

NETGEAR®

Wireless Cable Gateway CG3000D-1CXNAS User Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

May 2010
202-10666-01
v1.0

© 2010 by 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.

P/N: Part Number TBD v1.0

Technical Support

When you register your product at <http://www.netgear.com/register>, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, Inc.

350 East Plumeria Drive
San Jose, CA 95134 USA

E-mail: support@netgear.com

Website: <http://www.netgear.com>

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

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.

Revision History

Publication Part Number	Version	Publish Date
202-10666-01	v1.0	May 2010

Table of Contents

Chapter 1 Connecting to the Internet

Gateway Front Panel	6
Gateway Rear Panel	7
Logging Into Your Gateway	7
Viewing the Basic Settings	9

Chapter 2 Wireless Configuration

Setting Up Your Wireless Network	10
Manually Configuring Wireless Settings	11
WPA or WPA2 Wireless Security	11
WEP Security	12
Using Push 'N' Connect (WPS) Wireless Setup	13
Using the WPS Button	14
Using a PIN	15
Wi-Fi Multimedia	16
Advanced Wireless Settings	17
Start Configure Button	18
Access Control by MAC Address	18

Chapter 3 Managing Your Network

Viewing the Gateway Status	21
Viewing the Connection Status	22
Changing Passwords	22
Backing Up and Restoring Your Settings	23
Viewing the Event Log	24
Running the Diagnostic Ping Utility	25

Chapter 4 Advanced Settings

MAC Filtering	27
IP Filtering	28
Port Blocking	29
Port Forwarding	30
Considerations for Port Forwarding	31
Port Triggering	31
DMZ Host	32
LAN IP Setup	33
Reserving an IP Address for DHCP Use	34

Remote Management34
Configuring Universal Plug and Play (UPnP)36

Chapter 5 Troubleshooting

Basic Functions38
 Using LEDs to Troubleshoot.39
Connecting to the Gateway’s Main Menu39
Troubleshooting the ISP Connection40
Troubleshooting a TCP/IP Network Using a Ping Utility40
 Testing the LAN Path to Your Gateway41
 Testing the Path from Your PC to a Remote Device41
Wireless Performance and Gateway Location42

Appendix A Default Settings and Technical Specifications

Factory Default Settings43
Technical Specifications45

Appendix B Related Documents

Appendix C Notification of Compliance

Index

Connecting to the Internet

1

For help installing the gateway, see the *Wireless Cable Gateway CG3000D-1CXNAS Quick Install Guide*.

This chapter describes how to configure your gateway's Internet connection and includes these sections:

- “*Gateway Front Panel*” on page 6.
- “*Gateway Rear Panel*” on page 7.
- “*Logging Into Your Gateway*” on page 7.
- “*Viewing the Basic Settings*” on page 9.

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








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.

Gateway Front Panel



Figure 1 Gateway front view

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

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: One or more downstream channels is locked. • Blinking: The unit is scanning for a downstream channel. • Off: No downstream channel is locked.
 Upstream	<ul style="list-style-type: none"> • Green: One or more upstream channels is locked. • 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 cable provider's CMTS. • 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
 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>
 WPS	<p>Pushing this button opens a 2-minute window for the gateway to connect with other WPS-enabled devices. For more information, about using the WPS method to implement security, see the "Using Push 'N' Connect (WPS) Wireless Setup" on page 13</p>

Gateway Rear Panel

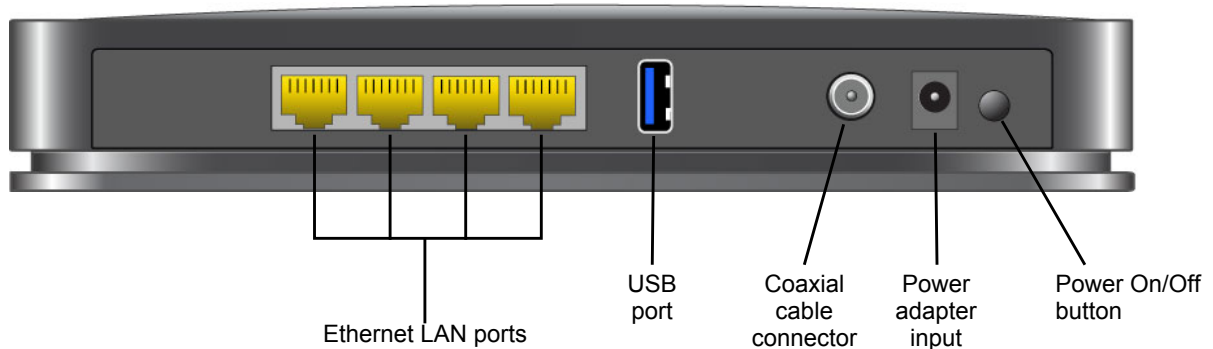



Figure 2 Gateway rear panel

The rear panel includes the following connections, viewed from left to right:

- **Four Gigabit-Ethernet LAN ports:** Use these ports to connect local computers.
- **USB port:** The USB port is a USB host and can be used for connecting a USB hard drive, flash drive, or printer.
- **Coaxial cable connector:** Attach coaxial cable to the cable service provider's connection.
- **Power:** Power adapter input.
- Power On/Off button.

Note: You can return the gateway to its factory settings. On the bottom of the gateway, 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](#)” in [Appendix A](#).”

Logging Into Your Gateway

You can log in to the gateway to view or change its settings. Links to Knowledge Base and documentation are also available on the gateway main menu.

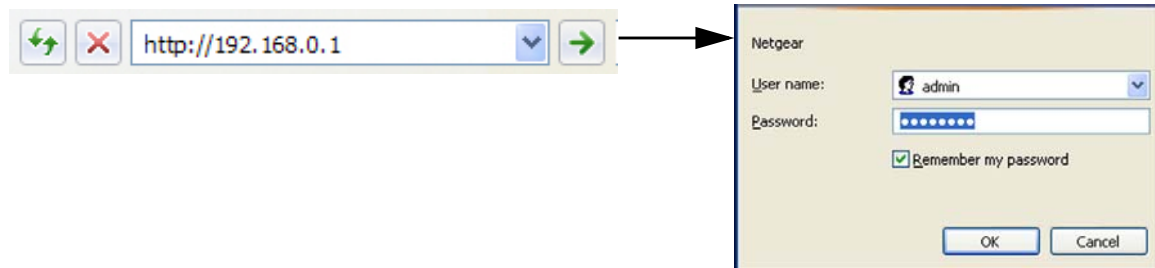
Note: To connect to the gateway you must use a computer configured for DHCP (most computers are). For help with configuring DHCP, see the instructions that came with your computer or see the link to the online document in “[Preparing a Computer for Network Access](#)” in [Appendix B](#).”

