

NETGEAR®

Wireless Cable Gateway CG3300CMR User Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

September 2012
202-11068-02
v1.0

© 2012 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at <http://support.netgear.com>.

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

Phone (Other Countries): See Support information card.

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. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2012 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Contents

Chapter 1 Connect to the Gateway

Gateway Front Panel	7
Gateway Rear Panel	9
Power Supply Manufacturers and Models	10
Gateway Label	10
Log In To Your Gateway	11
View the Gateway Home Screens	12
Basic Home Screen	12
Advanced Home Screen	13
Add Wireless Devices or Computers to Your Network	14

Chapter 2 genie Basic Settings

Wireless	16
Placement of the Router to Optimize Wireless Connectivity	16
Wireless Screen	16
Wireless Screen Fields	18
Attached Devices	19
Guest Networks	20
Guest Network Wireless Security Options	21

Chapter 3 genie Advanced Home

Setup Menu	23
Internet Setup	24
Internet Setup Screen Fields	24
WAN Setup	26
Default DMZ Server	27
Change the MTU Size	27
LAN Setup	28
LAN Setup Screen Settings	30
Use the Gateway as a DHCP Server	30
Address Reservation	31

Chapter 4 Security

Keyword Blocking of HTTP Traffic	34
Block Services (Port Filtering)	35
Security Event Email Notifications	38

Chapter 5 Administration

View Gateway Status	41
Router Information	42
Cable Network Information	43
Wireless Settings	45
Guest Network	46
View Logs of Web Access or Attempted Web Access	47
View Event Logs	48
Manage the Configuration File	49
Back Up Settings	49
Restore Configuration Settings	49
Erase	50
Set Password	51

Chapter 6 Advanced Settings

Advanced Wireless Settings	53
Advanced Wireless Settings	53
Wireless Card Access List	55
Nearby Wireless Access Points	57
Services	58
Port Forwarding and Port Triggering	59
Remote Computer Access Basics	59
Port Triggering to Open Incoming Ports	60
Port Forwarding to Permit External Host Communications	61
How Port Forwarding Differs from Port Triggering	63
Set Up Port Forwarding to Local Servers	63
Add a Custom Service	64
Edit or Delete a Port Forwarding Entry	65
Set Up Port Triggering	66
Dynamic DNS	68
Cable Status	70
Universal Plug and Play	70
IPv6	72
NAT	73

Chapter 7 Troubleshooting

Basic Functions	74
Using LEDs to Troubleshoot	75
Connect to the Main Menu of the Gateway	75
Troubleshoot the ISP Connection	76
Troubleshoot a TCP/IP Network Using a Ping Utility	76
Test the LAN Path to Your Gateway	76
Test the Path from Your Computer to a Remote Device	77
Wireless Performance and Gateway Location	78

Appendix A Supplemental Information

Factory Default Settings79

Technical Specifications80

Appendix B Notification of Compliance

Index

Connect to the Gateway

1

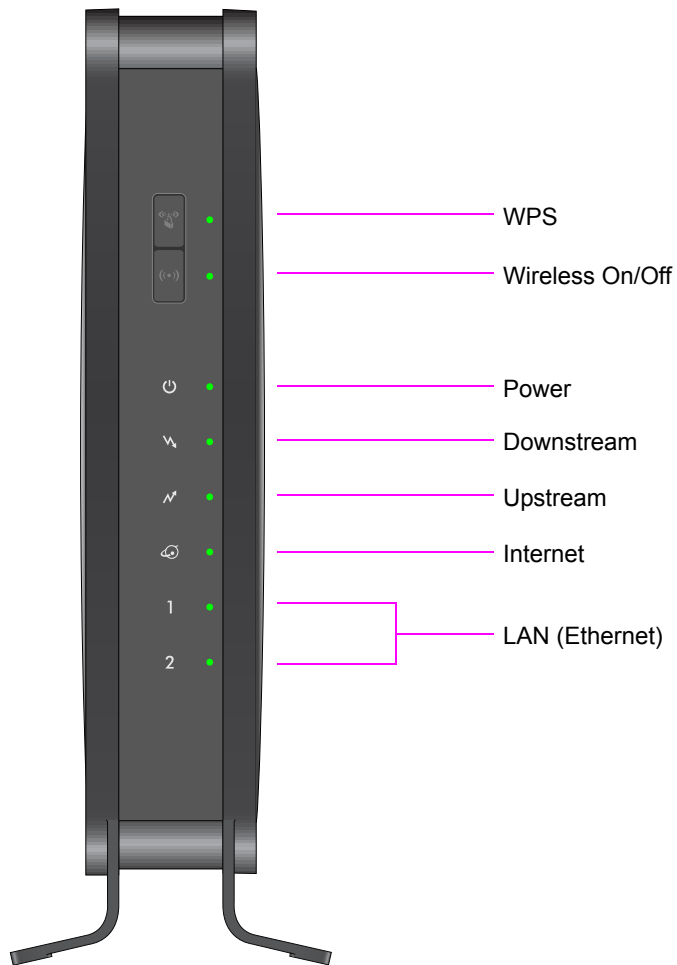
Getting to know your gateway

This chapter describes how to configure the Internet connection of your gateway and includes these sections:

- *Gateway Front Panel*
- *Gateway Rear Panel*
- *Gateway Label*
- *Log In To Your Gateway*
- *View the Gateway Home Screens*
- *Add Wireless Devices or Computers to Your Network*

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








Gateway Front Panel



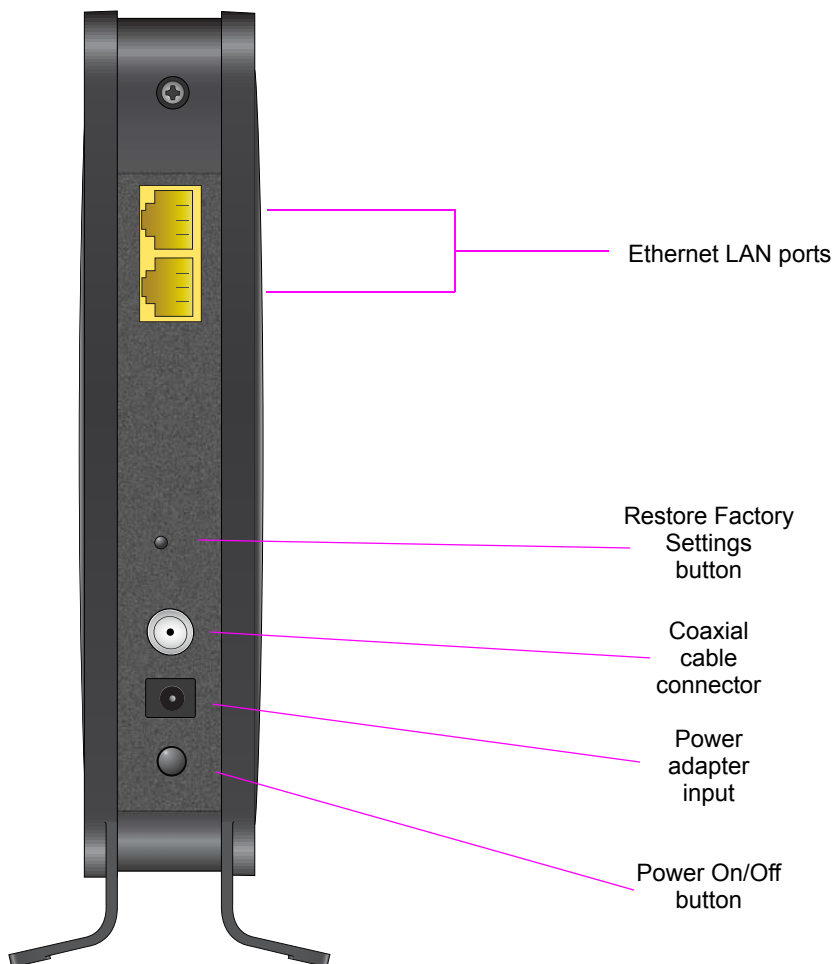
Note: For optimal performance, place the gateway vertically in the stand.
Do not mount this unit to a wall; it is not suitable for wall mounting.

Wireless Cable Gateway CG3300CMR

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	<ul style="list-style-type: none"> Green. Power is supplied to the cable modem. Blinking. Power-on self-test. Off. No power.
 Downstream	<ul style="list-style-type: none"> Green. More than one channel is locked (channel bonding). Amber. One channel is locked (no channel bonding). Blinking. The unit is scanning for a downstream channel. Off. No downstream channel is locked.
 Upstream	<ul style="list-style-type: none"> Green. More than one channel is locked (channel bonding). Amber. One channel is locked (no channel bonding). Blinking. The unit is scanning for an upstream channel. Off. No upstream channel is locked.
 Internet	<ul style="list-style-type: none"> Solid green. The cable modem is online. Blinking. The cable modem is synchronizing with the CMTS of the cable provider. 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.
Button	Description
 WPS	<p>Pressing this button opens a 2-minute window for the gateway to connect with other WPS-enabled devices.</p> <p>Note: WPS has been disabled.</p>
 Wireless On/Off	<p>Turn the wireless radio in the gateway on and off. The wireless radio is on by default. The LED located below this button indicates if the wireless radio is on or off.</p> <p>Note: Wireless On/Off button has been disabled.</p>

Gateway Rear Panel



The rear panel includes the following connections when viewed from top to bottom:

- **Two Gigabit Ethernet LAN ports.** Use these ports to connect local computers.
- **Restore Factory Settings button.** You can return the gateway to its factory settings. Press and hold the **Restore Factory Settings** button for over 7 seconds. The gateway resets and returns to its factory settings. See [Factory Default Settings](#) on page 79.
- **Coaxial cable connector.** Attach a coaxial cable to the cable service provider connection.
- **Power adapter input.** Connect the power adapter unit here.
- **Power On/Off button.** Press to turn on power. Press again to turn off power.

Power Supply Manufacturers and Models

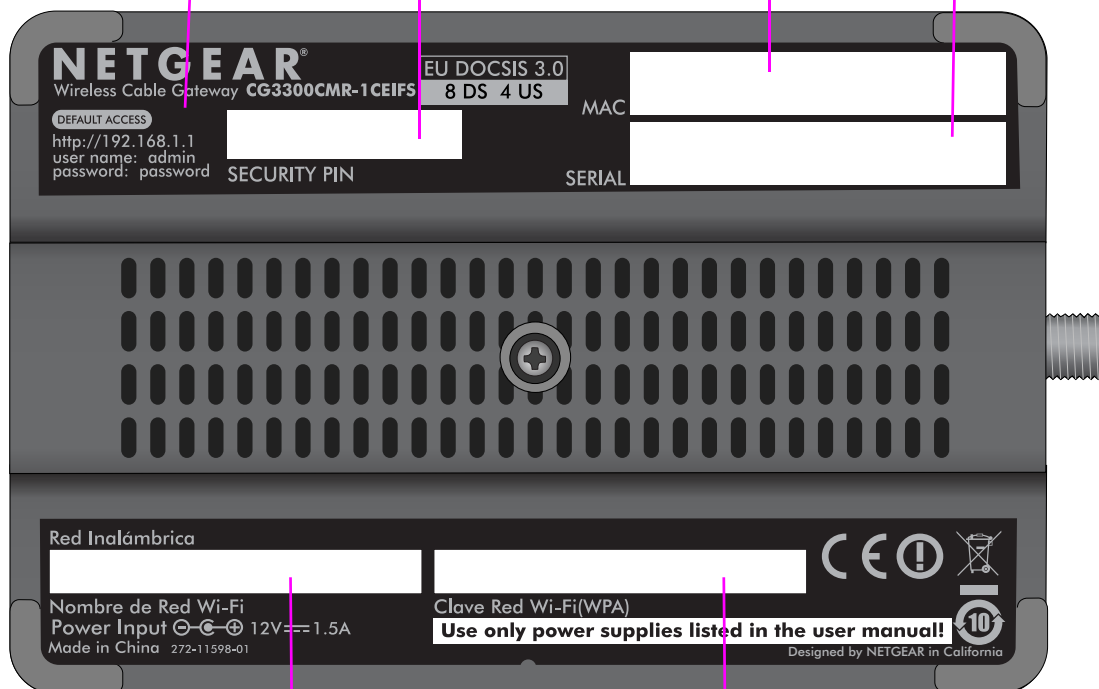
Note: Use only power supplies listed in the *User Manual*.

- Adaptor of CWT
Manufacturer: Channel Well Technology Co Ltd
Model: SAL018F2
- Adaptor of PI
Manufacturer: PI Electronics (H.K.) Ltd.
Model: AD817000

Gateway Label

The label on the bottom of the gateway shows the WPS PIN, login information, MAC address, and serial number.

Default access information Security PIN MAC address Serial number



Preset SSID

Preset WiFi password

Log In To Your Gateway

You can log in to the gateway to view or change its settings.


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

The gateway automatically logs you out after 5 minutes of no activity.

➤ **To log in to the gateway:**

1. On the computer that is connected to the gateway with an Ethernet cable, type **http://192.168.1.1** in the address field of your Internet browser.

A login window opens.

A screenshot of the Netgear login window. The window has a title bar and a light beige background. At the top left, the word "Netgear" is displayed. Below it, there are two labels: "User name:" and "Password:". The "User name:" field is a dropdown menu with "admin" selected. The "Password:" field is a text box with ten dots representing a masked password. Below the password field is a checkbox labeled "Remember my password" which is checked. At the bottom of the window are two buttons: "OK" and "Cancel".

