5. In the table, click the red **trash can** icon for VLAN.

   A warning pop-up window opens.

6. Click the **OK** button.

   The VLAN is removed from the table.

Manage reserved LAN IP addresses

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

Reserve a LAN IP Address for a LAN subnet

You can assign a reserved IP address for a device such as a computer or server that requires permanent IP settings.

To reserve an IP address for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see Add a LAN subnet on page 76) and want to reserve a LAN IP address for that LAN subnet, click the tab for that LAN subnet.

6. Above the Address Reservation table, click the **Add** button.

   The Add Address Reservation slide-out panel opens.

7. Either select the radio button for an attached device that displays in the table or specify the reserved IP address settings in the following fields:

   • **IP Address**. Enter the IP address to assign to the computer or device.
   Enter an IP address in the router's LAN subnet, such as 192.168.1.x.
   • **MAC Address**. Enter the MAC address of the computer or device.
   • **Device Name**. Enter the name of the computer or device.

8. Click the **Add** button.

The reserved address is entered into the Address Reservation table on the LAN Setup page for the LAN subnet.

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

Change a reserved IP address for a LAN subnet

You can change an existing reserved IP address entry for a LAN subnet.

To change a reserved IP address entry for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see Add a LAN subnet on page 76) and want to change a reserved LAN IP address for that LAN subnet, click the tab for that LAN subnet.

6. In the Address Reservation section, select the radio button for the reserved address.

7. Click the **Edit** button.

   The Edit Address Reservation slide-out panel opens.

8. Change the settings.

9. Click the **Apply** button.

   Your settings are saved.

Remove a reserved IP address entry for a LAN subnet

You can remove a reserved IP address entry that you no longer need.

To remove a reserved IP address entry for a LAN subnet:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **BASIC > Setup > LAN Setup**.

   The LAN Setup page displays for the default LAN subnet (LAN1).

5. If you added another LAN subnet (see Add a LAN subnet on page 76) and want to remove a LAN IP address entry for that LAN subnet, click the tab for that LAN subnet.

6. In the Address Reservation table, select the radio button for the reserved address.

7. Click the **Delete** button.

   A warning pop-up window opens.

8. Click the **OK** button.

   The IP address entry is removed.

Add and manage IPv4 static routes

Static routes provide detailed routing information to your router. Typically, you do not need to add static routes. You must configure static routes only for unusual cases such as when you use multiple routers 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 an ADSL modem to an ISP.

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

- Your company's network address is 134.177.0.0.

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

In this case, you must define a static route, instructing your router that 134.177.0.0 is accessed through the ISDN router at 192.168.1.100. Here is an example:

- Through the destination IP address and IP subnet mask, specify that this static route applies to all 134.177.x.x addresses.

- Through the gateway IP address, specify that all traffic for these addresses is forwarded to the ISDN router at 192.168.1.100.

- A metric value of 1 works fine because the ISDN router is on the LAN.

Add an IPv4 static route

You can add an IPv4 static route to a destination IP address and specify the subnet mask, gateway IP address, and metric.

To add an IPv4 static route:

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

2. Enter **https://www.routerlogin.net**.
   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.
   A login window opens.

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.
   The Dashboard displays.

4. Select **ADVANCED > Static Routes**.
   The Static Routes page displays.

5. Click the **Add** button.
   The Add IP Static Route slide-out panel opens.

6. In the **Name** field, enter a name for the route.

   The name is for identification purposes.

7. To make the route private, select the **Private** check box.

   A private static route is not reported in RIP.

8. To prevent the route from becoming active after you click the **Apply** button, clear the **Active** check box.

   In some situations, you might want to set up a static route but keep it disabled until a later time. By default, the **Active** check box is selected and a route becomes active after you click the **Apply** button.

9. Enter the route IP address and metric settings in the following fields:

   - **Destination IP Address**. Enter the IP address for the final destination of the route.

   - **IP Subnet Mask**. Enter the IP subnet mask for the final destination of the route. If the destination is a single host, enter **255.255.255.255**.

   - **Gateway IP Address**. Enter the IP address of the gateway. The IP address of the gateway must be on the same LAN subnet as the router.

   - **Metric**. Enter a number from 1 through 15. This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to **1**.

10. Click the **Apply** button.

    Your settings are saved. The static route is added to the table on the Static Routes page.

Change an IPv4 static route

You can change an IPv4 static route.

To change an IPv4 static route:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

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

    The Static Routes page displays.

5. In the Static Routes table, select the radio button for the route.

6. Click the **Edit** button.

    The Edit IPv4 Static Route slide-out panel opens.

7. Change the settings for the route.

    For more information about the settings, see Add an IPv4 static route on page 88.

8. Click the **Apply** button.

    The route settings are updated in the table on the Static Routes page.

Remove an IPv4 static route

You can remove an existing IPv4 static route that you no longer need.

To remove an IPv4 static route:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Static Routes page displays.

5. In the Static Routes table, select the radio button for the route.

6. Click the **Delete** button.

A warning pop-up window opens.

7. Click the **OK** button.

The route is removed from the table on the Static Routes page.

Enable an IPTV bridge for a port group or VLAN tag group

Some devices, such as an Internet Protocol television (IPTV), cannot function behind the router's Network Address Translation (NAT) service or firewall. Based on what your Internet service provider (ISP) requires, for the device to connect to the ISP's network directly, you can enable a bridge either between the device and the router's WAN (Internet) port or between the device and a VLAN tag group.

Note: If your ISP provides directions on how to set up a bridge for IPTV and Internet service, follow those directions.

Enable an IPTV bridge for a port group

If an IPTV device is connected to a LAN port, your ISP might require you to set up a bridge for a port group for the router's Internet interface.

A bridge with a port group allows packets that are sent between the IPTV device and the router WAN port to circumvent the router's NAT service, which otherwise could drop the packets.

To enable the IPTV bridge for a port group:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > IPTV**.

The IPTV page displays.

5. Select the **Enable VLAN/Bridge group** check box.
    The page expands.

6. Select the **By bridge group** radio button.
    The page adjusts.

7. Select the check box for the wired (LAN) port to which the IPTV device is connected.
    You must select at least one LAN port. You can select more than one LAN port.

8. Click the **Apply** button.
    Your settings are saved.

Enable an IPTV bridge for a VLAN tag group

If an IPTV device is connected to a LAN port, your ISP might require you to set up a bridge for a VLAN tag group for the router's WAN port.

If you are subscribed to IPTV service, the router might require VLAN tags to distinguish between the Internet traffic and the IPTV traffic. A bridge with a VLAN tag group allows packets that are sent between the IPTV device and the router WAN port to circumvent the router's NAT service, which otherwise could drop the packets.

IMPORTANT: You can either add one or more custom VLANs (that is, any VLAN other than default VLAN 1 and VLAN 2) or you can set up an IPTV bridge for a VLAN tag group. You cannot do both on the router because these features are not compatible. If you added custom VLANs (see Add a VLAN on page 81), you must first remove those VLANs (see Remove a VLAN on page 84) before you can enable the IPTV bridge for a VLAN tag group.

The router includes a default VLAN tag group with the name Internet, with VLAN ID 10, and with all LAN ports and the WAN port as members. If you enable the IPTV bridge for a VLAN tag group, this default VLAN tag group is also enabled.

You can add custom VLAN tag groups and assign a VLAN ID, priority value, and ports to each VLAN tag group.

To enable the IPTV bridge for a VLAN tag group:

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

2. Enter **https://www.routerlogin.net**.
    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPTV**.

   The IPTV page displays.

5. Select the **Enable VLAN/Bridge group** check box.

   The page expands.

6. Select the **By VLAN tag group** radio button.

   The page adjusts and the default VLAN tag group displays.

7. To add a custom VLAN tag group, do the following:

   a. Click the **Add** button.
      The Add VLAN Rule slide-out panel opens.

   b. Specify the settings in the following fields:

      • **Name**. Enter a name for the VLAN tag group.
        The name is for identification purposes.

      • **VLAN ID**. Enter a value from 1 to 4094.

      • **Priority**. Enter a value from 0 to 7.

   c. Select the check box for the LAN port to which the device is connected.
      You must select at least one LAN port. You can select more than one LAN port.

8. Click the **Apply** button.

   Your settings are saved. If you added a VLAN tag group, the group is added to the table on the Enable VLAN/Bridge group page.

5
Optimize Performance

You can set up the router to dynamically optimize performance for sevices and applications such as Internet gaming, high-definition video streaming, and VoIP communication.

This chapter includes the following sections:

- <u>Use Dynamic QoS to optimize Internet traffic management</u>
- <u>Improve network connections with Universal Plug and Play</u>

Use Dynamic QoS to optimize Internet traffic management

Dynamic Quality of Service (QoS) helps improve your router's Internet traffic management capabilities through better application and device identification, bandwidth allocation, and traffic prioritization techniques. Dynamic QoS resolves traffic congestion when the Internet bandwidth is limited and different demands compete for bandwidth.

