NETGEAR

Wireless Cable Modem Gateway CG2003D

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

January 2011
202-10773-01
v1.0

Technical Support

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

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

Phone (Other Countries): See Support information card.

Trademarks

Statement of Conditions

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

Contents

Chapter 4 Managing Your Network

Chapter 5 Advanced Settings

Chapter 6 Troubleshooting

Appendix A Technical Specifications and Factory Default Settings

Appendix B Related Documents

Appendix C Notification of Compliance

Index

Connecting the Gateway to the Internet 1

This chapter describes how to set up the Wireless Cable Modem Gateway on your Local Area Network (LAN), connect to the Internet, and perform basic configuration.

Unpack your Gateway

The product package should contain the following items:

- Wireless Cable Modem Gateway CG2003D
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- Stand

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you need to return the product for repair.

Gateway Stand

You can place the gateway vertically or horizontally. To place the gateway vertically, attach the stand to the bottom of the gateway, and place it on a flat surface, as shown.

Figure 1. Vertical position with stand

Front Panel

The front panel of the Wireless Cable Modem Gateway contains status LEDs.

Figure 2. Front view

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

Table 1. LED Descriptions

LED	Description
Power	• **On**: Power is supplied to the gateway, and the gateway has completed its initialization. • **Off**: Power is not supplied to the gateway.
Downstream Link	• **On**: The gateway completed its downstream scan. • **Blink**: The gateway has just powered up or it is performing a downstream scan. • **Off**: The gateway's self-test and initialization is complete but it has not completed the downstream scan.
Upstream Link	• **On**: The gateway has completed its upstream ranging operation. • **Blink**: The gateway has just powered up or it is getting upstream configuration information. • **Off**: The gateway's self-test and initialization is complete but it has not completed the upstream scan.
Cable Link	• **On (green)**: Configuration by your cable service provider is complete. • **Blink**: Both downstream and upstream links are established, but the configuration is not done. • **Off**: Configuration of the cable interface is in progress. The downstream and upstream links have not been established yet.
LAN (local area network)	• **On (green)**: The port has detected link with a 100 Mbps device. • **Blink (green)**: Data is being transmitted or received at 100 Mbps. • **On (yellow)**: The Local port has detected link with a 10 Mbps device. • **Blink (yellow)**: Data is being transmitted or received at 10 Mbps. • **Off**: No link is detected on this port.
Wireless	• **On**: The wireless access point is operating normally. • **Blink**: Data is being transmitted or received on the wireless interface. • **Blink in a fast pattern**: The gateway attempts to establish a connection to a wireless client through Wi-Fi Protected Setup (WPS). • **Off**: The wireless access point is disabled.

Rear Panel

The rear panel of the gateway contains the connections identified below:

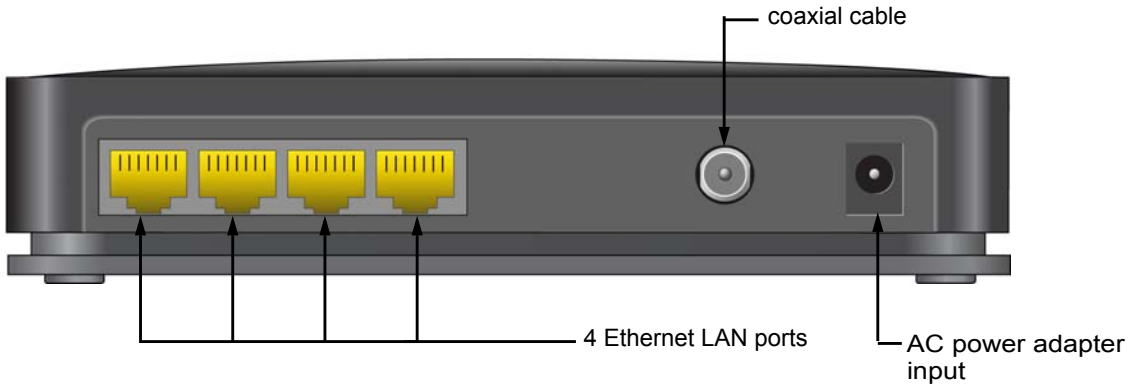


Figure 3. Rear view

Label

The label on the bottom of the gateway shows the gateway's factory reset button, its default wireless settings, MAC address, and serial number.

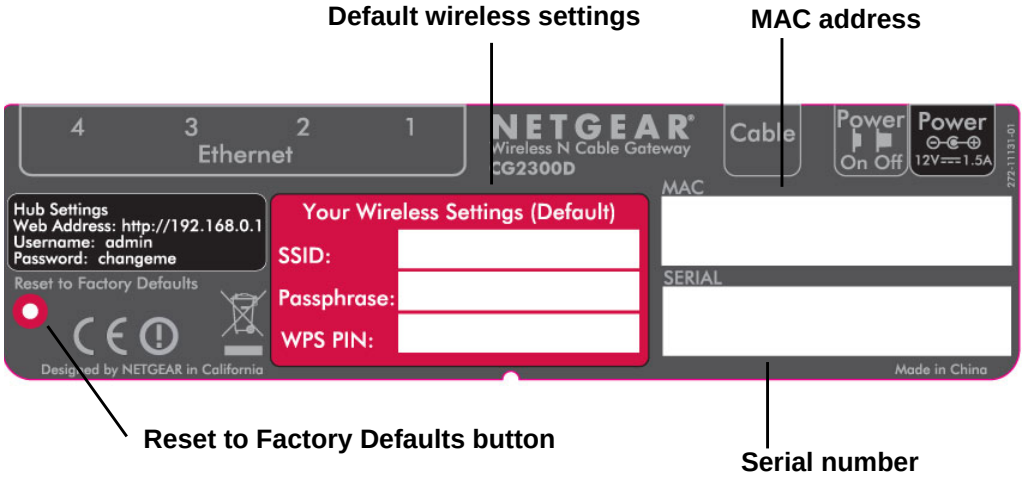


Figure 4. Label on gateway bottom

What You Need Before You Begin

- A computer with an Ethernet port to connect to the gateway while you set it up. The computer has to be set up to use DHCP. For help with DHCP configuration, see the link to the online document *ITCP/IP Networking Basics* in Appendix B.
- Active Data Over Cable Internet service provided by cable modem account.
- The Internet Service Provider (ISP) configuration information for your cable modem account.

Cabling the Gateway

1. Using the coaxial cable provided by your cable company, connect the gateway cable port (A) to your cable line splitter or outlet.

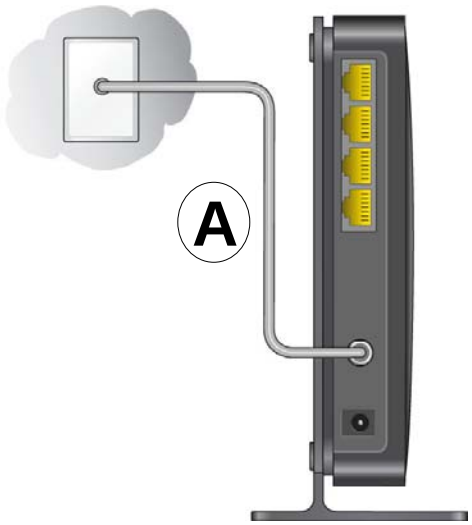


Figure 5. Gateway coaxial cable connection

2. Use the Ethernet cable that shipped with your gateway to connect a LAN port (B) to the Ethernet adapter in your computer.

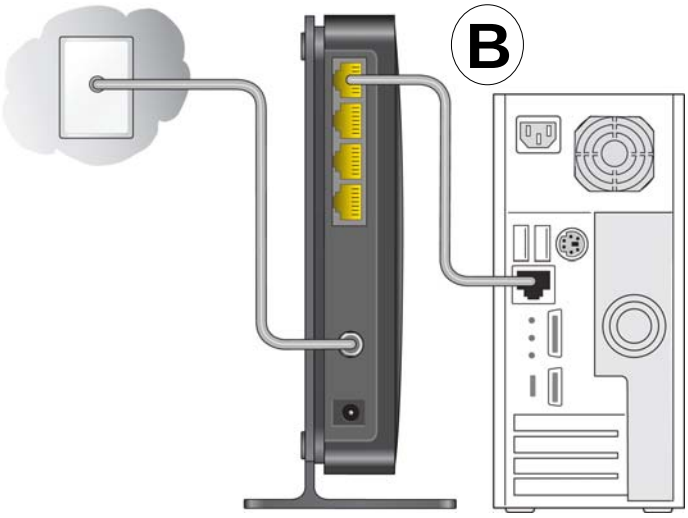


Figure 6. Gateway Ethernet cable connection

3. Connect the power adapter to the gateway, and plug it into an outlet.
4. Wait about 30 seconds for the lights to stop blinking, and then verify the following:

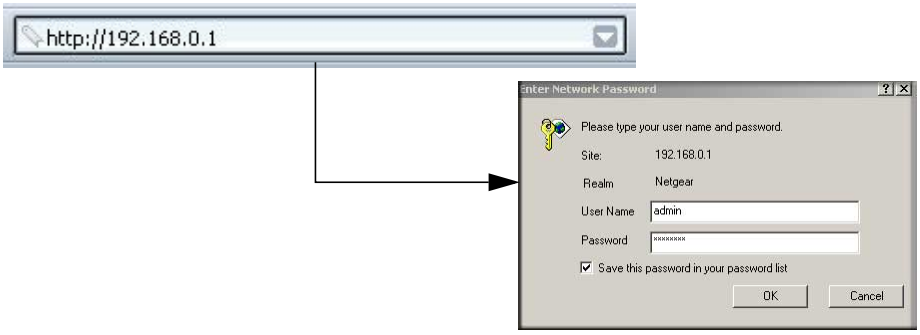
   The power LED is lit.

