

# NETGEAR®

---

## Wireless Cable Gateway CG3000

### User Manual



350 East Plumeria Drive  
San Jose, CA 95134  
USA

April 2011  
202-10842-01  
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](mailto: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.

# Table of Contents

## Chapter 1 Connect to the Internet

Gateway Front Panel .....	6
Gateway Rear Panel .....	7
Install the Voice Gateway .....	7
Check the Installation Requirements .....	8
Cable the Gateway .....	8
Log In to Your Gateway .....	9
Connect to the Internet and VoIP .....	10
View the Gateway Status .....	10

## Chapter 2 Wireless Configuration

Set Up Your Wireless Network .....	12
Manually Configure The Wireless Settings .....	12
WPA or WPA2 Wireless Security .....	13
WEP Security .....	15
Push 'N' Connect (WPS) Wireless Setup .....	16
WPS Button .....	16
PIN .....	17

## Chapter 3 Content Filtering

View or Email Logs .....	19
Block Keywords, Sites, and Services .....	19
Block Keywords and Domains .....	20
Services .....	21

## Chapter 4 Manage Your Network

Gateway Status .....	23
MTA Status .....	24
Signal Status .....	25
Change Password .....	26
Back Up and Restore Your Settings .....	26
Event Log .....	27
Diagnostic Ping Utility .....	27

## Chapter 5 Advanced Settings

Wireless Settings .....	30
Access Control by MAC Address .....	31

Firewall Rules: Port Blocking . . . . .	32
Firewall Rules: Port Forwarding . . . . .	33
Considerations for Port Forwarding . . . . .	34
WAN Setup. . . . .	34
Assign a Computer as The DMZ Host . . . . .	35
Remove a Computer from Being a DMZ Computer: . . . . .	35
Dynamic DNS. . . . .	35
LAN IP Setup . . . . .	36
Reserving an IP Address for DHCP Use . . . . .	37
Remote Management. . . . .	38
Universal Plug and Play (UPnP) . . . . .	40

## **Chapter 6 Troubleshooting**

Basic Functions . . . . .	42
Using LEDs to Troubleshoot. . . . .	42
Access the Gateway Configuration . . . . .	43
Troubleshoot the ISP Connection . . . . .	44
Troubleshoot a TCP/IP Network Using a Ping Utility . . . . .	44
Test the LAN Path to Your Gateway . . . . .	44
Test the Path from Your PC to a Remote Device. . . . .	45
Wireless Performance and Gateway Location . . . . .	45

## **Appendix A Technical Specifications**

Factory Default Settings. . . . .	47
Technical Specifications. . . . .	49

## **Appendix B Notification of Compliance**

## **Index**

# Connect to the Internet

---

# 1

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.
- *Log In to Your Gateway* on page 9.
- *View the Gateway Status* on page 10.

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

For information about the topics covered in this manual, visit the Support website at <http://support.netgear.com>.

For help installing the gateway, see the *Wireless Cable Gateway CG3000 Quick Install Guide*.

