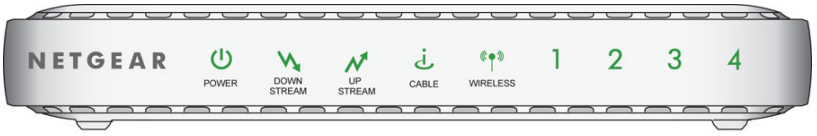
DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 User Manual



NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

202-10509-01
August 2009
v1.0

Technical Support

Please refer to the support information card that shipped with your product. By registering 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. Support Information

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

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, 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

In the interest of improving 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Voluntary Control Council for Interference (VCCI) Statement

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

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

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

EN300 328, EN301 489-17, EN60950

Europe – Declaration of Conformity in Languages of the European Community

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.
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, _e Radiolan spĺňa základné po_iadavky 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.

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., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

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

Grounding

The cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer conductive Shield of a Coaxial Cable.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (DOCSIS 2.0 Advanced Cable Gateway CGD24N v2) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-WG111

Product and Publication Details

Model Number:	CGD24N v2
Publication Date:	August 2009
Product Family:	Gateway
Product Name:	DOCSIS 2.0 Advanced Cable Gateway CGD24N v2
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10509-01
Publication Version Number:	1.0

Contents

DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 User Manual

About This Manual

Conventions, Formats, and Scope xi
Revision History xii

Chapter 1
Connecting the Gateway to the Internet

Package Contents 1-1
Gateway Front Panel 1-1
Gateway Rear Panel 1-3
Side Panel 1-3
Gateway Label 1-4
What You Need Before You Begin 1-4
Logging in to the Gateway 1-5
Configuring the Basic Settings 1-6

Chapter 2
Wireless Configuration

Planning Your Wireless Network 2-1
Wireless Placement and Range Guidelines 2-2
Wireless Security Options 2-3
Manually Configuring Your Wireless Settings and Security 2-3
Configuring WEP (Wired Equivalent Privacy) Wireless Security 2-5
Configuring WPA or WPA2 Wireless Security 2-7
Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security 2-9
Using a WPS Button to Add a WPS Client 2-9
Using a PIN Entry to Add a WPS Client 2-11
Connecting Additional Wireless Client Devices 2-12
Adding Just WPS Clients 2-13
Adding Both WPS and Non-WPS Clients 2-13
Guest Networks 2-13

Configuring a Wireless Guest Network 2-14

Chapter 3
Content Filtering and Firewall Rules

Configuring Logs 3-1
Blocking Site 3-2
Blocking Keywords and Domains 3-3
Blocking Services 3-4

Chapter 4
Managing Your Network

Viewing the Gateway Status 4-1
Viewing the Connection Status 4-3
Changing the Built-In Passwords 4-4
Backing Up and Restoring Your Settings 4-5
Viewing the Event Log 4-6
Running Diagnostic Utilities 4-7

Chapter 5
Customizing Your Network

Advanced Wireless Settings 5-2
Turning on Access Control to Restrict Access by MAC Address 5-3
Restricting Access by MAC Address 5-5
Configuring Port Blocking 5-7
Configuring Port Forwarding 5-9
Considerations for Port Forwarding 5-11
Configuring Port Triggering 5-11
Setting Up a DMZ Host 5-13
Using LAN IP Setup Options 5-14
Using the Gateway as a DHCP Server 5-16
Using Address Reservation 5-17
Enabling Remote Management 5-17
Configuring Universal Plug and Play (UPnP) 5-19

Chapter 6
Troubleshooting

Basic Functions 6-1
Using LEDs to Troubleshoot 6-2
Connecting to the Gateway's Main Menu 6-3

Troubleshooting the ISP Connection 6-4
Troubleshooting a TCP/IP Network Using a Ping Utility 6-4
Testing the LAN Path to Your Gateway 6-4
Testing the Path from Your PC to a Remote Device 6-5

Appendix A
Technical Specifications and Factory Default Settings

Technical Specifications A-1
Factory Default Settings A-2

Appendix B
Related Documents

Index

About This Manual

The *NETGEAR® DOCSIS 2.0 Advanced Cable Gateway CGD24N v2 User Manual* describes how to install, configure and troubleshoot the DOCSIS 2.0 Advanced Cable Gateway CGD24N v2. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions::

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

	**Note:** This format is used to highlight information of importance or special interest.

	**Tip:** This format is used to highlight a procedure that will save time or resources.

	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

- **Scope**. This manual is written for the Advanced Cable Gateway according to these specifications:

Product Version	DOCSIS 2.0 Advanced Cable Gateway CGD24N v2
Manual Publication Date	August 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents."

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/CGD24N v2.asp*.

Revision History

Part Number	Version Number	Date	Description
202-10046-02	1.0	August 2009	Original publication.

Chapter 1
Connecting the Gateway to the Internet

This chapter describes how to set up the gateway on your Local Area Network (LAN), connect to the Internet, and perform basic configuration. For help with installation, see the *Quick Installation Guide* that shipped with your product

Package Contents

The product package contains the following items:

- DOCSIS 2.0 Advanced Cable Gateway CGD24N v2
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- Two brackets
- *Quick Installation Guide*
- *Resource CD*

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

Gateway Front Panel

The front panel of the gateway contains status LEDs.

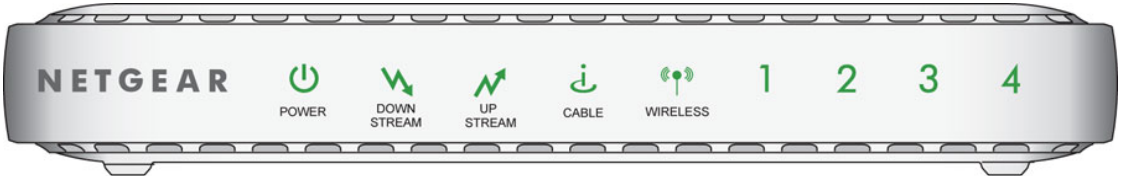


Figure 1-1

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

Table 1-1. LED Descriptions

LED	Description
Power 	• **On**: Power is supplied to the gateway. • **Off**: Power is not supplied to the gateway.
Downstream Traffic 	• **Blink**: Data is being received from the cable interface. • **Off**: The cable interface is idle.
Upstream Traffic 	• **Blink**: Data is being transmitted to the cable interface. • **Off**: The cable interface is idle.
Cable Link 	• **On (green)**: Configuration of the cable interface by your cable service provider is complete. • **Off:** Configuration of the cable interface is still in progress.
Wireless 	• **On**: The wireless access point is operating normally. • **Blink**: Data is being transmitted or received on the wireless interface. • **Fast blink**: The gateway attempts to establish a connection to a wireless client through Wi-Fi Protected Setup (WPS). • **Off**: The wireless access point is disabled.
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 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.

Gateway Rear Panel

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

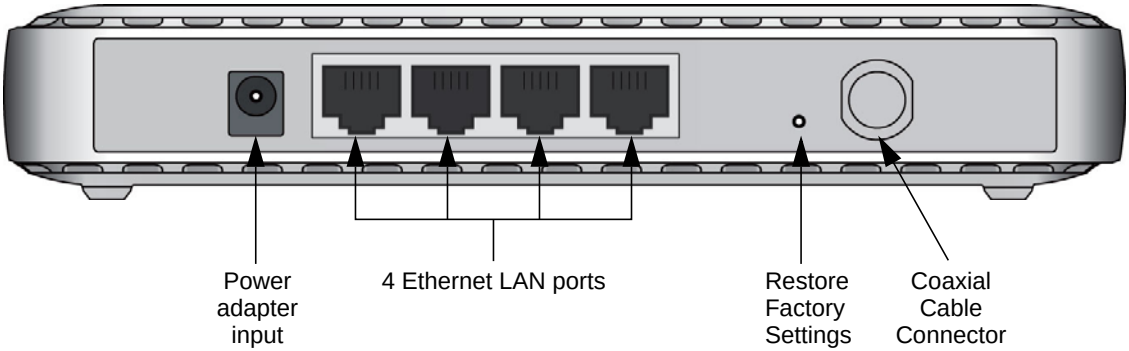


Figure 1-2

The rear panel of the gateway contains a WPS button. You can use the Wi-Fi Protected Setup (WPS) feature with clients on the network that are Wi-Fi certified and WPA capable. See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-8.