   The cable link LED is solid green, indicating a link has been established to the cable network.

Log in to the Gateway

You can log in to the gateway to view or change its settings. You can use an Ethernet cable to connect the computer to the gateway, or you can connect wirelessly.

1. Using the computer that you first used to access your cable modem Internet service, type **http://192.168.0.1** in the address field of your Internet browser. A login window opens.

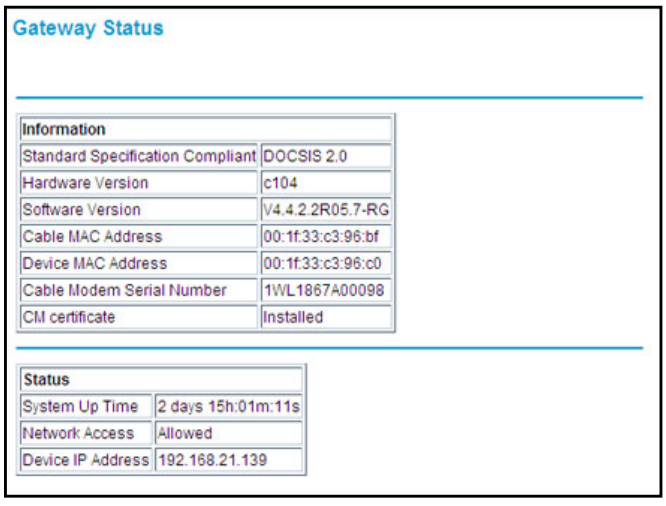


2. Log in to the gateway.

   There are two methods to log in:

   - For superuser access, enter **MSO** for the user name and **changeme** for the password. Both are case-sensitive.
   - To access the gateway features except for content filtering, enter **admin** for the user name and **password** for the password, both in lower case letters.

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



   For more information about this screen, see *Gateway Status* on page 33.

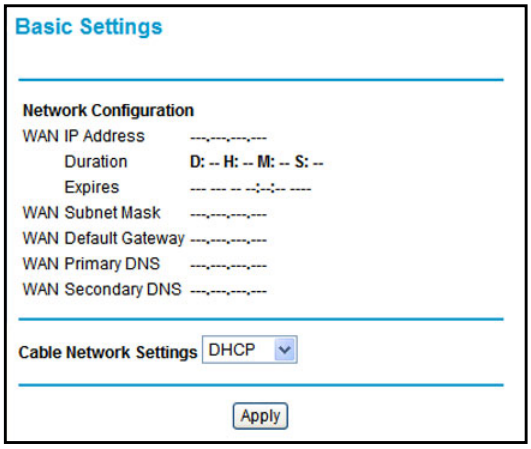
If you do not see the login prompt:

1. Check the LEDs on the gateway front panel to make sure that the gateway is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the gateway is connected to a LAN port.
2. If you connected the Ethernet cable and quickly launched your browser and typed in the router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the gateway wirelessly, NETGEAR recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the gateway.

Note: If you cannot connect to the gateway, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation or follow the links in *Related Documents* on page 146 for assistance.

Basic Cable Network Settings

To configure the cable network settings, in the main menu, under Setup, select Basic Settings. The Basic Settings screen displays.



The default setting is for DHCP. Click **Apply** to save your settings. After you connect to the Internet, the network configuration settings on this screen match the cable network settings.

Wireless Settings

2

For a wireless connection, you need to set up your wireless computer or device to use the gateway's SSID, also called the wireless network name, and wireless security settings. NETGEAR strongly recommends that you use wireless security.

This chapter includes:

Wireless Adapter Compatibility

A wireless adapter is the wireless radio in your PC or laptop that lets the PC or laptop connect to a wireless network. Most PCs and laptops come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the gateway.

Note: If you connect devices to your gateway using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 13, those devices assume the security settings of the gateway.

Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described above, your gateway has the security features described here and in *Chapter 4, Content Filtering Settings*.

- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Disable SSID Broadcast

By default, the gateway broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices will not find your gateway unless they are configured with the same SSID. See *Wireless Access Point Settings* on page 16 for the procedure.

Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific PCs based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the gateway.The Wireless Station MAC address filtering adds additional security protection to the wireless security option that you have in force. Access List determines which wireless hardware devices are allowed to connect to the gateway by MAC address. See *Advanced Wireless Settings* on page 79 for the procedure.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the most recent, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. Note that it is also possible to disable wireless security. NETGEAR does *not* recommend this. You can view or change the wireless security options in the Wireless Settings screen. See *Wireless Settings Screen* on page 14.

Add Clients (Computers or Devices) to Your Network

Choose either the manual or the WPS method to add wireless computers or devices to your wireless network.

Manual Method

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

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard that lets you easily join a secure wireless network with WPA or WPA2 wireless security. The gateway automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect[1].

Note: If the wireless network name (SSID) changes each time you add a WPS client, the Keep Existing Wireless Settings check box on the Advanced Wireless Settings screen has been cleared. See *WPS Settings* on page 80 for more information about this setting.

You can use a WPS button or the gateway interface method to add wireless computers and devices to your wireless network.

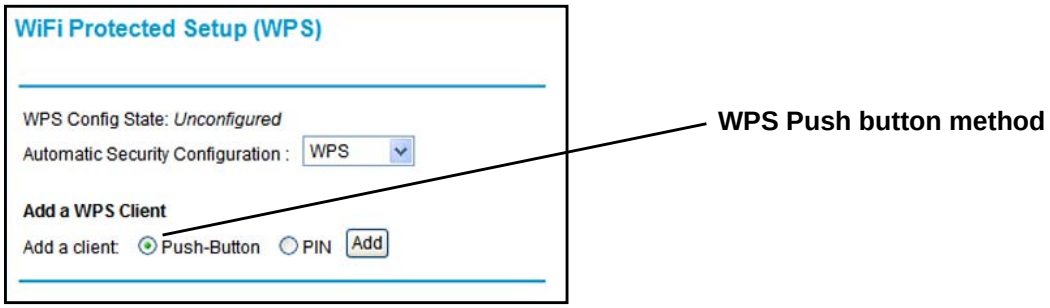
WPS Button Method

1. Press the WPS button on the gateway front panel  .
2. Within 2 minutes, press the WPS button on your wireless computer or device, or follow the WPS instructions that came with the computer. The device is now connected to your gateway.
3. Repeat steps 1 and 2 to add other WPS wireless computers or devices.

1. For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org.

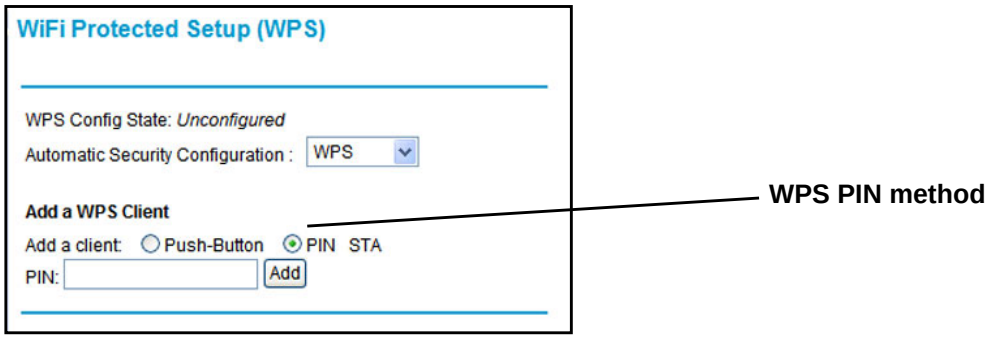
Gateway Interface Method

1. Select **Add WPS Client** at the top of the gateway menus.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



3. Select either **Push Button** or **PIN Number**. With either method, the gateway tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.

