

NETGEAR®

Broadband ADSL2+ Modem DM111PSPv2 User Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

August 2011
202-10913-01
v1.0

© 2011 NETGEAR, Inc. All rights reserved

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at <http://support.netgear.com>.

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

Phone (Other Countries): Check the list of phone numbers at http://support.netgear.com/app/answers/detail/a_id/984.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

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

Contents

Chapter 1 Hardware Setup

- Unpack Your New Modem. 7
- Hardware Features 8
 - Label 8
 - Back Panel. 8
 - Front Panel 9
- ADSL Microfilters. 10
 - One-Line ADSL Microfilter. 10
 - Two-Line ADSL Microfilter. 10
 - Summary 11
- Cable Your Broadband ADSL2+ Modem to a Computer. 11
- Cable Your Modem to a Router. 13

Chapter 2 Modem Internet Setup

- Modem Setup Preparation. 15
 - Gather ISP Information 15
- NETGEAR Genie CD Setup 15
 - View or Change Settings. 16
 - Settings Description. 16
- Log In to the Modem 17
- Upgrade Modem Firmware 18
- Modem Interface 19
- Setup Wizard 20
- Manual Setup (Basic Settings) 21
- ADSL Settings 24
- Unsuccessful Internet Connection. 25
- Change Password and Login Time-Out 25
- Log Out Manually 26
- Types of Logins 26

Chapter 3 Security Settings

- Keyword Blocking of HTTP Traffic. 28
 - Delete a Keyword or Domain. 28
 - Specify a Trusted Computer 29
- Firewall Rules to Control Network Access. 29
 - Remote Computer Access Basics 29
 - Open Inbound Ports (Port Forwarding) 30
 - Inbound Rules to Permit External Host Communications 32

- How Inbound Rules Differ from Outbound Rules 33
- Configure Firewall Rules 33
- Inbound Rules (Port Forwarding) 34
- Outbound Rules (Service Blocking) 36
- Configure Services 38
- Set the Time Zone 39
- Schedule Firewall Services 40
- Enable Security Event Email Notification 41

Chapter 4 Network Maintenance

- Upgrade the Modem Firmware. 44
 - Turn Off Automatic Firmware Checking 44
 - Automatic Firmware Checking On 45
- Manually Check for Firmware Upgrades 46
- Manage the Configuration File 47
 - Back Up 47
 - Restore. 47
 - Erase 48
- View Modem Status 48
- View Attached Devices. 51
- Run Diagnostic Utilities 52

Chapter 5 Advanced Settings

- WAN Setup. 54
- Dynamic DNS. 56
- LAN Setup 57
 - Access Modem Interface on Additional Port. 58
 - Use Modem as DHCP Server. 58
 - Reserved IP Address Setup 59
- Remote Management. 59
- Static Routes 61
 - Static Route Example. 61
 - Configure Static Routes 62
- Universal Plug and Play 63
- Change the Device Mode. 64

Chapter 6 Troubleshooting

- Modem Is Off 66
 - Power LED Is Off 66
 - Power LED Is Red 67
 - Ethernet LED Is Off 67
- No Internet Connection 67
 - DSL Link. 67
 - Internet LED Is Red 68
 - Cannot Obtain an Internet IP Address 68
 - Debug PPPoE or PPPoA 69

Cannot Load an Internet Web Page	70
TCP/IP Network Not Responding	70
Test the LAN Path to Your Modem	70
Test the Path from Your Computer to a Remote Device	71
Cannot Log in	71
Changes Not Saved	72
Firmware Needs to Be Reloaded	72
Incorrect Date or Time	73

Appendix A Technical Specifications

Factory Settings	75
Technical Specifications	76

Appendix B Notification of Compliance

Index

Hardware Setup

1

Getting to know your modem

The Broadband ADSL2+ Modem DM111PSPv2 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It has a built-in DSL modem, is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and can protect the devices (PCs, gaming consoles, and so on) that you connect to your home network.

If you have not already set up your new modem using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Modem Internet Setup*, explains how to set up your Internet connection.

For more information about the topics covered in this manual, visit the support website at <http://support.netgear.com>. If you want instructions about how to wall-mount your modem, see Wall-Mount Your Router at http://support.netgear.com/app/answers/detail/a_id/18725.

This chapter contains the following sections:

- *Unpack Your New Modem*
- *Hardware Features*
- *ADSL Microfilters*
- *Cable Your Broadband ADSL2+ Modem to a Computer*
- *Cable Your Modem to a Router*

Unpack Your New Modem

Your box should contain the following items:

- Broadband ADSL2+ Modem DM111PSPv2
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilter/splitter
- Installation guide with cabling and modem setup instructions
- *Resource CD* with NETGEAR Genie setup

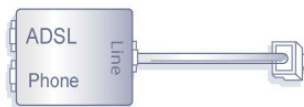
If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair. See [ADSL Microfilters](#) on page 10 for information about where to place and how to position your modem.



Resource CD



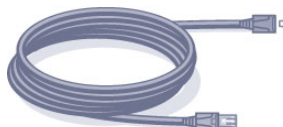
ADSL2+ modem



Filter/splitter



Modem stand



Telephone cable



Ethernet cable



Power adapter

Figure 1. Review the box contents

Hardware Features

Before you cable your modem, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Label

The label on the bottom of the modem shows the MAC address and serial number.

Back Panel

The back panel has the On/Off button and port connections as shown in the figure.

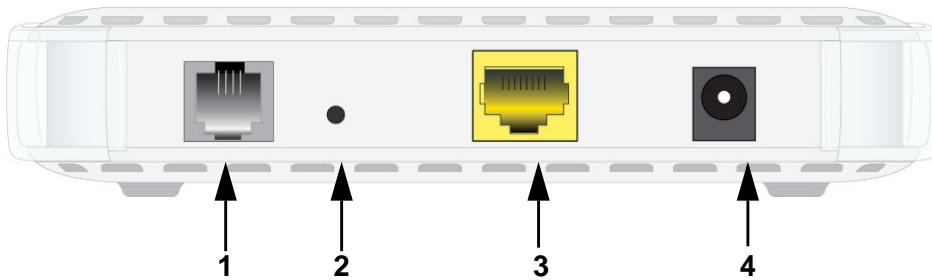


Figure 2. Back panel port connections

Viewed from left to right, the rear panel contains the following elements:

1. RJ-11 asynchronous DSL (ADSL) port for connecting the modem to a DSL line

Note: An ADSL port is capable of sending data over a DSL line at one speed and receiving it at another speed.

2. Restore Factory Settings button
3. One Ethernet RJ-45 Ethernet port for cabling the modem to a computer
4. AC power adapter input

Front Panel

The modem front panel has the status LEDs and icons shown in the following figure.

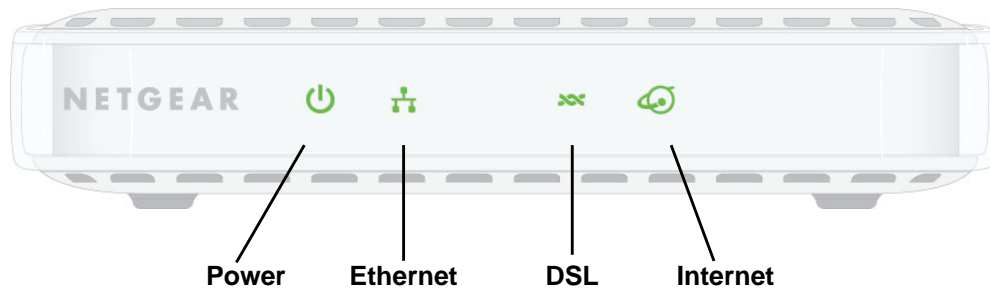






Figure 3. Front panel LED Icons

The following table describes the LEDs and icons on the front panel from left to right.

Table 1. LEDs

LED	Description
Power 	<ul style="list-style-type: none"> • Solid green. Power is supplied to the modem. • Solid red. POST (power-on self-test) failure or a device malfunction has occurred. • Off. Power is not supplied to the modem. • Restore factory settings. The LED blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the gateway resets to the factory defaults.
Ethernet 	<ul style="list-style-type: none"> • Solid green. The port has detected an Ethernet link with a device. • Blinking green. Data is being transmitted or received. • Off. No link is detected on the port.
DSL 	<ul style="list-style-type: none"> • Solid green. You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP's network-access device. • Blinking green. Indicates that the broadband ADSL2+ modem is negotiating the best possible speed on the DSL line. • Off. The unit is off or there is no DSL connection.
Internet 	<ul style="list-style-type: none"> • Solid green. You have an Internet connection. If this connection is dropped due to an idle time-out but the DSL connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off. • Blinking green. Data is being transmitted over the DSL port. • Solid red. The Internet (IP) connection failed. See No Internet Connection on page 67 for troubleshooting information. • Off. No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).

ADSL Microfilters

If this is the first time you have cabled a wireless modem between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to [Cable Your Broadband ADSL2+ Modem to a Computer](#) on page 11.

An ADSL microfilter is a small in-line device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries DSL service. That depends on the DSL service setup in your home.

Note: Often the ADSL microfilter is included in the box with the modem. If you purchased the broadband ADSL2+ modem in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem plugs directly into a separate DSL line. Plugging the wireless modem into the phone jack blocks the Internet connection. If you do not have a separate DSL line for the modem, the best thing to do is to use an ADSL microfilter with a built-in splitter (see the next paragraph).



Figure 4. One-line ADSL microfilter

Second best when you do not have a separate DSL line for the modem is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the broadband ADSL2+ modem and your telephone equipment. Plug the

ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the wireless modem into the jack labeled ADSL.

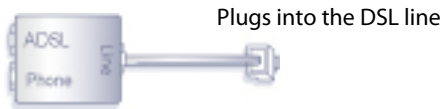


Figure 5. Two-line ADSL microfilter with built-in splitter

Summary

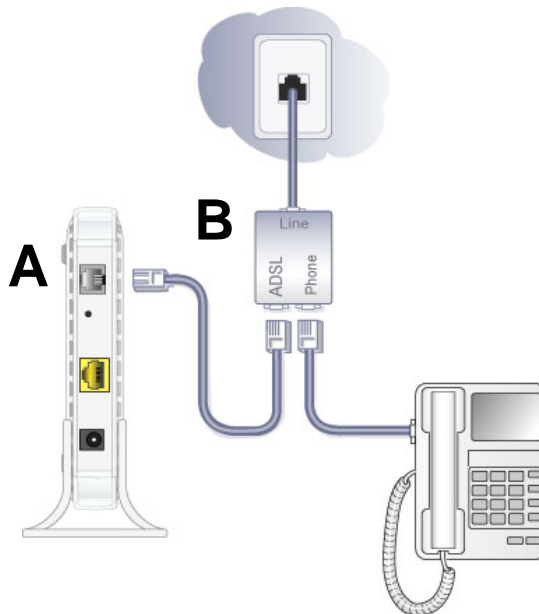
- One-line ADSL microfilter: Use with a phone or fax machine.
- Splitter: Use with a one-line ADSL microfilter to share an outlet with a phone and the modem.
- Two-line ADSL microfilter with built-in splitter: Use to share an outlet with a phone and the modem.

Cable Your Broadband ADSL2+ Modem to a Computer

The installation guide that came in the box has a cabling diagram on the first page. This section walks you through the cabling procedure with detailed illustrations.

