

NETGEAR®

DOCSIS 3.0 N450 Wi-Fi Data Gateway CG3000Dv2 User Manual



May 2013
202-11278-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at <https://my.netgear.com>. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-11278-01	v1.0	APRIL 2013	First publication

Contents

Chapter 1 Connecting to the Internet

Gateway Front Panel	6
Gateway Rear Panel	8
Label	9
Wireless Performance and Gateway Location	9
Log In to Your Gateway	10
View Basic Settings	11

Chapter 2 Configuring Your Wireless Network

Set Up Your Wireless Network	13
Configure Wireless Settings Manually	13
Use Push 'N' Connect (WPS) Wireless Setup	15
Set Up Wi-Fi Multimedia	18
Change the Password	19

Chapter 3 Filtering Content

View Denial of Service (DoS) Attack Logs	22
Limit Internet Site Access	23
Allow Unrestricted Access	24
Disable Gateway Features	24

Chapter 4 Maintaining Your Network

View the Gateway Status	28
View the Connection Status	29
Back Up and Restore Your Settings	29
View the Event Log	30
Run the Diagnostic Utilities	31
Ping Utility	31
Traceroute Utility	33

Chapter 5 Advanced Settings

Advanced Wireless Settings	35
MAC Filtering	36
IP Filtering	38
Port Blocking	39
Port Forwarding	39

Port Triggering	41
DMZ Host	42
LAN IP Setup	43
Reserve an IP Address for DHCP Use	44
LAN Switch	44
Configure Universal Plug and Play (UPnP)	45
Set Networking Protocols	46
Enable Network Address Translation	47
Remove USB Devices	47

Chapter 6 Troubleshooting

Basic Functions	49
Connect to the Gateway's Main Menu	49
Troubleshoot the ISP Connection	50
Troubleshoot a TCP/IP Network Using a Ping Utility	50
Test the LAN Path to Your Gateway	51
Test the Path from Your Computer to a Remote Device	51

Appendix A Supplemental Information

Factory Default Settings	54
Technical Specifications	55

Appendix B Notification of Compliance

Connecting to the Internet

1

For help installing the gateway, see the DOCSIS 3.0 N450 Wi-Fi Data Gateway CG3000Dv2 User Manual.

This chapter describes how to log in and monitor your gateway and includes these sections:

- *Gateway Front Panel*
- *Gateway Rear Panel*
- *Label*
- *Log In to Your Gateway*
- *View Basic Settings*

For information about product features and compatible NETGEAR products, visit the NETGEAR website at <http://www.netgear.com>.

Gateway Front Panel

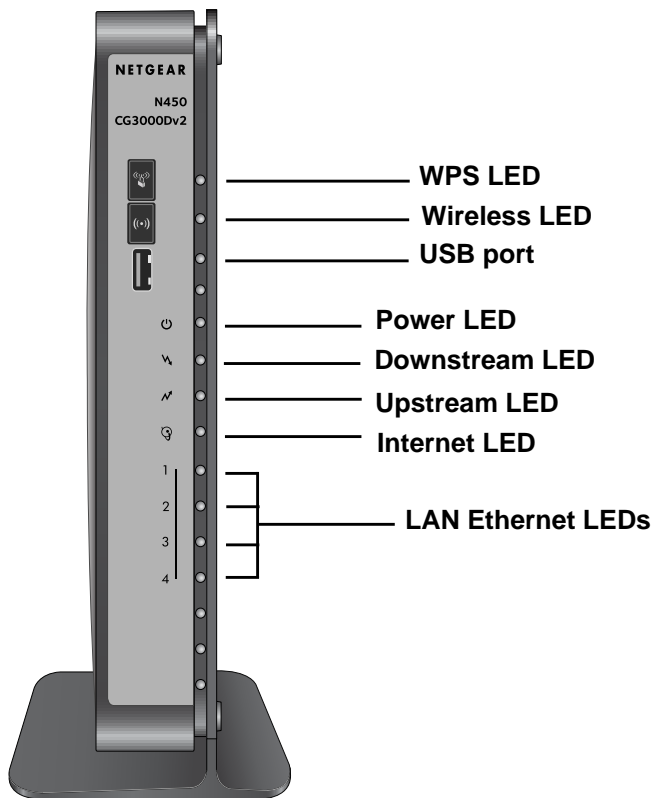









Figure 1. Gateway front view

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

Table 1. LEDs and buttons

LED	Description
 Power	<ul style="list-style-type: none"> • Solid green. Power is supplied to the cable modem. • Blinking. The modem is performing a power-on self-test. • Red. The unit is performing a self-test, or the thermal cutoff circuit has been triggered. • Off. The modem is not receiving power.
 Downstream	<ul style="list-style-type: none"> • Blue. More than one downstream channel is locked. • Green. One downstream channel is locked. • Blinking green. The unit is scanning for a downstream channel. • Off. No downstream channel is locked.

NETGEAR DOCSIS 3.0 N450 Wi-Fi Data Gateway

LED	Description (continued)
 Upstream	<ul style="list-style-type: none"> • Blue. More than one upstream channel is locked. • Solid. One upstream channel is locked. • Blinking green. The unit is ranging on the upstream. • Off. No downstream channel is locked.
 Internet	<ul style="list-style-type: none"> • Solid green. The cable modem is online. • Slow blink. The cable modem is receiving DHCP information. • Fast blink. The cable modem is downloading the configuration file. • Off. The cable modem is offline.
 LAN (Ethernet)	<p>Green indicates 1,000 Mbps. Amber indicates 100/10 Mbps.</p> <ul style="list-style-type: none"> • Solid. An Ethernet device is connected and powered on. • Blinking. Data is being transmitted or received on the Ethernet port. • Off. No Ethernet device is detected on the Ethernet port.
 Wireless On/Off	<ul style="list-style-type: none"> • Solid green. The wireless card is plugged in and enabled. • Blinking. There is traffic on the wireless card. • Off. The wireless card is either disabled or not plugged in. <p>To enable or disable the card, press this button for 3 seconds.</p>
 WPS	<p>Pressing this button opens a 2-minute window for the gateway to connect with other WPS-enabled devices. For more information, about using the WPS method to implement security, see the Use Push 'N' Connect (WPS) Wireless Setup on page 15.</p>

Gateway Rear Panel

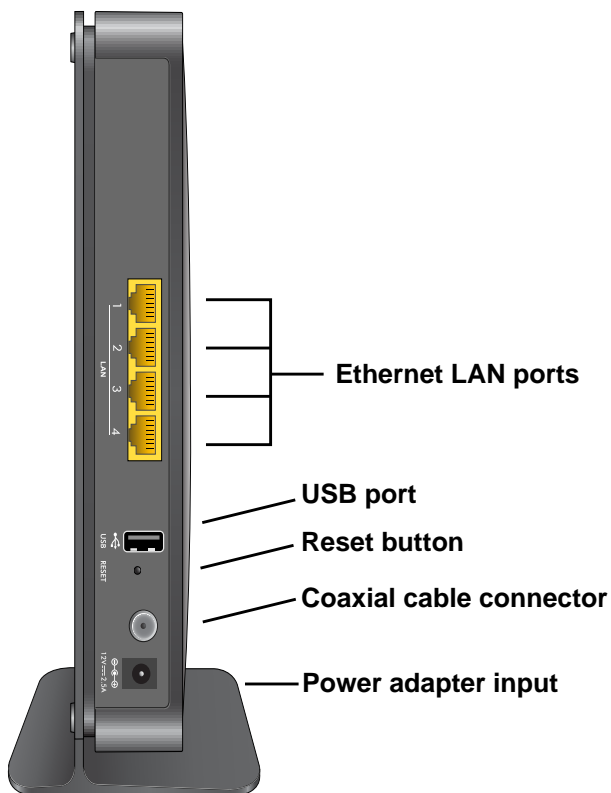


Figure 2. Gateway rear panel

The rear panel includes the following connectors, viewed from top to bottom:

- **Four Gigabit Ethernet LAN ports.** To connect local computers, use these ports.
- **USB port.** To connect a USB hard drive, flash drive, or printer, use this port.
- **Reset.** To set the gateway to the original factory settings, press and hold the **Reset** button for over 7 seconds. See [Factory Default Settings](#) on page 54.
- **Coaxial cable connector.** Attach a coaxial cable to the cable service provider's connection.
- **Power.** Power adapter input.

Label

The label on the bottom of the gateway shows the router's Restore Factory Settings button, WiFi network name (SSID), serial Number, and MAC address.