Side Panel

On the side panel is the Push 'N' Connect WPS button. Push 'N' Connect (WPS) automatically implements wireless security on the gateway while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-8

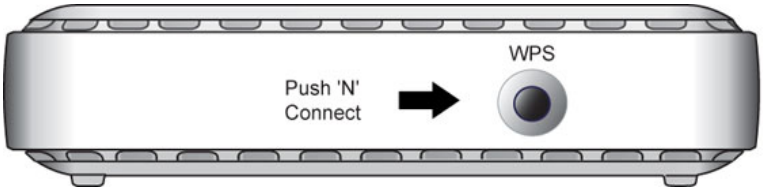


Figure 1-3

What You Need Before You Begin

Before you begin, make sure that you have the following:

- A computer with an active Ethernet port with DHCP enabled.

> **Note:** For help with DHCP configuration, see the link to the online document "ITCP/IP Networking Basics" in Appendix B.

- An active account with your Internet Service Provider (ISP) for data services.
- Depending on how your ISP set up the Internet account, you 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
- Each computer that will connect to the gateway must have an Ethernet Network Interface Card (NIC), USB host port, or 802.11b or 802.11g wireless adapter.

Logging in to the Gateway

Note: To connect to the gateway, your computer must be configured to obtain an IP address automatically via DHCP. For instructions on how to do this, see the link to the online document "Preparing Your Network" in Appendix B.

To log in to the gateway:

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

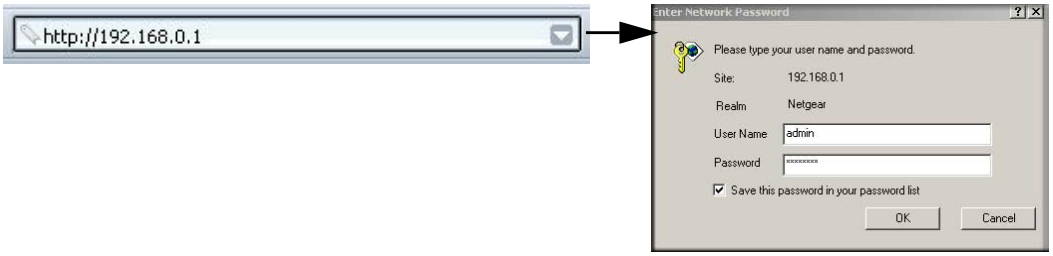


Figure 1-5

The gateway has two user names with passwords:

- To access all features of the gateway, log in with the user name **superuser** and its default password of **password**, both with lower-case letters.
- To access all features of the gateway except content filtering and MAC filtering, log in with the user name **admin** and its default password of **password**.

2. Enter a user name and password to log in to the gateway, both with lower-case letters.

Note: If you cannot connect to the gateway, see "Basic Functions" on page 6-1.

Configuring the Basic Settings

When you log in to the gateway the Basic Settings screen displays:

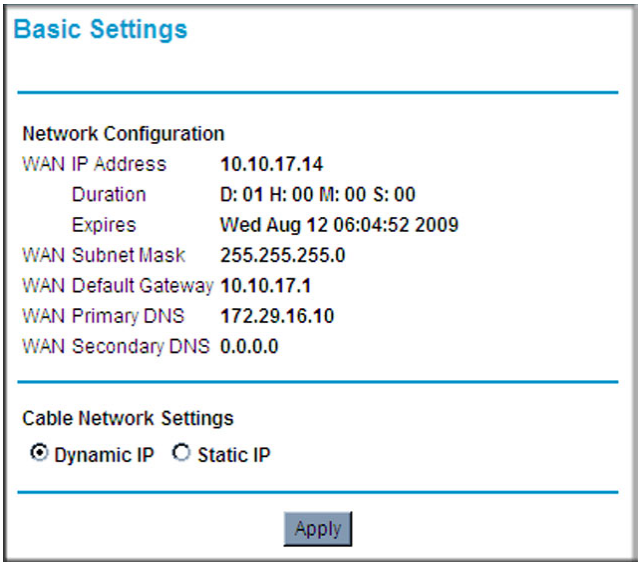


Figure 1-6

1. Make sure that the Cable Network Settings are correct based on the information from your Internet Service Provider (ISP).

   By default, the **Dynamic IP** radio button is selected, which enables the gateway to automatically download the network configuration from your ISP. Select the **Static IP** radio button only if your ISP has assigned you a permanent, fixed (static) IP address. If you select **Static IP**, the screen changes as shown in the following figure:

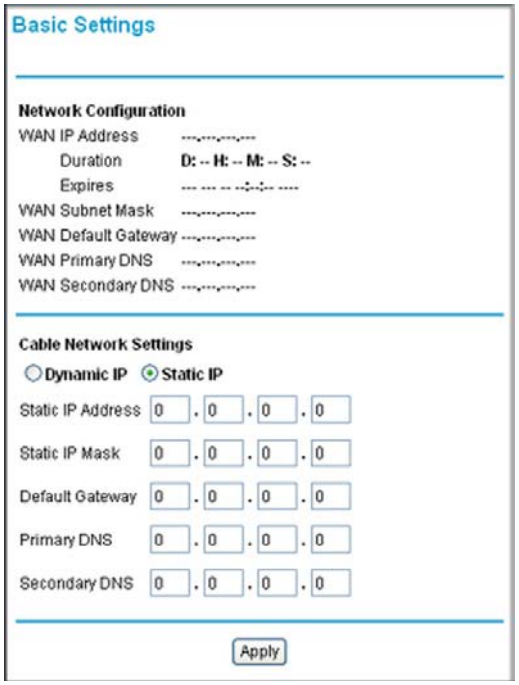


Figure 1-7

2. For a Static IP, enter the following settings to enable the gateway to connect to the Internet:
   - **Static IP Address**. The fixed IP address that your ISP has assigned to you.
   - **Static IP Mask**. The network number portion of an IP address. Unless you are implementing subnetting, use 255.255.0.0 as the subnet mask.
   - **Default Gateway**. This is the ISP's router to which your gateway will connect.
   - **Primary DNS**. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your gateway during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the gateway.
   - **Secondary DNS**. If applicable, enter the address of your ISP's secondary DNS server.
3. Click **Apply** to save your settings. After you have connected to the Internet, the network configuration settings on the Basic Settings screen match the cable network settings.

Chapter 2
Wireless Configuration

For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the gateway and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security. This chapter includes:

- "Planning Your Wireless Network"
- "Manually Configuring Your Wireless Settings and Security" on page 2-3
- "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-9
- "Connecting Additional Wireless Client Devices" on page 2-12
- "Guest Networks" on page 2-13

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the gateway is NETGEAR.
  - The wireless mode (802.11g, or 802.11b) that each wireless adapter supports.
  - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

  See "Manually Configuring Your Wireless Settings and Security" on page 2-3.
- Push 'N' Connect (WPS) automatically implements wireless security on the gateway while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the gateway, clicking an onscreen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

To set up your wireless network using the WPS feature:

– Use the WPS button on the rear panel of the gateway (there is also an onscreen WPS button), or enter the PIN of the wireless device.

– Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

See "Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security" on page 2-9.

Wireless Placement and Range Guidelines

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 PCs 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.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (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 placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Advanced Cable Gateway provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

For more information about wireless technology, see the link to the online document in "Wireless Networking Basics" in Appendix B.

Manually Configuring Your Wireless Settings and Security

You can view or manually configure the wireless settings for the gateway in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.

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

To view or manually configure the wireless settings:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Setup, select Wireless Settings. If you make changes, you must click **Apply** for them to take effect

Figure 2-1

Table 2-1. Wireless Settings

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. The characters are case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a wireless network must use the SSID.
	Region	Specify the region where the gateway will operate.
	Channel	The wireless channel used by the gateway. The default is channel 1. You should not need to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best.
	802.11 Mode	802.11b/gNext 2.4 GHz, Auto, 40 MHz?
Security Options	You can manually configure wireless security here. • **Disable**. Wireless security is disabled by default. After the gateway is connected to the Internet, NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy) 64-bit encryption or 128-bit encryption**. WEP provides data security with WEP Shared Key authentication and WEP data encryption. You can select 64-bit or 128-bit encryption. See “Configuring WEP (Wired Equivalent Privacy) Wireless Security” on page 2-5. • **WPA-PSK**. WPA-PSK uses the TKIP encryption type with authentication from a RADIUS server. • **WPA2-PSK**. WPA2-PSK uses the AES encryption type with authentication from a RADIUS server. • **WPA**. Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. . • See “Configuring WPA or WPA2 Wireless Security” on page 2-7.	