➤ To cable your modem:

1. Put an ADSL microfilter between the phone line and the phone as shown here. The illustration shows a two-line ADSL microfilter with built-in splitter. The phone plugs into the phone jack as shown.



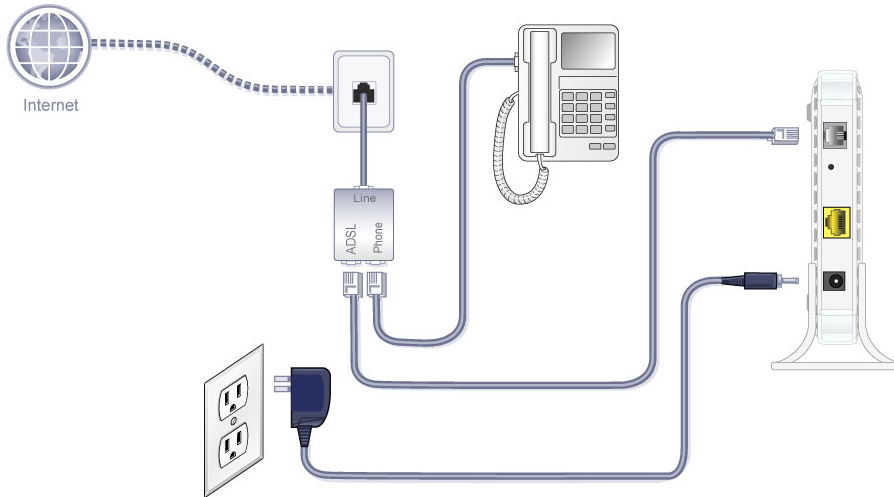
2. Use the included phone cable with RJ-11 jacks to connect the ADSL port (A) of the broadband ADSL2+ modem to the ADSL port (B) of the two-line ADSL microfilter.



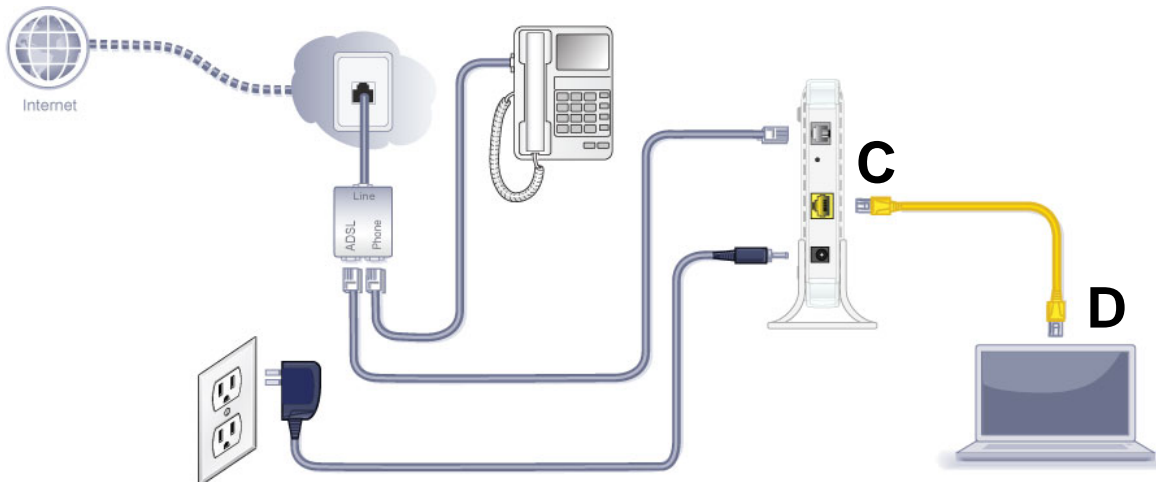
CAUTION:





Incorrectly connecting a filter to your broadband ADSL2+ modem blocks your DSL connection.

3. Connect the power adapter cord that came in the package to your modem, and plug it into an electrical outlet.



4. Connect the Ethernet cable (C) from the modem Ethernet port to the Ethernet adapter (D) in your computer.



5. Verify that your modem is cabled correctly by checking the LEDs.
 -  The Power LED is green.
 -  The Ethernet LED is green.
 -  The DSL LED is green when you have a DSL connection.
 -  The Internet LED is red when there is no Internet connection.

Cable Your Modem to a Router

The modem includes a built-in router, but you can connect it to a router if you want.

➤ **To use the broadband ADSL2+ modem with a router:**

1. Install the modem with the standard PC connection in Router mode.

The installation guide that shipped in the package shows how to do this. It is also explained in *Cable Your Broadband ADSL2+ Modem to a Computer* on page 11.

2. Set up the modem to work with your Internet connection.

See *Chapter 2, Modem Internet Setup*.

3. If you are an advanced user who wants to set up the modem to run in “pure bridge” or Modem mode, you need to log in to the modem and change the Device Mode setting to Modem mode.

See *Change the Device Mode* on page 64.

4. Follow the instructions that came with your router to install the router to work with the modem.

2 Modem Internet Setup

2

Connecting to the Internet

This chapter explains how to set up your Internet connection using one of these methods: use the Installation Guide with NETGEAR Genie CD (recommended), log in to the modem and use its Setup Wizard, or manual set up. If you have already set up your modem using one of these methods, the initial modem setup is complete. Refer to this chapter if you want to become familiar with the modem menus, view or adjust the initial settings, or change the modem password and login time-out.

This chapter contains the following sections:

- *Modem Setup Preparation*
- *NETGEAR Genie CD Setup*
- *Log In to the Modem*
- *Upgrade Modem Firmware*
- *Modem Interface*
- *Setup Wizard*
- *Manual Setup (Basic Settings)*
- *ADSL Settings*
- *Unsuccessful Internet Connection*
- *Change Password and Login Time-Out*
- *Log Out Manually*
- *Types of Logins*

Modem Setup Preparation

You can set up your modem with the NETGEAR Genie as described in *NETGEAR Genie CD Setup* on page 15, with the Setup Wizard as described in *Setup Wizard* on page 20, or manually as described in *Manual Setup (Basic Settings)* on page 21. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, PCs, and other devices in the network have the settings described here.

Note: If you have a Macintosh or Linux system, you have to use the manual setup method.

Gather ISP Information

You need the following information to set up your modem and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your broadband ADSL2+ modem automatically logs you in.

- Active Internet service provided by a DSL account
- The ISP configuration information for your DSL account
 - ISP login name and password
 - ISP Domain Name Server (DNS) addresses
 - Fixed or static IP address
 - Host and domain names
 - Depending on how your ISP set up your Internet account, you could need to know one or more of these settings for a manual setup:
 - Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
 - Multiplexing method
 - Host and domain names

NETGEAR Genie CD Setup


Use the printed installation guide in the package together with NETGEAR Genie on the *Resource CD*. NETGEAR Genie runs on a PC with Microsoft Windows 7, Windows Vista, Windows XP, or Windows 2000 with Service Pack 2 or later. It is the easiest way to set up the modem because it automates many of the steps and verifies that those steps have been successfully completed. It takes 20 to 30 minutes to complete.

Before running the NETGEAR Genie on a corporate PC, check with your company's network support staff. Corporate network settings or virtual private network (VPN) client software


might conflict with the default settings of a home modem. If you are unsure about whether there might be a conflict, use a different computer.

➤ **To run NETGEAR Genie:**

1. Locate the DSL settings information (user name and password) provided by your ISP. Contact your ISP if you do not have it.
2. Follow the instructions in the printed Installation Guide in the package to to cable and power up the modem.
3. Insert the *Resource CD* into your Windows PC. The CD automatically starts and detects the language you are using on your PC. Select a different language option, if you prefer.


Note: If the CD does not start, go to the CD drive (under My Computer on Windows), browse the CD, and double-click  .

4. When the Welcome screen displays, click **Setup** to start the Genie. Follow the instructions to complete the setup. NETGEAR Genie checks your hardware setup and guides you through connecting the modem to the Internet and adding computers to your network.

Your modem connects to the Internet when any of the computers connected to your network require access. When you launch a web browser to access the Internet, the modem's Internet LED  blinks to indicate ISP communication.

View or Change Settings

You can view and change the settings in the following ways:

- Log in to your modem by clicking the desktop shortcut  that was placed on your desktop during the NETGEAR Genie setup. The shortcut icon is put on your desktop only when you use the NETGEAR Genie setup method.
- Log in to your modem. See [Log In to the Modem](#) on page 17.
- Open the Modem_Setup.html file that was placed on your desktop during the NETGEAR Genie setup. This file provides setup and system information, the NETGEAR technical support number, links to the NETGEAR website, and a modem login link.

Settings Description

When the NETGEAR Genie setup is completed, your modem has the following configuration and informational settings. Some of these settings can be viewed in Router_Setup.html.

Configuration

- Internet connection including language and country as described in [Setup Wizard](#) on page 20.

- WAN port settings. This is your port address type (PPPoE by default) and ISP login name and password. See *Manual Setup (Basic Settings)* on page 21 for more information about address types.

Login and System Information

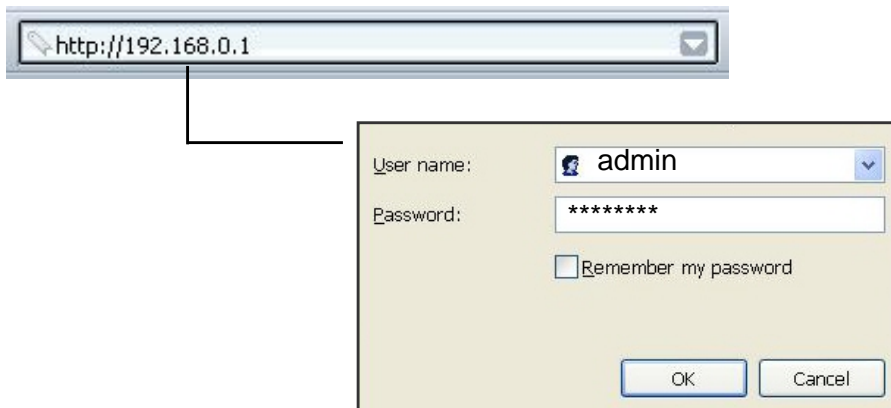
- Modem login. The modem administrator login name and password as described in *Log In to the Modem* on page 17.
- System information. PC operating system, modem serial number, and WAN Port MAC Address.

Log In to the Modem

Log in to the modem to view or change settings or to set up the modem.

➤ To log in:

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window. You can also enter either of these addresses to access the broadband ADSL2+ modem: **http://www.routerlogin.net** or **http://www.routerlogin.com**.



2. When prompted, enter **admin** for the modem user name and **password** for the modem password, both in lowercase letters.

Note: The modem user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 26 for more information.

If you do not see the login prompt:

1. Check the LEDs on the modem front panel to make sure that the modem is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the modem is connected to an Ethernet port.

2. If you connected the Ethernet cable and quickly launched your browser and typed in the modem URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the modem wirelessly, NETGEAR recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the modem.

Note: If you cannot connect to the wireless modem, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation for more information.

Upgrade Modem Firmware

When you log in and if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest available firmware. See [Chapter 4, Network Maintenance](#), for more information about upgrading firmware.

