

Wireless Cable Voice Gateway Model CVG834G Reference Manual



NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10306-02
v2.0
November 2007

© 2007 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR and the NETGEAR logo are trademarks of NETGEAR, Inc. Microsoft, Windows, and Windows NT 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.

FCC Statement

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 generates, 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 of the following measures:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

For product available in the USA market, only channels 1~11 can be operated.

Selection of other channels is not possible

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, EN60950-1

Português [Portuguese]	NETGEAR, Inc. declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že Radiolan spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Wireless Cable Voice Gateway 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the Wireless Cable Voice Gateway 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.

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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second 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.

Technical Support

Please call your Internet Service Provider (ISP) for technical support.

Product and Publication Details

Model Number:	CVG834G
Publication Date:	November 2007
Product Family:	Gateway
Product Name:	Wireless Cable Voice Gateway
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10306-02

Contents

About This Manual

Conventions, Formats, and Scope	xi
How to Use This Manual	xii
How to Print this Manual	xii
Revision History	xiii

Chapter 1

Installing the Gateway

The Gateway Front Panel	1-1
The Gateway Rear Panel	1-3
Installing the Voice Gateway	1-3
Installation Requirements	1-4
Connecting the Wireless Voice Gateway	1-4
Ethernet Connection	1-4
USB Connection	1-5
Logging In to the Wireless Voice Gateway	1-6
Connecting to the Internet and VoIP	1-7

Chapter 2

Wireless Configuration

Wireless Placement and Range Guidelines	2-2
SSID and Wireless Security Settings Form	2-3
Viewing or Changing Wireless Settings	2-4
WEP (Wired Equivalent Privacy)	2-7
WPA-PSK (WiFi Protected Access Pre-Shared Key)	2-8
WPA (WiFi Protected Access)	2-9
WPA2-PSK (WiFi Protected Access 2 Pre-Shared Keys)	2-10
WPA2 (WiFi Protected Access 2)	2-11
Configuring Your Wireless Card Access List	2-12
Adding or Deleting a Wireless Card from the Access List	2-13

Chapter 3

Protecting Your Network

Changing the Default Password	3-1
Logs	3-2
Blocking Keywords, Sites and Services	3-3
Blocking Keywords and Domains	3-3
Blocking Access by Time of Day	3-5
Enabling or Disabling Content Filtering Services	3-5
Using MAC Filtering to Block Access	3-6
Inbound and Outbound Rules	3-8
Port Blocking	3-8
Port Forwarding	3-10
Port Triggering	3-12
Setting Up a DMZ Host	3-13

Chapter 4

Managing Your Network

Gateway Status	4-1
Connection Status	4-2
Viewing and Emailing Event Logs	4-3
Restoring Factory Default Configuration Settings	4-4
Running Diagnostic Utilities	4-5
Setup Features	4-5
Viewing MTA Status	4-6
Guest Network	4-6
Wi-Fi Multimedia (WMM)	4-7
LAN IP Settings	4-7
Using the Gateway as a DHCP Server	4-8
Remote Management Access	4-10
Universal Plug and Play (UPnP)	4-12

Chapter 5

Troubleshooting

Basic Functions	5-1
Connecting to the Wireless Voice Gateway Main Menu	5-2
Troubleshooting the ISP Connection	5-3
Troubleshooting a TCP/IP Network Using a Ping Utility	5-4

Testing the LAN Path to Your Gateway	5-4
Testing the Path from Your PC to a Remote Device	5-5

Appendix A

Default Settings and Technical Specifications

Factory Default Settings	A-1
Technical Specifications	A-3

Appendix B

Related Documents

Index

About This Manual

The *NETGEAR® Wireless Cable Voice Gateway Model CVG834G Reference Manual* describes how to install, configure and troubleshoot the Wireless Cable Voice Gateway . 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:

<i>Italics</i>	Emphasis, books, CDs, URL names
Bold	User input
Fixed	Screen text, file and server names, extensions, commands, IP addresses

- **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 Voice Gateway according to these specifications:

Product Version	Wireless Cable Voice Gateway
Manual Publication Date	November 2007

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix B, “Related Documents”](#).

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons,  and , for browsing forwards or backwards through the manual one page at a time
- A  button that displays the table of contents and an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View.**

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter.**

Use the *PDF of This Chapter* link at the top left of any page.

- Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
- Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at <http://www.adobe.com>.

- Click the print icon in the upper left of the window.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual.**

Use the *Complete PDF Manual* link at the top left of any page.

- Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
- Click the print icon in the upper left of the window.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Part Number	Version Number	Date	Description
202-10306-01	1.0	August 2007	Original document.
202-10306-02	2.0	November 2007	Product update: New firmware and new user Interface .

Chapter 1

Installing the Gateway

This chapter describes how to set up the wireless voice gateway on your local area network (LAN), connect to the Internet, and perform basic configuration.

The Gateway Front Panel

The front panel of the Voice Gateway contains status LEDs.

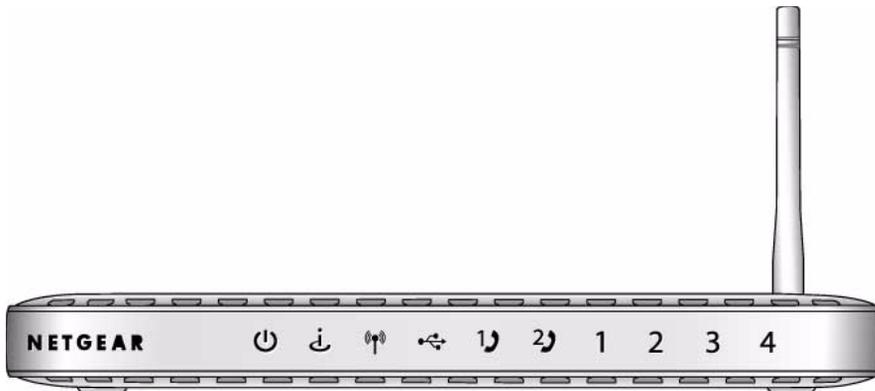


Figure 1-1

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

Table 1-1. LED Descriptions

LED	Description
Power 	<ul style="list-style-type: none">• Green solid: Power is supplied to the gateway.• Green blink: The battery is charged.• Amber solid: Discharge battery (when 110V power is shut down).• Amber blink: The battery capacity is low (<10%).• Off: Power is not supplied to the gateway.

Table 1-1. LED Descriptions (continued)

LED	Description
Cable Link 	<ul style="list-style-type: none"> • Amber slow blink: Scanning downstream channel. • Amber fast blink: Synchronization. • Green solid: Cable link. • Green blink: Upstream data traffic. • Off: No configuration.
Wireless 	<ul style="list-style-type: none"> • Green solid: The wireless connection is operating normally. • Green blink: Data is being transmitted or received on the wireless interface. • Off: No wireless link is detected.
USB 	<ul style="list-style-type: none"> • Green solid: A USB device is connected to the USB port. • Off: No USB device is connected.
Voice ports (1 and 2) 	<ul style="list-style-type: none"> • Green solid: Registered with the Call Agent. • Green blink: There is an active call. • Green slow blink: Phone is “on-hook”; registration with Call Agent is in progress. • Off: No phones are connected to the voice port.
LAN (Local Area Network) 	<ul style="list-style-type: none"> • Green on: The Local port has detected link with a 100 Mbps device. • Green blink: Data is being transmitted or received at 100 Mbps. • Amber on: The Local port has detected link with a 10 Mbps device. • Amber blink: Data is being transmitted or received at 10 Mbps. • Off: No link is detected on this port.

The Gateway Rear Panel

The label on the bottom of the gateway identifies the connections on the rear panel.

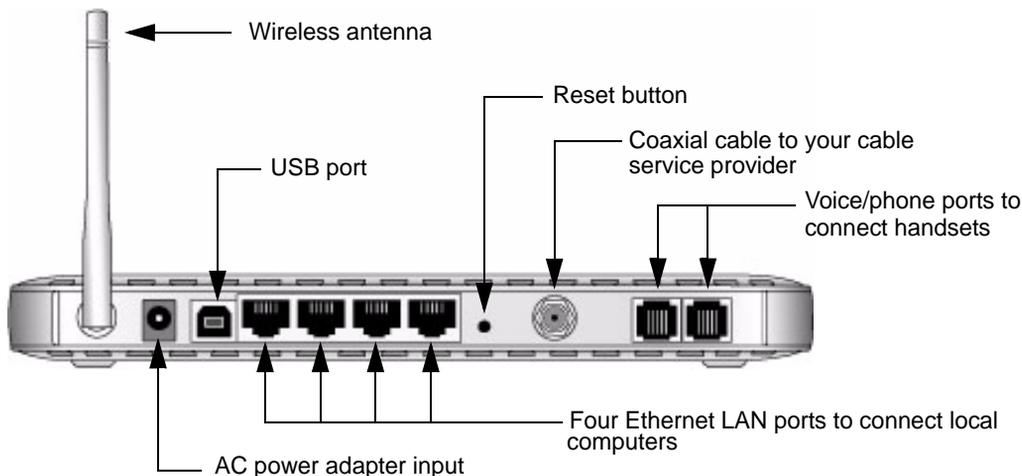


Figure 1-2

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

- **Wireless Antenna.** The gateway ships with the wireless antenna already attached.
- **Power.** AC power adapter input.
- **USB port.** If the USB driver is installed, you can connect a local computer to this port.
- **Four Ethernet LAN ports.** Use these ports to connect local computers.
- **Reset button.** Resets the gateway to its factory defaults.
- **Coaxial cable connector.** Attach coaxial cable to the cable service provider's connection.
- **Two Voice/Phone ports.** With VoIP service, connect one or two handsets to these ports.