---

**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

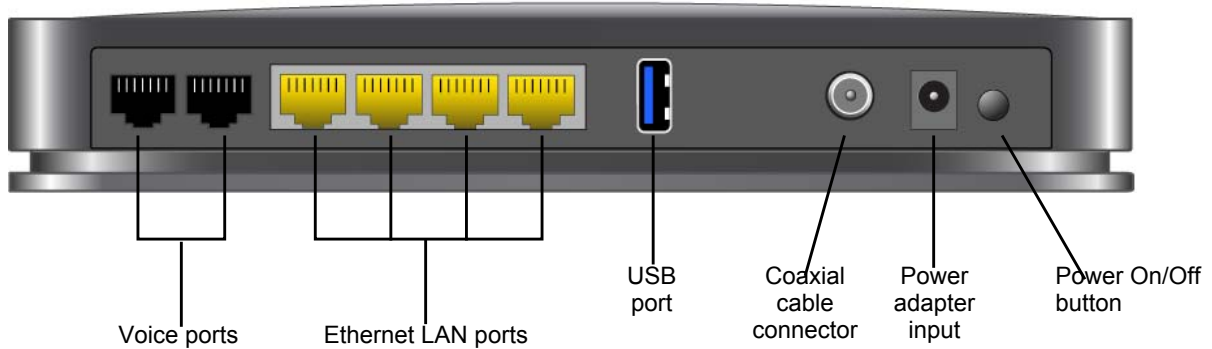


**Figure 1. Gateway front view**

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"> <li>• <b>Green.</b> Power is supplied to the cable modem.</li> <li>• <b>Blinking.</b> Power on self-test.</li> <li>• <b>Off.</b> No power.</li> </ul>
 Downstream	<ul style="list-style-type: none"> <li>• <b>Green solid.</b> One or more downstream channels is locked.</li> <li>• <b>Green slow blink.</b> The unit is scanning for a downstream channel.</li> <li>• <b>Green blink.</b> Data is being transmitted or received.</li> <li>• <b>Off:</b> No downstream channel is locked.</li> </ul>
 Upstream	<ul style="list-style-type: none"> <li>• <b>Green solid.</b> One or more upstream channels is locked.</li> <li>• <b>Green slow blink.</b> The unit is scanning for an upstream channel.</li> <li>• <b>Green blink.</b> Data is being transmitted or received.</li> <li>• <b>Off:</b> No upstream channel is locked.</li> </ul>
 Internet	<ul style="list-style-type: none"> <li>• <b>Solid green.</b> The cable modem is online.</li> <li>• <b>Blinking.</b> The cable modem is synchronizing with the cable provider's CMTS.</li> <li>• <b>Off:</b> The cable modem is offline.</li> </ul>
 LAN (Ethernet)	<p>Green indicates 1,000 Mbps. Amber indicates 100/10 Mbps.</p> <ul style="list-style-type: none"> <li>• <b>Solid.</b> An Ethernet device is connected and powered on.</li> <li>• <b>Blinking.</b> Data is being transmitted or received on the Ethernet port.</li> <li>• <b>Off.</b> No Ethernet device is detected on the Ethernet port.</li> </ul>
 Phone Port	<ul style="list-style-type: none"> <li>• <b>Green Solid.</b> Registered with the Call Agent.</li> <li>• <b>Green Blink.</b> There is an active call.</li> <li>• <b>Green Slow Blink.</b> Phone is on-hook, registration with Call Agent is in progress.</li> <li>• <b>Off.</b> No phones are connected to the phone port.</li> </ul>
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 <a href="#">Push 'N' Connect (WPS) Wireless Setup</a> on page 16</p>

## Gateway Rear Panel



**Figure 2. Gateway rear panel**


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

- **Two voice/phone ports.** With VoIP service, connect one or two handsets to these ports.
- **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 printer.

**Note:** USB functionality is only available with future firmware upgrades.

- **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.

---

## Install the Voice Gateway

Installation is the four-step process summarized here and described in the headings that follow. Make sure you complete the installation in this order.

1. Check the Installation Requirements.
2. Cable the Gateway.
3. Log in to the Gateway.
4. Connect to the Internet and VoIP.

After installation, set up the wireless connection as explained in [Chapter 2, Wireless Configuration](#).

## Check the Installation Requirements

Check the requirements listed below before installing the gateway:

- **Local Computer.** During installation, you need a local computer to connect to the gateway via Ethernet.
  - This computer should be set up to access the cable modem Internet service.
  - This computer must be set up to use DHCP to get its TCP/IP configuration from the gateway.
- **Cabling.** Use a Category 5 (CAT5) cable such as the one provided with your gateway for your LAN connections.
- **Cable Modem Service.** There must be active Data Over Cable Internet service provided by cable modem account.
- **Internet Service Provider (ISP) Configuration.** Depending on how the ISP set up the Internet account, you will need one or more of these configuration settings to connect the gateway to the Internet:
  - Host and Domain Names
  - ISP Domain Name Server (DNS) Addresses
  - Fixed or Static IP Address
- **Computers on the Network.** Each computer that will connect to the gateway must have either an installed Ethernet Network Interface Card (NIC), USB Host port, or 802.11b or 802.11g wireless adapter.

## Cable the Gateway

To install the gateway, connect it to a computer by an Ethernet according to the guidelines below.




### *Ethernet Connection*

If you are connecting a computer to the gateway with an Ethernet cable, following these instructions.

1. Turn off your computer.
2. Use the coaxial cable provided by your cable company to connect the wireless voice gateway cable port to your cable line splitter or outlet.
3. Connect the LAN port (for example, LAN port 4) on the gateway to your computer with the Ethernet cable included in the box.
4. Plug in the gateway and wait about 30 seconds for the lights to stop blinking.
5. Turn on your computer. If software usually logs you in to your Internet connection, do not run that software or cancel it if it starts automatically.



6. Verify the following:

- a. The power light  is lit after turning on the gateway.
- b. The Internet light  is solid green, indicating a link has been established to the cable network.
- c. The LAN LED  is lit for the port where you connected the computer.

## Log In to Your Gateway

You can log in to the gateway to view its settings. A link to the documentation is also available on the gateway main menu.

---

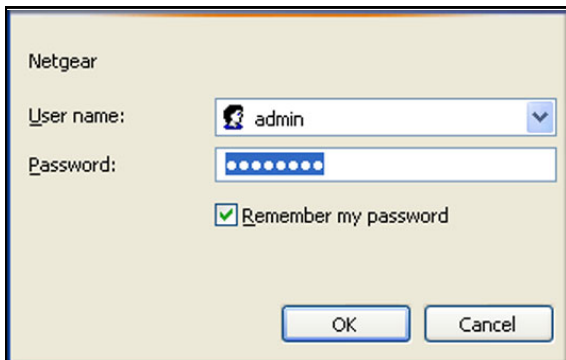
**Note:** To connect to the gateway you must use a computer configured for DHCP (most computers are).

---

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.

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.


A screenshot of the Netgear login window. The window has a title bar and a light beige background. At the top left, it says "Netgear". Below that, 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. Below the password field is a checkbox labeled "Remember my password" which is checked. At the bottom right, there are two buttons: "OK" and "Cancel".

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.

Gateway Status		
<b>Information</b>		
Standard Specification Compliant		DOCSIS 3.0
Hardware Version		1.04
Software Version		3.9.21.8.V0017
Cable MAC Address		00:26:f2:39:cd:a0
Device MAC Address		00:26:f2:39:cd:a2
Cable Modem Serial Number		2BG102U000F17
CM certificate		Installed
<b>Network Configuration</b>		
WAN	IP Address	---
	Duration	D: -- H: -- M: -- S: --
	Expires	---
WAN	Subnet Mask	---
WAN	Default Gateway	---
WAN	Primary DNS	---
WAN	Secondary DNS	---

To view the gateway's settings for the Internet connection, see the following section, [View the Gateway Status](#) on page 10.