1. Click **Yes** to check for new firmware (recommended). The modem checks the NETGEAR database for new firmware.
2. If no new firmware is available, click **No** to exit. You can check for new firmware later.
3. If new firmware is available, click **Yes** to upgrade the modem with the latest firmware. After the upgrade, the modem restarts.



CAUTION:

Do not try to go online, turn off the modem, shut down the computer, or do anything else to the modem until the modem finishes restarting and the Power LED has stopped blinking for several seconds.

You cannot upgrade firmware until you have established your Internet connection as described in [Setup Wizard](#) on page 20.

Modem Interface

The modem interface gives you access to the modem's current settings so you can view or change them (if needed). The left column has the modem menus, and the right column provides online help. The middle column is the screen for the current menu option.

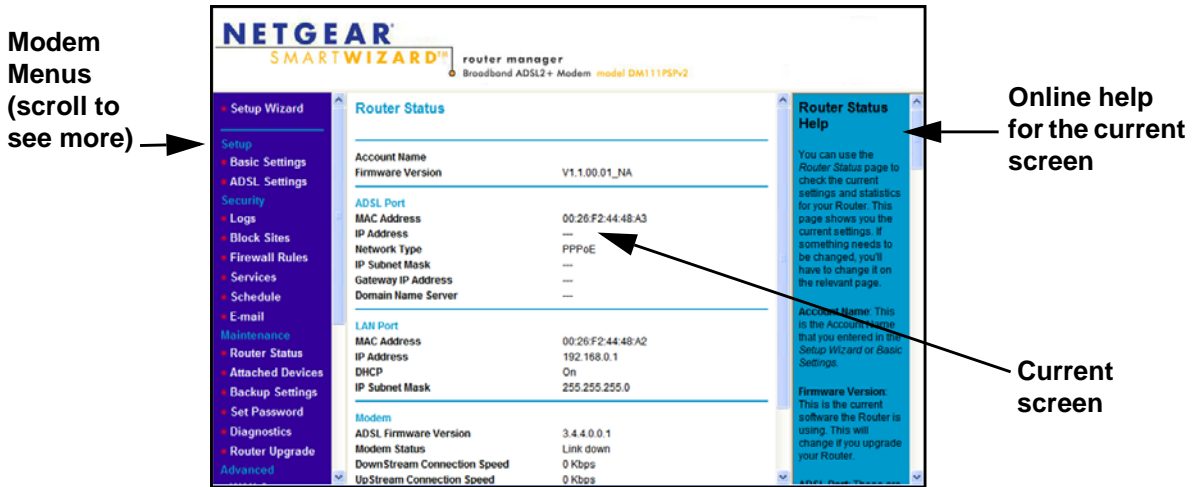


Figure 6. Modem menus in Router mode, Router Status screen, and online help

Note: If you go to the Advanced Device Mode screen and change the device mode setting to Modem Mode, then menu items not supported in Modem Mode will be grayed out.

- **Setup Wizard.** Specify the language, location, and automatically detect the Internet connection. See *Setup Wizard* on page 20.
- **Setup menu.** Set and check the ISP settings of your modem. See *Manual Setup (Basic Settings)* on page 21 and *ADSL Settings* on page 24.
- **Security menu.** View and configure the modem firewall settings to prevent objectionable content from reaching your PCs. See *Chapter 3, Security Settings*.
- **Maintenance menu.** Administer and maintain your modem and network. See *Chapter 4, Network Maintenance*.
- **Advanced menu.** Set the modem up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 5, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.
- **Web Support.** Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Setup Wizard

If you do not use the NETGEAR Genie CD, you have to log in to the modem to set the country, language, and Internet connection.

Note: If you performed the NETGEAR Genie CD setup, the country, language, Internet, and wireless network settings are already configured.

➤ **To run the Setup Wizard:**

1. Follow the instructions in the installation guide that came in the package to cable and power up the modem.
2. Select **Setup Wizard** from the top of the modem menus to display the following screen:



The screenshot shows the 'Setup Wizard' interface. At the top, it says 'Setup Wizard' in blue. Below that is a section titled 'Select Country and Language'. It has two dropdown menus: 'Country:' with 'USA' selected and 'Language:' with 'English' selected. Below this is another section titled 'Auto-Detect Connection Type'. It contains the text: 'This Setup Wizard can detect the type of Internet connection you have. Do You want The Smart Setup Wizard To try And detect The connection type now?'. There are two radio button options: 'Yes.' (which is selected) and 'No. I want to configure The Router myself.'. At the bottom center, there is a 'Next' button.

3. Select your country and language:
 - **Country.** It is important to specify the location where the broadband ADSL2+ modem operates so that the Internet connection works correctly. In some locations, it is not possible to change this setting.
 - **Language.** This defaults to English. You can select another language if you prefer.
4. Select either **Yes** or **No, I want to configure the Modem myself**. If you select No, proceed to *Manual Setup (Basic Settings)* on page 21.
5. If you selected Yes, click **Next**.

With automatic Internet detection, the Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

Note: The Setup Wizard cannot detect a Point-to-Point Tunneling Protocol (PPTP) connection. If your ISP uses PPTP, you have to set your Internet connection through the screen described in *Manual Setup (Basic Settings)* described on 21.

Manual Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Modem myself in the Setup Wizard and is also available from the modem menus. It is where you view or change ISP information. The fields that display vary depending on whether or not your Internet connection requires a login.

Note: Check that the country and language are set as described *Setup Wizard* on page 20 before proceeding with the manual setup.

➤ To perform a manual setup:

1. Select **Set Up > Basic Settings**, and select **Yes** or **No** depending on whether or not your ISP requires a login. The following Basic Settings screens show both forms of the Basic Settings screen.
 - **Yes.** Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
 - **No.** Enter the account and domain names, as needed.
2. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the DSL settings, and see *ADSL Settings* on page 24 for more information.
3. If no login is required, you can specify the MAC Address setting.
4. Click **Apply** to save your settings.
5. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, see *Troubleshooting* on page 65.

ISP does not require login

ISP does require login

The following descriptions explain all of the possible fields in the Basic Settings screen. Note that which fields appear in this screen depends on whether or not an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

- *When no login is required, these fields display:*

Account Name (If required). Enter the account name provided by your ISP. This might also be called the host name.

Domain Name (If required). Enter the domain name provided by your ISP.

- *When your ISP requires a login, these fields display:*

Encapsulation. Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM).

Login. The login name provided by your ISP. This is often an email address.

Password. The password that you use to log in to your ISP.

Idle Timeout (In minutes). If you want to change the login timeout, enter a new value in minutes. This determines how long the broadband ADSL2+ modem keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- *When a login is required, these fields display:*

Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.

Use Static IP Address. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's broadband ADSL2+ modem to which your broadband ADSL2+ modem will connect.

- *When a login is not required, this field displays:*

Use IP Over ATM (IPoA). Your ISP uses classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

Get Automatically from ISP. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.

Use These DNS Servers. If you know that your ISP does not automatically transmit DNS addresses to the broadband ADSL2+ modem during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). NAT automatically assigns private IP addresses (192.168.0.x) to LAN-connected devices.

Enable. Usually NAT is enabled.

Disable. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure you do not need it. When NAT is disabled, only standard routing is performed by this modem. Classical routing lets you directly manage the IP addresses that the broadband ADSL2+ modem uses. Classical routing should be selected only by experienced users.¹

Disable firewall. This check box disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.

When no login is required, this field displays:

Modem MAC Address. The Ethernet MAC address used by the broadband ADSL2+ modem on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your broadband ADSL2+ modem to use your computer's MAC address (this is also called cloning).

1. Disabling NAT reboots the broadband ADSL2+ modem and resets its configuration settings to the factory defaults. Disable NAT only if you plan to set up the broadband ADSL2+ modem in a setting where you will be manually administering the IP address space on the LAN side of the modem.

Use Default Address. Use the default MAC address.

Use Computer MAC Address. The broadband ADSL2+ modem will capture and use the MAC address of the computer that you are now using. You have to use the one computer that is allowed by the ISP.

Use This MAC Address. Enter the MAC address that you want to use.

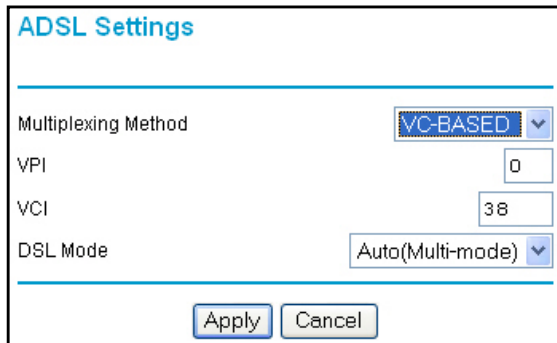
ADSL Settings

The DSL settings of your modem work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

Note: You are required to use the Setup Wizard to select the correct country for the default DSL settings to work.

➤ **If your ISP gave you a multiplexing method or VPI/VCI number, enter the setting:**

1. Select **Setup > ADSL Settings** to display the following screen:



The screenshot shows a dialog box titled "ADSL Settings". It contains the following fields and controls:

- Multiplexing Method:** A dropdown menu with "VC-BASED" selected.
- VPI:** A text input field containing the number "0".
- VCI:** A text input field containing the number "38".
- DSL Mode:** A dropdown menu with "Auto(Multi-mode)" selected.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

2. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 0.
4. For the VCI, type a number between 32 and 65535. The default is 35.
5. Click **Apply**.

Unsuccessful Internet Connection

If you cannot connect to the Internet, you can do one or more of the following:

- Review your settings to be sure you have selected the correct options and typed everything correctly.
- Contact your ISP to verify that you have the correct configuration information.
- Read [Chapter 6, Troubleshooting](#). If problems persist, register your NETGEAR product and contact NETGEAR technical support.
- Check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation for more information.

Change Password and Login Time-Out

For security reasons, the broadband ADSL2+ modem has its own user name and password that default to **admin** and **password**. You can and should change these to a secure user name and password that are easy to remember. The ideal password contains no dictionary words from any language and is a mixture of uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

Note: The modem user name and password are not the same as the user name and password for logging in to your Internet connection. See [Types of Logins](#) on page 26 for more information about login types.

➤ To change your password and login time-out:

1. Select **Maintenance > Set Password** to display the following screen.:

2. Enter the old password, and then enter the new password twice.
3. Change the login time-out to a value between 1 and 99 minutes if the default value of 5 minutes does not meet your needs.

The administrator's login to the modem configuration times out after a period of inactivity to prevent someone else from accessing the modem interface when you step away.

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

After changing the password, you are required to log in again to continue the configuration. If you have backed up the modem settings previously, you should do a new backup so that the saved settings file includes the new password. See [Back Up](#) on page 47 for information about backing up your network configuration.

Log Out Manually

The modem interface provides a Logout command at the bottom of the modem menus. Log out when you expect to be away from your computer for a relatively long period of time.

- **To log out manually:**

Click **Log Out** at the bottom of the modem menus.

Types of Logins

There are two separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Modem login** logs you in to the modem interface. See [Log In to the Modem](#) on page 17 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

3 Security Settings

3

Keeping unwanted content out of your network

This chapter explains how to use the basic firewall features of the modem to prevent objectionable content from reaching the PCs and other devices connected to your network.