Note: QoS does not increase your total Internet bandwidth or throughput. QoS just prioritizes the way the bandwidth and throughput are used.

Enable Dynamic QoS and set the Internet bandwidth

Because Dynamic QoS might not be suitable for all situations, it is disabled by default.

To enable Dynamic QoS:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > QoS Setup**.

    The QoS Setup page displays.

5. Select the **Dynamic QoS** check box.

    After your Internet bandwidth is established, Dynamic QoS enables the router to automatically prioritize traffic by application and device.

6. To specify your Internet bandwidth, do one of the following (although we recommend that you use the automatic speed test):

- **Use the automatic speed test**. Do the following:

    a. Make sure that the **Let Speedtest detect my Internet bandwidth** radio button is selected.
    By default, this radio button is selected.

    b. For more accurate speed test results, make sure that no other devices are accessing the Internet while your perform the automatic speedtest.

    c. Click the **Take a Speedtest** button.
    Speedtest determines your Internet bandwidth. The test make take up to one of minute.
    A pop-up window opens.

    d. To apply the detected Internet bandwidth settings, click the **Yes** button.

- **Manually set the Internet bandwidth**. Do the following:

    a. Select the **I want to define my Internet bandwidth** radio button.
    A warning pop-up window opens.

    b. Click the **OK** button.

    c. In the **Download Speed (Mbps)** field, enter the download speed.

    d. In the **Upload Speed (Mbps)** field, enter the upload speed.

7. Click the **Apply** button.
   A warning pop-up window opens.

8. Click the **OK** button.
   Your settings are saved.

Enable or disable the automatic update of the QoS database

The router uses a QoS database of the most popular applications and services to implement Dynamic QoS. By default, the router automatically updates this database. You can turn off this feature and manually update the database.

To enable or disable the automatic update of the QoS database:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > QoS Setup**.

The QoS Setup page displays.

If you are using Dynamic QoS, by default, the **Automatically update performance optimization database** check box is selected.

5. Select or clear the **Automatically update performance optimization database** check box.

6. Click the **Apply** button.

Your settings are saved.

Manually update the QoS database on the router

The router uses a QoS database of the most popular applications and services to implement Dynamic QoS. By default, the router automatically updates this database when you enable Dynamic QoS, but if you turned off the automatic update feature, you can manually update the database.

To manually update the QoS database:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > QoS Setup**.

    The QoS Setup page displays.

    The version and release date of the installed database display.

5. Click the **Update Now** button.

    The router checks for the newest version of the database and downloads it.

6. Click the **Apply** button.

    Your settings are saved.

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 the router must support applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging, enable UPnP.

To enable Universal Plug and Play:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > UPnP**.

    The UPnP page displays.

5. Make sure that the **Turn UPnP On** check box is selected.

By default, this check box is selected. If the **Turn UPnP On** check box is cleared, the router 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 router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points 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 is fine for most 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 router 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.

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

6

Maintain the Router

This chapter describes how you can maintain the router by managing the firmware, configuration file, admin password, and logs and by setting up the traffic meter.

The chapter includes the following sections:

- <u>Check for new firmware and update the router</u>
- <u>Change the admin password</u>
- <u>Set up password recovery</u>
- <u>Recover the admin password</u>
- <u>Manage the configuration file of the router</u>
- <u>Return the router to its factory default settings</u>
- <u>Manage the activity log</u>
- <u>Monitor and meter Internet traffic</u>

Check for new firmware and update the router

From time to time, or as needed, NETGEAR makes new firmware available.

The firmware is stored in flash memory.

To download new firmware manually and update your router:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. To locate new firmware, do one of the following:

   - At the top of the Dashboard, next to the firmware version, click the **Download** icon to open the support page for the router.

   - Visit netgear.com/support/download/ and locate the support page for the router.

5. If available, download the new firmware to your computer or mobile device.

6. Read the new firmware release notes to determine whether you must reconfigure the router after updating.

7. Select **ADVANCED > Firmware Update**.

   The Firmware Update page displays.

8. Locate and select the firmware file on your computer or mobile device:

   a. Click the **Browse** button.

   b. Navigate to and select the firmware file
      The file ends in `.img`.

9. Click the **Upload** button.

A warning pop-up window might open.

10. If a warning pop-up window opens, click the **OK** button.
    The current version and the version that you intend to upload display.

11. Click the **Yes** button.

    WARNING: To avoid the risk of corrupting the firmware, do not interrupt the upload. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED turns solid green.

    A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, your router restarts.

12. Verify that the router runs the new firmware version:

    a. Launch a web browser from a computer or mobile device that is connected to the router network.

    b. Enter **https://www.routerlogin.net**.
        Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.
        A login window opens.

    c. Enter the router user name and password.
        The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.
        The Dashboard displays.
        The version firmware is stated in the Firmware Version field at the top of the page.

Change the admin password

You can change the default password that is used to log in to the router with the user name admin.

Note: Be sure to change the password for the user name admin 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 mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Setup > Set Password**.

    The Set Password page displays.

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.

    We recommend that you enable password recovery.

7. If you enable password recovery, select two security questions and provide answers to them.

8. Click the **Apply** button.

    Your settings are saved.

Set up password recovery

We recommend that you enable password recovery if you change the password for the router 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 mobile device that is connected to the router network.

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **BASIC > Setup > Set Password**.

The Set Password page 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 settings are saved.

Recover the admin password

Note: After five login failures, you must wait five minutes before you can recover your admin password. During the time-out period of five minutes, you cannot recover your admin password.

To recover your admin password:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Click the **Cancel** button.

If password recovery is enabled (see <u>Set up password recovery</u> on page 103), you are prompted to enter the serial number of the router.

The serial number is on the product label.

4. Enter the serial number of the router.

5. Click the **Continue** button.

    A window opens requesting the answers to your security questions.

6. Enter the saved answers to your security questions.

7. Click the **Continue** button.

    A window opens and displays your recovered password.

8. Click the **Login again** button.

    A login window opens.

9. With your recovered password, log in to the router.

Manage the configuration file of the router

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

Back up the router configuration file

You can save a copy of the current configuration settings.

To back up the router's configuration file:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Backup Settings page displays.

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

6. Choose a location to store the file on your computer.

The backup file ends in `.cfg`.

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

Restore the router configuration settings

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

To restore configuration settings that you backed up:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Backup Settings page displays.

5. Click the **Browse** button and navigate to and select the saved configuration file.

    The backup file ends in `.cfg`.

6. Click the **Restore** button.

    A warning pop-up window opens

7. Click the **Yes** button.

    The configuration is uploaded to the router. When the restoration is complete, the router reboots. This process takes about two minutes.

    WARNING: To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED turns solid green.

Return the router to its factory default settings

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

If you do not know the current IP address of the router, first try to use the NETGEAR Insight mobile app or an IP scanner application to detect the IP address. If you still cannot find the current IP address of the router, reset the router to factory default settings.

To reset the router to factory default settings, you can use either the **Reset** button on the back of the router or the Erase function in the local browser interface. However, if you cannot find the IP address or lost the password to access the router and cannot recover it, you must use the **Reset** button.

After you reset the router to factory default settings, the user name is admin, the password is password, the LAN IP address is 192.168.1.1 (which is the same as www.routerlogin.net), and the DHCP server is enabled. For a list of factory default settings, see <u>Factory settings</u> on page 168.

Use the Reset button

CAUTION: This process erases all settings that you configured in the router.

To reset the router to factory default settings:

1. On the back of the router, locate the **Reset** button.

2. Using a straightened paper clip, press and hold the recessed **Reset** button until the Power LED lights amber, which takes about five seconds.

3. Release the **Reset** button.

    The Power LED starts blinking amber and the configuration is reset to factory default settings. When the reset is complete, the router reboots. This process takes about two minutes.

    WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, if you are connected to the router's web page, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED turns solid green.

Erase the settings

CAUTION: This process erases all settings that you configured in the router.

To erase the settings:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Backup Settings page displays.

5. Click the **Erase** button.

   A warning page displays.

6. Click the **Apply** button.

   The configuration is reset to factory default settings. When the reset is complete, the router reboots. This process takes about two minutes.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting and the Power LED turns solid green.

Manage the activity log

The log is a detailed record of the websites that users on your network accessed or attempted to access and many other router actions. You can manage which activities are logged.

Specify which activities the router logs

You can specify which activities the router logs. These activities display in the log.

To manage which activities are logged:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Logs**.

   The Logs page displays.