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

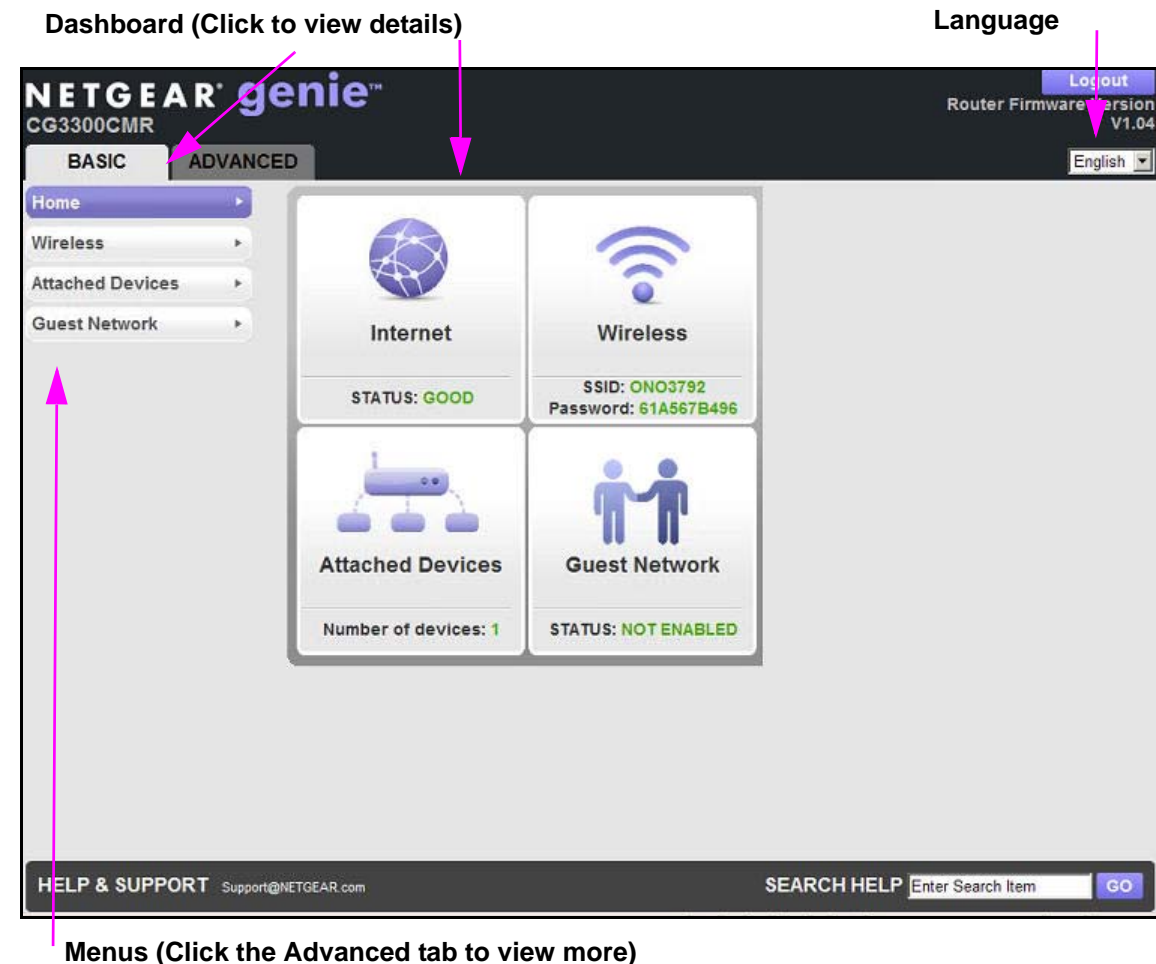
The gateway Basic Home screen displays when you log in (see [Basic Home Screen](#) on page 12).

View the Gateway Home Screens

The gateway home screens include a Basic Home screen and an Advanced Home screen.

Basic Home Screen

When you connect to the gateway, the gateway dashboard (Basic Home screen) displays.



The gateway Basic Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is an Advanced tab that is used to access additional menus and screens.

- **Home.** This dashboard screen displays when you log in to the gateway or select the Home tab.
- **Wireless.** View or change the wireless settings for your gateway.
- **Attached Devices.** View the devices that are connected to your network.

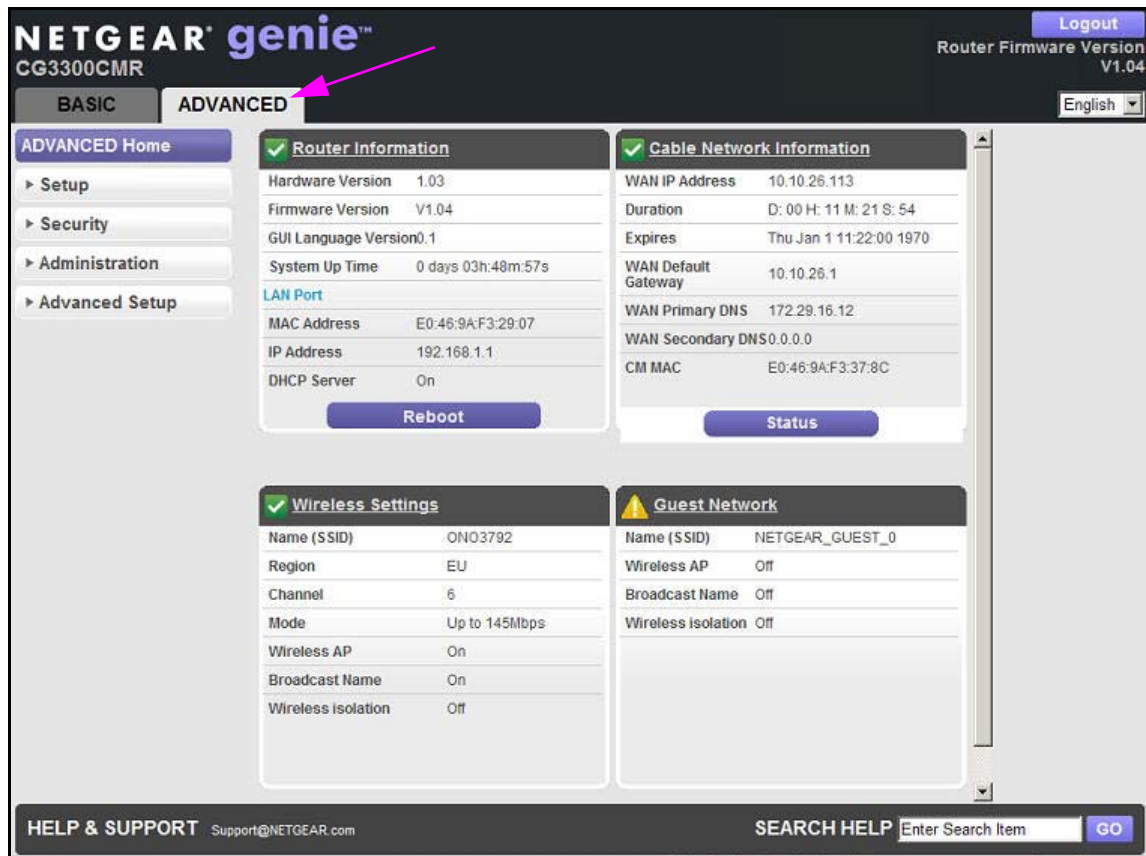
- **Guest Network.** Set up a guest network to allow visitors to use the Internet connection of your gateway.
- **Advanced tab.** Set the gateway up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See [Advanced Home Screen](#) on page 13. Using this tab requires a solid understanding of networking concepts.

For more information about the Basic settings, see [Chapter 2, genie Basic Settings](#).

Advanced Home Screen

Note: Using the Advanced Home screen requires a solid understanding of networking concepts.

To view the Advance Home screen, select the **Advanced** tab from the top menu.



The gateway Advanced Home screen has a dashboard that lets you see the configuration of your gateway and network at a glance. You can click any of the sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is a Basic tab that is used to the basic menus and screens.

- **Advanced Home.** This dashboard screen displays when you select the Advanced tab.

- **Setup.** Set up the Internet connection, wireless, guest network, WAN, and LAN.
- **Security.** Block sites, block services, and set up email notifications.
- **Administration.** View router status, logs, and event logs, back up and restore the configuration file, and change the gateway password.
- **Advanced Setup.** Configure advanced network features such as port forwarding, port triggering, Dynamic DNS, UPnP, and IPv6.
- **Home tab.** Return to the Basic Home screen. See [Basic Home Screen](#) on page 12.

For more information about the Advanced settings, see [Chapter 3, genie Advanced Home](#).

Add Wireless Devices or Computers to Your Network

See [Guest Networks](#) on page 20 for instructions on how to set up a guest network.

➤ To add wireless devices or computers to your network:

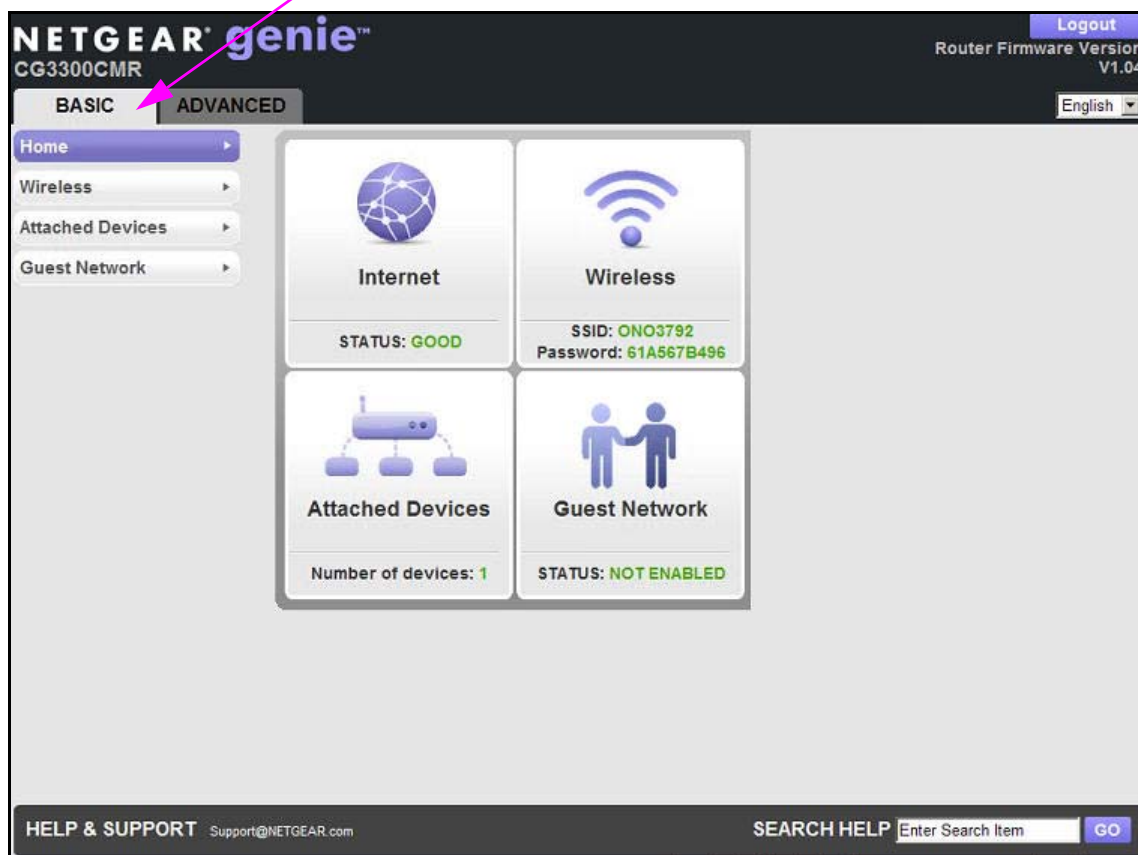
1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your gateway. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default WiFi network name (SSID) and select it. The default SSID is on the product label on the bottom of the gateway.
3. Enter the gateway password and click **Connect**. The default gateway passphrase is on the product label on the bottom of the gateway.
4. Repeat steps 1–3 to add other wireless devices.

genie Basic Settings

2

Your Internet connection and network

This chapter explains the features available from the genie Basic Home screen that is shown in the following figure:



This chapter contains the following sections:

- [Wireless](#)
- [Attached Devices](#)
- [Guest Networks](#)

Wireless

Note: To ensure proper agency compliance and compatibility between similar products in your area, set the operating channel and region correctly.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary based on the physical placement of the router. For best results, place your router:

- Near the center of the area in which your computers operate.
- In an elevated location such as a high shelf.
- Away from potential sources of interference, such as computers, microwave ovens, and cordless phones.
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to connect wirelessly to the gateway.

Wireless Screen

The Wireless screen lets you view or configure the wireless network setup.

The wireless cable gateway comes with preset security. This feature 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 bottom of the unit.

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

NETGEAR recommends that you do not change your preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place.

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

➤ To view or change basic wireless settings:

1. On the Basic Home screen, select **Wireless** to display the Wireless screen.

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

BASIC **ADVANCED**

Home
Wireless
Attached Devices
Guest Network

Wireless

Cancel Apply

Wireless Network

☒ Enable SSID Broadcast
☐ Enable Wireless Isolation

Name (SSID): ONO3792
Region: Europe
Channel: AUTO
Mode: Up to 145Mbps

Security Options

☐ Disabled
☐ WPA2-PSK [AES]
☒ WPA-PSK [TKIP] + WPA2-PSK [AES]
☐ WPA/WPA2 Enterprise

Security Options (WPA-PSK + WPA2-PSK)

Passphrase : 61A567B496 (8-63 characters or 64 hex digits)

Help Center

HELP & SUPPORT Support@NETGEAR.com

SEARCH HELP Enter Search Item GO

The screen sections, settings, and procedures are explained in the following sections.

2. Change what you need to, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
 - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
 - Does your wireless device or computer show up on the Attached Devices screen? If it does, then it is connected to the network.
 - If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your gateway.