This chapter contains the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Firewall Rules to Control Network Access*
- *Configure Services*
- *Set the Time Zone*
- *Schedule Firewall Services*
- *Enable Security Event Email Notification*

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➤ **To block by keywords:**

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

2. Select one of the keyword blocking options:
 - **Per Schedule.** Turn on keyword blocking according to the Schedule screen settings.
 - **Always.** Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain, click **Add Keyword**, and click **Apply**.

The Keyword list. supports up to 32 entries. Here are some sample entries:

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

Delete a Keyword or Domain

➤ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword**, and click **Apply** to save your changes.

Specify a Trusted Computer

You can exempt one trusted computer from blocking and logging. That computer has to be configured to use a fixed IP address.

- **To specify a trusted computer:**
 1. In the Trusted IP Address field, enter the IP address.
 2. Click **Apply** to save your changes.

Firewall Rules to Control Network Access

By default your router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. You might need to create exceptions to this rule to allow remote computers to access a server on your local network or to allow certain applications and games to work correctly. Your router provides firewall rules for creating these exceptions.

Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

- **Inbound.** Block all access from outside except responses to requests from the LAN side.
- **Outbound.** Allow all access from the LAN side to the outside.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type **http://www.example.com** into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

Source address. Your computer's IP address.

Source port number. 5678, which is the browser session.

Destination address. The IP address of **www.example.com**, which your computer finds by asking a DNS server.

Destination port number. 80, which is the standard port number for a web server process.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at `www.example.com`. Before sending the web page request message to `www.example.com`, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
 - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
 - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the web server at `www.example.com`.

4. The web server at `www.example.com` composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

Source address. The IP address of `www.example.com`.

Source port number. 80, which is the standard port number for a web server process.

Destination address. The public IP address of your router.

Destination port number. 33333.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from `www.example.com`. The message now contains the following address and port information:

Source address. The IP address of `www.example.com`.

Source port number. 80, which is the standard port number for a web server process.

Destination address. Your computer's IP address.

Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Open Inbound Ports (Port Forwarding)

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router does not recognize it and discards it. However, some application servers

(such as FTP and IRC servers) send replies back to multiple port numbers. By using the inbound rule function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an identify message to your computer on port 113. With inbound rules, you can tell the router, "When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the inbound rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your inbound rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an identify message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure inbound rules, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or the relevant user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Inbound Rules to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the inbound rules feature.

A typical application of inbound rules can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. By using inbound rules, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the inbound rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from `www.example.com`, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

Destination address. The IP address of `www.example.com`, which is the address of your router.

Destination port number. 80, which is the standard port number for a web server process.

The remote computer sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your inbound rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

The destination address is replaced with 192.168.1.123.

Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from `www.example.com`.

To configure inbound rules, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups or newsgroups.

How Inbound Rules Differ from Outbound Rules

The following points summarize the differences between inbound rules and outbound rules:

- Outbound rules can be used by any computer on your network, although only one computer can use them at a time.
- Inbound rules are configured for a single computer on your network.
- Outbound rules do not require that you know the computer's IP address in advance. The IP address is captured automatically.
- Inbound rules require that you specify the computer's IP address during configuration, and the IP address can never change.
- Outbound rules require specific outbound traffic to open the inbound ports, and the outbound ports are closed after a period of no activity.
- Inbound rules are always active and do not need to be made active.

Configure Firewall Rules

The Firewall Rules screen lets you configure custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence. See [Configure Services](#) on page 38 for information about services.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the Rules table from the top (highest precedence) to the default rules at the bottom. In some cases, the order of precedence is important to determine which communications are allowed into or out of the network.

➤ To configure firewall rules:

1. Select **Security > Firewall Rules** to display the following screen:

Firewall Rules

Outbound Services

#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
1	<input checked="" type="checkbox"/>	FINGER	BLOCK always	Any	Any	Never
Default	Yes	Any	ALLOW always	Any	Any	Never

Add Edit Move Delete

Inbound Services

#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
Default	Yes	Any	BLOCK Always	Any	Any	Never

Add Edit Move Delete

Instant Messaging (IM) Ports

Close IM Ports

Open IM Ports (IM ports are open by default)

Apply Cancel

2. To add an inbound or outbound rule:
 - For an outbound rule, click **Add** under Outbound Services.

- For an inbound rule, click **Add** under Inbound Services.
- 3. To edit or delete a rule, select its button on the left side, and click **Edit** or **Delete**.
- 4. To change the order of precedence:
 - a. Select its button on the left side of the table, and click **Move**.
 - b. At the prompt, enter the number of the new position, and click **OK**.
- 5. To open or close instant messaging, select a radio button, and click **Apply**.
 - **Close IM Ports**. Disables instant messaging traffic.
 - **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.
- 6. Click **Apply** to save your settings.

Inbound Rules (Port Forwarding)

Because the modem uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet.

The rule tells the modem to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding. Allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. The following are two examples of inbound rules.

Note: Some residential broadband ISP accounts do not let you run server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Inbound Rule Example: A Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of day, as shown here and described following the figure:

The screenshot shows the 'Inbound Services' configuration window. It has a title bar 'Inbound Services'. Below the title bar, there are several fields and dropdown menus. The 'Service' dropdown is set to 'HTTP(TCP:80)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field contains the IP address '192.168.0.99'. The 'WAN Users' dropdown is set to 'Any'. Below the 'WAN Users' dropdown, there are 'start:' and 'finish:' fields, each with four input boxes for IP address components. The 'Log' dropdown is set to 'Always'. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

Figure 7. Allow inbound web requests

Service. From this list, select the application or service you want to allow or block. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear. See [Configure Services](#) on page 38.

Action. Choose how you want to handle this type of traffic. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen, described in [Schedule Firewall Services](#) on page 40.

Send to LAN Server. Enter the IP address of the computer or server on your LAN that receives the inbound traffic covered by this rule.

WAN Users. These settings determine which packets are covered by the rule, based on their source (WAN) IP address:

Any. All IP addresses are covered by this rule.

Address range. When this option is selected, the Start and Finish fields are required.

Single address. Enter the required address in the Start field.

Log. You can select whether to log the traffic:

Never. No log entries are made for this service.

Always. Any traffic for this service type is logged.

Match. Traffic of this type that matches the settings and action is logged.

Not match. Traffic of this type that does not match the settings and action is logged.

Inbound Rule Example: Allowing Video Conferencing

Create an inbound rule to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In the following figure, CU-SeeMe connections are allowed from a specified range of external IP addresses only. In this case, logging of any incoming CU-SeeMe requests that do not match the allowed settings is always allowed.

The screenshot shows the 'Inbound Services' configuration window. It includes the following fields and values:

- Service:** CU-SEEME(TCP/UDP:7648,24032)
- Action:** ALLOW always
- Send to LAN Server:** 192 . 168 . 0 . 11
- WAN Users:** Address Range
 - start: 134 . 177 . 88 . 1
 - finish: 134 . 177 . 00 . 254
- Log:** Not Match

Buttons for 'Apply' and 'Cancel' are located at the bottom of the window.

Figure 8. Allow inbound video conferencing

Considerations for Inbound Rules

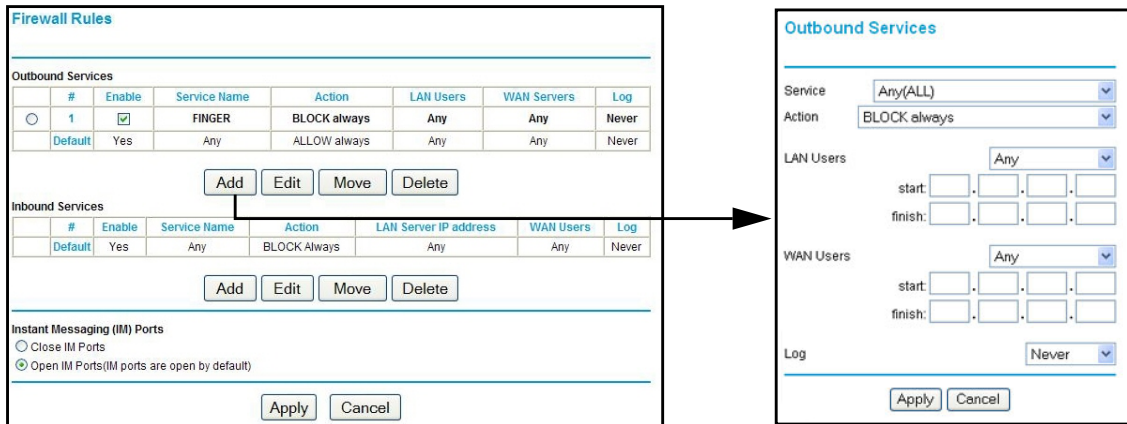
- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen described in *Dynamic DNS* on page 56 so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN Setup screen to keep the computer's IP address constant.
- Local computers are required to access the local server using the computer's local LAN address (192.168.0.11 in the example shown in *Figure 8, Allow inbound video conferencing*). Attempts by local computers to access the server using the external WAN IP address fail.

Outbound Rules (Service Blocking)

The modem lets you block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on local computer, Internet site being contacted, time of day, and type of service being requested.

➤ **To set up service blocking:**

1. Select **Security > Firewall Rules** to display the following screen:



2. Under Outbound Services, click **Add**.
3. Fill in the settings as follows, and click **Apply** to save your settings.

Service. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the **Add Custom Service** button in the Services screen described in [Configure Services](#) on page 38 to add any additional services or applications that do not already appear.

Action. Choose how to handle this type of traffic. You can block or allow always, or you can block or allow according to the schedule you defined, as described in [Schedule Firewall Services](#) on page 40.

LAN Users. These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the option that you want:

Any. All IP addresses are covered by this rule.

Address range. If this option is selected, fill in the Start and Finish fields.

Single address. Enter the required address in the Start field.

WAN Users. These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:

Any. All IP addresses are covered by this rule.

Address range. If this option is selected, fill in the Start and Finish fields.

Single address. Enter the required address in the Start field.

Log. You can select to log the traffic:

Never. No log entries are made for this service.

Always. Any traffic for this service type is logged.

Match. Traffic of this type that matches the settings and action is logged.

Not match. Traffic that does not match the settings and action is logged.

Configure Services

Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at <http://www.ietf.org>) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the broadband ADSL2+ modem already holds a list of many service port numbers, you are not limited to these choices.

➤ **To create your own service definitions:**

1. Select **Security > Services** to display the following screen:

The screenshot shows a web interface titled "Services". Below the title is a "Service Table" with three columns: "#", "Service Name", and "Ports". Underneath the table are three buttons: "Add Custom Service", "Edit Service", and "Delete Service".

- To create a new service, click the **Add Custom Service** button to display the Add Services screen.
- To edit a service, select its button on the left side of the table, and click **Edit Service**.
- To delete a service, select its button on the left side of the table, and click **Delete Service**.

2. Use the following screen to define or edit a service.

The screenshot shows a web interface titled "Add Services". Below the title is a "Service Definition" section with four fields: "Name:" (text input), "Type:" (dropdown menu with "TCP" selected), "Start Port:" (text input), and "Finish Port:" (text input). At the bottom are two buttons: "Apply" and "Cancel".

- **Name.** Enter a meaningful name for the service.

- **Type.** Select the correct type for this service. If in doubt, select **TCP/UDP**. The options are TCP, UDP, TCP/UDP.
 - **Start Port** and **End Port.** If a port range is required, enter the range here. If a single port is required, enter the same value in both fields.
3. Click **Apply** to save your changes.