When you have logged in, if you do not click **Logout**, the gateway waits for 5 minutes after no activity before it automatically logs you out.

To log in to the gateway:

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

A login window opens.



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

When you connect to the gateway the Gateway Status screen displays.

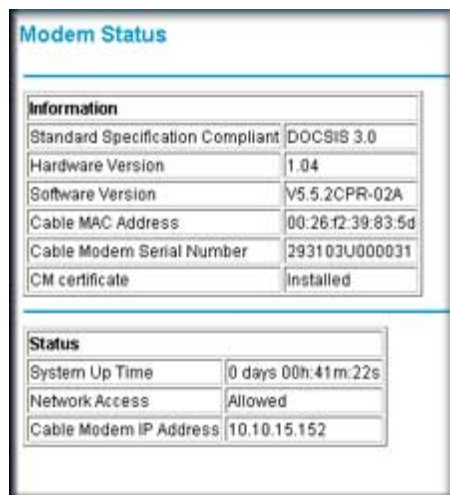


Figure 3 Gateway Status screen

To view the gateway's settings for the Internet connection, see the following section, [“Viewing the Basic Settings”](#) on page 9.

Viewing the Basic Settings

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

To view or configure the basic settings:

1. Select Basic Settings from the main menu.

2. You can fill in the **Domain Name** and **Device Name** fields.
 - By default, the **Dynamic IP** radio button is selected. This allows the gateway to download network configuration from your ISP.
 - Select **Static IP** only if your ISP has assigned you a permanent, fixed (static) IP address.
3. If you select Static IP, more fields appear on the screen. Fill in these fields so the gateway can connect to the Internet:
 - **Static IP Address.** The fixed IP address that your ISP has assigned to you.
 - **Static IP Mask.** The network number portion of an IP address. Unless you are implementing subnetting, use 255.255.0.0 as the subnet mask.
 - **Primary DNS.** A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your Gateway during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the Gateway.
 - **Secondary DNS.** If applicable, enter the address of your ISP's secondary DNS server.
4. If you made changes, click **Apply** so that the changes take effect.

2 Wireless Configuration

2

Note: Before changing wireless settings, connect the gateway and set up its Internet connection as described in the *Wireless Cable Gateway CG3000D-1CXNAS Quick Install Guide*.

This chapter includes:

- [Setting Up Your Wireless Network](#).
- [“Manually Configuring Wireless Settings”](#) on page 11.
- [“Using Push 'N' Connect \(WPS\) Wireless Setup”](#) on page 13.
- [“Wi-Fi Multimedia”](#) on page 16.
- [“Advanced Wireless Settings”](#) on page 17.

For more information about wireless technology, also see the link to the online document [“Wireless Communications”](#) in Appendix B.

Setting Up Your Wireless Network

To set up the wireless network, you can enter wireless settings, (see [“Manually Configuring Wireless Settings”](#) on page 11) or you can use Wi-Fi Protected Setup (WPS), described in [“Using Push 'N' Connect \(WPS\) Wireless Setup”](#) on page 13. To wirelessly connect to the gateway, a computer or wireless device must be configured with the same wireless settings as the gateway.

- The default wireless network name (SSID) for the gateway is Wireless. NETGEAR recommends that you change this for better wireless security and to make it easier to recognize your network when you want to connect to it wirelessly.
- By default the gateway works with WPA and WPA 2 wireless security. The default passphrase is the last 6 digits of the Wi-Fi MAC address.
- To use Push 'N' Connect (WPS), your wireless computers and equipment must support WPS technology. See [“Using Push 'N' Connect \(WPS\) Wireless Setup”](#) on page 13.

Manually Configuring Wireless Settings

You can manually configure the wireless settings and security for your gateway from the Wireless Settings screen.

To view or configure the wireless settings:

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

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

2. Log in to the gateway as described in *“Logging Into Your Gateway”* on page 7.
3. In the main menu, under Setup, select Wireless Settings to display this screen.
4. Specify the Wireless Network settings.
 - **Name (SSID):** The name of the wireless network.
 - **Region:** The location where the gateway will operate.
 - **Channel:** The available channels depend on the region. Some countries have laws specifying which channels should be used.
 - **802.11 Mode:** This is set to Up to 145 Mbps by default. You can specify the mode to support faster equipment or legacy equipment.
5. For help with Security Options, see the following sections
6. If you made changes, click **Apply** so that they take effect.

WPA or WPA2 Wireless Security

By default the gateway is set up to work with both WPA and WPA2 wireless security. (This security option is already selected.) You can specify the Network Key, which works like a password to access the wireless network.

To set up WPA or WPA2 wireless security:

- In the Security Options section of the Wireless Settings screen, leave the default setting or select one of the WPA settings:
 - WPA-PSK.** This setting provides the TKIP encryption type and a pre-shared key passphrase.
 - WPA2-PSK.** This setting provides the AES encryption type and a pre-shared key passphrase.
- Depending on the WPA settings that you select, enter the required information.

For WPA-PSK or WPA2-PSK, enter the pre-shared key, which is a passphrase between 8 and 63 characters. The default WPA passphrase is the 13-character serial number of your gateway.

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

Note: If you plan to use WPS, and you want to keep your wireless settings the same, go to the Advance Wireless Settings screen and make sure that the **Keep Existing Settings** checkbox is selected. See [“Advanced Wireless Settings”](#) on page 17.

- Configure your wireless computers with the same WPA2 or WPA settings as your gateway so that you will be able to connect.