   The PIN method displays this screen so you can enter the client security PIN number:



   While the gateway attempts to connect, the WPS LED on the front of the gateway blinks green. When the gateway establishes a WPS connection, the LED is solid green and the gateway WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

Wireless Settings Screen

The Wireless Settings screen lets you view or change the wireless network settings. If you change the settings, note the new settings and save them in a secure location.

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

Consider Every Device on Your Network

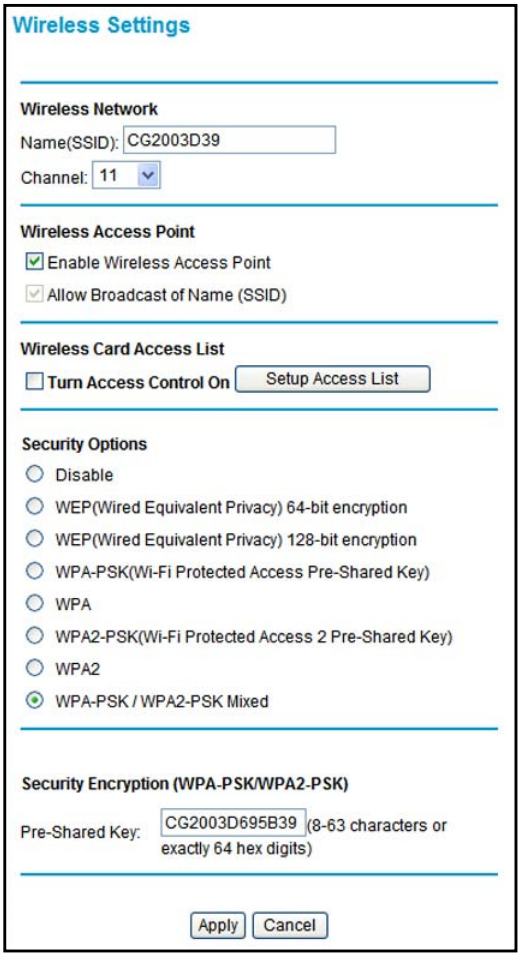
Before you begin, check the following:

- Every wireless computer has to be set up to get an IP address by DHCP from the gateway as described in *Use Standard TCP/IP Properties for DHCP* on page 18.
- To join your wireless network, each computer or wireless adapter has to be compatible with the wireless mode (bandwidth/data rate) of the gateway. Check that each wireless computer or device supports the mode you want to use.
- The security option on each wireless device in the network has to match the gateway. For example, if you use WPA2 or WPA, you need to use the pre-shared key from each wireless computer in order for it to join the wireless network.

View or Change Wireless Settings

To view or change the wireless settings:

1. Select **Setup > Wireless Settings**. The Wireless Settings screen displays.



2. If you make changes, you have to click **Apply** for them to take effect.

The following sections describe the fields in the Wireless Settings screen.

Wireless Network

- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and there is typically no need to change it. If you want to set up guest networks, NETGEAR does recommend that you customize the default guest network names (SSIDs).
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

Wireless Access Point Settings

- **Enable.** When this check box is not selected, the wireless signal in the gateway so it can accept wireless clients. When not enabled, the gateway accepts wired clients only. This check box is selected by default.
- **Allow Broadcast of Name (SSID).** This setting allows the gateway to broadcasts its SSID so wireless stations can see this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.

Wireless Card Access List

By default, any wireless PC that is configured with the correct SSID and network password is allowed to join your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses.

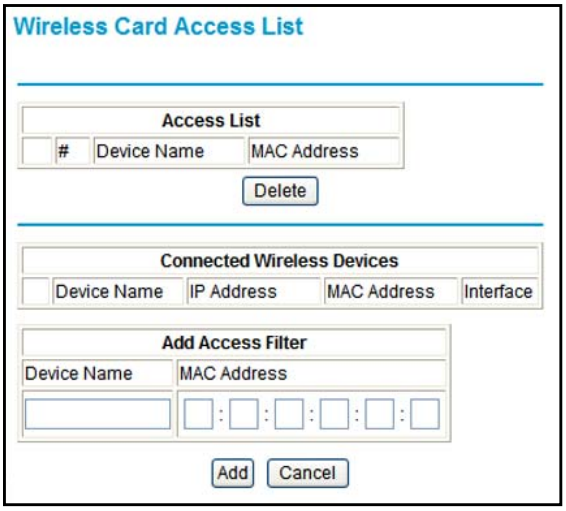
Set up Access Control by MAC Address

When you enable access control, the access point only accepts connections from clients on the selected access control list. This provides an additional layer of security

To restrict access based on MAC addresses:

1. In the Wireless Settings screen, select the **Turn Access Control On** check box.

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



By default, the Access List table is empty. You need to add wireless devices here so that they will have access to the wireless network when the list is enabled.

3. Adjust the access list as needed for your network. You can add devices to the access list using either of the following methods:
   - If the computer is in the Connected Wireless Devices table, click the radio button of that computer 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**.

Note: If no device name displays when you enter the MAC address, you can type a descriptive name for the computer that you are adding.

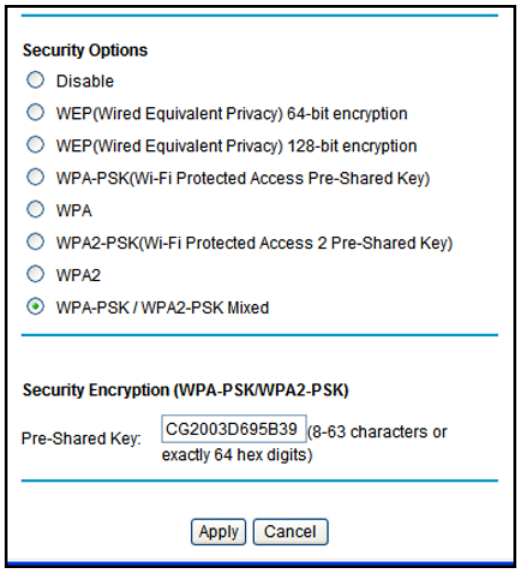
4. Click **Apply** to save these settings. Now, only devices in the Access List table are allowed to wirelessly connect to the gateway.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. The primary network for your gateway is already set up with WPA2 and WPA security. NETGEAR recommends that you set up wireless security for each guest network that you plan to use.For information about changing these settings, see the following section, *Change the WPA Security Option and Pre-Shared Key* on page 18and *Set WEP Encryption and Passphrase* on page 19.

Change the WPA Security Option and Pre-Shared Key

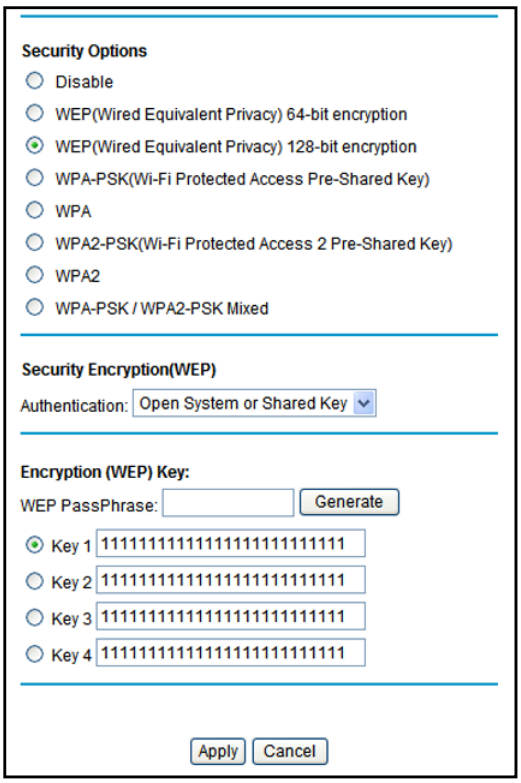
1. In the Security Options section, select the WPA option that you want.



2. Enter the pre-shared key that you want to use. The pre-shared key acts as a password to access your wireless network. It is a text string from 8 to 63 characters.
3. Click **Apply**.

Set WEP Encryption and Passphrase

1. In the Security Options section of the Wireless Settings screen, select the WEP radio button that you want.



2. Enter the four data encryption keys either manually or automatically. These values have to be identical on all computers and access points in your network.
   - **Automatic**. Enter a word or group of printable characters in the **Passphrase** field and click **Generate**. The four key fields are automatically populated.
   - **Manual**. The number of hexadecimal digits that you enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
3. Select the radio button for the key you want to make active.