Set the Time Zone

The modem uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. You can check and set (if needed) the time zone to ensure that time stamps match your local time.

➤ To set the time zone:

1. Select **Security > Schedule** to display the following screen:

The screenshot shows the 'Schedule' configuration page. It includes a 'Days' section with checkboxes for 'Every Day', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are checked. Below this is the 'Time of day' section, which has a checked 'All Day' option and fields for 'Start Time' and 'End Time', each with 'Hour' and 'Minute' sub-fields. The 'Time Zone' section features a dropdown menu currently set to '(GMT) Greenwich Mean Time : Edinburgh, London', and two unchecked checkboxes: 'Adjust for Daylight Savings Time' and 'Use this NTP Server'. At the bottom, the 'Current Time' is displayed as '2000-01-01 00:25:26'. 'Apply' and 'Cancel' buttons are located at the bottom right of the form.

2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.
3. If your time zone is in daylight savings time, select the **Adjust for Daylight Savings Time** check box to add one hour to standard time.

Note: If your region uses daylight savings time, select Adjust for Daylight Savings Time on the first day and clear it after the last day.

4. The modem has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.
5. Click **Apply** to save your settings.

Schedule Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

➤ To schedule firewall services:

1. Select **Security > Schedule** to display the following screen:

2. To block Internet services based on a schedule, select **Every Day**, or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the Start Time and End Time fields.

Note: Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.

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

Enable Security Event Email Notification

To receive logs and alerts by email, provide your email information in the Email screen and specify which alerts you want to receive and how often.

➤ **To enable email notification:**

1. Select **Security > Email** to display the following screen:

The screenshot shows the 'E-mail' configuration screen. At the top, there is a title 'E-mail' and a horizontal line. Below this is a checkbox labeled 'Turn E-mail Notification On'. Underneath is a section titled 'Send Alerts and Logs Via E-mail' containing three input fields: 'Send To This E-mail Address', 'Outgoing Mail Server', and 'My Mail Server requires authentication'. The 'My Mail Server requires authentication' checkbox is unchecked, and below it are two more input fields for 'User Name' and 'Password'. The next section is 'Send E-Mail alerts immediately', which has three checked checkboxes: 'If a DoS attack is detected.', 'If a Port Scan is detected.', and 'If someone attempts to access a blocked site.'. The final section is 'Send Logs According to this Schedule', which includes a dropdown menu set to 'Hourly', a 'Day' dropdown, and a 'Time' dropdown with radio buttons for 'a.m.' and 'p.m.'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

2. Fill in the fields as follows:

Turn E-mail Notification On. Select this check box if you want to receive email logs and alerts from the modem.

Send To This E-mail Address. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.

Outgoing Mail Server. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.

My Mail Server requires authentication. If you use an outgoing mail server provided by your current ISP, you do not need to select this field. If you use an email account that is not provided by your ISP, select this field, and enter the required user name and password information.

Send E-Mail alerts immediately. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.

Send Logs According to this Schedule. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

Day for sending logs specifies which day of the week to send the log. This is relevant when the log is sent weekly.

Time for sending log specifies the time of day to send the log. This is relevant when the log is sent daily or weekly.

Note: If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the modem's memory. If the modem cannot email the log file, the log buffer might fill up. In this case, the modem overwrites the log and discards its contents.

4 Network Maintenance

4

Administering your network

This chapter describes the modem settings for administering and maintaining the modem and home network.

This chapter contains the following sections:

- *Upgrade the Modem Firmware*
- *Manually Check for Firmware Upgrades*
- *Manage the Configuration File*
- *View Modem Status*
- *View Attached Devices*
- *Run Diagnostic Utilities*

Upgrade the Modem Firmware

The modem firmware (routing software) is stored in flash memory. By default, when you log in to your modem, it checks the NETGEAR website for new firmware and alerts you if there is a newer version.



WARNING!

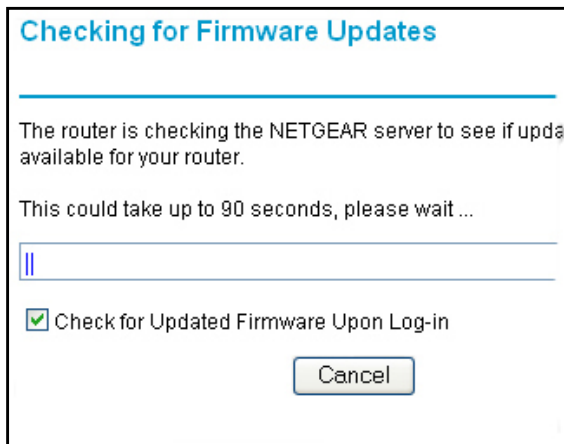
When uploading firmware to the broadband ADSL2+ modem, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

Turn Off Automatic Firmware Checking

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See [Manually Check for Firmware Upgrades](#) on page 46.

➤ **To turn off the automatic firmware check at log in:**

1. Select **Maintenance > Router Upgrade**.
2. Clear the **Check for Updated Firmware Upon Login** check box at the bottom of this screen:



Automatic Firmware Checking On

When automatic firmware checking is on, the modem performs the check and notifies you if an upgrade is available or not as shown here.

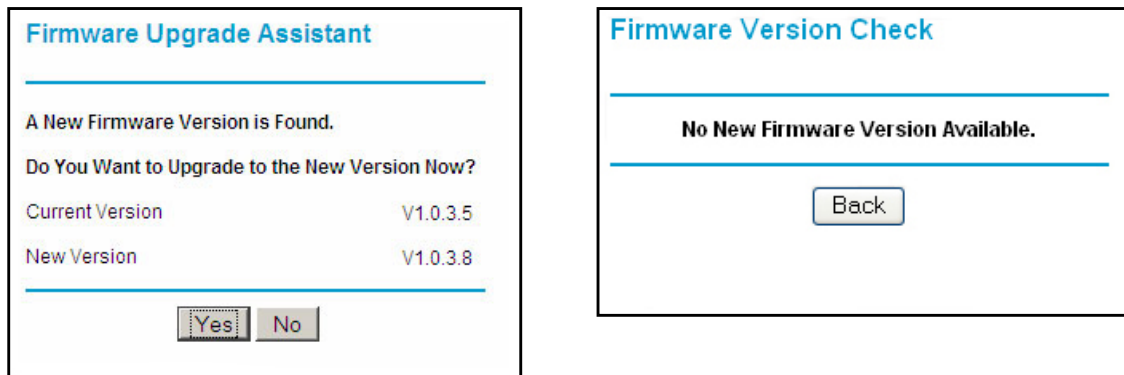


Figure 9. Firmware upgrade assistant and results screen

➤ **To upgrade the firmware:**

1. Click **Yes** to allow the modem to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your modem restarts.
2. Go to the DM111PSPv2 support page at <http://www.netgear.com/support>, and read the new firmware release notes to determine whether you need to reconfigure the modem after upgrading.

Note: If you get a “Firmware needs to be reloaded” message, it means a problem has been detected with the modem’s firmware. Follow the prompts to correct the problem, or see *Firmware Needs to Be Reloaded* on page 72 for a description of the steps.

Manually Check for Firmware Upgrades

You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.



WARNING!

When you upload firmware to the modem, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

➤ To check for firmware upgrades:

1. Select **Maintenance > Router Status**, and make a note of the modem firmware version number..

2. Go to the DM111PSPv2 support page on the NETGEAR website at <http://www.netgear.com/support>.
3. If the firmware version on the NETGEAR website is newer than the firmware on your modem, download the file to your computer.
4. To upload the newer firmware, select **Maintenance > Router Upgrade** to display the following screen:

5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img).
6. Click **Upload** to send the firmware to the modem.

When the upload is complete, your modem restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the modem after upgrading.

Manage the Configuration File

The modem configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or reverted to factory default settings.

Back Up

➤ **To back up the configuration file:**

1. Select **Maintenance > Backup Settings** to display the following screen:

The screenshot shows a web interface titled "Backup Settings". It is divided into three horizontal sections by blue lines. The first section is "Save a Copy of Current Settings" and contains a "Backup" button. The second section is "Restore Saved Settings from a File" and contains a text input field, a "Browse..." button, and a "Restore" button. The third section is "Revert to Factory Default Settings" and contains an "Erase" button.

2. Click **Backup** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore

➤ **To restore the configuration file from backup:**

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the modem.

Upon completion, the modem reboots.



WARNING!

Do not interrupt the reboot process.

Erase

➤ To erase the configuration and restore to factory defaults:

Under some circumstances (for example, if you move the modem to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings.

Click the **Erase** button to reset the modem to its factory default settings.

Erase sets the user name to admin, the password to password, the LAN IP address to 192.168.1.1, and enables the modem's DHCP.

To restore the factory default configuration settings when you do not know the login password or IP address, use the Restore Factory Settings button on the rear panel of the modem (see *Factory Settings* on page 75).

View Modem Status

➤ To view the modem status:

Select **Maintenance > Router Status** to display the following screen. The Router Status screen provides the status and usage information described in the following figure.

Router Status	
<hr/>	
Account Name	
Firmware Version	V1.1.00.01_NA
<hr/>	
ADSL Port	
MAC Address	00:26:F2:44:48:A3
IP Address	---
Network Type	PPPoE
IP Subnet Mask	---
Gateway IP Address	---
Domain Name Server	---
<hr/>	
LAN Port	
MAC Address	00:26:F2:44:48:A2
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
<hr/>	
Modem	
ADSL Firmware Version	3.4.4.0.0.1
Modem Status	Link down
DownStream Connection Speed	0 Kbps
UpStream Connection Speed	0 Kbps
VPI	8
VCI	35
<hr/>	
<input type="button" value="Show Statistics"/> <input type="button" value="Connection Status"/>	

The following fields are displayed:

Account Name. The host name assigned in the Basic Settings screen.

Firmware Version. The firmware version.

ADSL Port.

MAC Address. The Ethernet MAC address of the DSL port.

IP Address. The DSL port IP address. If no address is shown, the broadband ADSL2+ modem cannot connect to the Internet.

Network Type. The value depends on your ISP.

IP Subnet Mask. The DSL port IP subnet mask.

Gateway IP Address. The IP address used as a gateway to the Internet for computers configured to use DHCP.

Domain Name Server. The modem DNS server IP addresses. These addresses are usually obtained dynamically from the ISP.

LAN Port (Local Port).

MAC Address. The modem LAN port Ethernet MAC address.

IP Address. The modem LAN port IP address. The default is 192.168.0.1.

DHCP. If Off, the modem does not assign IP addresses to PCs on the LAN. If On, the modem does assign IP addresses to PCs on the LAN.

IP Subnet Mask. The IP subnet mask used by the modem LAN. The default is 255.255.255.0.

Modem.

ADSL Firmware Version. The version of the firmware.

Modem Status. The connection status of the modem.

DownStream Connection Speed. The modem receives data from the DSL line at this speed.

UpStream Connection Speed. The modem transmits data to the DSL line at this speed.

VPI. The Virtual Path Identifier setting.