WEP Security

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

To set up WEP wireless security:

1. In the Wireless Settings screen, select the **WEP** radio button in the Security Options section.
2. Select the Authentication from the drop-down list. The default is **Automatic**.
3. Depending on the encryption strength that you want, select one of these **WEP Encryption** options:
 - 64-bit encryption
 - 128-bit encryption
4. Enter a Passphrase (recommended) or WEP Keys:
 - To use a passphrase and generate keys, enter a passphrase and click **Generate**.
 - To enter the keys, fill in the **Key 1** through **Key 4** fields. Write down the keys and keep them in a secure location.
 - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9 or A–F). For 128-bit WEP, enter 26 hexadecimal digits.
 - Select which key will be the default, which will be used to encrypt data transmissions. The other keys can only be used to decrypt received data.
5. Click **Apply** to save your settings.
6. Configure your wireless computers with the same WEP settings as your gateway so that you will be able to connect. If you entered the keys, you will need to type them exactly as you did when you set up the gateway.

WEP

Authentication: Automatic

Encryption (WEP) Key:

WEP Encryption: WEP (64-bit)

WEP PassPhrase:


Key 1 1111111111


Key 2 1111111111

Key 3 1111111111

Key 4 1111111111

Using Push 'N' Connect (WPS) Wireless Setup

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

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

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

There are two Push 'N' Connect methods, Push Button and PIN (personal identification number).

- **Push Button.** This is the preferred method. See the following section, [Using the WPS Button](#).
- **PIN.** See [“Using a PIN”](#) on page 15.

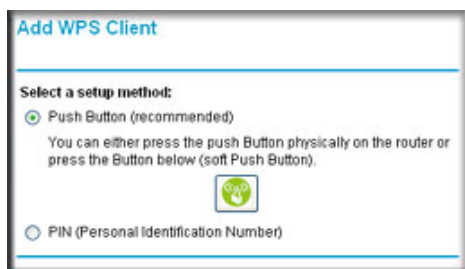
Using the WPS Button

You can use the WPS button to automatically set up wireless settings in your gateway and to set up your wireless computer to connect to it.



Note: The first time you use WPS it will assign a random network name (SSID) and a random passphrase to your wireless network. If you want to keep the network name and passphrase you specified in the Wireless Settings screen, you must select the **Keep Wireless Settings** checkbox in the Advanced Wireless Settings screen. See [“Advanced Wireless Settings”](#) on page 17.

To use the WPS button:

1. First, make sure you know how WPS works on your computer or wireless device. If it works with WPS, it has a WPS utility and might also have a WPS button that you can press.
2. Log in to the gateway as described in [“Logging Into Your Gateway”](#) on page 7.
3. In the main menu, select WPS Settings, and then click **Next**. The Add WPS Client screen displays:



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

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

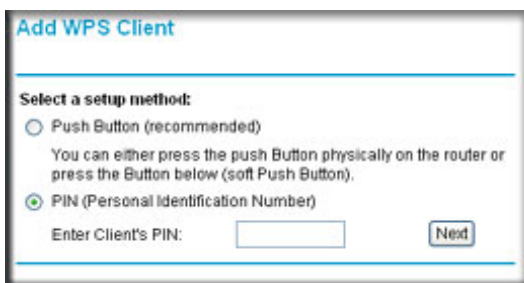


- The WPS LED on the front of the gateway begins to blink.
 - The gateway tries to communicate with the wireless computer or device for 2 minutes.
 - If the Security Option in the Wireless Settings screen was set to Disabled, it is automatically changed to WPA-PSK [TKIP] + WPA2-PSK [AES] including a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

When the computer connects to the wireless network, the gateway sends its SSID and WPA-PSK or WPA2-PSK configuration to that computer.
 6. On the computer that just joined the wireless network, make sure you can connect to the Internet. You should see the gateway's Internet LED blink, showing that its Internet connection is in use.

Using a PIN

1. First, make sure you know how WPS works on your computer or wireless device. If it works with WPS, it has a WPS utility. Use this utility to determine the PIN for your wireless computer or device.
2. Log in to the gateway as described in *“Logging Into Your Gateway”* on page 7.
3. In the main menu, select WPS Settings. The Add WPS Client screen displays.



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

4. Select the **PIN** radio button.
5. Type the PIN that you located in Step 1 in the **Enter Client's PIN** field, and then click **Next**.
 - The WPS LED on the front of the gateway begins to blink.

- The gateway tries to communicate with the wireless computer or device for 4 minutes.
- If the Security Option in the Wireless Settings screen was set to Disabled, it is automatically changed to WPA-PSK (including a PSK security password).

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

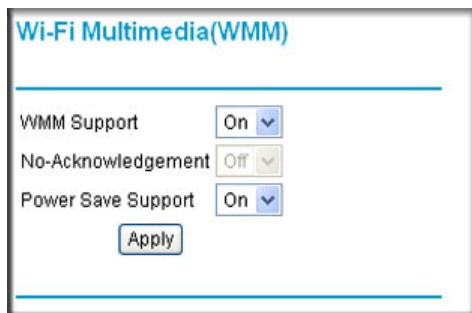
6. On the computer that just joined the wireless network, make sure you can connect to the Internet. You should see the gateway's Internet LED blink, showing that its Internet connection is in use.

Wi-Fi Multimedia

You can use the Multimedia page to set up wireless multimedia Quality of Service (QoS).

To set up Wi-Fi Multimedia:

1. Log in to the gateway as described in *"Logging Into Your Gateway"* on page 7.
2. In the main menu, under Setup, select Wi-Fi Multimedia.



3. In the **WMM Support** field, select **On** to enable WMM.
4. In the **No-Acknowledgement** field, select **Off** or **On** to specify whether acknowledgement (ACK) messages are used.

Usually, this field is set to **Off**. This might improve the efficiency of packet transmission. If wireless communication quality is poor at your location (this could happen if there is a lot of interference), set this field to **On** so that you are notified when a package is lost.

5. To conserve battery power in smaller devices that are connected to the gateway, set the **Power Save Support** field to **On**.
6. Click Apply to save your settings.

Advanced Wireless Settings

You can use the Advanced Wireless Settings screen to configure the wireless radio settings, and other advanced settings:

The following table describes the fields in the Advanced Wireless Settings screen.

