NETGEAR®

ADSL2+ Gateway

Model D2200D-1FRNAS

User Manual

May 2015
202-11541-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

Contact your Internet service provider for technical support.

Trademarks

Compliance

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

See the regulatory compliance document before connecting the power supply.

Contents

Chapter 1 Hardware Setup

Chapter 2 Connect to the Network and Access the Gateway

Chapter 3 Specify Your Internet Settings

Chapter 4 Control Access to the Internet

Chapter 5 Specify Network Settings

Chapter 6 Manage Your Network

1. Hardware Setup

1

This chapter covers the following topics:

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

Unpack Your Gateway

Your package contains the following items.

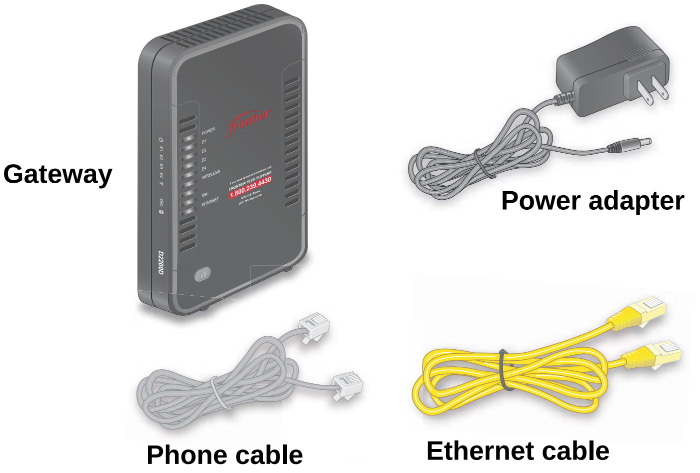


Figure 1. Package contents

Front and Top Panel

The gateway has status LEDs.

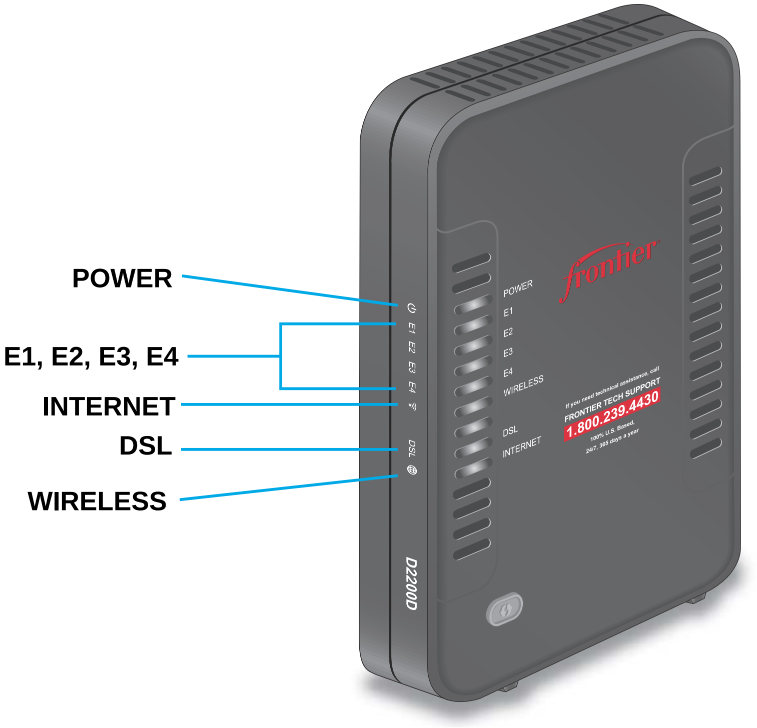


Figure 2. Gateway front and side view

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

LED	Description
POWER ⏻	- **Green**. Power is supplied to the gateway. - **Off**. No power is supplied to the gateway.
E1, E2, E3, E4 E2	- **Green**. A powered-on device is connected to this Ethernet port. - **Off**. No device is connected to this Ethernet port.
WIRELESS 📶	- **Green**. The wireless radio is on. - **Off**. The wireless radio is off.
DSL DSL	- **Green**. The gateway has a DSL connection. - **Slow blinking green**. The gateway is looking for a signal. - **Fast blinking green**. The gateway found the signal and is performing negotiation and handshaking. - **Off**. The gateway does not have a DSL connection.
INTERNET 🌐	- **Solid blue**. The gateway is online. - **Blinking blue**. The gateway is sending or receiving Internet traffic. - **Off**. The gateway is offline.

Rear Panel

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

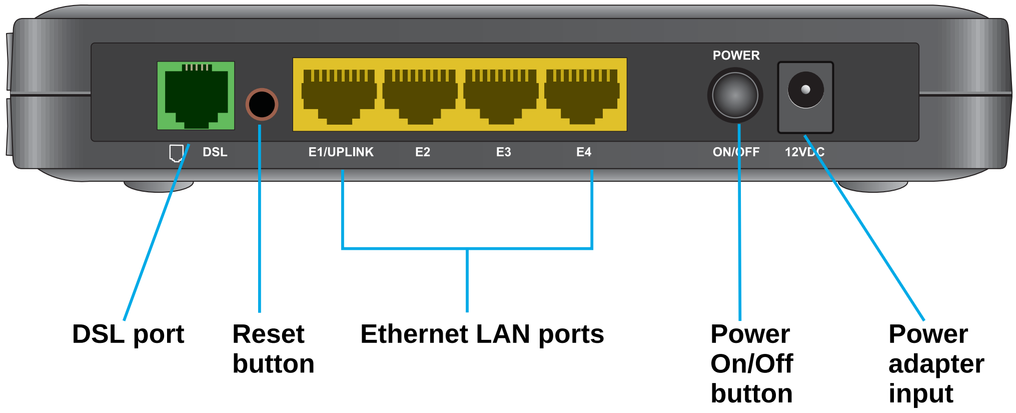


Figure 3. Gateway rear panel

Position Your Gateway

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

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

Position your gateway according to the following guidelines:

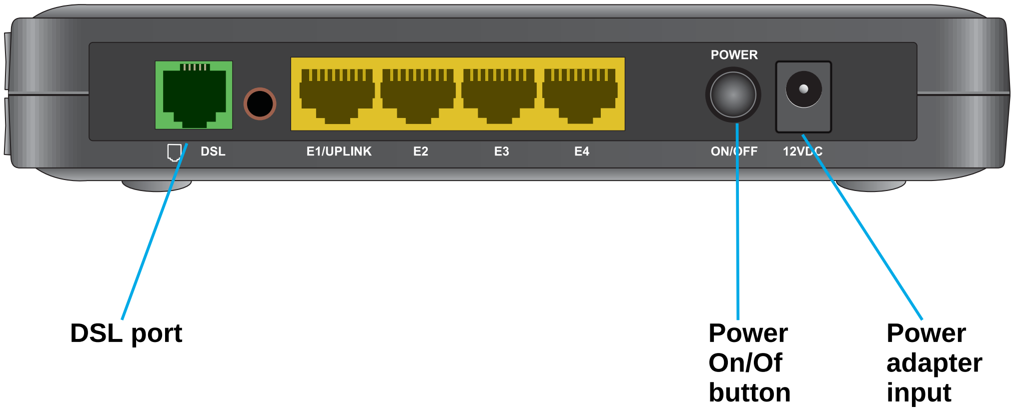
- Place your gateway near the center of the area where your computers and other devices operate, and within line of sight to your wireless devices.
- Make sure that the gateway is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the gateway in an elevated location, minimizing the number walls and ceilings between the gateway and your other devices.
- Place the gateway away from electrical devices such as these:
    - Ceiling fans
    - Home security systems
    - Microwaves
    - Computers
    - Base of a cordless phone
    - 2.4 GHz cordless phone
- Place the gateway away from large metal surfaces, large glass surfaces, and insulated walls such as these:
    - Solid metal doors
    - Aluminum studs
    - Fish tanks
    - Mirrors
    - Brick
    - Concrete

Cable Your Gateway

The gateway comes configured to work as both a modem and a router. You can share your Internet connection without connecting the gateway to a router or gateway.

➢ **To cable your gateway:**

1. Connect the phone line cable that came in the package to the DSL port.



2. Connect the other end of the phone line cable to your DSL line wall jack.
3. Connect the power adapter provided in the package to the gateway and plug the power adapter in to an electrical outlet.
4. Press the **Power On/Off** button.

   The Power LED lights green.

To set up your Internet connection, you must connect a computer or wireless device to the gateway’s network and use a web browser. See *Connect to the Network* on page 12 and *Chapter 3, Specify Your Internet Settings*.

Connect to the Network and Access the Gateway

2

This chapter contains the following sections:

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

Connect to the Network

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

Wired Connection

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

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

1. Make sure that the gateway has power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to Ethernet port **E2**, **E3**, or **E4** on the gateway.

   Note: Do not use port **E1** during setup.

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

WiFi Connection

You can connect to the gateway’s WiFi network with Wi-Fi Protected Setup (WPS) or you can find and select the WiFi network. For information about using WPS, see *WPS Overview* on page 49.

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

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

   The WiFi network name is on the gateway’s label.
3. Join the WiFi network and enter the WiFi password.

   The password is on the gateway’s label.

   Your wireless device connects to the WiFi network.

Label

The label on the gateway shows the login information, MAC address, and serial number.

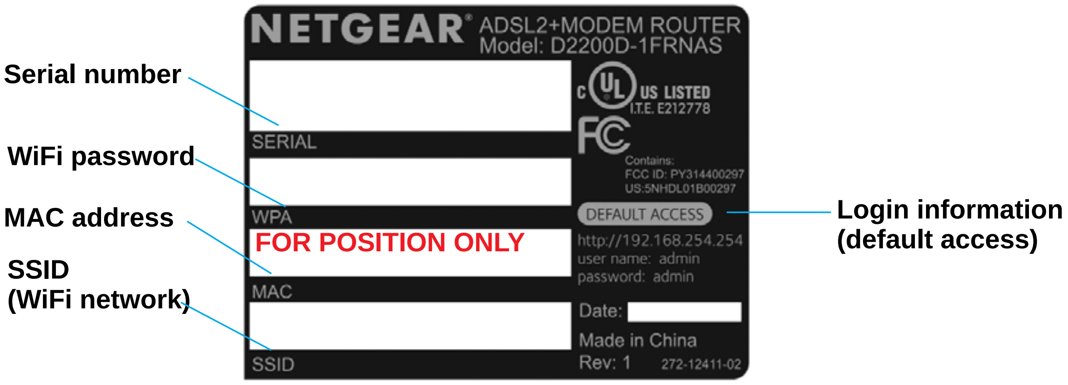


Figure 4. Gateway label

Types of Logins

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

Types of logins:

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

  Note: Your gateway broadcasts dual-band 2.4 GHz and 5 GHz WiFi signals. The label shows the SSID for the 2.4 GHz signal. For information about 5 GHz WiFi settings, see *Specify Basic WiFi Settings* on page 41.

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

Log In to the Gateway

When you first set up your gateway, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the gateway. If you want to view or change settings for the gateway, you can use genie again.

➢ **To log in to the gateway:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

If you are accessing the gateway for the first time, the Auto Configuration page displays. To bypass Auto Configuration, click the **Cancel** button.

The login window opens.

3. Enter the gateway user name and password.

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

   The Main page displays.

3. Specify Your Internet Settings

3

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

This chapter contains the following sections:

- *Use Auto Configuration to Set Up Your Internet Connection*
- *Rerun the Setup Wizard*

Use Auto Configuration to Set Up Your Internet Connection

The first time that you use a web browser to access the gateway, the Auto Configuration page displays. You can use Auto Configuration to detect the Internet connection, or you can click the **Cancel** button to exit, and then log in to the gateway.

➤ **To use Auto Configuration:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   The Auto Configuration page displays. The gateway detects your Internet connection.
3. Follow the onscreen instructions to complete your Internet setup.

Rerun the Setup Wizard

After you install the gateway, you can rerun the Setup Wizard to detect your Internet connection.

➤ **To rerun the Setup Wizard:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Re-Run Setup Wizard**.

   The Re-Run Setup Wizard page displays.
7. Click the **Detect Configuration** button.

   The gateway restarts and the Auto Configuration page displays.
8. Follow the Setup Wizard onscreen instructions.

If you are prompted to enter PPP account settings, enter your Frontier email address and password.

The gateway detects your Internet connection and the Main page displays.

Control Access to the Internet

4

The gateway comes with a built-in firewall that helps protect your home network from unwanted intrusions from the Internet.

This chapter includes the following sections:

- *Set General Firewall Settings*
- *Set Up Custom Firewall Rules*
- *View the Security Log*
- *Port Forwarding Overview*
- *Set Up a Default DMZ Host*
- *Set Up Static NAT*
- *Set Up Remote Management*
- *Specify ALG Settings*

Set General Firewall Settings

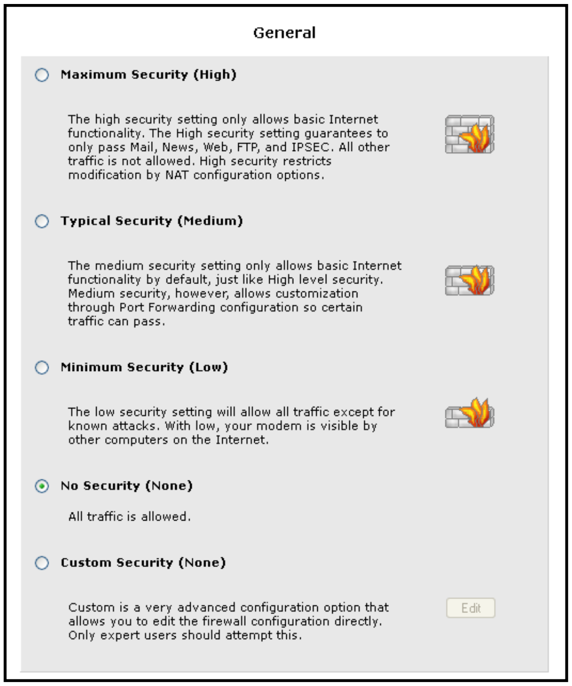
- **To set general firewall settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Firewall Settings > General**.



General

○ **Maximum Security (High)**

The high security setting only allows basic Internet functionality. The High security setting guarantees to only pass Mail, News, Web, FTP, and IPSEC. All other traffic is not allowed. High security restricts modification by NAT configuration options.

○ **Typical Security (Medium)**

The medium security setting only allows basic Internet functionality by default, just like High level security. Medium security, however, allows customization through Port Forwarding configuration so certain traffic can pass.

○ **Minimum Security (Low)**

The low security setting will allow all traffic except for known attacks. With low, your modem is visible by other computers on the Internet.

● **No Security (None)**

All traffic is allowed.

○ **Custom Security (None)**

Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this.

5. Select a radio button.
6. Click the **Apply** button.

   Your settings are saved.