Installing the Voice Gateway

Installation is a four-part process. Complete the installation in this order:

1. Check the Installation Requirements. See [“Installation Requirements”](#).
2. Connect the Gateway. See [“Connecting the Wireless Voice Gateway”](#).
3. Log in to the Gateway. See [“Logging In to the Wireless Voice Gateway”](#).

4. Connect to the Internet. See [“Connecting to the Internet and VoIP”](#).

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

Installation Requirements

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

- A computer with active Ethernet port with DHCP enabled. See the link [“Preparing a Computer for Network Access:”](#) in [Appendix B](#) for help with DHCP configuration.
- An active account with your Internet service provider for data and/or voice services.
- Depending on how your Internet Service Provider (ISP) set up the Internet account, you will need one or more of these configuration settings to connect the gateway to the Internet:
 - Host and Domain Names
 - ISP Domain Name Server (DNS) Addresses
 - Fixed or Static IP Address
- Each computer that will connect to the gateway must have either an installed Ethernet Network Interface Card (NIC), USB Host port, or 802.11b or 802.11g wireless adapter.

Connecting the Wireless Voice Gateway

To install the gateway, connect it to a computer either via an Ethernet or a USB according to the guidelines in the following sections.

Ethernet Connection

To connect a computer to the gateway with an Ethernet cable:

1. Use the coaxial cable provided by your cable company to connect the wireless voice gateway cable port to your cable line splitter or outlet.
2. Connect the power adapter to the wireless voice gateway. Plug in the power adapter and wait about 30 seconds for the lights to stop blinking.
3. Connect a LAN port on the gateway to your computer with the Ethernet cable included in the box.

4. If you have VoIP service, connect the phone to Voice Port 1. If your service includes a second line, you can connect that phone to Voice Port 2.
5. Verify the following:
 - The power light  is lit.
 - The cable link light  is solid green, indicating a link has been established to the cable network.
 - If you connected VoIP lines, the Voice port lights  blink.

USB Connection



Note: The USB connection option is only available for Windows PCs. Also, Windows 95 does not support USB without special operating system upgrades and patches.

To connect a computer to the USB port on the gateway:

1. You must install the USB driver. Insert your NETGEAR CD into the CD drive of your computer.
 - a. Connect the USB cable to your gateway and plug in the AC power for the gateway.
 - b. Use the USB cable to connect your computer to the gateway.
 - c. The Found New Hardware Windows installation wizard prompts for the drivers.
 - d. Browse to the NETGEAR CD and install the USB driver by clicking through the Windows wizard prompts.



Figure 1-3

2. Connect your computer to the USB port on the gateway.
3. Plug in your gateway and wait about 30 seconds for the lights to stop blinking.
4. Verify the following:
 - The power light  is lit.
 - The cable link light  is solid green, indicating a link has been established to the cable network.
 - The USB light  is lit.

Logging In to the Wireless Voice Gateway



Note: To connect to the gateway, your computer must be configured to use DHCP. For instructions on how to do this, see the link to [“Preparing a Computer for Network Access:” 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.

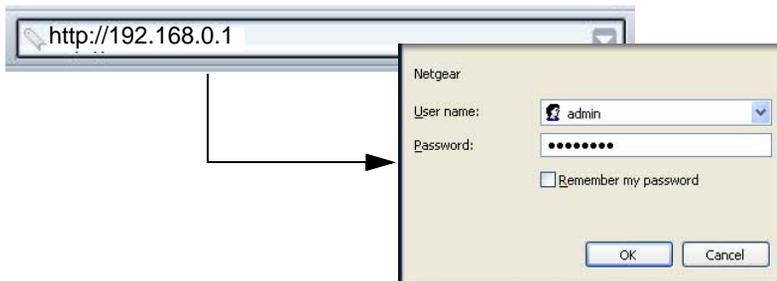


Figure 1-4

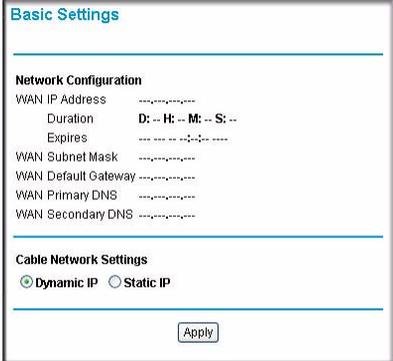
The gateway default user name is **admin**, with the default password of **password**, both in lower-case letters. When prompted to log in, enter the user name and password. You are now connected to the gateway.

Connecting to the Internet and VoIP

To configure the gateway to connect to the Internet.

- From the main menu, select Basic Settings. The Basic Settings screen appears:

Dynamic IP



Basic Settings

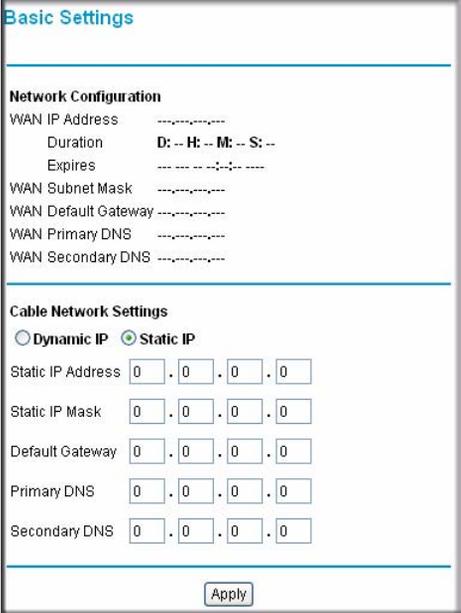
Network Configuration

WAN IP Address
 Duration **D:** -- **H:** -- **M:** -- **S:** --
 Expires
 WAN Subnet Mask
 WAN Default Gateway
 WAN Primary DNS
 WAN Secondary DNS

Cable Network Settings

Dynamic IP Static IP

Static IP



Basic Settings

Network Configuration

WAN IP Address
 Duration **D:** -- **H:** -- **M:** -- **S:** --
 Expires
 WAN Subnet Mask
 WAN Default Gateway
 WAN Primary DNS
 WAN Secondary DNS

Cable Network Settings

Dynamic IP Static IP

Static IP Address . . .

Static IP Mask . . .

Default Gateway . . .

Primary DNS . . .

Secondary DNS . . .

Figure 1-5

- The **WAN Default Gateway** is the ISP router to which your gateway will connect.
- A DNS server is a host on the Internet that translates Internet names (such as <http://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.

2. The **Dynamic IP** radio button is selected by default.
 - If your service provider assigns your IP address through DHCP, leave the **Dynamic IP** radio button selected.
 - If your service provider assigned you a permanent, fixed (static) IP address for your PC, select **Static IP**. Enter the IP address that your ISP assigned. Also enter the static IP mask (also known as netmask), Gateway IP address and Domain Name Server (DNS) Address.
3. Click **Apply** to accept these settings.
4. If you have VoIP service, connect the phone to a  Voice Port 1. If your service includes a second line, you can connect that phone to Voice Port 2. To check the voice status, see [“Viewing and Emailing Event Logs”](#) on page 4-3.

To set up a wireless connection, see [Chapter 2, “Wireless Configuration”](#).

Chapter 2

Wireless Configuration

This chapter describes how to set up the wireless features of your wireless voice gateway. In planning your wireless network, consider the level of security required. Select the location of your wireless equipment in order to maximize the network speed.

Set up wireless features for the wireless voice gateway in this order:

1. Install the wireless voice gateway as described in [Chapter 1, “Installing the Gateway”](#). The wireless voice gateway should be working on your LAN before you set up the wireless features.
2. Plan the location for the wireless voice gateway based on considerations in [“Wireless Placement and Range Guidelines”](#).
3. Use the form in section [“SSID and Wireless Security Settings Form”](#) on page 2-3 to keep track of your settings.
4. Enter the wireless settings, and verify wireless connectivity as described in [“Viewing or Changing Wireless Settings”](#) and [“WEP \(Wired Equivalent Privacy\)”](#).