Configuring WEP (Wired Equivalent Privacy) Wireless Security

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the gateway from a wired computer to make further changes.

To configure WEP data encryption:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Setup, select **Wireless Settings**.
3. By default, WEP is selected in the Security Options section of the screen.

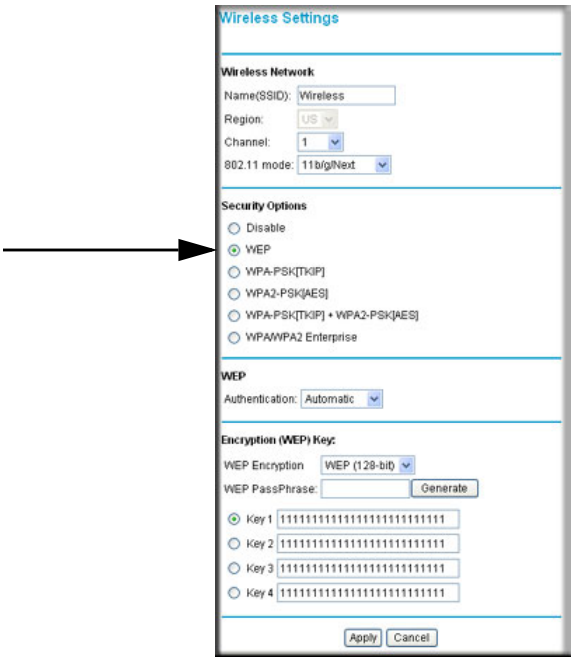


Figure 2-2

4. Depending on the encryption strength that you want, select one of these options:
   - **WEP (Wired Equivalent Privacy) 128-bit encryption**
   - **WEP (Wired Equivalent Privacy) 64-bit encryption**
5. Enter the WEP encryption key information:
   - **WEP PassPhrase**: To use a passphrase to automatically generate the keys, enter a passphrase and click **Generate**. Wireless stations must use the passphrase or keys to access the gateway.
   - **Key 1** through **Key 4**: You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. 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 of the four keys will be the default. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.

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

Configuring WPA or WPA2 Wireless Security

	Note: Newer wireless adapters support WPA. Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA. Consult the product documentation for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA in the gateway:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Setup, select Wireless Settings.
3. Select a WPA setting:

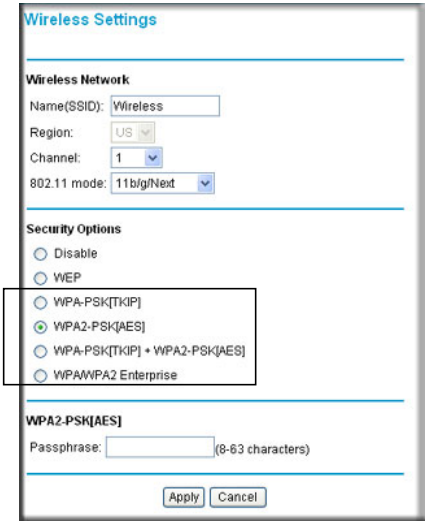


Figure 2-3

- **WPA-PSK [TKIP]**. TKIP encryption type and a pre-shared key passphrase.
- **WPA2-PSK [AES]**. AES encryption type and a pre-shared key passphrase.

- **WPA-PSK [TKIP] + WPA2-PSK [AES]**.
- **WPA/WPA2 Enterprise**. TKIP encryption type with authentication from a RADIUS server.

The content displayed in the screen depends on the WPA setting that you selected.

4. 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.
   - For WPA, enter the settings for the RADIUS Server:
     - **Primary Radius Server IP Address**. The IP address of the RADIUS server. The default is 0.0.0.0.
     - **Radius Port**. Port number of the RADIUS server. The default is 1812.
     - **Shared Key**. This is shared between the wireless access point and the RADIUS server while authenticating the supplicant.
5. Click **Apply** to save your settings.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the gateway's SSID and security settings and, at the same time, connect the wireless client securely and easily to the gateway. Look for the  symbol on your client device (computers that will connect wirelessly to the gateway are clients). WPS automatically configures the network name (SSID) and wireless security settings for the gateway (if the gateway is in its default state) and broadcasts these settings to the wireless client.

Note: NETGEAR's Push 'N' Connect feature based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.

- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices. See "Adding Both WPS and Non-WPS Clients" on page 2-13.

A WPS client can be added using the Push Button method or the PIN method.

- **Using the Push Button**. This is the preferred method. See the following section, "Using a WPS Button to Add a WPS Client.
- **Entering a PIN**. For information about using the PIN method, see "Using a PIN Entry to Add a WPS Client" on page 2-11.

Using a WPS Button to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the gateway wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

	**Note:** By default, the gateway is configured with WEP security, which is incompatible with WPS. If WEP is configured when you add a WPS client, the gateway will change the wireless security to WPA-PSK [TIP] + WPA2-PSK [AES] when it adds the client.

To use the gateway WPS button to add a WPS client:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. On the main menu, select Add WPS Client and click **Next**.

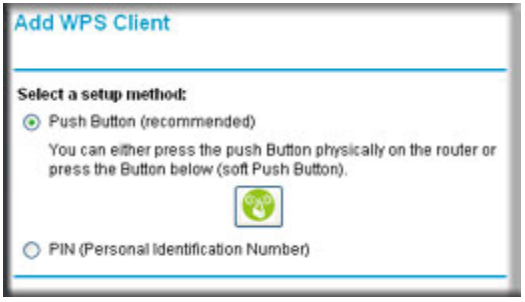


Figure 2-4

By default, **Push Button** is selected as the setup method.

3. Either push the WPS button on the side of your gateway or click the onscreen button.The screen displays the progress as the gateway tries to communicate with the client for 2 minutes:

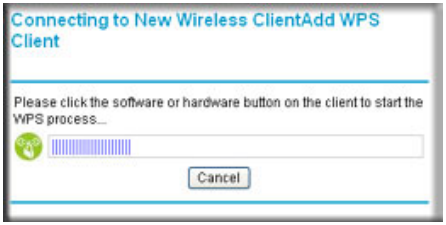


Figure 2-5

While the gateway tries to establish a connection, you can stop the process by clicking **Cancel**.

4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
5. Go back to the gateway screen and check the display:
   - **Success**. A connection is established. The gateway has generated an SSID, implemented WPA/WPA2 wireless security (including a PSK security password) on the gateway, and has sent this configuration to the wireless client.
   - **Failure**. No connection is detected, and no SSID or security settings are configured on the gateway.

   Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See "Manually Configuring Your Wireless Settings and Security" on page 2-3.

To access the Internet from any computer connected to your gateway, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the gateway's Internet LED blink, indicating communication to the ISP.

Using a PIN Entry to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the gateway wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

	Note: By default, the gateway is configured with WEP security, which is incompatible with WPS. If WEP is configured when you add a WPS client, the wireless security changes to WPA-PSK [TIP] + WPA2-PSK [AES] when the client is added.

To use a PIN to add a WPS client:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Setup, select Add WPS Client, and then click **Next**.

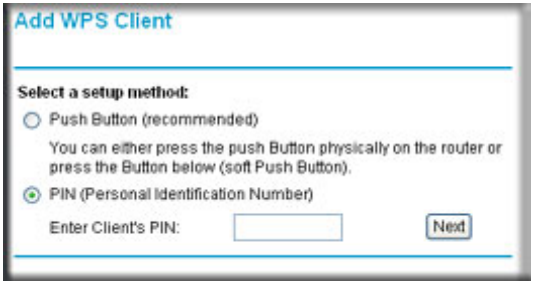


Figure 2-6

3. Select the **PIN (Personal Identification Number)** radio button and then click **Next**.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. Enter the client's PIN in the Add WPS Client screen of the gateway and then click **Next**.
   - The screen displays the progress as the gateway tries to communicate with the client for 4 minutes.
   - While the gateway attempts to establish a connection, you can stop this process by clicking **Cancel**.
6. Go back to the gateway screen and check the WPS status:
   - **Success**. A connection is established. The gateway has generated an SSID, implemented WPA/WPA2 wireless security (including a PSK security password) on the gateway, and has sent this configuration to the wireless client.
   - **Failure**. No connection is detected, and no SSID or security settings are configured on the gateway.

   Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See "Manually Configuring Your Wireless Settings and Security" on page 2-3.

To access the Internet from any computer connected to your gateway, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the gateway's Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute timeframe, the SSID will not be changed and no security will be implemented on the gateway.

Connecting Additional Wireless Client Devices

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Adding Just WPS Clients

To add a wireless client device that is WPS-enabled, follow the procedures in "Using a WPS Button to Add a WPS Client" on page 2-9 or "Using a PIN Entry to Add a WPS Client" on page 2-11.

Adding Both WPS and Non-WPS Clients

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see "Manually Configuring Your Wireless Settings and Security" on page 2-3).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the gateway:

1. Restore the gateway to its factory default settings (press the Restore Factory Settings button on the rear panel of the gateway for 5 seconds).

   When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the gateway.

2. Configure the network name (SSID), select the WPA/PSK [TKIP] + WPA2/PSK[AES] radio button on the Wireless Settings screen (see "Manually Configuring Your Wireless Settings and Security" on page 2-3). and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.

3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).

4. For the WPS devices that you want to connect, follow the procedure "Using a WPS Button to Add a WPS Client" on page 2-9 or "Using a PIN Entry to Add a WPS Client" on page 2-11.

The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the gateway.

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 configure up to three wireless guest networks and specify the security options for each wireless guest network.

Configuring a Wireless Guest Network

To configure a wireless guest network:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Setup, select Guest Network. The Wireless Guest Network Settings screen displays:

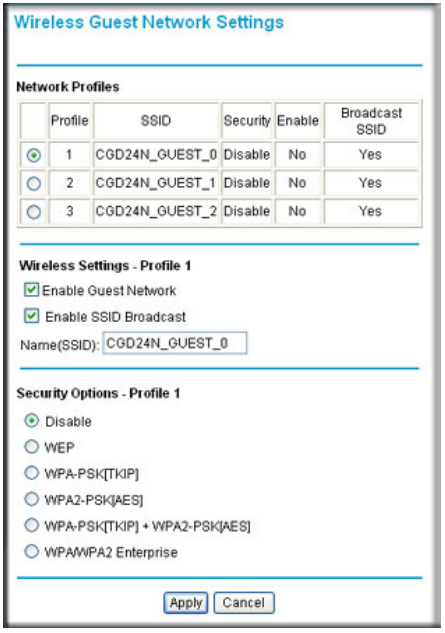


Figure 2-7

3. Select the **Enable Guest Network** check box. The **Enable SSID Broadcast** check box will be automatically selected.

4. Fill in the **Name (SSID)** field. You can enter a value of up to 32 alphanumeric characters. For the guest network, the same name must be assigned to all wireless devices in your network. The name is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.
5. At the bottom of the screen, click **Apply** to enable the selected guest network.
6. Configure wireless security for the guest network.

   This process that is very similar to configuring wireless security for the gateway. For more information, see "Configuring WEP (Wired Equivalent Privacy) Wireless Security" on page 2-5 and "Configuring WPA or WPA2 Wireless Security" on page 2-7.

Note: The **Restore Guest Defaults** button allows you to erase the changes made in this screen and return the settings to their factory defaults.

Chapter 3
Content Filtering

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

	Note: 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. To access the content filtering features you must log in to the gateway with the **mso** user name and its default password **changeme**, or whatever new password you have set up.

This chapter includes:

- "Configuring Logs" on this page
- "Blocking Sites" on page 3-2
- "Blocking Services" on page 3-4

Configuring Logs

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 by e-mail:

1. In the main menu, under Content Filtering, select Logs. The Logs screen displays:

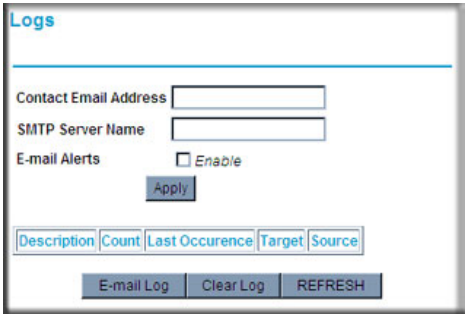


Figure 3-1

2. Enter the following information:
   - **Contact Email Address**. Enter an e-mail address to which the logs will be sent. Use a full e-mail 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 **E-mail Alerts Enable** check box to activate the e-mail alerts.
4. Click **Apply** to save your settings.

For information about event logs, see "Viewing the Event Log" on page 4-6.

Blocking Sites

The gateway provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the gateway prevents objectionable content from reaching your PCs. The gateway allows you to control access to Internet content by screening for keywords within Web addresses. It also has the capability to block access to all sites except those that are explicitly allowed.

Key content filtering options include:

- Blocking access from your LAN to Internet locations that contain keywords that your specify.
- Blocking access to websites that you specify as off-limits.
- Allowing access to only websites that you specify as allowed.

Blocking 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.

To block keywords and domains:

1. In the main menu, under Content Filtering, select Block Sites. The Block Sites screen displays.

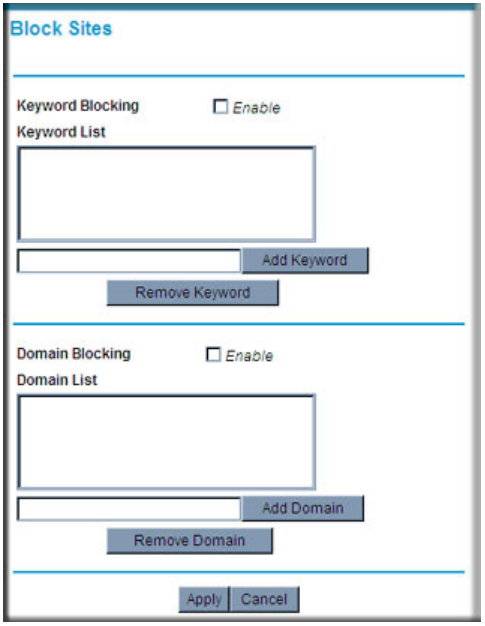


Figure 3-2

2. To use keyword blocking, select the **Keyword Blocking Enable** check box. You can enter up to eight keywords. After you have entered a keyword in the field to the left of the Add Keyword button, click **Add Keyword**. The keyword will be shown in the Keyword List.

   Note the following:

   - 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 the keyword, and then click **Remove Keyword**.

3. You can use the Domain List to create a list of allowed domains, or to create a list of denied domains. To use domain blocking, select the **Domain Blocking Enable** check box. After you have entered a domain in the field to the left of the Add Domain button, click **Add Domain**. The domain will be shown in the Domain List.

   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.

Blocking Services

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. In the main menu, under Content Filtering, select Services. The Services screen displays.

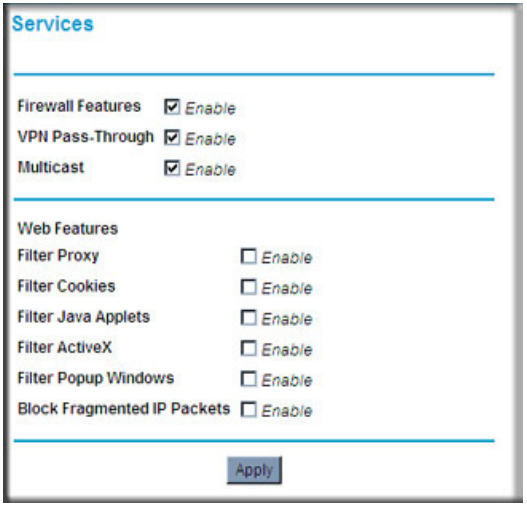


Figure 3-3

2. To enable a service, select its check box. To disable a service, clear its check box. The following table describes the services.

Table 3-1. Services

Settings	Description
Firewall Features	When firewall features are enabled, the gateway performs stateful packet inspection (SPI) and protects against denial of service (DoS) attacks.
VPN Pass Through	When VPN passthrough is enabled, IPSec and PPTP traffic are forwarded. When it is disabled, this traffic is blocked.