Wireless Screen Fields

Wireless Network

- **Enable SSID Broadcast.** This setting allows the gateway to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box, and click **Apply**.
- **Enable Wireless Isolation.** If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet. They cannot access each other or access Ethernet devices on the network, however.
- **Name (SSID).** The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and **NETGEAR strongly recommends that you do not change the SSID**.
- **Region.** The location where the gateway is used.
- **Channel.** This setting is the wireless channel that the gateway uses. Choose a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (such as lost connections or slow data transfers). If any interference happens, experiment with different channels to see which is the best.
- **Mode.** Up to 145 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 300 Mbps setting allows 802.11n devices to connect at this speed.

Security Options Settings

The Security Options section of the Wireless screen lets you change the security option and passphrase. **NETGEAR recommends that you do not change the security option or passphrase**, but if you want to change these settings, this section explains how.



CAUTION:

Do not disable security.

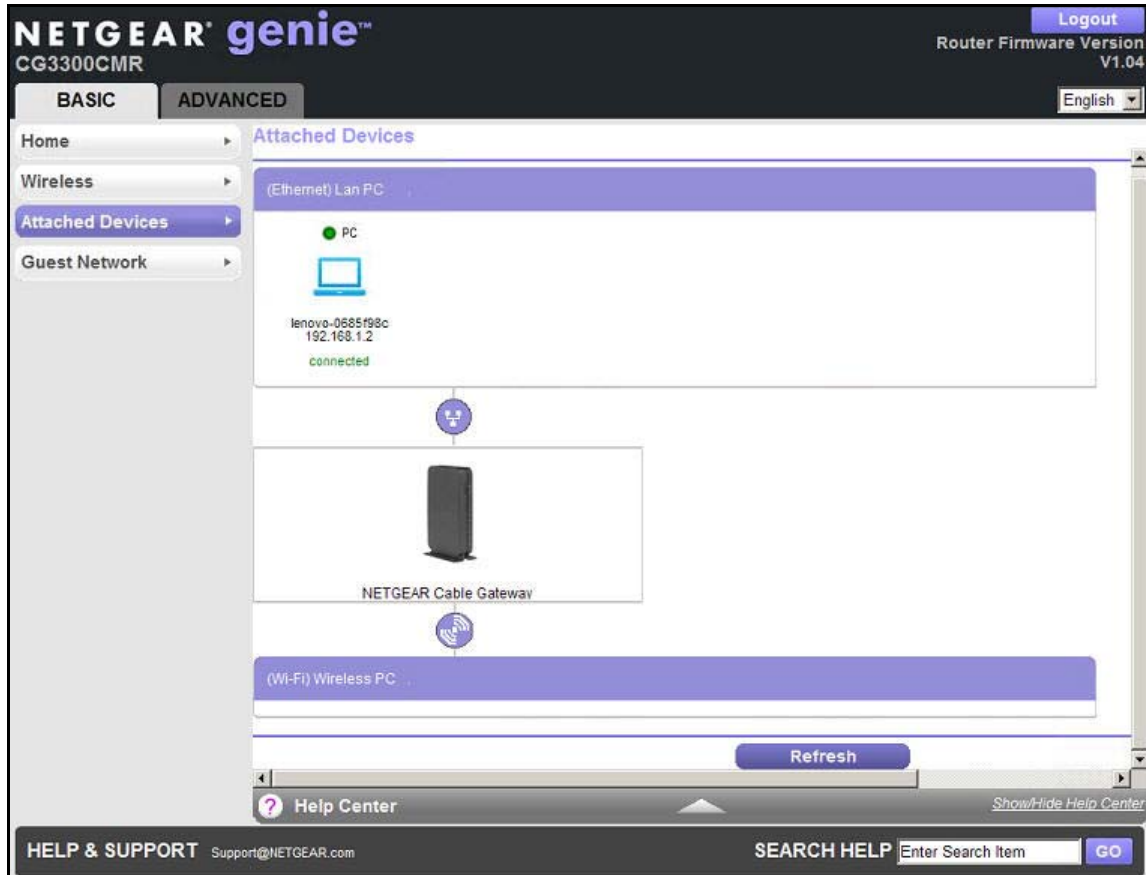
➤ To change the WPA security option and passphrase:

1. Under Security Options, select the WPA option that you want.

2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Attached Devices

You can view all computers or devices that are currently connected to your network here. From the Basic Home screen, select **Attached Devices** to display the following screen:



Wired devices are connected to the gateway with Ethernet cables. Wireless devices have joined the wireless network.

- **IP Address.** The IP address that the gateway assigned to this device when it joined the network. This number can change when a device disconnects and then rejoins the network.
- **Device Name.** If the device name is known, it is shown here.

You can click **Refresh** to update this screen.

Guest Networks

You can add a guest network to allow visitors at your home to use the Internet without providing them with your wireless security key.

➤ **To set up a guest network:**

1. Select **Basic > Guest Network** to display the following screen:

The screenshot displays the NETGEAR genie CG3300CMR web interface. The 'BASIC' tab is selected, and the 'Guest Network' page is shown. The 'Wireless Network' section contains three checkboxes: 'Enable Guest Network', 'Enable SSID Broadcast', and 'Enable Wireless Isolation'. The 'Guest Wireless Network Name (SSID)' is set to 'NETGEAR_GUEST_0' and the 'Select Guest Network Group' is set to '0'. The 'Security Options' section has four radio buttons: 'Disabled' (selected), 'WPA2-PSK [AES]', 'WPA-PSK [TKIP] + WPA2-PSK [AES]', and 'WPAWPA2 Enterprise'. The page also features a 'Logout' button, 'Router Firmware Version V1.04', and a 'Help Center' link.

2. 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.

- **Enable Wireless Isolation.** If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet. They cannot access each other or access Ethernet devices on the network, however.
3. 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 nonguest SSID.

4. Select the guest network group from the list.
5. Select a security option from the list. The security options are described in [Guest Network Wireless Security Options](#) on page 21.
6. Click **Apply** to save your selections.

Guest Network Wireless Security Options

A security option is the type of security protocol that is applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.

This section presents an overview of the security options and provides guidance on when to use which option. It is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend not using wireless security.

Wi-Fi Protected Access (WPA) encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product complies with the worldwide single standard for high-speed wireless local area networking that the Wi-Fi Alliance (<http://www.wi-fi.org/>) established.

WPA-PSK uses a passphrase to perform authentication and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption and implements most of the IEEE 802.11i standard. It is designed to work with all wireless network interface cards. Not all wireless access points work with this standard. WPA2-PSK supersedes WPA-PSK.

WPA2-PSK is stronger than WPA. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is implemented through hardware, while WPA-PSK is implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

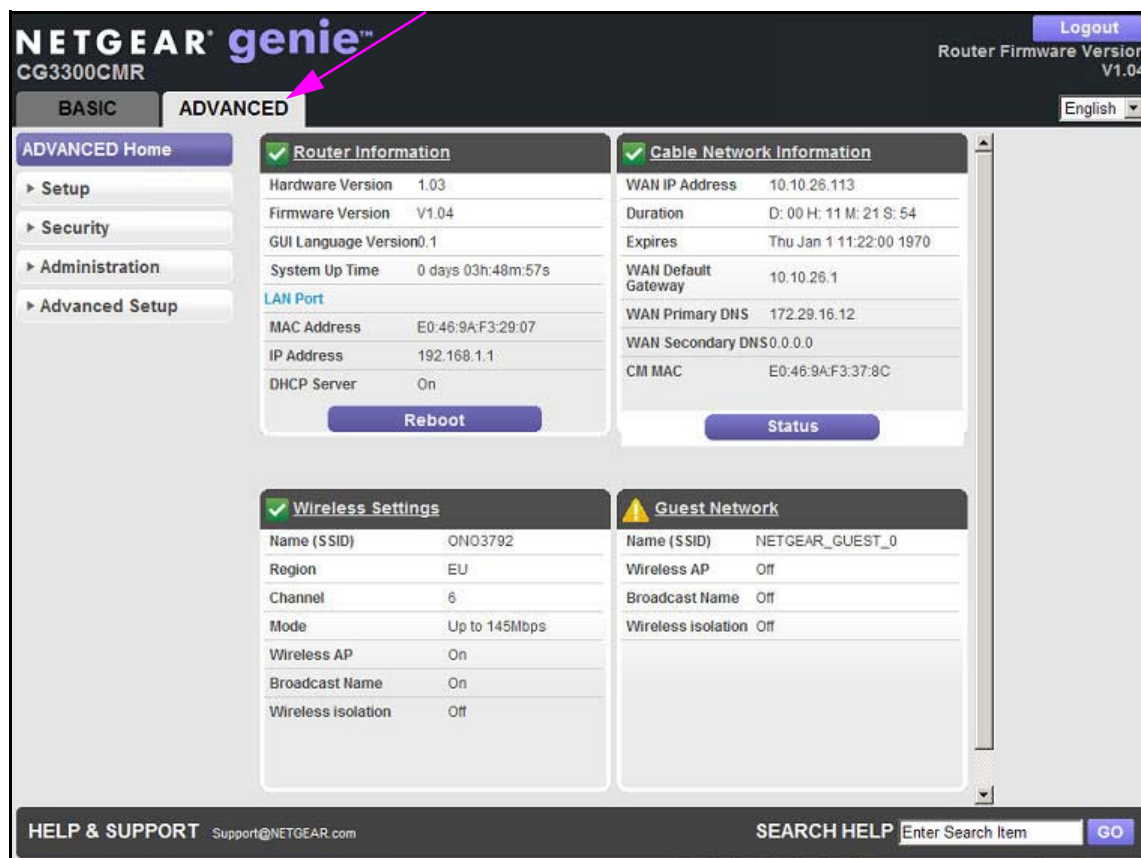
WPA-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software has instructions about configuring their WPA settings.

genie Advanced Home

3

Specifying custom settings

This chapter explains the features available from the genie Advanced Home screen that is shown in the following figure:



This chapter contains the following sections:

- [Setup Menu](#)
- [WAN Setup](#)
- [LAN Setup](#)

Some selections on the Advanced Home screen are described in separate chapters:

- **Security.** See [Chapter 4, Security](#).

- **Administration.** See [Chapter 5, Administration](#).
- **Advanced Setup.** See [Chapter 6, Advanced Settings](#).

Setup Menu

Select **Advanced > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup.** See [Internet Setup](#) on page 24.
- **Wireless Setup.** This menu item is a shortcut to the same Wireless screen that you can access from the dashboard on the Basic Home screen. See [Wireless](#) on page 16.
- **Guest Network.** This menu item is a shortcut to the same Guest Network screen that you can access from the dashboard on the Basic Home screen. See [Guest Networks](#) on page 20.
- **WAN Setup.** Internet wide area network (WAN) setup. See [WAN Setup](#) on page 26.
- **LAN Setup.** Local area network (LAN) setup. See [LAN Setup](#) on page 28.

Internet Setup

The Internet Setup screen is where you view or change ISP information.

➤ **To change the Internet settings:**

1. From the Advanced Home screen, select **Setup > Internet**. The following screen displays:

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
3. Click **Apply** to save your settings.

Internet Setup Screen Fields

The following descriptions explain all of the possible fields in the Internet Setup screen.

Internet IP Address.

- If you log in to your service or your ISP did not provide you with a fixed IP address, the router finds an IP address for you automatically when you connect. Select **Get Dynamically from ISP**.

- If you have a fixed (or static) IP address, your ISP has provided you with the required information. Select **Use Static IP Address** and type the IP address, IP subnet mask, and gateway IP address in the correct fields.

For example:

- IP Address. 24.218.156.183
- Subnet Mask. 255.255.255.0
- Gateway IP Address. 24.218.156.1

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses that are based on their names.

- If your ISP gave you one or two DNS addresses, select **Use These DNS Servers** and type the primary and secondary addresses.
- Otherwise, select **Get Automatically from ISP**.

Note: If you get address not found errors when you go to a website, it is likely that your DNS servers are not set up correctly. Contact your ISP to get the DNS server addresses.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the gateway to respond to a ping on the WAN (Internet) port.

➤ **To change the WAN settings:**

Select **Advanced > Setup > WAN Setup** to view the following screen:

- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See [Default DMZ Server](#) on page 27 for more details.
- **Respond to Ping on Internet Port.** If you want the gateway to respond to a ping from the Internet, select this check box. Use this feature only as a diagnostic tool because it also allows your gateway to be discovered. Do not select this check box unless you have a specific reason.
- **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, reduce the MTU. Reducing the MTU size is rarely required, and you should not do this unless you are sure that it is necessary for your ISP connection. See [Change the MTU Size](#) on page 27.

Default DMZ Server

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



WARNING:

DMZ servers pose a security risk. A computer that is 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 discards incoming traffic from the Internet unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➤ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

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

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

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications often require an MTU change:
 - A secure website that does not open, or displays only part of a web page
 - Yahoo email
 - MSN portal
 - America Online DSL service

- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting causes Internet communication problems. These problems include the inability to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

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

Table 1. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This size is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR gateways, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for ping. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial up ISPs.

➤ **To change the MTU size:**

1. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size from 64 through 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup 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.

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

- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires you to use a different IP addressing scheme, make those required changes in the LAN Setup screen.

➤ **To change the LAN settings:**

Note: If you change the LAN IP address of the gateway while connected through the browser, you are disconnected. Open a new connection to the new IP address and log in again.