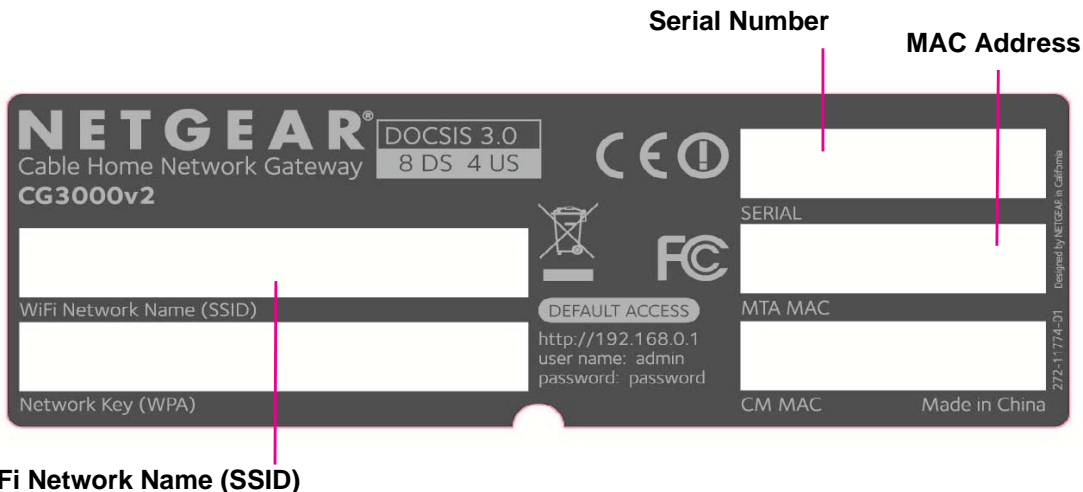


Figure 3. Label on router bottom

See [Factory Default Settings](#) on page 54 for information about the Restore Factory Settings button and the factory setting values.

Wireless Performance and Gateway Location

The range of your wireless connection can vary based on the physical placement of the gateway. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

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

- Near the center of the area in which your computers operate.
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- To provide the best side-to-side coverage, put the gateway in a vertical position.

The time it takes to establish a wireless connection can vary depending on both your security settings and the gateway location. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Log In to Your Gateway

Log in to the gateway to view or change its settings.

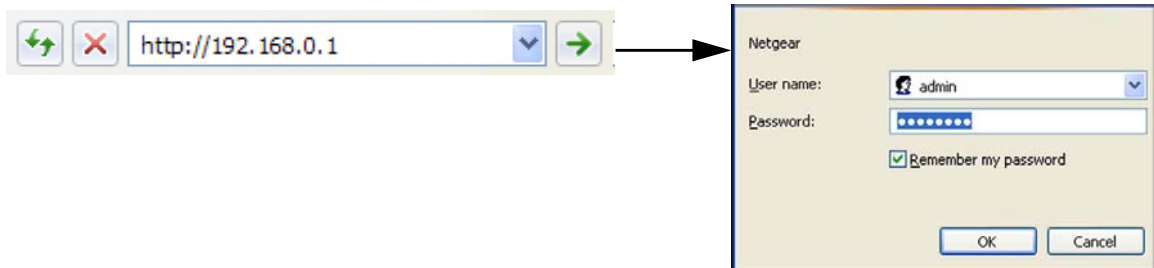
Note: To connect to the gateway, use a computer configured for DHCP (most computers are). For help with configuring DHCP, see the instructions that came with your computer.

If you do not click **Logout**, when you have logged in, the gateway waits for activity for 5 minutes before it automatically logs you out.

➤ **To log in to the gateway:**

1. On the computer that is connected to the gateway with an Ethernet cable, type **http://192.168.0.1** in the address field of your Internet browser.

A login window displays.



2. Log in with the user name **admin** and the default password, **password**.

When you connect to the gateway, the Modem Status screen displays.

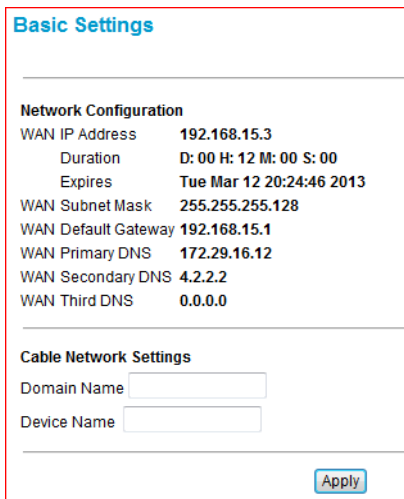
Modem Status	
Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	2.05
Software Version	V1.01.01T
Cable MAC Address	e0:46:9a:f3:43:a4
Device MAC Address	e0:46:9a:f3:43:a5
Cable Modem Serial Number	e0469af343a4
CM certificate	Installed
Status	
System Up Time	0 days 21h:13m:32s
Network Access	Allowed
Cable Modem IP Address	10.10.15.6

View Basic Settings

The Basic Settings screen displays the Internet settings for the gateway.

➤ **To view or configure basic settings:**

1. From the main menu, select **Basic Settings**.



The screenshot shows the 'Basic Settings' page. It is divided into two main sections: 'Network Configuration' and 'Cable Network Settings'. The 'Network Configuration' section lists several WAN settings: WAN IP Address (192.168.15.3), Duration (D: 00 H: 12 M: 00 S: 00), Expires (Tue Mar 12 20:24:46 2013), WAN Subnet Mask (255.255.255.128), WAN Default Gateway (192.168.15.1), WAN Primary DNS (172.29.16.12), WAN Secondary DNS (4.2.2.2), and WAN Third DNS (0.0.0.0). The 'Cable Network Settings' section contains two input fields: 'Domain Name' and 'Device Name'. An 'Apply' button is located at the bottom right of the form.

2. Enter the domain name.

If your Internet service provider requires a domain name, type that name here.

3. Enter the device name.

This name is a user-friendly name representing the gateway in the network computers running Windows Vista and the Network Explorer on all other Windows computers.

4. Click **Apply**.

2. Configuring Your Wireless Network

2

This chapter describes how to configure your gateway's Internet connection and add devices to your network. It includes the following sections:

- *Set Up Your Wireless Network*
- *Set Up Wi-Fi Multimedia*
- *Change the Password*

Note: Before changing wireless settings, connect the gateway and set up its Internet connection as described in the *DOCSIS3.0 N450 Wi-Fi Data Gateway CG3000Dv2 Quick Installation Guide*.

Set Up Your Wireless Network

To set up the wireless network, you can enter wireless settings, or you can use Wi-Fi Protected Setup (WPS). To wirelessly connect to the gateway, a computer or wireless device must be configured with the same wireless settings as the gateway.

Configure Wireless Settings Manually

You can manually configure the wireless settings and security in the Wireless Settings screen.

➤ **To view or configure the wireless settings:**

1. If you are located near the gateway, use an Ethernet cable to connect your computer to the gateway while you are changing the wireless settings.

Note: If you connect wirelessly to the gateway and then change its wireless network name (SSID) or wireless security, you will be disconnected after you click Apply.

2. Log in to the gateway.

For more information, see [Log In to Your Gateway](#) on page 10.

3. In the main menu, under Setup, select **Wireless Settings**.

The following screen displays.

Wireless Settings

Wireless Network

Name(SSID):

Region:

Channel: Current: 1

802.11 mode:

Security Options

Disable
 WEP
 WPA-PSK[TKIP]
 WPA2-PSK[AES]
 WPA-PSK[TKIP] + WPA2-PSK[AES]
 WPA/WPA2 Enterprise

WPA2-PSK[AES]

Passphrase: (8-63 characters)

Hide Key

4. Specify the Wireless Network settings for your network:

- **Name (SSID).** The name of the wireless network.

The default wireless network name (SSID) for the gateway appears on the label of the gateway. You can enter a different name here for better wireless security and to make it easier to recognize your network when you want to connect to it wirelessly.

- **Region.** The location where the gateway operates.
- **Channel.** The available channels depend on the region. Some countries have laws specifying which channels should be used. To reduce interference when using more than one access point, NETGEAR recommends using 5-channel spacing between adjacent access points (for example, use Channels 1 and 6, or 6 and 11).
- **802.11 Mode.** This value is set to Up to 217 Mbps by default. You can specify the mode to support faster equipment or legacy equipment.