## Connect to the Internet and VoIP

If you have VoIP service, connect the phone to a Voice Port 1 . If your service includes a second line, you can connect that phone to Voice Port 2.

To check the voice status, see [MTA Status](#) on page 24. To set up a wireless connection, see [Chapter 2, Wireless Configuration](#).

## View the Gateway Status

The Gateway Status screen shows the Network Configuration for the gateway. Select **Gateway Status** from the main menu and the Network Configuration section is in the middle of the page.

Network Configuration		
WAN	IP Address	192.168.15.72
	Duration	: D: 01 H: 00 M: 00
	Expires	Fri Apr 30 00:11:31 2010
WAN	Subnet Mask	255.255.255.128
WAN	Default Gateway	192.168.15.1
WAN	Primary DNS	172.29.16.12
WAN	Secondary DNS	0.0.0.0

## 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 CG3000 Quick Install Guide*.

---

This chapter includes:

- *Set Up Your Wireless Network* on page 12.
- *Manually Configure The Wireless Settings* on page 12.
- *Push 'N' Connect (WPS) Wireless Setup* on page 16.
- *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.* on page 17..

## Set Up Your Wireless Network

To set up the wireless network, you can enter wireless settings, (see [Manually Configure The Wireless Settings](#) on page 12) or you can use Wi-Fi Protected Setup (WPS), described in [Push 'N' Connect \(WPS\) Wireless Setup](#) on page 16. 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 shown on the product label. This product comes with a preconfigured Wi-Fi SSID and passphrase.
- By default the gateway works with WPA and WPA 2 wireless security. The default passphrase is shown on the product label.
- To use Push 'N' Connect (WPS), your wireless computers and equipment must support WPS technology. See [Push 'N' Connect \(WPS\) Wireless Setup](#) on page 16.

## Manually Configure The Wireless Settings

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

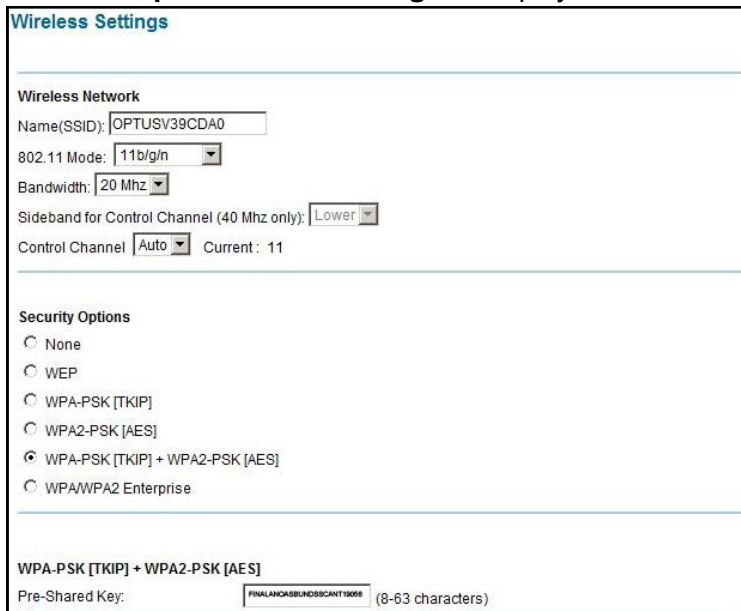
1. If you are located near the gateway, use an Ethernet cable to connect your computer to the gateway while you are changing the wireless settings.

---

**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. Select **Setup > Wireless Settings** to display this screen.



**Wireless Settings**

---

**Wireless Network**

Name(SSID):

802.11 Mode:

Bandwidth:

Sideband for Control Channel (40 Mhz only):

Control Channel:  Current: 11

---

**Security Options**

☐ None  
☐ WEP  
☐ WPA-PSK [TKIP]  
☐ WPA2-PSK [AES]  
☒ WPA-PSK [TKIP] + WPA2-PSK [AES]  
☐ WPA/WPA2 Enterprise

---

**WPA-PSK [TKIP] + WPA2-PSK [AES]**

Pre-Shared Key:  (8-63 characters)

3. Specify the Wireless Network settings.
  - **Name (SSID).** The name of the wireless network.
  - **802.11 Mode.** This is set to Up to 11 b/g/n by default.
  - **Bandwidth.** The rate of data transfer.
  - **Sideband for Control Channel (40Mhz only).** Sideband is a band of frequencies that is either lower or higher than the carrier frequency. You would adjust this setting if you want to refine the gateway's use of electrical power and bandwidth.
  - **Control channel.** Which operating channel is used. Normally, the channel is not changed unless there are interference problems with a nearby access point. The available channels depend on the region. Some countries have laws specifying which channels can be used.
4. For help with Security Options, see the following sections
5. 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.

1. In the Security Options section of the Wireless Settings screen, leave the default setting or select one of the WPA settings:

**Security Options**

☐ Disable

☐ WEP

☐ WPA-PSK[TKIP]

☐ WPA2-PSK[AES]

☒ WPA-PSK[TKIP] + WPA2-PSK[AES]

☐ WPA/WPA2 Enterprise

---

**WPA-PSK[TKIP] + WPA2-PSK[AES]**

Passphrase:  (8-63 characters)

- **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.
2. 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. This product comes with a preconfigured WPA passphrase.
  3. Click **Apply** to save your settings.
  4. 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.


---

1. On the Wireless Settings screen, select the **WEP** radio button under Security Options.

2. Select the Authentication type 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.

## 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 Configure The 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>.