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

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the wireless voice 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 wireless voice gateway:

- 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.

SSID and Wireless Security Settings Form

For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the person who set up or is responsible for the network can get the settings. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID.** The Service Set Identification (SSID) identifies the wireless local area network. NETGEAR is the default SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

The SSID in the wireless voice gateway is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID.

- **Authentication.**

Circle one: Open System or Shared Key. Choose Shared Key for more security.

To use Shared Key, all devices in the network must be set to Shared Key and have the same keys in the same positions as those in the CVG834G.

- **WEP Encryption Keys.** For all four keys, choose the Key Size. Circle one: 64, or 128 bits.

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

- **WPA-PSK (Pre-Shared Key) and WPA2-PSK.** Record the WPA-PSK or WPA2-PSK key.

Key: _____ (8-63 characters)

- **WPA and WPA2 RADIUS Settings.** For WPA and WPA2, record the following settings for the primary and secondary RADIUS servers.

Server Name/IP Address: _____

Port: _____

Shared Key: _____

Use the procedures described in the following sections to configure the CVG834G. Store this information in a safe place.

Viewing or Changing Wireless Settings



Note: If you use a wireless computer to change wireless settings such as the SSID, you will be disconnected when you click **Apply**. Reconfigure your wireless computer to match the new settings, or access the wireless voice gateway from a wired computer to make further changes.

To view or change the wireless settings:

1. Connect a computer to the wireless voice gateway using an Ethernet or USB cable as described in “[Connecting the Wireless Voice Gateway](#)” on page 1-4.
2. Enter **http://192.168.0.1** in the address field of your Internet browser.
3. From the main menu, select Wireless Settings. The Wireless Setting screen appears:

Wireless Settings

Wireless Network
Name(SSID):
Channel:

Wireless Access Point
 Enable Wireless Access Point
 Allow Broadcast of Name (SSID)

Wireless Card Access List
 Turn Access Control On

Security Options
 Disable
 WEP(Wired Equivalent Privacy) 64-bit encryption
 WEP(Wired Equivalent Privacy) 128-bit encryption
 WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)
 WPA
 WPA2-PSK(Wi-Fi Protected Access 2 Pre-Shared Key)
 WPA2

Security Encryption(WEP)
Authentication:

Encryption (WEP) Key:
WEP PassPhrase:
 Key 1
 Key 2
 Key 3
 Key 4

Figure 2-1

4. For initial configuration and test, leave the settings unchanged.
5. If you make changes, you must click **Apply** to save the changes.
6. Configure and test your computers for wireless connectivity.

Program the wireless adapter of your computers to have the same SSID and wireless security settings as your wireless voice gateway. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless voice gateway. If there is interference, adjust the channel

The following table explains the Wireless Setting screen.

Table 2-1. Wireless Settings

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. The default SSID is Wireless. Any wireless device that will connect to this wireless voice gateway must use the same SSID. If you want to change the SSID, you can enter a 32-character (maximum) name in this field. The characters are case-sensitive.
	Region	The location where the gateway is used.
	Channel	The wireless channel used by the gateway. The default is Channel 6. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
	Mode	The default is g & b, which allows both 802.11g and 802.11b wireless stations access. Note that in b only mode, 802.11g wireless stations can connect if they can operate in 802.11b mode.

Table 2-1. Wireless Settings (continued)

Settings		Description
Wireless Access Point	Enable Wireless Access Point	On by default, this setting enables the wireless radio, which allows the wireless voice gateway to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.
	Allow Broadcast Name (SSID)	On by default, the wireless voice gateway broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with 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.
Wireless Station Access List	Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect. See "Configuring Your Wireless Card Access List" .
Security Option WEP (Wired Equivalent Privacy) 128-bit encryption is the default setting		WEP security uses encryption keys and data encryption for data security. See "WEP (Wired Equivalent Privacy)" .
Other Security Options		<ul style="list-style-type: none"> • Disable. Wireless security is disabled. This setting can be used to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you use wireless security. • WEP (Wired Equivalent Privacy) 64-bit. WEP security uses encryption keys and data encryption for data security. You can select 64-bit. See "WEP (Wired Equivalent Privacy)". • WPA options: The wireless voice gateway supports WPA-PSK, WPA, WPA2-PSK, and WPA2 security. See "WPA-PSK (WiFi Protected Access Pre-Shared Key)", or "WPA2-PSK (WiFi Protected Access 2 Pre-Shared Keys)".

WEP (Wired Equivalent Privacy)

To configure WEP data encryption:

1. From the Wireless Settings screen, select **WEP (Wired Equivalent Privacy) 64-bit encryption** or **WEP (Wired Equivalent Privacy) 128-bit encryption**.

The figure shows two side-by-side screenshots of a web-based configuration interface for wireless settings. Both screenshots are titled 'Security Options' and have a similar layout. The left screenshot shows 'WEP (Wired Equivalent Privacy) 64-bit encryption' selected with a green radio button. The right screenshot shows 'WEP (Wired Equivalent Privacy) 128-bit encryption' selected with a green radio button. Both screenshots show an 'Authentication' dropdown menu set to 'Open System or Shared Key'. Below that is an 'Encryption (WEP) Key' section with a 'WEP PassPhrase' field and a 'Generate' button. Underneath are four 'Key' fields (Key 1 through Key 4), each with a radio button and a text input field. In the left screenshot, Key 1 is selected and contains '0000000000'. In the right screenshot, Key 1 is selected and contains '00000000000000000000000000000000'.

Figure 2-2

2. In the **Authentication** drop-down list, select **Open System or Shared Key**, or select **Shared Key**.
3. If you use encryption keys, enter them. These values must be identical on all computers in your network. There are two ways to enter the keys:
 - **Passphrase:** Enter a word or group of printable characters in the Passphrase field, and then click **Generate**. The **Key1** through **Key4** fields are populated with key values.
 - **Manual:** Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be the default.

See the link to the online document [“Wireless Communications:” in Appendix B](#) for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

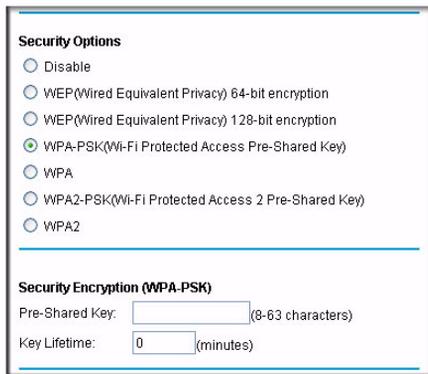
4. Click **Apply** to save your settings.

WPA-PSK (WiFi Protected Access Pre-Shared Key)

Not all wireless adapters support WPA-PSK. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK:

1. On the Wireless Settings screen, select the Security Option **WPA-PSK**.



Security Options

Disable

WEP(Wired Equivalent Privacy) 64-bit encryption

WEP(Wired Equivalent Privacy) 128-bit encryption

WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)

WPA

WPA2-PSK(Wi-Fi Protected Access 2 Pre-Shared Key)

WPA2

Security Encryption (WPA-PSK)

Pre-Shared Key: (8-63 characters)

Key Lifetime: (minutes)

Figure 2-3

2. In the **Passphrase Key** field under Security Encryption (WPA-PSK), enter a word or group of printable characters and enter the **Key Lifetime**.

The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.

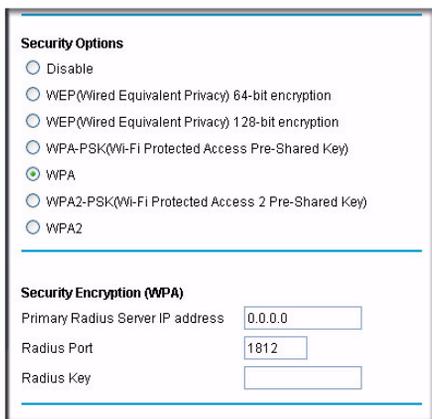
3. Click **Apply** to save your settings.

WPA (WiFi Protected Access)

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA setting.

To configure WPA:

1. On the Wireless Settings screen, select Security Option **WPA**.



The screenshot shows a configuration window titled "Security Options". It contains a list of radio buttons for security options: "Disable", "WEP(Wired Equivalent Privacy) 64-bit encryption", "WEP(Wired Equivalent Privacy) 128-bit encryption", "WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)", "WPA" (which is selected), "WPA2-PSK(Wi-Fi Protected Access 2 Pre-Shared Key)", and "WPA2". Below this list is a section titled "Security Encryption (WPA)" with three input fields: "Primary Radius Server IP address" containing "0.0.0.0", "Radius Port" containing "1812", and "Radius Key" which is empty.

Figure 2-4

2. Enter the Security Encryption (WPA) settings.

These settings are required for communication and authentication from a Radius server. A Secondary Radius Server can be configured which is used if the Primary Radius Server fails.