Table 3-1. Services (continued)

Settings		Description
Multicast		When multicast is enabled, the gateway passes multicasting streams through the firewall.
Web Features	Filter Proxy	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.
	Filter Cookies	
	Filter Java Applets	
	Filter ActiveX	
	Filter Popup Windows	
	Block Fragmented IP Packets	

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

Chapter 4
Managing Your Network

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

This chapter includes:

- "Viewing the Gateway Status"
- "Viewing the Connection Status" on page 4-3
- "Changing the Built-In Passwords" on page 4-4
- "Backing Up and Restoring Your Settings" on page 4-5
- "Viewing the Event Log" on page 4-6
- "Running Diagnostic Utilities" on page 4-7

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.

Viewing the Gateway Status

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

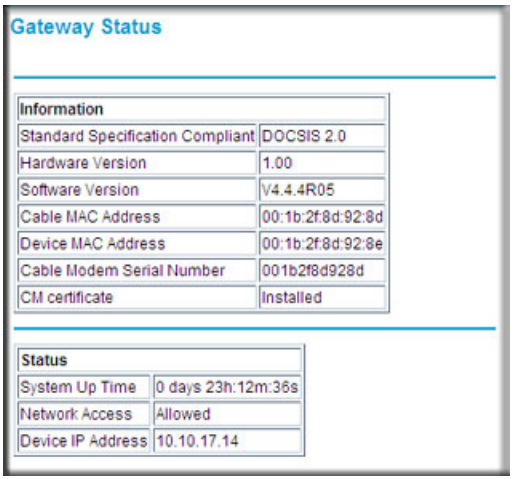


Figure 4-1

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

Table 4-1. Gateway Status Fields

Field		Description
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 Modem 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 of the router side of the gateway. This is the equivalent of your PC when connected to a cable modem. You can use the MAC Cloning feature to replace this MAC address with another address when sending packets to the WAN.
	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.

Table 4-1. Gateway Status Fields (continued)

Field		Description
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 you gateway, as seen from the Internet.

Viewing the 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.

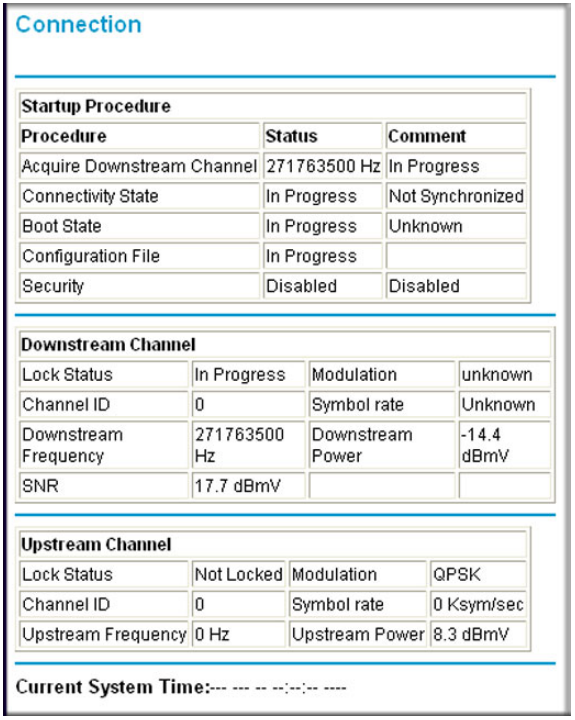


Figure 4-2

The gateway automatically goes through the following steps 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

Changing the Built-In Passwords

For security reasons, the gateway has its own user names and passwords. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect.You can use procedures below to change the gateway's passwords.

Note: The user names and passwords are not the same as any user name or password you may use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. 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. Your password can be up to 30 characters.

To change the password:

1. 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.

The gateway has two user names with passwords:

- To access all features of the gateway, log in with the user name **superuser** and its default password of **password**, both with lower-case letters.
- To access all features of the gateway except content filtering and MAC filtering, log in with the user name **admin** and its default password of **password**.

2. In the main menu, under Maintenance, select **Set Password**. The Set Password screen displays.

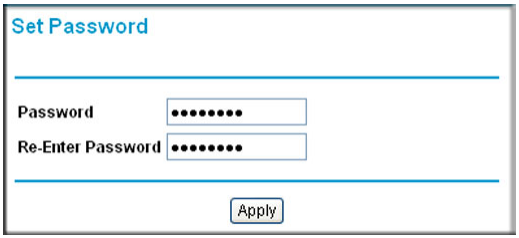


Figure 4-3

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

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

Backing Up and Restoring Your Settings

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

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Maintenance, select **Backup**. The Backup Settings screen displays.

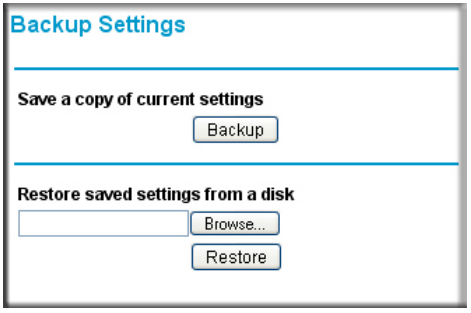


Figure 4-4

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

- To save a copy of the current configuration settings, click **Backup**.
- To restore the saved configuration settings from a backup file:

  a. Click **Browse**.

  b. Locate and select the previously saved backup file (by default, CGD24G-100NAS.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.

Viewing the Event Log

The gateway logs security-related events such as denied incoming service requests and hacker probes. To see the event log:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Maintenance, select **Event Log**. The Event Log screen displays.

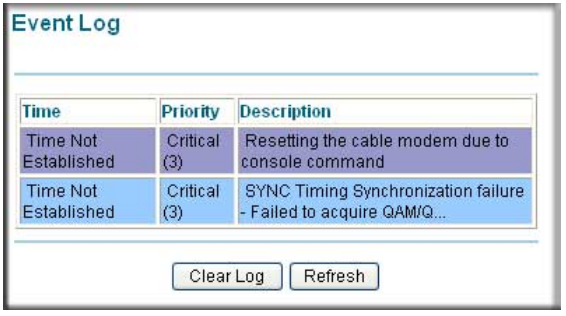


Figure 4-5

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

Running the Ping Diagnostic Utility

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

To start a ping test:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Maintenance, select **Diagnostics**. The Diagnostics screen displays.

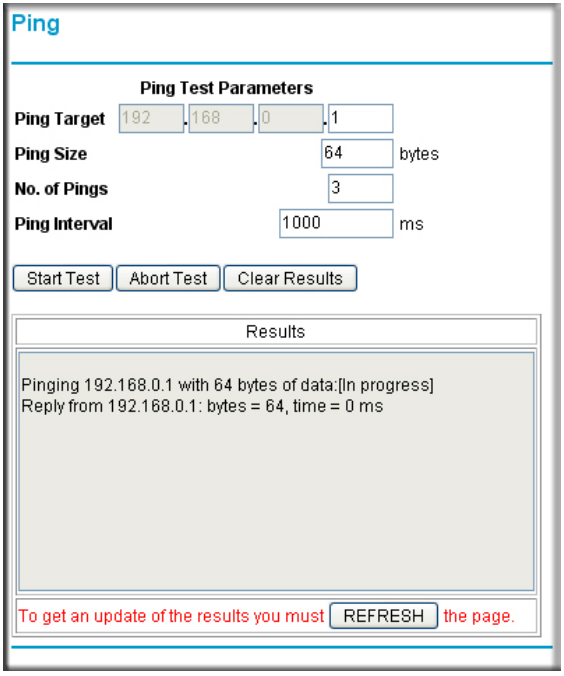


Figure 4-6

3. Under Ping Test Parameters, enter the following settings:
   - **Ping 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.
4. Click **Start Test**.To stop the test while in progress, click **Abort Test**.
5. To see the results of the ping test, click **REFRESH**. To clear the test results after the test has completed, click **Clear Test**.