5. Specify the security options:

- By default the gateway works with WPA and WPA 2 wireless security. You can specify the network key, which works like a password to access the wireless network.
 - a. Set up WPA or WPA2 wireless security.
 - **WPA-PSK.** This setting provides the TKIP encryption type and a pre-shared key.
 - **WPA2-PSK.** This setting provides the AES encryption type and a pre-shared key.

Note: Configure your wireless computers with the same WPA2 or WPA settings as your gateway so that you can connect.

- b. Depending on the WPA setting that you select, enter the required information.


For WPA-PSK or WPA2-PSK, enter the pre-shared key, which is a password between 8 and 63 characters. The default WPA password appears on the label of your gateway.


Note: By default, the gateway is set up to work with WPA and WPA2 wireless security, both of which are newer than WEP. Typically, the only reason you might need to set up WEP would be to allow access to older wireless computers or devices that cannot support WPA.

6. Click **Apply**.

Note: If you plan to use WPS, and you want to keep your wireless settings the same, go to the Advance Wireless Settings screen and make sure that the **Keep Existing Settings** check box is selected. See *Advanced Wireless Settings* on page 35.

Use Push 'N' Connect (WPS) Wireless Setup

Push 'N' Connect (WPS) can be a quick way to automatically set up your gateway's wireless network and set up your wireless computer to connect to it at the same time. WPS, also called Wi-Fi Protected Setup, is relatively new technology, so before you decide to use it, check to make sure your wireless computers and devices support WPS. Look for the  symbol on all the computers that connect wirelessly to the gateway.

If you do not see the  symbol on all the computers that connect to the wireless network, then you should manually set up your network first (see *Configure Wireless Settings Manually* on page 13). After that, you can still use WPS to set up the wireless connection for the computers that support WPS.

Note: All WPS-capable products should be compatible with the gateway. For more information about the WPS standard, visit <http://www.wi-fi.org>.

Two Push 'N' Connect methods are available, WPS button and PIN (personal identification number).

Add a Client Using the WPS Button

Note: The first time you use WPS, it assigns a random network name (SSID) and a random password to your wireless network. If you want to keep the network name and password you specified in the Wireless Settings screen, you must select the **Keep Existing Settings** check box in the Advanced Wireless Settings screen. See *Advanced Wireless Settings* on page 35.

Any computer or wireless device that connects wirelessly to the gateway is a client. After a device is added as a client, it can automatically connect to the gateway.

- **To add a wireless device to your gateway using the WPS button:**
 1. Make sure that you know how WPS works on your computer or wireless device.

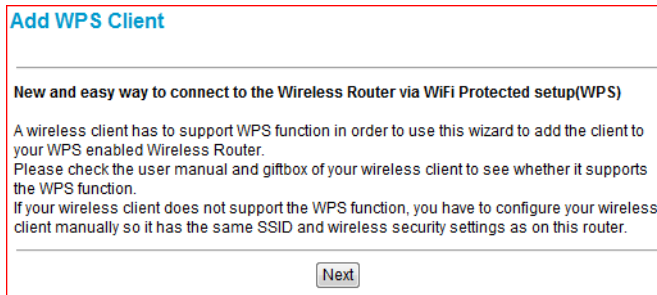
If it works with WPS, it has a WPS utility and might also have a WPS button that you can press.

2. Log in to the gateway.

For more information, see [Log In to Your Gateway](#) on page 10.

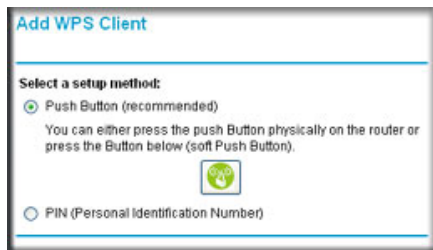
3. In the main menu, select **Add WPS Client**.



The following screen displays.

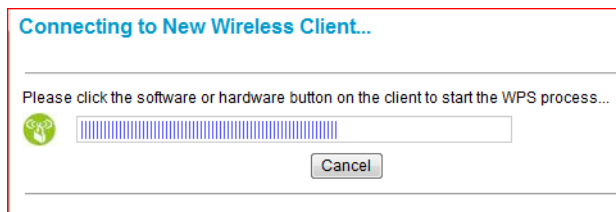


4. Click **Next**.

The Add WPS Client screen displays:



5. Either click the  **WPS** button, or press the  button on the front of the gateway.



- The WPS LED on the front of the gateway begins to blink.
 - The gateway tries to communicate with the wireless computer or device for 2 minutes.
 - If the security option in the Wireless Settings screen was set to Disable, it is automatically changed to WPA-PSK [TKIP] + WPA2-PSK [AES], including a random wireless security password.
6. Go to the wireless computer, and run its WPS configuration utility.
 7. To click the WPS button, follow the utility's instructions.

When the computer connects to the wireless network, the gateway sends its SSID and WPA-PSK or WPA2-PSK configuration to that computer.

8. On the computer that just joined the wireless network, make sure you can connect to the Internet.

You should see the gateway's Internet LED blink, showing that the Internet connection is in use.

Add a Client Using a PIN

Any computer or wireless device that connects wirelessly to the gateway is a client. After a device is added as a client, it can automatically connect to the gateway.

➤ **To add a wireless device to your gateway using a PIN:**

1. Make sure that you know how WPS works on your computer or wireless device.

If it works with WPS, it has a WPS utility. To determine the PIN for your wireless computer or device, use this utility.

2. Log in to the gateway.

For more information, see [Log In to Your Gateway](#) on page 10.

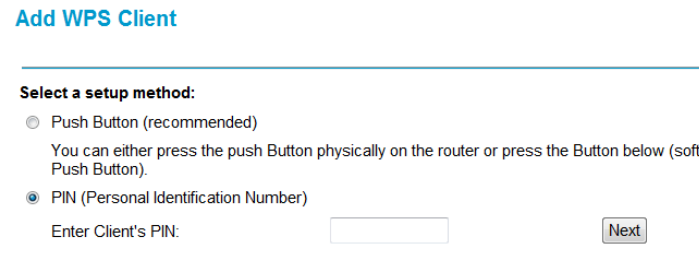
3. In the main menu, select **Add WPS Client**.

The following screen displays.



4. Click **Next**.

The Add WPS Client screen displays.



5. Select the **PIN** radio button.
6. In the Enter Client's PIN field, type the PIN that you located in Step 1.
7. Click **Next**.

- The WPS LED on the front of the gateway begins to blink.
- The gateway tries to communicate with the wireless computer or device for 4 minutes.
- If the security option in the Wireless Settings screen was set to Disable, it is automatically changed to WPA-PSK (including a PSK security password).

When the computer connects to the wireless network, the gateway sends its SSID and WPA-PSK or WPA2-PSK configuration to that computer.

8. On the computer that just joined the wireless network, make sure you can connect to the Internet.

You should see the gateway's Internet LED blink, showing that the Internet connection is in use.

Set Up Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) provides basic Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four access categories, voice, video, best effort, and background. It does not, however, provide guaranteed throughput. You can use the Wi-Fi Multimedia screen to set up wireless multimedia Quality of Service (QoS).

➤ To set up Wi-Fi Multimedia:

1. Log in to the gateway.

For more information, see [Log In to Your Gateway](#) on page 10.

2. In the main menu, under Setup, select **Wi-Fi Multimedia**.

The following screen displays.

The screenshot shows the 'Wi-Fi Multimedia(WMM)' configuration page. It has a title bar with the text 'Wi-Fi Multimedia(WMM)'. Below the title bar, there are three rows of settings, each with a label and a dropdown menu:

- WMM Support: On
- No-Acknowledgement: Off
- Power Save Support: On

At the bottom of the settings area, there is an 'Apply' button.

3. Specify the Wi-Fi Multimedia setting for the network:

- **WMM Support.** Select **On** to enable WMM.
- **No-Acknowledgement.** Select **Off** if you want to use Acknowledgement (ACK) messages. Select **On** if you do not want to use acknowledgement messages.

Usually, Off is selected. If wireless communication quality is poor at your location, select **On** so that you are notified when a package is lost. High interference levels can cause poor communication.

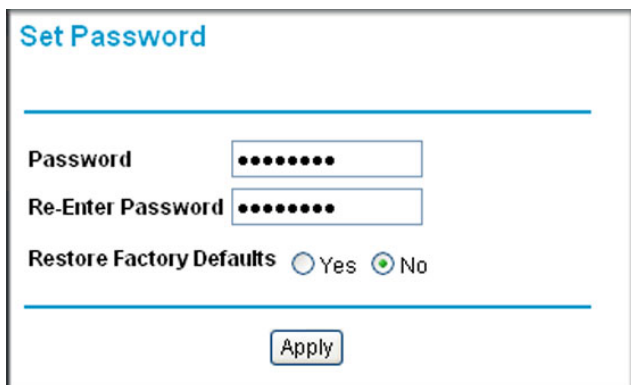
- **Power Save Support.** To conserve battery power in smaller devices that are connected to the gateway, select **On**.
4. Click **Apply**.