- **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.
- **Radius Key.** This is shared between the gateway and the Radius Server during authentication.

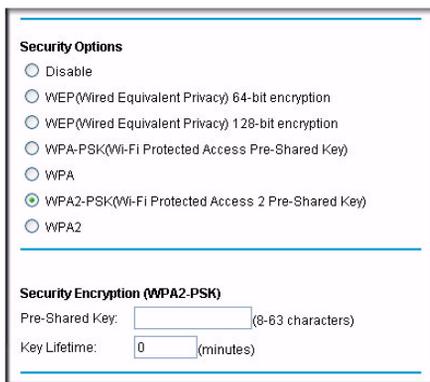
3. Click **Apply** to save your settings.

WPA2-PSK (WiFi Protected Access 2 Pre-Shared Keys)

Not all wireless adapters support WPA2-PSK. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA2. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA2-PSK:

1. On the Wireless Settings screen, select **WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)**.



The screenshot shows a configuration window with two sections. The first section, titled "Security Options", contains a list of radio buttons: "Disable", "WEP(Wired Equivalent Privacy) 64-bit encryption", "WEP(Wired Equivalent Privacy) 128-bit encryption", "WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)", "WPA", "WPA2-PSK(Wi-Fi Protected Access 2 Pre-Shared Key)" (which is selected with a green dot), and "WPA2". The second section, titled "Security Encryption (WPA2-PSK)", contains two input fields: "Pre-Shared Key:" followed by a text box and "(8-63 characters)", and "Key Lifetime:" followed by a text box containing the number "0" and "(minutes)".

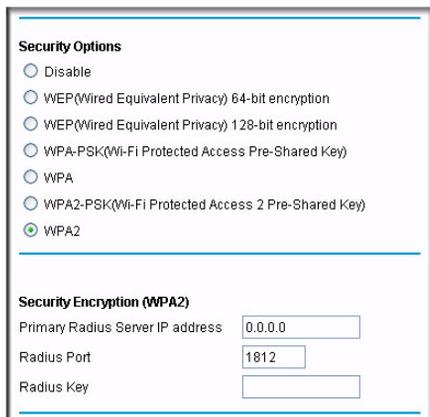
Figure 2-5

2. Enter the Security Encryption (WPA2-PSK) settings:
 - **Pre-Shared Key.** Enter a word or group of printable characters. The passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
 - **Key Lifetime.** Enter the key lifetime in minutes.
3. Click **Apply** to save your settings.

WPA2 (WiFi Protected Access 2)

To configure WPA2:

1. On the Wireless Settings page, select the Security Option **WPA2**.



The screenshot shows a configuration window with two sections. The first section, titled "Security Options", contains a list of radio buttons: "Disable", "WEP (Wired Equivalent Privacy) 64-bit encryption", "WEP (Wired Equivalent Privacy) 128-bit encryption", "WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)", "WPA", "WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)", and "WPA2". The "WPA2" option is selected, indicated by a filled green circle. The second section, titled "Security Encryption (WPA2)", contains three input fields: "Primary Radius Server IP address" with the value "0.0.0.0", "Radius Port" with the value "1812", and "Radius Key" which is currently empty.

Figure 2-6

2. Enter the Security Encryption (WPA2) settings.

These settings are required for communication and authentication from a Radius server. A secondary Radius server can be configured, which is used if the primary Radius server fails.

- **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.
- **Radius Key.** This is shared between the gateway and the Radius Server during authentication.

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

Configuring Your Wireless Card Access List

By default, any wireless PC that is configured with the SSID and WEP/WPA settings has 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.

To restrict access based on MAC addresses:

1. Connect to the gateway and log in as described in [“Viewing or Changing Wireless Settings” on page 2-4](#).

	<p>Note: If your computer is connected wirelessly to the wireless voice gateway, be careful about selecting the Turn Access Control On check box. If your computer’s MAC address is not in the access control list, then you will lose your wireless connection when you click Apply. You must then access the wireless voice gateway from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.</p>
---	--

2. From the main menu, select Wireless Settings. The Wireless Settings screen displays as shown in [Figure 2-1 on page 2-4](#).
3. Scroll down to the Wireless Card Access List and select the **Turn Access Control On** check box.



Figure 2-7

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

4. Click **Apply** to confirm this setting.

Adding or Deleting a Wireless Card from the Access List

To add or delete a wireless card from the Setup Access List:

1. Click **Setup Access List**. The Wireless Card Access List screen displays.

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

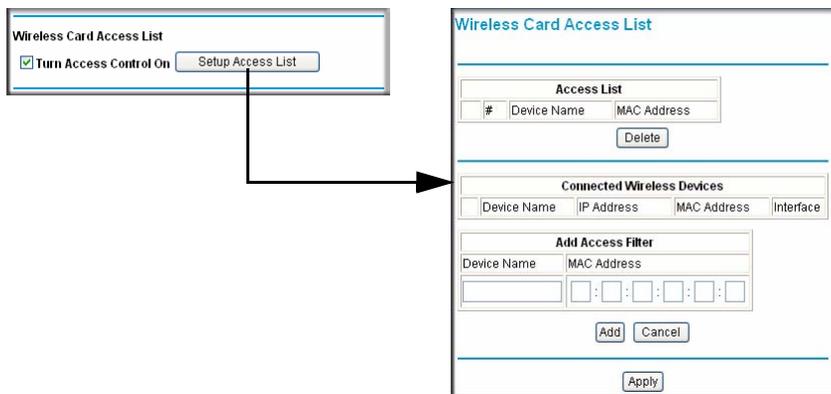


Figure 2-8

2. You can add a device to the Access List using either of these methods:
 - If the computer is in the **Connected Wireless Devices** table, click the radio button of that computer to capture its MAC address.
 - Specify the MAC address of the device to be added in the **Add Access Filter** fields. The MAC address can usually be found on the bottom of the wireless device.



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

3. Click **Add**.
4. Repeat Steps 2 and 3 for each wireless PC that you are adding.
5. Click **Apply** to save these changes. Now, only devices on this list will be allowed to wirelessly connect to the gateway.

To delete an entry from the Access List, select the corresponding radio button in the Access List and then click **Delete**.

Chapter 3

Protecting Your Network

This chapter describes how to control access to your gateway and how to use the firewall features of the gateway to protect your network.

Changing the Default Password

For security reasons, the gateway has its own user name and password. The administrator user name is **admin**, with the default password of **password**. After a period of inactivity for a set length of time, the administrator login automatically disconnects. You can change the password, and you can change the amount of time for the administrator login timeout.



Note: The user name and password 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 default password:

1. Log in to the gateway by entering the default LAN address of **http://192.168.0.1** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the gateway.



Figure 3-1

- Under the Maintenance heading, select Set Password. The Set Password screen appears:



Figure 3-2

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

	<p>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.</p>
---	---

Logs

A log is a detailed record of the denial of service (DoS) attacks directed at your network. You can view the logs here, or you can use e-mail notification to view the logs (see [“Viewing and Emailing Event Logs”](#) in Chapter 4).

From the main menu, under the Content Filtering heading, select Logs. The Logs screen appears:



Figure 3-3

Blocking Keywords, Sites and Services

The gateway provides a variety of options for blocking Internet content and communications to the gateway. You can control access to Internet content by screening for keywords within Web addresses; you also can block access to all sites except those that are explicitly allowed. Blocking options include:

- Blocking access from your LAN to Internet locations that contain keywords that you specify.
- Blocking access to Web sites (domains) that you specify as off-limits.
- Allowing access to only Web sites (domains) that you specify as allowed.

You can also block access to the Internet by a specific computer based on the hardware MAC address of that computer. Blocking access to the Internet based on the hardware MAC address of the computer or wireless adapter is described in [“Using MAC Filtering to Block Access” on page 3-6](#).

Blocking Keywords and Domains

You can restrict access to Internet content based on Web address keywords and domain names. A domain name is the name of a particular Web site. For example, for the address www.netgear.com, the domain name is NETGEAR.com.

To configure Block Sites:

1. Log in to the gateway by entering the default LAN address of **http://192.168.0.1**, the default user name of **admin**, and default password of **password** or use whatever password and LAN address you have chosen for the gateway.