Chapter 5
Customizing Your Network

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

Note: To access the MAC Filtering feature you must log in with the user name **superuser.** For all other advanced features you can log in with the user name **admin**. See "Logging in to the Gateway" on page 1-5

This chapter includes:

- "Advanced Wireless Settings
- "Restricting Access by MAC Address" on page 5-5
- "Configuring Port Blocking" on page 5-7
- "Configuring Port Forwarding" on page 5-9
- "Configuring Port Triggering" on page 5-11
- "Setting Up a DMZ Host" on page 5-13
- "Using LAN IP Setup Options" on page 5-14
- "Enabling Remote Management" on page 5-17
- "Configuring Universal Plug and Play (UPnP)" on page 5-19

Configuring Advanced Wireless Settings

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. From the main menu, below the Advanced heading, select Wireless Settings to display the Advanced Settings screen:

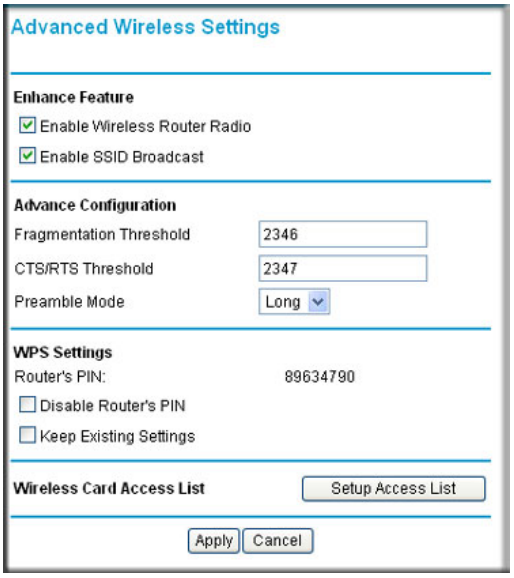


Figure 5-1

For information about setting up an access list, see "Turning on Access Control to Restrict Access by MAC Address" on page 5-3.

3. If you make changes in this screen you must click **Apply** for them to take effect.

Table 5-1. Advanced Wireless Settings

Advanced Wireless Settings		Description
Wireless Access Point (Enhanced Features)	Enable Wireless Access Point	On by default, 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 Broadcast Name (SSID)	On by default, the gateway broadcasts its SSID so that it is easier to identify the correct wireless network from a wireless station. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.

Table 5-1. Advanced Wireless Settings

Advanced Wireless Settings		Description
Advanced Configuration	• Fragmentation Threshold • CTS/RTS Threshold • Preamble Mode	The default settings for these fields usually work fine. Change them only if you have a specific reason for doing so.
WPS Settings	Disable Router's PIN	Selecting this checkbox disables the PIN that WPS clients use to connect to the gateway with the PIN method. Normally this checkbox is cleared, which is the default setting.
	Keep Existing Settings	If a WPS client is added the gateway automatically selects this checkbox. When the Keep Existing Settings checkbox is selected, the SSID and wireless security settings remain the same when additional WPS clients are added.
Wireless Card Access List	Set up Access List	Access control is disabled by default so that any computer that is configured with the correct SSID can connect. For information about access control, see the following section "Turning on Access Control to Restrict Access by MAC Address .

Turning on Access Control to Restrict Access 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.

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

You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Advanced Cable Gateway. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

To restrict access based on MAC addresses:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.

2. In the main menu, under Advanced, select Wireless Settings.

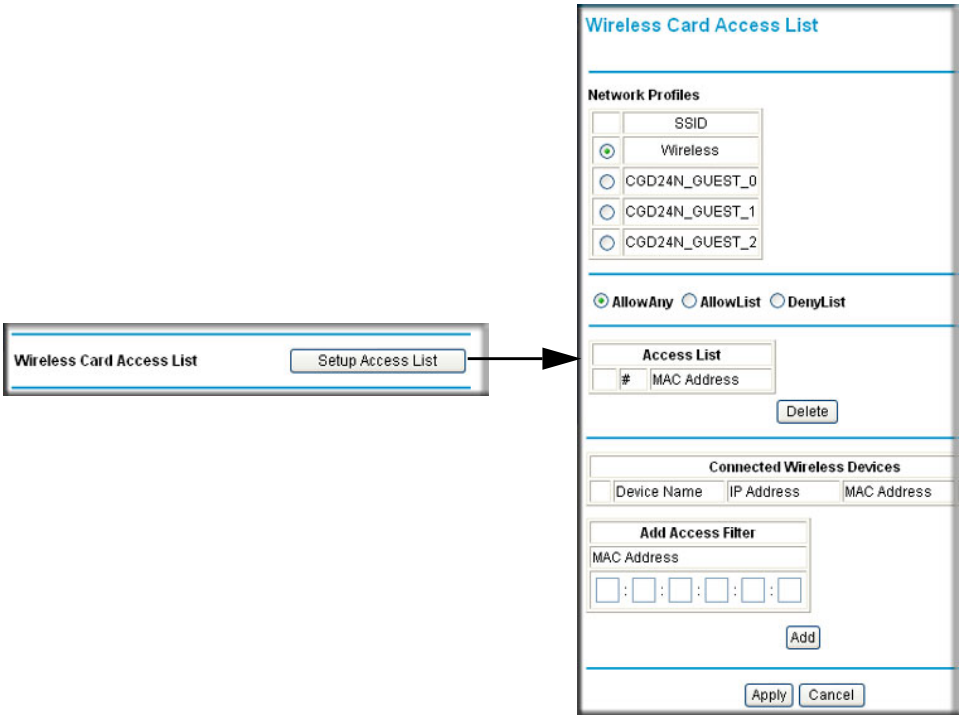


Figure 5-2

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.

The Access List table displays a list of wireless clients that will have access to the wireless network when the list is enabled.

4. Adjust the access list as needed for your network. You can add a devices to the access list using either one 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 to be added to the access list in the Add Access Filter fields. The MAC address can usually be found on the bottom of the wireless device. Then click **Add**.

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

Restricting Access by MAC Address

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

To configure MAC filtering:

1. In the main menu, under Advanced, select MAC Filtering. The MAC Filtering screen displays.

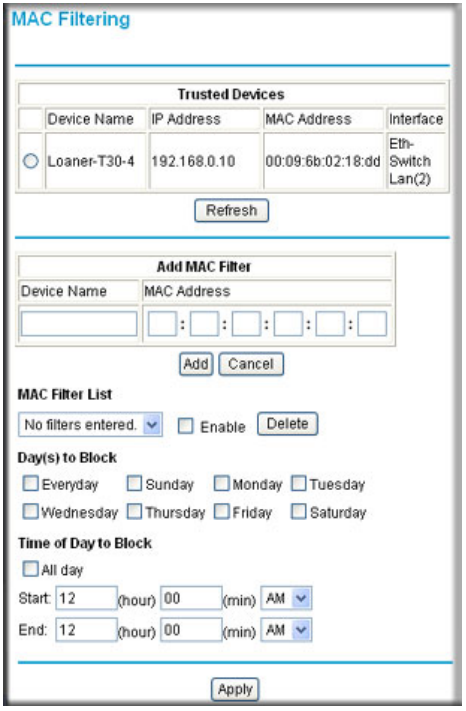


Figure 5-3

The Trusted Devices table shows the PCs that are allowed access to the Internet through the gateway. Click **Refresh** to update the Trusted Devices table.

2. Select a device that will be added to the Add MAC Filter table through one of the following methods:
   - If the PC that you want to block appears in the Trusted Devices table, click the radio button for that PC to capture its MAC address in the Add MAC Filter table. If a MAC address but no device name appears in the Add MAC Filter table, you can type a descriptive name for the PC that you are adding to the table.
   - Manually enter the device name and MAC address of the PC you want to block to the Add MAC Filter table.
3. To add the device that you selected in step 2 to the MAC Filter List, click **Add**. When you do so, the **Enable** check box is automatically selected for that PC. Also note the following:
   - To deselect a PC from the MAC Filter List, select the PC from the drop-down list, and then clear its **Enable** check box. Doing so leaves the PC in the MAC Filter List but ensures that the PC is not blocked.
   - To remove a PC from the MAC Filter List, select the PC from the drop-down list, and then click **Delete**.
4. Select the days and times that a selected PC will be blocked:
   a. **Day(s) to Block**. Select the days on which the PC that is selected in the MAC Filter List will be blocked. The default is Everyday.
   b. **Time of Day to Block**. Select a start time and an end time to specify a period during which the PC that is selected in the MAC Filter List will be blocked. The default is All Day. Be sure that you deselect the **All Day** check box if you want to enter specific times. The selected period applies to each day that you selected in the previous step.
5. Click **Add** to save your settings.
6. Repeat step 2 through step 5 for all PCs that you want to block.

Configuring Port Blocking

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

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. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Advanced, select Port Blocking. The Port Blocking screen displays.