Change the Password

For security reasons, the gateway has its own user name and password. NETGEAR recommends that you change the default password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both uppercase and lowercase letters, numbers, and symbols. Passwords can contain up to 30 characters.

➤ **To change the password:**

1. In the main menu, under Maintenance, select **Set Password**.



The screenshot shows the 'Set Password' configuration page. It features a title 'Set Password' at the top left. Below the title is a horizontal line. There are two text input fields: 'Password' and 'Re-Enter Password', both containing seven black dots. Below these fields is a 'Restore Factory Defaults' section with two radio buttons: 'Yes' (unselected) and 'No' (selected). At the bottom of the form is an 'Apply' button.

2. Enter the new password twice.
3. To restore the factory default values, select the Yes radio button.
See [Label](#) on page 9 for default values.
4. Click **Apply**.

Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the gateway settings previously, create a new backup so that the saved settings file includes the updated password.

3. Filtering Content

3

This chapter describes how to monitor and filter the content traveling on your network. When you log in to the gateway (see *Log In to Your Gateway* on page 10), these tasks are grouped under Content Filtering. This chapter includes the following sections:

- *View Denial of Service (DoS) Attack Logs*
- *Limit Internet Site Access*
- *Allow Unrestricted Access*
- *Disable Gateway Features*

View Denial of Service (DoS) Attack Logs

A content filter log is a detailed record of the denial of service (DoS) attacks directed at your network. You can set up email notification or you can view the logs on the gateway.

➤ **To receive notification of attacks by email:**

1. In the main menu, under Content Filtering, select **Logs**.

Logs

Contact Email Address

SMTP Server Name

E-mail Alerts Enable

Description	Count	Last Occurrence	Target	Source
TCP- or UDP-based Port Scan	7	Mon Apr 15 21:41:05 2013	192.168.15.50:59325	172.29.16.12:53

2. Enter an email address.

This address is the full email address to which you want the gateway to send logs.

3. Enter the SMTP server name.

Type the outgoing SMTP mail server of your ISP. If you leave this box blank, the gateway does not send logs.

4. Select the E-mail Alerts **Enable** check box.

5. Click **Apply**.

6. Perform any of the following actions:

- To refresh the display, click **Refresh**.
- To send the log to the contact email address, click **E-mail Log**.
- To clear the log entries from the display, click **Clear Log**.

Limit Internet Site Access

You can establish rules to limit access to certain Internet websites in one of two ways:

- Blocking sites that contain certain words.
- Blocking access to certain domains.

➤ **To block access to sites containing certain words:**

1. In the main menu, under Content Filtering, select **Block Sites**.

2. Select the Keyword Blocking **Enable** check box.
3. In the Keyword List, enter the words you want to block.
4. Click **Add Keyword**.

➤ **To allow a keyword that was previously blocked:**

1. Select the keyword.
2. Click **Remove Keyword**.

➤ **To block access to certain domains:**

1. In the main menu, under Content Filtering, select **Block Sites**.

2. Select the Domain Blocking **Enable** check box.
3. In the Keyword List, enter the domain you want to block.

4. Click **Add Domain**.

➤ **To unblock a domain:**

1. Select the domain name.
2. Click **Remove Domain**.

Allow Unrestricted Access

You can specify up to three computers to have unrestricted access to the Internet.

➤ **To allow unrestricted access:**

1. In the main menu, under Content Filtering, select **Block Sites**.

Allow Trusted Computer to Visit Blocked Sites

Trusted Computer 00 : 00 : 00 : 00 : 00 : 00

00 : 00 : 00 : 00 : 00 : 00

00 : 00 : 00 : 00 : 00 : 00

Apply Cancel

2. Select the **Allow Trusted Computer to Visit Blocked Sites** check box.
3. Enter the MAC address of each computer.
4. Click **Apply**.

Disable Gateway Features

You can disable the following types of gateway features:

- Firewall features
- Web features
- NAT ALG status features

➤ **To disable specific firewall features:**

In the main menu, under Content Filtering, select **Services**.

Firewall features appear near the top of the screen.

Firewall Features Enable

IPSec PassThrough Enable

PPTP PassThrough Enable

Multicast Enable

Port Scan Detection Enable

IP Flood Detection Enable

The following table describes the fields displayed in this screen.

Table 1. Firewall features

Feature	Description
Firewall	<ul style="list-style-type: none"> • Enable. The gateway performs stateful packet inspection (SPI). • Disable. The gateway does not perform SPI.
IPSec Pass-Through	<ul style="list-style-type: none"> • Enable. The gateway forwards IPS traffic. • Disable. The gateway blocks traffic.
PPTP Pass-Through	<ul style="list-style-type: none"> • Enable. The gateway forwards PPTP traffic. • Disable. The gateway blocks PPTP traffic.
Multicast	<ul style="list-style-type: none"> • Enable. The gateway passes multicasting streams through the firewall. • Disable. The gateway blocks multicasting streams.
Port Scan Detection	<ul style="list-style-type: none"> • Enable. The gateway responds to Internet-based port scans. • Disable. The gateway does not respond to Internet-based port scans.
IP Flood Detection	<ul style="list-style-type: none"> • Enable. The gateway blocks malicious devices that are attempting to flood devices. • Disable. The gateway does not block malicious devices.

➤ **To disable specific web features:**

In the main menu, under Content Filtering, select **Services**.

Web features appear near the middle of the screen.

Web Features	
Filter Proxy	<input type="checkbox"/> <i>Enable</i>
Filter Cookies	<input type="checkbox"/> <i>Enable</i>
Filter Java Applets	<input type="checkbox"/> <i>Enable</i>
Filter ActiveX	<input type="checkbox"/> <i>Enable</i>
Filter Popup Windows	<input type="checkbox"/> <i>Enable</i>
Block Fragmented IP Packets	<input type="checkbox"/> <i>Enable</i>

To block certain web-oriented cookies, Java scripts, and pop-up windows, select the corresponding check boxes.

➤ **To disable specific NAT ALG Status features:**

In the main menu, under Content Filtering, select **Services**.

NAT ALG status features appear near the bottom of the screen.

NAT ALG Status	
RSVP	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable
Kerb88	<input checked="" type="checkbox"/> Enable
NetBios	<input checked="" type="checkbox"/> Enable
IKE	<input checked="" type="checkbox"/> Enable
RTSP	<input checked="" type="checkbox"/> Enable
Kerb1293	<input checked="" type="checkbox"/> Enable
H225	<input checked="" type="checkbox"/> Enable
PPTP	<input checked="" type="checkbox"/> Enable
MSN	<input checked="" type="checkbox"/> Enable
SIP	<input checked="" type="checkbox"/> Enable
ICQ	<input checked="" type="checkbox"/> Enable
IRC666x	<input checked="" type="checkbox"/> Enable
ICQTalk	<input checked="" type="checkbox"/> Enable
Net2Phone	<input checked="" type="checkbox"/> Enable
IRC7000	<input checked="" type="checkbox"/> Enable

To allow NAT traversal filters for certain application layer control/data protocols, select the corresponding check boxes.

4 Maintaining Your Network

4

This chapter describes how to perform network maintenance tasks with your gateway. When you log in to the gateway (see *Log In to Your Gateway* on page 10), these tasks are grouped under Maintenance.

This chapter includes the following sections:

- *View the Gateway Status*
- *View the Connection Status*
- *Back Up and Restore Your Settings*
- *View the Event Log*
- *Run the Diagnostic Utilities*

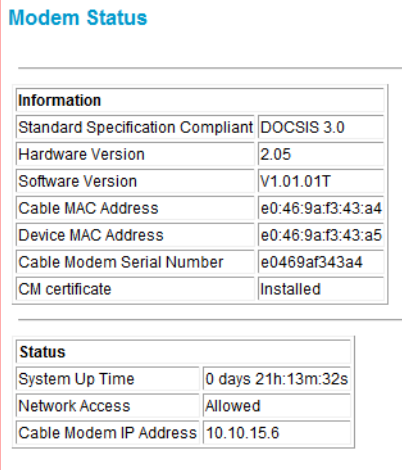
View the Gateway Status

To see hardware and firmware details and basic status information about the gateway, use the Modem Status screen.