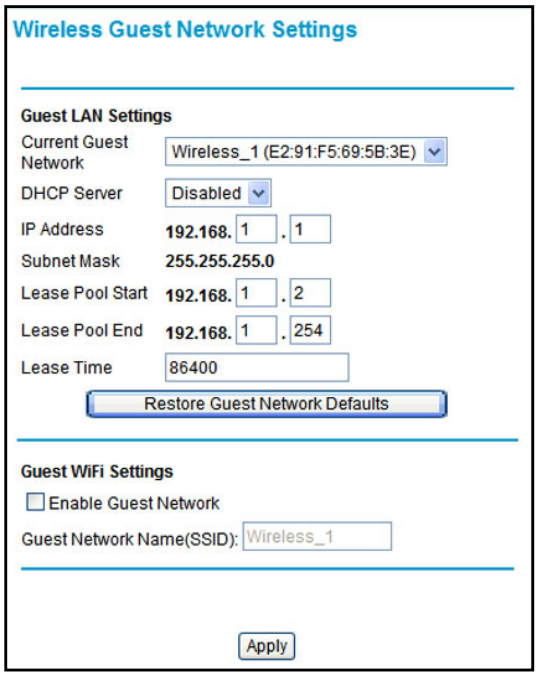
   Make sure you understand how to set up the WEP key settings in your wireless computers or adapters. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the gateway.
4. Click **Apply**.

Wireless Guest Networks

A wireless guest network allows you to provide guests access to your wireless network without prior authorization of each individual guest. You can wet up 3 wireless guest networks and specify the security options for each wireless guest network.

To set up a wireless guest network:

1. Select **Setup > Wireless Guest Network**.



2. Select the guest network that you want to work with.
   - NETGEAR strongly recommends that you change the SSID to a different name. Note that the SSID is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.
   - For guest networks, wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
3. Select a security option for the guest network and specify the password.
4. Select the **Enable Guest Network** check box.
5. You can now change the Guest Network Name (SSID) for the selected guest network. Enter a value of up to 32 alphanumeric characters.
6. When you have finished making changes, click **Apply**.

Wireless Guest Network Screen Fields

Guest LAN Settings

- **Current Guest Network**. You can select a guest network from the drop-down list.
- **DHCP Server**. Select whether or not the DHCP server is enabled for the currently selected guest network.
- **IP Address**. Enter the IP address for the guest network. The default IP addresses are as follows:
  - 192.168.1.1
  - 192.168.2.1
  - 192.168.3.1

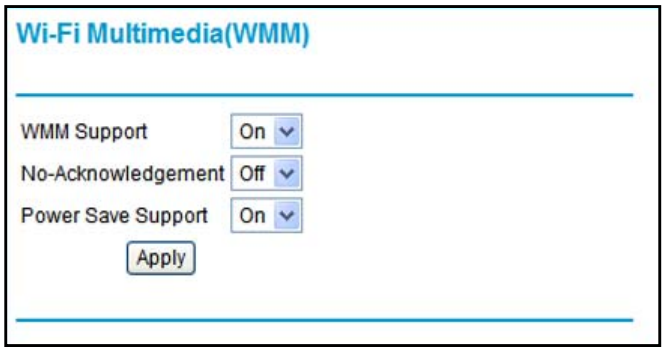
  The subnet mask has a permanent address of 255.255.255.
- **Lease Pool Start** and **Lease Pool End**. Enter the lease pool start and end IP address for the guest network. The default lease pool start IP addresses are as follows:
  - 192.168.1.10 and 192.168.1.99
  - 192.168.2.10 and 192.168.2.99
  - 192.168.3.10 and 192.168.3.99
- **Lease Time**. Enter the lease time for the guest network. The default is 86400 seconds (24 hours).
- **Enable Guest Network** check box.
- **Guest Network Name (SSID)**. You can use this field to change the SSID for the selected guest network.

Set up Wi-Fi Multimedia

Wi-Fi Multimedia (WMM), also referred to as Wireless Multimedia, is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video, audio, or voice have a higher priority than normal traffic.With WMM you can configure quality of service (QoS) to prioritize multimedia traffic in four access categories: voice, video, best effort, and background. For WMM to function correctly, wireless clients have to support WMM.

To configure WMM:

1. Select **Setup > Wi-Fi Multimedia**. The Wi-Fi Multimedia (WMM) screen displays.



2. Enter the following WMM settings:
   - **WMM Support**. Select the WMM mode:
     - **On**. WMM is enabled
     - **Off**. WMM is disabled.
   - **No-Acknowledgement**. When the wireless communication quality is good, you do not need an acknowledgement message (ACK) to confirm the reception of a packet. Disabling acknowledgement messages might improve the efficiency of packet transmission. When the wireless communication quality is poor, enable acknowledgement messages so that you are notified when a package is lost.
     - **On**. Acknowledgement messages are enabled.
     - **Off**. Acknowledgement messages are disabled.
   - **Power Save Support**. Select the power save mode to conserve battery power in smaller devices that are connected to the gateway:
     - **On**. Power save support is enabled.
     - **Off**. Power save support is disabled.
3. Click **Apply** to save your settings.

Content Filtering and Firewall Rules

3

This chapter describes how to use content filtering and firewall rules for the gateway.

This chapter includes:

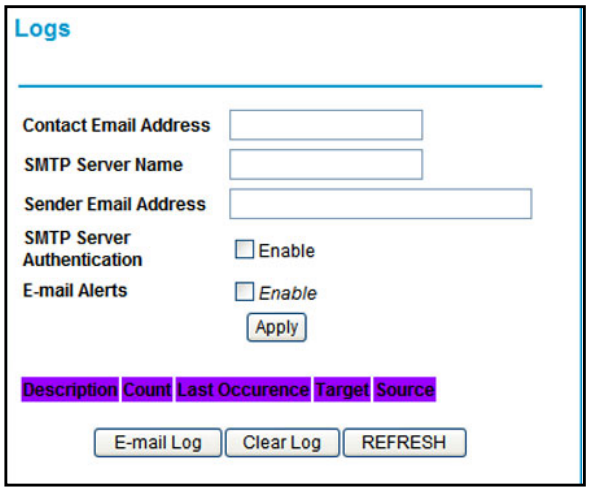
Logs

To access this feature you have to log in to the gateway with the **MSO** user name and its default password **changeme**, or whatever new password you have set up.

A log is a detailed record of the Denial of Service (DoS) attacks directed at your network. You can use e-mail notification to receive these logs in an e-mail message. If you do not have e-mail notification set up you can connect to the gateway to view the logs.

To receive logs or alerts by email:

1. Select **Content Filtering > Logs**. The Logs screen displays.



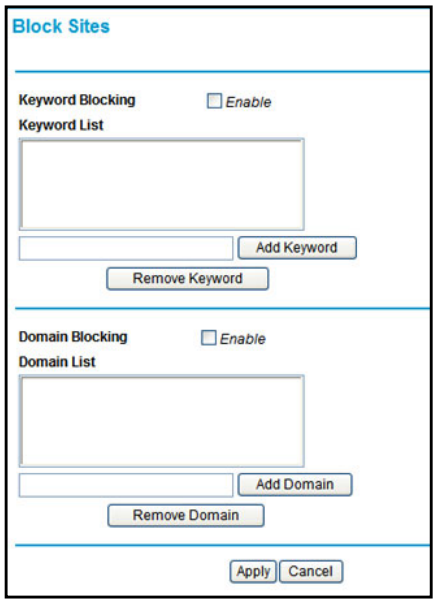
2. Enter the following information:
   - **Contact Email Address**. Enter an email address to which the logs will be sent. Use a full email address (for example, ChrisXY@myISP.com).
   - **SMTP Server Name**. Enter the outgoing SMTP mail server of your ISP (for example, mail.myISP.com). If you leave this box blank, no alerts or logs will be sent.
   - **Sender Email Address**. Enter an e-mail address from which the logs will be sent. Use a full e-mail address (for example, JohnXY@myISP.com).
3. Select the **SMTP Server Authentication** check box if authentication is required.
4. Select the **Email Alerts Enable** check box to activate the e-mail alerts.
5. Click **Apply** to save your settings.

For information about event logs, see *Event Log* on page 36.

Block HTTP Traffic by Keywords or Domains

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

1. Select **Security > Block Sites**.s



2. In the Add Keyword field, enter a keyword and click **Add Keyword**.

   The Keyword List supports up to 32 entries.