Advanced Wireless Settings		Description
Wireless Access Point (Enhanced Feature)	Enable Wireless Access Point	By default this checkbox is selected so that the gateway works as a wireless access point. You can turn off the wireless radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
Advanced Configuration	<ul style="list-style-type: none"> Fragmentation Threshold CTS/RTS Threshold Preamble Mode 	The default settings for these fields usually work fine. Change them only if you have a specific reason for doing so.
WPS Settings	Disable Router's PIN	Selecting this checkbox disables the PIN that WPS clients use to connect to the gateway with the PIN method. Normally this checkbox is cleared, which is the default setting.
	Keep Existing Settings	If a WPS client is added the gateway automatically selects this checkbox. When the Keep Existing Settings checkbox is selected, the SSID and wireless security settings remain the same when additional WPS clients are added.
Wireless Card Access List	Set up Access List	Access control is disabled by default so that any computer that is configured with the correct SSID can connect. For information about access control, see the following section.

Start Configure Button

This button can be used to start WPS configuration.

Note: The first time you use WPS it will assign a random network name (SSID) and a random passphrase to your wireless network. If you want to keep the network name and passphrase you specified in the Wireless Settings screen, you must select the **Keep Wireless Settings** checkbox.

1. Click the **Start Configure** button.



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

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

On the computer that just joined the wireless network, make sure you can connect to the Internet. You should see the gateway's Internet LED blink, showing that its Internet connection is in use.

Access Control by MAC Address

You can use access control to specify which wireless computers or devices can connect to the gateway based on their MAC addresses. If you do not set up access control, any wireless computer or device that is configured with the correct SSID and wireless security settings will be allowed to access to your wireless network.

To control access based on MAC addresses:

1. Log in to the gateway as described in *"Logging Into Your Gateway"* on page 7.
2. In the main menu, under Advanced, select Wireless Settings.

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

The screenshot shows the 'Wireless Card Access List' configuration interface. On the left, a smaller window titled 'Wireless Card Access List' contains a 'Setup Access List' button. An arrow points from this button to the main configuration window. The main window is titled 'Wireless Card Access List' and contains the following sections:

- Network Profiles:** A table with columns for a selection icon and 'SSID'. The entry 'CG3000D58' is selected with a green circle.
- Access Control:** Three radio buttons: AllowAny, AllowList, and DenyList.
- Access List:** A table with a header '# | MAC Address' and a 'Delete' button below it.
- Connected Wireless Devices:** A table with headers 'Device Name', 'IP Address', 'MAC Address', and 'Interface'.
- Add Access Filter:** A section with a 'MAC Address' label and a form with six input fields separated by colons, followed by an 'Add' button.

Note: If you are configuring the gateway from a wireless computer, make sure to add your computer's MAC address to the Access List. Otherwise you will lose your wireless connection when you click Apply. You must then access the gateway from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

- In the Network Profiles section, select the radio button for a wireless network.
- By default the **Allow Any** radio button is selected. You can either allow computers to connect to the network based on their MAC addresses, or deny connections based on MAC address. Select either the **Allow List** or **Deny List** radio button.
- Add devices to the Access List using either of these methods:
 - If the computer is in the Connected Wireless Devices table, click its radio button to capture its MAC address. Then click **Add**.
 - Enter the MAC address of the device in the **Add Access Filter** fields. The MAC address can usually be found on the bottom of the wireless device. Then click **Add**.
- Click **Apply** to save these settings.

Managing Your Network

3

This chapter describes how to perform network management tasks with your gateway. When you log in to the gateway (see *“Logging Into Your Gateway”* on page 7), these tasks are grouped under Maintenance.

This chapter includes:

- Viewing the Gateway Status.
- *“Viewing the Connection Status”* on page 22.
- *“Changing Passwords”* on page 22.
- *“Backing Up and Restoring Your Settings”* on page 23.
- *“Viewing the Event Log”* on page 24.
- *“Running the Diagnostic Ping Utility”* on page 25.

Viewing the Gateway Status

Use the Modem Status screen to see hardware and firmware details about the gateway and basic status information. In the main menu, under Maintenance, select Gateway Status.



The screenshot shows a web interface titled "Modem Status". It contains two main sections: "Information" and "Status".

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.04
Software Version	V5.5.2CPR-02A
Cable MAC Address	00:26:12:39:83:5d
Cable Modem Serial Number	293103U000031
CM certificate	Installed

Status	
System Up Time	0 days 00h:41m:22s
Network Access	Allowed
Cable Modem IP Address	10.10.15.152

The following table describes the fields displayed in this screen

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

Viewing the Connection Status

To view this screen, from Gateway Status screen, click the **Connection Status** button.

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	591000000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	
Security	Enabled	BPI+

Downstream Bonded Channels							
Lock Status	Modulation	Channel ID	Symbol rate	Frequency	Power	SNR	Docsis/EuroDocsis locked
Locked	QAM256	17	5360537 sym/sec	591000000 Hz	1.5 dBmV	41.7 dBmV	Docsis
Locked	QAM256	11	5360537 sym/sec	555000000 Hz	1.6 dBmV	41.3 dBmV	Docsis
Locked	QAM256	12	5360537 sym/sec	561000000 Hz	1.7 dBmV	40.5 dBmV	Docsis
Locked	QAM256	13	5360537 sym/sec	567000000 Hz	1.7 dBmV	40.4 dBmV	Docsis
Locked	QAM256	14	5360537 sym/sec	573000000 Hz	2.2 dBmV	41.0 dBmV	Docsis
Locked	QAM256	15	5360537 sym/sec	579000000 Hz	2.1 dBmV	42.5 dBmV	Docsis
Locked	QAM256	16	5360537 sym/sec	585000000 Hz	1.8 dBmV	42.1 dBmV	Docsis
Locked	QAM256	10	5360537 sym/sec	549000000 Hz	2.0 dBmV	41.1 dBmV	Docsis

Upstream Bonded Channels					
Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power
Locked	ATDMA	10	5120 Ksym/sec	18000000 Hz	50.7 dBmV
Locked	ATDMA	11	5120 Ksym/sec	24400000 Hz	50.7 dBmV
Locked	ATDMA	12	5120 Ksym/sec	30800000 Hz	50.7 dBmV
Locked	ATDMA	13	5120 Ksym/sec	37200000 Hz	50.7 dBmV