2. Click Block Sites under the Content Filtering heading on the main menu.

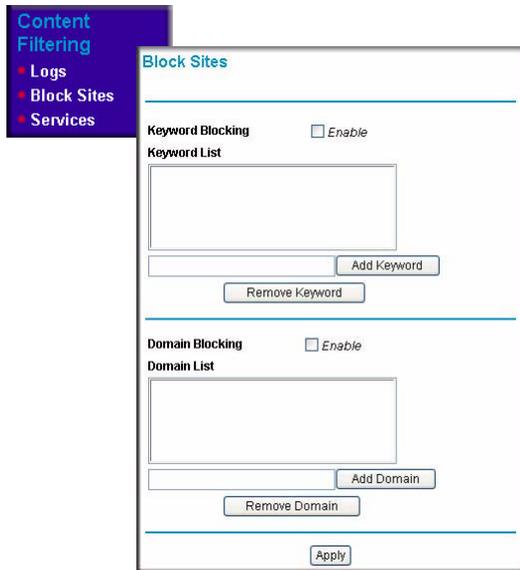


Figure 3-4

Keywords

To enable keyword blocking:

1. On the Block Sites screen, select the **Enable** check box in the Keyword section.
2. Add keywords by entering them into the Add Keyword List. An example of some Keyword applications are:
 - If the keyword “XXX” is specified, the URL “http://www.badstuff.com/xxx.html” is blocked.
 - If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
 - If the keyword “.” is specified, all Internet browsing access is blocked.

Up to eight entries are supported in the Keyword List.

3. When you have completed your entries, click **Add Keyword**.

Domain Blocking

To enable domain blocking:

1. Select the **Enable** radio box adjacent to Domain Blocking.
2. Enter the Domain Name of the site name you want to block in the **Domain List** field.

If the domain “badstuff.com” is specified, the URL “http://www.badstuff.com/xxx.html” will be blocked, along with all other URLs in the badstuff.com site.

Up to eight entries are supported in the **Domain List**.

3. When you have completed your entries, click **Add Domain**.
4. Click **Apply** to save your settings

To delete a an entry in either the Keyword List or Domain List field:

1. Select it from the list, and click **Remove Keyword** or click **Remove Domain**.
2. Click **Apply** to save your settings.

Blocking Access by Time of Day

The default blocking schedule is to block access all day. However, you can also block access according to a daily schedule for each PC individually.

To block access for a PC:

1. In the MAC Filtering screen, select the PC for which the schedule will be modified.
2. In the Day(s) to Block section, select the check boxes next to the days when you want access blocked.
3. In the Time of Day to Block section, select either **All Day**, or set the hours for Internet blocking
4. Click **Apply** to activate the settings.

Enabling or Disabling Content Filtering Services

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

From the main menu, select Services. The Services screen appears:

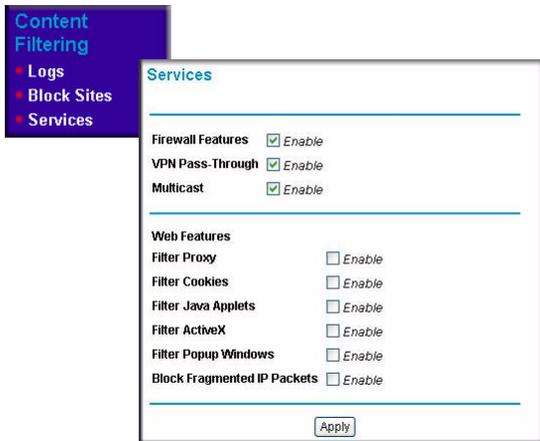


Figure 3-5

Selecting the check box for a service enables it. Clearing the check box disables the corresponding service. If you make changes, then you must click **Apply** in order for the changes to take effect. The services are described as follows:

- **Firewall Features.** Enabled by default. The gateway will perform stateful packet inspection (SPI) and protect against Denial of Service (DoS) attacks. .
- **VPN Pass-Through.** Enabled by default. IPSec and PPTP traffic will be forwarded. When it is disabled, this traffic will be blocked.
- **Multicast.** Enabled by default. The gateway can pass multicasting streams through the firewall.
- **Web Features.** Disabled by default. If enabled, certain Web-oriented features such as cookies, java scripts, or pop-up windows will be blocked by the firewall. For example, if you enable **Filter Cookies**, many websites will not allow you to access their site.

Using MAC Filtering to Block Access

By default, any computer has access to the Internet through your gateway. MAC Filtering allows you to block access to the Internet to any computer on your LAN based on the hardware MAC address of its Ethernet or wireless adapter.

To configure MAC Filtering:

1. Log in to the gateway at its default LAN address by entering **http://192.168.0.1**, the default user name **admin**, and default password of **password**; or use whatever password and LAN address you have chosen for the gateway.
2. Under the Advanced heading on the main menu, select MAC Filtering. The MAC Filtering screen appears:

The screenshot shows the MAC Filtering configuration interface. At the top, there is a table titled "Trusted Devices" with columns for Device Name, IP Address, MAC Address, and Interface. A single entry is shown for "Loaner-T30-4" with IP 192.168.0.10 and MAC 00:09:6b:02:18:dd on interface Eth-Switch Lan(1). Below the table is a "Refresh" button. The "Add MAC Filter" section has fields for "Device Name" and "MAC Address" (with a dotted input mask), and "Add" and "Cancel" buttons. The "MAC Filter List" section shows "No filters entered" in a dropdown, an "Enable" checkbox, and a "Delete" button. The "Day(s) to Block" section has checkboxes for "Everyday", "Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", and "Saturday". The "Time of Day to Block" section has an "All day" checkbox and "Start" and "End" time pickers (hour, minute, AM/PM).

Figure 3-6

The Trusted Devices table is at the top of this screen. It shows devices that are currently connected to the wireless voice gateway.

To add a device to the Trusted Devices table:

1. Select a device using one of the following methods:
 - If the device is in the Trusted Devices table, click the radio button of that PC to capture its MAC address.
 - If the device is not in the Trusted Devices table, you can manually enter the MAC address of the PC you want to block. If no Device Name appears when you enter its MAC address, you can type a descriptive name in the **Device Name** field.
2. Click **Add**. The device appears in the Trusted Devices table.

To delete a device from the Trusted Devices table:

1. Select the MAC address of the PC from the Trusted Devices table.
2. Click **Delete** to delete the entry.
3. Click **Apply** to activate the settings.

Inbound and Outbound Rules

You can use firewall rules to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the gateway are:

- **Inbound:** Block all access from outside except responses to requests from the LAN side. Instructions for setting up inbound rules can be found in [“Port Forwarding” on page 3-10](#)
- **Outbound:** Allow all access from the LAN side to the outside. Use Port Blocking to set up outbound rules (see [“Enabling or Disabling Content Filtering Services” on page 3-5](#)).

You may define more rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day.

Port Blocking

You can use Port Blocking to block outbound traffic on specific ports.

To configure port blocking:

1. Under the Advanced heading on the main menu, select Port Blocking. The Port Blocking screen displays.

The screenshot shows the 'Port Blocking' configuration interface. It includes sections for adding predefined or custom services, a list of active filters, and options to block traffic by day of the week or by a specific time range.

Figure 3-7

2. Select the service that you want to block from the **Add Predefined Services** drop-down list. If the service that you want to block is not in the predefined list, you can add a custom service.
3. Enter the range of ports that you want to block and select whether the ports are TCP, UDP or Both.
4. Enter the Local IP Address for the computer to which this rule will apply.
5. Click **Add**. The selected service will appear in the Port Filter List

Blocking a Rule by Day or Time

To specify specific days or times to block a rule:

1. From the **Port Filter List**, select a rule, and then select the corresponding **Enable** check box.
2. Select the check box for the **Day(s) to Block** when you want to apply the rule.
3. For the time of day, either select the **All Day** check box or specify a **Start Time** and **End Time** from the pull-down menus.

4. Click **Add**. The new Port Blocking rule appears in the Outbound Rules table.

To delete an existing rule:

1. Select the rule from the **Port Filter List**.
2. Click **Delete**.

Port Forwarding

You can use port forwarding to set up a rule that directs inbound traffic for a particular service to a local server (for example, a Web server or game server) based on the destination port. This makes the server visible and available to the Internet.

Unless you set up port forwarding, the gateway prevents this type of traffic. The gateway uses Network Address Translation (NAT). NAT presents a single IP address for your network to the Internet. Outside users cannot directly address your local computers.



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 check for servers and may suspend your account if it discovers active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Before setting up Port Forwarding, consider the following:

- 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.
- Local computers must access the local server using the local LAN address of the computer (192.168.0.XXX, by default). Attempts by local computers 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.

Forwarding Inbound Traffic

To forward inbound traffic:

1. Select the service that you want to forward from the **Predefined Services** drop-down list.

If the service that you want to forward is not in the predefined list, you can add a custom service. Enter the range of ports that you want to forward and select whether the ports are TCP, UDP or Both.

2. If you want to change the suggested port numbers, enter a new **Start Port** and **End Port**.
3. From the drop-down **Protocol** list, select the protocol: TCP, UDP, or Both.
4. Enter the IP address of the computer on your network to which you would like to direct the inbound traffic in the **Local IP Address** field.
5. Click **Add**. The new Port Forwarding rule appears in the Active Forwarding Rules table.