---

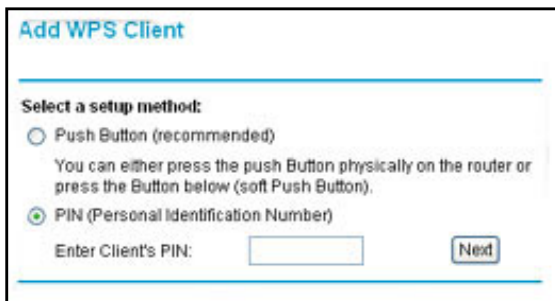
There are two Push 'N' Connect methods, Push Button and PIN (personal identification number).

- **Push Button.** This is the preferred method. See the following section, [WPS Button](#).
- **PIN.** See [PIN](#) on page 17.

### 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.

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. Select **Add WPS Client** and then click **Next**. The Add WPS Client screen displays:



**Add WPS Client**

Select a setup method:



☐ Push Button (recommended)  
You can either press the push Button physically on the router or press the Button below (soft Push Button).

☒ PIN (Personal Identification Number)

Enter Client's PIN:

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.



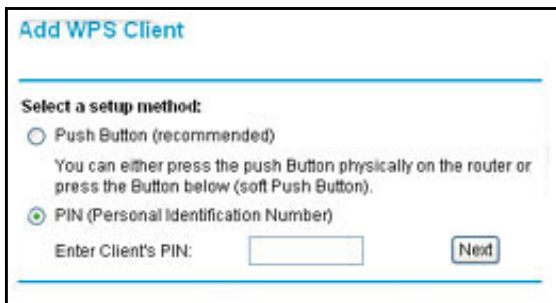
3. Either click the  WPS button, or press the  button on the front of the gateway.
  - The WPS LED on the front of the gateway begins to blink.
  - The gateway tries to communicate with the wireless computer or device for 2 minutes.
  - If the Security Option in the Wireless Settings screen was set to Disabled, it is automatically changed to WPA-PSK [TKIP] + WPA2-PSK [AES] including a random wireless security password.
4. 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.

5. 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.

## 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. 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.

3. Select the **PIN** radio button.
4. 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.

5. 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.

## 3. Content Filtering

---

# 3

This chapter describes how to use content filtering s for the gateway. This chapter includes:

- *View or Email Logs* on page 19.
- *Block Keywords, Sites, and Services* on page 19.
- *Services* on page 21.

## View or Email Logs

Your gateway logs security-related events such as Denial of Service (DoS) attacks, hacker probes, and administrator logins, based on the settings on the Logs screen. If you set up content filtering on the Block Sites screen, you can also log when someone on your network tried to access a blocked site. You can specify which events are logged and you can send the logs to the specified email address.

1. Select **Content Filtering > Logs**.

The screenshot shows the 'Logs' configuration page. It includes the following fields and controls:

- Contact Email Address**: A text input field.
- SMTP Server Name**: A text input field.
- Sender Email Address**: A text input field.
- SMTP Server Authentication**: A checkbox labeled 'Enable'.
- E-mail Alerts**: A checkbox labeled 'Enable'.
- Apply**: A button to save the settings.
- Log Table Headers**: A row of buttons for 'Description', 'Count', 'Last Occurrence', 'Target', and 'Source'.
- Action Buttons**: A row of buttons for 'E-mail Log', 'Clear Log', and 'REFRESH'.

2. To use email, fill in the **Contact Email Address** and **SMTP Server Name** fields.
3. Select the **Enable** check box for E-mail Alerts.
4. Click **Apply** so your changes take effect.
5. To email the log now, click **E-mail Log**.
6. To delete all log entries, click **Clear Log**.
7. To see the most recent entries, click **Refresh**.

## Block Keywords, Sites, and Services

With its content filtering feature, the gateway prevents objectionable content from reaching your computers. The gateway allows you to control access to Internet content by screening for keywords within Web addresses. It can also block access to all sites except those that are explicitly allowed. For example, you can set up the gateway to do the following:

- Block access from to Internet locations that contain keywords that you specify.
- Block access to websites that you specify as off-limits.
- Allow access to only websites that you specify as allowed.

## Block Keywords and Domains

The gateway allows you to restrict access to Internet content based on functions such as Web address keywords and Web domains. A domain name is the name of a particular website. For example, for the address www.NETGEAR.com, the domain name is NETGEAR.com.

1. Select **Content Filtering > Block Sites**.
2. To block keywords, select the **Keyword Blocking Enable** check box. Type the keyword and then click **Add Keyword**.

**Block Sites**

---

**Keyword Blocking** ☐ *Enable*

**Keyword List**

---

**Domain Blocking** ☐ *Enable*

**Domain List**

---

- If the keyword XXX is specified, the URL www.zzzyyqq.com/xxx.html is blocked.
  - If the keyword .com is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.
  - Enter the keyword "." to block all Internet browsing access.
  - To remove a keyword from the Keyword List, select it, and click **Remove Keyword**.
3. To block domains, select the **Domain Blocking Enable** check box. Enter a domain and click **Add Domain**.
    - If the domain www.zzzyyqq.com is specified, the URL <http://www.zzzyyqq.com/xxx.html> is blocked, along with all other URLs in the www.zzzyyqq.com site.
    - To remove a domain from the Domain List, select the domain, and then click **Remove Domain**.
  4. Click **Apply** to save your settings.

## Services

You can use the Services screen to disable certain gateway features.