Current System Time: Thu Apr 29 00:53:40 2010

Use the Connection screen to track the gateway's initialization procedure, 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:

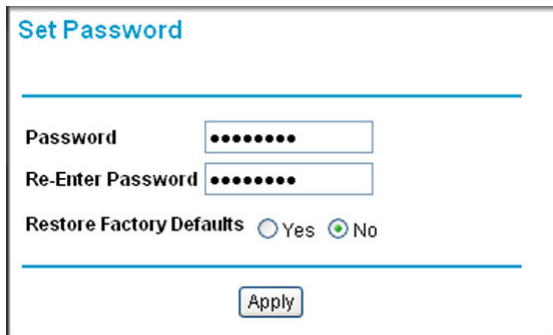
- Scan and lock the downstream frequency, and then link back in upstream direction.
- Obtain an IP address for the gateway itself. Then the gateway assigns an IP address for the connected PC.
- Connect to the Internet.

Changing Passwords

For security reasons, the gateway has its own user names and passwords. NETGEAR recommends that you change the default passwords to more secure passwords. The ideal passwords should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your passwords can be up to 30 characters.

To change the password:

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



The screenshot shows a web page titled "Set Password". It features two input fields for "Password" and "Re-Enter Password", both containing masked characters. Below these fields is a "Restore Factory Defaults" section with radio buttons for "Yes" and "No", where "No" is selected. At the bottom of the form is an "Apply" button.

2. To change the password, enter the new password twice.
3. Click **Apply** to save your changes.

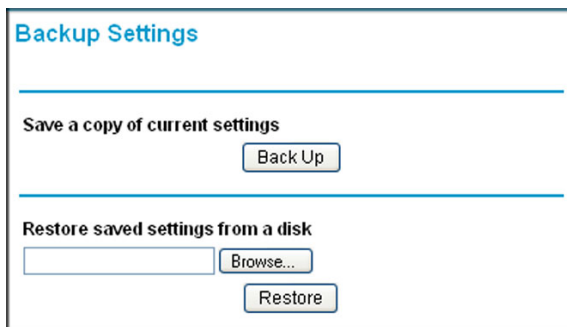
Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the gateway settings previously, you should do a new backup so that the saved settings file includes the new password.

Backing Up and Restoring Your Settings

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

To save or restore the backup settings:

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



The screenshot shows a web page titled "Backup Settings". It has two main sections. The first section is "Save a copy of current settings" with a "Back Up" button. The second section is "Restore saved settings from a disk" which includes a text input field, a "Browse..." button, and a "Restore" button.

2. You can save the current configuration settings or restore saved settings:
 - To save the current configuration settings, click **Back Up**.

- To restore the saved configuration settings from a backup file, click **Browse**, locate and select the previously saved backup file. Then click **Restore**.

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

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

Viewing the Event Log

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

To see the event log:

- In the main menu, under Maintenance, select Event Log.

The screenshot shows the 'Logs' page with configuration fields and a table of event logs.

Configuration fields:

- Contact Email Address:
- SMTP Server Name:
- E-mail Alerts: Enable
- Apply button

Description	Count	Last Occurrence	Target	Source
TCP- or UDP-based Port Scan	1	Thu Apr 08 23:49:28 2010	192.168.15.72:16453	172.29.16.12:53
SYN Flood	11	Fri Apr 09 22:44:37 2010	172.29.16.20:21	192.168.0.13:43521
Illegal TCP header	1	Thu Apr 15 00:01:26 2010	192.168.0.13:0	216.252.124.30:0
TCP- or UDP-based Port Scan	2	Thu Apr 15 00:07:54 2010	192.168.15.72:17142	172.29.16.12:53
SYN Flood	1	Thu Apr 15 00:09:33 2010	192.168.0.13:49810	205.209.143.101:80
TCP- or UDP-based Port Scan	7	Mon Apr 19 22:22:13 2010	192.168.15.72:41720	172.29.16.12:53

Buttons at the bottom: E-mail Log, Clear Log, REFRESH

- To clear the log, click **Clear Log**; to refresh the log, click **Refresh**.

Running the Diagnostic Ping Utility

From the Diagnostics screen you can use Ping.

To use diagnostics:

1. Log in to the gateway as described in *“Logging Into Your Gateway”* on page 7.
2. In the main menu, under Maintenance, select Diagnostics.

The screenshot shows the 'Diagnostics' screen with the 'Ping' utility selected. The 'Ping Test Parameters' section includes the following fields:

- Target: 192.168.0.1
- Ping Size: 64 bytes
- No. of Pings: 3
- Ping Interval: 1000 ms

Buttons for 'Start Test', 'Abort Test', and 'Clear Results' are visible. Below the parameters is a 'Results' section containing the text 'Waiting for input...'.

3. To start a ping test, enter the IP address in the Diagnostics screen, and click the **Ping** button. The Ping Results are displayed:

The screenshot shows the 'Diagnostics - Ping' screen with the following output:

```

Ping Results
PING 192.168.0.2 (192.168.0.2): 56 data bytes
64 bytes from 192.168.0.2: icmp_seq=0 ttl=128 time=0.0 ms
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=0.0 ms

--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
  
```

A 'Back' button is located at the bottom of the screen.

4. To return to the Diagnostics screen and stop the test, click **Back** and then click **Abort Test**.

4 Advanced Settings

4

This chapter describes how to customize your network through the advanced settings on your gateway. When you log in to the gateway (see *“Logging Into Your Gateway”* on page 7), these tasks are grouped under Advanced.

This chapter includes:

- *“MAC Filtering”* on page 27.
- *“IP Filtering”* on page 28.
- *“Port Blocking”* on page 29.
- *“Port Forwarding”* on page 30.
- *“Port Triggering”* on page 31.
- *“DMZ Host”* on page 32.
- *“LAN IP Setup”* on page 33.
- *“Remote Management”* on page 34.
- *“Configuring Universal Plug and Play (UPnP)”* on page 36.

Note: For information about advanced wireless settings, see *“Advanced Wireless Settings”* on page 17.