5. Select the check boxes that correspond to the activities that you want to be logged. By default, all check boxes are selected, and the following activities are logged:

   - Attempted access to allowed sites
   - Attempted access to blocked sites and services
   - Connections to the local browser interface of the router
   - Router operation such as startup, getting the time, and so on
   - Known DoS attacks and port scans
   - Port forwarding and port triggering
   - VPN service

6. Clear the check boxes that correspond to the activities that you do not want to be logged.

7. Click the **Apply** button.

   Your settings are saved.

View or clear the logs

In addition to viewing the logs, you can clear them.

To view or clear the logs:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Logs**.

   The Logs page displays.

   In addition to the current date and time, the Logs page displays the following information:

   - **Action**. The action that occurred, such as whether Internet access was blocked or allowed.

   - **Source**. If applicable, the name, IP address, or MAC address of the target device, application, or website for this log entry.

   - **Target**. If applicable, the name, IP address, or MAC address of the target device, application, or website for this log entry.

   - **Date and Time**. The date and time at which the action occurred.

5. To refresh the log entries onscreen, click the **Refresh** button.

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

Monitor and meter Internet traffic

Traffic metering allows you to monitor the volume of Internet traffic that passes through the router WAN port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

Start the traffic meter without traffic restrictions

You can monitor the traffic volume without setting a limit on the volume or connection time.

To start or restart the traffic meter without configuring traffic volume or connection time restrictions:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Traffic Meter page displays.

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

   By default, no traffic limit is specified and the traffic volume or connection time is not controlled.

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

7. To start the traffic counter immediately, click the **Restart Counter Now** button.

8. Click the **Apply** button.

   Your settings are saved.

   The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 114.

Restrict Internet traffic by volume

You can record and restrict the traffic by volume in MB. This is useful when your ISP measures your traffic volume.

To record and restrict the Internet traffic by volume:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

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

   The Traffic Meter page displays.

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

6. Select the **Traffic volume control by** radio button.

7. From the corresponding menu, select an option:

   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.

8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.

9. If your ISP charges you 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.

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

11. In the Traffic Control section, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.

    This setting is optional. The router issues a warning when the balance falls below the number of minutes that you enter. By default, the value is 0 and no warning message is issued.

12. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to flashing green/amber**. This setting is optional. When the traffic limit is reached, the Internet LED alternates blinking green and amber.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

13. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 114.

Restrict Internet traffic by connection time

You can record and restrict the traffic by connection time. This is useful when your ISP measures your connection time.

To record and restrict the Internet traffic by connection time:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Traffic Meter page displays.

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

6. Select the **Connection time control** radio button.

    The router must be connected to the Internet for you to be able to select the **Connection time control** radio button.

7. In the **Monthly Limit** field, enter how many hours per month are allowed.

The router must be connected to the Internet for you to be able to enter information in the **Monthly Limit** field.

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

9. In the Traffic Control section, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.

    This setting is optional. The router issues a warning when the balance falls under the number of minutes that you enter. By default, the value is 0 and no warning message is issued.

10. Select one or more of the following actions to occur when the limit is reached:

    *   **Turn the Internet LED to flashing green/amber**. This setting is optional. When the traffic limit is reached, the Internet LED alternates blinking green and amber.
    *   **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

11. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 114.

View the Internet traffic volume and statistics

If you enabled the traffic meter (see Start the traffic meter without traffic restrictions on page 111), you can view the Internet traffic volume and statistics.

To view the Internet traffic volume and statistics shown by the traffic meter:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Traffic Meter page displays.

5. Scroll down to the Internet Traffic Statistics section.

    The Internet Traffic Statistics section displays when the traffic counter was started and what the traffic balance is. The table displays information about the connection time and traffic volume in MB.

6. To refresh the information onscreen, click the **Refresh** button.

    The information is updated.

7. To display more information about the data traffic and to change the polling interval, click the **Traffic Status** button.

    The Traffic Status slide-out panel displays.

Unblock the traffic meter after the traffic limit is reached

If you configured the traffic meter to disconnect and disable the Internet connection after the traffic limit is reached, you cannot access the Internet until you unblock the traffic meter.

CAUTION: If your ISP set a traffic limit, your ISP might charge you for the overage traffic.

To unblock the traffic meter:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

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

    The Traffic Meter page displays.

5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.

6. Click the **Apply** button.
    Your settings are saved.

7
Monitor the router and the router network

This chapter describes how you can monitor the router and the router network.

The chapter includes the following sections:

- View devices currently on the network
- Display the network map and VPN map
- View VPN groups and VPN devices in a VPN network of an Insight managed router
- Check the Internet connection status and manage the connection
- Display the port statistics
- Display the router status, CPU and memory usage, and temperature
- Display the WAN traffic processed on the router
- Monitor the router throughput

View devices currently on the network

You can view the active wired devices (also called attached devices) in the router network.

To display the wired devices:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > Attached Devices**.

    The Attached Devices page displays. The NETWORK MAP pane shows the network topology, including the Internet connection and the devices that are connected to the router. The ATTACHED DEVICES LIST pane shows the devices that are connected to the router.

    Depending on the connected device, the following information displays in the ATTACHED DEVICES LIST pane:

    *   **Type**. The type of device, which is indicated by a device icon.

    *   **Name**. The device network name.

    *   **IP address**. The IP address that the router assigned to the device when it joined the router network. This address can change when a device is disconnected and rejoins the router network.

    *   **MAC address**. The MAC address of the connected device.

    *   **Access control**. If access control is enabled (see Manage network access control lists on page 53), the status of the device (either Allowed or Blocked).

5. To view the same device information in a table, select **Dashboard**, and scroll down to the ATTACHED DEVICES pane.

Display the network map and VPN map

To display the network map and VPN map:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

   The NETWORK MAP pane shows the network topology, including the Internet connection and the devices that are connected to the router.

4. In the NETWORK MAP pane, click the **VPN MAP** tab.

   The VPN MAP pane shows the network topology for connected VPN devices.

View VPN groups and VPN devices in a VPN network of an Insight managed router

You can view the VPN groups and active VPN devices in the VPN network on an Insight managed router. Any changes must be made using the NETGEAR Insight mobile app or Cloud Portal.

ATTENTION: VPN groups apply only to a router that functions in an Insight network. If you router is not managed by the NETGEAR Insight mobile app or Cloud Portal, no information displays on this page. If you router *is* managed by the NETGEAR Insight mobile app or Cloud Portal but no VPN groups are set up, no information displays on this page either.

To display the VPN groups and active VPN devices in the VPN network on an Insight managed router:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **BASIC > VPN**.

    The VPN GROUP MAP page displays.

    If any VPN groups are set up, they display on this page, including information about the health of the VPN connections.

5. Click the **LIST MODE** button.

    The VPN GROUP LIST table shows information about the VPN groups that are set up, including the VPN network that is part of a VPN group and the number of group members that are online and offline.

    The DEVICES LIST table shows information about the router and VPN devices. Depending on the type of device, the following information displays in the DEVICES LIST table:

    *   **Status**. Whether the router or VPN device is online or offline.

    *   **Serial Number**. The serial number of the router or the MAC address of the VPN device.

    *   **Virtual IP**. The virtual IP address assigned to the router or the remote VPN device after it made a connection to the VPN network. This address can change when the router or remote VPN device is disconnected and reconnects to the VPN network.

    *   **WAN IP**. The WAN IP address of the router.

    *   **Subnet IP**. The LAN subnet address of the router. Users of VPN devices that are members of the same VPN group can access each other's LAN subnets.

6. To return to the VPN GROUP MAP page, click the **MAP MODE** button.

Consider the following VPN example for Insight managed routers with a site-to-site connection and a remote VPN client:

- **Site 1**. An ISP assigns a BR500 router a public WAN IP address of 12.34.56.78, the router virtual IP address is 10.1.11.1, the router LAN subnet is 192.168.1.x, and a ReadyNAS storage device receives a DHCP-assigned IP address of 192.168.1.2.

- **Site 2**. Another BR500 router is connected to an existing office network, receives a private (that is, non-public) WAN IP address of 10.20.1.119, the router virtual IP address is 10.1.11.2, and the router LAN subnet is 192.168.2.x.

- **Remote VPN client**. In a hotel, a remote VPN client is assigned LAN IP address 192.168.3.3, the user does not know the WAN IP of the hotel, and the VPN client is assigned virtual IP address 10.1.11.3 through its VPN client program.

In this VPN configuration, the following applies:

- The remote VPN client can ping both BR500 routers (that is, IP address 10.1.11.1 and IP address 10.1.11.2) because the remote client and the routers function in the same VPN network.

- The remote VPN client can also ping WAN IP address 12.34.56.78 of the BR500 router at Site 1 because it is a public IP address.

- The remote VPN client cannot ping WAN IP address 10.20.1.119 of the BR500 router at Site 2 because it is a private IP address.

- The remote VPN client can access Site 1 at an IP address in LAN subnet 192.168.1.x. For example, the remote VPN client can access the SMB share of the ReadyNAS storage device at \\192.168.1.2.