Port Forwarding

Active Forwarding Rules

Name	Start Port	End Port	Protocol	Local IP Address
------	------------	----------	----------	------------------

Choose Predefined Service

Service: -SERVICES-

Add Custom Rules

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

Add Delete Reset

Figure 3-8

Deleting a Rule

To delete an existing rule:

1. Select the radio button for the rule that you want to delete.
2. Click **Delete** to delete the Port Forwarding rule.

Port Triggering

Port Triggering is an advanced feature that allows you to dynamically open inbound ports based on outbound traffic on different ports. This feature can be used for gaming and other Internet applications.



Note: Port Forwarding is similar to port triggering, but it is static and has some limitations. Ports are open to traffic from the Internet until the port forwarding rule is removed. Additionally, port forwarding does not work well for some applications when your WAN IP address is assigned by DHCP, and is changed frequently. Port Triggering opens an incoming port temporarily and does not require the server on the internet to track your IP address if it is changed.

Port Triggering monitors outbound traffic. When the gateway detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and “triggers” the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

For example, port triggering can be used for Internet Relay Chat (IRC). When you connect to an IRC server, the server tries to connect back on the port to do an Ident lookup. Unless you have configured Port Forwarding to open that port, the traffic will be blocked. In this example, the initial login to the server in the range of ports is detected. This triggers the gateway to temporarily forward the port to the PC that initiated the login.

To configure Port Triggering:

1. Under the Advanced heading on the main menu, select Port Triggering. The Port Triggering screen appears:

Port Triggering List						
Trigger Range		Target Range		Protocol	Enable	
Start Port	End Port	Start Port	End Port			
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	
> 0	0	0	0	Both	<input type="checkbox"/>	

Apply Delete Reset

Figure 3-9

2. In the **Trigger Range** field, enter the outbound ports that will be monitored for activity. This will be the “trigger.”
3. In the **Target Range** field, enter the inbound ports that should be forwarded when the trigger occurs.
4. Select the appropriate protocol: TCP, UDP or Both.
5. Select the **Enable** check box
6. Click **Apply**.

There are two ways to clear a Port Triggering rule:

- Clear the **Enable** check box to temporarily disable the rule.
- Select the rule, and then click **Delete**.

Setting Up a DMZ Host

The Default DMZ Server feature is helpful when using some online games and video conferencing applications that are incompatible with NAT. The gateway is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC’s IP address is entered as the Default DMZ Host.

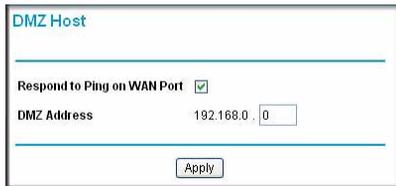


Note: For security, you should avoid using the Default DMZ Server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the gateway unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding or Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ host.

To assign a computer or server to be a DMZ host:

1. From the main menu, under the Advanced heading, select DMZ Host. The DMZ Host screen appears:



DMZ Host

Respond to Ping on WAN Port

DMZ Address 192.168.0.

Apply

Figure 3-10

2. In the **DMZ Address** field, enter the IP address of the computer that you want to assign as a DMZ host.
3. Click **Apply**.

To disable the DMZ host, enter **0** (zero), and then click **Apply**.

If you want the gateway to respond to a ping from the Internet, select the **Respond to Ping on WAN Port** check box. This should only be used as a diagnostic tool, since it allows your gateway to be discovered. Do not select this check box unless you have a specific reason to do so.

Chapter 4

Managing Your Network

This chapter describes how to perform network management tasks such as viewing the gateway status, running diagnostics, restoring factory default settings, and backing up your configuration files.

Gateway Status

Under the Maintenance heading on the main menu, select Gateway Status. This Gateway Status fields are described in the following table:

Table 4-1. Gateway Status Screen Settings

Setting		Description
Information	Standard Specification Compliant	DOCSIS 2.0. This is the specification to which the gateway's cable interface is compatible.
	Hardware Version	The hardware version of the gateway.
	Software Version	The software version of the gateway.
	Cable MAC Address	The MAC address used by the cable modem port of the gateway. This MAC address may need to be registered with your cable service provider.
	Device MAC Address	The MAC address 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 Screen Settings (continued)

Setting		Description
Status	System Up Time	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 the gateway, as seen from the Internet.

Connection Status

Under the Maintenance heading on the main menu, select Connection. The Connection screen appears:

The screenshot shows the 'Connection' screen with the following data:

Startup Procedure			
Procedure	Status	Comment	
Acquire Downstream Channel	565778200 Hz	In Progress	
Connectivity State	In Progress	Not Synchronized	
Boot State	In Progress	Unknown	
Configuration File	In Progress		
Security	Disabled	Disabled	

Downstream Channel			
Lock Status	Not Locked	Modulation	unknown
Channel ID	0	Symbol rate	Unknown
Downstream Frequency	565778200 Hz	Downstream Power	-28.7 dBmV
SNR	23.4 dB		

Upstream Channel			
Lock Status	Not Locked	Modulation	QPSK
Channel ID	0	Symbol rate	0 Ksym/sec
Upstream Frequency	0 Hz	Upstream Power	8.3 dBmV

Current System Time:

Figure 4-1

This screen shows detailed information about the status of your cable service provider connection that can be used for troubleshooting. The gateway goes through these steps to be provisioned:

1. Acquire and lock Downstream Channel.
2. Acquire upstream parameters and range.
3. Lock Upstream Channel.
4. Acquire IP Address through DHCP.

The date and time is acquired from your cable service provider as part of the registration procedure.

Viewing and Emailing Event Logs

The gateway logs security-related events such as denied incoming service requests and hacker probes. You can enable e-mail notification to receive these logs in an e-mail message. Log entries are described in the following table.

Table 4-1: Security Log entry descriptions

Field	Description
Description	The type of event and what action was taken if any.
Count	This is a reference number for each event.
Last Occurrence	The date and time the log entry was recorded.
Target	The name or IP address of the destination device of Web site.
Source	The IP address of the initiating device for this log entry.

To receive logs and alerts by e-mail, you must provide your e-mail information in the Email section of the Event Logs screen. From the main menu, select Event Log. The Event Log screen displays:

Time	Priority	Description
Tue Jul 10 14:52:23 2007	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Tue Jul 10 14:52:19 2007	Critical (3)	DHCP FAILED - Discover sent, no offer received
Tue Jul 10 14:51:44 2007	Critical (3)	No Ranging Response received - T3 time-out
Time Not Established	Critical (3)	DHCP WARNING - Non-critical field invalid in response.
Time Not Established	Critical (3)	No Ranging Response received - T3 time-out
Time Not Established	Critical (3)	Resetting the cable modem due to console command
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Critical (3)	Resetting the cable modem due to console command

Figure 4-2

To enable emailing of logs:

1. In the **Contact Email Address** field, type the e-mail address to which the logs will be sent. Use a full e-mail address (for example, ChrisXY@myISP.com).
2. In the **SMTP Server Name** field, type the outgoing SMTP mail server of your ISP (for example, mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this field blank, no alerts or logs will be sent.
3. Select the **E-mail Alerts Enable** check box.
4. Click **E-mail Log** to send the log immediately
5. Click **Apply**.

Restoring Factory Default Configuration Settings

The configuration settings are stored in a configuration file in the gateway. You can use Erase to restore the factory default configuration settings. The default settings are listed in “[Factory Default Settings](#)” in [Appendix A](#).

To erase the configuration settings and return them to the factory default settings:

1. Under the Maintenance heading on the main menu, select Set Password.

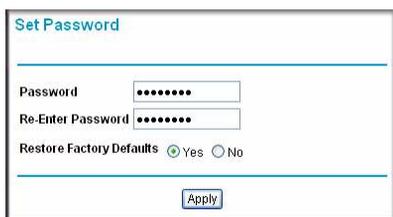


Figure 4-3

2. For **Restore Factory Defaults**, select **Yes**.
3. Click **Apply**. The gateway reboots.

After an erase, the gateway user name is **admin** and the password is **password**. The LAN IP address is 192.168.0.1, and the DHCP client is enabled.



Note: To restore the factory default configuration settings without knowing the login password or IP address, use the reset button on the rear panel of the gateway. Use a paper clip to press the button for at least 5 seconds.

Running Diagnostic Utilities

You can use diagnostics to test connectivity to a PC with the ping command. From the main menu, below the Maintenance heading, select Diagnostics. The Ping screen appears:

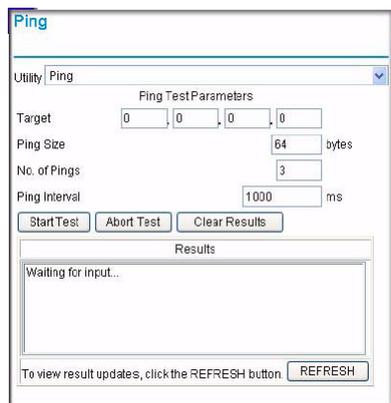


Figure 4-4

To perform a ping test:

1. In the **Target** field, enter the IP address of the PC that you want to ping.
2. If you want to specify additional details, you can set the Ping Size, No. of Pings, and the Ping Interval.
3. Click **Start Test** to begin the test. Test results are displayed on this screen.
 - To stop a test in progress, click **Abort Test**.
 - To delete the results of a ping test from the Results display, click **Clear Results**.
 - To update the results of a ping test, click **REFRESH**.