3. In the Add Domain field, enter a domain and click **Add Domain**.

   Here are some sample entries:

   - Specify XXX to block http://www.badstuff.com/xxx.html
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov
   - Enter a period (**.**) to block all Internet browsing access.

4. When you are finished making changes, click **Apply**.

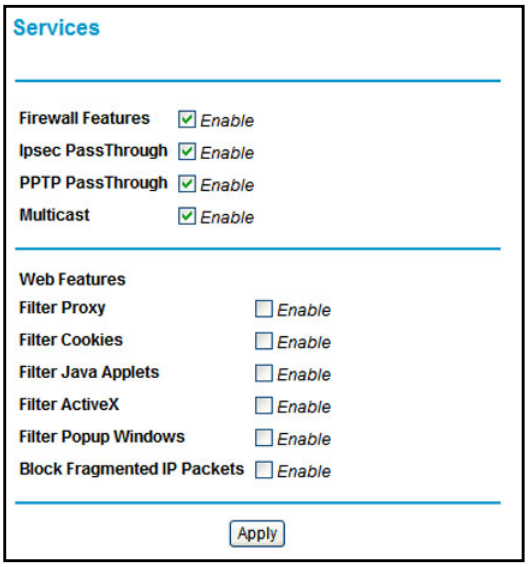
Note: To delete a keyword or domain, select it from the list, click **Remove Keyword** or **Remove Domain**, and then click **Apply**.

Block Services

To access this feature you have to log in to the gateway with the **MSO** user name and its default password **changeme**, or whatever new password you have set up.

You can use the Services screen to control which services are enabled or disabled. To enable or disable certain gateway features and web features:

1. Select **Content Filtering > Services**. The Services screen displays.



2. To enable a service, select its check box. To disable a service, clear its check box.
   - **Firewall Features**. When firewall features are enabled, the gateway performs stateful packet inspection (SPI) and protects against denial of service (DoS) attacks.
   - **Ipsec PassThrough**. When Ipsec passthrough is enabled, IPSec traffic is forwarded. When it is disabled, this traffic is blocked.
   - **PPTP PassThrough**. When PPTP passthrough is enabled, PPTP traffic is forwarded. When it is disabled, this traffic is blocked.
   - **Multicast**. When multicast is enabled, the gateway passes multicasting streams through the firewall.
   - **Web Features**. When enabled, these features are *not* blocked by the firewall. When disabled, these features *are* blocked by the firewall. You can enable or disable each of these features individually.
3. Click **Apply** to save your settings.

Port Forwarding and Port Blocking

A firewall has two default rules, one for inbound traffic (WAN to LAN) and one for outbound traffic.

- Inbound Rules (Port Forwarding)
  These rules restrict access from outsiders. The default rule is to block all access from outside except responses to requests from the LAN side. You can use port forwarding to add predefined or custom rules to specify exceptions to the default rule.
- Outbound Rules (Port Blocking)
  These 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 rules.

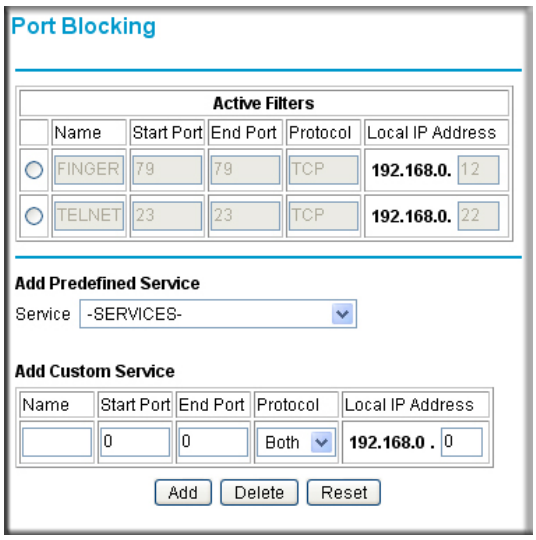
Set Up Port Blocking

You can use port blocking to block outbound traffic on specific ports.

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:

1. Select **Advanced > Port Blocking**. The Port Blocking screen displays.



2. Under Add Predefined Service, select a predefined service from the Service field. (For example, FTP, which uses TCP ports 20 and 21.)

3. As an option, you can also specify a custom rule that is not in the list of predefined services by specifying the following settings in the Add Custom Service 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.

Note: To reset the selection in the Service field and to clear all the fields in the Add Custom Rules table, click **Reset**.

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**.

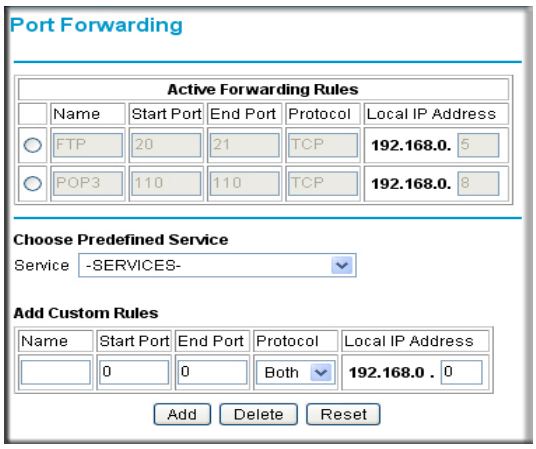
Set Up Port Forwarding

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.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

To configure port forwarding and services for specific inbound traffic:

1. Select **Advanced > Port Forwarding**. The Port Forwarding screen displays.



2. Under Choose Predefined Service, select a predefined service from the Service field. (For example, FTP, which uses TCP ports 20 and 21.)
3. As an option, you can also specify a custom rule that is not in the list of predefined services by specifying the following 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.

Note: To reset the selection in the Service field and to clear all the fields in the Add Custom Rules table, click **Reset**.

4. Perform one of the following actions:
   - Click **Add** to save your settings. The Active Forwarding Rules table now displays the list of ports that are currently forwarded.
   - 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**.

Considerations for Port Forwarding

- If the IP address of the local server PC is assigned by DHCP, it may 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 the rest of your LAN. By default, the IP addresses in the range of 192.168.0.2 through 192.168.0.9 are reserved for this purpose.
- Local PCs 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.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

Set up Port Triggering

Port triggering is an advanced feature that can be used to easily enable gaming and other Internet applications that would otherwise be blocked by the firewall. Using this feature requires that you know the port numbers that are used by the application.

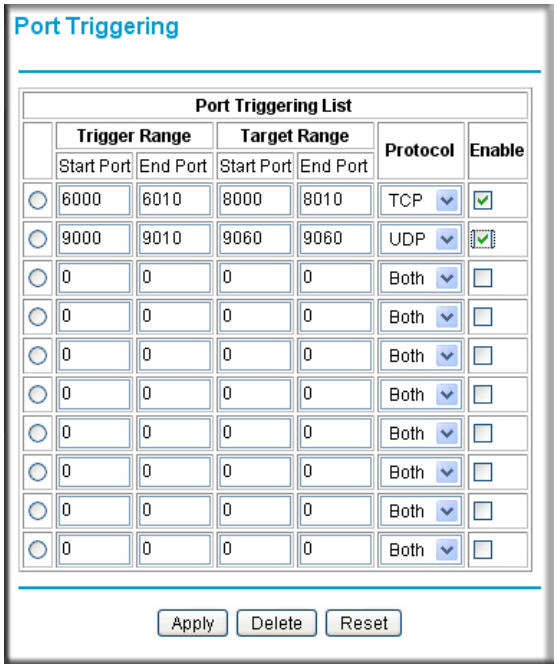
Once set up, port triggering operation is as follows:

1. A PC 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 PC can use a port triggering application at any time. After a PC has finished using a port triggering application, there is a short time-out period before the application can be used by another PC.

To set up port triggering:

1. Select **Advanced > Port Triggering**. The Port Triggering screen displays.



2. For each port trigger that you would like to enable, enter the following settings in the Port Trigger List and enable the port trigger:
   - **Trigger Range**. The trigger range consists of the range of outgoing ports to be monitored to trigger the incoming port forwarding rule:
     - **Start Port**. Enter the start port for the trigger range.
     - **End Port**. Enter the start port for the trigger range.
   - **Target Range**. The target range consists of the range of incoming ports to be opened when triggered:
     - **Start Port**. Enter the start port for the target range.
     - **End Port**. Enter the start port for the target range.
   - **Protocol**. Select the protocol for the ports,:
     - **TCP**. Select TCP only.
     - **UDP**. Select UDP only.
     - **Both**. Select both TCP and UDP.
   - Select the **Enable** check box to activate the port trigger.
3. Perform one of the following actions:
   - Click **Apply** to save your settings and activate the port triggers that you have enabled in **step 2**.
   - Click **Delete** to remove a port trigger that you can select by clicking the radio box next to the port trigger that you want to delete.
   - Click **Reset** to return all trigger and target ranges to their default values of zero.