1. Select **Content Filtering > Services**.

Services	
Firewall Features	<input checked="" type="checkbox"/> Enable
Ipssec PassThrough	<input checked="" type="checkbox"/> Enable
PPTP PassThrough	<input checked="" type="checkbox"/> Enable
Multicast	<input checked="" type="checkbox"/> Enable
Port Scan Detection	<input type="checkbox"/> Enable
IP Flood Detection	<input checked="" type="checkbox"/> Enable
<hr/>	
Web Features	
Filter Proxy	<input type="checkbox"/> Enable
Filter Cookies	<input type="checkbox"/> Enable
Filter Java Applets	<input type="checkbox"/> Enable
Filter ActiveX	<input type="checkbox"/> Enable
Filter Popup Windows	<input type="checkbox"/> Enable
Block Fragmented IP Packets	<input type="checkbox"/> Enable
<hr/>	
Apply	

2. To disable a feature, clear its check box.
3. Click **Apply** for your changes to take effect.

The following Services are available in this screen:

- **Firewall Features.** The gateway performs Stateful Packet Inspection (SPI) and protect against Denial of Service (DoS) attacks.
- **IPSec Pass-Through.** IPSec traffic is forwarded. If you clear this check box then this traffic will be blocked.
- **PPTP Pass-Through.** PPTP traffic is forwarded. If you clear this check box then this traffic will be blocked.
- **Multicast.** The gateway can pass multicasting streams through the firewall.
- **Port Scan Detection.** When enabled, the gateway can respond to Internet-based port scans.
- **IP Flood Detection.** Allows the is gateway to block malicious devices that are attempting to flood devices.
- You can use the Web Features to set certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall.

## 4. Manage Your Network

---

# 4

This chapter describes how to perform network management tasks with your gateway. When you log in to the gateway (see [Log In to Your Gateway](#) on page 9), these tasks are grouped under Maintenance.

This chapter includes:

- [Gateway Status](#) on page 23.
- [MTA Status](#) on page 24
- [Signal Status](#) on page 25
- [Change Password](#) on page 26.
- [Back Up and Restore Your Settings](#) on page 26.
- [Event Log](#) on page 27.
- [Diagnostic Ping Utility](#) on page 27.

## Gateway Status

Use the Gateway Status screen to see hardware and firmware details about the gateway and basic status information. Select **Maintenance > Gateway Status**.

Gateway Status		
<b>Information</b>		
Standard Specification Compliant	DOCSIS 3.0	
Hardware Version	1.04	
Software Version	3.9.21.8.V0017	
Cable MAC Address	00:26:f2:39:cd:a0	
Device MAC Address	00:26:f2:39:cd:a2	
Cable Modem Serial Number	2BG102U000F17	
CM certificate	Installed	
<b>Network Configuration</b>		
WAN	IP Address	---
	Duration	D: -- H: -- M: -- S: --
	Expires	---
WAN	Subnet Mask	---
WAN	Default Gateway	---
WAN	Primary DNS	---
WAN	Secondary DNS	---
<b>Status</b>		
System Up Time	0 days 00h:01m:30s	
Network Access	Denied	
Cable Modem IP Address	---	

The following table describes the fields displayed in this screen.

Information:

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.
Device MAC address	The MAC address used by the cable modem.
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.

## Network Configuration:

Modem Status Field	Description
IP Address	The gateway's public IP address so you can manage this gateway from the Internet. Note that if your ISP account uses a dynamic IP address, this value changes each time you connect to your ISP. You can either request your IP allocate a fixed IP address to you or use the Dynamic DNS (DDNS) feature to connect with a domain name instead of an IP address.
Duration	The length of time in days, hours, minutes, and seconds for the remote access.
Expires	When the remote access ends.
Subnet Mask	The network number portion of an IP address.
Default Gateway	Make sure the IP address of your gateway is listed here.
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.
Secondary DNS	If applicable, the address of the secondary DNS server of your ISP.

## Status:

Modem Status Field	Description
System Up Time	Time since the last boot up.
Network Access	Shows whether traffic can be forwarded from the LAN to the network
Cable Modem IP Address	The current Internet IP address. If assigned dynamically and not connected to the Internet, this field is blank.

## MTA Status

The Multimedia Terminal Adaptor (MTA) Status shows the status of the voice ports on the gateway. This page refreshes every ten seconds to update the status.

MTA Status	
<b>Information</b>	
MTA Provision Status	Not Ready
MTA MAC Address	00:26:f2:39:cd:a1
MTA IP Address	---
MTA Telephony Signaling	SIP

**MTA Provision Status.** Shows which of your telephone lines are active and registered with your service provider.

**MTA MAC Address.** The MAC address of the MTA interface.

**MTA IP Address.** The IP MTA address.

**MTA Telephony Signaling.** The type of telephony signaling the MTA current uses.



## Signal Status

Signal Status lets you follow the startup procedure and get details on the Downstream and Upstream cable channel.

Signal Status

Startup Procedure		
Procedure	Status	Comment
Acquire Downstream Channel	270000000 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File	In Progress	
Security	Disabled	Disabled

Downstream Bonded Channels

Lock Status	Modulation	Channel ID	Symbol rate	Frequency	Power	SNR	Docsis/EuroDocsis locked
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow
Not Locked	Unknown	0	0 sym/sec	0 Hz	0.0 dBmV	0.0 dB	Unknow

Upstream Bonded Channels

Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV
Not Locked	Unknown	0	0 Ksym/sec	0 Hz	0.0 dBmV

Current System Time:--- -- -- --[---]-- --

**Figure 1. Startup, downstream, and upstream information**

Use the Signal Status 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.