VCI. The Virtual Channel Identifier setting.

➤ **To view statistics:**

From the Router Status screen, click the **Show Statistics** button to display a screen similar to this:

System Up Time 03:52:30							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoA	1131	55	0	4	1	03:52:02
LAN	10M/100M	864	1869	0	29	13	03:52:25
WLAN	11M/54M/270M	411	0	0	7	0	03:52:21

ADSL Link	Downstream	Upstream
Connection Speed	8128 kbps	832 kbps
Line Attenuation	0.0 db	1.0 db
Noise Margin	19.7 db	6.0 db

Poll Interval: (secs)

The following fields are displayed:

Port. The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:

Status. The link status of the port.

TxPkts. The number of packets transmitted since reset or manual clear.

RxPkts. The number of packets received since reset or manual clear.

Collisions. The number of collisions since reset or manual clear.

Tx B/s. The current line utilization—percentage of current bandwidth used.

Rx B/s. The average line utilization.

Up Time. The time elapsed since the last power cycle or reset.

ADSL Link Downstream or Upstream. The statistics for the upstream and downstream DSL link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.

Connection Speed. Typically, the downstream speed is faster than the upstream speed.

Line Attenuation. The line attenuation increases the farther you are physically located from your ISP's facilities.

Noise Margin. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.

Poll Interval. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

➤ **To view the connection status:**

In the Router Status screen, click the **Connection Status** button to display a screen similar to this:

The screenshot shows a window titled "Connection Status" with a table of connection details and three buttons: "Connect", "Disconnect", and "Close Window".

Connection Status	
Connection Time	05:15:17
Connecting to Server	Connected
Negotiation	Success
Authentication	Success
Getting IP Addresses	69.110.231.81
Getting Network Mask	255.255.255.255

Buttons: Connect, Disconnect, Close Window

The following fields are displayed:

Connection Time. The time elapsed since the last connection to the Internet through the DSL port.

Connecting to sender. The connection status.

Negotiation. Success or Failed.

Authentication. Success or Failed.

Obtaining IP Address. The IP address assigned to the WAN port by the ISP.

Obtaining Network Mask. The network mask assigned to the WAN port by the ISP.

View Attached Devices

The Attached Devices screen presents a table of all IP devices that the modem has discovered on the local network.

➤ **To view attached devices:**

1. Select **Maintenance > Attached Devices** to view the following table:

The screenshot shows a window titled "Attached Devices" with a table of discovered IP devices and a "Refresh" button.

#	IP Address	Device Name	MAC Address
1	192.168.0.2	9300UNIT2	00:11:43:71:D1:92

Button: Refresh

2. Click **Refresh** to update the screen.

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the modem is rebooted, the table data is lost until the broadband ADSL2+ modem rediscovers the devices. To force the broadband ADSL2+ modem to look for attached devices, click the **Refresh** button.

Run Diagnostic Utilities

The modem has a diagnostics feature that you can use to perform the following functions:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other broadband ADSL2+ modems the modem is communicating with.
- Reboot the modem to enable new network configurations to take effect or to clear problems with the modem's network connection.

➤ To run diagnostic utilities:

1. Select **Maintenance > Diagnostics** to display the following screen.

The screenshot shows a web interface titled "Diagnostics". It contains four main sections, each with a button to execute a function:

- Ping an IP address:** A form with four input boxes for IP address digits and a "Ping" button.
- Perform a DNS Lookup:** A form with an "Internet Name:" input box and a "Lookup" button. Below the button, it displays "IP address:" and "DNS Server: 206.13.28.12" and "206.13.29.12".
- Display the Routing Table:** A "Display" button.
- Reboot the Router:** A "Reboot" button.

2. Get diagnostic information as follows:
 - a. To ping an IP address, fill in the IP address, and click **Ping**.
 - b. To perform a DNS lookup, fill in the Internet Name and click **Lookup**.
 - c. To display the routing table, click **Display**.
 - d. To reboot the router, click **Reboot**.

Advanced Settings

5

Configuring for unique situations

This chapter describes the advanced features of your modem. The information is for users with a solid understanding of networking concepts who want to set the modem up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter contains the following sections:

- *WAN Setup*
- *Dynamic DNS*
- *LAN Setup*
- *Remote Management*
- *Static Routes*
- *Universal Plug and Play*
- *Change the Device Mode*

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the wireless modem to respond to a ping on the WAN (Internet) port.

➤ **To set up the WAN:**

1. Select **Advanced > WAN Setup** to display the following screen:

The screenshot shows the WAN Setup configuration interface. It includes the following elements:

- WAN Setup** (Section Header)
- Connect Automatically, as Required**
- Enable PPPoE Relay**
- Disable Port Scan and DOS Protection**
- Default DMZ Server** (IP address: 192.168.0.0)
- Respond to Ping on Internet WAN Port**
- MTU Size (in bytes)** (Value: 1492)
- Disable SIP ALG**
- Apply** and **Cancel** buttons

2. Fill in the fields as follows:

Connect Automatically, as Required. This option is enabled by default so that Internet connections are made automatically whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting and connect manually from the Router Status screen. See [View Modem Status](#) on page 48.

Enable PPPoE Relay. When enabled, this feature allows a PPPoE client on a local PC to connect to a remote PPPoE server with the gateway acting as a relay agent.

Disable Port Scan and DOS Protection. The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.

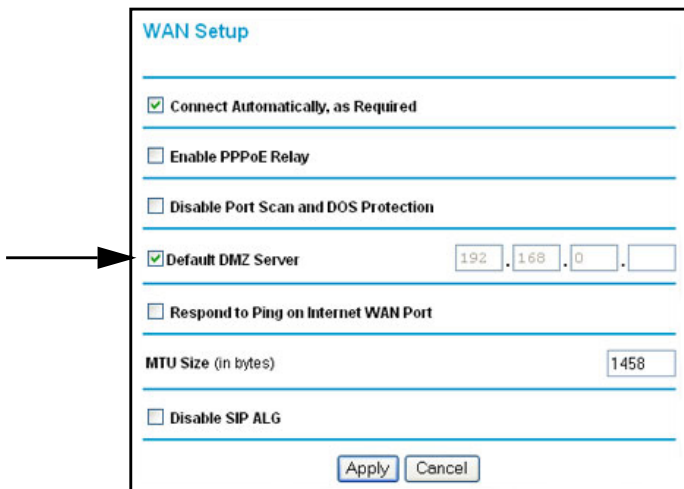
Default DMZ Server. The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. The modem is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

Note: For security reasons, 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 usually discarded by the modem unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➤ **To assign a computer or server to be a default DMZ server:**

1. In the WAN Setup screen, select the **Default DMZ Server** check box.



2. Type the IP address for that server.
3. Fill in the following fields, and click **Apply**:

Respond to Ping on Internet WAN Port. If you want the broadband ADSL2+ modem to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, because it allows your modem to be discovered. Do not select this check box unless you have a specific reason to do so.

MTU Size (in bytes). The normal Maximum Transmit Unit (MTU) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Disabling SIP ALG. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when you are running certain applications.

Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address is, and the address can change frequently. In this case, use a commercial Dynamic DNS service that lets you register your domain to its IP address and forwards traffic directed at your domain to your frequently changing IP address.

The modem has a client that can connect to a Dynamic DNS service provider. Once you have configured your ISP account information in the modem, whenever your ISP-assigned IP address changes, your modem contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

➤ To set up Dynamic DNS:

1. Select **Advanced > Dynamic DNS** to display the following screen.

2. Access the website of one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Type the host name that your Dynamic DNS service provider gave you. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then your host name is myName.
6. Type the user name for your Dynamic DNS account.
7. Type the password (or key) for your Dynamic DNS account.
8. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
9. Click **Apply** to save your settings.

Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses are not routed on the Internet.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and Routing Information Protocol (RIP). The modem is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem's default LAN IP configuration is as follows:

- **LAN IP address.** 192.168.0.1
- **Subnet mask.** 255.255.255.0

These addresses are part of the private address range designated by the Internet Engineering Task Force (IETF <http://www.ietf.org>) 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 Setup screen.

Note: If you change the LAN IP address of the modem while connected through the browser, you are disconnected. To reconnect, open a new connection to the new IP address and log in.

➤ To change the LAN setup:

1. Select **Advanced > LAN Setup**.

LAN Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: RIP-1

Access Router Management Interface on additional port: 8080
(NAT-disabled mode only)

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

2. Enter the LAN Setup configuration, and click **Apply** to save your changes.

IP Address. The LAN IP address of the broadband ADSL2+ modem.

IP Subnet Mask. The LAN subnet mask of the modem. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or broadband ADSL2+ modem.

RIP Direction. RIP allows a modem to exchange routing information with other modems. The RIP Direction selection controls how the broadband ADSL2+ modem sends and receives RIP packets. The default setting is Both.

- When set to **Both** or **Out Only**, the modem broadcasts its routing table periodically.
- When set to **Both** or **In Only**, the modem incorporates the RIP information that it receives.
- When set to **None**, the modem does not send any RIP packets and ignores any RIP packets received.

RIP Version. This controls the format and the broadcasting method of the RIP packets that the modem sends. It recognizes both formats when receiving. By default, this is set for RIP-1.

- **RIP-1.** This version is universally supported. It is probably adequate for most networks, unless you have an unusual network setup.
- **RIP-2.** This version carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
- **RIP-2B.** This version uses subnet broadcasting.
- **RIP-2M.** This version uses multicasting.

Access Modem Interface on Additional Port

When NAT is disabled, the modem's management interface can be accessed at the modem's LAN address using the port number you enter. This feature is not available when NAT is enabled.

Use Modem as DHCP Server

By default, the modem functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem's LAN. The assigned default gateway address is the LAN address of the modem. IP addresses are assigned to the attached PCs from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the modem are satisfactory.

Reserved IP Address Setup

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

➤ **To reserve an IP address:**

1. Select **Advanced > LAN Setup**, and click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the modem's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.

Tip: If the computer is already present on your network, copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address is not assigned until the next time the computer contacts the modem's DHCP server. Reboot the computer or access its IP configuration to force a DHCP release and renew.

➤ **To edit or delete a reserved address entry:**

1. Select the button next to the reserved address that you want to edit or delete.
2. Click **Edit** or **Delete**.

Remote Management

The Remote Management screen lets you allow a user or users on the Internet to configure, upgrade, and check the status of your modem.

➤ **To configure remote management:**

1. Select **Advanced > Remote Management** to display this screen:

2. Select the **Turn Remote Management On** check box.
3. Specify the external addresses that can access remote management. For security, restrict access to as few external IP addresses as practical:
 - To allow access from a single IP address on the Internet, select **Only This Computer**, and enter the IP address that is allowed access.
 - To allow access from a range of IP addresses on the Internet, select **IP Address**, and enter a beginning and ending IP address to define the allowed range.
 - To allow access from any IP address on the Internet, select **Everyone**.
4. Specify the port number to be used for accessing the modem interface.

Web browser access usually uses the standard HTTP service port 80. For greater security, you can change it so the remote modem interface uses a custom port by entering that number in the field 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. Click **Apply** to save your changes.

To access your modem from the Internet, type your modem's WAN IP address in your browser's Address field, followed by a colon (:) and the custom port number.

For example, if your external address is 134.177.0.123 at port number 8080, enter the following in your browser:

http://134.177.0.123:8080

Note: The http:// is required in the address.