Managing Your Network

4

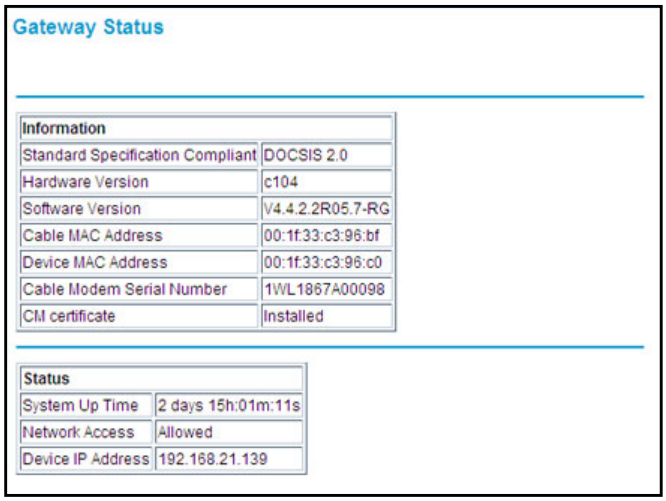
This chapter describes how to perform network management tasks with your Wireless Cable Modem Gateway. When you log in to the gateway, these tasks are grouped under Maintenance.

This chapter includes:

Log in to the gateway using its default address of **http://192.168.0.1** or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or the password you have set up.

Gateway Status

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



The Gateway Status screen fields are explained in the following sections.

Information

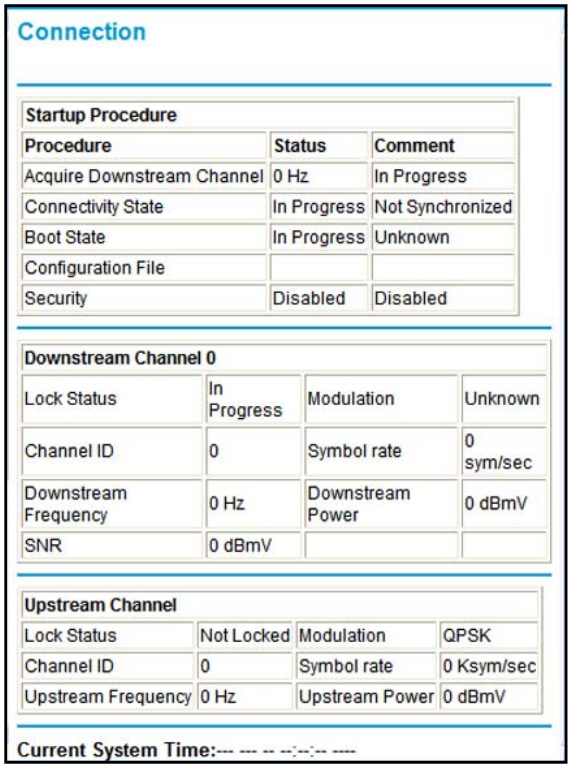
- **Standard Specification Compliant**. The specification to which the gateway's cable interface is compatible.
- **Hardware Version**. The hardware version of the gateway.
- **Software Version**. The software version of the gateway.
- **Cable MAC Address**. The MAC address used by the cable modem port of the gateway. This MAC address may need to be registered with your Cable Service Provider.
- **gatewayCable Modem Serial Number**. The serial number of the gateway.
- **CM certificate**. If the Cable Modem certificate is Installed, it is possible for the service provider to upgrade your Data Over Cable service securely.

Status

- **System Up Time**. This is the time since the gateway has registered with your cable service provider.
- **Network Access**. This field will change to Allowed when the registration with your cable service provider is complete.
- **Device IP Address**. The IP address of your gateway, as seen from the Internet.

Connection Status

Use the Connection screen to track the gateway's initialization procedure, and to get details about the downstream and upstream cable channel. After the cable modem is initialized you can see the current time.



Connection

Startup Procedure		
Procedure	**Status**	**Comment**
Acquire Downstream Channel	0 Hz	In Progress
Connectivity State	In Progress	Not Synchronized
Boot State	In Progress	Unknown
Configuration File		
Security	Disabled	Disabled

Downstream Channel 0			
Lock Status	In Progress	Modulation	Unknown
Channel ID	0	Symbol rate	0 sym/sec
Downstream Frequency	0 Hz	Downstream Power	0 dBmV
SNR	0 dBmV		

Upstream Channel			
Lock Status	Not Locked	Modulation	QPSK
Channel ID	0	Symbol rate	0 Ksym/sec
Upstream Frequency	0 Hz	Upstream Power	0 dBmV

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

This screen shows the progress of the steps that the gateway automatically goes through in the provisioning process:

1. It acquires and locks the downstream channel
2. It acquires the upstream parameters and range.
3. It locks the upstream channel
4. It acquires the IP address through DHCP

Change Passwords

The gateway has two user names and passwords. They are case-sensitive.

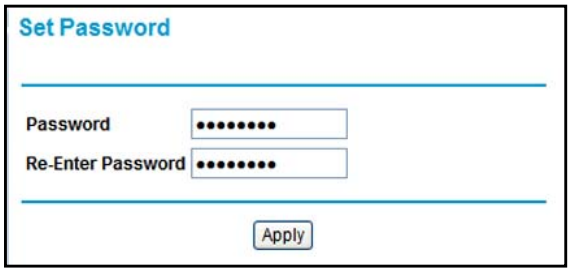
- For superuser access, the user name is **MSO** and its default password is **changeme**.
- For access to all gateway features except content filtering, the user name is **admin** and its default password is **password** for the password, both in lower case letters.

NETGEAR recommends that you change these passwords be more secure. The ideal password should contain no dictionary words from any language, and should be a mixture of

both upper and lower case letters, numbers, and symbols. Passwords can be up to 30 characters.

To change a password:

1. Select **Maintenance > Set Password**. The Set Password screen displays.



2. To change the password, first enter the old password, and then 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.

Reset to Factory Default Settings

You can erase the Gateway configuration and reset it to the factory default settings. For information about the factory default settings, see *Factory Default Settings* in Appendix A. To reset the gateway to its factory settings:

1. In the Set Password screen (see *Figure 1, Select Maintenance > Set Password. The Set Password screen displays.*), to the right of Restore Factory Defaults, select the **Yes** radio button.
2. Click **Apply** to save your changes.

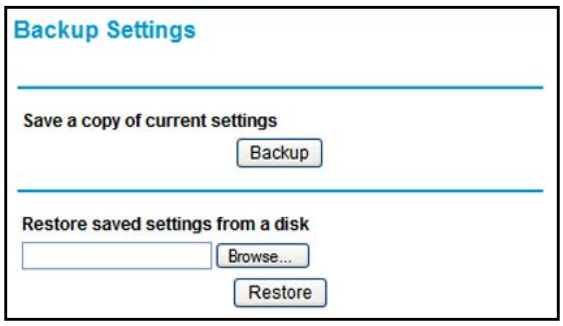
   The gateway reboots automatically. After rebooting, the gateway's password will be **password**, the LAN IP address will be **192.168.1.1**, and the gateway's DHCP client will be enabled.

> **Note:** If you do not know the login password or IP address, you can use the reset button on the rear panel of the gateway to restore the factory default settings. When erasing and resetting the configuration, do not interrupt the process by going on online, turning off the gateway, or shutting down the computer.

Back Up and Restore Your Settings

The configuration settings of the gateway are stored in a configuration file in the gateway. To see the backup settings:

1. Select **Maintenance > Backup Settings**. The Backup Settings screen displays.



You can save a copy of the current configuration settings or restore the saved settings:

2. To save a copy of the current configuration settings, click **Backup**.
3. To restore the saved configuration settings from a backup file:
   a. Click **Browse**.
   b. Locate and select the previously saved backup file (by default, CG2003D.cfg).
   c. Click **Restore**.

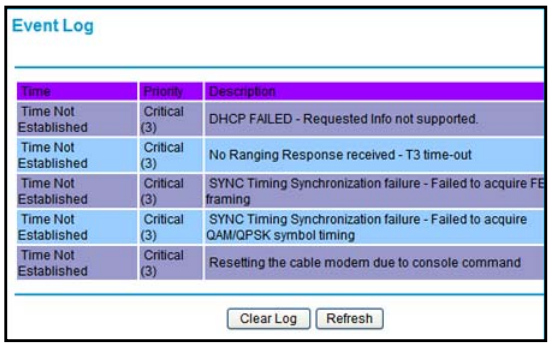
   A message notifies you when the gateway has been restored to previous settings. Then, the gateway restarts, which takes about one minute.