MAC Filtering

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

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

- In the main menu, under Advanced, select MAC Filtering.
The Trusted Devices table shows computers that have access to the Internet through the gateway. Click **Refresh** to update the Trusted Devices table.

- In the Add MAC Filter table, you can use either of these methods to specify computers to block:
 - If the computer is in the Trusted Devices table, click its radio button. The MAC address will be added into the Add MAC Filter table.
 - Fill in the **Device Name** and **MAC address fields**.

- Click **Add**.

The MAC Filter List **Enable** checkbox is automatically selected for that computer.

- Select the days and times to block the computer:
 - Day(s) to Block.** Select the days to block the computer selected in the **MAC Filter List**. The default is Everyday.
 - Time of Day to Block.** You can specify the time of day to block the computer. The default is All Day. Be sure that you clear the **All Day** checkbox if you want to enter specific times. The selected period applies to each day that you selected.
- Click **Apply** to save your settings.
- Repeat these steps for all computers that you want to block.

To stop blocking a computer:

- To stop blocking a computer, select it from the **MAC Filter List** field, and then clear its **Enable** check box. This leaves the computer in the list but ensures that it is not blocked.
- To remove a computer from the list, select it from the **MAC Filter List** field, and then click **Delete**.

IP Filtering

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

To set up IP filtering:

- In the main menu, under Advanced, select IP Filtering.
 - The Trusted Devices table shows computer that are allowed access to the Internet through your gateway.
 - You can click **Refresh** to update the Trusted Devices.
- Add device to the IP Filter List as needed:
 - If the computer is in the Trusted Devices table, click its radio button to capture its IP address; or enter the IP address of the computer you want to block.
 - If no device name appears, you can type a name for the computer you are adding.
- When you have finished entering the IP address click **Add**.

The screenshot shows the 'IP Filtering' configuration interface. It includes a 'Trusted Devices' table with columns for Device Name, IP Address, MAC Address, and Interface. Below this is an 'Add IP Filter' section with input fields for Device Name and IP Address, and 'Add' and 'Cancel' buttons. The 'IP Filter List' section shows a dropdown menu with 'No filters entered.', an 'Enable' checkbox, and a 'Delete' button. The 'Day(s) to Block' section has checkboxes for Everyday, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The 'Time of Day to Block' section has an 'All day' checkbox and 'Start' and 'End' time pickers. An 'Apply' button is located at the bottom of the form.

To delete a device from the IP Filtering List, select it, and then click **Delete**.

- Select the Day(s) to Block.
- In the Time of Day to Block, choose a Start time and an End time. This time range will apply to each day you selected in Day(s) to Block for the specific computer. All day is the default value for specific computers.
- When you have finished configuration, click **Apply** to activate the settings.

Port Blocking

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

Note: Any outbound traffic that is not blocked by rules that you have created is allowed by the default rule.

To configure port blocking and services to block specific outbound traffic:

- In the main menu, under Advanced, select Port Blocking.
- In the **Services** field, select a service from the drop-down list. (For example, FTP, which uses TCP ports 20 and 21.)
- To add a custom rule that is not in the list of services, specify these settings in the Add Custom Rules table:
 - Name.** Enter a name for the service.
 - Start Port.** Enter the start port for the service.
 - End Port.** Enter the end port for the service.
 - Protocol.** Select the protocol for the ports:
 - TCP.** Select TCP only.
 - UDP.** Select UDP only.
 - Both.** Select both TCP and UDP.
 - Local IP Address.** Complete the local IP address for the computer that is using the service.
- Perform one of the following actions:
 - Click **Add** to save your settings. The Active Filters table now displays the list of ports that are currently forwarded.
 - To delete a service, select the radio button in the Active Filters table for the service that you want to delete, and then click **Delete**.
 - To reset the selection in the Services drop-down list and to clear all the fields in the Add Custom Rules table, click **Reset**.

Port Blocking

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

Add Predefined Service
Service:

Add Custom Service

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

Port Forwarding

A firewall has default rules for inbound traffic (WAN to LAN) and for outbound traffic. Port forwarding affects the inbound rules. These rules restrict access from outsiders. By default, the gateway blocks access from outside except responses to requests from the LAN side. You can use port forwarding to add rules to specify exceptions to the default rule.

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

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

To configure port forwarding and services for specific inbound traffic:

- In the main menu, under Advanced, select Port Forwarding.
- In the **Service** field, select a service from the drop-down list. (For example, FTP, which uses TCP ports 20 and 21.)
- To add a custom rule that is not in the list of services, specify these settings in the Add Custom Rules table:
 - Name.** Enter a name for the service.
 - Start Port.** Enter the start port for the service.
 - End Port.** Enter the end port for the service.
 - Protocol.** Select the protocol for the ports:
 - TCP.** Select TCP only.
 - UDP.** Select UDP only.
 - Both.** Select both TCP and UDP.
 - Local IP Address.** Complete the local IP address for the computer that is using the service.
- Perform one of these actions:
 - Click **Add**. The Active Forwarding Rules table displays the list of forwarded ports.
 - To delete a service, select the radio button in the Active Forwarding Rules table for the service that you want to delete, and then click **Delete**.
 - To reset the selection in the **Services** field and to clear all the fields in the Add Custom Rules table, click **Reset**.

Port Forwarding

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

Choose Predefined Service

Service:

Add Custom Rules

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

Considerations for Port Forwarding

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

Port Triggering

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

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

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

To configure port triggering:

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

2. For each port trigger, enter the settings in the Port Trigger List:
 - **Trigger Range.** To specify the range of outgoing ports that will be monitored to trigger the incoming port forwarding rule, enter the **Start Port** and **End Port**.
 - **Target Range.** To specify the range of incoming ports that will be opened when triggered, enter the **Start Port** and **End Port**.
 - **Protocol.** Select the protocol for the ports:
3. Select the **Enable** checkbox for the port trigger.
4. Perform one of the following actions:
 - Click **Apply** to save your settings and activate the port triggers.
 - To remove a port trigger, select its radio button and click **Delete**.
 - To return all trigger and target ranges to zero, click **Reset**.

Port Triggering

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

DMZ Host

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

To set up a DMZ host:

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

DMZ Host

Respond to Ping on WAN Port

DMZ Address 192.168.0 .