1. Select **Advanced > Setup > LAN Setup** to display the following screen:

NETGEAR genie™
CG3300CMR Router Firmware Version V1.04

BASIC **ADVANCED** Logout English

ADVANCED Home **LAN Setup** Cancel Apply

Setup

- Internet Setup
- Wireless Setup
- Guest Network
- WAN Setup
- LAN Setup

Security

Administration

Advanced Setup

LAN TCP/IP Setup

Device Name: CG3300CMR

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

☒ Use Router as DHCP Server

Starting IP Address: 192.168.1.2

Ending IP Address: 192.168.1.254

Lease time: 1440 minutes

Address Reservation

#	IP Address	Device Name	MAC Address

+ Add Edit × Delete

? Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com **SEARCH HELP** Enter Search Item GO

2. Enter the settings that you want to customize. These settings are described in the following section, [LAN Setup Screen Settings](#).
3. Click **Apply** to save your changes.

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address.** The LAN IP address of the gateway.
- **IP Subnet Mask.** The LAN subnet mask of the gateway. When combined with the IP address, the IP subnet mask allows a device to know the following:
 - Which other addresses are local to it
 - Which other addresses have to be reached through a gateway

Use Router as a DHCP Server

This check box is selected so that the gateway functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address.** Specify the start of the range for the pool of IP addresses in the same subnet as the gateway.
- **Ending IP Address.** Specify the end of the range for the pool of IP addresses in the same subnet as the gateway.

Address Reservation

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

Use the Gateway as a DHCP Server

By default, the gateway functions as a DHCP server. This capability allows the gateway to assign IP, DNS server, and default gateway addresses to all computers connected to the LAN that is connected to the gateway. The assigned default gateway address is the LAN address of the gateway. The gateway assigns IP addresses to the attached computers from a pool of addresses that are specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the gateway are satisfactory.

You can specify the pool of IP addresses that can be assigned by setting the starting IP address and ending IP address. These addresses are part of the same IP address subnet as the LAN that is connected to the gateway. Using the default addressing scheme, you define a range between 192.168.1.2 and 192.168.1.254. You can save part of the range for devices with fixed addresses.

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

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address (the LAN IP address of the gateway)

- Primary DNS server (if you entered a primary DNS address in the Internet Setup screen; otherwise, the LAN IP address of the gateway)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Setup screen)

To use another device on your network as the DHCP server or to configure manually the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, set the IP addresses of your computer manually or other devices cannot access the gateway.

Address Reservation

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 DHCP server of the gateway. Assign reserved IP addresses to computers or servers that require permanent IP settings.

➤ To reserve an IP address:

1. In the Address Reservation section of the LAN Setup screen, click the **Add** button.

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

BASIC **ADVANCED**

ADVANCED Home

Address Reservation

Refresh Cancel Add

#	IP Address	Device Name	MAC Address
1	192.168.1.2	lenovo-0685f98c	00:1A:6B:5A:BC:95

IP Address: [] [] [] []

MAC Address: [] [] [] [] [] []

Device Name: [] [] [] [] [] [] [] [] [] []

Help Center

HELP & SUPPORT Support@NETGEAR.com

SEARCH HELP Enter Search Item GO

2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the LAN subnet of the gateway, such as 192.168.1.x.)

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

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

4. Click **Apply** to enter the reserved address into the table.

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

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Security

4

Keeping unwanted content out of your network

This chapter explains how to prevent objectionable content from reaching the computers and other devices that are connected to your network.

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Security Event Email Notifications*

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network.

1. Select **Advanced > Security > Block Sites** to display the following screen:

2. Select one of the keyword blocking options:
 - **Never.** Turn off keyword blocking.
 - **Always.** Turn on keyword blocking.
3. In the keyword field, enter a keyword or domain, click **Add URL Keyword**, and click **Apply**.
 The keyword list supports up to 32 entries. Here are some sample entries:
 - Specify XXX to block http://www.badstuff.com/xxx.html.
 - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
 - Enter a period (.) to block all Internet browsing access.

➤ **To delete a keyword or domain:**

1. Select the keyword that you want to delete from the list.
2. Click **Delete URL Keyword**, and then **Apply** to save your changes.

➤ **To specify a trusted computer:**

You can exempt one trusted computer from blocking and logging. The computer that you exempt has to have a fixed IP address.

1. Select **Allow trusted IP address to visit blocked sites**.
2. In the Trusted IP Address field, enter the IP address.
3. Click **Apply** to save your changes.

Block Services (Port Filtering)

Server computers perform services at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, a service or port number identifies the requested service. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at <http://www.ietf.org/>) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the gateway already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This capability is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers the application uses.

➤ To block services:

1. Select **Advanced > Security > Block Services** to display the following screen:

NETGEAR genie™
CG3300CMR Router Firmware Version V1.04

BASIC ADVANCED English

ADVANCED Home

Setup

Security

Block Sites

Block Services

E-mail

Administration

Advanced Setup

Block Services

Cancel Apply

Services Blocking

Never

Always

Service Table

#	Service Type	Port	IP
+ Add Edit Delete			

Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

2. Select one of the service blocking options:
 - **Never.** Turn off service blocking.
 - **Always.** Turn on service blocking.

- Click **Add** to add a service. The Block Services Setup screen displays:

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

Logout

English

BASIC ADVANCED

ADVANCED Home

► Setup

▼ Security

Block Sites

Block Services

E-mail

► Administration

► Advanced Setup

Block Services Setup

Cancel Add

Service Type User Defined

Protocol TCP

Starting Port (1-65535)

Ending Port (1-65535)

Service Type/User Defined

IP Address: 192 . 168 . 1

Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com

SEARCH HELP Enter Search Item GO

- From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.
- For User Defined, select the protocol, and enter the name and the range of port numbers of the service. For known services, these fields are filled in automatically.
If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **TCP/UDP**.
- Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
- Enter the IP address of the computer that you want to block.
- Click **Add** to enable your Block Services Setup selections.

Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the E-mail screen and specify which alerts you want to receive and how often.

➤ **To set up email notifications:**

1. Select **Advanced > Security > E-mail** to display the following screen:

The screenshot shows the NETGEAR genie web interface for the CG3300CMR router. The 'E-mail' configuration page is displayed under the 'ADVANCED' tab. The sidebar on the left lists navigation options: 'ADVANCED Home', 'Setup', 'Security', 'Block Sites', 'Block Services', 'E-mail', 'Administration', and 'Advanced Setup'. The main content area includes a 'Turn E-mail Notification On' checkbox, a 'Send alerts and logs through e-mail' section with input fields for 'Your Outgoing Mail Server' and 'Send to This E-mail Address', and a 'My mail server requires authentication' checkbox with input fields for 'User Name' and 'Password'. The top right corner shows a 'Logout' button and 'Router Firmware Version V1.04'. The bottom of the screen features a 'HELP & SUPPORT' section with 'Support@NETGEAR.com', a 'SEARCH HELP' bar with 'Enter Search Item' and a 'GO' button, and a 'Show/Hide Help Center' link.

2. To receive email logs and alerts from the gateway, select the **Turn E-mail Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of the outgoing (SMTP) mail server of your ISP (such as mail.myISP.com). You can find this information in the configuration screen of your email program. When this field is blank, log and alert messages are not sent.
4. Enter the email address to which logs and alerts are sent in the Send to This E-mail Address field. This email address is also used as the From address. When this field is blank, log and alert messages are not sent.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.

After the log is sent, the log is cleared from the memory of the gateway. If the gateway cannot email the log file, the log buffer fills up. In this case, the gateway overwrites the log and discards its contents.

Click **Apply** to save your settings.

Administration

5

Managing your network

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

This chapter includes the following sections:

- *[View Gateway Status](#)*
- *[View Logs of Web Access or Attempted Web Access](#)*
- *[View Event Logs](#)*
- *[Manage the Configuration File](#)*
- *[Set Password](#)*

View Gateway Status

- To view gateway status and usage information:

Select **Advanced Home**, or select **Administration > Router Status** to display the following screen:

The screenshot displays the NETGEAR genie CG3300CMR Advanced Home page. The interface includes a top navigation bar with 'Logout' and 'Router Firmware Version V1.04'. The main content area is divided into four sections:

- Router Information:** Displays hardware and software details.

Hardware Version	1.03
Firmware Version	V1.04
GUI Language Version	0.1
System Up Time	0 days 04h:31m:22s
LAN Port	
MAC Address	E0:46:9A:F3:29:07
IP Address	192.168.1.1
DHCP Server	On

 A 'Reboot' button is located at the bottom of this section.
- Cable Network Information:** Displays WAN configuration details.

WAN IP Address	10.10.26.113
Duration	D: 00 H: 11 M: 21 S: 54
Expires	Thu Jan 1 11:22:00 1970
WAN Default Gateway	10.10.26.1
WAN Primary DNS	172.29.16.12
WAN Secondary DNS	0.0.0.0
CM MAC	E0:46:9A:F3:37:8C

 A 'Status' button is located at the bottom of this section.
- Wireless Settings:** Displays wireless configuration details.

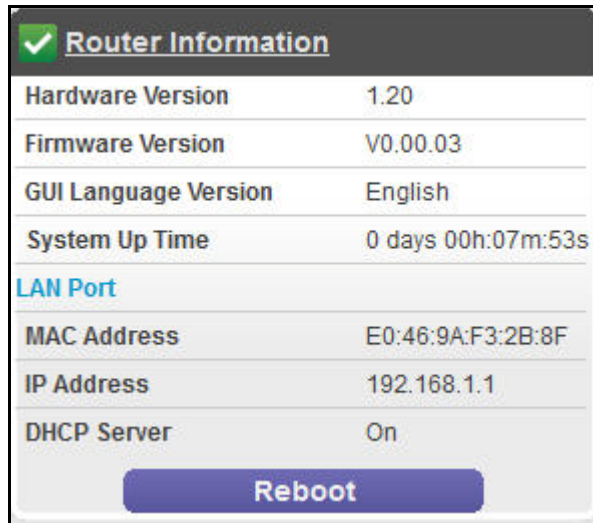
Name (SSID)	ON03792
Region	EU
Channel	6
Mode	Up to 145Mbps
Wireless AP	On
Broadcast Name	On
Wireless Isolation	Off
- Guest Network:** Displays guest network configuration details.

Name (SSID)	NETGEAR_GUEST_0
Wireless AP	Off
Broadcast Name	Off
Wireless Isolation	Off

The left sidebar contains navigation links: 'ADVANCED Home', 'Setup', 'Security', 'Administration' (expanded), 'Router Status', 'Logs', 'Event Logs', 'Attached Devices', 'Backup Settings', 'Set Password', and 'Advanced Setup'. The bottom of the page features a 'HELP & SUPPORT' section with the email 'Support@NETGEAR.com' and a 'SEARCH HELP' bar with a search input field and a 'GO' button.

For a description of the Attached Devices menu item, see [Attached Devices](#) on page 19.

Router Information



✓ Router Information	
Hardware Version	1.20
Firmware Version	V0.00.03
GUI Language Version	English
System Up Time	0 days 00h:07m:53s
LAN Port	
MAC Address	E0:46:9A:F3:2B:8F
IP Address	192.168.1.1
DHCP Server	On
Reboot	

The following settings are displayed:

Hardware Version. The gateway model.

Firmware Version. The version of the gateway firmware. It changes if you upgrade the gateway firmware.

GUI Language Version. The localized language of the user interface.

System Up Time. The length of time that the system has been operating.

LAN Port.

- **MAC Address.** The Media Access Control address. This address is the unique physical address that the Ethernet (LAN) port of the gateway uses.
- **IP Address.** The IP address that the Ethernet (LAN) port of the gateway uses. The default is 192.168.1.1.
- **DHCP Server.** Identifies whether the built-in DHCP server of the gateway is active for the LAN-attached devices.

Click the **Reboot** button to reboot the gateway.

Cable Network Information

✓ Cable Network Information	
WAN IP Address	10.10.26.113
Duration	D: 00 H: 11 M: 21 S: 54
Expires	Thu Jan 1 11:22:00 1970
WAN Default Gateway	10.10.26.1
WAN Primary DNS	172.29.16.12
WAN Secondary DNS	0.0.0.0
CM MAC	E0:46:9A:F3:37:8C
Status	

The following settings are displayed:

WAN IP Address. The IP address that the Internet (WAN) port of the gateway uses. If no address is shown or the address is 0.0.0.0, the gateway cannot connect to the Internet.

Duration. The time that the unit has been up so far.

Expires. Expiration time for the WAN DHCP lease.

WAN Subnet Mask. The IP subnet mask that the Internet (WAN) port of the gateway uses.

WAN Default Gateway.

WAN Primary DNS. The primary Domain Name Server address that the gateway uses. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

WAN Secondary DNS. The secondary Domain Name Server address that the gateway uses.

Cable Connection Status

➤ **To view the cable connection status:**

Click the **Status** button to see the Cable Connection screen.

Cable Connection

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	570000000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	Complete	netgear_snmp.cfg
Security	Enabled	BPI+

Downstream Bonded Channels

Lock Status	Modulation	Channel ID	Max Raw Bit Rate	Frequency	Power	SNR	Docsis/EuroDocsis locked
Locked	256 QAM	1	6952000 sym/sec	570000000 Hz	-10.1375 dBmV	39.8548 dBmV	EuroDocsis
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknown

Upstream Bonded Channels

Lock Status	Modulation	Channel ID	Max Raw Bit Rate	Frequency	Power
Locked	16QAM	1	1280 Ksym/sec	214000000 Hz	51.0000 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0 dBmV

Current System Time: Wed Jan 7 23:17:04 1970

Use the Cable Connection screen to track the initialization procedure of the gateway, and to get details about the downstream and upstream cable channel. The time is displayed after the gateway is initialized.

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

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

Wireless Settings

Wireless Settings	
Name (SSID)	ON02B92
Region	EU
Channel	10
Mode	Up to 145Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup Configured	

The following settings are displayed:

Name (SSID). The wireless network name (SSID) that the gateway uses.