> **Note:** When restoring configuration settings, do not interrupt the process by going on 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. To see the event log:

1. Select **Maintenance > Event Log**. The Event Log screen displays.



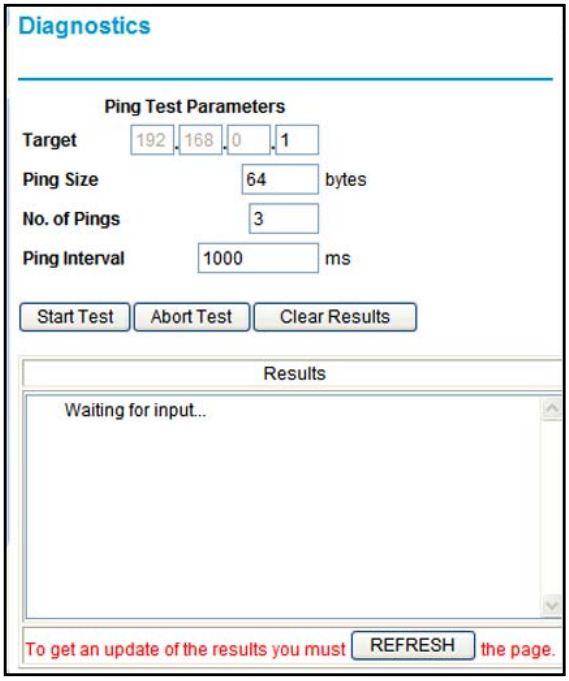
   To clear the log, click **Clear Log**; to refresh the log, click **Refresh**. You can enable email notification to receive these logs in an e-mail message. For information about email notifications, see *Logs* on page 24.

Run the Diagnostic Ping Utility

You can use the Diagnostics screen to test connectivity to a PC using the ping command.

To start a ping test:

1. Select **Maintenance > Diagnostics.** The Diagnostics screen displays.



2. Under Ping Test Parameters, enter the following settings:
   - **Target**. Enter the IP address of the computer that you would like to ping.
   - **Ping Size**. Enter the size of the ping packet.

- **No. of Pings**. Enter the number of times you would like to ping the computer.
- **Ping Interval**. Enter the time you would like to wait between the pings.

3. Click **Start Test**.To stop the test while in progress, click **Abort Test**.
4. To see the results of the ping test, click **REFRESH**. To clear the test results after the test has completed, click **Clear Results**.

Advanced Settings

5

This chapter describes how to customize your network through the advanced settings on your Wireless Cable Modem Gateway. When you log in to the gateway, these tasks are grouped under Advanced.

This chapter includes:

Note: For information about port forwarding and port blocking, see *Chapter 3, Content Filtering and Firewall Rules*.

Log in to the gateway using its default address of **http://192.168.0.1** or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or the password you have set up.

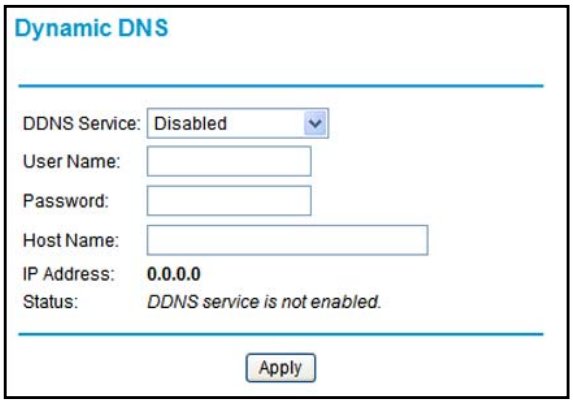
Dynamic DNS

A dynamic DNS service provides a central public database where information (such as e-mail 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.

If you want to use a dynamic DNS service, you have to register for it. The dynamic DNS client service provider will give you a password or key.

To configure dynamic DNS:

1. Select **Advanced > Dynamic DNS**. The DDNS screen displays.



2. Select **www.DynDNS.org** in the DDNS Service drop-down list.
3. Enter the following information:
   - **User Name**. Enter the user name for your dynamic DNS account.
   - **Password**. Enter the password (or key) for your dynamic DNS account.
   - **Host Name**. Enter the host same that your dynamic DNS service provider gave you. (The DDNS service provider may call this the domain name.)
4. Click **Apply** to save your settings.

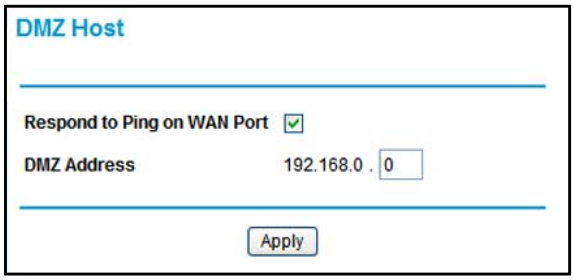
To disable dynamic DNS:

1. In the DDNS Service field, select **Disabled**.
2. Click **Apply** to save your settings.

Set Up a DMZ Host

You can use the DMZ Host screen to set the gateway to respond to a ping and specify a DMZ address. To configure a default DMZ host:

1. Select **Advanced > DMZ Host**. The DMZ Host screen displays.



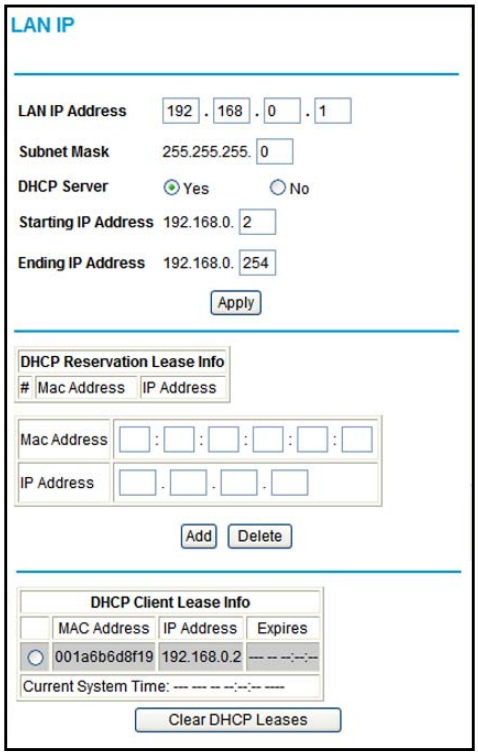
2. If you want the gateway to respond to a ping from the Internet, select the **Respond to Ping on WAN** check box. Responding to pings can be useful in a diagnostic situation.
3. Complete the DMZ IP address in the DMZ Address field to designate a PC that is available to anyone on the Internet for services that you have not defined. Because of security concerns, only do this if you are willing to risk open access. If you do not assign a DMZ address, the gateway discards any undefined service request.
4. Click **Apply** to save your settings.

LAN IP Settings

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

To view or change LAN IP settings:

1. Select **Advanced > LAN IP**. The LAN IP screen displays.



2. Enter the following LAN IP settings:
   - **LAN IP Address**. Enter the LAN IP address that you would like to assign for your gateway in dotted decimal notation. The factory default settings is 192.168.0.1.
   - **Subnet Mask**. Enter 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 gateway is set up by default as a Dynamic Host Configuration Protocol (DHCP) server, which provides the TCP/IP configuration for all the computers that are connected to the gateway. You can change the default setting.
     - **Yes**. Select this settings to enable the DHCP server on the gateway and assign IP addresses to computers on your LAN automatically.
     - **No**. Select this settings to assign IP addresses manually, or if you have another DHCP server on your network.

     If you disable the DHCP server, you will need to assign to your PC a static IP address to reconnect to the gateway and enable the DHCP server again.
   - **Starting IP Address**. Complete the first of the contiguous addresses in the IP address pool. 192.168.0.10 is the default start address.
   - **Ending IP Address**. Complete the last of the contiguous addresses in the IP address pool. 192.168.0.19 is the default end address.
3. Click **Apply** to save your LAN IP settings.

Reserve an IP Address for DHCP Use

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

1. Enter the MAC address of the PC for which you want to reserve an IP address.
2. Enter the permanent IP address for the PC.
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.