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

2. If desired, select the **Respond to Ping on WAN Port** checkbox.
3. Type the last digit(s) of the IP address in the **DMZ Address** field.
4. Click **Apply**.

LAN IP Setup

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

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

To configure LAN IP settings:

1. In the main menu, under Advanced, select LAN IP.
2. Specify these settings:

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

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

- **Starting IP Address and Ending IP Address:** These fields specify the range in the IP address pool.
- **Max Users:** The maximum number of users on the network.
- **DHCP Lease:** See the following section, [Reserving an IP Address for DHCP Use](#).

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

LAN IP

Device Name ---

LAN IP Address . . .

Subnet Mask 255.255.255.

DHCP Server Yes No

Starting IP Address 192.168.0.

Ending IP Address 192.168.0.

Max Users

Lease Time

DHCP Reservation Lease Info

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

DHCP Client Lease Info

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

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

Reserving an IP Address for DHCP Use

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

To reserve an IP address for DHCP:

1. Enter the MAC address of the computer for which you want to reserve an IP address.
2. Enter the permanent IP address for the computer.
3. Click **Add** to save your settings.

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

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

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

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

Remote Management

With remote management, you can allow a user or users on the Internet to configure, upgrade, and check the status of the gateway.

Note: Use very secure passwords if you enable remote management. Passwords should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 16 characters.

To manage this gateway through the Internet, you need its public IP Address, as seen from the Internet. This public IP address is allocated by your ISP. But if your ISP account uses a dynamic IP address, the address can change each time you connect to your ISP. There are two solutions to this problem:

- Have your ISP allocate you a fixed IP address.
- Use the DDNS (Dynamic DNS) feature so you can connect using a domain name, rather than an IP address.

To configure the gateway for remote management:

1. In the main menu, under Advanced, select Remote Management.
2. Select one of the **Allow Remote Management** checkboxes.
3. Fill in the **Remote User Name** and **Remote Password** fields.
4. Specify the port numbers to access the gateway remotely in your browser when you connect. To specify the port numbers:

- a. From a remote location, start a browser.
- b. In the Address or Location field, enter the Internet IP address of this gateway (NOT the LAN IP address), followed by a colon and the port number, as follows:

`http://ip_address:pn ||`
`https://ip_address:pn`

where:

ip_address is the Internet IP address of this gateway.

pn is the port number assigned on this screen.

- c. You will be prompted for the password for this gateway.
5. If you want the ability to reset to factory default settings remotely, and then log in again remotely, select the **Allow Remote management after Factory Default Reset** checkbox.
 6. Click **Apply** to save your changes.

Remote Management Settings	Description
Allow Remote Management (HTTP/HTTPS) CM interface	If selected, remote management is enabled, and connection from the Internet to this gateway with HTTP and HTTPS is possible. The correct port number must be used when connecting
Allow Remote Management (HTTP/HTTPS) WAN interface	If selected, remote management is enabled, and connection from the Internet to this gateway with HTTP and HTTPS is possible.
Remote User Name and Remote Password	Enter the User Name and Password that will be used from the remote PC to manage the gateway. Use a very secure password.
Port Number fields	Web browser access normally uses the standard HTTP service port 80. NETGEAR recommends that you use a different port number for remote management, as using port 80 will prevent the use of a Web Server on your LAN, and can be more readily discovered by hackers. Use the default (8080) or choose a port number between 1 and 65535.

Remote Management Settings (Continued)	Description (Continued)
Revert to factory default settings	Allow Remote management after Factory Default Reset
IP Address to connect this device	
Allow Management via Telnet Allow Management via SSH	You can select LAN interface (local management), CM Interface (remote management), or WAN Interface (remote management) in order to connect to the gateway from the Internet. The correct port number must be used when connecting

Configuring Universal Plug and Play (UPnP)

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

- **Advertisement Period.** This specifies how often the gateway broadcasts its UPnP information. The default is 30 minutes. Lower numbers ensure that control points have current device status at the expense of additional network traffic. Larger numbers may compromise the freshness of the device status but can significantly reduce network traffic.
- **Advertisement Time to Live.** The time to live for the advertisement, measured in hops (steps) for each UPnP packet that is sent. A hop is the number of steps that are 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 should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value slightly.

To configure UPnP:

1. In the main menu, under Advanced, select UPnP.
2. Select the **Turn UPnP On** check box. The default setting is disabled, which prevents the gateway from allowing any device to automatically control of its the resources, such as port forwarding.
3. Fill in the **Advertisement Period** and **Advertisement Time to Live** fields.

The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the gateway and which internal and external ports of the

gateway were opened by that device. The UPnP Portmap Table also displays the protocol for the port that was opened and if that port is still active for each IP address.

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

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

- Have I connected the gateway correctly?
Go to *“Basic Functions”* on page 38.
- I cannot access the gateway configuration with my browser.
Go to *“Connecting to the Gateway’s Main Menu”* on page 39.
- I have configured the gateway but I cannot access the Internet.
Go to *“Troubleshooting the ISP Connection”* on page 40.
- I cannot remember the gateway’s configuration password or I want to clear the configuration and start over again.
Go to *“Factory Default Settings”* in Appendix A.

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

Basic Functions

After you have turned on power to the gateway, you should 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 12VDC power adapter supplied by NETGEAR for this product.</p> <p>If the error persists, you have a hardware problem and should contact technical support.</p>
All LEDs Stay On	<ul style="list-style-type: none"> • Clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. See "Factory Default Settings" in Appendix A. • If the error persists, you might have a hardware problem and should 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 PC. • Make sure that power is turned on to the connected hub or PC. • Be sure 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 should verify that the signal quality is good enough for cable modem service. • Remove any excessive splitters you may have on your cable line. It may be necessary to run a "home run" back to the point where the cable enters your home.

Connecting to the Gateway's Main Menu

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

- Check the Ethernet connection between the computer and the gateway as described in the previous section.
- Make sure that your PC's IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.10 to 192.168.0.254. Refer to the link to the online document ["Internet Networking and TCP/IP Addressing" in Appendix B](#) for help configuring your computer.

Note: If your PC's IP address is shown as 169.254.x.x:
Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These

auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the gateway and reboot your PC.