- The remote VPN client can access devices at Site 2 at an IP address in LAN subnet 192.168.2.x.

- Local users at Site 1 and Site 2 can access each other's devices at an IP address in the LAN subnet of each BR500 router.

Check the Internet connection status and manage the connection

To check the Internet connection status and manage the connection:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. In the PORTS STATUS pane, click the **CONNECTION STATUS** tab.

    The connection status information displays.

    Note: The information that displays depends on the type of Internet connection. If the Internet connection is PPPoE, PPTP, or L2TP, other information might display than if the Internet connection is an IP address that the ISP assigns dynamically (the most common situation).

    If the ISP assigned an IP address to the router dynamically, the following information displays:

    - **IP Address**. The IP address that is assigned to the router.

    - **Subnet Mask**. The subnet mask that is assigned to the router.

    - **Default Gateway**. The IP address for the default gateway that the router communicates with.

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

    - **DNS Server**. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

    - **Lease Obtained**. The date and time when the lease was obtained.

    - **Lease Expires**. The date and time that the lease expires.

5. To release (stop) the Internet connection, click the **Release** button.

6. To renew (restart) the Internet connection, click the **Renew** button.

Display the port statistics

To display the port statistics:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. In the PORTS STATUS pane, in the router graphic, point to the Internet LED for status information on the WAN port or to one of the LAN LEDs for status information on the LAN port.

    For the port that you point to, a pop-up window displays the following information:

    - **Tx B/s**. The number of Bytes per second transmitted on the port since the router started.

    - **Rx B/s**. The number of Bytes per second received on the port since the router started.

Display the router status, CPU and memory usage, and temperature

To display the router status, CPU and memory usage, and temperature:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

   - **Internet Status**. Shows ONLINE or OFFLINE.
   - **Serial Number**. The serial number of the router.
   - **LAN IP Address**. By default, 192.168.1.1.
   - **WAN IP Address**. This address depends on how your router receives a WAN IP address.
   - **DHCP Status**. Shows ON or OFF.

   The page also displays the router label, which allows you to add the router to an Insight network by using the scan option in the NETGEAR Insight mobile app.

4. Scroll down to the CURRENT STATUS pane.

   The CURRENT STATUS pane displays the CPU usage, memory usage, and temperature of the router.

Display the WAN traffic processed on the router

To display the uploaded and downloaded WAN traffic that the router processed.

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. The CURRENT STATUS pane, click the **WAN TRAFFIC** tab.

The WAN TRAFFIC pane displays, showing the total uploaded and downloaded WAN traffic that the router processed since it started or since you reset the traffic meter.

Monitor the router throughput

To monitor the download throughput and upload throughput on the router:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

   The DOWNLOAD THROUGHPUT pane and UPLOAD THROUGHPUT pane display the throughput rate in Bytes per second (B/s, see the vertical rate bar) over time (see the horizontal time bar) for the WAN port, for all LAN port together, and for each LAN port individually.

4. To view more information about the throughput, point to a node on the horizontal time bar.

   A pop-up window opens and displays specific throughput information.

5. To exclude an individual port from a graph, click the colored circle icon for an individual port.

   The traffic information for the port is excluded from the graph.

6. To refresh the information on the page, click the **Refresh** button.

8
Set Up VPN Connections

ATTENTION: The router is designed to provide virtual private networking (VPN) using the NETGEAR Insight mobile app and Cloud Portal. For information about how you can use NETGEAR Insight to set up Instant VPN connections, see the NETGEAR knowledge base articles at netgear.com/support/ and the Insight user manual at downloads.netgear.com/files/GDC/Insight/Insight_UM_EN.pdf. For general information about NETGEAR Insight, visit netgear.com/insight.

If you do *not* use NETGEAR Insight, you can do the following:

- **Use IPSec VPN**. With IPSec VPN, you can set up a site-to-site VPN connection between a NETGEAR BR500 and another VPN router, each at a different site. This setup lets you connect two local LANs and join separate networks together as if they were physically connected and colocated.

- **Use OpenVPN**. With OpenVPN software, you can set up a client-to-gateway VPN connection and remotely access an office or site at which a NETGEAR BR500 router is installed.

This chapter describes how to set up IPSec VPN on the router and how to set up OpenVPN on both the router and on a computer or mobile device.

The chapter includes the following sections:

- About Instant VPN connections
- Set up an IPSec VPN connection
- Set up an OpenVPN connection

Note: For information about monitoring VPN devices and connections, see Monitor the router and the router network on page 117.

About Instant VPN connections

A virtual private network (VPN) connection lets remote users securely access a network over the Internet. The network can be at an office or headquarters, behind the firewall that the router provides.

The router is designed to function with NETGEAR Insight as an Insight managed device and to provide Instant VPN with the NETGEAR Insight mobile app and Cloud Portal.

With Instant VPN, the router supports the following types of VPN connections:

- **Client-to-gateway VPN connection**. VPN access in which remote users access a protected network. The device is the client, and the router is the gateway.

  Note: If you use Instant VPN, the Mac VPN client does not function in a client-to-gateway VPN connection.

- **Site-to-site VPN connection**. VPN access with two routers, each at a different site, which lets you connect two local LANs and separate networks together as if they were physically connected and colocated.

For information about NETGEAR Insight and how you can use the NETGEAR Insight mobile app and Cloud Portal to discover the router, add it to an Insight network, and use Instant VPN on the router to set up VPN connections, see the following:

- NETGEAR knowledge base articles at netgear.com/support/

- Insight user manual at downloads.netgear.com/files/GDC/Insight/Insight_UM_EN.pdf

For general information about NETGEAR Insight, visit netgear.com/insight.

Note: For a site-to-site connection, you can simultaneously establish an independent Instant VPN connection and an independent IPSec VPN connection. However, do not use an IPSec VPN connection as a backup connection for an Instant VPN connection, or the other way around. These simultaneous VPN connections do *not* provide redundancy or load balancing, nor are they supposed to do so because these modes of operation are not supported.

Set up an IPSec VPN connection

You can set up a site-to-site VPN tunnel using IP security (IPSec) between two VPN routers. You do not need to install software such as OpenVPN to establish an IPSec tunnel, but the router at the other site must be capable of supporting IPSec VPN. The IPSec settings on each VPN router must be consistent for the tunnel to function. That is,

both VPN routers must use the same type of tunnel authentication and negotiation exchange settings and tunnel encapsulation settings.

Note: For a site-to-site IPSec VPN connection, the router must be running firmware version 5.5.1.1 or a later firmware version. If you use two BR500 routers for your site-to-site IPSec VPN connection, both BR500 routers must be running the same firmware version.

When you set up an IPSec VPN policy for a tunnel between two VPN routers, you are defining the following IPSec VPN settings:

- **IP address settings**. The address settings that allow the VPN routers to contact each other. These include the WAN IP address of the remote VPN router, the remote LAN subnet of the remote VPN router, and the local LAN subnet of the local VPN router (that is, *your* router).

- **Phase 1 settings**. The Internet Key Exchange (IKE) Phase 1 settings that define the authentication and negotiation exchange between the two VPN routers before the IPSec tunnel is established. You must specify the pre-shared key (basically, a password) and encryption and authentication algorithms on both VPN routers so that the communication between the routers can be authenticated and is secure. For this phase, the routers use the following:

  - For encryption, an encryption algorithm (MD5 or an SHA version)

  - For authentication, a hash algorithm (3DES or an AES version)

  - For verification and exchange of keys, a Diffie-Hellman group algorithm from DH1 (less secure) to DH24 (more secure)

  We recommend that you use the default Phase 1 settings, but you can customize the Phase 1 settings for increased security.

- **Phase 2 settings**. The IKE Phase 2 settings that define how the IPSec tunnel is set up and encapsulated between the two VPN routers and how the tunnel traffic is kept secure. To guard against modification of the traffic that is transported through the tunnel, the routers use an encapsulation protocol, encryption algorithm, and an integrity check algorithm.
  For this phase, the routers use the following:

  - To secure the tunnel, the Encapsulating Security Protocol (ESP)

  - For encryption, an encryption algorithm (MD5 or an SHA version)

  - For an integrity check (that is, to verify that the network traffic is not altered during transmission in the tunnel), a hash algorithm (3DES or an AES version)

  - As an option for verification and exchange of keys, a Diffie-Hellman group algorithm from DH1 (less secure) to DH24 (more secure)

We recommend that you use the default Phase 2 settings, but you can customize the Phase 2 settings for increased security.

IMPORTANT: The settings that you define on both VPN routers must match. That is, on each VPN router, the IP addressing scheme must be coordinated with the other VPN router, the IKE Phase 1 settings must be identical on both VPN routers, and the IKE Phase 2 settings must be identical on both VPN routers.