Setup Features

Setup features include viewing the MTA status, guest network, and Wi-Fi Multimedia (WMM).

Viewing MTA Status

The MTA Status screen shows the status of the voice ports on the gateway. From the main menu, under the Setup heading, select MTA Status. The MTA Status screen appears:



Information	
MTA Provision Status	Not Ready
MTA MAC Address	00:14:6c:ba:02:2e
MTA IP Address	---
MTA FQDN	[N/A]
Mta Telephony Signaling	MGCP

Figure 4-5

Guest Network

The guest network feature allows you to set up an additional wireless guest network. From the main menu, under the Setup heading, select Guest Network. The Wireless Guest Network Setting screen appears:



Wireless Guest Network Settings

Guest LAN Settings

DHCP Server: Disabled

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Lease Pool Start: 192.168.2.10

Lease Pool End: 192.168.2.99

Lease Time: 86400

Restore Guest Network Defaults

Guest WiFi Settings

Enable Guest Network

Guest Network Name (SSID):

Apply

Figure 4-6

See the NETGEAR online help for assistance with setting up a wireless guest network.

Wi-Fi Multimedia (WMM)

The Voice Gateway includes Wi-Fi Multimedia (WMM), which is a Quality of Service (QoS) feature. This feature is enabled, and the Voice Gateway uses it automatically with clients running applications that support WMM.

WMM QoS provides prioritization of wireless data packets from different applications based on four categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM-enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

From the main menu, under the Setup heading, select Wi-Fi Multimedia. The Wi-Fi Multimedia screen appears:



Figure 4-7

The default setting is **Auto**. You can change the setting to **On** or **Off**. If you make a change, click **Apply** to change the settings.

LAN IP Settings

The gateway is preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The LAN IP settings are explained below:

- **LAN IP address.** This is the IP address of the gateway. The default is 192.168.0.1.



Note: If you change the LAN IP address of the gateway while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again

- **Subnet mask.** This is the LAN subnet mask of the gateway. The default is 255.255.255.0. Combined with the IP address, the subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN IP page.

- **DHCP Server.** By default, the gateway is a Dynamic Host Configuration Protocol (DHCP) server. See [“Using the Gateway as a DHCP Server” on page 4-8.](#)
- **Starting Address and Ending Address.** 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 192.168.0.10 and 192.168.0.253. The range of IP addresses between 192.168.0.2 and 192.168.0.9 can be used for devices with fixed (or static) addresses.
- **DHCP Reservation Lease Info.** View information about each PC that has been assigned a DHCP lease by the gateway. The MAC address of the PC, IP address assigned and the expiration time of the DHCP lease are listed. You can manually revoke the DHCP leases by clicking Clear DHCP Leases.

Using the Gateway as a DHCP Server

By default, the gateway is a DHCP server. It can assign IP, DNS server, and default gateway addresses to all computers connected to the LAN. The default wireless voice gateway address is its LAN address. The wireless voice gateway assigns IP addresses to the network computers from a pool of addresses specified in the Starting Address and Ending Address fields. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.



Note: If another device on your network is the DHCP server, or if you will manually configure the network settings of all of your computers, select No for the DHCP Server. For more information about DHCP and IP addresses, see the link to [“Preparing a Computer for Network Access:” in Appendix B.](#)

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

- An IP Address from the range you have defined.
- Subnet Mask.
- Gateway IP Address is the gateway’s LAN IP address.
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings page; otherwise, the gateway’s LAN IP address.

- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings page.



Note: The gateway implements a DNS Relay function. When it receives a DNS request on the LAN, it passes it to the DNS server specified on the WAN. It then relays the response back to the original requesting PC.

Configuring the LAN IP Settings

You can use the LAN IP Setup page to configure LAN IP services such as the IP address of the gateway and DHCP.

To configure the LAN IP:

1. Under the Advanced heading on the main menu, select LAN IP. The LAN IP screen displays.

Figure 4-8

2. Enter the following information:
 - **LAN IP Address.** The LAN IP address that you want to assign to your gateway. The default is 192.168.0.1.
 - **Subnet Mask.** The subnet mask for your network IP address. The default is 255.255.255.0. (Unless you are implementing subnetting, use the default subnet mask.)
 - **DHCP Server.** To assign IP addresses to your computers automatically, select Yes. To disable the DHCP Server and assign IP addresses to your computers manually, select No.



Note: If you select no for the DHCP server setting, then you must assign a static IP address to your PC in order to reconnect to the gateway and enable the DHCP server again.

- **Starting IP Address.** Enter the first of the contiguous addresses in the address pool. The default start address is 192.168.0.10.
- **Ending IP Address.** Enter the last of the contiguous addresses in the address pool. The default end address is 192.168.0.19.

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

To configure DHCP server reservation parameters for your LAN:

1. Enter the MAC address of the PC for which you want to reserve an IP Address.
2. Enter a free IP Address for the PC.
3. Click **Add**.

To remove a reserved IP from the DHCP Reservation Lease Info table:

1. Select the radio button adjacent to the entry that you want to remove from the table.
2. Click **Delete**.

The DHCP Client Lease details for all computers in the LAN gateway are shown in the DHCP Client Lease Info table. To clear all DHCP Client leases, click **Clear DHCP Leases**.

Remote Management Access

You can use remote management to configure, upgrade, and check the status of your gateway through the Internet.

To configure remote management:

1. Under the Advanced heading on the main menu, select Remote Management. The Remote Management screen appears:

Remote Management

Allow Remote Management

Remote User Name:

Remote Password:

Port Number:

Revert to factory default settings:

Allow Remote Management after Factory Default Reset

IP Address to connect this device:

Figure 4-9

2. Select the **Allow Remote Management** check box.
3. Enter the **Remote User Name** and **Remote Password** that will be required to remotely access your gateway.
4. Enter the **Port Number** that will be used for accessing the management interface.

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 box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. To make sure that you can use remote management even if the wireless voice gateway is reset, select the **Allow Remote Management after Factory Default Reset** check box.

If you do not select this check box, you will not be able to remotely access the gateway if you use the Erase feature to revert to the Factory Default settings.

6. Click **Apply** to have your changes take effect.

When accessing your wireless voice gateway from the Internet, type the WAN IP address of your gateway into your browser, followed by a colon (:) and the port number. For example, if your WAN IP address is 134.177.0.123 and you use port number 8080, type the following in your browser:

http://134.177.0.123:8080

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.

UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

Other features of UPnP:

- **Advertisement Period.** The number entered in this field (in minutes) determines how often the router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 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.** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then you may need to increase this value a little.
- **UPnP Portmap Table.** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

To activate UPnP:

1. From the main menu, select UPnP. The UPnP screen displays:

Active	Protocol	Int. Port	Ext. Port	IP Address
--------	----------	-----------	-----------	------------

Figure 4-10

2. Select the **Turn UPnP On** check box, and then click **Apply**.

To save, cancel or refresh the table:

- To save the new settings to the gateway router, click **Apply**.
- To disregard any unsaved changes, click **Cancel**.
- To update the UPnP Portmap table and to show the active ports that are currently opened by UPnP devices, click **Refresh**.

Chapter 5

Troubleshooting

This chapter gives information about troubleshooting your gateway. For the common problems listed, go to the section indicated.

- Is the gateway on?
- Have I connected the gateway correctly?
Go to [“Basic Functions” on page 5-1.](#)
- I cannot access the gateway’s configuration with my browser.
Go to [“Connecting to the Wireless Voice Gateway Main Menu” on page 5-2.](#)
- I have configured the gateway but I cannot access the Internet.
Go to [“Troubleshooting the ISP Connection” on page 5-3.](#)
- I cannot remember the gateway’s password.
- I want to clear the configuration and start over again.
Go to [“Restoring Factory Default Configuration Settings” on page 4-4.](#)

Basic Functions

After you turn on power to the gateway, the following sequence of events should occur:

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:
 - a. The LAN LEDs are lit for any local ports that are connected.
 - b. The Internet Link port LED is lit.

If any of these conditions does not occur, see the table below:

Table 5-1. Basic Troubleshooting with LEDs

Problem	Action
Power LED is off. 	If the Power and other LEDs are off when your gateway is turned on: <ul style="list-style-type: none"> • 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 when the gateway is turned on.	<ul style="list-style-type: none"> • Clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in "Restoring Factory Default Configuration Settings" on page 4-4. • If the error persists, you might have a hardware problem and should contact technical support.
LAN LEDs are off, but ports are connected. 	Check the following: <ul style="list-style-type: none"> • Make sure that the Ethernet cable connections are secure at the gateway and at the hub or PC. • Make sure that power is turned on to the connected computer. • Be sure you are using the correct cable: When connecting the gateway use the cable that was supplied.