## Change Password

For security, 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.

1. Select **Maintenance > Set Password**.



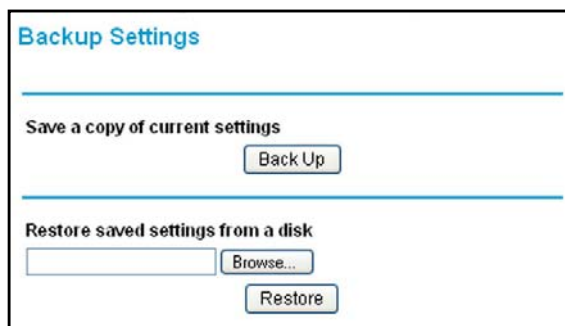
2. To change the password, enter the new password twice.
3. Click **Apply** to save your changes.

After changing the password, you are 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.

## Back Up and Restore Your Settings

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

1. Select **Maintenance > Backup Settings**.



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 is restored to its previous settings. Then, the gateway restarts, which takes about one minute.

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

## Event Log

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

1. Select **Maintenance > Event Log**.

Event Log		
Time	Priority	Description
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC framing;CM-MAC=00:26:f2:39:cd:a0;CMTS-MAC=00:00:00:00:00:00;CM-QOS=1.0;CM-VER=3.0;
<div>Clear Log Refresh</div>		

2. To clear the log, click **Clear Log**, and to refresh the log, click **Refresh**.

## Diagnostic Ping Utility

From the Diagnostics screen you can use Ping.

1. Select **Maintenance > Diagnostics**.

**Diagnostics**

Utility Ping

Ping Test Parameters

Target

Ping Size  bytes

No. of Pings

Ping Interval  ms

Start Test Abort Test Clear Results

Perform a DNS Lookup

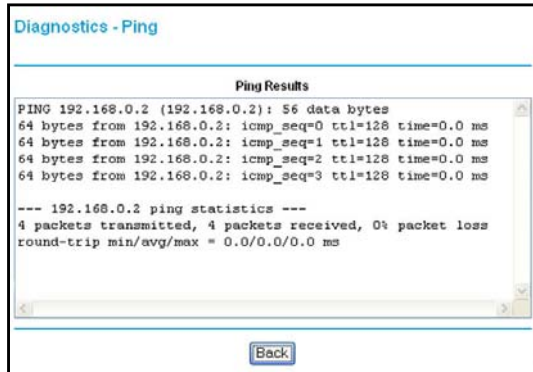
Internet Name:  Lookup

Display the Routing Table Display

Reboot the Router Reboot

Revert to factory default settings Reset to Factory Default

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



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

## 5 Advanced Settings

---

# 5

This chapter describes how to customize your network through the advanced settings on your gateway. When you log in to the gateway (see [Log In to Your Gateway](#) on page 9), these tasks are grouped under Advanced.

This chapter includes:

- [Wireless Settings](#) on page 30
- [Firewall Rules: Port Blocking](#) on page 32.
- [Firewall Rules: Port Forwarding](#) on page 33.
- [WAN Setup](#) on page 34
- [Dynamic DNS](#) on page 35
- [LAN IP Setup](#) on page 36.
- [Remote Management](#) on page 38.
- [Universal Plug and Play \(UPnP\)](#) on page 40.

## Wireless Settings

Select **Advanced > Wireless Settings** to display the following screen where you can configure the wireless radio settings, and other advanced settings:

**Advanced Wireless Settings**

**Wireless Access Point**

☒ Enable Wireless Router Radio

☒ Enable SSID Broadcast

**Advanced Configuration**

Fragmentation Threshold: 2346

CTS/RTS Threshold: 2347

Preamble Mode: Long

**WPS Settings**

Router's PIN: 12345670

**Wireless Card Access List**

☐ Turn Access Control On [Setup Access List](#)

[Apply](#) [Cancel](#)

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

Advanced Wireless Settings		Description
Wireless Access Point	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.
	Enable SSID Broadcast	By default this checkbox is selected so that the gateway broadcasts its Wi-Fi network name (SSID) so devices can find it. Deselect this checkbox if you do not want wireless devices to find this gateway unless they have the same SSID.
Advanced Configuration	<ul style="list-style-type: none"> <li>Fragmentation Threshold</li> <li>CTS/RTS Threshold</li> <li>Preamble Mode</li> </ul>	The default settings for these fields usually work fine. Change them only if you have a specific reason for doing so.
WPS Settings	Router's PIN	The PIN that WPS clients use to connect to the gateway using the PIN method.
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.

## 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.

1. Log in to the gateway as described in [Log In to Your Gateway](#) on page 9.
2. In the main menu, under Advanced, select Wireless Settings.
3. Click the **Setup Access List** button to display the Wireless Card Access List screen.

**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.

4. 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.
5. 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**.
6. Click **Apply** to save these settings.

## Firewall Rules: 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.

---

1. Select **Advanced > Firewall Rules**. The Port Blocking section is near the bottom of the screen.

**Port Blocking**

Add Predefined Service  
Service: -SERVICES-

Add Custom Service

Name	Start Port	End Port	Protocol	Local IP Address
	0	0	Both	192.168.0.0

Add Reset

Port Filter List  
No filters entered. ☐ Enable Delete

Day(s) to Block  
☐ Everyday ☐ Sunday ☐ Monday ☐ Tuesday  
☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Time of Day to Block  
☐ All day  
 Start: 12 (hour) 00 (min) AM  
 End: 12 (hour) 00 (min) AM

Apply Cancel

2. In the **Services** field, select a service from the drop-down list. (For example, FTP, which uses TCP ports 20 and 21.)
3. 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.