Add an IPSec VPN policy on the router

When you add an IPSec VPN tunnel, you must define the name for the tunnel, the IP addresses, the pre-shared key, and either keep the Internet Key Exchange (IKE) version 1 (IKE1) advanced settings (which are the Phase 1 settings) or select the IKE version 2 (IKE2) advanced settings (which are the Phase 2 settings).

The advanced settings *are* the Phase 1 and Phase 2 settings. We recommend that you use the default Phase 1 and Phase 2 settings. However, for increased security, or if your network environments require it, you can customize these settings (see Customize Phase 1 and Phase 2 settings for an IPSec policy on page 131).

The following table shows the default Phase 1 and Phase 2 settings that the router uses.

Table 2. Default Phase 1 and Phase 2 settings for IKE1 and IKE2

Setting	Defaults
Phase 1 settings	
Proposal	md5, 3des, dh1
Exchange Mode	Main Mode
Negotiation Mode	Initiator/Responder Mode
SA Lifetime	28800 seconds
DPD	Enabled
DPD Interval	10 seconds
Phase 2 settings	
Proposal	esp, sha1, aes256
PFS (IKE1 only)	Disabled
SA Lifetime	28800 seconds

For more information about these default settings, see Customize Phase 1 and Phase 2 settings for an IPSec policy on page 131.

To add an IPSec VPN policy on the router and use the default Phase 1 and Phase 2 settings:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPSec VPN**.

   The IPSec VPN Policy List displays.

5. Click the **Add** button.

   The Add Policy slide-out panel opens.

6. In the **Policy Name** field, enter a name.

   The name is used to identify the VPN policy and can be from 1 to 32 characters.

   Note: The selection from the **Mode** menu is always **Net-to-Net**.

7. In the **Remote Gateway** field, enter the IP address or domain name of the remote VPN router.

   The IP address is usually a public (WAN) IP address or DNS name. A DNS name can be up to 255 characters.

8. Specify the remote LAN and local LAN settings:

   - **Remote Subnet**. The LAN IP subnet address of the remote VPN router.

   - **Remote Mask**. The LAN IP subnet mask of the remote VPN router.

   - **Local Subnet**. The LAN IP subnet address of the local VPN router (that is, the router that you are currently configuring).

   - **Local Mask**. The LAN IP subnet mask of the local VPN router (that is, the router that you are currently configuring).

Note: The remote LAN IP address and the local LAN IP address cannot be in the same subnets. For example, if the local subnet is 192.168.1.x, then the remote subnet can be 192.168.2.x. but cannot be 192.168.1.x.

9. In the **Pre-shared Key** field, enter the key.

   This key must be a minimum of 8 characters and can be a maximum of 128 characters.

   You must the same key on the remote VPN router.

10. Either leave the **IKE1** radio button selected or select the **IKE2** radio button.

    If the remote VPN router also supports IKE2, we recommend that you use IKE2.

11. Click the **Apply** button.

    Your settings are saved. The VPN policy is added to the IPSec VPN Policy List.

    The VPN tunnel that is defined by the new VPN policy is disabled (indicated by a red icon in the Status column). After you define the VPN policy on the remote router, the VPN tunnel can be enabled (indicated by a green icon in the Status column).

Customize Phase 1 and Phase 2 settings for an IPSec policy

We recommend that you use the default Phase 1 and Phase 2 settings. However, if you need greater security, or for specific network environments, you can customize these settings.

For information about the default Phase 1 and Phase 2 settings, see the table in Add an IPSec VPN policy on the router on page 129.

Note: Customizing the Phase 1 and Phase 2 settings is an advanced task that requires some knowledge about IPSec policies.

To customize the Phase 1 and Phase 2 settings for an IPSec policy:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > IPSec VPN**.

    The IPSec VPN Policy List displays.

5. In the IPSec VPN Policy List, click the blue **pencil** icon for the VPN policy that you want to edit.

    The Edit Policy slide-out panel opens.

6. Click the **Advanced Settings** link.

    The panel adjusts.

7. In the Phase 1 Settings section, customize the settings as described in the following table.

Table 3. Phase 1 settings

Setting	Options		
Proposal (You can specify up to four proposals.)	Encryption algorithm	Authentication algorithm	Diffie-Hellman group algorithm
	md5 (**default**)	3des (**default**)	no (= DH is disabled)
	sha1, sha256, sha384, or sha512	aes128, aes192, or aes256	dh1 (**default**), dh2, dh5, dh14, dh15, dh16, dh17, dh18, dh19, dh20, dh21, dh22, dh23, or dh24
	Note: The higher the SHA version, AES version, and DG group, the more secure the exchange.		
Exchange Mode	**Main Mode**. This mode is slower than the aggressive mode but more secure. This is the default mode. **Aggressive Mode**. This mode is faster than the main mode but less secure. This mode is not available for IKE2.		
Negotiation Mode	**Initiator/Responder Mode**. The router can both initiate a connection to the remote VPN router and respond to an IKE request from the remote VPN router. This is the default mode. **Responder Mode**. The router can respond to an IKE request from the remote VPN router.		
SA Lifetime	The period in seconds for which the IKE security association (SA) is valid. When the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours). The period can be between 600 and 604800 seconds.		

Table 3. Phase 1 settings (Continued)

Setting	Options
DPD	Dead Peer Detection (DPD) is enabled by default. When the router detects an IKE connection failure, it deletes the IPSec and IKE SA and forces a reestablishment of the connection. Specify the detection period in the DPD Interval field.
DPD Interval	The period in seconds between consecutive DPD messages. The default is 10 seconds. The period can be between 1 and 300 seconds.

8. In the Phase 2 Settings section, customize the settings as described in the following table.

Table 4. Phase 2 settings

Setting	Options		
Proposal (You can specify up to four proposals.)	Encapsulation protocol	Encryption algorithm	Authentication algorithm
	esp (**default** and only option)	md5	3des
		sha1 (**default**), sha256, sha384, or sha512	aes128, aes192, or aes256 (**default**)
	Note: The higher the SHA and AES versions, the more secure the exchange.		
PFS	For IKE1, you can enable Perfect Forward Secrecy (PFS) and select a Diffie-Hellman (DH) group algorithm. For IKE2, you cannot enable PFS.		
	no (= DH is disabled, **default**)		
	dh1, dh2, dh5, dh14, dh15, dh16, dh17, dh18, dh19, dh20, dh21, dh22, dh23, or dh24		
	Note: The higher the DH group, the more secure the exchange.		
SA Lifetime	The period in seconds for which the IKE security association (SA) is valid. When the period times out, the next rekeying occurs. The default is 28800 seconds (8 hours). The period can be between 600 and 604800 seconds.		

9. Click the **Apply** button.
   Your settings are saved.

   Note: If you changed the Phase 1 and Phase 2 settings, make sure that you change them accordingly on the remote VPN router.

Enable or disable an IPSec VPN tunnel

You can enable or disable an IPSec VPN tunnel.

To enable or disable an IPSec VPN tunnel on the router:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPSec VPN**.

   The IPSec VPN Policy List page displays.

5. For the VPN tunnel that you want enable or disable, do one of the following:

   • **Enable**. Click the button in the Operation column so that the button moves to the right and displays blue.

   • **Disable**. Click the button in the Operation column so that the button moves to the left and displays gray.

6. Click the **Refresh** button.

   The new tunnel status displays:

   • If the tunnel is enabled and established, the icon in the Status column display green.

   • If the tunnel is disabled, the icon in the Status column display red.

   Note: If you enabled the tunnel but the icon still displays red after one minute, a connectivity problem might exist between the VPN routers, or the settings might not match on the VPN routers.

Change an existing IPSec VPN policy

You can change the settings for an existing IPSec VPN policy.

To change the settings for an existing IPSec VPN policy on the router:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > IPSec VPN**.

    The IPSec VPN Policy List page displays.

5. In the IPSec VPN Policy List, click the blue **pencil** icon for the VPN policy that you want to change.

    The Edit Policy slide-out panel opens.

6. Change the settings as needed.

    For information about the basic settings, see Add an IPSec VPN policy on the router on page 129.

    For information about customizing the Phase 1 and Phase 2 settings, see Customize Phase 1 and Phase 2 settings for an IPSec policy on page 131.

7. Click the **Apply** button.

    Your settings are saved.

    Note: When you change the settings, make sure that you change them accordingly on the remote VPN router.

Remove an existing IPSec VPN policy

If you no longer need an IPSec VPN policy, you can permanently remove it.

To remove an existing IPSec VPN policy from the router:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > IPSec VPN**.

   The IPSec VPN Policy List page displays.

5. In the IPSec VPN Policy List, click the red **trash can** icon for the VPN policy that you want to remove.

   A warning pop-up window opens.

6. Click the **OK** button.

   The VPN policy is removed.