Connecting to the Wireless Voice Gateway Main Menu

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

- Check the Ethernet connection between the PC 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 ["Preparing a Computer for Network Access:"](#) in [Appendix B](#) for more information about IP address configuration.



Note: If your PC's IP address is shown as 169.254.x.x:
Recent versions of Windows and Mac OS 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 ["Restoring Factory Default Configuration Settings" on page 4-4](#).
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The 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, check the following:

- When entering configuration settings, be sure to click **Apply** before moving to another menu or page, 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 Device MAC Address of you gateway with your cable service provider. This is described in ["Installing the Voice Gateway" on page 1-3](#).

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 as described in ["Preparing a Computer for Network Access:" 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 ping the gateway from your PC to verify that the LAN path is set up correctly.

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

1. From the Windows toolbar, click **Start**, and then 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 functioning correctly, you could have one of the following problems:

- Wrong physical connections
 - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in [“LAN LEDs are off, but ports are connected.” on page 5-2](#)”.
 - 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 working 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 as described in [“Preparing a Computer for Network Access:” 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 page.
- Your ISP could be rejecting the Device MAC Address of your gateway because it does not match the MAC Address of the PC you previously used to connect to a cable modem. In this case you will need to clone your PC's MAC Address. Refer to [“Installing the Voice Gateway” on page 1-3](#).

Appendix A

Default Settings and Technical Specifications

Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the Test LED blinks rapidly). Your device will return to the factory configuration settings shown in the table below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Feature	Description
Smart Wizard	Enabled
Gateway Login	
Gateway login URL	http://192.168.0.1
Login name	admin
Password	password
Internet Connection	
WAN MAC address	Use default hardware address
MTU Size	1500
Local Network	
LAN IP Address (aka Gateway IP address)	192.168.0.1
Gateway subnet mask	255.255.255.0
DHCP server	Enabled
LAN IP starting IP address	192.168.0.10
LAN IP ending IP address	192.168.0.19
Static IP address pool	192.168.0.2 to 192.168.0.9 inclusive

Feature		Description
Wireless		
	Wireless communication	Enabled
	Wireless network name (SSID)	Unique for each wireless voice gateway. It is printed on the product label.
	Security	WEP (Wired Equivalent Privacy) 128-bit encryption
	WEP Keys	Unique for each wireless voice gateway. It is printed on the product label.
	SSID Broadcast	Enabled
	Turn Radio On	Enabled
	Default Channel	6
	Operating Mode	802.11g and 801.11b
	Country/Region	Default is United States in US; selectable in ROW
	Wireless Card Access List	Off
	Security	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests except for traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	DMZ Host	Disabled
	UPnP	Disabled
	VPN Pass-Through	Enabled
	Multicast	Enabled
	Remote Management	Disabled

Technical Specifications

The table below describes the technical specifications for the Wireless Cable Voice Gateway .

Feature	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)	North America (input) 120V, 60 Hz, input
All regions (output)	15 V DC @ 1.2A output, 15W maximum
Physical specifications	
Dimensions	6.9 by 4.5 by 1.2 in. (175 by 114 by 30 mm)
Weight	0.68 lb (0.31 kg)
Environmental Specifications	
Operating temperature	32° to 140° F (0° to 40° C)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	Meets requirements of: FCC Part 15 Class B
Interface Specifications	
Local	10BASE-T or 100BASE-Tx, RJ-45 USB 1.1 Function 802.11g and 802.11b wireless access point
Internet	DOCSIS 2.0. Downward compatible with DOCSIS 1.0 and DOCSIS 1.1.

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

Numerics

192.168.0.1, default login *1-6, 2-4, 3-1, 3-3, 3-7*

B

Basic Settings *1-7, 1-8*

blocking

- outbound traffic *3-8*
- Web sites *3-3*

C

Coaxial cable

- connection location *1-3*

coaxial cable *1-4*

computer connections

- LAN port to gateway *1-4*

connected wireless devices

- adding to *2-13*
- list of *2-13*

Content Filtering *3-4, 3-5*

D

default gateway login *1-6*

default settings

- restoring *4-4*

default Subnet mask *4-7*

Denial of Service attacks DoS. See Denial of Service attacks.

DHCP Client

- reservations leases *4-10*

DHCP server *4-8, 4-9*

- configuring reservation parameters *4-10*
- default use *4-8*
- reservation parameters *4-10*

DMZ Host *3-13*

DMZ Server

- as Host *3-13*

DNS Address *1-4*

DNS Relay *4-9*

DNS server *1-8*

Domain Name *1-4*

Domain Name Server Address. See DNS Address

E

Ethernet Network Interface Card *1-4*

F

factory default settings

- list of *A-1*
- reset button, using *4-4*
- restoring *4-4*

Firewall Features *3-6*

firewall rules

- inbound traffic *3-8*
- LAN to WAN *3-8*
- outbound traffic *3-8*
- WAN to LAN *3-8*

Fixed IP address pool. See Static IP address pool

Fixed IP Address. See Static IP Address

forwarding inbound traffic *3-10*

front panel *1-1*

front panel diagram *1-1*

G

gaming

- port triggering *3-12*
- setting up DMZ Host *3-13*

gateway

- connection diagram 1-4
- default IP address 4-7
- default login 1-6
- placement of 2-2, 2-4

I

- Inbound Rules 3-10
- inbound traffic 3-8
 - forwarding of 3-10
 - open ports 3-12
- Internet Relay Chat
 - port triggering, used with 3-12
- IP address pool 4-8
- IP addresses
 - auto-generated 5-3
- IPSec 3-6
- IRC. See Internet Relay Chat

K

- keyword blocking 3-3
 - adding keywords 3-4

L

- LAN IP
 - address pool 4-10
 - configuring 4-9
 - default address 4-7

- LEDs
 - description 1-1

M

- MAC address 5-5
 - location of 2-13
 - restricting access 2-12
- MAC filtering 3-6
- Multicast 3-6

N

- Network Access

- about B-1

- network configuration
 - Dynamic IP Address 1-8
 - Static IP Address 1-8

- NIC. See Ethernet Network Interface Card

O

- Outbound Rules 3-8
- outbound traffic
 - blocking of 3-8
 - rules 3-8

P

- parental controls 3-3
 - blocking key words 3-3
 - blocking Web sites 3-3
 - content filtering services 3-5
 - MAC filtering 3-6
- Passphrase
 - WEP, use with 2-7
 - WPA-PSK, use with 2-8
- password, default password 3-7
- ping command 4-5
- port blocking 3-8
- port forwarding 3-10
- port triggering 3-12
 - gaming setup 3-12
- PPTP 3-6

Q

- Quality of Service (QoS) 4-7

R

- rear panel diagram 1-3
- remote management 4-10
- Reset button 1-3
- restricting access 2-12
 - MAC address 2-12
 - wireless card access list 2-12

Rules

- inbound 3-10
- outbound 3-8

S

- security, adding WEP. See Wireless Settings
- security, adding WPA-PSK. See Wireless Settings
- SPI. See Stateful Packet Inspection 3-6
- Stateful Packet Inspection 3-6
- Static IP Address 1-4
- Static IP address pool 4-8
- Subnet mask, default 4-7
- superuser, default parent login 3-7

T

- TCP/IP
 - connections, troubleshooting 5-4
- technical specifications A-3
- test connectivity
 - ping command, using 4-5
- troubleshooting 5-1
 - gateway connection 5-2
 - Internet connection 5-3
 - LAN to gateway 5-4
 - PC to remote device 5-5
 - ping command 5-4
 - power LEDs 5-1

U

- Universal Plug and Play. See UPnP
- UPnP 4-12
- USB
 - driver install 1-5
 - gateway, connection to 1-5
 - host port 1-4
 - operating system requirements 1-5
 - port location 1-3

V

- video conferencing

- setting up DMZ Host 3-13

- VPN Pass-Through 3-6

W

- Web Features 3-6
- Web site blocking 3-3
- Web sites
 - blocking of 3-3
- WEP, configuring 2-7
- Wi-Fi Multimedia (WMM) 4-7
- wireless
 - antenna location 2-2
 - channel setup 2-2
 - connection latency 2-2
 - interference 2-2
 - range 2-2
 - settings form 2-3
- wireless adapter
 - 802.11b 1-4
 - 80211g 1-4
- wireless communications, about B-1
- Wireless Settings
 - configuring 2-4
 - WEP, configuring 2-7
 - WPA2-PSK, configuring 2-10
 - WPA-PSK, configuring 2-8
- WPA2-PSK, configuring 2-10
- WPA-PSK, configuring 2-8