Region. The geographic region where the gateway is being used. It is illegal to use the wireless features of the gateway in some parts of the world.

Channel. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the gateway finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 145 Mbps (default), and Up to 300 Mbps.

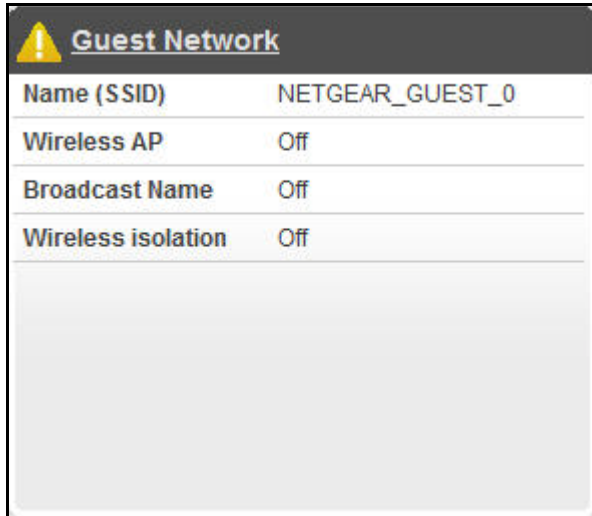
Wireless AP. Indicates whether the radio feature of the gateway is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.


Broadcast Name. Indicates whether the gateway is broadcasting its SSID.

Wireless Isolation. Indicates that the wireless clients can connect to the Internet. However, they cannot access each other or access Ethernet devices on the network.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

Guest Network



 Guest Network	
Name (SSID)	NETGEAR_GUEST_0
Wireless AP	Off
Broadcast Name	Off
Wireless isolation	Off

The following settings are displayed:

Name (SSID). The 11N wireless network name (SSID) that the gateway uses. The default name is NETGEAR_Guest_0.

Wireless AP. Indicates whether the radio feature of the gateway is enabled. If this feature is not enabled, the Wireless LEDs on the front panel are off.

Broadcast Name. Indicates whether the gateway is broadcasting its SSID.

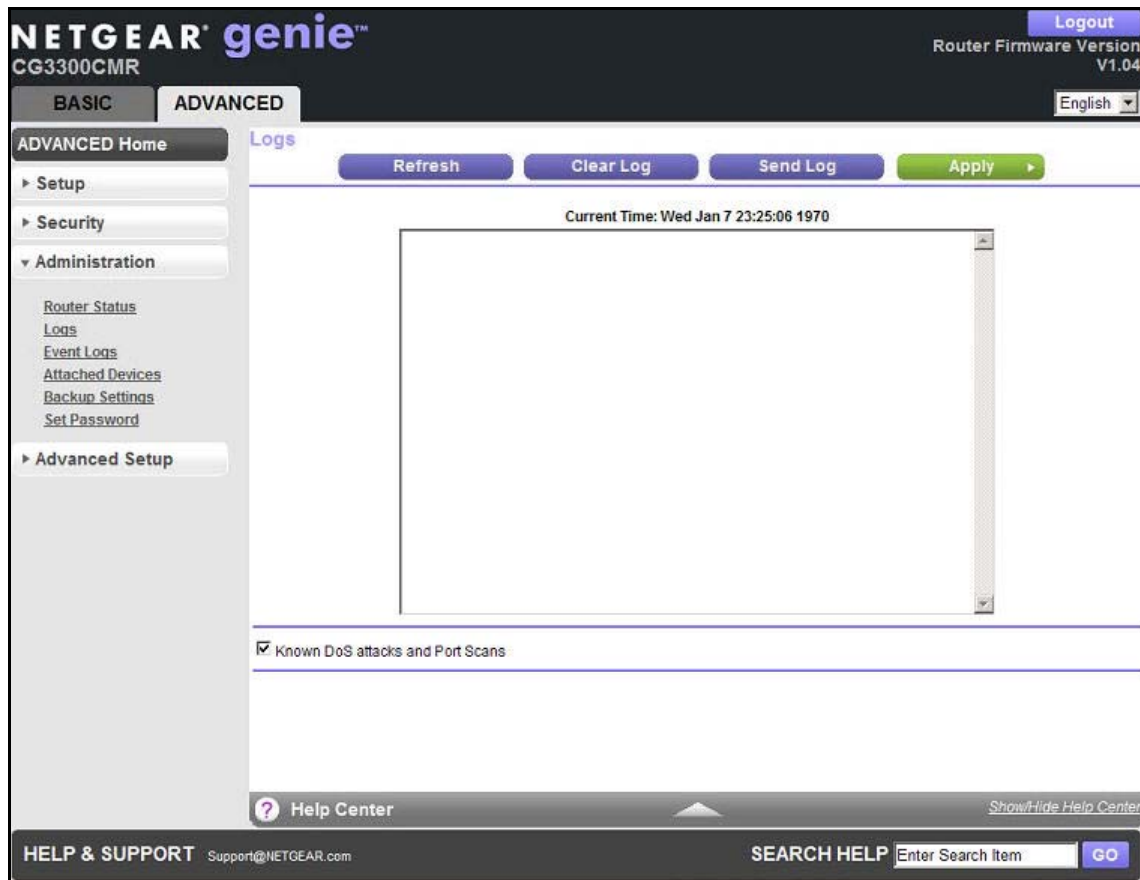
Wireless Isolation. Indicates that the wireless clients can connect to the Internet. However, they cannot access each other or access Ethernet devices on the network.

View Logs of Web Access or Attempted Web Access

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

➤ **To view the logs:**

Select **Advanced > Administration > Logs**. The Logs screen displays.



The log screen shows the following information:

- **Date and time.** The date and time the log entry was recorded.
- **Source IP.** The IP address of the initiating device for this log entry.
- **Target address.** The name or IP address of the website or news group visited or to which access was attempted.
- **Action.** Whether the access was blocked or allowed.
- **Known DoS attacks and Port Scans.** Clear this check box to ignore known DoS attacks and port scans.

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

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

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

To save your changes, click the **Apply** button.

View Event Logs

Event logs capture important gateway events.

➤ **To view the event logs:**

Select **Advanced > Administration > Event Logs**. The Event Logs screen displays.

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

BASIC **ADVANCED**

Event Logs

Refresh Clear Log

Current Time: Wed Jan 7 23:25:42 1970

Time	Priority	Description
Time Not Established	Warning (5)	System over temperature;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:...
Time Not Established	Warning (5)	Lost MDD Timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:90:d...
Time Not Established	Warning (5)	MDD message timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:9...
Time Not Established	Critical (3)	No Ranging Response received - T3 time-out;CM-MAC=e0:46:9a:f3:...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...
Time Not Established	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...
Time Not Established	Error (4)	ToD request sent. No Response received;CM-MAC=e0:46:9a:f3:37:...
Time Not Established	Warning (5)	Lost MDD Timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:90:d...
Time Not Established	Warning (5)	MDD message timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:9...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...
Time Not Established	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...
Time Not Established	Error (4)	ToD request sent. No Response received;CM-MAC=e0:46:9a:f3:37:...
Time Not Established	Warning (5)	Lost MDD Timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:90:d...
Time Not Established	Warning (5)	MDD message timeout;CM-MAC=e0:46:9a:f3:37:8c;CMTS-MAC=00:22:9...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...
Time Not Established	Warning (5)	MIMO Event MIMO: Stored MIMO=-1 post cfg file MIMO=-1;CM-MAC=...
Time Not Established	Warning (5)	ToD request sent - No Response received;CM-MAC=e0:46:9a:f3:37...

Help Center

HELP & SUPPORT Support@NETGEAR.com

SEARCH HELP Enter Search Item GO

The log screen shows the following information:

- **Time.** The time the event log entry was recorded.
- **Priority.** The severity for this event log entry.
- **Description.** A description of this event log entry.

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

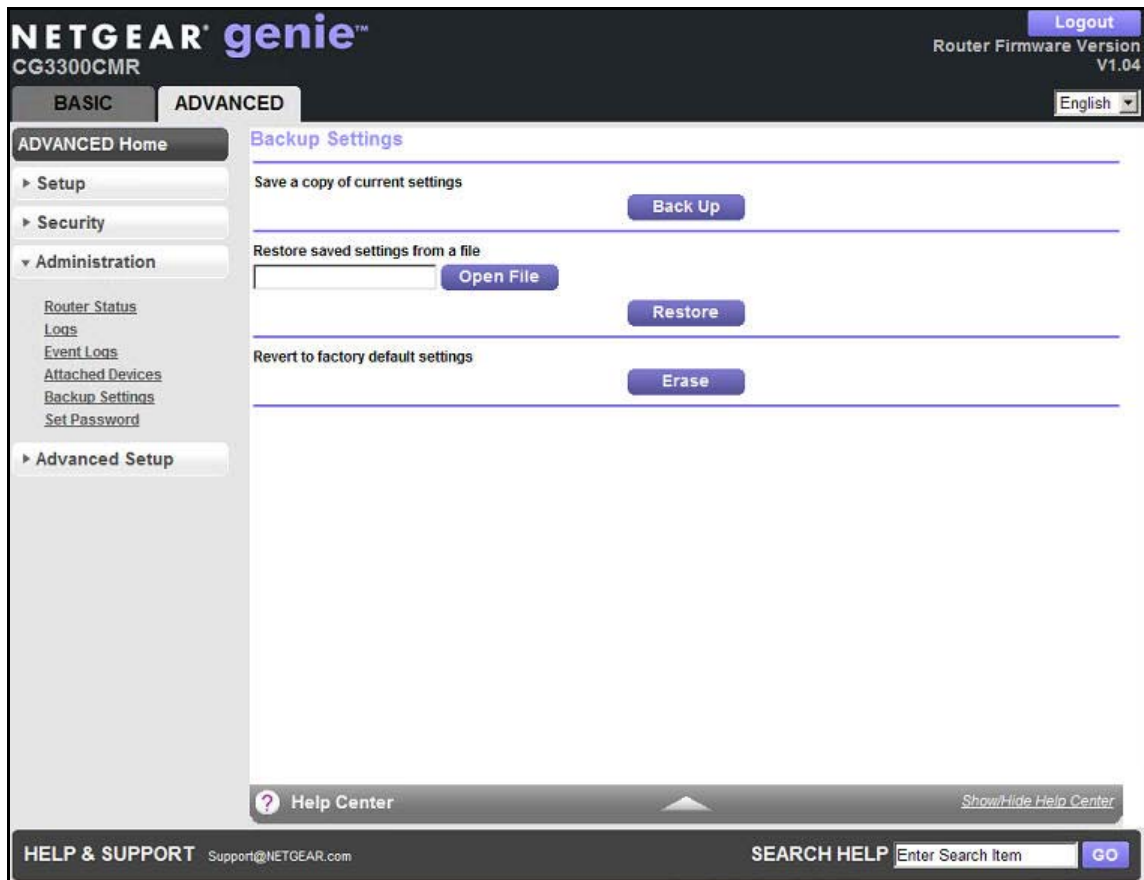
To clear the log entries, click the **Clear Log** button.

Manage the Configuration File

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

Back Up Settings

- To back up the configuration settings of the gateway:
 1. Select **Advanced > Administration > Backup Settings** to display the following screen:



2. Click **Back Up** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

- To restore configuration settings that you backed up:
 1. Enter the full path to the file on your network, or click the **Browse** button to find the file.

2. When you have located the .cfg file, click the **Restore** button to upload the file to the gateway.

Upon completion, the gateway reboots.



WARNING:

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the gateway to a different network or if you have forgotten the password), you want to erase the configuration and restore the factory default settings.

Either press the **Restore Factory Settings** button on the back of the gateway (see [Factory Default Settings](#) on page 79) or click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the DHCP of the gateway.

Set Password

This feature allows you to change the default password that is used to log in to the gateway with the user name **admin**.

This gateway password is not the same as the password for wireless access. The label on the bottom of your gateway shows your unique wireless network name (SSID) and password for wireless access (see [Gateway Label](#) on page 10).

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

1. Select **Advanced > Administration > Set Password** to display the following screen:

The screenshot displays the NETGEAR genie CG3300CMR web interface. The top navigation bar includes the 'Logout' button and 'Router Firmware Version V1.04'. The 'ADVANCED' tab is active, and the 'Set Password' page is shown. The sidebar on the left lists various system management options. The main form area has three text input fields for password entry and two action buttons: 'Cancel' and 'Apply'.

2. Type the old password, and type the new password twice in the fields on this screen.
3. Click **Apply** so that your changes take effect.

Advanced Settings

6

Fine-tuning your network

This chapter describes the advanced features of your gateway. The information requires a solid understanding of networking concepts and is for people who want to set up the gateway for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Services*
- *Port Forwarding and Port Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Dynamic DNS*
- *Cable Status*
- *Universal Plug and Play*
- *IPv6*
- *NAT*

Advanced Wireless Settings

➤ To view the advanced wireless settings:

Select **Advanced > Advanced Setup > Advanced Wireless Settings** to display the following screen:

The screenshot displays the 'Advanced Wireless Settings' page for a NETGEAR CG3300CMR router. The interface includes a top navigation bar with 'BASIC' and 'ADVANCED' tabs, and a left sidebar with a tree view showing 'Advanced Setup' expanded. The main content area contains the following settings:

- Advanced Wireless Settings**
 - ☒ Enable Wireless Router Radio
 - ☐ Enable Wireless Isolation
 - ☒ Enable SSID Broadcast
 - ☒ Enable WMM (Wi-Fi multimedia) settings
- Fragmentation Length (256-2346): 2346
- CTS/RTS Threshold (1-2347): 2347
- Preamble Mode: Long Preamble
- Transmit Power Control: 100.0%
- Wireless Card Access List: Set Up Access List
- Nearby Wireless Access Points: Scan Wifi AP

The bottom of the page features a 'Help Center' link, a 'SEARCH HELP' bar, and a 'GO' button.