Set up an OpenVPN connection

The type of virtual private network (VPN) access in which remote users access a protected network is called a client-to-gateway tunnel. The computer is the client, and the router is the gateway. If you are not using NETGEAR Insight and you want to allows users to access the router over a VPN connection, you must enable and configure OpenVPN service on the router. Remote users must install and run OpenVPN client software on their computer or mobile device.

OpenVPN requires a static IP address or DDNS service on the router to enable a remote client such as a computer or mobile device to connect with the router. (If you use the router for VPN connections in an Insight managed network with the NETGEAR Insight mobile app or Cloud Portal, the router doesn't require a static IP address and doesn't need to use DDNS.)

If the router uses a static WAN IP address that never changes, OpenVPN can use that IP address to connect to the network over a VPN connection.

If the router does not use a static WAN IP address, you can use a DDNS service for the router and register for an account with a host name (also referred to as a domain name). A remote client such as a computer or mobile device can use that host name to connect with the router and access the network over a VPN connection. For more information, see <u>Set Up and Manage Dynamic DNS</u> on page 42.

Enable and configure OpenVPN on the router

You must enable OpenVPN and specify the OpenVPN service settings on the router before someone can set up a VPN connection using OpenVPN.

Note: Make sure that remote clients install their VPN configuration files after you configure OpenVPN on the router. If you make changes to the OpenVPN configuration on the router, the VPN configuration files that the remote clients use might change, requiring the remote clients to download and install the new VPN configuration files.

To enable and configure OpenVPN on the router:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. Select **ADVANCED > Open VPN**.

    The Open VPN page displays.

5. Select the **Open VPN Service** check box.

We recommend that you use the default TUN mode and TAP mode settings. However, if you know that you need other settings, you can change the TUN mode and TAP mode settings by doing the following:

- To change the TUN mode service type, select the **UDP** or **TCP** radio button.

- To change the TUN mode service port, type the port number that you want to use in the field.
  The default port number is 12973.

- To change the TAP mode service type, select the **UDP** or **TCP** radio button.

- To change the TAP mode service port, type the port number that you want to use in the field.
  The default port number is 12974.

6. Specify how client VPN connections can be used on the router by selecting one of the following radio buttons:

- **Auto**. The router automatically uses the VPN service only for necessary access, that is, the router allows access to sites and services that would not be accessible without a VPN connection. However, if some sites or services are not accessible to the VPN client, or if a user cannot access some sites on the Internet, select another radio button.

- **All sites on the Internet & BR500 Network**. The VPN client can access the Internet and all sites and services on the router network, that is, behind the router firewall. Accessing the Internet remotely through a VPN connection might be slower than accessing the Internet directly.

- **BR500 Network only**. The VPN client can access all sites and services on the router network, that is, behind the router firewall, but cannot access the Internet.

7. Click the **Apply** button.
   Your settings are saved. OpenVPN service is enabled on the router.

   Users must install and set up OpenVPN software on their computer or mobile device before they can establish a VPN connection to the router.

Install OpenVPN client software on a remote client

To establish a VPN connection to the router using OpenVPN software, a remote client must install OpenVPN client software on their computer or mobile device. A remote client can install this software on a Windows computer, Mac computer, iOS device, or Android device.

Install the OpenVPN client utility and VPN configuration files on a Windows-based computer To download and install the OpenVPN client utility and the router's VPN configuration files on a Windows-based computer:

1. Visit openvpn.net/index.php/download/community-downloads.html, download the OpenVPN client utility for a Windows-based computer, and install it on the Windows-based computer.

   You might need administrative privileges to install the OpenVPN client utility.

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

3. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

5. Select **ADVANCED > Open VPN**.

   The Open VPN Service page displays.

6. Make sure that the **Open VPN Service** check box is selected.

   For more information, see Enable and configure OpenVPN on the router on page 137.

7. In the OpenVPN configuration package download section, click the **For Windows** button, and download the router's VPN configuration files.

8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.

9. Modify the VPN interface name to NETGEAR-VPN by doing the following:

   a. In Windows, open Network Connection or Network and Sharing Center.

      The network connection information displays.

   b. In the local area connection list, find the local area connection with the device name TAP-Windows Adapter.

   c. Change the name of the associated local area connection to **NETGEAR-VPN**.

      Make sure that you change the name of the local area connection, *not* the device name (TAP-Windows Adapter).

If you do not change the local area connection name, the VPN connection to the router will fail.

The computer is now ready to for you to set up a VPN connection to the router.

For more information about using OpenVPN on a Windows-based computer, visit openvpn.net/index.php/open-source/documentation/howto.html#quick.

Install the OpenVPN client utility and VPN configuration files on a Mac

To download and install the OpenVPN client utility and the router's VPN configuration files on a Mac:

1. Visit code.google.com/p/tunnelblick/, download the OpenVPN client utility for a Mac, and install it on the Mac.

   You might need administrative privileges to install the OpenVPN client utility.

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

3. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

5. Select **ADVANCED > Open VPN**.

   The Open VPN Service page displays.

6. Make sure that the **Open VPN Service** check box is selected.

   For more information, see Enable and configure OpenVPN on the router on page 137.

7. In the OpenVPN configuration package download section, click the **For MacOSX** button, and download the router's VPN configuration files.

8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.

   The Mac is now ready to for you to set up a VPN connection to the router.

   For more information about using OpenVPN on a Mac computer, visit openvpn.net/index.php/access-server/docs/admin-guides/183-how-to-connect-to-access-server-from-a-mac.html.

Install the OpenVPN client utility and VPN configuration files on an iOS device

To download and install the OpenVPN client utility and the router's VPN configuration files on an iOS device:

1. On your iOS device, visit the Apple app store and download and install the OpenVPN Connect app.

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

3. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

5. Select **ADVANCED > Open VPN**.

   The Open VPN Service page displays.

6. Make sure that the **Open VPN Service** check box is selected.

   For more information, see <u>Enable and configure OpenVPN on the router</u> on page 137.

7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the router's VPN configuration files to your iOS device or computer.

   If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your iOS device.

   The configuration files include the `.ovpn` file.

8. On your iOS device, open the `.ovpn` file, select the OpenVPN Connect app, and import the `.ovpn` file.

   Your iOS device is now ready to for you to set up a VPN connection to the router.

   For more information about using OpenVPN on an iOS device, visit <u>vpngate.net/en/howto_openvpn.aspx#ios</u>.

Install the OpenVPN client utility and VPN configuration files on an Android device

To download and install the OpenVPN client utility and the router's VPN configuration files on an Android device:

1. On your Android device, visit the Google Play Store and download and install the OpenVPN Connect app.

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

3. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

5. Select **ADVANCED > Open VPN**.

   The Open VPN Service page displays.

6. Make sure that the **Open VPN Service** check box is selected.

   For more information, see Enable and configure OpenVPN on the router on page 137.

7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the router's VPN configuration files to your Android device or computer.

   If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your Android device.

   The configuration files include the `.ovpn` file.

8. On your Android device, start the OpenVPN Connect app, and search for and import the `.ovpn` file.

   Your Android device is now ready to for you to set up a VPN connection to the router.

   For more information about using OpenVPN on an Android device, visit vpngate.net/en/howto_openvpn.aspx#android.

9

Manage Port Forwarding and Port Triggering Traffic Rules

As an advanced function of the firewall, you can use port forwarding and port triggering to set up port traffic rules for Internet services and applications. These rules apply specifically to ports. You need networking knowledge to set up port traffic rules.

This chapter includes the following sections:

- Manage port forwarding to a local server for services and applications
- Manage port triggering for services and applications

Manage port forwarding to a local server for services and applications

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

The router 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 router forwards all other incoming protocols (see Set up a default DMZ server on page 48).

Forward incoming traffic for a default service or application

You can forward traffic for a default service or application to a computer on your network.

To forward incoming traffic for a default service or application:

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 receive the same IP address. To specify this setting, use the reserved IP address feature. See Manage reserved LAN IP addresses on page 85.

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

4. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

5. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

6. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

    The Port Forwarding / Port Triggering page displays.

7. Make sure that the **Port Forwarding** radio button is selected.

8. From the **Service Name** menu, select the service or application.

   If the service or application that you want to add is not in the list, create a port forwarding rule with a custom service or application (see <u>Add a port forwarding rule for a custom service or application</u> on page 145).

9. In the **Server IP Address** field, enter the IP address of the computer that must provide the service or that runs the application.

10. Click the **Add** button.

    Your settings are saved and the rule is added to the table.

Add a port forwarding rule for a custom service or application

The router lists default services and applications that you can use in port forwarding rules. If the service or application is not predefined, you can add a port forwarding rule with a custom service or application.

To add a port forwarding rule with a custom service or application:

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

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

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

3. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

5. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

6. Make sure that the **Port Forwarding** radio button is selected.

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

The Add Custom Services slide-out panel opens.

8. Set up a new port forwarding rule for a custom service or application by specifying the following settings:

- **Service Name**. Enter the name of the custom service or application.