4. 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**.

## Firewall Rules: 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 the Acceptable Use policy of your ISP.

To configure port forwarding and services for specific inbound traffic:

1. Select **Advanced > Firewall Rules**. The Port Forwarding section is on the top.
2. In the **Service** field, select a service from the drop-down list. (For example, FTP, which uses TCP ports 20 and 21.)
3. 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 port protocol:
    - **TCP**. Select TCP only.
    - **UDP**. Select UDP only.
    - **Both**. Select both TCP and UDP.

**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: -SERVICES-

**Add Custom Rules**

Name	Start Port	End Port	Protocol	Local IP Address
	0	0	Both	192.168.0.0

- **Local IP Address.** Enter the local IP address for the computer that uses the service.
4. 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**.

## 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 192.168.1.2 through 192.168.1.9 are reserved for this purpose.
- Local PCs must access the local server using the PCs' local LAN address (192.168.1.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.

## WAN Setup

Select **Advanced > WAN Setup** to set up a Default DMZ Computer to display the following screen. A Default DMZ Computer lets you set up a PC that is available to anyone on the Internet for services that you haven't defined. For security reasons, do this only if you are willing to risk open access. If you do not assign a Default DMZ Computer, the gateway discards any undefined service request.

**WAN Setup**

Respond to Ping on WAN Port ☐

DMZ Address 192.168.0. 0

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

**Respond To Ping On Internet Port.** If you want the CG3000 to respond to a 'Ping' from the Internet, click this check box. This can be used as a diagnostic tool.

**MTU Size.** The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection

## Assign a Computer as The DMZ Host

1. Type the last field of the IP address field in the DMZ Address field.
2. Click **Apply**.

## Remove a Computer from Being a DMZ Computer:

1. Type 0 in last field of the IP address field in DMZ Address.
2. Click **Apply**.

## Dynamic DNS

A Dynamic DNS (DDNS) Service provides a central public database where information such as email addresses, host names and IP addresses can be stored and retrieved. The Dynamic DNS server also stores password-protected information and accepts queries based on e-mail addresses. The Router supports only basic DDNS and the login and password may not be secure. If you have a private WAN IP address, do not use DDNS service as it may lead to problems.

**Note:** you have to register for the DNS service. When you register, the DDNS client service provider gives you a password or key.

Select **Advanced > Dynamic DNS** to display the following screen:

The screenshot shows the 'Dynamic DNS' configuration page. At the top, the title 'Dynamic DNS' is in blue. Below it, there's a section with the following fields: 'DDNS Service' is a dropdown menu currently showing 'Disabled'; 'Host Name' is an empty text box; 'User Name' is an empty text box; 'Password' is an empty text box; 'IP Address' is a text box containing '0.0.0.0'; and 'Status' shows a yellow warning icon and the text 'DDNS service is not enabled.' Below these fields is a 'Use Wildcards' checkbox, which is currently unchecked. At the bottom right of the form are two buttons: 'Apply' and 'Cancel'.

Select the **Use A Dynamic DNS Service** check box.

1. Select the name of your dynamic DNS Service Provider.
2. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
3. Type the **User Name** for your DDNS account.
4. Type the **Password** (or key) for your DDNS account.
5. Click **Apply** to have the DDNS service used.

**Use Wildcards.** If you have DYNDNS as your DDNS service provider, you may select the Use Wildcards check box to activate this optional feature.

## 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.

---

1. Select **Advanced > LAN IP**.
2. Enter these settings:
  - **LAN IP Address.** The factory default setting is 192.168.1.1.
  - **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

The screenshot shows the 'LAN IP' configuration page. At the top, the title 'LAN IP' is displayed. Below it, several configuration fields are visible: 'Device Name' (set to ---), 'LAN IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), 'DHCP Server' (radio buttons for Yes and No, with Yes selected), 'Starting IP Address' (192.168.0.2), 'Ending IP Address' (192.168.0.254), 'Max Users' (253), and 'Lease Time' (3600). An 'Apply' button is located below these fields. Below the main configuration section, there are two tables. The first table is titled 'DHCP Reservation Lease Info' and has columns for '#', 'Mac Address', and 'IP Address'. It contains one row with a radio button, the MAC address '001641156fb1', and the IP address '192.168.000.002'. Below this table are 'Add' and 'Delete' buttons. The second table is titled 'DHCP Client Lease Info' and has columns for 'MAC Address', 'IP Address', and 'Expires'. It contains one row with the same MAC and IP addresses, and an 'Expires' field showing '--- --:--:--'. Below this table is a 'Clear DHCP Leases' button.

## 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.

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 display in the DHCP Client Lease Info table. The current system time is also displayed.

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.
1. In the main menu, under Advanced, select Remote Management.
  2. Select one of the **Allow Remote Management** check boxes.

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**  
 ip\_address is the Internet IP address of this gateway.  
 pn is the port number assigned on this screen.

- c. You are 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** check box.
  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) CM 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.
Revert to factory default settings	Allow Remote management after Factory Default Reset
IP Address to connect this device	The gateway's public IP address so you can manage this gateway from the Internet. Note that if your ISP account uses a dynamic IP address, this value changes each time you connect to your ISP. You can either request your IP allocate a fixed IP address to you or use the Dynamic DNS (DDNS) feature to connect with a domain name instead of an IP address.

## 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 life of 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.

1. Select **Advanced > 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 CG3000. For the common problems listed, go to the section indicated.