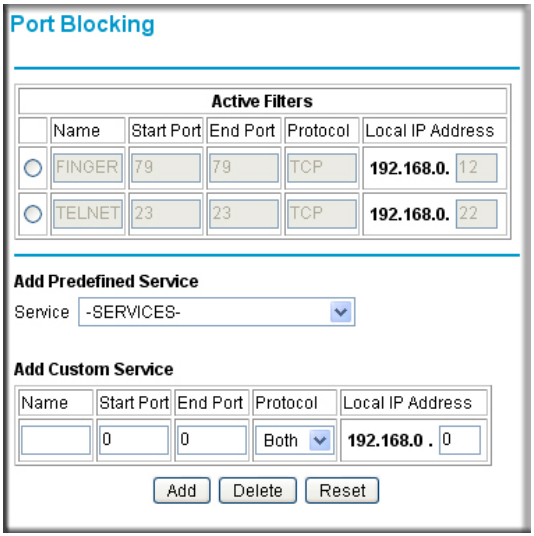


Figure 5-4

3. Under Add Predefined Service, select a predefined service from the Services pull-down menu. (For example, FTP, which uses TCP ports 20 and 21.)
4. 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**. Enter the local IP address for the computer that is using the service.

	**Note:** To reset the selection in the Services pull-down menu and to clear all the fields in the Add Custom Rules table, click **Reset**.

5. 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**.

Configuring Port Forwarding

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

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. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Advanced, select Port Forwarding. The Port Forwarding screen displays.

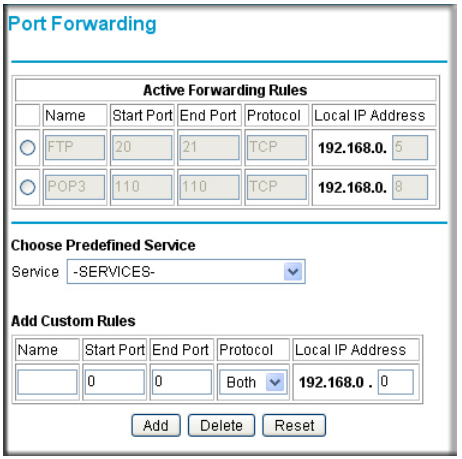


Figure 5-5

3. Under Choose Predefined Service, select a predefined service from the Services pull-down menu. (For example, FTP, which uses TCP ports 20 and 21.)
4. 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 **Services** field and to clear all the fields in the Add Custom Rules table, click **Reset**.

5. 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 must access the local server using the PCs' local LAN address (192.168.0.XXX, by default). Attempts by local PCs to access the server using the external WAN IP address will fail.

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

Configuring 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.

	Note: For information about port blocking and port forwarding, see "Configuring Port Blocking" on page 5-7and "Configuring Port Forwarding" on page 5-9..

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 configured, 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 configure port triggering:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.

2. In the main menu, under Advanced, select Port Triggering to display the following screen:

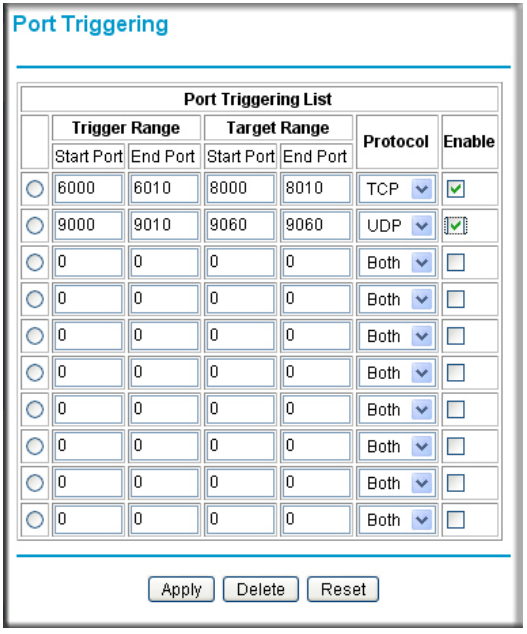


Figure 5-6

3. 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 that will 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 that will 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.
   - Click the **Enable** check box to activate the port trigger.
4. Perform one of the following actions:
   - Click **Apply** to save your settings and activate the port triggers that you have enabled.
   - Click **Delete** to remove a port trigger that you can select by clicking the radio button for the port trigger that you want to delete.
   - Click **Reset** to return all trigger and target ranges to their default values of zero.

Setting 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. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Advanced, select DMZ Host. The DMZ Host screen displays.

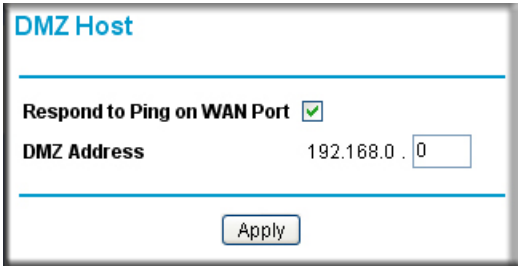


Figure 5-7

3. 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.
4. 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.
5. Click **Apply** to save your settings.

Using LAN IP Setup Options

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 configure LAN IP settings:

1. Log in to the gateway as described in “Logging in to the Gateway” on page 1-5.

2. In the main menu, under Advanced, select LAN IP. The LAN IP screen displays.

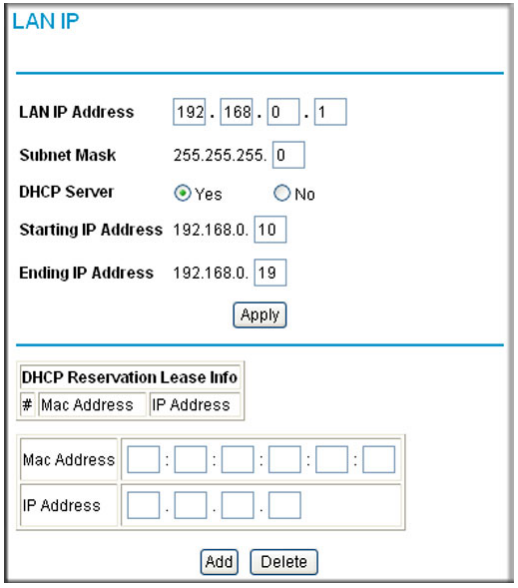


Figure 5-8

3. 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.

	Note: 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.

4. Click **Apply** to save your LAN IP settings.

Using the Gateway as a DHCP Server

By default, the gateway functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the gateway's LAN. The assigned default gateway address is the LAN address of the gateway. The gateway assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the gateway are satisfactory. Click the link to the online document "ITCP/IP Networking Basics" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the gateway's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you might wish to save part of the range for devices with fixed addresses.

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

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to manually specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router.

Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

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**.

Enabling 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 configure the gateway for remote management:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.

2. In the main menu, under Advanced, select Remote Management to display this screen:

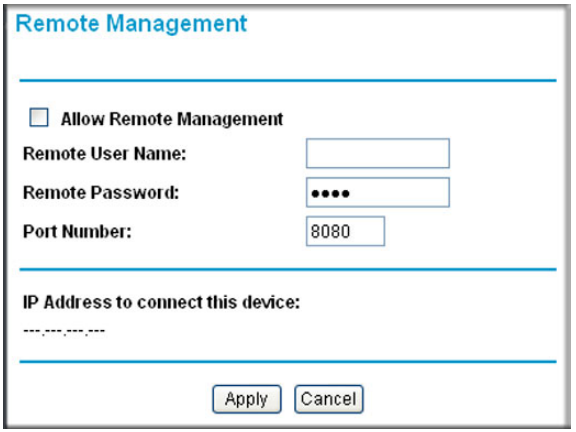


Figure 5-9

3. Select the **Allow Remote Management** check box.
4. 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.

	Note: 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.

	Note: Web browser access normally uses the standard http service port 80. For greater security, you can specify a custom port by entering that number in the **Port Number** field. 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.

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

Configuring Universal Plug and Play (UPnP)

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

To configure UPnP:

1. Log in to the gateway as described in "Logging in to the Gateway" on page 1-5.
2. In the main menu, under Advanced, select **UPnP**. The UPnP screen displays.