➤ **To view the gateway status:**

From the main menu, under Maintenance, select **Modem Status**.

The following screen displays.



The screenshot shows the 'Modem Status' screen with two tables. The first table, titled 'Information', lists various modem details. The second table, titled 'Status', shows system and network information.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	2.05
Software Version	V1.01.01T
Cable MAC Address	e0:46:9a:f3:43:a4
Device MAC Address	e0:46:9a:f3:43:a5
Cable Modem Serial Number	e0469af343a4
CM certificate	Installed

Status	
System Up Time	0 days 21h:13m:32s
Network Access	Allowed
Cable Modem IP Address	10.10.15.6

The following table describes the fields displayed in this screen:

Modem field	Description
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	The hardware version of the gateway.
Software Version	The version of firmware currently running on the gateway.
Cable MAC Address	The MAC address used by the cable modem port of the gateway. This MAC address might need to be registered with your cable service provider.
Device MAC Address	The WAN MAC address used by the device.
Cable Modem Serial Number	The serial number of the gateway hardware.
CM certificate	If the cable modem certificate is installed, it is possible for the service provider to upgrade your Data Over Cable service securely.
System Up Time	Time since the last boot-up.
Network Access	Shows whether traffic can be forwarded from the LAN to the network.
Cable Modem IP Address	The current Internet IP address. If assigned dynamically and not connected to the Internet, this field is blank.

View the Connection Status

To track the gateway's initialization procedure, and to get details about the downstream and upstream cable channel, use the Connection screen. The time appears after the gateway is initialized.

- **To view the gateway's initialization procedure:**

In the main menu, under Maintenance, select **Connection**.

Connection							
Startup Procedure							
Procedure	Status	Comment					
Acquire Downstream Channel	591000000 Hz	Locked					
Connectivity State	OK	Operational					
Boot State	OK	Operational					
Configuration File	OK						
Security	Enabled	BPI+					
Downstream Bonded Channels							
Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power	SNR	Docsis/EuroDocsis locked
Locked	QAM256	17	5360537 sym/sec	591000000 Hz	1.5 dBmV	41.7 dBmV	Docsis
Locked	QAM256	11	5360537 sym/sec	555000000 Hz	1.6 dBmV	41.3 dBmV	Docsis
Locked	QAM256	12	5360537 sym/sec	561000000 Hz	1.7 dBmV	40.5 dBmV	Docsis
Locked	QAM256	13	5360537 sym/sec	567000000 Hz	1.7 dBmV	40.4 dBmV	Docsis
Locked	QAM256	14	5360537 sym/sec	573000000 Hz	2.2 dBmV	41.0 dBmV	Docsis
Locked	QAM256	15	5360537 sym/sec	579000000 Hz	2.1 dBmV	42.5 dBmV	Docsis
Locked	QAM256	16	5360537 sym/sec	585000000 Hz	1.8 dBmV	42.1 dBmV	Docsis
Locked	QAM256	10	5360537 sym/sec	549000000 Hz	2.0 dBmV	41.1 dBmV	Docsis
Upstream Bonded Channels							
Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power		
Locked	ATDMA	10	5120 Ksym/sec	18000000 Hz	50.7 dBmV		
Locked	ATDMA	11	5120 Ksym/sec	24400000 Hz	50.7 dBmV		
Locked	ATDMA	12	5120 Ksym/sec	30800000 Hz	50.7 dBmV		
Locked	ATDMA	13	5120 Ksym/sec	37200000 Hz	50.7 dBmV		
Current System Time: Thu Apr 29 00:53:40 2010							

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

- Scans and locks the downstream frequency and links back in the upstream direction.
- Obtains a gateway IP address for the gateway itself.
- Assigns an IP address for the connected computer.
- Connects to the Internet.

Back Up and Restore Your Settings

The configuration settings of the gateway are stored in a configuration file in the gateway.

➤ **To back up the settings:**

1. In the main menu, under Maintenance, select **Backup**.

Backup Settings

Save a copy of current settings

Restore saved settings from a disk

2. Click **Back Up**.

If you did not set up your browser to save downloaded files automatically, indicate where you want to save the file and click **Save**.

If you did set up your browser to save downloaded files automatically, the file is saved to the browser's download location on the hard drive.

➤ **To restore the backup settings:**

1. In the main menu, under Maintenance, select **Backup**.

Backup Settings

Save a copy of current settings

Restore saved settings from a disk

2. Click **Browse**.
3. Locate and select the previously saved backup file, then click **Restore**.

A message notifies you when the gateway has been restored to the previous settings. Then the gateway restarts, which takes about 1 minute.

Note: When restoring configuration settings, do not interrupt the process by going online, turning off the gateway, or shutting down the computer.

View the Event Log

The gateway logs security-related events such as denied incoming service requests and hacker probes.

➤ **To view the event log:**

1. In the main menu, under Maintenance, select **Event Log**.

Event Log		
Time	Priority	Description
Tue Mar 12 11:54:23 2013	Error (4)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:17:10:00:69:87;CM-QOS=1.1;CM-VER=3.0;
Tue Mar 12 08:24:21 2013	Error (4)	DHCP RENEW WARNING - Field invalid in response v4 option;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:17:10:00:69:87;CM-QOS=1.1;CM-VER=3.0;
Tue Mar 12 08:20:50 2013	Error (4)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:17:10:00:69:87;CM-QOS=1.1;CM-VER=3.0;
Tue Mar 12 02:24:21 2013	Error (4)	DHCP RENEW WARNING - Field invalid in response v4 option;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:17:10:00:69:87;CM-QOS=1.1;CM-VER=3.0;
Mon Mar 11 14:17:27 2013	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:22:90:de:69:4c;CM-QOS=1.0;CM-VER=3.0;
Mon Mar 11 14:16:59 2013	Warning (5)	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=e0:46:9a:f3:43:a4;CMTS-MAC=00:22:90:de:69:4c;CM-QOS=1.0;CM-VER=3.0;

2. Do either of the following:
 - To clear the log, click **Clear Log**.
 - To refresh the log, click **Refresh**.

Run the Diagnostic Utilities

From the Diagnostics screen, you can run ping and traceroute utilities.

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. Log in to the gateway.

For more information, see *Log In to Your Gateway* on page 10.

2. In the main menu, under Maintenance, select **Diagnostics**.

3. In the Utility list, select **Ping**.

The screenshot shows the 'Diagnostics' page with the 'Utility' dropdown set to 'Ping'. Under 'Ping Test Parameters', the 'Target' is 192.168.0.1, 'Ping Size' is 64 bytes, 'No. of Pings' is 3, and 'Ping Interval' is 1000 ms. There are buttons for 'Start Test', 'Abort Test', and 'Clear Results'. The 'Results' section is currently empty, displaying 'Waiting for input...'.

4. Specify the following parameters for the ping utility.
- **Target.** The IP address of the ping target computer.
 - **Ping Size.** The size of the ping packet.
 - **No. of Pings.** The number of times to ping the target computer.
 - **Ping Interval.** The time between pings.
5. Click **Start Test**.

The ping results display:

The screenshot shows the 'Diagnostics' page with the 'Utility' dropdown set to 'Ping'. The 'Ping Test Parameters' are the same as in the previous screenshot. The 'Results' section now displays the following text:

```
Pinging 192.168.0.1 with 64 of data:[Complete]
Reply from 192.168.0.1: bytes = 64, time = 0 ms
Reply from 192.168.0.1: bytes = 64, time = 0 ms
Reply from 192.168.0.1: bytes = 64, time = 0 ms
3/3 replies received.
min time=0 ms, max time=1 ms, avg time=0 ms
```

- **To stop a ping test:**
Click **Abort Test**.
- **To clear the results from the display:**
Click **Clear Results**.

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. Log in to the gateway.
For more information, see [Log In to Your Gateway](#) on page 10.
2. In the main menu, under Maintenance, select **Diagnostics**.
3. In the Utility list, select **Traceroute**.

4. Specify the following parameters for the traceroute utility.
 - **Target.** 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.
 - **Data Size.** The input the size of the packet.
 - **Base Port.** The port number to send the packet to.
 - **Resolve Host.** Select **on** to resolve the host name to the IP address.
5. Click **Start Test**.

The traceroute results display.

➤ **To clear the results from the display:**

Click **Clear Results**.