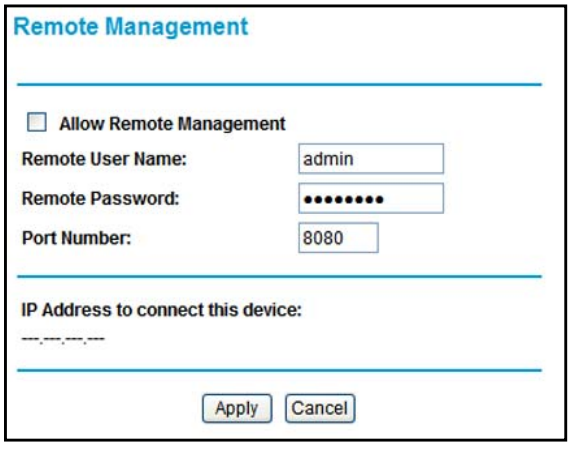
To remove all information from the DHCP Client Lease Info table, click **Clear DHCP Leases**.

Set up 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.

To set up the gateway for remote management:

1. Select **Advanced > Remote Management**. The Remote Management screen displays.



2. Select the **Allow Remote Management** check box.
3. Enter the following information:
   - **Remote Password**. Enter the user name that will be used from the remote PC to manage the gateway. This password is different from the password that you use to log into the gateway from your LAN.

Be sure to change the gateway's remote management password to a very secure password before enabling remote management. The ideal password 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.

- **Port Number**. Specify the port number that will be used for accessing the management interface. The default port number is 80.

  Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click **Apply** to save your changes.

Remote Management After a Reset

If you would like to erase settings but continue to allow access from the WAN after the settings have been erased, select the **Allow Remote Management after Factory Default Reset** check box under "Revert to factory default settings" in the Remote Management screen. Then, click **Erase**.

CAUTION:

Do not attempt to go online, turn off the gateway, shut down the computer, or do anything else to the gateway until the gateway finishes restarting. When the test light turns off, wait a few more seconds before you do anything with the gateway.

After you have erased the gateway's current settings, the gateway's password is password, the LAN IP address is 192.168.0.1, the gateway functions as a DHCP server on the LAN, and as a DHCP client to the Internet.

URL to Connect to The Gateway

To manage the gateway via the Internet, you need its public IP address, as seen from the Internet. This public IP address is allocated by your ISP, and is shown under "IP Address to connect this device" in the Remote Management screen. Note that if your ISP account uses a dynamic IP address instead of a fixed IP address, the address can change each time you connect to your ISP. There are two solutions for this issue:

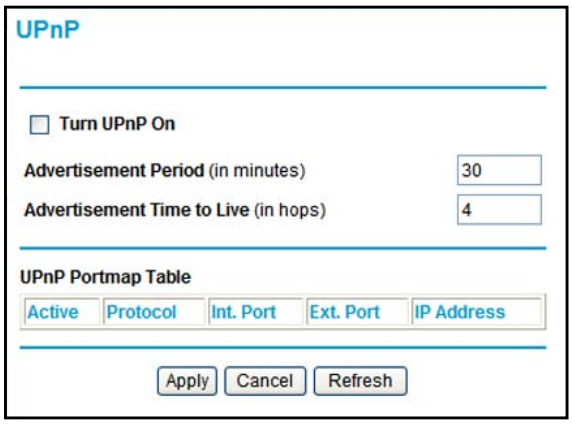
- Be sure that your ISP allocates a fixed IP address for the gateway.
- Use the Dynamic DNS feature so you can connect using a domain name, rather than an IP address. See *Dynamic DNS* on page 40.

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.

To configure UPnP:

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



2. Select the **Turn UPnP On** check box. The default setting is disabled, which prevents the gateway from allowing a device to automatically control resources such as port forwarding.
3. Enter the following information:
   - **Advertisement Period**. Enter how often the gateway broadcasts its UPnP information. The default is 30 minutes.Shorter time periods mean that control points have current device status at the expense of more network traffic. Longer time periods reduce network traffic, but can result in less fresh device status.
   - **Advertisement Time to Live**. Enter the time to live for the advertisement, which is 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.

   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.

Troubleshooting

6

This chapter gives information about troubleshooting your gateway.

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

This chapter includes:

Using LEDs to Troubleshoot

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

1. When power is first applied, verify that the Power LED is on.
2. Verify that the numbered Ethernet LEDs come on momentarily.
3. After a few seconds, verify that the Local port Link LEDs are lit for any local ports that are connected.

The LEDs on the front panel indicate gateway activity and can be used for troubleshooting.

LEDs Stay Off When the Gateway Is Plugged in

- Make sure that the power cord is properly connected to your gateway and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by NETGEAR for this product.
- If the error persists, you have a hardware problem and should contact technical support.

All LEDs Stay On

- Clear the Gateway's configuration to factory defaults. This will set the Gateway's IP address to 192.168.0.1. See *Back Up and Restore Your Settings* on page 36.
- If the error persists, you might have a hardware problem and should contact technical support.

LAN LED Stays Off

If a LAN LED is off for a port with an Ethernet connection, check the following:

- 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.

Cable Link LED Is Off and the Gateway is Cabled to the Wall Jack

- 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 have on your cable line. It might be necessary to run a "home run" back to the point where the cable enters your home.

Cannot Log in to the Gateway

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 *ITCP/IP Networking Basics* 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 *Set up Remote Management* on page 43.
- 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 has two user names both lower-case (**Caps Lock** should be off):
  - The superuser login name is **MSO** with the default password of **changeme**.
  - The other login name is **admin** with 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 Internet 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 you gateway with your cable service provider. This is described in *Cabling the Gateway* on page 8.

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 *ITCP/IP Networking Basics* 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.

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, 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 *The LEDs on the front panel indicate gateway activity and can be used for troubleshooting.* on page 47.
     - 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. See the link to the online document *ITCP/IP Networking Basics* 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 menu.

Technical Specifications and Factory Default Settings

A

This appendix provides technical specifications and default factory settings for the gateway.

Technical Specifications

Table 1. Technical Specifications

Specification		Description
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		• North America (input): 120V, 60 Hz, input • All regions (output): 12 V DC @ 1A output, 12W maximum
Physical Specifications		• Dimensions: 175 by 114 by 30 mm (6.9 by 4.5 by 1.2 in.) • Weight: 0.31 kg (0.68 lb)
Environmental Specifications		• Operating temperature: 32°-140° F (0° to 40° C) • Operating humidity: 90% maximum relative humidity, noncondensing.
Electromagnetic Emissions		Meets requirements of FCC Part 15 Class B
Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx, RJ-45 802.11g and 802.11b Wireless Access Point
	WAN	DOCSIS 2.0. Downward compatible with DOCSIS 1.0 and DOCSIS 1.1.

Table 1. Technical Specifications (Continued)

Specification		Description
Wireless		
	Radio data rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps Auto Rate Sensing
	Frequency	2.4-2.5 GHz
	Operating frequency ranges	2.412~2.462 GHz (US) 2.412~2.472 GHz (Japan) 2.412~2.472 GHz (Europe ETSI)
	Encryption	40-bit (also called 64-bit), 128-bit WEP data encryption, WPA-PSK(TKIP), and WPA2-PSK(AES)

Factory Default Settings

You can use the Restore Factory Settings located on the bottom of your gateway to reset all settings to their factory defaults.

This is called a hard reset. To perform a hard reset, push and hold the reset button for 5 seconds. The gateway reboots and returns to the settings shown in the following table.

Table 2. Default Configuration Settings

Feature		Default Behavior
Gateway Login		
	User login URL	http://192.168.1.1
	User names and passwords (case sensitive)	• MSO/changme • admin/password
Local Network (LAN)		
	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.10
	DHCP Ending IP address	192.168.0.19
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

Table 2. Default Configuration Settings (Continued)

Feature		Default Behavior
Internet Connection		
	WAN MAC address	Use default hardware address
	WAN MTU size	1500
Wireless		
	Wireless communication	Enabled
	SSID name	Wireless
	Security	WEP (Wired Equivalent Privacy) 128-bit encryption
	Broadcast SSID	Enabled
	Transmission speed	Auto[a]
	Country/region	United States (varies by region)
	RF channel	6
	Operating mode	g and b
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless card access list	All wireless stations allowed

a. 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, lower actual data throughput rate.

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.

Table 1.

Document	Link
Using Microsoft Vista and Windows XP to Manage Wireless Network Connections	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
ITCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Notification of Compliance

C

NETGEAR Wireless Routers, Gateways, APs

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.

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Wireless Cable Modem Gateway CG2003D complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, Wireless Cable Modem Gateway CG2003D, 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.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement:

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

This device has been designed to operate with an antenna having a maximum gain of 5.59 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

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 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/*

Table 2. EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, 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 *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, 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 *NETGEAR Inc.* 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 *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* 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 *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Table 2. EDOC in Languages of the European Community

Language	Statement
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* 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 *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

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

Index

M

N

O

P

R

S

T

U

W