- **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.

- **External port range**. If the service or application uses a single port, enter the port number in the **External port range** field. If the service or application uses a range or ranges of ports, specify the range in the **External port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.

- **Internal port range**. Specify the internal port or ports by one of these methods:

  - If the external and internal port or ports are identical, leave the **Use the same port range for Internal port** check box selected.

  - If the service or application uses a single port, clear the check box and enter the port number in the **Internal port range** field.

  - If the service or application uses a range or ranges of ports, clear the check box and specify the range in the **Internal port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.

- **Internal IP address**. Either enter an IP address in the **Internal IP address** field or select the radio button for an attached device that is listed in the table.

9. Click the **Apply** button.

Your settings are saved. The rule is added to the table on the Port Forwarding / Port Triggering page.

Change a port forwarding rule

You can change an existing port forwarding rule.

To change a port forwarding rule:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

5. Make sure that the **Port Forwarding** radio button is selected.

6. In the table, select the radio button for the service or application name.

7. Click the **Edit Service** button.

   The Edit Forwarding Service slide-out panel opens.

8. Change the settings.

   For information about the settings, see Add a port forwarding rule for a custom service or application on page 145.

9. Click the **Apply** button.

   Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Remove a port forwarding rule

You can remove a port forwarding rule that you no longer need.

To remove a port forwarding rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.
    The Port Forwarding / Port Triggering page displays.

5. Make sure that the **Port Forwarding** radio button is selected.

6. In the table, select the radio button for the service or application name.

7. Click the **Delete Service** button.
    A warning pop-up window opens.

8. Click the **OK** button.
    The rule is removed from the table.

    A default rule remains available in the **Service Name** menu. A custom rule is removed.
    If you want to reinstate the custom rule, you must redefine it.

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 router always gives your web server an IP address of 192.168.1.33.

2. On the Port Forwarding / Port Triggering page, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**.
    HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and specify that name on the Dynamic DNS page of the router.
    Dynamic DNS makes it much easier to access a server from the Internet because you can enter the name in the web browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the router implements a port forwarding rule

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

1. When you enter 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 router.

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

2. The router receives the message and finds your port forwarding rule for incoming port 80 traffic.

3. The router changes the destination IP address in the message to 192.168.1.123 and sends the message to that computer.

4. Your web server at IP address 192.168.1.123 receives the request and sends a reply message to your router.

5. Your router performs Network Address Translation (NAT) on the source IP address and sends the reply through the Internet to the computer or mobile device that sent the web page request.

Manage port triggering for services and applications

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

• An application must use port forwarding to more than one local computer (but not simultaneously).

• An application must open incoming ports that are different from the outgoing port.

With port triggering, the router monitors traffic to the Internet from an outbound "trigger" port that you specify. For outbound traffic from that port, the router saves the IP address of the computer that sent the traffic. The router 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 use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, enable Universal Plug-N-Play (UPnP, see <u>Improve network connections with Universal Plug and Play</u> on page 98).

Add a port triggering rule

The router does not provide default services and applications for port triggering rules. You must define a custom service or application for each port triggering rule.

To add a port triggering rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

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

   The port triggering settings display.

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

   The Add Triggering Service slide-out panel opens.

7. Set up a new port triggering rule with a custom service or application by specifying the following settings:

   - **Service Name**. Enter the name of the custom service or application.

   - **Service User**. From the **Service User** menu, select **Any**, or select **Single address** and enter the IP address of one computer:

     - **Any**. This is the default setting and allows any computer on the Internet to use this service.

- **Single address**. Restricts the service to a particular computer. Enter the IP address in the **Service IP** fields, which become available with this selection from the menu.

- **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application.

- **Triggering Port**. Enter the number of the outbound traffic port that must open the inbound ports.

- **Service Type**. Select the protocol (**TCP** or **UDP**) that is associated with the inbound connection. If you are unsure, select **TCP/UDP**.

- **Starting Port**. Enter the start port number for the inbound connection.

- **Ending Port**. Enter the end port number for the inbound connection.

8. Click the **Apply** button.

   Your settings are saved and the rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Change a port triggering rule

You can change an existing port triggering rule.

To change a port triggering rule:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

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

The port triggering settings display.

6. In the Port Triggering Portmap Table, select the radio button for the service or application name.

7. Click the **Edit Service** button.

The Edit Triggering Service slide-out panel opens.

8. Change the settings.

For information about the settings, see Add a port triggering rule on page 150.

9. Click the **Apply** button.

Your settings are saved. The changed rule displays in the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Remove a port triggering rule

You can remove a port triggering rule that you no longer need.

To remove a port triggering rule:

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

2. Enter **https://www.routerlogin.net**.

Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

A login window opens.

3. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

The Port Forwarding / Port Triggering page displays.

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

The port triggering settings display.

6. In the Port Triggering Portmap Table, select the radio button for the service or application name.

7. Click the **Delete Service** button.

A warning pop-up window opens.

8. Click the **OK** button.

   The rule is removed from the Port Triggering Portmap Table. If you want to reinstate the rule, you must redefine it.

Specify the time-out for port triggering

The time-out period for port triggering controls how long the inbound ports stay open when the router detects no activity. A time-out period is required because the router cannot detect when the service or application terminates.

To specify the time-out for port triggering:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

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

   The port triggering settings display.

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

   The default setting is 20 minutes.

7. Click the **Apply** button.

   Your settings are saved.

Disable port triggering

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering rules.

To disable port triggering:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **ADVANCED > Firewall > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

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

   The port triggering settings display.

6. Select the **Disable Port Triggering** check box.

   If this check box is selected, the router does not apply port triggering rules even if you specified them.

7. Click the **Apply** button.

   Your settings are saved.

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 router 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 router, "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 router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and observing the destination port number of 6667, your router creates another session entry to send any incoming port 113 traffic to your computer.

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

6. When your router 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 router restores the original address information replaced by NAT and sends this reply message to your computer.

7. When your router 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 router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

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

10

Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with your router. If you do not find the solution here, check the NETGEAR support site at netgear.com/support for product and contact information.

The chapter contains the following sections:

- Reboot the router from the local browser interface
- Quick tips
- Troubleshoot with the LEDs
- You cannot log in to the router
- You cannot access the Internet
- Changes are not saved
- Troubleshoot your network using the ping utility of your computer

Reboot the router from the local browser interface

You or NETGEAR technical support can reboot the router from its local browser interface, either locally or remotely, for example, when the router seems to be unstable or is not operating normally.

To reboot the router from its local browser interface:

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

2. Enter **https://www.routerlogin.net**.

    Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

    A login window opens.

3. Enter the router user name and password.

    The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

    The Dashboard displays.

4. At the top of the page, click the **Reboot** button.

    A pop-up warning window opens.

5. Click the **OK** button.

    The router reboots.

Quick tips

This section describes tips for troubleshooting some common problems.

Sequence to restart your network

If you must restart your network, follow this sequence:

1. Turn off and unplug the modem.

2. Turn off the router.

3. Plug in the modem and turn it on. Wait two minutes.

4. Turn on the router and wait two minutes.

Check Ethernet cable connections

If the router does not power on, make sure that the Ethernet cables are securely plugged in. The Internet LED on the router is lit if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on. If one or more powered-on devices are connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED lights.

Network settings

Make sure that the network settings of the computer with which you want to connect to the router are correct. Wired computers (and mobile devices that are connected to an access point that is directly connected to the router) must use network IP addresses on the router's LAN network. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.

Some service providers require you to use the MAC address of the computer that was initially registered on the account, but this is an uncommon situation. You can view the MAC address on the Attached Devices page (see <u>View devices currently on the network</u> on page 118).

Troubleshoot with the LEDs

You can troubleshoot by checking the LEDs.

For complete information about the router LEDs, see the hardware installation guide, which you can download by visiting <u>netgear.com/support/download/</u>.

Standard LED behavior when the router is powered on

After you turn on power to the router, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is lit.

2. After about two minutes, verify the following:

   - The Power LED is solid green.

   - The WAN LED is solid or blinking green.

   - The LAN LED for a powered-on device that attached to the corresponding LAN port is solid or blinking green.

   You can use the LEDs on the front panel of the router for troubleshooting.

Power LED is off

This could occur for a number of reasons. Check the following:

- Make sure that you pressed the **On/Off** power button on the back of the router.

- Make sure that the power adapter is securely connected to your router and securely connected to a working power outlet.

- Make sure that you are using the power adapter that NETGEAR supplied for this product.

Power LED stays amber

When the router is turned on, the Power LED turns amber for up to two minutes and then turns green. If the LED does not turn green, this indicates a problem with the router.

If the Power LED is still amber three minutes after you turn on power to the router, do the following:

- Reboot the router to see if the router recovers.

- If the router does not recover, press and hold the **Reset** button to return the router to its factory default settings. For more information, see Use the Reset button on page 107.