Advanced Wireless Settings

The following settings are available on this part of the screen:

- **Enable Wireless Router Radio.** You can completely turn off the wireless portion of the wireless gateway by clearing this check box. Select this check box again to enable the wireless portion of the gateway. When the wireless radio is disabled, other members of your household can use the gateway by connecting their computers to the gateway with an Ethernet cable.
- **Enable Wireless Isolation.** If this check box is selected, then wireless clients (computers or wireless devices) that join the network can use the Internet. They cannot, however, access each other or access Ethernet devices on the network.
- **Enable SSID Broadcast.** The setting enables broadcast of the SSID.

- **Enable WMM (Wi-Fi multimedia) settings.** WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function properly, wireless clients have to support WMM also.

Note: The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

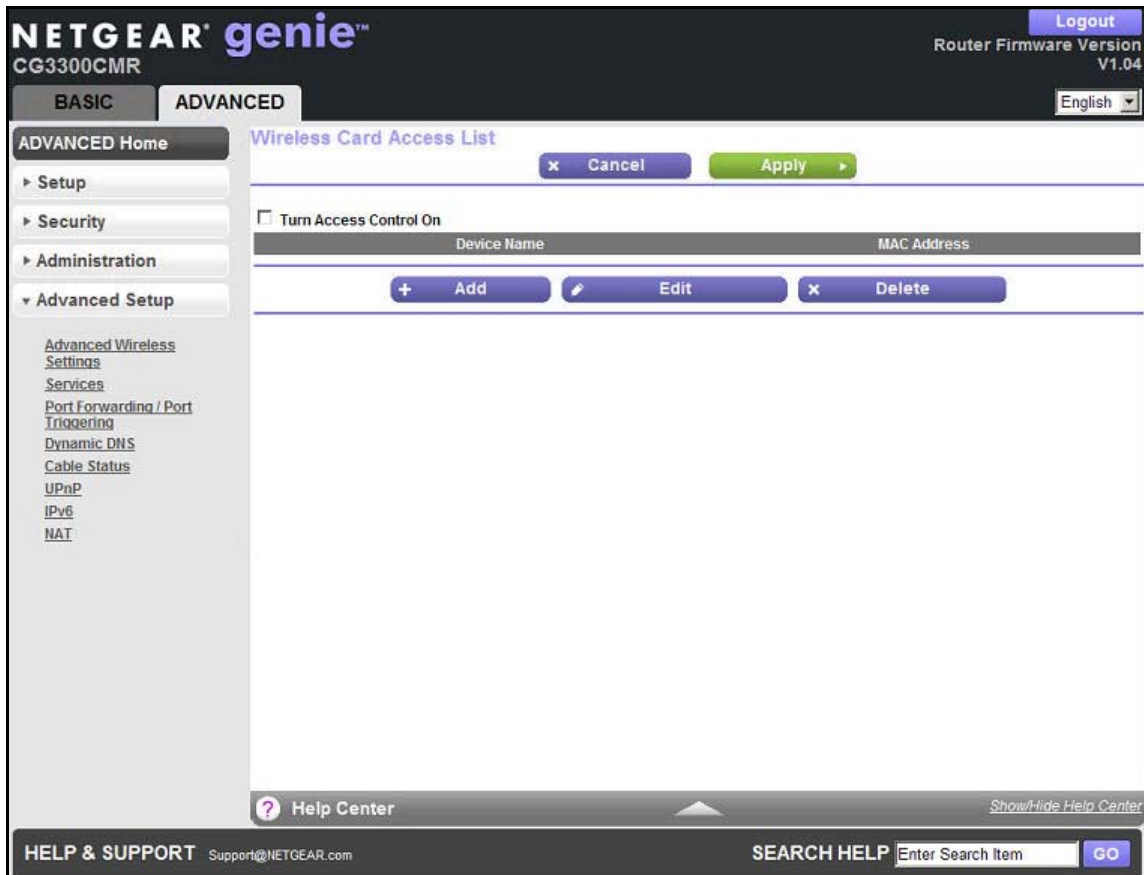
- **Transmit Power Control.** With the default setting of 100%, the gateway uses the power level that NETGEAR recommends for transmitting wireless packets. If you change this setting to a lower percentage, it saves power, but also reduces wireless coverage.

Wireless Card Access List

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

➤ **To enable wireless card access:**

1. Click the **Set Up Access List** button display the Wireless Card Access List screen.



On this screen, you can restrict access to your network to specific devices based on their MAC address.

2. Select the **Turn Access Control On** check box to enable the restricting of wireless computers and devices by their MAC addresses.

Note: If Turn Access Control On is enabled and the Access Control List is blank, then all wireless computers and devices are unable to connect to your wireless network.

3. For information about how to add wireless computers and devices to the Access Control List, see [Wireless Client Access List Setup](#) on page 56.

- Click the **Apply** button to save changes and return to the Advanced Wireless Settings screen.

Wireless Client Access List Setup

➤ To set up the access control list:

- Click the **Add** button on the Wireless Card Access List screen to display the Wireless Card Access Setup screen.

The screenshot displays the NETGEAR genie web interface for the CG3300CMR router. The top navigation bar includes 'BASIC' and 'ADVANCED' tabs, with 'ADVANCED' currently selected. A sidebar on the left lists various configuration options under 'ADVANCED Setup', including 'Advanced Wireless Settings', 'Services', 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Cable Status', 'UPnP', 'IPv6', and 'NAT'. The main content area is titled 'Wireless Card Access Setup'. It features a table for 'Available Wireless Cards' with columns for 'Device Name' and 'MAC Address'. Below the table is a 'Wireless Card Entry' section with input fields for 'Device Name' and 'MAC Address'. At the bottom of this section are three buttons: '+ Add', 'x Cancel', and 'Refresh'. The footer contains a 'Help Center' link, 'HELP & SUPPORT' information, and a search bar.

This screen displays a list of currently active wireless computers and devices and their Ethernet MAC addresses.

- If the wireless computer or device you want appears in the list, click its radio button to capture its MAC address. Otherwise, manually enter the MAC address of the authorized wireless computer or device. The MAC address is found on the computer or device.
- If no device name appears, type a descriptive name for the computer or device that you are adding.
- When finished entering the MAC address, return to the Wireless Access List screen by clicking the **Add** button.
- Repeat steps 1 through 4 for each wireless computer or device.

- When finished adding wireless computers and devices to this list, on the Wireless Card Access Setup screen, select the **Turn Access Control On** check box to enable access control.
- On the Wireless Card Access Setup screen, click **Apply** to save changes and return to the Advanced Wireless Settings screen.

Nearby Wireless Access Points

Click the **Scan With AP** button to find access points that are near the CG3300CMR. The Nearby Wireless Access Points screen displays.

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

BASIC **ADVANCED** English

ADVANCED Home

- Setup
- Security
- Administration
- Advanced Setup
 - Advanced Wireless Settings
 - Services
 - Port Forwarding / Port Triggering
 - Dynamic DNS
 - Cable Status
 - UPnP
 - IPv6
 - NAT

Nearby Wireless Access Points

Cancel Refresh

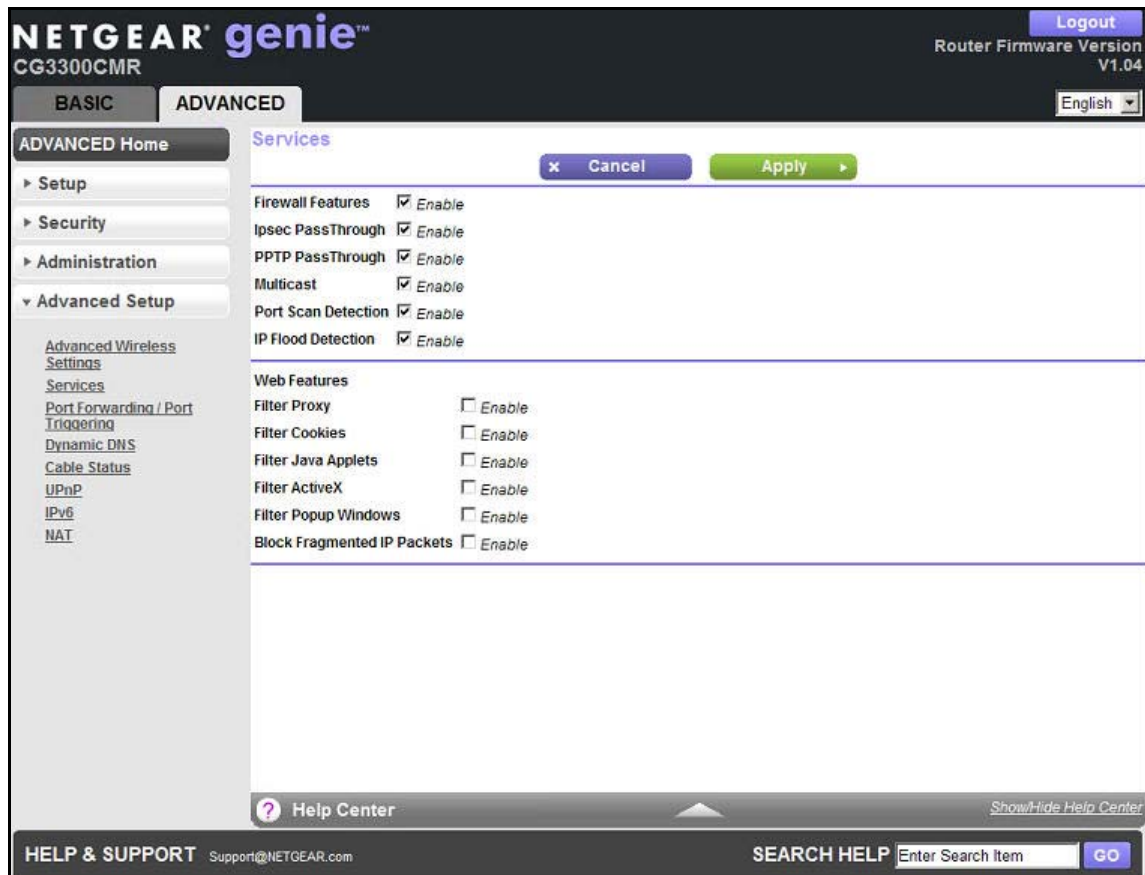
Network Name	Security Mode	Mode	PHY Mode	RSSI	Channel	BSSID
ngHub_319124N700021	CCMP CCMP PSK	Master	802.11n	-53 dBm	1	20:4E:7F:D6:DF:95
CBU_11g	CCMP CCMP PSK	Master	802.11n	-71 dBm	1	E0:91:F5:A3:6C:60
NGLab-2.4G	CCMP CCMP PSK	Master	802.11b/g	-57 dBm	1	00:C0:02:45:72:95
NUMERICABLE-0001	TKIP CCMP-TKIP PSK	Master	802.11n	-67 dBm	1	00:60:0F:00:00:01
snfest	CCMP CCMP PSK	Master	802.11b/g	-68 dBm	6	74:44:01:2E:38:96
NETGEAR49	CCMP CCMP PSK	Master	802.11b/g	-55 dBm	6	E0:46:9A:13:0A:BB
NETGEAR-Guest	CCMP CCMP PSK	Master	802.11b/g	-80 dBm	6	2E:B0:5D:3C:1A:25
CBU_11g	CCMP CCMP PSK	Master	802.11n	-67 dBm	6	74:44:01:96:CD:00
NETGEAR68	CCMP CCMP PSK	Master	802.11b/g	-42 dBm	6	2C:B0:5D:2F:DF:33
WNDR4500-2.4G	CCMP CCMP PSK	Master	802.11b/g	-45 dBm	6	20:4E:7F:9D:01:F4
WNDR4500-Guest	TKIP CCMP-TKIP PSK	Master	802.11b/g	-45 dBm	6	22:4E:7F:9D:01:F5
NSBU-DI-G	CCMP CCMP PSK	Master	802.11b/g	-70 dBm	6	00:1E:2A:79:BA:64
NETGEAR92	CCMP CCMP PSK	Master	802.11b/g	-82 dBm	6	2C:B0:5D:3C:1A:24
6c97	CCMP CCMP PSK	Master	802.11b/g	-83 dBm	6	00:1E:2A:09:50:F0
BelI088A	TKIP CCMP-TKIP PSK	Master	802.11b/g	-42 dBm	11	E0:46:9A:74:08:8A
nggquest	TKIP CCMP-TKIP PSK	Master	802.11n	-70 dBm	10	20:4E:7F:58:33:01
Eco24	CCMP CCMP PSK	Master	802.11b/g	-71 dBm	11	74:44:01:55:89:58
NETGEAR16	TKIP CCMP-TKIP PSK	Master	802.11n	-53 dBm	11	E0:46:9A:A3:90:7C
Customer ID	TKIP TKIP PSK	Master	802.11b/g	-64 dBm	11	00:18:F3:EF:DA:63
NSBU-HW	TKIP CCMP-TKIP PSK	Master	802.11b/g	-65 dBm	11	00:24:B2:06:7D:88
homelab-4500	CCMP CCMP PSK	Master	802.11b/g	-76 dBm	11	20:4E:7F:1B:D3:C1
IPrimus70373E	TKIP CCMP-TKIP PSK	Master	802.11b/g	-52 dBm	10	C4:3D:C7:70:37:40
NETGEAR89	CCMP CCMP PSK	Master	802.11b/g	-39 dBm	10	E0:46:9A:B7:C3:FF
NETGEAR-4G	TKIP CCMP-TKIP PSK	Master	802.11b/g	-69 dBm	11	84:1B:5E:33:5D:D8

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

Services

- To view the advanced wireless settings:

Select **Advanced > Advanced Setup > Services** to display the following screen:



Use the Services screen to disable certain gateway features. To disable a feature, clear the check box.