Static Routes

Static routes provide additional routing information to your modem. Under normal circumstances, the modem has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. Configure static routes only for unusual cases, such when you have multiple routers or multiple IP subnets on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN modem on your home network for connecting to the company where you are employed. This modem's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your modem, two implicit static routes were created. A default route was created with your ISP as the broadband ADSL2+ modem, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your modem that 134.177.0.0 should be accessed through the ISDN modem at 192.168.0.100.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses are to be forwarded to the ISDN modem at 192.168.0.100.
- The value in the **Metric** field represents the number of modems between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Configure Static Routes

➤ To configure static routes:

1. Select **Advanced > Static Routes** to display the following screen.

The screenshot shows a window titled "Static Routes". Below the title is a table with the following columns: #, Active, Name, Destination, and Gateway. Below the table are three buttons: Add, Edit, and Delete.

Figure 10. View additional routing information

2. To add a static route:
 - a. Click **Add** to open the following screen.

The screenshot shows a window titled "Static Routes" with the following fields and options:

- Route Name: [Text Input Field]
- Private
- Active
- Destination IP Address: [Four separate input boxes for IP octets]
- IP Subnet Mask: [Four separate input boxes for subnet mask octets]
- Gateway IP Address: [Four separate input boxes for gateway IP octets]
- Metric: [Text Input Field]

 At the bottom are "Apply" and "Cancel" buttons.

- b. In the Route Name field, enter a route name for this static route. This name is for identification purpose only.
- c. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
- d. Select **Active** to make this route effective.
- e. Enter the destination IP address of the final destination.
- f. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.
- g. Enter the gateway IP address, which has to be a modem on the same LAN segment as the modem.
- h. In the Metric field, enter a number between 2 and 15 as the metric value. This represents the number of modems between your network and the destination. Usually, a setting of 2 or 3 works.

- Click **Apply** to save your changes. The Static Routes table updates to show the new entry.

#	Active	Name	Destination	Gateway
1	Yes	ex_rt	134.177.0.0	192.168.0.100

Universal Plug and Play

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

➤ To configure UPnP:

- Select **Advanced > UPnP** to display the following screen:

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

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

- Fill in the settings as follows:

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

Advertisement Period. The advertisement period is how often the modem advertises (broadcasts) its UPnP information. This value ranges from 1 to 1440 minutes. The default is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the device status freshness but can significantly reduce network traffic.

Advertisement Time To Live. This is measured in hops (steps) for each UPnP packet sent. Hops are 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 is 4 hops, which works for most home networks. If you notice that some devices are not being updated or reached correctly, you might 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 modem 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.

3. To save your settings, cancel your changes, or refresh the table:
 - Click **Apply** to save the new settings to the modem.
 - Click **Cancel** to disregard any unsaved changes.
 - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

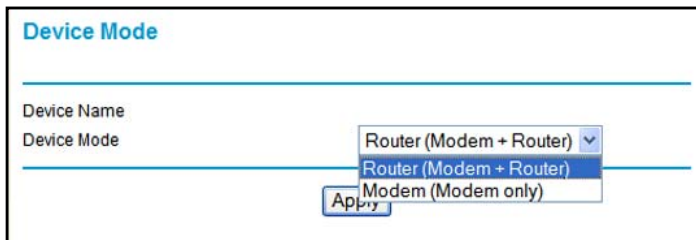
Change the Device Mode

The modem includes a built-in router. If you want to configure the modem as a “pure bridge” in Modem mode, first set up the Internet connection and then change the Device Mode setting to Modem mode.

In Modem mode, the device acts as a “pure bridge” or DSL modem. When the device is in Modem mode, features that are not available are grayed out.

➤ To change the device mode:

1. Select **Advanced > Device Mode**. The following screen displays:



The screenshot shows a web interface titled "Device Mode". It contains two input fields: "Device Name" and "Device Mode". The "Device Mode" field is a dropdown menu with three options: "Router (Modem + Router)", "Router (Modem + Router)", and "Modem (Modem only)". The "Modem (Modem only)" option is currently selected. Below the "Device Mode" field is an "Apply" button.

By default, the modem is in Router mode.

2. Select the device mode that you want from the drop-down list.
3. Click **Apply** so that your changes take effect.

6 Troubleshooting

6

Diagnosing and solving problems

This chapter provides information to help you diagnose and solve problems you might have with your modem. If you do not find the solution here, check the NETGEAR support site at <http://support.netgear.com> for product and contact information.

This chapter contains the following sections:

- *Modem Is Off*
- *No Internet Connection*
- *TCP/IP Network Not Responding*
- *Cannot Log in*
- *Changes Not Saved*
- *Firmware Needs to Be Reloaded*
- *Incorrect Date or Time*

Modem Is Off

When you turn the power on, the Power, LAN, and DSL LEDs should light as described here. If they do not, refer to the sections that follow for help.

➤ To check the LEDs:

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, the Ethernet and DSL LEDs light as follows:
 - a. The Ethernet port LED lights when the modem is connected.
 - b. The DSL link LED lights to indicate that there is a link to the connected device.
 - c. If the Ethernet port is connected to a 100 Mbps device, verify that the Ethernet port's LED is green. Note that if the Ethernet device is 10 Mbps, the LED is amber.

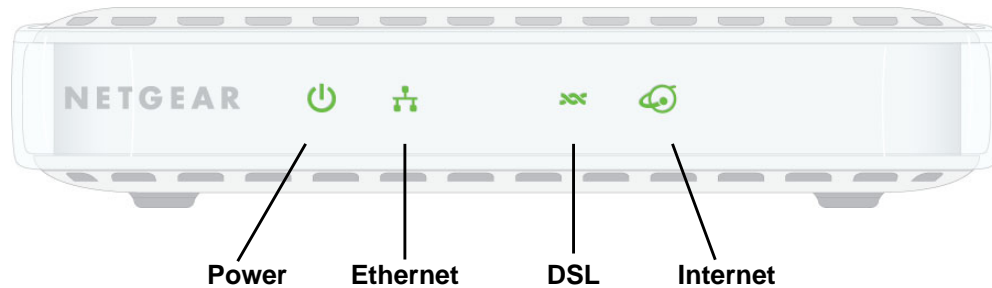


Figure 11. Front panel LED icons

Power LED Is Off

If the Power and other LEDs are off when your modem is turned on:

- Check that the power cord is correctly connected to your modem and the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the 12V DC power adapter supplied by NETGEAR for this product.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

Power LED Is Red

When the modem is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the modem.

If the Power LED turns red to indicate a modem fault, turn the power off and on to see if the broadband ADSL2+ modem recovers. If the power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the broadband ADSL2+ modem recovers.
- Clear the modem's configuration to factory defaults as explained in [Factory Settings](#) on page 75. This sets the modem's IP address to 192.168.0.1.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

Ethernet LED Is Off

If the Ethernet LED does not light when the Ethernet connection is made, check the following:

- The Ethernet cable connections are secure at the modem and at the hub or workstation.
- The power is turned on to the connected hub or workstation.
- You are using the correct cable. When connecting the DSL port, use the cable that was supplied with the modem. If the DSL link LED is still off, this could mean that there is no DSL service or the cable connected to the DSL port is bad.

See also [DSL Link LED Is Off](#) on page 68.

No Internet Connection

If your modem cannot access the Internet, first check the DSL connection, and then check the WAN TCP/IP connections. See [Figure 11, Front panel LED icons](#) on page 66 for the location of the LEDs.

DSL Link

First determine whether you have a DSL link with the service provider. The state of this connection is indicated by the DSL LED.

DSL Link LED Is Green or Blinking Green

You have a good DSL connection. The service provider has connected your line correctly, and your wiring is correct.

DSL Link LED Is Blinking Green

Your broadband ADSL2+ modem is attempting to make a DSL connection with the service provider. The LED should turn green within several minutes.

If the DSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone as described in [ADSL Microfilters](#) on page 10. If you connect the microfilters correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL link LED, there might be a problem with your wiring. If the telephone company has tested the DSL signal at your network interface device (NID), you might have poor-quality wiring in your house.

DSL Link LED Is Off

First disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, and use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL link LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the DSL service. It could be necessary to use a swapper if your DSL signal is on pins 1 and 4 or the RJ-11 jack. The modem uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device could not connect to the Internet. Verify the following:

- Check that your log-in credentials are correct. See [Log In to the Modem](#) on page 17 for more information.
- Check that the information you entered on the Basic Settings screen is correct. See [Manual Setup \(Basic Settings\)](#) on page 21.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the DSL settings screen are correct.
- Find out if the ISP is having a problem. If it is, wait until that problem is cleared up, and try again.

Cannot Obtain an Internet IP Address

If your modem cannot access the Internet, and your Internet LED is green or blinking green, check whether the modem can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem has to request an IP address from the ISP. You can determine whether the request was successful as follows:

1. Access the modem menus at <http://192.168.0.1> and log in.

2. Under Maintenance, select **Router Status**, and check that an IP address shows for the WAN port. If 0.0.0.0 shows, your modem has not obtained an IP address from your ISP.

If your modem cannot obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrect. See *Debug PPPoE or PPPoA* on page 69.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem in the browser-based Setup Wizard. See *Setup Wizard* on page 20 for more information.
- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your computer's MAC address. In this case, do one of the following:
 - Inform your ISP that you have bought a new network device, and ask them to use the modem's MAC address.
 - Configure your modem to spoof your computer's MAC address through the Basic Settings screen. See *Manual Setup (Basic Settings)* on page 21.

Debug PPPoE or PPPoA

➤ To debug the PPPoE or PPPoA connection:

1. Access the modem menus at <http://192.168.0.1> and log in.
2. Select **Maintenance > Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, your PPPoE or PPPoA connection is working.
5. If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**.

The modem continues to attempt to connect indefinitely. If you do not connect after several minutes, check that the service name, user name, and password you are using are correct. Also check with your ISP to be sure that there is no problem with their service.

Note: Unless you connect manually, the modem does not authenticate with PPPoE or PPPoA until data is transmitted to the network.

Cannot Load an Internet Web Page

If your modem can obtain an IP address, but your browser cannot load any Internet web pages:

- Your computer might not recognize any DNS server addresses.
A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the broadband ADSL2+ modem's configuration, reboot your computer, and verify the DNS address. Alternately, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer might not have the modem configured as its TCP/IP router.
If your computer obtains its information from the modem by DHCP, reboot the computer, and verify the modem address.

TCP/IP Network Not Responding

Most TCP/IP terminal devices and modems have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem

You can ping the modem from your computer to verify that the LAN path to your modem is set up correctly.

- **To ping the modem from a PC running Windows 95 or later:**
1. From the Windows taskbar, click the **Start** button, and select **Run**.
 2. In the field provided, type **ping** followed by the IP address of the modem, as in this example:
ping 192.168.0.1
 3. Click **OK**.
 - a. You should see a message like this one:
"Pinging <IP address> with 32 bytes of data"
 - b. If the path is working, you see this message:
"Reply from < IP address >: bytes=32 time=NN ms TTL=xxx"
 - c. 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 [Ethernet LED Is Off](#) on page 67.
- 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 modem.
- 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 modem and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, type:

ping -n 10 IP address

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

If the path is functioning correctly, replies as described in [Test the LAN Path to Your Modem](#) on page 70 display. If you do not receive replies:

- Check that your PC has the IP address of your modem listed as the default broadband ADSL2+ modem. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the modem is listed as the default modem.
- Check 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 or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single PC connected to that modem. In this case, configure your modem to clone or spoof the MAC address from the authorized PC.