- If your gateway's IP address has been changed and you don't know the current IP address, clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in "[Factory Default Settings](#)" in [Appendix A](#).
- Make sure 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 you are using the correct login information. The gateway user name **admin** is lower-case (**Caps Lock** should be 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 may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

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

Additionally, your PC may not have the gateway configured as its TCP/IP gateway. If your PC obtains its information from the gateway by DHCP, reboot the PC and verify the gateway address. See the link to the online document "[Internet Networking and TCP/IP Addressing](#)" in [Appendix B](#).

Troubleshooting 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. Troubleshooting a TCP/IP network is made easier by using the ping utility in your PC or workstation.

Testing 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 on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the gateway, as in this example:

ping 192.168.0.1

3. Click OK.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections.
 - Make sure the LAN port LED is on. If the LED is off, see [“Using LEDs to Troubleshoot”](#) on page 39.
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- Wrong network configuration.
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your gateway and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC 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 your ISP’s DNS server.

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

- Check that your PC has the IP address of your gateway listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway. See the link to the online document "[Internet Networking and TCP/IP Addressing](#)" in Appendix B.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your Cable Link LED is on.
- If your ISP assigned a host name to your PC, 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 significantly 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 will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- 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 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.


A Default Settings and Technical Specifications



This chapter includes:

- [Factory Default Settings](#)
- *“Technical Specifications”* on page 45

Factory Default Settings

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

Factory Default Settings		
Gateway Login	User login URL	http://192.168.0.1
	User name and password (case sensitive)	admin/password
Local Network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP Ending IP address	192.168.0.254
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the http port)
	Outbound communication to the Internet	Enabled (all)
	Source MAC filtering	Disabled

Factory Default Settings (Continued)		
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
Wireless	Wireless communication	Enabled
	SSID name	The last 3 octets of the Wi-Fi MAC address
	Security	WPA/WPA2 The default WPA/WPA2 passphrase is the 13-character serial number of the gateway.
	Broadcast SSID	Enabled
	Transmission speed	Auto ¹
	Country/region	United States (varies by region)
	RF channel	Auto
	Operating mode	n, g, and b
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless card access list	All wireless stations allowed

¹ Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput 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 pass through (IPSec, PPTP)
Power adapter	<ul style="list-style-type: none"> North America (input): 120V, 60 Hz, input All regions (output): 12 V DC @ 1.5A output 15W maximum
Physical specifications	<ul style="list-style-type: none"> Dimensions: 8.5 by 5.75 by 1.3 in (216 by 146 by 33 mm) Weight: 0.95 lb (0.42 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.
Interface	Local: 10BASE-T, 100/1000BASE-Tx, RJ-45 USB 2.0/1.1 function 802.11n/g/b
	Internet: DOCSIS 3.0. Downward compatible with DOCSIS 2.0, 1.1 and 1.0

B Related Documents

B

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Windows XP and Vista Wireless Configuration Utilities	http://documentation.netgear.com/reference/enu/winzerocfg/index.htm
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

Notification of Compliance



Certificate of the Manufacturer/Importer

It is hereby certified that the TBD has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das TBD gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

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.

Regulatory Compliance Information

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

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, EN301 489-17, EN60950

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at:
http://kb.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

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.
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.

EDOC in Languages of the European Community

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.
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.

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

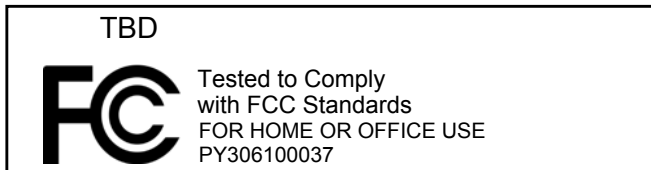
We, *NETGEAR, Inc.*, 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the model MS2110 TBD complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

- 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.



Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (TBD) 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.

Canada ID: 4054A-FVX538

Index

Numerics

192.168.0.1, default IP address [1-8](#)

B

backing up the configuration file [3-23](#)

Basic Settings [1-9](#)

blocking

PCs based on MAC address [4-27](#)

blocking ports [4-29](#)

C

cable channel [3-22](#)

configuration

backup [3-23](#)

erasing [3-23](#)

D

default gateway field (Basic Settings) [1-9](#)

DHCP [4-34](#)

reserved IP address [4-34](#)

server [4-33](#)

DMZ Host [4-32](#)

DNS primary and secondary server [1-9](#)

E

Erase configuration [3-23](#)

Event log [3-24](#)

F

firewall rules

inbound [4-30](#)

port forwarding [4-30](#)

front panel [1-6](#)

G

gateway

backup [3-23](#)

main menu [5-39](#)

placement and range guidelines [2-10](#)

remote management [4-34](#)

gateway front panel [1-6](#)

gateway rear panel [1-7](#)

I

IP address [1-8](#)

IP addresses, auto-generated [5-40](#)

L

LAN

IP address [4-33](#)

IP settings [4-33](#)

LEDs

troubleshooting [5-39](#)

logging in [1-7](#)

logging out [1-8](#)

logs [3-24](#)

M

MAC filtering [4-27](#)

Modem Status [3-21](#)

P

passphrase [2-13](#)

ping utility [5-40](#)

port blocking [4-29](#)

port forwarding [4-30](#), [4-31](#)

primary DNS server [1-9](#)

R

remote management [4-34](#)

S

secondary DNS server [1-9](#)

static IP address [1-9](#)

T

TCP/IP

network, troubleshooting **5-40**

technical specifications **A-45**

troubleshooting **5-38**

ISP connection **5-40**

LEDs **5-39**

ping utility **5-40**

TCP/IP network **5-40**

U

Universal Plug and Play (UPnP) **4-36**

W

WEP **2-13**

keys **2-13**

passphrase **2-13**

Wi-Fi Protected Setup (WPS)

Push 'N' Connect **2-17**

wireless

access point **2-17**

card access list **2-17**

manually configuring settings **2-11**

wireless network

planning **2-10**

wireless security **2-16**

Wireless Security Options **2-10**

WPA **2-12**

WPA2 **2-12**

WPA2-PSK **2-12**

WPA-PSK **2-12**

WPS **2-14**

WPS button **1-6**

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>