- When Firewall Features are enabled, the gateway performs stateful packet inspection (SPI) and protects against denial of service (DoS) attacks.
- When IPsec Pass-Through is enabled, IPsec traffic is forwarded. When it is disabled, this traffic is blocked.
- When PPTP Pass-Through is enabled, PPTP traffic is forwarded. When it is disabled, this traffic is blocked.
- When Multicast is enabled, the cable gateway passes multicasting streams through the firewall.
- When Port Scan Detection is enabled, the cable gateway responds to Internet-based port scans.
- When IP Flood Detection is enabled, the cable gateway blocks malicious devices that are attempting to flood devices.

Use Web Features to have the firewall block certain web-oriented cookies, Java scripts, and pop-up windows.

Click the **Apply** button to save your settings.

Port Forwarding and Port Triggering

By default, the gateway blocks inbound traffic from the Internet to your computers except for replies to your outbound traffic. Create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when your gateway does not recognize their replies.

Your gateway provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network accesses a computer on the Internet, your computer sends your gateway a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your gateway has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type `http://www.example.com` into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your gateway.

Source address. The IP address of your computer.

Source port number. 5678, which is the browser session.

Destination address. The IP address of `www.example.com`, which your computer finds by asking a DNS server.

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

3. Your gateway creates an entry in its internal session table describing this communication session between your computer and the web server at `www.example.com`. Before sending the web page request message to `www.example.com`, your gateway stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

- The source address is replaced with the public IP address of your gateway. This step is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
- The source port number is changed to a number that is chosen by the gateway, such as 33333. This step is necessary because two computers could independently be using the same session number.

Your gateway then sends this request message through the Internet to the web server at www.example.com.

4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your gateway.

Source address. The IP address of www.example.com.

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

Destination address. The public IP address of your gateway.

Destination port number. 33333.

5. Upon receiving the incoming message, your gateway checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the gateway then modifies the message to restore the original address information that is replaced by NAT. Your gateway sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

Source address. The IP address of www.example.com.

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

Destination address. The IP address of your computer.

Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your gateway eventually detects a period of inactivity in the communications. Your gateway then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your gateway from a particular service port number, and replies from the remote computer to your gateway are directed to that port number. If the remote server sends a reply to a different port number, your gateway does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your gateway, you can tell the gateway to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but

also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the gateway, “When you initiate a session with destination port 6667, you have to allow incoming traffic also on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your gateway.
3. Your gateway creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your gateway stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your gateway creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your gateway using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an identify message to your gateway with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your gateway checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the gateway restores the original address information that is replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your gateway checks its session table and learns that there is an active session for port 113, associated with your computer. The gateway replaces the destination IP address of the message with the IP address of your computer and forwards the message to your computer.
8. When you finish your chat session, your gateway eventually senses a period of inactivity in the communications. The gateway then removes the session information from its session table, and incoming traffic is no longer accepted on ports 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that triggers the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you 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 browser on a remote computer accesses 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 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 is 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. Usually you can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering is used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and is never triggered.

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 want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding/Port Triggering screen 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 determine which type of service, application, or game you want to provide, and the local IP address of the computer that provides the service. The server computer always has to have the same IP address.

➤ To set up port forwarding:

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your wireless cable gateway.

1. Select **Advanced Setup > Port Forwarding/Port Triggering** to display the following screen:

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

Logout English

BASIC ADVANCED

ADVANCED Home

- ▶ Setup
- ▶ Security
- ▶ Administration
- ▼ **Advanced Setup**
 - Advanced Wireless Settings
 - Services
 - Port Forwarding / Port Triggering
 - Dynamic DNS
 - Cable Status
 - UPnP
 - IPv6
 - NAT

Port Forwarding / Port Triggering

Please select the service type.

☒ Port Forwarding
☐ Port Triggering

Service Name: [Dropdown] Server IP Address: [192] [168] [1] [] + Add

#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
<p>Edit Service X Delete Service</p> <p>+ Add Custom Service</p>						

Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

Port Forwarding is selected as the service type.

2. From the Service Name list, select the service or game that you host on your network. If the service does not appear in the list, see [Add a Custom Service](#) on page 64.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that provides this service.
4. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➤ To add a custom service:

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.

3. Click the **Add Custom Service** button to display the following screen:

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

BASIC **ADVANCED** English

ADVANCED Home **Ports - Custom Services** Cancel Apply

Service Name:

Protocol:

External Starting Port:
External Ending Port:

☒ Use the same port range for internal port

Internal Starting Port:
Internal Ending Port:

Internal IP address:

Or select from currently attached devices

IP Address	Device Name
192.168.1.2	lenovo-0685f98c

HELP & SUPPORT Support@NETGEAR.com **SEARCH HELP** GO

4. In the Service Name field, enter a descriptive name.
5. In the Protocol list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Starting Port fields, enter the beginning port number.
 - If the application uses a single port, enter the same port number in the Ending Port field.
 - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
7. In the Internal IP Address field, enter the IP address of your local computer that provides this service.
8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➤ To edit or delete a port forwarding entry:

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➤ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your gateway always gives your web server an IP address of 192.168.1.33.
2. In the Port Forwarding/Port Triggering screen, configure the gateway to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your gateway to use the name as described in [Dynamic DNS](#) on page 68. To access your web server from the Internet, a remote user has to know the IP address that your ISP assigns. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

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

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application opens incoming ports that are different from the outgoing port.

When port triggering is enabled, the gateway monitors outbound traffic looking for a specified outbound “trigger” port. When the gateway detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The gateway then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

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

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), enable Universal Plug and Play (UPnP) according to the instructions in [Universal Plug and Play](#) on page 70.

To set up port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that triggers the opening of the inbound

ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➤ **To set up port triggering:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.

NETGEAR genie™
CG3300CMR

Router Firmware Version V1.04

Logout

English

BASIC **ADVANCED**

ADVANCED Home

- ▶ Setup
- ▶ Security
- ▶ Administration
- ▼ **Advanced Setup**
 - Advanced Wireless Settings
 - Services
 - Port Forwarding / Port Triggering**
 - Dynamic DNS
 - Cable Status
 - UPnP
 - IPv6
 - NAT

Port Forwarding / Port Triggering

Cancel Apply

Please select the service type.

☐ Port Forwarding

☒ Port Triggering

☒ Disable Port Triggering

Port Triggering Time-out(in minutes) 10

Port Triggering Portmap Table

#	Enable	Service Name	Service Type	Inbound Connection	Service User
+ Add Service Edit Service Delete Service					

Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

3. Clear the **Disable Port Triggering** check box if it is selected.

Note: If the *Disable Port Triggering* check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the gateway is retained even though it is not used.

4. In the Port Triggering Time-out field, enter a value up to 9999 minutes.
5. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This step is required because the gateway cannot be sure when the application has terminated.

6. Click **Add Service** to display the following screen:

The screenshot displays the 'Port Triggering - Services' configuration page in the NETGEAR genie interface. The page is titled 'NETGEAR genie CG3300CMR' and shows the 'Router Firmware Version V1.04'. The 'ADVANCED' tab is selected, and the 'Port Triggering - Services' section is active. The left sidebar contains navigation links: 'ADVANCED Home', 'Setup', 'Security', 'Administration', and 'Advanced Setup'. The 'Advanced Setup' section includes links for 'Advanced Wireless Settings', 'Services', 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Cable Status', 'UPnP', 'IPv6', and 'NAT'. The main configuration area includes fields for 'Service Name', 'Service User' (set to 'Any'), 'Service Type' (set to 'TCP'), and 'Triggering Port'. Below these are 'Inbound Connection' settings for 'Connection Type' (set to 'TCP/UDP'), 'Starting Port', and 'Ending Port'. The page also features a 'Cancel' button, an 'Apply' button, a 'Help Center' link, and a 'SEARCH HELP' bar at the bottom.

7. In the Service Name field, type a descriptive service name. No spaces are allowed for the service name field.
8. In the Service User list, select **Any** (the default) to allow any computer on the Internet to use this service. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
9. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
10. In the Triggering Port field, enter the number of the outbound traffic port that causes the inbound ports open.
11. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
12. Click **Apply**. The service appears in the Port Triggering Portmap table.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP

address, you do not know in advance what your IP address is, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your 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.

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

➤ **To set up Dynamic DNS:**

1. On the Advanced tab, select **Advanced Setup > Dynamic DNS** to display the following screen:

The screenshot shows the NETGEAR genie CG3300CMR web interface. The top navigation bar includes 'Logout', 'Router Firmware Version V1.04', and a language dropdown set to 'English'. The main interface has two tabs: 'BASIC' and 'ADVANCED'. The 'ADVANCED' tab is selected, and the left sidebar shows 'ADVANCED Home' with sub-links for 'Setup', 'Security', 'Administration', and 'Advanced Setup'. Under 'Advanced Setup', there are links for 'Advanced Wireless Settings', 'Services', 'Port Forwarding / Port Triggering', 'Dynamic DNS' (which is highlighted), 'Cable Status', 'UPnP', 'IPv6', and 'NAT'. The main content area is titled 'Dynamic DNS' and contains a 'Show Status' button, a 'Cancel' button, and an 'Apply' button. Below these buttons is a checkbox labeled 'Use a Dynamic DNS Service'. Under this checkbox, there are four input fields: 'Service Provider' (with a dropdown menu showing 'www.DynDNS.org'), 'Host Name', 'User Name', and 'Password'. At the bottom of the page, there is a 'Help Center' link and a 'SEARCH HELP' section with a text input field and a 'GO' button.

2. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider list.
3. Select the **Use a Dynamic DNS Service** check box.

4. Select the name of your Dynamic DNS service provider. If your Dynamic DNS service provider is DynDNS.org, for example, select **www.dyndns.org**.
5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
6. Type the user name for your Dynamic DNS account. This name is the name that you use to log in to your account, not your host name.
7. Type the password (or key) for your Dynamic DNS account.
8. Click **Apply** to save your configuration.

Cable Status

For information about this topic, see [Cable Connection Status](#) on page 44.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to 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.

Note: 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 turn on Universal Plug and Play:

1. Select **Advanced > Advanced Setup > UPnP**. The UPnP screen displays.

NETGEAR genie™
CG3300CMR Router Firmware Version V1.04

BASIC ADVANCED English

ADVANCED Home

- ▶ Setup
- ▶ Security
- ▶ Administration
- ▼ Advanced Setup
 - Advanced Wireless Settings
 - Services
 - Port Forwarding / Port Triggering
 - Dynamic DNS
 - Cable Status
 - UPnP
 - IPv6
 - NAT

UPnP

Refresh x Cancel Apply

☒ Turn UPnP On

Advertisement Period(in minutes) 30

Advertisement Time to Live(in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

2. Specify the following settings:

Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If this check box is not selected, the gateway does not allow any device to control the resources automatically, such as port forwarding (mapping) of the gateway.

Advertisement Period. The advertisement period is how often the gateway broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

Advertisement Time to Live. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which are fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it is necessary to increase this value.

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

- 3.** Click **Apply** to save your settings.

IPv6

You can use this feature to display the IPv6 Internet connection type.

- **To display the IPv6 Internet connection readings:**

Select **Advanced > Advanced Setup > IPv6** to display the following screen:

NETGEAR genie™
CG3300CMR

Logout
Router Firmware Version V1.0

BASIC ADVANCED English

ADVANCED Home

- Setup
- Security
- Administration
- Advanced Setup

[Advanced Wireless Settings](#)
[Services](#)
[Port Forwarding / Port Triggering](#)
[Dynamic DNS](#)
[Cable Status](#)
[UPnP](#)
[IPv6](#)
[NAT](#)

IPv6

WAN Interface:
 WAN MAC Address: E0:46:9A:F3:37:8E
 WAN IPv6 Address: Not Available
 WAN IPv6 Prefix: ::/64

LAN Interface:
 LAN MAC Address: E0:46:9A:F3:29:07
 LAN IPv6 Address: Not Available
 LAN IPv6 Prefix: /0

IPv6 Hosts

Host MAC Address	Host IPv6 Address

? Help Center Show/Hide Help Center

HELP & SUPPORT Support@NETGEAR.com SEARCH HELP Enter Search Item GO

The following information is displayed in this screen:

WAN MAC Address. The address of the gateway interface that is facing the MSO. This interface acquires its IPv6 provisioning directly from the MSO provisioning server.

WAN IPv6 Address. The address of the gateway interface that is facing the MSO. This interface acquires its IPv6 provisioning directly from the MSO provisioning server.

WAN IPv6 Prefix.

LAN MAC Address. The address of the gateway interface that is facing hosts on the subscriber side of the gateway. This interface derives its IPv6 provisioning using the IPv6 prefix that is supplied by the MSO provisioning server.

LAN IPv6 Address. The address of the gateway interface that is facing hosts on the subscriber side of the gateway. This interface derives its IPv6 provisioning using the IPv6 prefix that is supplied by the MSO provisioning server.

LAN IPv6 Prefix.