Cannot Log in

If you cannot log in to the broadband ADSL2+ modem from a computer on your local network, check the following:

- The modem is plugged in and it is on.
- You are using the correct login information. The login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

- Check the Ethernet connection between the computer and the modem. The Ethernet LED should light up to show your connection.
- Your computer's IP address is on the same subnet as the modem. If you are using the recommended addressing scheme, your computer's address should be in the range 192.168.0.2 to 192.168.0.254.
- If the computer IP address is 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address when the computer cannot reach a DHCP server. The auto-generated addresses are in the range 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem, and reboot your computer.
- If your modem's IP address was changed and you do not know the current IP address, clear the modem's configuration to factory defaults as explained in [Factory Settings](#) on page 75. This sets the modem's IP address to 192.168.0.1.
- 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 closing the browser and relaunching it.

Changes Not Saved

If the modem does not save the changes you make in the modem interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Firmware Needs to Be Reloaded

When you attempt to connect to the Internet, the browser might display a message similar to the following figure telling you that you need to reload the modem's firmware. This means a problem has been detected with the modem's firmware.

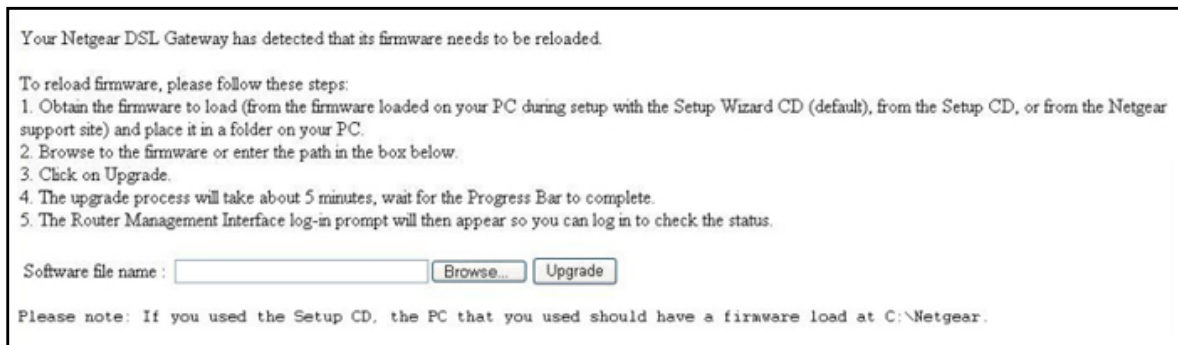


Figure 12. Reload firmware

➤ **To reload the firmware:**

1. If you already have the firmware file on your PC, go directly to *step 2*. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at <http://www.netgear.com/support> through another working Internet connection.
2. Click **Browse**.
3. Navigate to the firmware file.
4. Click **Upgrade**. A progress bar displays. The reload takes about 5 minutes to complete. When the firmware recovery is completed, the login screen displays so you can log in.

Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The modem uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. This means the modem has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the modem, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The modem does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

A Technical Specifications



This appendix includes the factory default settings, technical specifications for the modem, related documents, and instructions for wall-mounting the unit.

This appendix contains the following sections:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the modem to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Restore Factory Settings** button for at least 7 seconds. The modem resets, and returns to the factory settings. Your device will return to the factory settings shown in the following table.

Feature	Default Behavior
Modem Login	
User login URL	http://www.routerlogin.net or http://www.routerlogin.com
User name (case-sensitive)	admin
Login password (case-sensitive)	password
Internet Connection	
WAN MAC address	Use default address
WAN MTU size	1492
Port speed	AutoSense
Local Network (LAN)	
Lan IP	192.168.0.1
Subnet mask	255.255.255.0
RIP direction	None
RIP version	Disabled
RIP authentication	None
DHCP server	Enabled
DHCP starting IP address	192.168.0.2
DHCP ending IP address	192.168.0.254
DMZ	Disabled
Time zone	GMT-8 Pacific time
Time zone adjusted for Daylight Saving time	Disabled
SNMP	Disabled
Firewall	
Inbound (from the Internet)	Disabled (except traffic on port 80, the HTTP port)
Outbound (out to the Internet)	Enabled (all)
Source MAC filtering	Disabled

Technical Specifications

Feature	Specification
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter (North America)	120V, 60 Hz, input 12 V @1.0A output
Dimensions	5.79 x3.76 x 1.2 inches (47 x 95.5 x 30.5 mm)
Weight	0.42 lbs (190 grams)
Operating temperature	0° to 40° C (32° to 104° F)
Operating humidity	10% to 90% relative humidity, noncondensing
Storage temperature	-20° to 70° C (-4° to 158° F)
Storage humidity	5 to 95% relative humidity, noncondensing
Meets requirements of	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	DSL, RJ-11, pins 2 and 3 ITU 992.1 (G.dmt) Annex A, ITU 992.2 (G.lite), ITU 992.3 ADSL2 (G.dmt.bis), ITU 992.5 ADSL2+

Notification of Compliance



NETGEAR Wired Products

Regulatory Compliance Information

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

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

FCC Requirements for Operation in the United States

FCC Information to User

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

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 Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Broadband ADSL2+ Modem DM111PSPv2 complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and

- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

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

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

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, Broadband ADSL2+ Modem DM111PSPv2, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

European Union

The Broadband ADSL2+ Modem DM111PSPv2 complies with essential requirements of EU EMC Directive 2004/108/EC and Low Voltage Directive 2006/95/EC as supported by applying the following test methods and standards:

- EN55022: 2006 / A1: 2007
- EN55024: 1998 / A1: 2001 / A2 : 2003
- EN60950-1: 2005 2nd Edition
- EN 61000-3-2:2006
- EN 61000-3-3:1995 w/A1: 2001+A2: 2005

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to <ftp://downloads.netgear.com/files/GPLnotice.pdf>.

Broadband ADSL2+ Modem DM111PSPv2

For GNU General Public License (GPL) related information, please visit http://support.netgear.com/app/answers/detail/a_id/2649.

Index

A

- AC power adapter input **8**
- accessing remote computer **29**
- addresses, DNS **23**
- ADSL microfilters **10**
 - cabling **11**
 - described **10**
- ADSL port **8**
- ADSL settings **24**
- ADSL statistics, viewing **50**
- alerts, emailing **41**
- Application Level Gateway (ALG), disabling **55**
- attached devices, viewing **51**
- automatic firmware checking **44**
- automatic Internet connection **20**

B

- back panel **8**
- backing up configuration **47**
- Basic Settings screen
 - described **22**
 - manual setup **21**
- blocking
 - content and services **27**
 - keywords, examples **28**
- box contents **7**

C

- cabling
 - Ethernet **12**
 - phone line **11**
- changes not saved, router **72**
- compliance **77**
- configuration file **47, 48**
 - managing **47**
- connection, Internet **16**
- content filtering **27**
- country setting **20**
- CU-SeeMe **36**

D

- date and time **73**
- daylight savings time **39, 73**
- default demilitarized zone (DMZ) server **55**
- default factory settings **75**
- deleting configuration **48**
- denial of service (DoS)
 - port scans **54**
 - protection **27**
- diagnostic utilities **52**
- disabling
 - firewalls **23**
 - SIP ALG **55**
- DNS servers **29**
- Domain Name Server (DNS) addresses **23, 56**
- DSL port settings **49**
- Dynamic DNS **56**
- Dynamic Host Configuration Protocol (DHCP) server **58**

E

- email notices **41**
- erasing configuration **48**
- Ethernet cable **12**

F

- factory default settings
 - restoring **48**
- factory settings
 - list of **75**
 - restoring **8**
- filtering content **27**
- firewalls
 - CU-SeeMe connection **36**
 - IM ports **34**
 - inbound rules **34, 35, 36**
 - outbound rules **36**
 - rules **33**
- firmware
 - automatic check **44**
 - reload firmware message **72**

- upgrade at log in **18**
- upgrading **44**
- upgrading manually **46**

front panel **9**

front panel LEDs **9**

G

gateway IP address **23**

Genie, NETGEAR **15**

H

host name **22**

host trusted **29**

I

inbound firewall rules **34**

installation

- manual setup **21**
- NETGEAR Genie **15**

Instant Messaging (IM) ports **34**

Internet port **16, 20**

Internet port, no connection **25**

Internet Relay Chat (IRC) **31**

Internet Service Provider (ISP), see ISP

IP address

- LAN service **57**
- reserved **59**

IP setup, LAN **57**

ISP

- account information **15**
- ADSL settings **24**
- Basic Settings screen **22**
- DSL synchronization **9**

ISP login **15**

K

keywords **28**

L

LAN port (local port) **49**

LAN setup **57**

language setting **20**

LEDs

- troubleshooting **66**
- verifying cabling **12**

logging in

- cannot **71**
- changing password **25**

ISP **15**

- router **17**
- time-out **26**
- types **26**
- upgrade firmware **18**

login time-out **25**

logs, emailing **41**

logs, traffic **35**

M

MAC addresses

- rejected **71**
- spoofing **69**

maintenance settings **43**

manual logout **26**

manual setup **21**

Maximum Transmit Unit (MTU) **55**

menus, described **19**

metric, number of routers **62**

modem interface, described **19**

modem status **49**

multicasting **58**

N

NETGEAR Genie **15**

Network Address Translation (NAT) **23, 30, 58**

Network Time Protocol (NTP) **39, 73**

networks

- controlling access **29**
- troubleshooting **70**

no Internet connection **25**

O

one-line ADSL microfilter **10**

online help **19**

outbound firewall rules **36**

P

passwords **8**

phone line, cabling **11**

Plug and Play, Universal (UPnP) **63**

Point-to-Point over Ethernet (PPPoE)

- enabling relay **54**
- WAN port setting default **17**

Point-to-Point Tunneling Protocol (PPTP) **21**

port forwarding **32, 33**

port numbers **38**

port scanning, WAN settings **54**

port triggering **30, 33**
ports
 filtering **36**
 forwarding **34**
 Instant Messaging **34**
power adapter, AC **8**
primary DNS addresses **23**

R

remote management **59**
reserved IP address **59**
restoring
 factory default settings **48, 75**
router menus, access from additional port **58**
router, status **48**
Router_Setup.html **16**
Routing Information Protocol (RIP) **57**

S

security settings **27**
sending logs by email **41**
services **36, 38**
Session Initiation Protocol (SIP), disabling **55**
setting time zone **39**
settings.viewing **16**
Setup Wizard **20**
Simple Mail Transfer Protocol (SMTP) **41**
sites, blocking **28**
static routes **61, 62**
statistics, viewing **50**
status
 Internet connection **51**
 router **48**

T

TCP/IP
 network troubleshooting **70**
 no Internet connection **25**
technical specifications **76**
technical support **2**
time of day **73**
time zone, setting **39**
time-stamping **39**
trademarks **2**
traffic, log **35**
troubleshooting **65**
 cannot log in **71**
 date or time incorrect **73**

firmware reload **72**
LEDs **66, 67**
network **70**
router changes not saved **72**
router not on **66**

trusted host **29**
two-line ADSL microfilter **10**

U

Universal Plug and Play (UPnP) **63**
upgrading firmware **44**

V

virtual channel identifier (VCI) **15, 24**
virtual path identifier (VPI) **15, 24**

W

WAN port
 default **17**
WAN settings **54, 55**
 pinging WAN port **55**
wrong date or time **73**