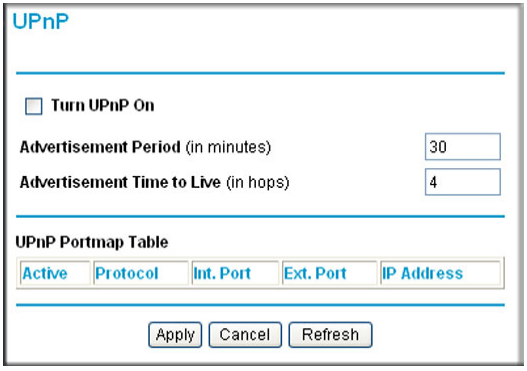


Figure 5-10

3. 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.
4. Enter the following information:
   - **Advertisement Period**. Enter how often the gateway broadcasts its UPnP information. The default is 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time to Live**. Enter the time to live for the advertisement, which is measured in hops (steps) from 1 to 255 for each UPnP packet that is sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The default setting is 4 hops, which is fine for most home networks. If some devices are not 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 router 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.

5. 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.

Chapter 6
Troubleshooting

This chapter gives information about troubleshooting your DOCSIS 2.0 Advanced Cable Gateway CGD24N v2. For the common problems listed, go to the section indicated.

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

- Have I connected the gateway correctly?

  Go to "Basic Functions" on page 6-1.
- I cannot access the gateway configuration with my browser.

  Go to "Connecting to the Gateway's Main Menu" on page 6-3.
- I have configured the gateway but I cannot access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 6-4.
- I cannot remember the gateway's configuration password or I want to clear the configuration and start over again.

  Go to "Backing Up and Restoring Your Settings" on page 4-5.

Basic Functions

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 approximately 30 seconds, verify that:
   - The Local port Link LEDs are lit for any local ports that are connected.
   - The Internet Link port LED is lit.

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.

Table 6-1. Using LEDs to Troubleshoot

LED Behavior	Action
All LEDS are 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 "Backing Up and Restoring Your Settings" on page 4-5. • If the error persists, you might have a hardware problem and should contact technical support.
LAN LED is off for a port with an Ethernet connection.	• 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: • When connecting the gateway's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.
Cable Link LED is off and the gateway is connected to the cable television cable.	• Make sure that the coaxial cable connections are secure at the gateway and at the wall jack. • Make sure that your cable internet service has been provisioned by your cable service provider. Your provider should verify that the signal quality is good enough for cable modem service. • Remove any excessive splitters you may have on your cable line. It may be necessary to run a "home run" back to the point where the cable enters your home.

Connecting to the Gateway's Main Menu

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

- Check the Ethernet connection between the computer and the gateway as described in the previous section.
- Make sure that your PC's IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.10 to 192.168.0.254. Refer to the link to the online document "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 "Enabling Remote Management" on page 5-17.
- 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 factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the gateway does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

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

Additionally, your PC may not have the gateway configured as its TCP/IP gateway. If your PC obtains its information from the gateway by DHCP, reboot the PC and verify the gateway address. See the link to the online document "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.

Testing the LAN Path to Your Gateway

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

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

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

   `ping 192.168.0.1`
3. Click OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   `Request timed out`

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

- Wrong physical connections.
  - Make sure the LAN port LED is on. If the LED is off, see "Using LEDs to Troubleshoot" on page 6-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- Wrong network configuration.
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your gateway and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

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

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

- Check that your PC has the IP address of your gateway listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway. See the link to the online document "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.

Appendix A
Technical Specifications and Factory Default Settings

This appendix provides technical specifications and default factory settings for the DOCSIS 2.0 Advanced Cable Gateway CGD24N v2.

Technical Specifications

Table A-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, 15W maximum
Physical Specifications		• Dimensions: 17.5 cm x 11.5 cm x 2.5 cm • Weight: 280 g
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 USB 1.1 Function 802.11g and 802.11b Wireless Access Point
	WAN	DOCSIS 2.0. Downward compatible with DOCSIS 1.0 and DOCSIS 1.1.

Table A-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 button located on the rear panel 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 Restore Factory Settings button for 5 seconds. The gateway will reboot and return to the settings shown in the following table.

Table A-2. Default Configuration Settings

Feature		Default Behavior
Gateway Login		
	User login URL	http://192.168.1.1
	User name (case sensitive)	admin
	Login Password (case sensitive)	password

Table A-2. Default Configuration Settings (continued)

Feature		Default Behavior
Local Network (LAN)		
	LAN IP	192.168.1.1
	Subnet Mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP Ending IP Address	192.168.1.254
	DMZ	Enabled or disabled
	Time zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Internet Connection		
	WAN MAC address	Use default hardware address
	WAN MTU size	1500

Table A-2. Default Configuration Settings (continued)

Feature		Default Behavior
Wireless		
	Wireless Communication	Disabled
	SSID Name	NETGEAR
	802.11 Band	2.4 GHz
	802.11 n-mode	Auto
	802.11 Bandwidth	40 MHz
	Sideband for channel control (40 MHz only)	Upper
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission Speed	Auto[a]
	Country/Region	United States (varies by region)
	RF Channel	6 until the region is selected
	Operating Mode	g and b until the region is selected
	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.

Appendix B
Related Documents

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

Document	Link
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*

Index

A

adding reserved IP addresses *5-17*

B

backing up gateway configuration *4-5*

backing up the configuration file *4-5*

Basic Settings *1-7*

Basic Settings screen *1-6*

blocking
- keywords *3-2*
- PCs based on MAC address *5-5*
- services *3-4*
- sites *3-2*

blocking ports *5-7*

C

cable channel *4-3*

Cable Link LED *1-2*

configuration
- backup *4-5*
- erasing *4-6*

connection status *4-3*

crossover cable *6-2*

D

default gateway field (Basic Settings) *1-7*

Denial of Service (DoS) *3-1*

DHCP *1-6*
- reserved IP address *5-17*
- server *5-15*, *5-16*

diagnostics *4-7*

DMZ host *5-13*

DNS primary and secondary server *1-7*

Downstream Traffic LED *1-2*

E

e-mailing logs *3-1*

Erase configuration *4-6*

Ethernet
- crossover cable *6-2*
- LED *1-2*

event log *4-6*

F

factory default settings *A-2*

firewall rules
- inbound *5-9*
- port blocking *5-7*
- port forwarding *5-9*

front panel *1-1*

G

gateway
- backup *4-5*
- diagnostics *4-7*
- event log *4-6*
- factory default settings *A-2*
- initialization procedure *4-3*
- password *4-4*
- remote management *5-17*
- status *4-1*
- technical specifications *A-1*

I

IP addresses, auto-generated *6-3*

IP addresses, reserved *5-17*

L

label (bottom of gateway) *1-4*
LAN IP settings *5-14*
LAN LED *1-2*
LEDs
  description *1-2*
  troubleshooting *6-2*
Logging in to the gateway *1-5*

M

MAC address *4-2*
MAC filtering *5-5*

O

outbound rules *3-4*

P

package contents *1-1*
password *4-4*
ping utility *6-4*
placement of the gateway *2-1*
port blocking *3-4*, *5-7*
port forwarding *5-9*, *5-11*
port triggering *5-11*
Power LED *1-2*
primary DNS server *1-7*
Push 'N' Connect *2-9*

R

rear panel *1-3*
remote management *5-17*
reserved IP adresses *5-17*
Restore Factory Settings button *1-3*, *A-2*
restrict wireless access by MAC address
  access control *2-15*
router log *3-1*
rules
  outbound *3-4*

S

secondary DNS server *1-7*
security options (wireless) *2-5*
SSID *2-5*
static IP address *1-7*

T

TCP/IP, network troubleshooting *6-4*
technical specifications *A-1*
troubleshooting *6-1*
  access to gateway main menu *6-3*
  ISP connection *6-4*
  LEDs *6-2*
  ping utility *6-4*
  TCP/IP network *6-4*

U

Universal Plug and Play (UPnP) *5-19*
Upstream Traffic LED *1-2*
URL *3-3*

W

WEP *2-5*, *2-6*
WiFi On/Off button *1-3*
Wi-Fi Protected Setup (WPS)
  Push 'N' Connect *5-3*
wireless
  access point *5-2*
  card access list *5-3*
  channel *2-5*
  guest network *2-13*
  manually configuring settings *2-3*
  range and interference *2-2*
Wireless LED *1-2*
wireless security *2-3*
Wireless Settings screen *2-4*, *2-5*
WPA *2-5*, *2-8*

RADIUS settings *2-8*
WPA2-PSK *2-5*, *2-8*
WPA-PSK *2-5*, *2-8*
WPS button. *1-3*
WPS Push 'N' Connect *2-9*, *2-13*