If the error persists, a hardware problem might be the cause. Contact technical support at netgear.com/support.

WAN LED or LAN LEDs are off

If either the WAN LED or LAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connection is secure at the router and at the modem that is connected to the WAN port.

- Make sure that the Ethernet cable connections are secure at the router and at the devices that are connected to the LAN ports.

- Make sure that power is turned on to the connected modem and connected devices.

- Be sure that you are using the correct cables.

When you connect the router's WAN port to a modem, use the cable that was supplied with the modem. This cable can be a standard straight-through Ethernet cable or an Ethernet crossover cable.

You cannot log in to the router

If you are unable to log in to the router from a computer on your local network and use the router's local browser interface, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router.

- Make sure that the IP address of your computer is on the same subnet as the LAN subnet or the router. If you are using the recommended addressing scheme, your computer's address is in the range of 192.168.1.2 to 192.168.1.254.

- Make sure that your computer can reach the router's DHCP server. 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 router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, use the NETGEAR Insight mobile app or an IP scanner application to detect the IP address. If you still cannot find the IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. For more information, see Use the Reset button on page 107.

- 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.

- Try quitting the browser and launching it again.

- Make sure that you are using the correct login information. The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.

You cannot access the Internet

If you can access your router but not the Internet, check if the router can obtain an IP address from your Internet service provider (ISP).

Check the WAN IP address

Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Dashboard.

To check the WAN IP address:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see Log in to the local browser interface on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. In the PORTS STATUS pane, click the **CONNECTION STATUS** tab.

   The connection status information displays.

   Note: The information that displays depends on the type of Internet connection. If the Internet connection is PPPoE, PPTP, or L2TP, other information might display than if the Internet connection is an IP address that the ISP assigns dynamically (the most common situation).

5. Check to see that a valid IP address is shown in the IP address field..

   If 0.0.0.0 is shown, your router did not obtain an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your modem to recognize your new router by restarting your network. For more information, see Sequence to restart your network on page 157.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, the login name and password might be set incorrectly.

- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name on the WAN Setup page (see Manually set up the router Internet connection on page 22).

- 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 router's MAC address.

  - Configure your router to clone your computer's MAC address.

If your router obtained an IP address, but your computer does not load any web pages from the Internet, it might be for one or more 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 router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- The router might not be configured as the TCP/IP gateway on your computer.
  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address.

- You might be running login software that is no longer needed.
  If your ISP provided a program to log you in to the Internet, you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**. Other browsers provide similar options.

Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

To troubleshoot a PPPoE connection:

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

2. Enter **https://www.routerlogin.net**.

   Your browser might display a security message, which you can ignore. For more information, see <u>Log in to the local browser interface</u> on page 16.

   A login window opens.

3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. If you didn't change the password, enter **password**. The user name and password are case-sensitive.

   The Dashboard displays.

4. In the PORTS STATUS pane, click the **CONNECTION STATUS** tab.

   The connection status information displays.

   Note: The information that displays depends on the type of Internet connection. If the Internet connection is PPPoE, PPTP, or L2TP, other information might display than if the Internet connection is an IP address that the ISP assigns dynamically (the most common situation).

5. Check the information to see if your PPPoE connection is up and working.

   If the router is not connected, click the **Connect** button.

   The router continues to attempt to connect indefinitely.

6. If you cannot connect after several minutes, the router might be set up with an incorrect login name, password, or service name, or your ISP might be experiencing a provisioning problem.

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

Troubleshoot Internet browsing

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

- The traffic meter is enabled, and the limit was reached.
  By configuring the traffic meter not to block Internet access when the traffic limit is reached, you can resume Internet access (see Unblock the traffic meter after the traffic limit is reached on page 115). If your ISP sets a usage limit, they might charge you for the overage.

- 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 router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- The router might not be configured as the default gateway on your computer. Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.

- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection**. Other browsers provide similar options.

Changes are not saved

If the router does not save the changes that you make through the local browser interface, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab, or your changes are lost.

- Click the **Refresh** button in the local browser interface. It is possible that the changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot your network using the ping utility of your computer

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network using the ping utility in your computer.

Test the LAN path from your computer to the router

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

To ping the router from a Windows-based computer:

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 router, as in this example:

    ping www.routerlogin.net

3. Click the **OK** button.

    You see a message like this one:

    ```
    Pinging <IP address > with 32 bytes of data
    ```

    If the path is working, you see this message:

    ```
    Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
    ```

    If the path is not working, you see this message:

    ```
    Request timed out
    ```

If the path is not functioning correctly, one of the following problems might be present:

*   Wrong physical connections
    Make sure that the numbered LAN LED is lit for the LAN port to which your computer is connected.
    Check to see that the appropriate LEDs are lit for your network devices. If your router 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 router.

*   Wrong network configuration
    Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
    Verify that the IP addresses for your router and your computer are correct and that the addresses are on the same subnet.

Test the path from your computer to a remote device

To test the path from a Windows-based computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.

2. In the Windows Run window, type

   ping -n 10 *<IP address>*

   in which *<IP address>* is the IP address of a remote device such as your ISP DNS server.

   If the path is functioning correctly, messages display that are similar to those shown in Test the LAN path from your computer to the router on page 165.

3. If you do not receive replies, check the following:

   - Check to see that IP address of your router is listed as the default gateway for your computer. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the router is listed as the default gateway.

   - Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

   - Check to see that your modem is connected and functioning.

   - If your ISP assigned a host name to your computer, enter that host name as the account name on the WAN Setup page (see Manually set up the router Internet connection on page 22).

   - 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. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If your ISP does this, configure your router to "clone" or "spoof" the MAC address from the authorized computer.

A

Supplemental information

This appendix includes technical information about your router.

The appendix covers the following topics:

- Factory settings
- Technical specifications

Factory settings

You can reset the router to the factory default settings that are shown in the following table.

For more information about resetting the router to its factory settings, see <u>Return the router to its factory default settings</u> on page 107.

The following table shows the factory default settings.

Table 5. Router factory default settings

Feature	Default Settings
Router login	
User login URL	www.routerlogin.net (or www.routerlogin.com or 192.168.1.1)
User name (case-sensitive)	admin
Login password (case-sensitive)	password
Internet connection	
WAN MAC address	Use default hardware address
WAN MTU size	Determined by the protocol that is used for the Internet connection (see <u>Change the MTU size</u> on page 40)
Port speed	AutoSensing
Local network (LAN)	
LAN IP address	192.168.1.1
Subnet mask	255.255.255.0
DHCP server	Enabled
DHCP range	192.168.1.2 to 192.168.1.254 for the default LAN subnet (LAN1)
DHCP starting IP address	192.168.1.2 for the default LAN subnet (LAN1)
DHCP ending IP address	192.168.1.254 for the default LAN subnet (LAN1)
VLANs	VLAN 1 with all LAN ports as untagged members VLAN 2 with the WAN port as an untagged member
DMZ	Disabled
Time zone	North America: Pacific Standard Time Europe: GMT Other continents: Varies by region

Table 5. Router factory default settings (Continued)

Feature	Default Settings
Time adjusted for daylight saving time	Disabled
Firewall and WAN security	
Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
Outbound (communications going out to the Internet)	Enabled (all)
Source MAC filtering	Disabled
Port scan and DoS protection	Enabled
Respond to ping on Internet port	Disabled
IGMP proxying	Disabled
VPN pass-through	Enabled, nonconfigurable
SIP ALG	Enabled
NAT filtering	Secured
Traffic rules	None set up
Access control	None set up
Port rules	None set up
Blocked sites or services	None set up

Technical specifications

The following table shows the technical specifications.

For more technical specifications, see the data sheet, which you can download by visiting netgear.com/support/download/.

Table 6. Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, Dynamic DNS, and UPnP
Power adapter (varies by region)	North America, UK, Australia, and Europe: 100–240V, 50/60Hz universal input All regions: 5VDC @ 5A output
Dimensions (W x D x H)	Dimensions: 13 x 8.2 x 1.7 in. (33 x 20.9 x 4.3 mm)
Weight	4.6 lb (2.1 kg)
Operating temperature	32 to 113°F (0 to 45°C)
Storage temperature	–4 to 158° F (–20 to 70°C)
Operating humidity	90% maximum relative humidity, noncondensing
Storage humidity	95% maximum relative humidity, noncondensing
Certifications	VPNC (Basic, AES Interop), ICSA Firewall
Major regulatory environmental compliance	RoHS, China RoHS Safety: CE/LVD, cUL EMI: FCC Part 15 Class A, CE mark commercial, C-Tick Class A, VCCI
LAN	Four RJ-45 ports supporting 10BASE-T, 100BASE-TX, and 1000BASE-T
WAN	One RJ-45 port supporting 10BASE-T, 100BASE-TX, and 1000BASE-T