- Have I connected the gateway correctly?  
Go to *Basic Functions* on page 42.
- I cannot access the gateway configuration with my browser.  
Go to *Access the Gateway Configuration* on page 43.
- I have configured the gateway but I cannot access the Internet.  
Go to *Troubleshoot the ISP Connection* on page 44.
- 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"> <li>• Clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. See <a href="#">Factory Default Settings</a> in Appendix A.</li> <li>• If the error persists, you might have a hardware problem and should contact technical support.</li> </ul>
LAN LED is off for a port with an Ethernet connection.	<ul style="list-style-type: none"> <li>• Make sure that the Ethernet cable connections are secure at the gateway and at the hub or PC.</li> <li>• Make sure that power is turned on to the connected hub or PC.</li> <li>• Be sure you are using the correct cable.</li> </ul>
Internet LED is off and the gateway is connected to the cable television cable.	<ul style="list-style-type: none"> <li>• Make sure that the coaxial cable connections are secure at the gateway and at the wall jack.</li> <li>• 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.</li> <li>• 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.</li> </ul>

## Access the Gateway Configuration

If you are unable to access the gateway's configuration 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 192.168.0.2 to 192.168.0.254.

---

**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.

## Troubleshoot the ISP Connection

If your gateway cannot access the Internet and your Cable Link LED is on, you might need to register the cable MAC address and/or device MAC address of your gateway with your cable service provider. Your PC might 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.

## 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 responds with an echo reply. Troubleshooting a TCP/IP network is made easier by using the ping utility in your PC 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 on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the gateway like this:  
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 42.
  - 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.

## Test 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.
- 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 Technical Specifications


---



This chapter covers the following topics:

- *Factory Default Settings*
- *Technical Specifications* on page 49

## Factory Default Settings

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

**Table 1.**

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
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500

Table 1.

Factory Default Settings (Continued)		
Wireless	Wireless communication	Enabled
	SSID name	As shown on the product label.
	Security	WPA/WPA2
	Broadcast SSID	Enabled
	Transmission speed	Auto <sup>1</sup>
	Country/region	Depends on the country where the product is sold.
	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 product family.

**Table 2.**

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"> <li>• North America (input): 120V, 60 Hz, input</li> <li>• All regions (output): 12 V DC @ 1.5A output 18W maximum or 12 V DC @ 2.5A output 30W maximum</li> </ul>
Physical specifications	<ul style="list-style-type: none"> <li>• Dimensions: 8.5 by 5.75 by 1.3 in (216 by 146 by 33 mm)</li> <li>• Weight: 0.95 lb (0.42 kg)</li> </ul>
Environmental	<ul style="list-style-type: none"> <li>• Operating temperature: 32° to 140° F (0° to 40° C)</li> <li>• Operating humidity: 90% maximum relative humidity, noncondensing</li> <li>• Electromagnetic emissions: Meets requirements of: FCC Part 15 Class B.</li> </ul>
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

# Notification of Compliance



## Europe – EU Declaration of Conformity



Marking with 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, EN301 893 (5GHz), EN60950-1
- 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.
- For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:  
[http://kb.netgear.com/app/answers/detail/a\\_id/11621/](http://kb.netgear.com/app/answers/detail/a_id/11621/)

Table 3.

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.

**Table 3.**

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-Direttiva 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.

# Index

## Numerics

192.168.1.1, default IP address [9](#)

## B

backing up the configuration file [26](#)

Basic Settings [10](#)

blocking

    keywords [20](#)

    sites [20](#)

blocking ports [32](#)

## C

cable channel [25](#)

configuration

    backup [26](#)

    erasing [26](#)

## D

DHCP [37](#)

    reserved IP address [37](#)

    server [36](#)

## E

Erase configuration [26](#)

Ethernet connection [8](#)

Event log [27](#)

## F

firewall rules

    inbound [33](#)

    port forwarding [33](#)

front panel [6](#)

## G

gateway

    backup [26](#)

    main menu [43](#)

    placement and range guidelines [12](#)

    remote management [38](#)

gateway front panel [6](#)

gateway rear panel [7](#)

## I

IP address [9](#)

IP addresses, auto-generated [43](#)

## L

LAN

    IP address [36](#)

    IP settings [36](#)

LEDs

    troubleshooting [42](#)

logging in [9](#)

logging out [9](#)

logs [19](#), [27](#)

## M

Modem Status [23](#)

## P

passphrase [15](#)

ping utility [44](#)

port blocking [32](#)

port forwarding [33](#), [34](#)

## R

remote management [38](#)

## S

Services (firewall) [21](#)

## T

TCP/IP

    network, troubleshooting [44](#)

technical specifications [49](#)

troubleshooting [41](#)

    ISP connection [44](#)

LEDs **42**  
ping utility **44**  
TCP/IP network **44**

## U

Universal Plug and Play (UPnP) **40**  
URL **20**

## V

voice  
    Ethernet connection **8**  
voice gateway, installing **7**  
voice ports **7**  
VoIP service **7**

## W

WEP **15**  
    keys **15**  
    passphrase **15**  
Wi-Fi Protected Setup (WPS)  
    Push 'N' Connect **30**  
wireless  
    access point **30**  
    card access list **30**  
    manually configuring settings **12**  
wireless network  
    planning **12**  
wireless security **17**  
Wireless Security Options **12**  
WPA **14**  
WPA2 **14**  
WPA2-PSK **14**  
WPA-PSK **14**  
WPS **16**  
WPS button **6**