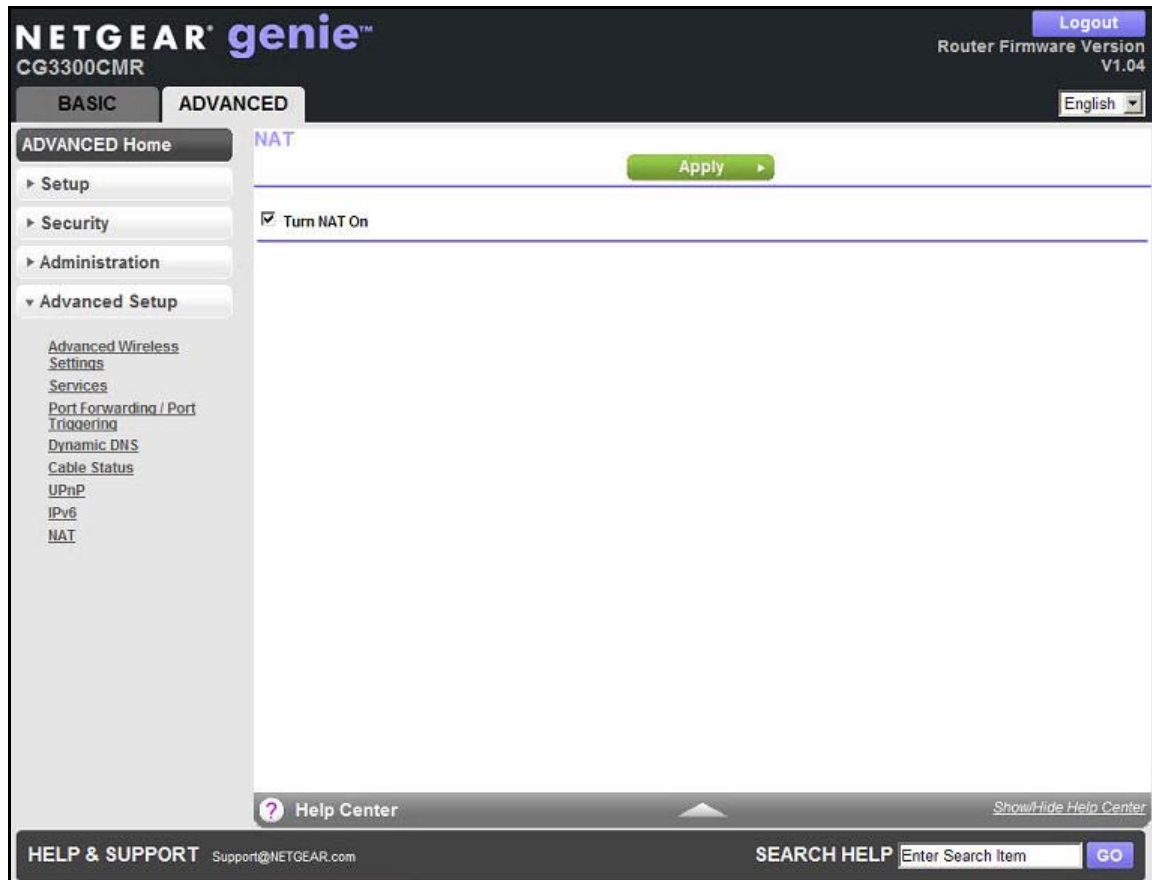
IPv6 Hosts. A table with one row for each IPv6 host that is connected to the gateway.

NAT

You can enable or disable Network Address Translation.

➤ **To enable or disable Network Address Translation:**

1. Select **Advanced > Advanced Setup > NAT** to display the following screen:



2. Select or clear the **Turn NAT On** check box.
3. Click the **Apply** button to save your settings.

Troubleshooting

7

Find and fix common issues

This chapter gives information about troubleshooting your Wireless Cable Gateway CG3300CMR. For the common problems listed, go to the section indicated.

- Have I connected the gateway correctly?
Go to [Basic Functions](#) on page 74.
- I cannot access the gateway configuration with my browser.
Go to [Connect to the Main Menu of the Gateway](#) on page 75.
- I have configured the gateway but I cannot access the Internet.
Go to [Troubleshoot the ISP Connection](#) on page 76.
- I cannot remember the configuration password of the gateway or I want to clear the configuration and start over again.
Go to [Factory Default Settings](#) on page 79.

Tip: NETGEAR provides helpful articles, documentation, and the latest software updates at support.netgear.com.

Basic Functions

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

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

If any of these conditions does not occur, refer to the appropriate following section.

Using LEDs to Troubleshoot

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

LED Behavior	Action
All LEDs are off when the gateway is plugged in.	<p>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.</p> <p>Check that you are using the 12V DC power adapter from NETGEAR for this product.</p> <p>If the error persists, you have a hardware problem. Contact technical support.</p>
All LEDs stay on.	<ul style="list-style-type: none"> • Clear the configuration of the gateway to its factory defaults. This operation sets the IP address of the gateway to 192.168.1.1. See Factory Default Settings on page 79. • If the error persists, you have a hardware problem. Contact technical support.
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 Internet service has been provisioned by your cable service provider. Your provider can verify that the signal quality is good enough for cable modem service. • Remove any excessive splitters that you have on your cable line. Run a “home run” back to the point where the cable enters your home.

Connect to the Main Menu of the Gateway

If you are unable to access the main menu of the gateway 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 IP address of your computer is on the same subnet as the gateway. If you are using the recommended addressing scheme, the address of your computer is in the range of 192.168.1.10 to 192.168.1.254.

Note: If the IP address of your computer is shown as 169.254.x.x: Recent versions of Windows and Mac OS generate and assign an IP address when 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 the IP address of your gateway has been changed and you do not know the current IP address, clear the configuration of the gateway to its factory defaults. This operation sets the IP address of the gateway to 192.168.1.1. This procedure is explained in [Factory Default Settings](#) on page 79.
- 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 **admin** is lower-case (Caps Lock is off). The default password of **password**.

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 have occurred, but the web browser might be caching the old configuration.

Troubleshoot the ISP Connection

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

Additionally, your computer does not have the gateway that is 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.

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 PC running Windows 95 or later:**

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

ping 192.168.1.1

3. Click **OK**.

You see a message like this one:

Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

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

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

Request timed out

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

- Wrong physical connections.
 - Make sure that the LAN port LED is on. If the LED is off, see [Using LEDs to Troubleshoot](#) on page 75.
 - Check the corresponding link LEDs are on for your network interface card and 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 menu, type:

ping -n 10 <IP address>

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

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 is listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in the Network Control Panel of your computer. Verify that the IP address of the gateway is listed as the default gateway.
- Check 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.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.

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 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).

The time that 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.

Supplemental Information



This appendix provides factory default settings and technical specifications for the Wireless Cable Gateway CG3300CMR.

Factory Default Settings

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

Factory Default Settings		
Gateway login	User login URL	http://192.168.1.1
	User name and password (case-sensitive)	admin/password
Local network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
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

Factory Default Settings (continued)		
Wireless	Wireless communication	Enabled
	SSID name	As shown on the product label
	Security	WPA/WPA2 The default WPA/WPA2 passphrase is as shown on the product label.
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	Country/region	EU
	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

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

Technical Specifications

The following table describes the technical specifications for the gateway.

Technical Specifications	
Network protocol and standards compatibility	Data and routing protocols: TCP/IP, DHCP server and client, DNS relay, NAT (many-to-one), TFTP client, VPN passthrough (IPSec, PPTP)
Power adapter	<ul style="list-style-type: none"> Europe (input): 230V, 50 Hz, input All regions (output): 12V DC @ 1.5A output 18W maximum
Physical specifications	<ul style="list-style-type: none"> Dimensions: 7.5 by 3.8 by 1.4 in. (195 by 112 by 33 mm) Weight: 0.65 lb (0.28 kg)
Environmental	<ul style="list-style-type: none"> Operating temperature: 32° to 140°F (0° to 40°C) Operating humidity: 90% maximum relative humidity, noncondensing Electromagnetic emissions: Meets requirements of: FCC Part 15 Class B.

Technical Specifications (continued)	
Interface	Local: 10BASE-T, 100/1000BASE-Tx, RJ-45 802.11n/g/b
	Internet: DOCSIS 3.0. Downward compatible with DOCSIS 2.0, 1.1 and 1.0

Notification of Compliance



NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: 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.

Note: 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



Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4GHz), EN301 489-17 EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:

http://support.netgear.com/app/answers/detail/a_id/11621

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	<i>NETGEAR Inc.</i> tímto prohlašuje, že tento Radiolan je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede <i>NETGEAR Inc.</i> erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erkläre <i>NETGEAR Inc.</i> , dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab <i>NETGEAR Inc.</i> seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, <i>NETGEAR Inc.</i> , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Wireless Cable Gateway CG3300CMR

Español [Spanish]	Por medio de la presente <i>NETGEAR Inc.</i> declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>NETGEAR Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente <i>NETGEAR Inc.</i> déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente <i>NETGEAR Inc.</i> dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>NETGEAR Inc.</i> deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>NETGEAR Inc.</i> deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart <i>NETGEAR Inc.</i> dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, <i>NETGEAR Inc.</i> , jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, <i>NETGEAR Inc.</i> nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym <i>NETGEAR Inc.</i> oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	<i>NETGEAR Inc.</i> declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	<i>NETGEAR Inc.</i> izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>NETGEAR Inc.</i> týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	<i>NETGEAR Inc.</i> vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar <i>NETGEAR Inc.</i> att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Wireless Cable Gateway CG3300CMR

Íslenska [Icelandic]	Hér með lýsir <i>NETGEAR Inc.</i> yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	<i>NETGEAR Inc.</i> erklærer herved at utstyret <i>Radiolan</i> er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

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 Wireless Cable Gateway CG3300CMR 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 market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Wireless Cable Gateway CG3300CMR) 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.

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.

Caution:

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.

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 table below 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

Index

A

- access, viewing logs [47](#)
- accessing remote computer [59](#)
- adding
 - custom services [64](#)
 - guest network [20](#)
- address reservation [31](#)
- advertisement period [71](#)
- alerts, emailing [38](#)
- attached devices [19](#)
- authentication, required by mail server [38](#)

B

- backing up configuration [49](#)
- basic settings [13](#)
- blocking
 - inbound traffic [59](#)
 - keywords [34](#)
 - services [35](#)
 - sites [34](#)

C

- cable channel [44](#)
- compliance [82](#)
- configuration file [49](#)
- configuring
 - DMZ server [27](#)
 - Dynamic DNS [69](#)
 - port forwarding [63](#)
 - port triggering [66](#)
 - user-defined services [35](#)
- CTS/RTS Threshold [54](#)
- custom service (port forwarding) [64](#)

D

- dashboard [12](#)
- data packets, fragmented [27](#)
- default DMZ server [27](#)
- default factory settings [50](#)
- deleting

- configuration [50](#)
- keywords [34](#)
- port forwarding entry [65](#)
- denial of service (DoS) protection [33](#)
- devices, attached [19](#)
- DHCP server [30](#)
- DMZ server [27](#)
- DNS servers [59](#)
- Domain Name Server (DNS) addresses [25](#)
- Dynamic DNS [68](#)

E

- email notices [38](#)
- erasing configuration [50](#)

F

- factory default settings, restoring [50](#)
- firewall settings [33](#)
- firmware version [42](#)
- fragmentation length [54](#)
- fragmented data packets [27](#)
- front panel [7](#)

G

- gateway front panel [7](#)
- gateway interface, described [12](#)
- gateway main menu [75](#)
- gateway rear panel [9](#)
- genie, NETGEAR, settings
 - advanced [22](#)
 - basic [15](#)
- guest networks [20](#), [46](#)

H

- host, trusted [35](#)

I

- inbound traffic, allowing or blocking [59](#)

Internet connection, setting up **24**
Internet Relay Chat (IRC) **60**
Internet services, blocking access **35**
IP addresses **11**
 auto-generated **76**
 dynamic **68**
 reserved **31**

K

keywords **34**

L

label, product **10**
LAN port settings **42**
LAN setup **28**
LEDs, troubleshooting using **75**
local servers, port forwarding to **63**
logging in **11**
logs
 emailing **38**
 viewing **47**

M

MAC addresses, product label **10**
mail server, outgoing **38**
maintenance settings **40**
menus, described **12, 13**
mixed mode security options **21**
MTU size **27**

N

NAT (Network Address Translation) **27, 59**
NETGEAR genie settings
 advanced **22**
 basic, initial **15**
networks, guest **20, 46**

O

outgoing mail server **38**

P

packets, fragmented **27**
passphrases
 changing **18**
 product label **10**
ping utility **76**

port filtering **35**
port forwarding **59, 61, 63**
port numbers **35**
port triggering **59, 60, 63, 66**
Preamble mode **54**
preset security
 about **16**
 passphrase **18**

R

radio, wireless **53**
reserved IP addresses **31**
restoring configuration file **49**
router interface, described **12**
router status, viewing **41**

S

security options **21**
security PIN **10**
sending logs by email **38**
serial number, product label **10**
services, blocking **35**
settings, default **79**
sites, blocking **34**
SMTP server **38**
specifications, technical **79**
SSID
 described **18, 53**
 product label **10**
status, router, viewing **41**

T

TCP/IP network, troubleshooting **76**
technical specifications **79, 80**
technical support **2**
Temporal Key Integrity Protocol (TKIP) **21**
time to live, advertisement **71**
time-out, port triggering **67**
trademarks **2**
troubleshooting **74**
 ISP connection **76**
 ping utility **76**
 TCP/IP network **76**
 using LEDs **75**
trusted host **35**

U

Universal Plug and Play (UPnP) **70**
user-defined services **35**

V

viewing
 logs **47**
 router status **41**

W

WAN setup **26**
wireless channel **18**
wireless mode **18**
wireless network name (SSID)
 broadcasting **18**
 described **18, 53**
 product label **10**
wireless network settings **18, 53**
wireless radio **53**
wireless security options **21**
wireless settings **16, 18**
WPA encryption **21**
WPA2 encryption **21**
WPA2-PSK encryption **21**
WPA-PSK + WPA2-PSK encryption **21**
WPA-PSK encryption **21**
WPA-PSK/WPA2-PSK mixed mode **21**
WPS button **8**