5. Advanced Settings

5

This chapter describes how to customize your network through the advanced settings on your gateway. When you log in to the gateway (see *Log In to Your Gateway* on page 10), these tasks are grouped under Advanced.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *MAC Filtering*
- *IP Filtering*
- *Port Blocking*
- *Port Forwarding*
- *Port Triggering*
- *DMZ Host*
- *LAN IP Setup*
- *Reserve an IP Address for DHCP Use*
- *LAN Switch*
- *Configure Universal Plug and Play (UPnP)*
- *Set Networking Protocols*
- *Enable Network Address Translation*
- *Remove USB Devices*

Advanced Wireless Settings

To configure the wireless radio settings, and other advanced settings, use the Advanced Wireless Settings screen.

➤ **To configure advanced wireless settings:**

1. In the main menu, under Advanced, select **Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. Configure the settings described in the following table.

Advanced Wireless Settings		Description
Wireless Access Point	Enable	By default this check box is selected so that the gateway works as a wireless access point. You can turn off the wireless radio to disable access through this device, which can be helpful for configuration, network tuning, or troubleshooting activities.
Advanced Configuration	<ul style="list-style-type: none"> • Fragmentation Threshold • CTS/RTS Threshold • Preamble Mode 	The default settings for these fields usually work fine. Change them only if you have a specific reason for doing so.

Advanced Wireless Settings		Description
WPS Settings	Disable router's PIN	Selecting this check box disables the PIN that WPS clients use to connect to the gateway with the PIN method. Normally this check box is cleared, which is the default setting.
	Keep Existing Settings	If a WPS client is added, the gateway automatically selects this check box. When the Keep Existing Settings check box is selected, the SSID and wireless security settings remain the same when more WPS clients are added.
Wireless Access List	Set up Access List	Access control is disabled by default so that any computer that is configured with the correct SSID can connect.

3. Click **Apply**.

MAC Filtering

By default, the gateway allows any connected computer to access the Internet. The MAC Filtering screen lets you block specific computers, based on their MAC addresses, from access to the Internet on selected days and times.

➤ **To use MAC filtering to block Internet access for a specific computer:**

1. In the main menu, under Advanced, select **MAC Filtering**.

The Trusted Devices table shows computers that have access to the Internet through the gateway.

2. In the Add MAC Filter table, use one of these methods to specify computers to block:

- If the computer is in the Trusted Devices table, select its radio button. The MAC address is added into the Add MAC Filter table.
- If the computer you want is not listed, click **Refresh** to update the Trusted Devices table.

If the computer is still not listed, complete the Device Name and MAC Address fields.

3. Click **Add**.

The Enable check box for the computer in the MAC Filter List is automatically selected.

4. To block the computer, select the days and times:

- **Days to Block.** Select the days to block the computer selected in the MAC Filter List. The default is Everyday.

- **Time of Day to Block.** You can specify the time of day to block the computer. The default is All Day. Be sure that you clear the **All Day** check box if you want to enter specific times. The selected period applies to each day that you selected.
5. Click **Apply**.
 6. Repeat these steps for all computers that you want to block.
- **To stop blocking a computer:**
1. In the MAC Filter List, select the computer.
 2. Clear its **Enable** check box.
The computer remains in the list; however, it is not blocked.
 3. Click **Apply**.
- **To remove a computer from the list:**
1. In the MAC Filter List, select the computer.
 2. Click **Delete**.
 3. Click **Apply**.

IP Filtering

By default, any computer is allowed access to the Internet through your gateway. You can use IP filtering to block specific computers based on their IP addresses from access to the Internet on selected days and times.

➤ To set up IP filtering:

1. In the main menu, under Advanced, select **IP Filtering**.

The Trusted Devices table shows computers that are allowed access to the Internet through your gateway.

2. Add devices to the IP Filter List as needed:

- If the computer you want to add appears in the Trusted Devices table, select its radio button to capture its IP address.

If the computer you want is not listed, click **Refresh** to update the Trusted Devices table.

- If the name of the computer you want to add does not display, you can type a name for the computer you are adding; or enter the IP address of the computer you want to block.

3. Click **Add**.

The Enable check box is automatically selected.

4. Select the days to block.

5. In the Time of Day to Block section, select a start time and an end time. This time range applies to each day you selected in Day(s) to Block section for the specific computer. All day is the default value.

6. Click **Apply**.

➤ To delete a device from the IP Filter List:

1. In the main menu, under Advanced, select **IP Filtering**.
2. Select the computer.
3. Click **Delete**.
4. Click **Apply**.

The screenshot shows the 'IP Filtering' configuration page. It features a 'Trusted Devices' table with columns for Device Name, IP Address, MAC Address, and Interface. A radio button is selected next to the device 'betsym' with IP 192.168.0.3. Below the table is a 'Refresh' button. The 'Add IP Filter' section includes input fields for Device Name and IP Address, and 'Add' and 'Cancel' buttons. The 'IP Filter List' section has a dropdown menu set to 'No filters entered.', an 'Enable' checkbox (checked), and a 'Delete' button. The 'Day(s) to Block' section has checkboxes for Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The 'Time of Day to Block' section has an 'All day' checkbox and 'Start' and 'End' time pickers, both set to 12:00 AM.

Port Blocking

You can use port blocking to block outbound traffic on specific ports. Outbound traffic rules control access to outside resources from local users. The default rule is to allow all access from the LAN side to the outside. You can use port blocking to add predefined or custom rules to specify exceptions to the default rule.

Note: The default rule allows any outbound traffic not blocked by rules that you create.

➤ To configure port blocking:

- In the main menu, under Advanced, select **Port Blocking**.
- From the Service list, select the service you want to block.
- To add a custom service that is not in the list of services, specify these settings in the Add Custom Service table:
 - Name.** A name for the service.
 - Start Port.** The start port for the service.
 - End Port.** The end port for the service.
 - Protocol.** The protocol for the ports:
 - **TCP.** TCP only.
 - **UDP.** UDP only.
 - **Both.** Both TCP and UDP.
 - Local IP Address.** Complete the local IP address for the computer that is using the service.
- Perform one of the following actions:
 - Click **Add** to save your settings. The Active Filters table now displays the list of ports that are currently blocked.
 - To delete a service, select the radio button in the Active Filters table for the service that you want to delete, and click **Delete**.
 - To reset the selection in the Services drop-down list and to clear all the fields in the Add Custom Service table, click **Reset**.

Port Blocking

Active Filters					
	Name	Start Port	End Port	Protocol	Local IP Address
<input type="radio"/>	FINGER	79	79	TCP	192.168.0.12
<input type="radio"/>	TELNET	23	23	TCP	192.168.0.22

Add Predefined Service

Service:

Add Custom Service

Name	Start Port	End Port	Protocol	Local IP Address
<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="Both"/>	192.168.0. <input type="text" value="0"/>

Port Forwarding

A firewall has default rules for inbound traffic (WAN to LAN) and for outbound traffic. Port forwarding affects the inbound rules. These rules restrict access from outsiders. By default,

the gateway blocks access from outside except for responses to requests from the LAN side. You can use port forwarding to add rules to specify exceptions to the default rule.

Because the gateway uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) or computer visible and available to the Internet. The rule tells the gateway to direct inbound traffic for a particular service to one local server or computer based on the destination port number. Directing traffic is also known as port forwarding.

Some residential broadband ISPs do not allow you to run server processes (such as a web or FTP server) from your location. Your ISP might check for servers and suspend your account if it finds active services at your location. See the ISP's Acceptable Use policy.

Pay attention to the following considerations before configuring port forwarding:

- If the DHCP assigns the IP address of the local server computer, the address might change when the computer is rebooted. To keep the address from changing, you can assign a static IP address to your server outside the range that DHCP assigns, but in the same subnet as your LAN. By default, the IP addresses from 192.168.0.2 through 192.168.0.9 are reserved for this purpose.
- Local computers must access the local server using the computers' local LAN address (192.168.0.XXX, by default). Attempts by local computers to access the server using the external WAN IP address fail.
- Port forwarding opens holes in your firewall. Enable only ports that are necessary.

➤ **To configure port forwarding and services for specific inbound traffic:**

1. In the main menu, under Advanced, select **Port Forwarding**.

2. From the Service list, select the service for which you want to configure port forwarding.

3. To add a custom rule that is not in the list of services, specify these settings in the Add Custom Rules table:

- **Name.** A name for the service.
- **Start Port.** The start port for the service.
- **End Port.** The end port for the service.
- **Protocol.** The protocol for the ports:
 - **TCP.** TCP only.
 - **UDP.** UDP only.
 - **Both.** Both TCP and UDP.
- **Local IP Address.** Complete the local IP address for the computer that is using the service.