Set Up Custom Firewall Rules

➢ **To add a custom firewall rule:**

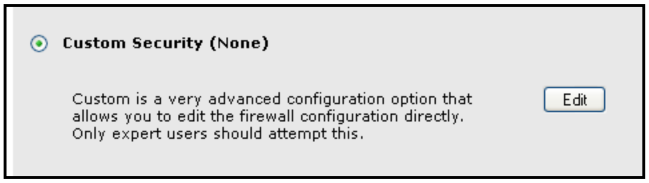
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Firewall Settings > General**.

   The General page displays.
5. Select the Custom Security (None) radio button.

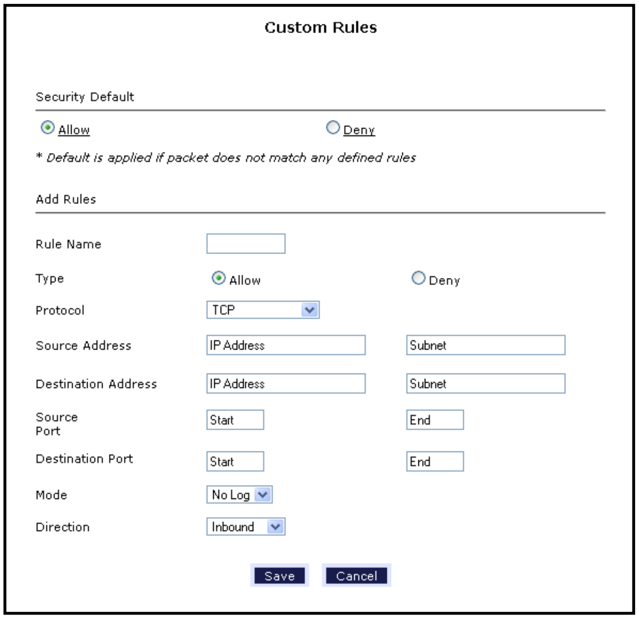


● Custom Security (None)

Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this.

6. When prompted, click the **OK** button to confirm.

   The **Edit** button is activated.
7. Click the **Edit** button.



Custom Rules

Security Default

● Allow ○ Deny

* *Default is applied if packet does not match any defined rules*

Add Rules

Rule Name		
Type	● Allow	○ Deny
Protocol	TCP	
Source Address	IP Address	Subnet
Destination Address	IP Address	Subnet
Source Port	Start	End
Destination Port	Start	End
Mode	No Log	
Direction	Inbound	

8. Select a **Security Default** radio button:
   - **Allow**. Allow the packet if no rule matches it.
   - **Deny**. Block the packet if no rule matches it.

   This specifies the default action to be taken if no rule is found to match the given packet.

9. In the Add Rules section, complete the following fields:
   - **Rule Name**. Name of the new rule.
   - **Type**. Allow or deny the packet matching this rule.
   - **Protocol**. Protocol to match for the new rule.
   - **Source Address**. The source address of the packet to check the rule against.The subnet mask is also to be provided.
   - **Destination Address**. The destination address of the packet to check the rule against.The subnet mask is also to be provided.
   - **Source Port**. The source port of the packet to check the rule against.The start and end ports should be mentioned.
   - **Destination Por**t. The destination port of the packet to check the rule against.The start and end ports should be mentioned.
   - **Mode**. Specify if packets needs to be logged.
   - **Direction**. The traffic direction for which the rule is to be applied. The direction whether inbound or outbound or both can be specified.

10. Click the **Apply** button.

    Your settings are saved.

View the Security Log

The log is a detailed record of the websites you have accessed or attempted to access and other gateway actions.

➢ **To view the security log:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

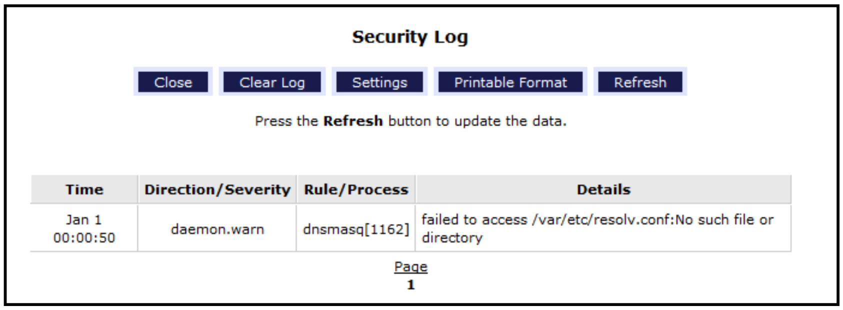
3. Enter the user name and password.

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

   The Main page displays.

4. Select **Firewall Settings > Security Log**.

5. When prompted, click the **Yes** button to proceed.



Security Log

Press the **Refresh** button to update the data.

Time	Direction/Severity	Rule/Process	Details
Jan 1 00:00:50	daemon.warn	dnsmasq[1162]	failed to access /var/etc/resolv.conf:No such file or directory

Page
1

6. To customize the log, do the following:
   - **a.** Click the **Settings** button.

     The Security Log Settings page displays.
   - **b.** Select **Enabled** or **Disabled** for each of these settings:
     - **Log Allowed Traffic**.
     - **Log Blocked Traffic**.
     - **Log Traffic Specified in Rules**.
     - **Log Administrative Access**.
   - **c.** Select or clear the Remote Logging **Enable** check box
   - **d.** If you enabled remote logging, complete the **Remote IP Address** field.
   - **e.** Click the **Apply** button.
7. To refresh the log page, click the **Refresh** button.
8. To clear the log entries, click the **Clear Log** button.
9. To save the log in a printable format, click the **Printable Format** button.

Port Forwarding Overview

Port forwarding allows you to forward incoming traffic from the outside network, to a range of WAN ports on an IP address on the LAN. You can also enable traffic from local network to a specified port range to be allowed to go outside of the network in medium firewall settings.

All the settings on this page are associated with a Service Profile in the Current Profile drop-down list. If no profile has been created, the default profile is used.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups or news groups.

A typical application of port forwarding occurs when a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the gateway, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your gateway. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address www.example.com, which is the gateway's address.

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

   The remote computer then sends this request message through the Internet to your gateway.

2. Your gateway receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your gateway modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your gateway then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends the gateway a reply message.
4. Your gateway performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

Port Forwarding to Permit External Host Communications

In both the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your gateway ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the gateway, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your gateway. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address of www.example.com, which is the address of your gateway.

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

The remote computer sends this request message through the Internet to your gateway.

2. Your gateway receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your gateway modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your gateway then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your gateway.
4. Your gateway performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. To find out, contact the publisher of the application or the relevant user groups or news groups.

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

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

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

> **Tip:** To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product.

Add a Port Forwarding Rule

You can select an existing service or rule, or you can create a new custom rule.

➢ **To add a port forwarding service or rule:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

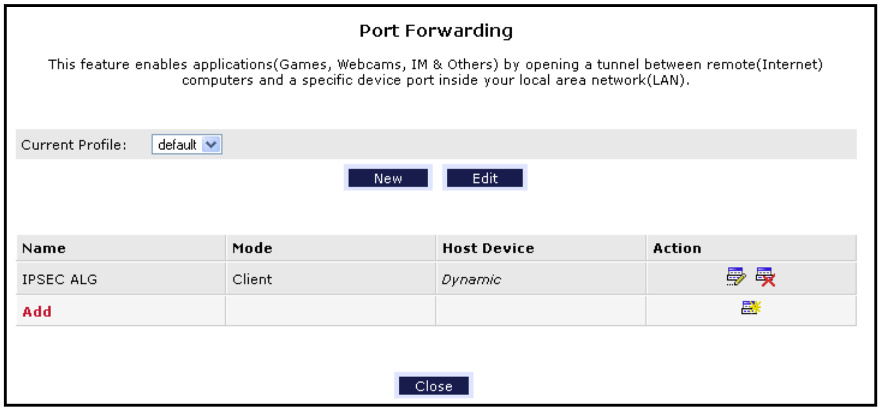
   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

4. Select **Firewall Settings > Port Forwarding**.
5. When prompted, click the **Yes** button to proceed.



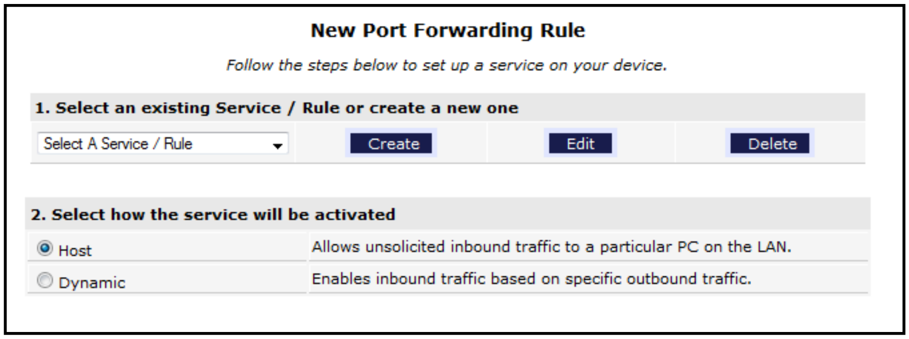
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: default

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

6. Click the **Add** button.



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

Select A Service / Rule

2. Select how the service will be activated

● Host	Allows unsolicited inbound traffic to a particular PC on the LAN.
○ Dynamic	Enables inbound traffic based on specific outbound traffic.

7. To create a new rule, click the **Create** button and specify the settings.

   The new rule displays in the list below Custom Defined Service.

8. To edit a rule, select it in the list and click the **Edit** button.
9. In the Port Forwarding page, click the **Add** button to add the rule that you created.
10. Click the **Apply** button.

    Your settings are saved.

Add or Edit a Port Forwarding Profile

The service profile associates a service profile with one or more of your Connection Profiles. This means different connections can allow different services to be associated with them.

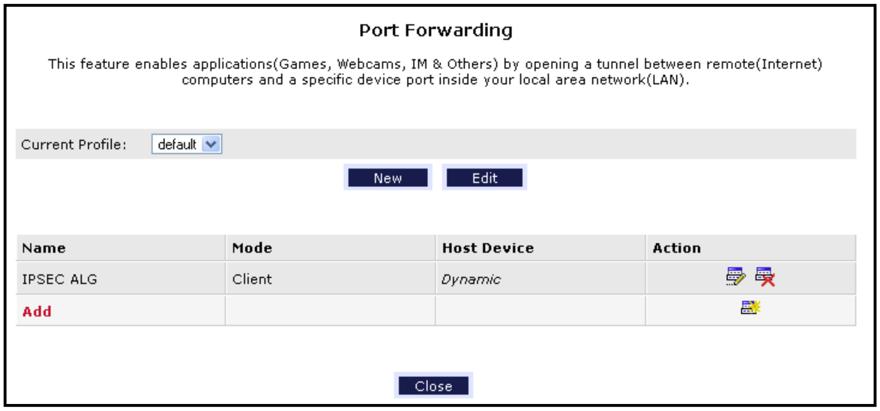
- **To add or edit a port forwarding profile:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Firewall Settings > Port Forwarding**.
5. When prompted, click the **Yes** button to proceed.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: default

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

   The **Current Profile** list shows the selected profile.
6. To add a profile, click the **New** button and follow the steps to create a custom service entry.

   The new profile is added to the **Current Profile** list.
7. To edit the selected profile, click the **Edit** button and follow the steps to change a service profile.
8. Click the **Apply** button.

   Your settings are saved.

Set Up a Default DMZ Host

The default DMZ Host feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The gateway is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the default DMZ server.

WARNING:

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

The gateway usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering page. Instead of discarding this traffic, you can have the gateway forward the traffic to one computer on your network. This computer is called the default DMZ server.

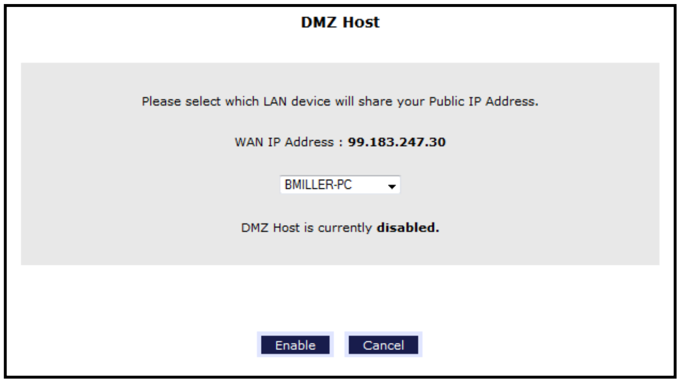
➢ **To set up a DMZ host:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Firewall Settings > DMZ Host**.
5. When prompted, click the **Yes** button to proceed.



DMZ Host

Please select which LAN device will share your Public IP Address.

WAN IP Address : **99.183.247.30**

DMZ Host is currently **disabled.**

6. In the list, select the LAN device to share your public IP address.
7. Click the Enable button.

   A message displays notifying you that the gateway must restart.
8. Click the **OK** button.

   The gateway restarts and DMZ hosting is enabled.

Set Up Static NAT

Static NAT provides a one-to-one private to public static IP address mapping. This can be useful when you want to access a local computer from outside the network.

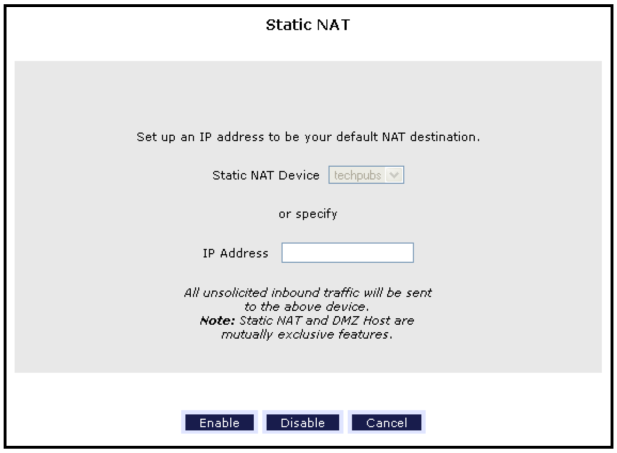
➢ **To set up static NAT:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Firewall Settings > Static NAT**.
5. When prompted, click the **Yes** button to proceed.



Static NAT

Set up an IP address to be your default NAT destination.

Static NAT Device: techpubs

or specify

IP Address:

All unsolicited inbound traffic will be sent to the above device.
***Note:** Static NAT and DMZ Host are mutually exclusive features.*

6. In the **Static NAT Device** list, select the DNS acquired name of the device that will function as the default NAT destination.
7. In the **IP Address** field, type the IP address of the device that will function as the default NAT destination.
8. To enable static NAT, click the **Enable** button.
9. To disable static NAT, click the **Disable** button.
10. Click the **Apply** button.

    Your settings are saved.

Set Up Remote Management

You can use remote management to access your gateway over the Internet to view or change its settings. You need to know the gateway's WAN IP address to use this feature. For information about remote access using Dynamic DNS, see *Dynamic DNS* on page 72.

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. See *Change the admin Password* on page 57.

➢ **To set up remote management:**

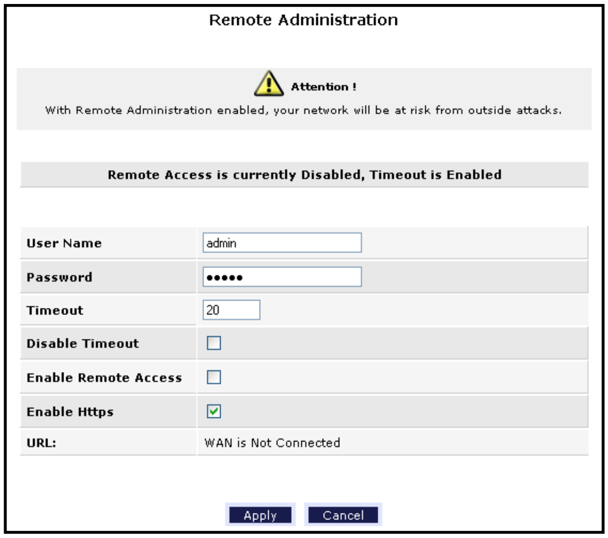
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Remote Administration**.



Remote Administration

Attention !

With Remote Administration enabled, your network will be at risk from outside attacks.

Remote Access is currently Disabled, Timeout is Enabled

User Name	admin
Password	●●●●●
Timeout	20
Disable Timeout	□
Enable Remote Access	□
Enable Https	☑
URL:	WAN is Not Connected

7. Select the **Enable Remote Access** check box.
8. Click the **Apply button**.

   Your changes take effect.

Specify ALG Settings

You can configure the ALG services. When the firewall is set to High, some services are not configurable.

➢ **To specify ALG settings:**

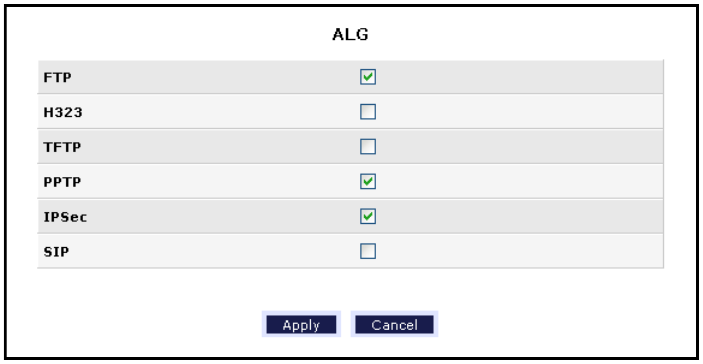
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **ALG**.



ALG

FTP	☑
H323	□
TFTP	□
PPTP	☑
IPSec	☑
SIP	□

7. Select or clear the check boxes.
8. Click the **Apply** button.

   Your settings are saved.

5. Specify Network Settings

5

This chapter includes the following sections:

View Network Computers and Devices

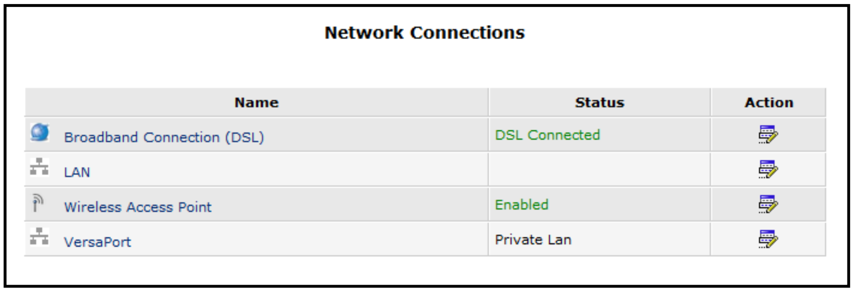
To view network computers and devices:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **My Connected Home > Network Connections**..



Network Connections

Name	Status	Action
Broadband Connection (DSL)	DSL Connected	✎
LAN		✎
Wireless Access Point	Enabled	✎
VersaPort	Private Lan	✎

Specify the IP Addresses that the Gateway Assigns

By default, the gateway acts as a Dynamic Host Configuration Protocol (DHCP) server. The gateway assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the gateway.

These addresses must be part of the same IP address subnet as the gateway’s LAN IP address. Using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you can save part of the range for devices with fixed addresses.

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

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

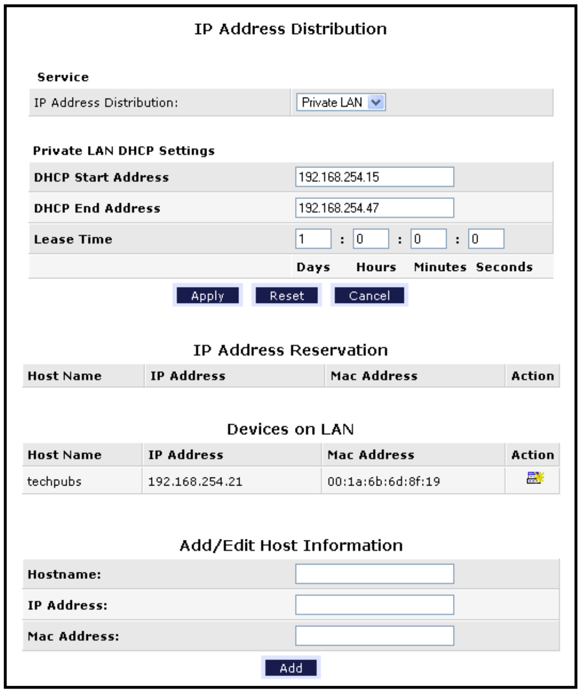
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

The Main page displays.

4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **IP Address Distribution**.



IP Address Distribution

Service

IP Address Distribution:	Private LAN

Private LAN DHCP Settings

DHCP Start Address	192.168.254.15
DHCP End Address	192.168.254.47
Lease Time	1 : 0 : 0 : 0
	Days Hours Minutes Seconds

IP Address Reservation

Host Name	IP Address	Mac Address	Action

Devices on LAN

Host Name	IP Address	Mac Address	Action
techpubs	192.168.254.21	00:1a:6b:6d:8f:19	

Add/Edit Host Information

Hostname:	
IP Address:	
Mac Address:	

7. In the **DHCP Start Address** field, enter the lowest IP address in the range.
8. In the **DHCP End Address** field, enter the highest IP address in the range.
9. Click the **Apply** button.

   Your settings are saved.

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

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

Disable the DHCP Server Feature in the Gateway

By default, the gateway acts as a DHCP server. The gateway assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the gateway.

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

➢ **To disable the DHCP server feature in the gateway:**

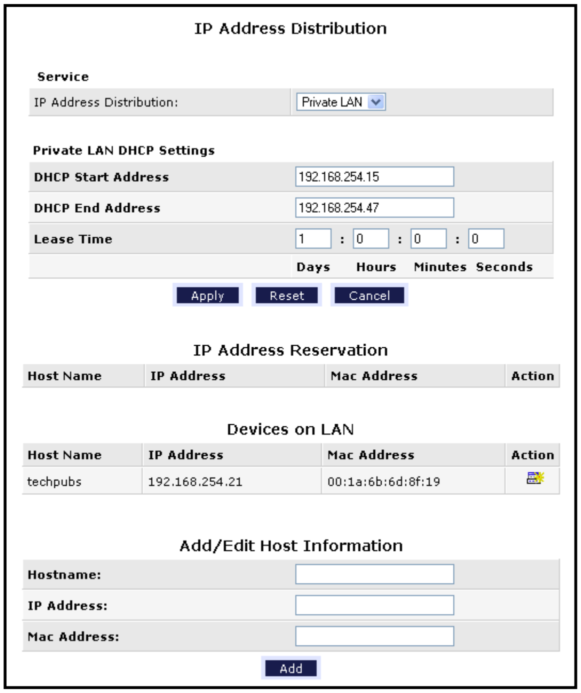
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **IP Address Distribution**.



IP Address Distribution

Service

IP Address Distribution:	Private LAN

Private LAN DHCP Settings

DHCP Start Address	192.168.254.15
DHCP End Address	192.168.254.47
Lease Time	1 Days : 0 Hours : 0 Minutes : 0 Seconds

IP Address Reservation

Host Name	IP Address	Mac Address	Action

Devices on LAN

Host Name	IP Address	Mac Address	Action
techpubs	192.168.254.21	00:1a:6b:6d:8f:19	

Add/Edit Host Information

Hostname:	
IP Address:	
Mac Address:	

7. In the **IP Address Distribution** list, select **Off**.
8. Click the **Apply** button.

   Your settings are saved.
9. (Optional) If this service is disabled and no other DHCP server is on your network, set your computer IP addresses manually so that they can access the gateway.

Specify Private LAN Settings

You can specify how the gateway interacts with computers and devices that are connected to its network.

➢ **To specify private LAN settings:**

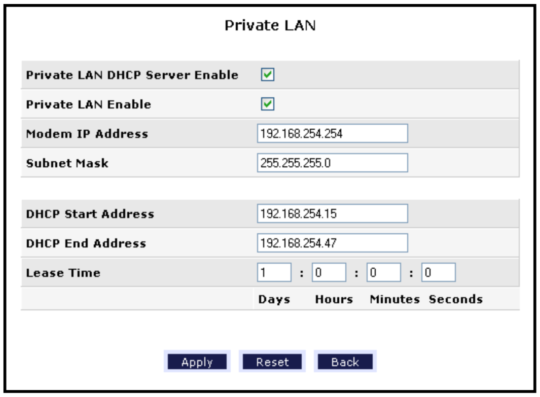
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Private LAN**.



Private LAN

Private LAN DHCP Server Enable	☑
Private LAN Enable	☑
Modem IP Address	192.168.254.254
Subnet Mask	255.255.255.0
DHCP Start Address	192.168.254.15
DHCP End Address	192.168.254.47
Lease Time	1 : 0 : 0 : 0
	Days Hours Minutes Seconds

7. Select the **Private LAN Server Enable** check box.

   Enabling DHCP server allows the gateway to automatically assign IP addresses to devices that connect to its network.
8. Select the **Public LAN Enable** check box.

   Enabling Public LAN allows a global subnet to exist behind your gateway.
9. In the **Modem's Public IP Address** field, enter the IP address that the gateway uses for local communication.
10. In the **Subnet Mask** field, enter the subnet mask used to determine if an IP address belongs to your local network.
11. To specify the IP address pool that the gateway uses, complete the **DHCP Start Address** and **DHCP End Address** fields.

12. Click the **Apply** button.

    Your settings are saved.

Specify Public LAN Settings

You can specify how the gateway interacts with computers and devices that are connected to its network.

➢ **To specify public LAN settings:**

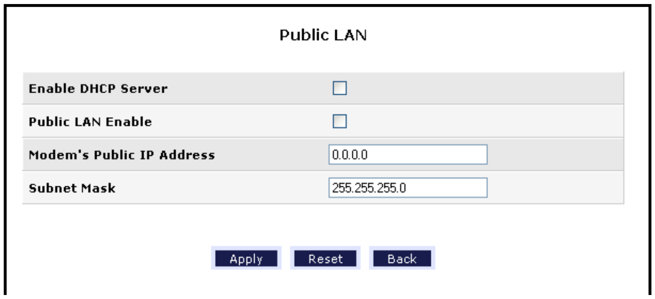
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Public LAN**.



Public LAN

Enable DHCP Server	□
Public LAN Enable	□
Modem's Public IP Address	0.0.0.0
Subnet Mask	255.255.255.0

7. To enable Public LAN, select the **Enable DHCP Server** check box.

   Enabling DHCP server allows the gateway to automatically assign IP addresses to devices that connect to its network.
8. Select the **Public LAN Enable** check box.

   Enabling Public LAN allows a global subnet to exist behind your gateway.
9. In the **Modem’s Public IP Address** field, enter the IP address that the gateway uses for local communication.
10. In the **Subnet Mask** field, enter the subnet mask used to determine if an IP address belongs to your local network.
11. Click the **Apply** button.

Your settings are saved.

Reserve LAN IP Addresses

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

➢ **To reserve an IP address:**

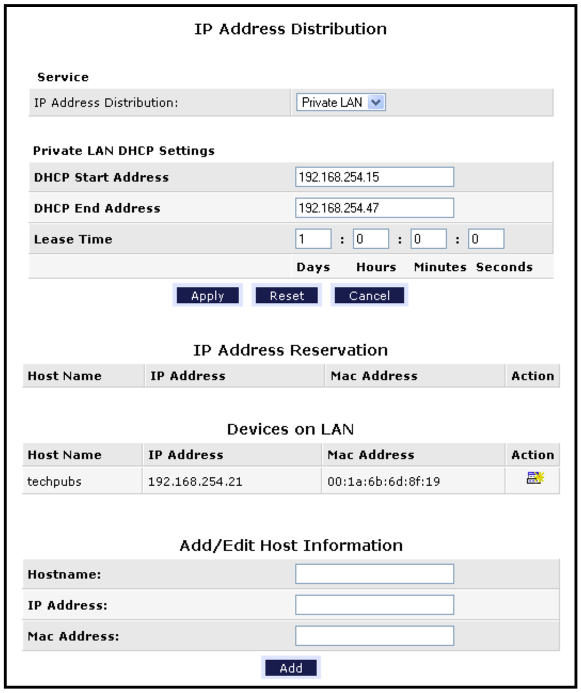
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **IP Address Distribution**.



IP Address Distribution

Service

IP Address Distribution:	Private LAN

Private LAN DHCP Settings

DHCP Start Address	192.168.254.15
DHCP End Address	192.168.254.47
Lease Time	1 : 0 : 0 : 0
	Days Hours Minutes Seconds

IP Address Reservation

Host Name	IP Address	Mac Address	Action

Devices on LAN

Host Name	IP Address	Mac Address	Action
techpubs	192.168.254.21	00:1a:6b:6d:8f:19	

Add/Edit Host Information

Hostname:	
IP Address:	
Mac Address:	

The IP Address Reservation table displays a list of IP addresses from the DHCP pool range that are reserved for specific LAN devices.

7. To add an entry into the Address Reservation table, complete the fields in the Add/Edit Host Information section:
   - **Host Name**. The name of the LAN device to be added.
   - **IP Address**. The IP address to be reserved for this LAN device by the DHCP server.
   - **MAC Address**. The MAC address of the device.
8. Click the **Add** button.

   The device is added to the Address Reservation table.

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

RIP Configuration

You can specify RIP settings for the LAN and WAN.

➢ **To specify RIP configuration:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

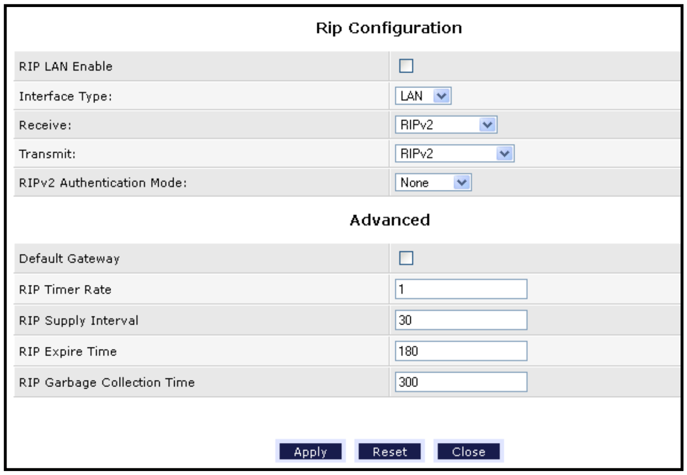
   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **RIP Configuration**.



Rip Configuration

RIP LAN Enable	□
Interface Type:	LAN
Receive:	RIPv2
Transmit:	RIPv2
RIPv2 Authentication Mode:	None

Advanced

Default Gateway	□
RIP Timer Rate	1
RIP Supply Interval	30
RIP Expire Time	180
RIP Garbage Collection Time	300

7. To enable RIP, select the **RIP LAN Enable** check box.
8. In the Interface Type list, select **LAN** or **WAN**.

   The WAN side is receive-only.

9. Complete the fields to specify the RIP version and the authentication mode.
10. To specify a default gateway, select the **Default Gateway** check box.

    This setting controls whether the gateway advertises itself as a gateway.

11. Click the **Apply** button.

    Your settings are saved.

Note: You can click the **Reset** button to return the gateway RIP configuration settings to their default values.

Enable or Disable Multicast IGMP Proxy

By default, IGMP proxy is enabled.

➢ **To enable multicast IGMP proxy:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

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

The Main page displays.

4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Multicast**..

   The Multicast page displays.
7. Select or clear the **IGMP Proxy Enable** check box.
8. Click the **Apply** button.

   Your settings are saved.

View the Routing Table

➢ **To view the routing table:**

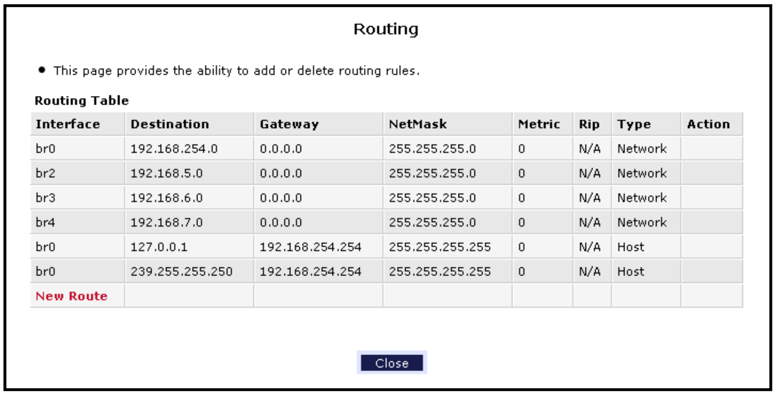
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Routing**.



Routing

- This page provides the ability to add or delete routing rules.

Routing Table

Interface	Destination	Gateway	NetMask	Metric	Rip	Type	Action
br0	192.168.254.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br2	192.168.5.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br3	192.168.6.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br4	192.168.7.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br0	127.0.0.1	192.168.254.254	255.255.255.255	0	N/A	Host	
br0	239.255.255.250	192.168.254.254	255.255.255.255	0	N/A	Host	
New Route							

Improve Network Connections with Universal Plug and Play

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

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

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

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Universal Plug and Play**.

   The UPnP page displays.
7. Select the **UPnP Enable** check box.

   By default, this check box is selected. UPnP for automatic device configuration can be enabled or disabled. If the Turn UPnP On check box is cleared, the gateway does not allow any device to automatically control gateway resources, such as port forwarding.
8. Click the **Apply** button.

Specify Basic WiFi Settings

The gateway comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the product label.

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

It is recommended that you do not change your preset security settings. If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

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

➢ **To specify basic wireless settings:**

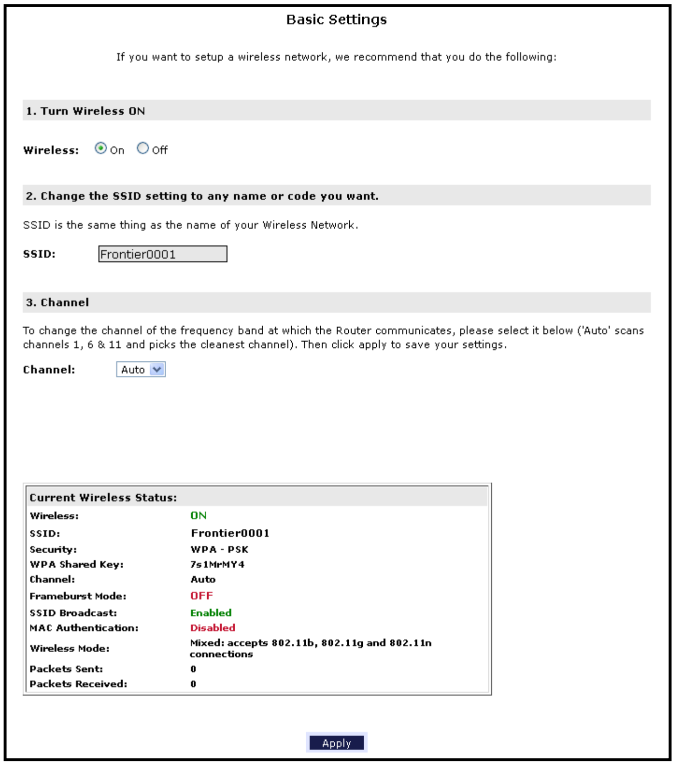
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **Wireless**.



Basic Settings

If you want to setup a wireless network, we recommend that you do the following:

1. Turn Wireless ON

Wireless: ● On ○ Off

2. Change the SSID setting to any name or code you want.

SSID is the same thing as the name of your Wireless Network.

SSID: Frontier0001

3. Channel

To change the channel of the frequency band at which the Router communicates, please select it below ('Auto' scans channels 1, 6 & 11 and picks the cleanest channel). Then click apply to save your settings.

Channel: Auto

Current Wireless Status:	
Wireless:	ON
SSID:	Frontier0001
Security:	WPA - PSK
WPA Shared Key:	7s1MrMY4
Channel:	Auto
Frameburst Mode:	OFF
SSID Broadcast:	Enabled
MAC Authentication:	Disabled
Wireless Mode:	Mixed: accepts 802.11b, 802.11g and 802.11n connections
Packets Sent:	0
Packets Received:	0

5. To change the network name (SSID), type a new name in the **SSID** field.

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

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

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

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

7. Click the **Apply** button.

   Your settings are saved.

   If you connected wirelessly to the network and you changed the SSID, you are disconnected from the network.

8. Make sure that you can connect wirelessly to the network with its new settings.

   If you cannot connect wirelessly, check the following:

- Is your computer or wireless device connected to another wireless network in your area? Some wireless devices automatically connect to the first open network without wireless security that they discover.
- Is your computer or wireless device trying to connect to your network with its old settings (before you changed the settings)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

Change the WiFi Security Settings

Your gateway comes with preset WPA2 or WPA security. The password that you enter to connect to your network is unique to your gateway and is on the product label. NETGEAR recommends that you use the preset security, but you can change them. NETGEAR recommends that you do not disable security.

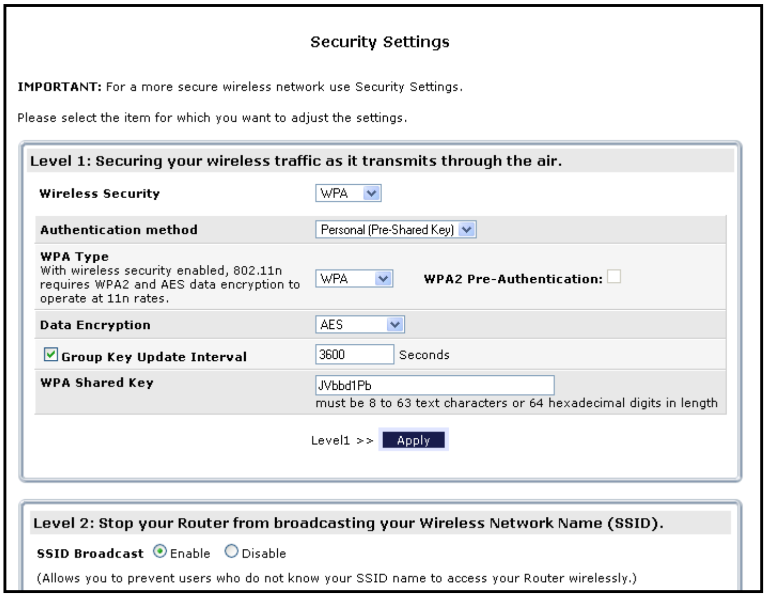
➢ **To change the wireless security settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Security Settings**.



Security Settings

IMPORTANT: For a more secure wireless network use Security Settings.

Please select the item for which you want to adjust the settings.

Level 1: Securing your wireless traffic as it transmits through the air.

Wireless Security	WPA
Authentication method	Personal (Pre-Shared Key)
WPA Type With wireless security enabled, 802.11n requires WPA2 and AES data encryption to operate at 11n rates.	WPA **WPA2 Pre-Authentication:** □
Data Encryption	AES
☑ **Group Key Update Interval**	3600 Seconds
WPA Shared Key	JVbbd1Pb must be 8 to 63 text characters or 64 hexadecimal digits in length

Level 2: Stop your Router from broadcasting your Wireless Network Name (SSID).

SSID Broadcast ● Enable ○ Disable

(Allows you to prevent users who do not know your SSID name to access your Router wirelessly.)

5. In the **Wireless Security** list, select **WPA**, **WEP**, or **Disable**.

   The WPA is recommended because it uses the newest standard for the strongest security. The fields displayed in this page depend on what is currently selected in the **Wireless Security** List.

6. To specify WPA, do the following:
   - In the **WPA Type** list, select **WPA Any**, **WPA2**, or **WPA**.
   - In the **Data Encryption** field, select **AES** or **TKIP + AES**.
   - In the **WPA Shared Key** field, enter the WiFi network key (password).

     The shared key is a text string from 8 to 63 characters.

7. To specify WEP, do the following:
   - In the **Network Authentication** field, select **Open System Authentication** or **Shared Key Authentication**.
   - Complete the fields to enter the encryption keys, the entry method, and the key length,

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

9. Click the **Apply** button.

   Your settings are saved.

Create a Hidden Wireless Network

A hidden wireless network does not broadcast its wireless name (SSID). To connect to a hidden wireless network, you must know the wireless name and password and type them.

➢ **To create a hidden network:**

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

2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

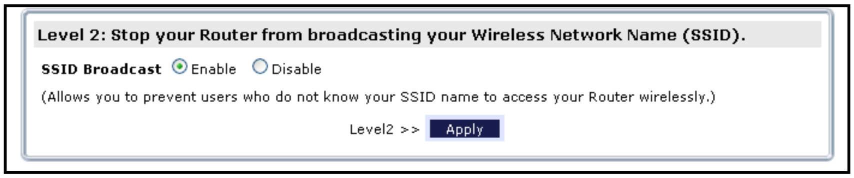
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

   The Main page displays.

4. Select **Wireless Security**.

   The Wireless Security page displays.

5. Scroll down to the Level 2 section.



Level 2: Stop your Router from broadcasting your Wireless Network Name (SSID).

SSID Broadcast ● Enable ○ Disable

(Allows you to prevent users who do not know your SSID name to access your Router wirelessly.)

6. Select the SSID Broadcast **Disable** radio button.
7. Click the **Apply** button.

   Your settings are saved.

Restrict Wireless Access by MAC Address

You can restrict wireless access to certain computers and wireless devices based on their MAC addresses. This is called MAC filtering.

➢ **To restrict wireless access by MAC address:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

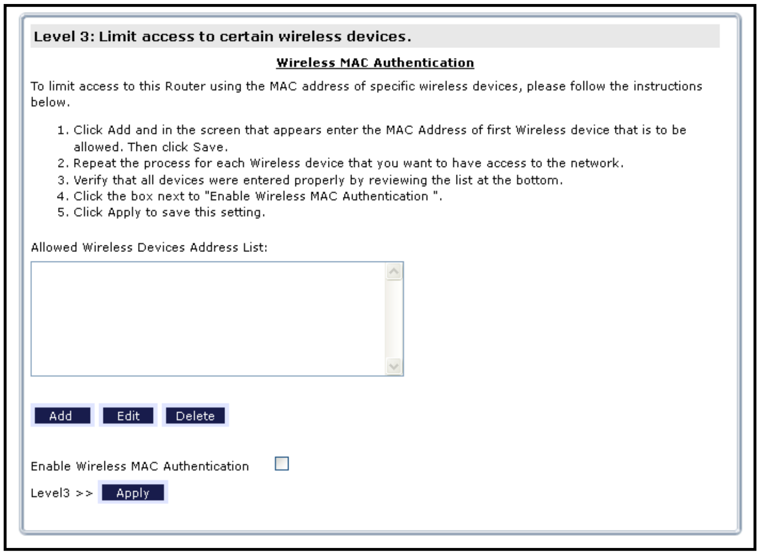
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

   The Main page displays.

4. Select **Wireless Security**.

   The Wireless Security page displays.

5. Scroll down to the Level 3 section.



Level 3: Limit access to certain wireless devices.

Wireless MAC Authentication

To limit access to this Router using the MAC address of specific wireless devices, please follow the instructions below.

1. Click Add and in the screen that appears enter the MAC Address of first Wireless device that is to be allowed. Then click Save.
2. Repeat the process for each Wireless device that you want to have access to the network.
3. Verify that all devices were entered properly by reviewing the list at the bottom.
4. Click the box next to "Enable Wireless MAC Authentication ".
5. Click Apply to save this setting.

Allowed Wireless Devices Address List:

Add Edit Delete

Enable Wireless MAC Authentication □

Level3 >> Apply

6.
7. Click the **Add** button.
8. Click the **Apply** button.

   Your settings are saved.

Set Up a Guest Network

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

➢ **To set up a guest network:**

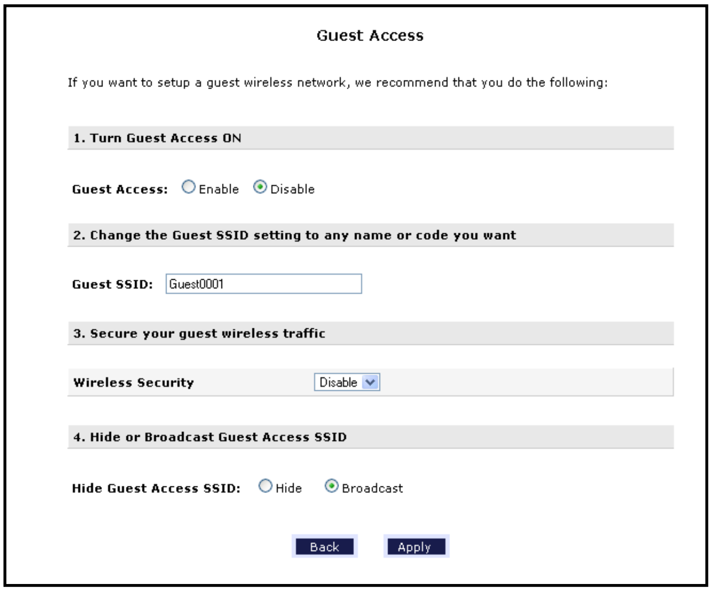
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **Guest Network**.



Guest Access

If you want to setup a guest wireless network, we recommend that you do the following:

1. Turn Guest Access ON

Guest Access: ○ Enable ● Disable

2. Change the Guest SSID setting to any name or code you want

Guest SSID: Guest0001

3. Secure your guest wireless traffic

Wireless Security: Disable

4. Hide or Broadcast Guest Access SSID

Hide Guest Access SSID: ○ Hide ● Broadcast

5. Select any of the following wireless settings:
   - **Enable Guest Network**. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
   - **Enable SSID Broadcast**. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.
   - **Allow guest to see each other and access my local network**. If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.
6. Give the guest network a name.

   The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.
7. Select a radio button for a security option.

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

   Your settings are saved.

WPS Overview

Wi-Fi Protected Setup (WPS) lets you add a wireless computer or device to your WiFi network without typing the WiFi password.

Enable WPS Simple Config

To use WPS, you must enable WPS simple config first.

➢ **To enable WPS connections (simple config):**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Wireless Settings > Simple Config**.
5. Select the **Enable Simple Config** button.

   The radio buttons are activated.

Connect Using WPS

➢ **To connect using a WPS button:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

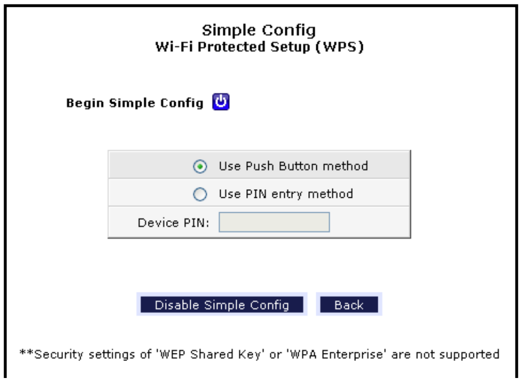
   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Wireless Settings > Simple Config**.

   The Simple Config page displays.
5. Select the radio button for the setup method that you want to use:

- **Use Push Button method**. Click the **Begin Simple Config** button.



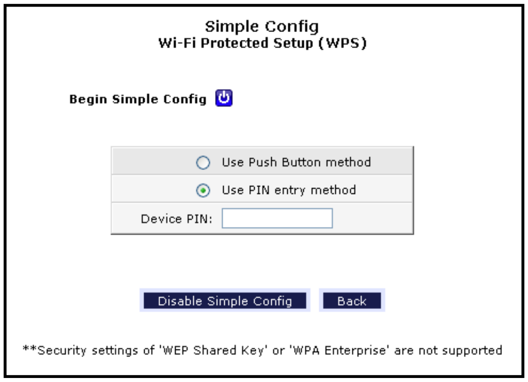
Simple Config
Wi-Fi Protected Setup (WPS)

Begin Simple Config

● Use Push Button method
○ Use PIN entry method
Device PIN:

**Security settings of 'WEP Shared Key' or 'WPA Enterprise' are not supported

- **Use PIN entry method**. In the **Device PIN** field, type the client security PIN and click the **Begin Simple Config** button.



Simple Config
Wi-Fi Protected Setup (WPS)

Begin Simple Config

○ Use Push Button method
● Use PIN entry method
Device PIN:

**Security settings of 'WEP Shared Key' or 'WPA Enterprise' are not supported

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

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

Control the Wireless Radios

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

➢ **To turn the wireless radios off and on:**

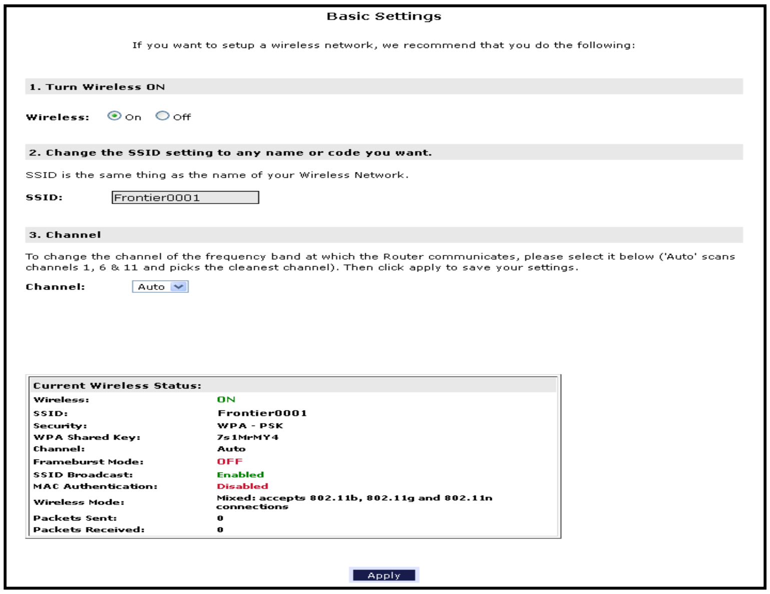
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

The Main page displays.

4. Select **Wireless Settings > Basic Settings**.



Basic Settings

If you want to setup a wireless network, we recommend that you do the following:

1. Turn Wireless ON

Wireless: ● On ○ Off

2. Change the SSID setting to any name or code you want.

SSID is the same thing as the name of your Wireless Network.

SSID: Frontier0001

3. Channel

To change the channel of the frequency band at which the Router communicates, please select it below ('Auto' scans channels 1, 6 & 11 and picks the cleanest channel). Then click apply to save your settings.

Channel: Auto

Current Wireless Status:	
Wireless:	ON
SSID:	Frontier0001
Security:	WPA - PSK
WPA Shared Key:	7s1MrMY4
Channel:	Auto
Frameburst Mode:	OFF
SSID Broadcast:	Enabled
MAC Authentication:	Disabled
Wireless Mode:	Mixed: accepts 802.11b, 802.11g and 802.11n connections
Packets Sent:	0
Packets Received:	0

5. Select The Wireless **On** or **Off** radio button.
6. Click the **Apply** button.

   If you turned off the wireless radios, the WiFi On/Off LED turns off. If you turned on the wireless radios, the WiFi On/Off LED lights.

Quality of Service

Quality of Service (QoS) provides differentiated levels of service for network traffic. Disabling QoS also disables fragmentation.

Enable QoS

➢ **To enable QoS:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

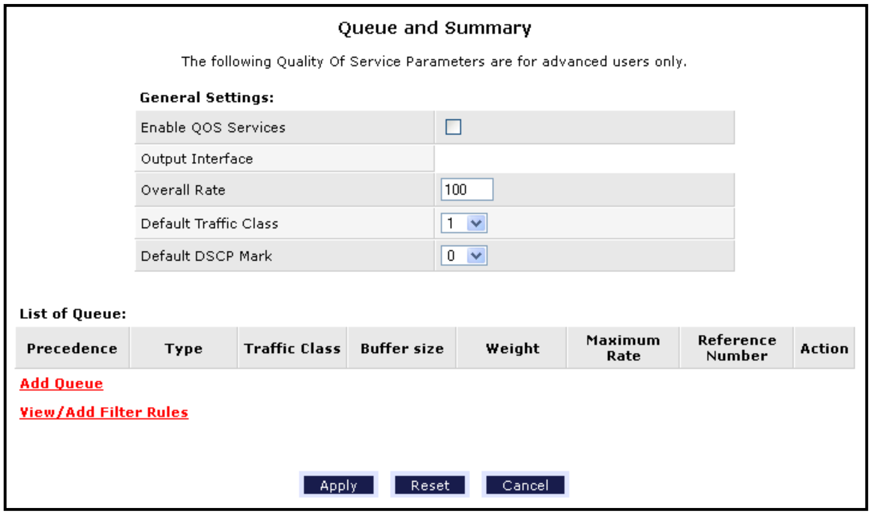
   A login window opens.
3. Enter the user name and password.

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

The Main page displays.

4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Quality of Service (QoS)**.



Queue and Summary

The following Quality Of Service Parameters are for advanced users only.

General Settings:

Enable QOS Services	☐
Output Interface	
Overall Rate	100
Default Traffic Class	1
Default DSCP Mark	0

List of Queue:

Precedence	Type	Traffic Class	Buffer size	Weight	Maximum Rate	Reference Number	Action

Add Queue

View/Add Filter Rules

7. To enable QoS, select the **Enable QoS Services** check box.

Manage QoS Rules and Filters

You can add, edit, or delete QoS filters and you can control the priority of the rules in relation to each other.

➢ To manage QoS rules and filters:

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

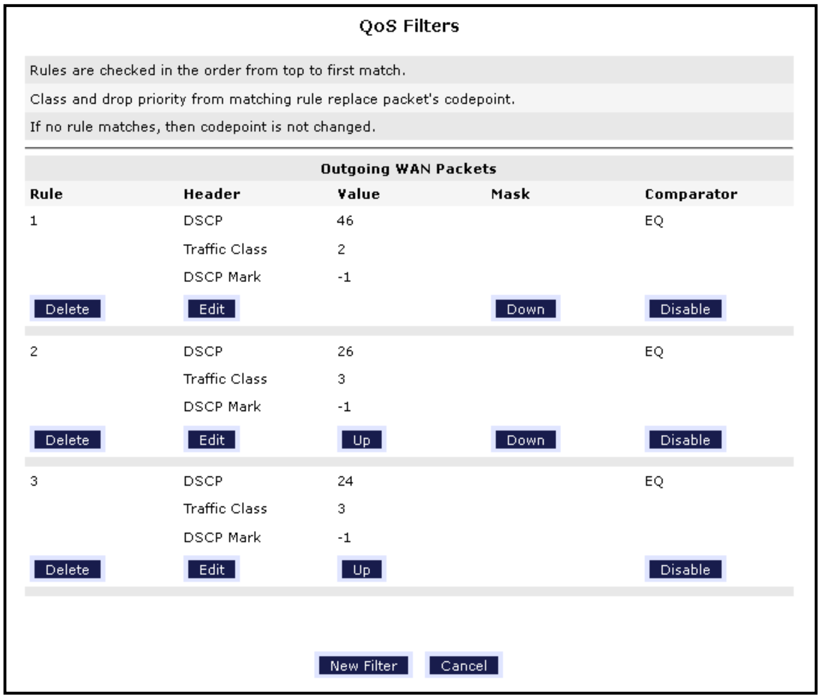
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Quality of Service (QoS)**.

The Queue and Summary page displays.

7. Click the **View/Add Filter Rules** link.



QoS Filters

Rules are checked in the order from top to first match.

Class and drop priority from matching rule replace packet's codepoint.

If no rule matches, then codepoint is not changed.

Outgoing WAN Packets

Rule	Header	Value	Mask	Comparator
1	DSCP	46		EQ
	Traffic Class	2		
	DSCP Mark	-1		
Delete	Edit		Down	Disable
2	DSCP	26		EQ
	Traffic Class	3		
	DSCP Mark	-1		
Delete	Edit	Up	Down	Disable
3	DSCP	24		EQ
	Traffic Class	3		
	DSCP Mark	-1		
Delete	Edit	Up		Disable

8. To add a filter, click the **New Filter** button.
9. To modify a filter, click the **Edit** button for a rule.
10. To delete a filter, click the **Delete** button.
11. To change the priority of a rule, click the **Down** button or the **Up** button.
12. Click the **Apply** button.

    Your settings are saved.

Add a Queue

➤ **To add a queue:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.

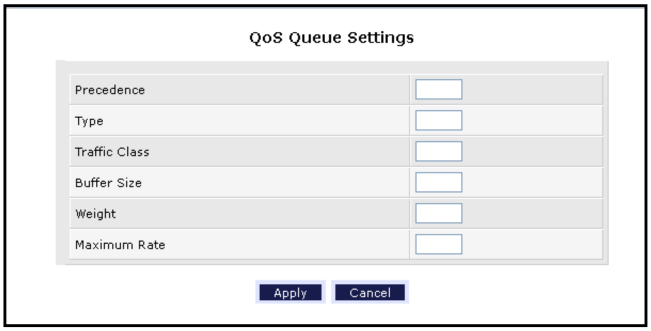
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Quality of Service (QoS)**.

   The Queue and Summary page displays.

7. Click the **Add Queue** link.



QoS Queue Settings

Precedence	
Type	
Traffic Class	
Buffer Size	
Weight	
Maximum Rate	

8. Specify the following:
   - **Precedence**. The range is 1 to 15. Lower values have higher priority.
   - **Type**. SP or WFQ.
   - **Traffic Class**. The range is 1 to 15. Lower values have higher priority.
   - **Buffer Size**. The range is 1 to 10000.
   - **Weigh**t. The range is 1 to 65535.
   - **Maximum Rate**. The range is 1 to 100.

9. Click the **Apply** button.

   The queue is added.

Change the Wireless Mode

➢ **To turn the wireless radios off and on:**

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

2. Type **http:/192.168.254.254**.

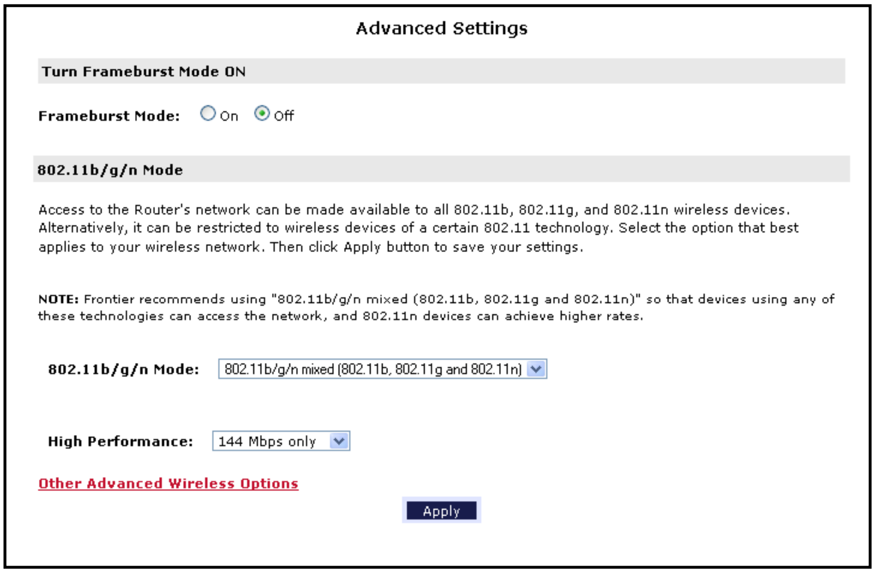
   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

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



Advanced Settings

Turn Frameburst Mode ON

Frameburst Mode: ○ On ● Off

802.11b/g/n Mode

Access to the Router's network can be made available to all 802.11b, 802.11g, and 802.11n wireless devices. Alternatively, it can be restricted to wireless devices of a certain 802.11 technology. Select the option that best applies to your wireless network. Then click Apply button to save your settings.

NOTE: Frontier recommends using "802.11b/g/n mixed (802.11b, 802.11g and 802.11n)" so that devices using any of these technologies can access the network, and 802.11n devices can achieve higher rates.

802.11b/g/n Mode: 802.11b/g/n mixed (802.11b, 802.11g and 802.11n)

High Performance: 144 Mbps only

5. In the **802.11b/ Mode** list, select an option.
6. In the **High Performance** list, select an option.
7. Click the **Apply** button.

   Your settings are saved.

6. Manage Your Network

6

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

This chapter includes the following sections:

- *Change the admin Password*
- *View Gateway Status*
- *Run the Ping Utility*
- *Run the Traceroute Utility*
- *View Devices Currently on the Network*
- *Manage the Gateway Configuration File*
- *Dynamic DNS*
- *Specify the Date and Time Settings*
- *Reboot the Gateway*

Change the admin Password

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

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

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

   Select **Users**.
6. Type the old password, and type the new password twice.
7. Click the **Apply** button.

   Your changes take effect.

View Gateway Status

➢ **To view gateway status:**

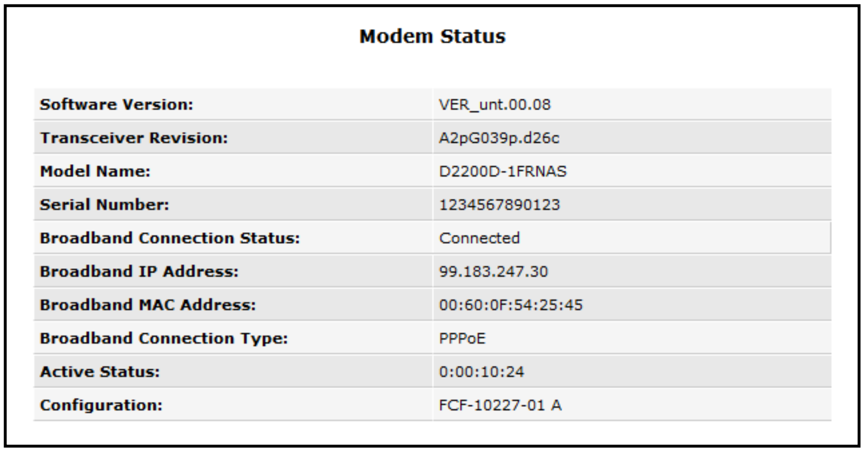
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring**.



Modem Status

Software Version:	VER_unt.00.08
Transceiver Revision:	A2pG039p.d26c
Model Name:	D2200D-1FRNAS
Serial Number:	1234567890123
Broadband Connection Status:	Connected
Broadband IP Address:	99.183.247.30
Broadband MAC Address:	00:60:0F:54:25:45
Broadband Connection Type:	PPPoE
Active Status:	0:00:10:24
Configuration:	FCF-10227-01 A

5. For information about the displayed settings, click the **Help** icon in the upper right corner of the page.

View Advanced Status

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

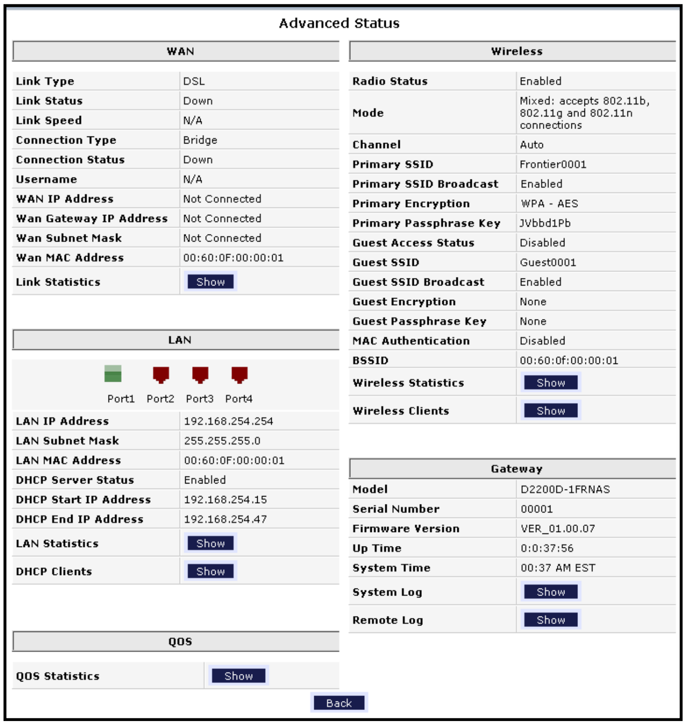
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring > Advanced Status**.



Advanced Status

WAN	
Link Type	DSL
Link Status	Down
Link Speed	N/A
Connection Type	Bridge
Connection Status	Down
Username	N/A
WAN IP Address	Not Connected
Wan Gateway IP Address	Not Connected
Wan Subnet Mask	Not Connected
Wan MAC Address	00:60:0F:00:00:01
Link Statistics	Show

LAN	
LAN IP Address	192.168.254.254
LAN Subnet Mask	255.255.255.0
LAN MAC Address	00:60:0F:00:00:01
DHCP Server Status	Enabled
DHCP Start IP Address	192.168.254.15
DHCP End IP Address	192.168.254.47
LAN Statistics	Show
DHCP Clients	Show

QOS	
QOS Statistics	Show

Wireless	
Radio Status	Enabled
Mode	Mixed: accepts 802.11b, 802.11g and 802.11n connections
Channel	Auto
Primary SSID	Frontier0001
Primary SSID Broadcast	Enabled
Primary Encryption	WPA - AES
Primary Passphrase Key	JVbbd1Pb
Guest Access Status	Disabled
Guest SSID	Guest0001
Guest SSID Broadcast	Enabled
Guest Encryption	None
Guest Passphrase Key	None
MAC Authentication	Disabled
BSSID	00:60:0f:00:00:01
Wireless Statistics	Show
Wireless Clients	Show

Gateway	
Model	D2200D-1FRNAS
Serial Number	00001
Firmware Version	VER_01.00.07
Up Time	0:0:37:56
System Time	00:37 AM EST
System Log	Show
Remote Log	Show

For information about the content of this page, click the **Help** icon.

View the Ethernet Status

➢ **To view the gateway Ethernet status:**

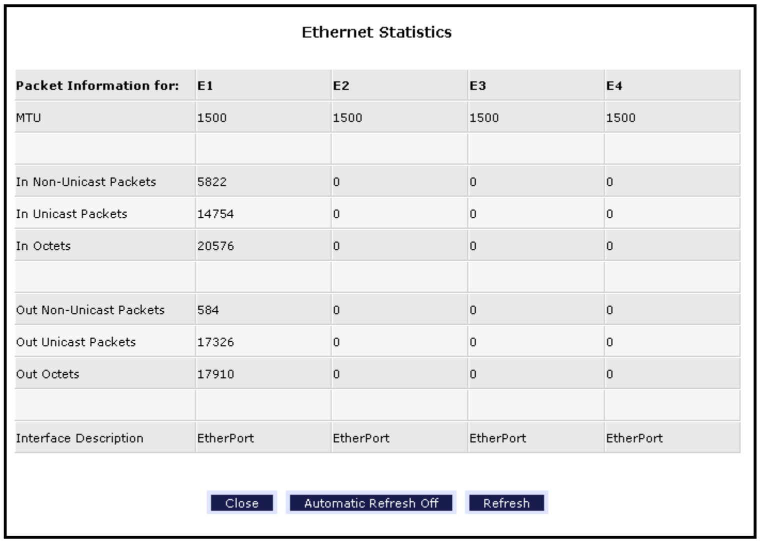
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring > Advanced Status > Ethernet**.



Ethernet Statistics

Packet Information for:	E1	E2	E3	E4
MTU	1500	1500	1500	1500
In Non-Unicast Packets	5822	0	0	0
In Unicast Packets	14754	0	0	0
In Octets	20576	0	0	0
Out Non-Unicast Packets	584	0	0	0
Out Unicast Packets	17326	0	0	0
Out Octets	17910	0	0	0
Interface Description	EtherPort	EtherPort	EtherPort	EtherPort

View the ATM Status

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

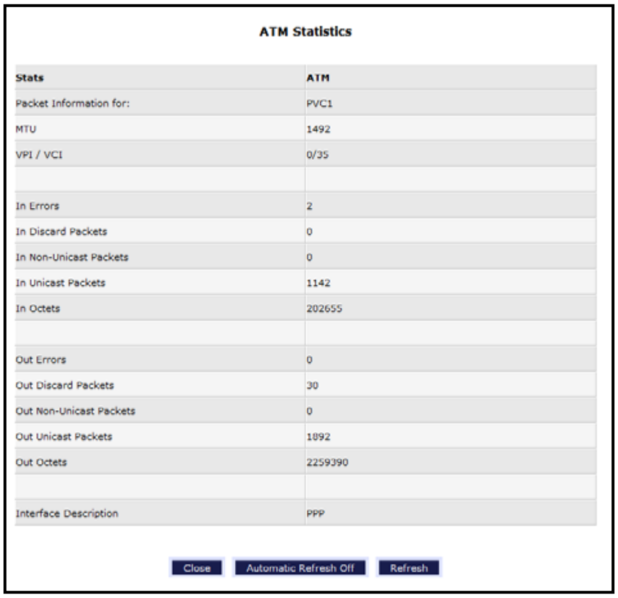
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring > Advanced Status > ATM**.



ATM Statistics

Stats	ATM
Packet Information for:	PVC1
MTU	1492
VPI / VCI	0/35
In Errors	2
In Discard Packets	0
In Non-Unicast Packets	0
In Unicast Packets	1142
In Octets	202655
Out Errors	0
Out Discard Packets	30
Out Non-Unicast Packets	0
Out Unicast Packets	1892
Out Octets	2259390
Interface Description	PPP

View the DSL Status

➢ **To view the gateway DSL status:**

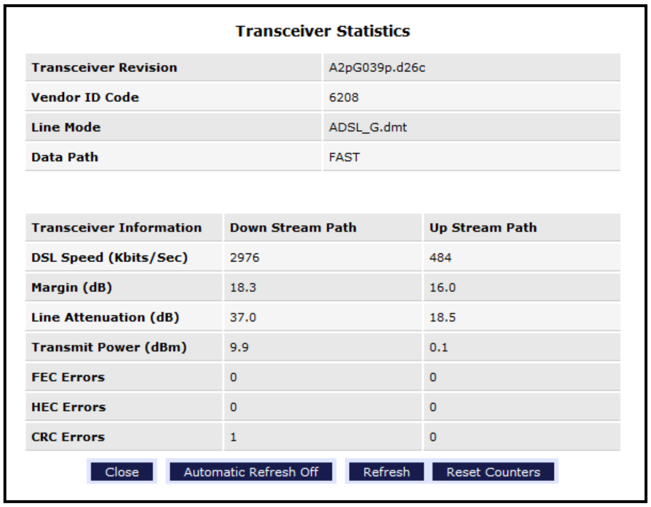
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring > Advanced Status > DSL**.



Transceiver Statistics

Transceiver Revision	A2pG039p.d26c
Vendor ID Code	6208
Line Mode	ADSL_G.dmt
Data Path	FAST

Transceiver Information	Down Stream Path	Up Stream Path
DSL Speed (Kbits/Sec)	2976	484
Margin (dB)	18.3	16.0
Line Attenuation (dB)	37.0	18.5
Transmit Power (dBm)	9.9	0.1
FEC Errors	0	0
HEC Errors	0	0
CRC Errors	1	0

View the ADSL Status

- **To view the gateway ADSL status:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

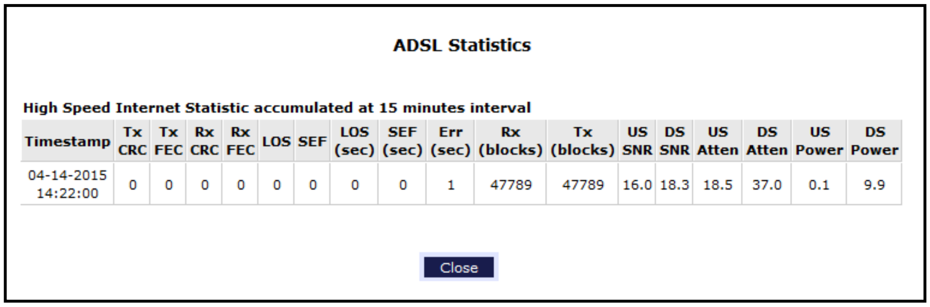
   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

4. Select **System Monitoring > Advanced Status > ADSL**.



ADSL Statistics

High Speed Internet Statistic accumulated at 15 minutes interval

Timestamp	Tx CRC	Tx FEC	Rx CRC	Rx FEC	LOS	SEF	LOS (sec)	SEF (sec)	Err (sec)	Rx (blocks)	Tx (blocks)	US SNR	DS SNR	US Atten	DS Atten	US Power	DS Power
04-14-2015 14:22:00	0	0	0	0	0	0	0	0	1	47789	47789	16.0	18.3	18.5	37.0	0.1	9.9

View the Wireless Status

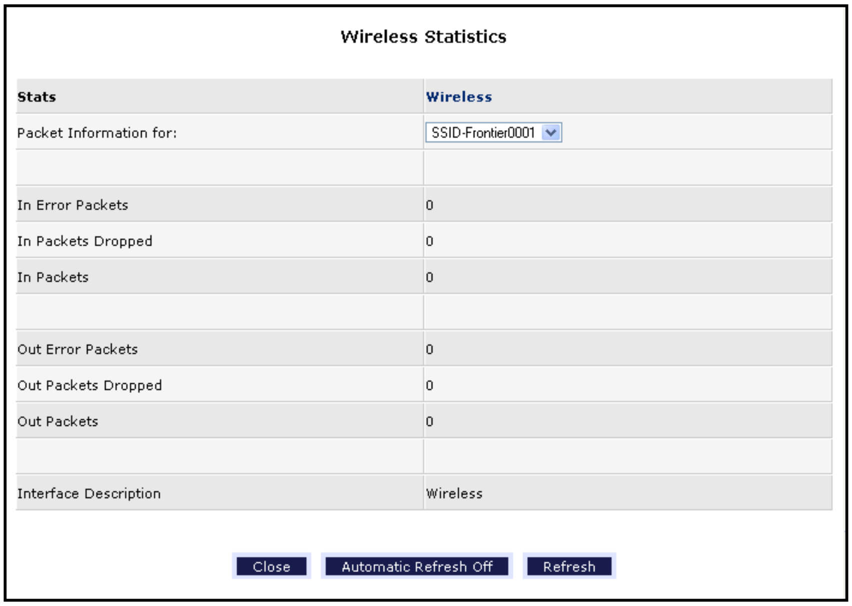
➢ **To view the gateway wireless status:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **System Monitoring > Advanced Status > Wireless**.



Wireless Statistics

Stats	Wireless
Packet Information for:	SSID-Frontier0001
In Error Packets	0
In Packets Dropped	0
In Packets	0
Out Error Packets	0
Out Packets Dropped	0
Out Packets	0
Interface Description	Wireless

Upgrade the Firmware

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

Upgrade Firmware from the Internet

➢ **To upgrade the firmware from the Internet::**

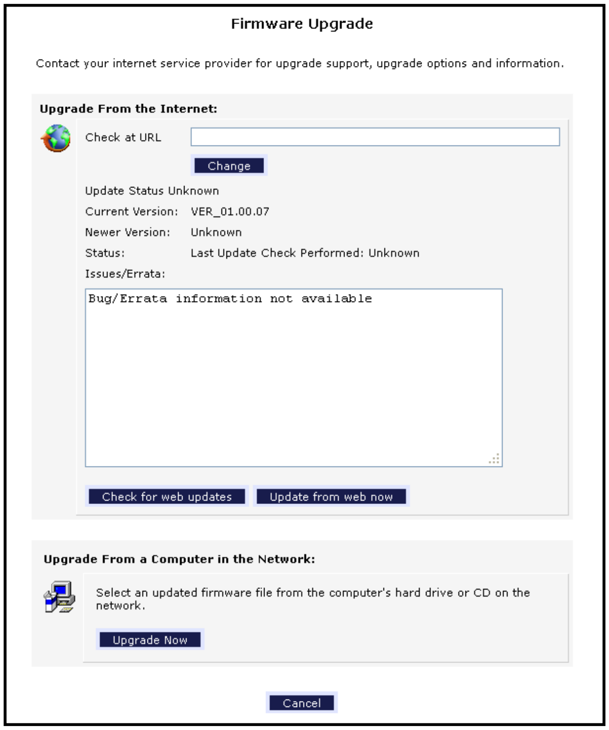
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Firmware Upgrade**.



Firmware Upgrade

Contact your internet service provider for upgrade support, upgrade options and information.

Upgrade From the Internet:

Check at URL

Update Status Unknown

Current Version: VER_01.00.07

Newer Version: Unknown

Status: Last Update Check Performed: Unknown

Issues/Errata:

```
Bug/Errata information not available
```

Upgrade From a Computer in the Network:

Select an updated firmware file from the computer's hard drive or CD on the network.

7. To check to see if new firmware is available over the Internet, in the **Check at URL** field, type the URL where your Internet service provider provides new firmware and do one of the following:
   - Click the **Check for web updates** button.
   - Click the **Update from web now** button.

The gateway checks for new firmware. If new firmware is available, the modem downloads it. If you clicked the **Update from web now** button, the gateway loads the new firmware and reboots.

⚠ WARNING:

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

When the upload is complete, your gateway restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to find out if you need to reconfigure the gateway after upgrading.

Upgrade Firmware from a Computer

➢ **To upgrade the firmware from the Internet::**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

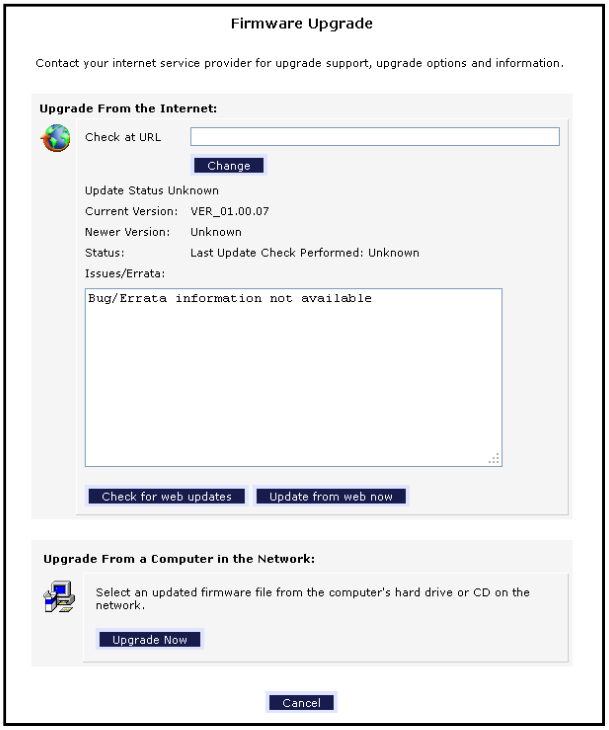
   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Firmware Upgrade**.



Firmware Upgrade

Contact your internet service provider for upgrade support, upgrade options and information.

Upgrade From the Internet:

Check at URL

Update Status Unknown

Current Version: VER_01.00.07

Newer Version: Unknown

Status: Last Update Check Performed: Unknown

Issues/Errata:

```
Bug/Errata information not available
```

Upgrade From a Computer in the Network:

Select an updated firmware file from the computer's hard drive or CD on the network.

7. Scroll down and click Upgrade From a Computer in the Network **Update Now** button.

   The Software Upgrade page displays.

8. Click the **Browse** button and select the upgrade file.
9. Click the **Upload File** button.

   If you clicked the **Update from web now** button, the gateway loads the new firmware and reboots.

WARNING:

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

When the upload is complete, your gateway restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to find out if you need to reconfigure the gateway after upgrading.

Run the Ping Utility

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

➢ **To run a ping test:**

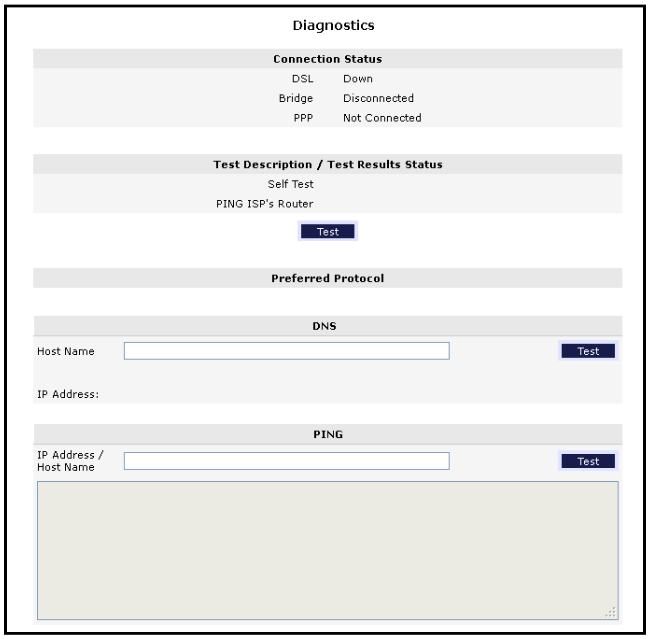
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Diagnostics**.



Diagnostics

Connection Status

DSL	Down
Bridge	Disconnected
PPP	Not Connected

7. Do one of the following:
   - To ping the ISP’s router, click the **Test** button.
   - To ping a host name, complete the **Host Name** field and click the Host Name **Test** button.

- To ping an IP address, complete the **IP Address/Host Name** field, and click the IP Address Host Name **Test** button.

The ping results display.

Run the Traceroute Utility

To display the route and measure transit delays of packets across an IP, run the traceroute utility.

➢ **To run a traceroute test:**

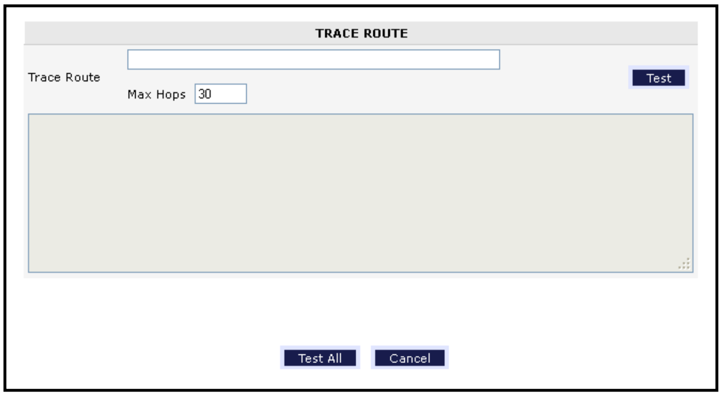
1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Diagnostics** and scroll down to the TRACE ROUTE section.



Max Hops 30

7. Specify the following parameters for the traceroute utility:
   - **Trace Route**. The IP address or host name of the computer you are tracing.
   - **Max Hops**. The maximum number of hops to allow when tracing the route.
8. Click the **Test** button.

   The traceroute results display.

View Devices Currently on the Network

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

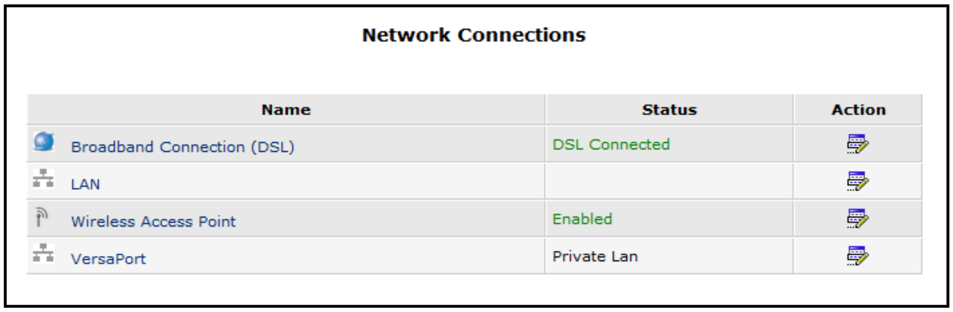
➢ **To view devices on the network:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the gateway user name and password.

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

   The Main page displays.
4. Select **My Connected Home > Network Connections**.



Network Connections

Name	Status	Action
Broadband Connection (DSL)	DSL Connected	✎
LAN		✎
Wireless Access Point	Enabled	✎
VersaPort	Private Lan	✎

Manage the Gateway Configuration File

The configuration settings of the gateway are stored within the gateway in a configuration file. You can save this file on the gateway or on your computer. You can load a saved configuration file onto the gateway.

Save the Configuration Settings

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

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.
3. Enter the user name and password.

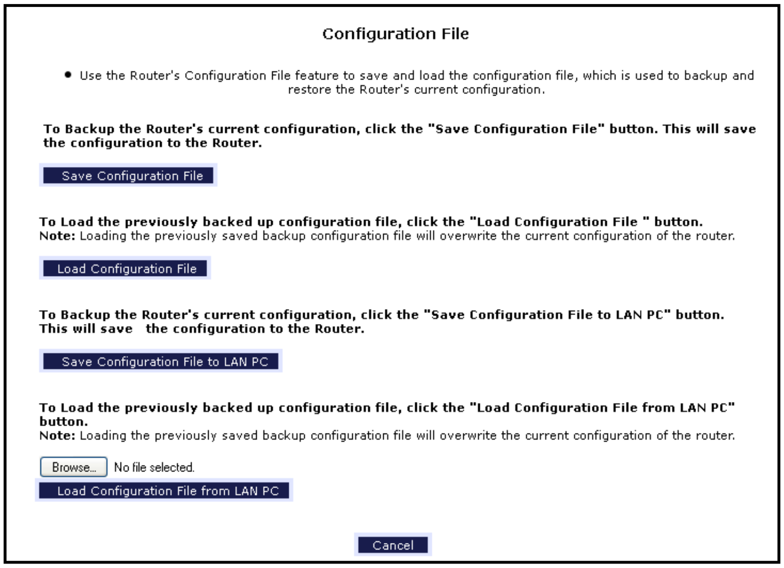
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

The Main page displays.

4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Configuration File**.



Configuration File

- Use the Router's Configuration File feature to save and load the configuration file, which is used to backup and restore the Router's current configuration.

To Backup the Router's current configuration, click the "Save Configuration File" button. This will save the configuration to the Router.

To Load the previously backed up configuration file, click the "Load Configuration File " button.
Note: Loading the previously saved backup configuration file will overwrite the current configuration of the router.

To Backup the Router's current configuration, click the "Save Configuration File to LAN PC" button. This will save the configuration to the Router.

To Load the previously backed up configuration file, click the "Load Configuration File from LAN PC" button.
Note: Loading the previously saved backup configuration file will overwrite the current configuration of the router.

No file selected.

Save Configuration File
Load Configuration File
Save Configuration File to LAN PC
Browse...
Load Configuration File from LAN PC
Cancel

7. To save the configuration settings onto the gateway, click the **Save Configuration File** button.
8. To save the configuration settings onto a computer, click the **Save Configuration File to LAN PC** button.
9. Specify a location on your network.

   A confirmation message displays.

10. Click the **OK** button.

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

Load Configuration Settings

➤ **To load configuration settings from a file that you saved:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

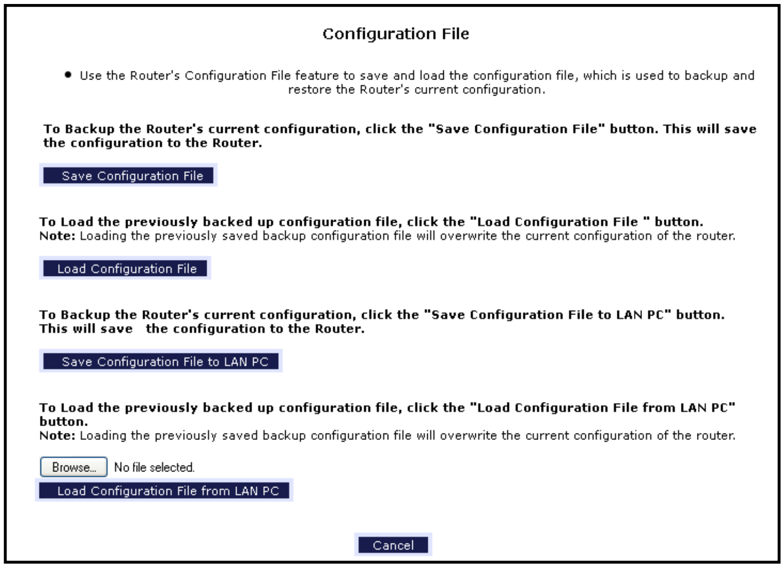
3. Enter the user name and password.

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

The Main page displays.

4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.
6. Select **Configuration File**.



Configuration File

- Use the Router's Configuration File feature to save and load the configuration file, which is used to backup and restore the Router's current configuration.

To Backup the Router's current configuration, click the "Save Configuration File" button. This will save the configuration to the Router.

To Load the previously backed up configuration file, click the "Load Configuration File " button.
Note: Loading the previously saved backup configuration file will overwrite the current configuration of the router.

To Backup the Router's current configuration, click the "Save Configuration File to LAN PC" button. This will save   the configuration to the Router.

To Load the previously backed up configuration file, click the "Load Configuration File from LAN PC" button.
Note: Loading the previously saved backup configuration file will overwrite the current configuration of the router.

No file selected.

7. To load configuration settings that you saved on the gateway, click the **Load Configuration File** button.
8. To load configuration files that you saved on a computer, click the **Load Configuration File from LAN PC** button.

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

WARNING:

Do not interrupt the reboot process.

Restore the Factory Settings

You can restore the gateway to its factory default settings except the PPP user name and password, which are retained. This process erases the other gateway configuration settings that you have set up.

➢ **To restore the gateway to its factory default settings:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Restore Defaults**.

   The Restore Defaults page displays.

7. Click the **Restore Defaults** button.

   The gateway is restored to its factory default settings. The gateway reboots.

Dynamic DNS

Internet service providers (ISPs) assign numbers called 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 don’t know what their IP addresses are or when this number changes.

To make it easier to connect, 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 gateway to use Dynamic DNS. Then the gateway 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.

Specify a DNS Account

➢ **To set up Dynamic DNS in the gateway:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

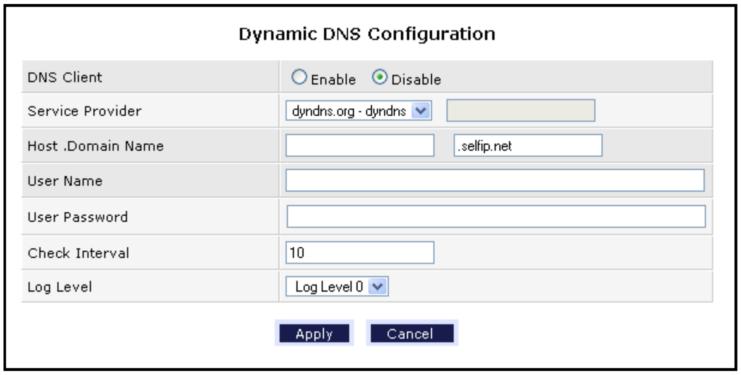
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

The Main page displays.

4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Dynamic DNS**.



Dynamic DNS Configuration

DNS Client	○ Enable ● Disable	
Service Provider	dyndns.org - dyndns	
Host .Domain Name		.selfip.net
User Name		
User Password		
Check Interval	10	
Log Level	Log Level 0	

7. Select the DNS Client **Enable** radio button.
8. In the **Service Provider** list, select your service provider.
9. In the **Host .Domain Name** field, type the host name (sometimes called the domain name) for your account.
10. In the **User Name** field, enter the user name for your account.
11. In the **User Password** field, type the password for your DDNS account.
12. Check Interval
13. Log Level
14. Click the **Apply** button.

    Your changes are saved.

Specify a DNS Server

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

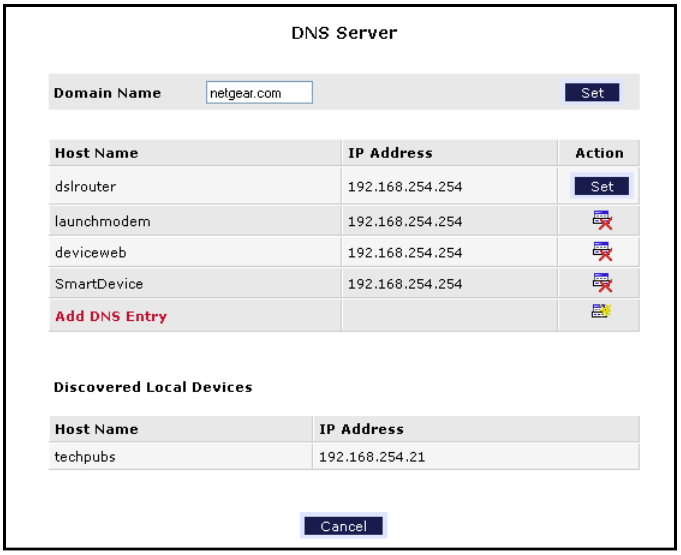
   The user name is **admin**. The default password is **admin**. The user name and password are case-sensitive.

   The Main page displays.

4. Select **Advanced.**
5. When prompted, click the **Yes** button to proceed.

The Advanced page displays.

6. Select **DNS Server**.



DNS Server

Domain Name: netgear.com

Host Name	IP Address	Action
dslrouter	192.168.254.254	Set
launchmodem	192.168.254.254	✗
deviceweb	192.168.254.254	✗
SmartDevice	192.168.254.254	✗
Add DNS Entry		✚

Discovered Local Devices

Host Name	IP Address
techpubs	192.168.254.21

7. To add a DNS entry, click the **Add DNS Entry** link and complete the fields.
8. To specify the DNS server, click the **Set** button.
9. Click the **Apply** button.

   Your changes are saved.

Specify the Date and Time Settings

By default, the gateway is set to Eastern time with Daylight Saving Time enabled. The gateway uses the Internet to access a time server to automatically set the time. You can view and change these settings.

➢ **To set the date and time:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

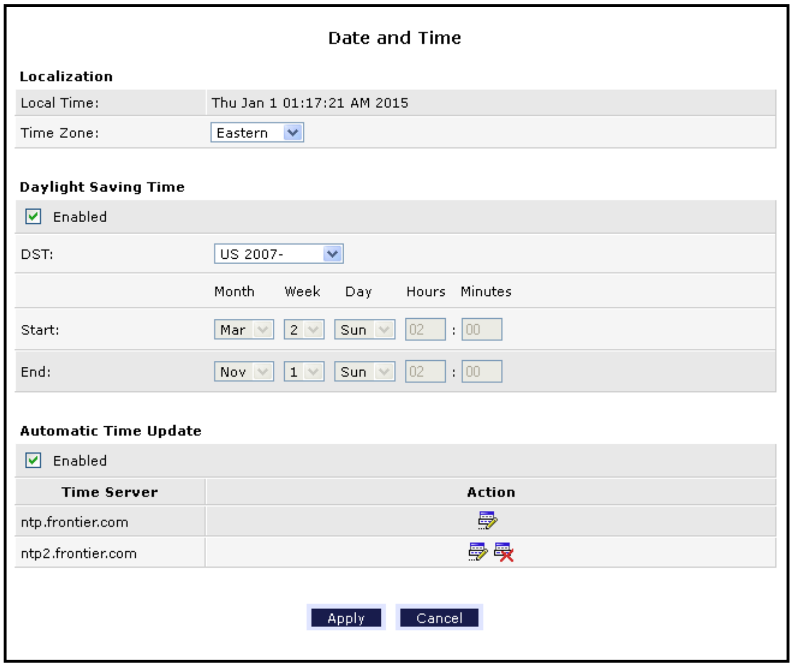
   A login window opens.
3. Enter the user name and password.

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

   The Main page displays.
4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

The Advanced page displays.

6. Select **Date and Time**.



Date and Time

Localization

Local Time:	Thu Jan 1 01:17:21 AM 2015
Time Zone:	Eastern

Daylight Saving Time

☑ Enabled

DST:	US 2007-				
	Month	Week	Day	Hours	Minutes
Start:	Mar	2	Sun	02	00
End:	Nov	1	Sun	02	00

Automatic Time Update

☑ Enabled

Time Server	Action
ntp.frontier.com	✎
ntp2.frontier.com	✎ ✗

7. Complete the fields to specify the date and time settings.

8. Click the **Apply** button.

   Your settings are saved.

Reboot the Gateway

➢ **To reboot the gateway:**

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

2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

4. Select **Advanced**.

5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **Reboot Modem**.

7. When prompted, click the OK button to confirm that you want to reboot the gateway.

   The gateway reboots.

Specify the VPN Pass-Through Method

You can specify which kind of VPN pass-through the gateway uses. By default, the gateway is set up to use PPTP, L2TP, and IPSec.

➢ **To specify VPN passthrough:**

1. Launch an Internet browser from a computer or wireless device that is connected to the network.
2. Type **http:/192.168.254.254**.

   A login window opens.

3. Enter the user name and password.

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

   The Main page displays.

4. Select **Advanced**.
5. When prompted, click the **Yes** button to proceed.

   The Advanced page displays.

6. Select **VPN**.

   The VPN page displays.

7. Select or clear the following check boxes:
   - **PPTP PassThru**
   - **L2TP PassThru**
   - **IPSec PassThru**
8. Click the **Apply** button.

   Your settings are saved.

A. Supplemental Information

A

This appendix covers the following topics:

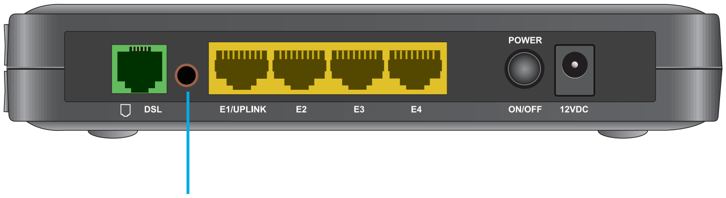
- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the gateway to its factory settings.

➤ **To reset the gateway:**

Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the gateway for 10 seconds.



Reset button

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

Table 1. Factory default settings

Feature		Default behavior
Gateway login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	admin
Local network (LAN)	LAN IP	192.168.254.254
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	
	Time zone	Pacific time
	DHCP starting IP address	Configured by the Internet provider
	DHCP ending IP address	
	DMZ	Disabled
	Time zone	As per the ISP/MSO ToD (Time of Day) Configuration
	Time zone adjusted for daylight savings time	As per ISP/MSO ToD (time of Day) server configuration
	SNMP	Enabled

Table 1. Factory default settings (continued)

Feature		Default behavior
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
Wireless	Wireless communication	Enabled
	SSID name	See the product label
	Security	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Country/region	United States
Wireless (continued)	RF channel (2.4 GHz)	Auto[1]
	Operating mode	Up to 300 Mbps at 2.4 GHz

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

Technical Specifications

Table 2. Gateway specifications

Feature	Description
Data and routing protocols	TCP/IP, DHCP, Dynamic DNS, UPnP, and SMB
Power adapter (North America)	120V, 60 Hz, input 12V/3.5A DC output
Dimensions	Dimensions: mm x mm x mm (in. x in. x in.)
Weight	Weight: g (0. lb)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B
LAN	10BASE-T or 100BASE-TX or 1000BASE-T, RJ-45
WAN	24 x 8 DOCSIS 3.0 WAN Interface
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing

Table 2. Gateway specifications (continued)

Feature	Description
Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11g IEEE 802.11b 2.4 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency range	2.4 GHz: 2.412–2.462 GHz
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2

B.

Wall-Mount the Gateway

B

This appendix describes how to wall-mount the gateway.

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

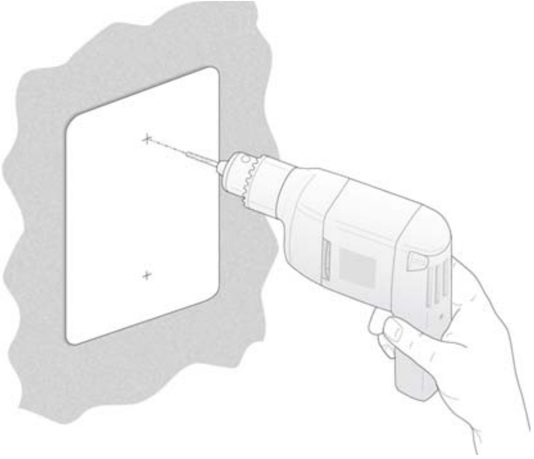
For best results, place your gateway according to the following guidelines:

- Place your gateway on an upper floor of a multifloor home or office.
- Place your gateway close to a window but avoiding direct sunlight. A window location gives the best conditions for receiving a strong 4G LTE signal.
- Place your gateway near the center of the area where your computers and other devices operate, and within line of sight to your wireless devices.
- Make sure that the gateway is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the gateway in an elevated location, minimizing the number of walls and ceilings between the gateway and your other devices.
- Place the gateway away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz cordless phone
- Place the gateway away from large metal surfaces, large glass surfaces, and insulated walls such as these:
  - Solid metal doors
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick

- Concrete

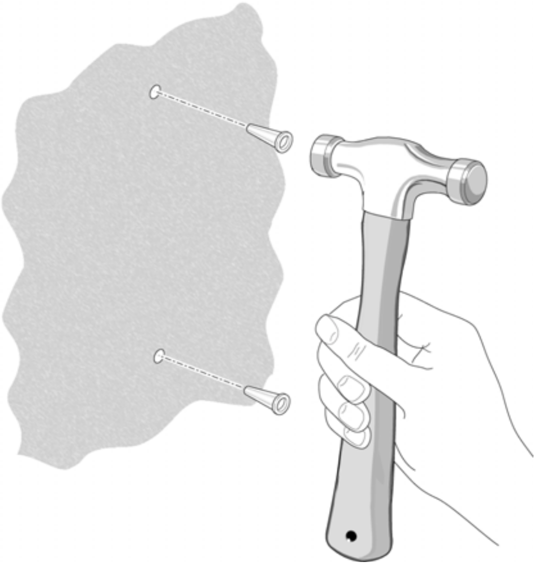
➢ **To wall-mount the gateway:**

1. Drill holes in the wall where you want to wall-mount the gateway.

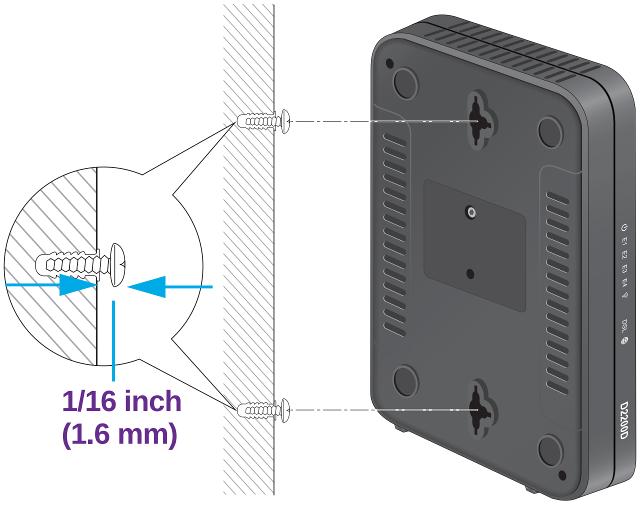


Holes must be 6-9/16 in. (167 cm) center to center.

2. Install wall anchors in the holes.



3. Use pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or No. 6 type screws, 1" inch long (U.S.).
4. Insert screws into the wall anchors, leaving 1/8 inch (3 mm) of each screw exposed.



5. Attach the gateway to the screws and secure it into place.

FCC statement

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- **Reorient or relocate the receiving antenna.**
- **Increase the separation between the equipment and receiver.**
- **Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.**
- **Consult the dealer or an experienced radio/TV technician for help.**

"FCC RF Radiation Exposure Statement Caution: To maintain compliance with the FCC's RF exposure guidelines, place the product at least 20cm from nearby persons."