4. Perform one of these actions:

- Click **Add**. The Active Forwarding Rules table displays the list of forwarded ports.

Port Forwarding

Active Forwarding Rules					
	Name	Start Port	End Port	Protocol	Local IP Address
<input type="radio"/>	FTP	20	21	TCP	192.168.0.5
<input type="radio"/>	POP3	110	110	TCP	192.168.0.8

Choose Predefined Service
Service:

Add Custom Rules

Name	Start Port	End Port	Protocol	Local IP Address
<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="Both"/>	<input type="text" value="192.168.0.0"/>

- To delete a service, select the radio button in the Active Forwarding Rules table for the service that you want to delete, and click **Delete**.
- To reset the selection in the Service list and to clear all the fields in the Add Custom Rules, click **Reset**.

Port Triggering

Port triggering is an advanced feature that you can use to allow gaming and other Internet applications that the firewall would otherwise block. You must know the port numbers the application uses. Port triggering operates as follows:

1. A computer makes an outgoing connection using a port number defined in the Port Triggering table.
2. The gateway records this connection, opens the incoming port or ports associated with this entry in the Port Triggering List, and associates them with the computer.
3. The remote system receives the computer's request, and responds using a different port number.
4. The gateway matches the response to the previous request, and forwards the response to the computer. (Without port triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the port forwarding rules.)

Note: Only one computer at a time can use port triggering. After a computer finishes using a port triggering application, there is a short time-out period before another computer can use the application.

➤ **To configure port triggering:**

1. In the main menu, under Advanced, select **Port Triggering**.

2. For each port trigger, enter the settings in the Port Triggering List:

- **Trigger Range.** To specify the range of outgoing ports that are monitored to trigger the incoming port forwarding rule, enter the start port and end port.
- **Target Range.** To specify the range of incoming ports that are opened when triggered, enter the start port and end port.
- **Protocol.** Select the protocol for the ports:
 - **TCP.** Select TCP only.
 - **UDP.** Select UDP only.
 - **Both.** Select both TCP and UDP.

3. Select the **Enable** check box for the port trigger.

4. Perform one of the following actions:

- Click **Apply** to save your settings and activate the port triggers.
- To remove a port trigger, select its radio button, and click **Delete**.
- To return all trigger and target ranges to zero, click **Reset**.

Port Triggering List						
	Trigger Range		Target Range		Protocol	Enable
	Start Port	End Port	Start Port	End Port		
<input checked="" type="radio"/>	6000	6010	8000	8010	TCP	<input checked="" type="checkbox"/>
<input checked="" type="radio"/>	9000	9010	9060	9060	UDP	<input checked="" type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>
<input type="radio"/>	0	0	0	0	Both	<input type="checkbox"/>

Apply Delete Reset

DMZ Host

You can use the DMZ Host screen to set up a default DMZ computer. Specifying a default DMZ computer allows you to set up a computer that is available to anyone on the Internet for services that you have not defined. To minimize security risks, set up the DMZ host only if you are willing to risk open access. If you do not define a DMZ host, the gateway discards any undefined service requests.

➤ **To set up a DMZ host:**

1. In the main menu, under Advanced, select **DMZ Host**.

DMZ Host

Respond to Ping on WAN Port

DMZ Address 192.168.0.0

MTU Size 0 (256-1500 octets, 0 = use default)

Apply

2. Select the **Respond to Ping on WAN Port** check box.

When you select this check box, the gateway, not the DMZ computer, responds to a ping request.

For example, some systems tracking the performance of the broadband connections in terms of latency and packet loss need the gateway to reply to ping requests.

3. Type the last digits of the IP address in the DMZ Address field.

The DMZ host feature is disabled when the last digit is zero.

4. Click **Apply**.

LAN IP Setup

The LAN IP screen allows you to configure LAN services such as the IP address of the gateway and DHCP. The TCP/IP and DHCP default values work fine in most cases.

Note: If you disable the DHCP server, assign to your computer a static IP address to reconnect to the gateway and enable the DHCP server again.

➤ To configure LAN IP settings:

1. In the main menu, under Advanced, select **LAN IP**.

2. Specify these settings:

- **LAN IP Address.** The factory default setting is 192.168.0.1.
- **Subnet Mask.** The network number portion of an IP address. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.
- **DHCP Server.** The **Yes** radio button is selected by default so the gateway acts as a DHCP server, providing the TCP/IP configuration for all the computers connected to it.

If you plan to assign IP addresses manually, or you have another DHCP server on your network, select the **No** radio button.

- **Starting IP Address** and **Ending IP Address.** These fields specify the range in the IP address pool.
- **Max Users.** The maximum number of users on the network.

LAN IP

Device Name: ---

LAN IP Address: . . .

Subnet Mask: 255.255.255.

DHCP Server: Yes No

Starting IP Address: 192.168.0.

Ending IP Address: 192.168.0.

Max Users:

Lease Time:

DHCP Reservation Lease Info

#	Mac Address	IP Address
	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	<input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/>

DHCP Client Lease Info

	MAC Address	IP Address	Expires
<input type="radio"/>	001641156fb1	192.168.000.002	--- --:--:--

Current System Time: --- --:--:--

- **DHCP Lease.** For more information, see the following section, [Reserve an IP Address for DHCP Use](#).
3. Click **Apply**.

Reserve an IP Address for DHCP Use

To reserve an IP address for DHCP use, enter the DHCP server reservation settings for the private LAN under DHCP Reservation Lease Info in the LAN IP screen.

➤ **To reserve an IP address for DHCP:**

1. In the main menu, under Advanced, select **LAN IP**.
2. In the DHCP Reservation Lease Info section, enter the MAC address of the computer for which you want to reserve an IP address.
3. Enter the permanent IP address for the computer.
4. Click **Add** to save your settings.

The MAC address and IP address are displayed in the DHCP Client Lease Info table. The current system time is also displayed.

➤ **To delete an IP address from the DHCP Client Lease Info table:**

1. In the DHCP Client Lease Info table, select the radio button for the MAC and IP address that you want to remove.
2. Click **Delete**.

The information for the selected MAC and IP address is removed from the DHCP Client Lease Info table.

To remove all information from the DHCP Client Lease Info table, click **Clear DHCP Leases**.

LAN Switch

The gateway's LAN interface is a 10/100/1GBASE-T Ethernet switch. The switch ports are set to automatically negotiate speed and duplex communication with any connected device. You might want to configure the port if the devices do not auto-negotiate correctly.

➤ **To configure the switch ports:**

1. In the main menu, under Advanced, select **LAN Switch**.

Switch Port Control

Port	Auto	Speed			Duplex		Active
		10	100	1000	half	full	
1	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

2. For each port, select the appropriate speed and duplex setting.
3. Click **Apply**.

➤ **To disable a LAN port:**

1. In the main menu, under Advanced, select **LAN Switch**.
2. In the Auto column corresponding to the port you want to disable, clear the check box.
3. Click **Apply**.

Configure Universal Plug and Play (UPnP)

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. With UPnP, you can specify the following:

- **Advertisement period.** Specifies how often the gateway broadcasts its UPnP information. The default is 30 minutes. Lower numbers ensure that control points have current device status at the expense of more network traffic. Larger numbers compromise the freshness of the device status but can significantly reduce network traffic.
- **Advertisement time to live.** The time to live for the advertisement, measured in hops (steps) for each UPnP packet that is sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is four hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value slightly.

➤ **To configure UPnP:**

1. In the main menu, under Advanced, select **UPnP**.
2. Select the **Turn UPnP On** check box.

By default, this check box is cleared. This prevents the gateway from allowing any devices to automatically control the resources, such as port forwarding, of the gateway.

3. Complete the Advertisement Period and Advertisement Time to Live fields.

The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the gateway and which internal and external ports of the gateway that device opened. The UPnP Portmap Table also displays the protocol for the port that was opened and if that port is still active for each IP address.

4. Perform one of the following actions:
 - Click **Apply** to save your settings.
 - Click **Cancel** to disregard any unsaved changes.
 - Click **Refresh** to update the UPnP Portmap Table and to show the active ports that are currently opened by UPnP devices.

Set Networking Protocols

Network Time Protocol (NTP) is a networking protocol that synchronizes clocks between computer systems over packet-switched, variable-latency data networks.

➤ To enable NTP:

1. In the main menu, under Advanced, select **NTP**.

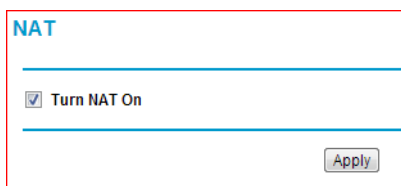
2. Select the **NTP enable** check box.
3. Enter the IP server addresses.
 - a. Enter the first server IP address in the Server IP Address 1 field.
 - b. Enter the second server IP address in the Server IP Address 2 field.
 - c. Enter the third server IP address in the Server IP Address 3 field.
4. Click **Apply**.

Enable Network Address Translation

Network Address Translation (NAT) provides one-to-many translation of IP addresses between devices. This means that your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. Enable NAT to allow multiple computers on your network to access the Internet using a single public IP address. NAT is enabled by default.

➤ **To disable NAT:**

1. In the main menu, under Advanced, select **NAT**.

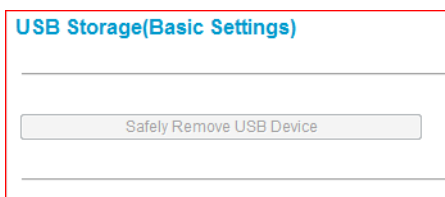


2. Deselect the **Turn NAT On** box.
3. Click **Apply**.

Remove USB Devices

➤ **To remove a USB device:**

1. In the main menu, under USB Storage, select **Basic Settings**.



2. Click **Safely Remove USB Device**.

6 Troubleshooting

6

This chapter gives information about troubleshooting your NETGEAR DOCSIS 3.0 N450 Wi-Fi Data Gateway. For the common problems listed, see the section indicated.

- Have I connected the gateway correctly?
See *Basic Functions* on page 49.
- I cannot access the gateway configuration with my browser.
See *Connect to the Gateway's Main Menu* on page 49.
- I have configured the gateway but I cannot access the Internet.
See *Troubleshoot the ISP Connection* on page 50.
- My gateway is not responding.
- See *Troubleshoot a TCP/IP Network Using a Ping Utility* on page 50

If you cannot remember the gateway's configuration password or you want to clear the configuration and start over again, see *Factory Default Settings* on page 54.

Tip: NETGEAR provides helpful articles, documentation, and the latest software updates at <http://www.netgear.com/support>.

Basic Functions

After you have turned on power to the gateway, do the following:

1. Check to see that the Power LED is lit.
2. Check that the numbered Ethernet LEDs light momentarily.
3. After a few seconds, check that the LEDs are lit for any local ports that are connected.

The following table provides help when you are using the LEDs for troubleshooting.

Table 1. LED behavior

LED Behavior	Action
All LEDs are off when the gateway is plugged in.	<ul style="list-style-type: none"> • Make sure that the power cord is properly connected to your gateway and that the power supply adapter is properly connected to a functioning power outlet. • Check that you are using the 12V-DC power adapter supplied by NETGEAR for this product. <p>If the error persists, you have a hardware problem and should contact technical support.</p>
All LEDs stay on.	<p>Clear the gateway's configuration to factory defaults. This sets the gateway's IP address to 192.168.0.1. See Factory Default Settings on page 54.</p> <p>If the error persists, you might have a hardware problem and should contact technical support.</p>
LAN LED is off for a port with an Ethernet connection.	<ul style="list-style-type: none"> • Make sure that the Ethernet cable connections are secure at the gateway and at the hub or computer. • Make sure that power is turned on to the connected hub or computer. • Be sure that you are using the correct cable.
Internet LED is off and the gateway is connected to the cable television cable.	<ul style="list-style-type: none"> • Make sure that the coaxial cable connections are secure at the gateway and at the wall jack. • Make sure that your cable service provider provisioned your cable Internet service. Your provider should verify that the signal quality is good enough for cable modem service. • Remove any excessive splitters you might have on your cable line. It might be necessary to run a "home run" back to the point where the cable enters your home.

Connect to the Gateway's Main Menu

If you are unable to access the gateway's main menu from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the gateway as described in the previous section.

- Make sure that your computer's IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.10 to 192.168.0.254.

Note: If your computer's IP address is shown as 169.254.x.x:
Recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the gateway and reboot your computer.

- If your gateway's IP address has been changed and you do not know the current IP address, clear the gateway's configuration to factory defaults. This sets the gateway's IP address to 192.168.0.1. For more information, see [Factory Default Settings](#) on page 54.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to make sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The gateway user name is **admin**, and the default password is **password**, both in lower case letters. (Caps Lock should be off when you enter these.)

If the gateway does not save changes you have made, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

Troubleshoot the ISP Connection

If your gateway is unable to access the Internet and your Internet LED is on, you might need to register the cable MAC address or device MAC address of your gateway with your cable service provider.

Additionally, your computer might not have the gateway configured as its TCP/IP gateway. If your computer obtains its information from the gateway by DHCP, reboot the computer and verify the gateway address. For more information, see [Reserve an IP Address for DHCP Use](#) on page 44.

Troubleshoot a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can

easily troubleshoot a TCP/IP network by using the ping utility in your computer or workstation.

Test the LAN Path to Your Gateway

You can use ping to verify that the LAN path to your gateway is set up correctly.

➤ To ping the gateway from a computer running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the gateway, as in this example:

ping 192.168.0.1

3. Click **OK**.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not working correctly, you could have one of the following problems:

- Wrong physical connections.
 - Make sure that the LAN port LED is lit. If the LED is off, see *Basic Functions* on page 49.
 - Check that the corresponding LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- Wrong network configuration.
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
 - Verify that the IP address for your gateway and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows Run dialog box, type:

ping -n 10 <IP address>

where *<IP address>* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your gateway listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your Internet LED is on.

A Supplemental Information



This appendix includes the following sections:

- *Factory Default Settings*
- *Technical Specifications*

Factory Default Settings


You can return the gateway to its factory settings. On the rear panel of the gateway, press and hold the **Reset** button  for over 7 seconds. The gateway resets and returns to the factory configuration settings shown in the following table.

Table 2. Factory default settings

Feature	Parameter	Default
Gateway login	User login URL	http://192.168.0.1
	User name and password (case-sensitive)	admin/password
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP Ending IP address	192.168.0.254
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communication to the Internet	Enabled (all)
	Source MAC filtering	Disabled
Internet connection	WAN MAC address	Use default hardware address.
	WAN MTU size	1500

Feature	Parameter	Default
Wireless	Wireless communication	Enabled
	SSID name	Appears on the label of the gateway.
	Security	WPA/WPA2 The default WPA/WPA2 password appears on the label of the gateway.
	Broadcast SSID	Enabled
	Transmission speed	Auto ¹
	Country/region	United States (varies by region)
	RF channel	Auto
	Operating mode	n, g, and b
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless Card Access List	All wireless stations allowed

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

Technical Specifications

The following table describes the technical specifications for the gateway.

Table 3. Technical specifications

Component	Specification
Network protocol and standards compatibility	Data and routing protocols: TCP/IP, DHCP server, and client, DNS relay, NAT (many-to-one), TFTP client, VPN pass-through (IPSec, PPTP)
Power adapter	<ul style="list-style-type: none"> North America (input): 120V, 60 Hz, input All regions (output): 12 V-DC @ 2.5A output 30W maximum
Physical specifications	<ul style="list-style-type: none"> Dimensions: 10.2 by 6.49 by 3.65 in. (259.17 by 164.77 by 92.72 mm) Weight: 1.30 lb (590 g)
Environmental	<ul style="list-style-type: none"> Operating temperature: 32° to 140°-F (0° to 40°-C) Operating humidity: 90% maximum relative humidity, non-condensing Electromagnetic emissions: Meets requirements of: FCC Part 15 Class B.

NETGEAR DOCSIS 3.0 N450 Wi-Fi Data Gateway

Component	Specification
Interface	Local: 10BASE-T, 100/1000BASE-Tx, RJ-45 USB 2.0/1.1 function 802.11n/g/b
	Internet: DOCSIS 3.0. Downward compatible with DOCSIS 2.0, 1.1, and 1.0

B Notification of Compliance

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the **CE** marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the NETGEAR DOCSIS 3.0 N450 Wi-Fi Data Gateway complies with Part 15 Subpart B of FCC CFR47 Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

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 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. 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 methods:

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- 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.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR DOCSIS 3.0 N450 Wi-Fi Data Gateway) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada 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.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The following table shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby monitor - Analog	20 feet / 6 meters
Baby monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters