

N300 Wireless Router WNR2000v3 User Manual



NETGEAR®

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

202-10706-01
September 2010
v1.0

© 2010 by NETGEAR, Inc. All rights reserved.

Product Registration, Support, and Documentation

Register your product at <http://www.NETGEAR.com/register>. Registration is required before you can use our telephone support service. Product updates and Web support are always available by going to:

<http://www.netgear.com/support>.

Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the Knowledgebase or the Documentation link under Web Support in the main menu to view support information.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and RangeMax and Smart Wizard are trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Windows Vista is a trademark of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the N300 Wireless Router WNR2000v3 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das N300 Wireless Router WNR2000v3 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

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

EN300 328, EN301 893, EN301 489-17, EN60950

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WNR2000v3 product package.

Europe – Declaration of Conformity in Languages of the European Community

Cesky [Czech]	<i>NETGEAR Inc.</i> tímto prohlašuje, že tento Radiolan je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede <i>NETGEAR Inc.</i> erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erkläre <i>NETGEAR Inc.</i> , dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab <i>NETGEAR Inc.</i> seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, <i>NETGEAR Inc.</i> , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente <i>NETGEAR Inc.</i> declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>NETGEAR Inc.</i> ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente <i>NETGEAR Inc.</i> déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente <i>NETGEAR Inc.</i> dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>NETGEAR Inc.</i> deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>NETGEAR Inc.</i> deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart <i>NETGEAR Inc.</i> dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, <i>NETGEAR Inc.</i> , jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, <i>NETGEAR Inc.</i> nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym <i>NETGEAR Inc.</i> oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	<i>NETGEAR Inc.</i> declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	<i>NETGEAR Inc.</i> izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>NETGEAR Inc.</i> týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	<i>NETGEAR Inc.</i> vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar <i>NETGEAR Inc.</i> att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir <i>NETGEAR Inc.</i> yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	<i>NETGEAR Inc.</i> erklærer herved at utstyret <i>Radiolan</i> er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the model WNR2000v3 N300 Wireless Router WNR2000v3 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.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

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

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

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

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

Caution:

N300 Wireless Router WNR2000v3



Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

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

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Product and Publication Details

Model Number:	WNR2000v3
Publication Date:	September 2010
Product Family:	Wireless Router
Product Name:	N300 Wireless Router WNR2000v3
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10706-01

Contents

About This Manual

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

Chapter 1

Configuring Your Internet Connection

Using the Setup Manual	1-1
Logging In to Your Wireless Router	1-2
Selecting a Language for Your Screen Display	1-4
Using the Setup Wizard	1-6
Viewing or Manually Configuring Your ISP Settings	1-6

Chapter 2

Safeguarding Your Network

Planning Your Wireless Network	2-1
Wireless Placement and Range Guidelines	2-2
Wireless Security Options	2-3
Manually Configuring Your Wireless Settings	2-4
Configuring WEP Wireless Security	2-9
Configuring WPA, WPA2, or WPA/WPA2 Wireless Security	2-11
Using Push 'N' Connect (WPS) to Configure Your Wireless Network	2-13
Using a WPS Button to Add a WPS Client	2-14
Using PIN Entry to Add a WPS Client	2-15
Configuring Advanced WPS Settings	2-17
Connecting Additional Wireless Client Devices After WPS Setup	2-18
Adding More WPS Clients	2-18
Adding Both WPS and Non-WPS Clients	2-18
Restricting Access to Your Router	2-20
Adding Guest Networks	2-21

Chapter 3**Protecting Your Network**

Protecting Access to Your Wireless Router	3-1
Changing the Built-In Password	3-2
Restricting Access by MAC Address	3-2
Blocking Access to Internet Sites	3-4
Blocking Access to Internet Services	3-5
Configuring a User-Defined Service	3-7
Scheduling Blocking	3-8
Viewing Logs of Web Access or Attempted Web Access	3-8
Configuring E-mail Alert and Web Access Log Notifications	3-9
Setting the Time	3-11

Chapter 4**Using Network Monitoring Tools**

Upgrading the Router Firmware	4-1
Upgrading Automatically to New Router Software	4-3
Upgrading Manually to New Router Software	4-3
Viewing Wireless Router Status Information	4-5
Connection Status	4-8
Statistics	4-9
Viewing a List of Attached Devices	4-10
Managing the Configuration File	4-11
Backing Up and Restoring the Configuration	4-11
Erasing the Configuration	4-12
Enabling Remote Management Access	4-13
Traffic Meter	4-15

Chapter 5**Customizing Your Network Settings**

Using the LAN Setup Options	5-1
Using the Router as a DHCP Server	5-4
Address Reservation	5-4
Using a Dynamic DNS Service	5-5
Configuring the WAN Setup Options	5-7
Setting Up a Default DMZ Server	5-8
Configuring Static Routes	5-9

Allowing Inbound Connections to Your Network	5-11
How Your Computer Accesses a Remote Computer through Your Router	5-11
How Port Triggering Changes the Communication Process	5-13
How Port Forwarding Changes the Communication Process	5-14
How Port Forwarding Differs from Port Triggering	5-15
Configuring Port Forwarding to Local Servers	5-16
Adding a Custom Service	5-17
Editing or Deleting a Port Forwarding Entry	5-18
Configuring Port Triggering	5-18
Wireless Repeating (Also Called WDS)	5-22
Wireless Repeating Function	5-23
Setting Up the Base Station	5-24
Setting Up a Repeater Unit	5-26

Chapter 6

Fine-Tuning Your Network

Assessing Your Speed Requirements	6-2
Optimizing Your Network Bandwidth	6-3
Optimizing Wireless Performance	6-5
Changing the MTU Size	6-6
Quality of Service (QoS)	6-7
Using WMM QoS for Wireless Multimedia Applications	6-8
Configuring QoS for Internet Access	6-8
Universal Plug and Play	6-13

Chapter 7

Troubleshooting

Quick Tips	7-1
Troubleshooting Basic Functions	7-3
Cannot Access the Router Main Menu	7-4
Cannot Access the Internet	7-5
Troubleshooting a Network Using the Ping Utility	7-6
Testing the LAN Path to Your Router	7-7
Testing the Path from Your Computer to a Remote Device	7-8
Problems with Date and Time	7-8

Wireless Connectivity	7-9
Using Your Wireless Card Setup Program	7-9
Setting Up and Testing Basic Wireless Connectivity	7-10
Restoring the Default Configuration and Password	7-14
Appendix A	
Default Configuration and	
Technical Specifications	
Restoring the Default Factory Configuration Settings	A-1
Technical Specifications	A-3
Appendix B	
Related Documents	
Index	

About This Manual

The user manual provides information for configuring the features of the NETGEAR® N300 Wireless Router with USB WNR2200 beyond initial configuration settings. Initial configuration instructions can be found in the *NETGEAR Wireless Router Setup Manual*. You should have basic to intermediate computer and Internet skills.


Conventions, Formats, and Scope


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


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

<i>Italic</i>	Emphasis, books, CDs
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>Italic</i>	URL links

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

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

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

	Warning: Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data.
---	---

- **Scope.** This manual is written for the WNR2000v3 router according to these specifications:

Product Version	N300 Wireless Router with USB WNR2200
Manual Publication Date	September 2010

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



Note: Product updates are available on the NETGEAR, Inc. website at <http://www.netgear.com/support>.

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.



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

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the WNR2000v3 router was introduced.

Table 1-1. Publication Revision History

Version	Date	Description
v1.0	September 2010	Original publication.

Chapter 1

Configuring Your Internet Connection

This chapter describes how to configure your WNR2000v3 router Internet connection. When you install your wireless router using the *Resource CD* as described in the *NETGEAR Router Setup Manual*, these settings are configured automatically for you. This chapter provides instructions on how to log in to the wireless router for further configuration.



Note: NETGEAR recommends using the Smart Wizard™ on the *Resource CD* for initial configuration, as described in the *NETGEAR Wireless Router Setup Manual*.

This chapter includes:

- “Using the Setup Manual”
- “Logging In to Your Wireless Router” on page 1-2
- “Selecting a Language for Your Screen Display” on page 1-4
- “Using the Setup Wizard” on page 1-6
- “Viewing or Manually Configuring Your ISP Settings” on page 1-6

Using the Setup Manual

For first-time installation of your wireless router, refer to the *NETGEAR Router Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless router.

For installation instructions in a language other than English, see the language options on the *Resource CD*.

Logging In to Your Wireless Router

You can log in to the wireless router to view or change its settings.



Note: Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in [“Preparing Your Network”](#) in [Appendix B](#).

To log in to the wireless router:

1. Type **http://www.routerlogin.net**, or **http://www.routerlogin.com**, or the router’s LAN IP address (default is 192.168.1.1) in the address field of your browser, and then press Enter. A login window displays:

The screenshot shows a login dialog box with a light gray background. It has two text input fields: 'User name:' and 'Password:'. The 'User name:' field contains the text 'admin' and has a small dropdown arrow on the right. The 'Password:' field contains a series of dots. Below the password field is a checkbox labeled 'Remember my password' which is currently unchecked. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 1-1

2. Enter **admin** for the router user name and your password (or the default, **password**). For information about how to change the password, see [“Changing the Built-In Password”](#) on [page 3-2](#).



Note: The router user name and password are not the same as any other user name or password you might use to log in to your Internet connection.

The Checking for Firmware Updates screen displays unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.

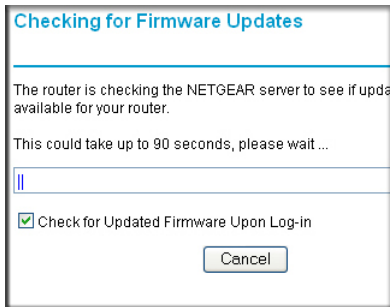


Figure 1-2

If the router discovers a newer version of the software, you are asked if you want to upgrade to the new software (see [“Upgrading the Router Firmware”](#) on page 4-1 for details). If no new firmware is available, the following message displays.

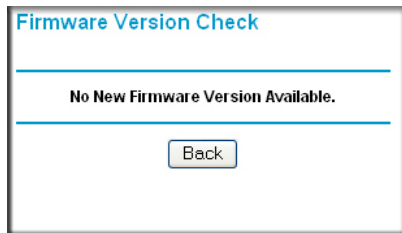


Figure 1-3

3. The Basic Settings screen displays showing the wireless router's settings.

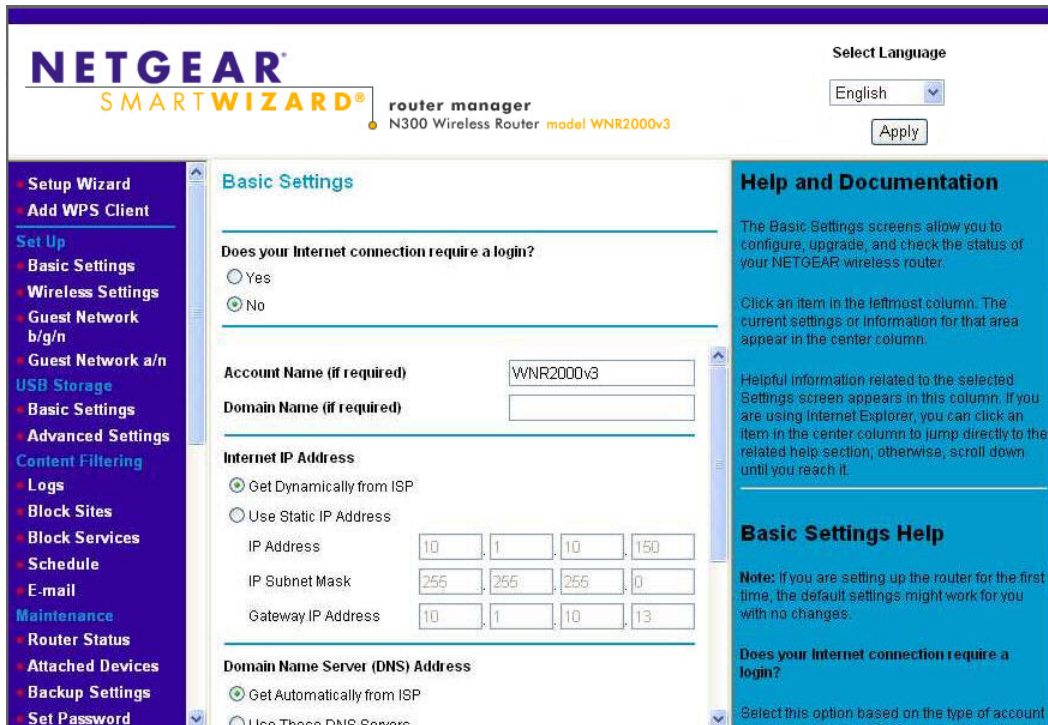


Figure 1-4

If the wireless router is connected to the Internet, you can click the **Knowledge Base** link or the **Documentation** link under Web Support to view support information or the documentation for the wireless router. If you do not click **Logout**, the wireless router waits for 5 minutes after no activity before it automatically logs you out.

Selecting a Language for Your Screen Display

Using the Select Language drop-down menu, located in the upper right corner of the Router Manager screen, you can display the router manager screens in any of languages shown in Figure 1-5:

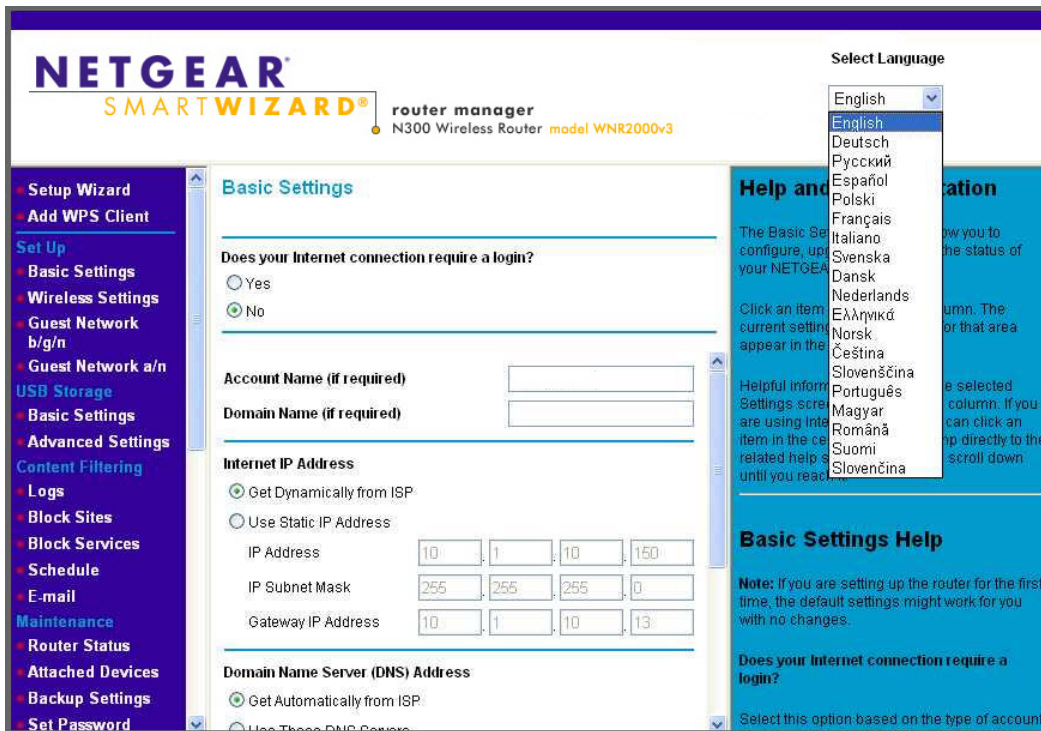


Figure 1-5

The language is set to English by default. The default language, as well as German, Russian, and Portuguese are always stored in memory. When you select a language other than those automatically stored in flash memory, if you are connected to the Internet at the time you select it, that language is also stored in memory.

- If you are connected to the Internet and select a language that is not already stored in flash memory, the language is downloaded from the NETGEAR server and stored in the current language partition of flash memory.
- If you are not connected to the Internet when you select a language, you can only select as the current language one of the languages that is stored in flash memory.

To specify a language to be used on your router manager screens, do the following:

1. Expand the list and select the language you want.
2. Click **Apply**.

The language you select is then downloaded and displayed in the language selection box, and your screen display will be in the selected language.



Note: If you are not connected to the Internet and select a language that is not stored in flash memory, your selection may fail. If you see a “download fails” message after your language selection, make sure you are connected to the Internet and make your selection again.

Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Smart Setup Wizard to detect your Internet connection. The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

This feature is not the same as the Smart Wizard on the *Resource CD* that is used for installation. To use the Smart Setup Wizard to assist with configuration or to verify the Internet connection settings, follow this procedure:

1. From the top of the main menu, select **Setup Wizard**.
2. Select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.
3. Enter your ISP settings, as needed.
4. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see [Chapter 7, “Troubleshooting.”](#)

Viewing or Manually Configuring Your ISP Settings

To view or configure the basic settings:

1. Log in to the wireless router as described in [“Logging In to Your Wireless Router” on page 1-2](#).
2. On the Basic Settings screen, select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.
 - **Yes.** If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.
 - **No.** If your ISP does not require a login, enter the account name, if required, and the domain name, if required.

3. Enter the settings for the IP address and DNS server. If you enter or change a DNS address, restart the computers on your network so that these settings take effect.
4. If no login is required, you can specify the MAC Address setting.
5. Click **Apply** to save your settings.
6. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, see [Chapter 7, “Troubleshooting”](#).

When your Internet connection is working, you do not need to launch the ISP’s login program on your computer to access the Internet. When you start an Internet application, your wireless router automatically logs you in.

The fields that are displayed depend on whether or not your Internet connection requires a login.

ISP does not require login

Basic Settings

Does Your Internet Connection Require A Login?

Yes

No

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Router MAC Address

Use Default Address

Use Computer MAC Address

Use This MAC Address

ISP does require login

Basic Settings

Does your Internet connection require a login?

Yes

No

Internet Service Provider

Login

Password

Service Name (if required)

Connection Mode

Idle Time-out (in minutes)

Internet IP Address

Get Dynamically from ISP

Use Static IP Address

IP Address

Domain Name Server (DNS) Address

Get Automatically from ISP

Use These DNS Servers

Primary DNS

Secondary DNS

Figure 1-6

The following table explains the fields in the Basic Settings screen.

Table 1-1. Basic Settings screen fields

Settings		Description
Does Your ISP Require a Login?		<ul style="list-style-type: none"> • Yes • No
These fields appear only if no login is required.	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.
These fields appear only if your ISP requires a login.	Internet Service Provider	<ul style="list-style-type: none"> • PPTP (Point to Point Tunneling Protocol). This is used primarily in Austrian DSL services. • Telstra Bigpond. This setting is only for older cable modem service accounts that still require a Bigpond Login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cable modem accounts should select No for Does Your Internet Connection Require A Login? • Other. This is the default setting. It is for PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide.
	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password provided by your ISP.
	Service Name	If your ISP provided a Service Name, enter it here.
	Connection Mode	Specify when the router will connect to and disconnect from the Internet. <ul style="list-style-type: none"> • Always On. The router logs in to the Internet immediately after booting and never disconnects. • Dial on Demand. The router logs in only when outgoing traffic is present and logs out after the idle time-out. • Manually Connect. The router logs in or logs out only when you click Connect or Disconnect in the Router Status screen.
	Idle Timeout (In minutes)	If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.

Table 1-1. Basic Settings screen fields (continued)

Settings		Description
Internet IP Address		<ul style="list-style-type: none"> • 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 that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's wireless router to which your wireless router will connect.
Domain Name Server (DNS) Address		<p>The DNS server is used to look up site addresses based on their names.</p> <ul style="list-style-type: none"> • 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 wireless router 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.
This field appears only if no login is required.	Router MAC Address	<p>The Ethernet MAC address that will be used by the wireless router on the Internet port. Some ISPs register the Ethernet 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 wireless router to masquerade as that computer by "cloning" its MAC address.</p> <ul style="list-style-type: none"> • Use Default Address. Use the default MAC address of the router (normally the LAN MAC address). • Use Computer MAC Address. The wireless router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • Use This MAC Address. Enter the MAC address that you want to use.

Chapter 2

Safeguarding Your Network

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



Warning: Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- “Planning Your Wireless Network”
- “Manually Configuring Your Wireless Settings” on page 2-4
- “Using Push 'N' Connect (WPS) to Configure Your Wireless Network” on page 2-13
- “Connecting Additional Wireless Client Devices After WPS Setup” on page 2-18
- “Restricting Access to Your Router” on page 2-20



Note: For information about restricting access to USB storage devices, see “Configuring USB Storage Advanced Settings” on page 7-7.

Planning Your Wireless Network

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

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

- To manually configure the wireless settings, you must know the following:
 - SSID. The default SSID for the wireless router is NETGEAR.

- The wireless radio frequency (2.4GHz or 5GHz) that each wireless adapter supports.
- Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See “[Manually Configuring Your Wireless Settings](#)” on page 2-4.

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



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

To set up your wireless network using the WPS feature:

- Use the WPS button on the side of the wireless router (there is also an onscreen WPS button), or enter the PIN of the wireless device.
- Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

See “[Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network](#)” on page 2-13.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the wireless router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your wireless router according to the following guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

- Put the router in a vertical position to provide the best side-to-side coverage. Put the router in a horizontal position to provide the best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

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

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WNR2000v3 router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

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

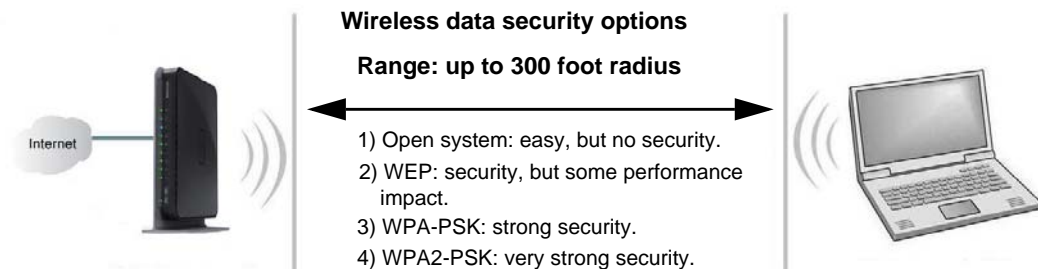


Figure 2-1

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

For more information about wireless technology, see the link to the online document in “[Wireless Networking Basics](#)” in Appendix B.

Manually Configuring Your Wireless Settings

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



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

To view or manually configure the wireless settings:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the wireless router.

2. Select **Wireless Settings** from the main menu to display the Wireless Settings screen:

Wireless Settings

Region Selection
Region: United States

Wireless Network(2.4GHz b/g/n)
 Enable SSID Broadcast
Name (SSID): NETGEAR
Channel: Auto
Mode: Up to 130 Mbps

Security Options
 None
 WEP
 WPA-PSK (TKIP)
 WPA2-PSK (AES)
 WPA-PSK (TKIP) + WPA2-PSK (AES)
 WPAWPA2 Enterprise

Wireless Network (5GHz a/n)
 Enable SSID Broadcast
 Enable Video Network
Name (SSID): NETGEAR-5G
Channel: 36
Mode: Up to 300 Mbps

Security Options
 None
 WEP
 WPA-PSK (TKIP)
 WPA2-PSK (AES)
 WPA-PSK (TKIP) + WPA2-PSK (AES)
 WPAWPA2 Enterprise

Apply Cancel

Figure 2-2

The settings for this screen are explained in [Table 2-1 on page 2-6](#).

3. Select the region in which the wireless router will operate.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.

6. Configure and test your computers for wireless connectivity.

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

Table 2-1. Wireless Settings

Settings		Description
Region Selection		The location where the router is used. Select from the countries in the drop-down list. Note: In the US, the region is pre-selected as the United States.
Wireless Network	Enable SSID Broadcast	The SSID of any wireless access adapter must match the SSID you configure in the wireless router. If they do not match, you will not get a wireless connection to the wireless router. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP.
	Name (SSID)	This is the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device that you want to participate in a wireless network must use the SSID.
	Channel	The wireless channel fields determine the operating frequency used for the 11N or 11G wireless networks. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
	Mode	Specify the wireless mode to be used. The options are: <ul style="list-style-type: none"> • Up to 54 Mbps. Legacy mode, using a maximum speed of up to 54 Mbps for b/g networks. • Up to 130 Mbps. Neighbor friendly mode, for reduced interference with neighboring wireless networks. Provides two transmission streams with different data on the same channel at the same time, but also allows 802.11b and 802.11g wireless devices. • Up to 300 Mbps. Performance mode, using a maximum Wireless-N speed of up to 300 Mbps.

Table 2-1. Wireless Settings (continued)

Settings	Description
Security Options	<ul style="list-style-type: none"> • None. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • WEP (Wired Equivalent Privacy). Use encryption keys and data encryption for data security. Select 64-bit or 128-bit encryption. See “Configuring WEP Wireless Security.” When you select this option, these additional areas appear on your screen: <ul style="list-style-type: none"> • Security Encryption (WEP). Select the Authentication Type (Automatic or Shared Key) and the Encryption Strength (64 bit or 128 bit). • Security Encryption (WEP) Key. Enter the Passphrase, select a key, and click Generate. • WPA-PSK [TKIP] (WiFi Protected Access Pre-Shared Key). Allow only computers configured with WPA to connect to the wireless router. When you select this option, this additional area appears on your screen: <ul style="list-style-type: none"> • Security Options (WPA-PSK). Enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits. • WPA2-PSK [AES] (Wi-Fi Protected Access with 2 Pre-Shared Keys). Allow only computers configured with WPA2 to connect to the wireless router. When you select this option, this additional area appears on your screen: <ul style="list-style-type: none"> • Security Options (WPA2-PSK). Enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits. • WPA-PSK [TKIP] + WPA2-PSK [AES]. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router. When you select this option, this additional area appears on your screen: <ul style="list-style-type: none"> • Security Options (WPA-PSK + WPA2-PSK). Enter the WPA passphrase (Network key). The passphrase must be between 8 and 63 ASCII characters or exactly 64 hex digits.

Table 2-1. Wireless Settings (continued)

Settings	Description
	<ul style="list-style-type: none"> • WPA/WPA2 Enterprise. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router. When you select this option, this additional area appears on your screen: <p style="margin-left: 20px;">Security Options (WPA/WPA2 Enterprise)</p> <ul style="list-style-type: none"> • WPA Mode. Select the WPA Mode from the drop-down list (WPA [TKIP], WPA2 [AES], or WPA [TKIP + WPA2 [AES]). • RADIUS server IP Address. Enter the IP address of the RADIUS server. • RADIUS server Port. The RADIUS server port number is listed in this field. • RADIUS server Shared Secret. Enter the Shared Secret.

Configuring WEP Wireless Security



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

To configure WEP data encryption:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the wireless router.
2. From the main menu, select **Wireless Settings** to display the Wireless Settings screen.

3. Set the Security Options by selecting the **WEP** radio button in the Security Options section:

Figure 2-3

4. Select the **Authentication Type: Automatic or Shared Key**.



Note: The authentication scheme is separate from the data encryption. You can select an automatic authentication scheme, which may not run authentication, but still leaves the data transmissions encrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

5. Select the **Encryption Strength** setting:
- **WEP 64-bit encryption.** Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
 - **WEP 128-bit encryption.** Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network:

- **Passphrase.** To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the wireless router.



Note: Not all wireless adapters support passphrase key generation.

- **Key 1 – Key 4.** These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

7. Select which of the four keys will be the default.

Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.

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

Configuring WPA, WPA2, or WPA/WPA2 Wireless Security

To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see “Using Push 'N' Connect (WPS) to Configure Your Wireless Network” on page 2-13).

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later. NETGEAR recommends using WPA2 with AES, which provides the strongest security. WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.



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

To configure WPA or WPA2 in the wireless router:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless router.
2. Select **Wireless Settings** from the main menu.
3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.

Wireless Network(2.4GHz b/g/n)

Enable SSID Broadcast

Name (SSID)

Channel

Mode

Security Options

None

WEP

WPA-PSK (TKIP)

WPA2-PSK (AES)

WPA-PSK (TKIP) + WPA2-PSK (AES)

WPA/WPA2 Enterprise


Security Options (WPA2-PSK)

Passphrase (8-63 characters or 64 hex digits)

Figure 2-4

4. The settings displayed on the screen depend on which security option you select.
5. For WPA-PSK or WPA2-PSK, enter the passphrase.
6. For WPA/WPA2 Enterprise, enter the settings for the Radius server. For WPA-802.1x or WPA2-802.1x, these settings are required for communication with the primary Radius server.
 - **WPA Mode.** Select WPA [TKIP], WPA2 [AES], or WPA [TKIP] + WPA2 [AES].
 - **RADIUS Server IP Address.** The IP address of the Radius server. The default is 0.0.0.0
 - **RADIUS Server Port.** Port number of the Radius server. The default is 1812.
 - **RADIUS Server Shared Secret.** This shared key is shared between the wireless access point and the Radius server during authentication.
7. To save your settings, click **Apply**.

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

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



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

Some considerations regarding WPS are:

- WPS supports these types of wireless security: None, WPA-PSK, WPA2-PSK, and WEP (with the authentication type set to **Automatic** on the Wireless Settings screen). WEP security with shared key authentication is not supported by WPS.
- If your wireless network will include a combination of WPS capable devices and non-WPS capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding additional WPS capable devices. See [“Adding Both WPS and Non-WPS Clients” on page 2-18](#).

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

- **Using the Push Button.** This is the preferred method. See the following section, [“Using a WPS Button to Add a WPS Client” on page 2-14](#).
- **Entering a PIN.** For information about using the PIN method, see [“Using PIN Entry to Add a WPS Client” on page 2-15](#).

Using a WPS Button to Add a WPS Client

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

To use the wireless router WPS button to add a WPS client:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the wireless router main menu, select Add a WPS Client, and then click **Next**. The following screen displays:

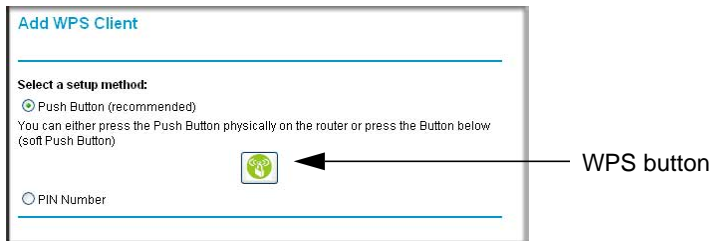


Figure 2-5

By default, the **Push Button (recommended)** radio button is selected.

3. Either press the WPS button on the side of the wireless router, or click the onscreen button. The wireless router tries to communicate with the client for 2 minutes.
4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
5. Go back to the wireless router screen to check for a message.

The wireless router WPS screen displays a message confirming that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security. The wireless router will keep these wireless settings unless you change them, or you clear the **Keep Existing Wireless Settings** check box in the WPS Settings screen.

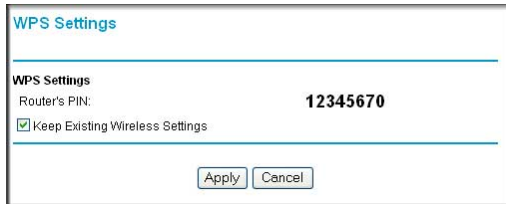


Figure 2-6

- Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See [“Manually Configuring Your Wireless Settings” on page 2-4.](#)

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



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

Using PIN Entry to Add a WPS Client

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

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the wireless router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use a PIN to add a WPS client:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the wireless router main menu, select Add a WPS Client (computers that will connect wirelessly to the wireless router are clients), and then click **Next**. The Add WPS Client screen displays:

Figure 2-7

3. Select the **PIN Number** radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. From the wireless router Add WPS Client screen, enter the client PIN number, and then click **Next**.
 - The wireless router tries to communicate with the client for 4 minutes.
 - The wireless router WPS screen displays a message confirming that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See [“Manually Configuring Your Wireless Settings” on page 2-4](#)

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



Note: If no WPS-capable client devices are located during the 4-minute time frame, the SSID will not be changed and no security will be implemented on the wireless router.

Configuring Advanced WPS Settings

From the Advanced menu, select Advanced Wireless Settings to display the following screen:

Figure 2-8

The WPS Settings area displays the wireless router PIN, and allow you to **Disable Router's PIN** and the **Keep Existing Wireless Settings**.

By default, both **Keep Existing Wireless Settings** check boxes are unchecked. This allows the wireless router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented or changes in wireless settings are applied, the wireless router automatically selects this check box so that your SSID and wireless security settings remain the same if you add WPS-enabled devices or if you manually add non WPS-capable devices later.



Note: If you clear either **Keep Existing Wireless Settings** check box, all wireless settings and connections will be lost for that wireless network.

Connecting Additional Wireless Client Devices After WPS Setup

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

Adding More WPS Clients



Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** check box is selected in the Advanced Wireless screen (listed under the Advanced heading in the wireless router main menu). If you clear this check box, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the wireless router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in [“Using a WPS Button to Add a WPS Client”](#) on page 2-14 or [“Using PIN Entry to Add a WPS Client”](#) on page 2-15.
2. To view a list of all devices connected to your wireless router (including wireless and Ethernet-connected), see [“Viewing a List of Attached Devices”](#) on page 4-10.

Adding Both WPS and Non-WPS Clients

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see [“Manually Configuring Your Wireless Settings”](#) on page 2-4).

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

1. Restore the wireless router to its factory default settings (press both the Wireless and WPS buttons on the side of the wireless router for 5 seconds).

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

2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see [“Manually Configuring Your Wireless Settings”](#) on page 2-4). and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.

3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
4. For the WPS devices that you want to connect, follow the procedure [“Using a WPS Button to Add a WPS Client”](#) on page 2-14 or [“Using PIN Entry to Add a WPS Client”](#) on page 2-15.

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



Note: To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the WPS Settings screen.

5. To view a list of all devices connected to your wireless router (including wireless and Ethernet-connected), see [“Viewing a List of Attached Devices”](#) on page 4-10.

Restricting Access to Your Router

You can use the Advanced Wireless Settings screen to enable or disable the wireless router. From the main menu, select **Advanced Wireless Settings** to display the following screen:

Advanced Wireless Settings

Advanced Wireless Settings (2.4GHz b/g/n)

Enable Wireless Router Radio

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

Advanced Wireless Settings (5GHz a/n)

Enable Wireless Router Radio

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

WPS Settings

Router's PIN

Disable Router's PIN

Keep Existing Wireless Settings (2.4G-hz b/g/n)

Keep Existing Wireless Settings (5GHz a/n)

Wireless Card Access List

Figure 2-9

- **Enable Wireless Router Radio.**

You can completely turn off the wireless portion of the wireless router. For example, if you use your notebook computer to wirelessly connect to your wireless router, and you take a business trip, you can turn off the wireless portion of the wireless router while you are traveling. Other members of your household who use computers connected to the wireless router via Ethernet cables can still use the wireless router. To do this, clear the **Enable Wireless Router Radio** check box on the Advanced Wireless Settings screen, and then click **Apply**.

The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

- **WPS Settings.** For information about WPS settings, see “Using Push 'N' Connect (WPS) to Configure Your Wireless Network” on page 2-13.
- **Restricting access by MAC address.** You can use a Wireless Card Access List to restrict access. See “Restricting Access by MAC Address” on page 3-2.

Adding Guest Networks

Adding a guest network allows visitors at your home to use the Internet without having to know your wireless security key.

To add a guest network, do the following:

1. Select **Guest Network** from the Setup menu. The Guest Network Settings screen appears

Figure 2-10

2. Select any of the following Wireless settings:
 - **Enable Guest Network** – When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
 - **Enable SSID Broadcast** – If selected, the Wireless Access Point broadcasts its name (SSID) to all Wireless Stations. Stations with no SSID can adopt the correct SSID for connections to this Access Point.

- **Allow Guest to access MY Local Network** – If selected any user who connects to this SSID can access local networks associated with the router like users in the primary SSID.

3. Give the wireless network a name.

The name is case-sensitive and can be up to 32 characters. The same name must be assigned to all wireless devices in your network. NETGEAR recommends that you change the name to a different value.

4. Select a Security option from the list.

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

Chapter 3

Protecting Your Network

This chapter describes how to use the content filtering and reporting features of the N300 Wireless Router WNR2000v3 to protect your network. You can find these features by selecting the items under Content Filtering in the wireless router main menu.

This chapter includes the following sections:

- “Protecting Access to Your Wireless Router”
- “Restricting Access by MAC Address” on page 3-2
- “Blocking Access to Internet Sites” on page 3-4
- “Blocking Access to Internet Services” on page 3-5
- “Scheduling Blocking” on page 3-8
- “Viewing Logs of Web Access or Attempted Web Access” on page 3-8
- “Configuring E-mail Alert and Web Access Log Notifications” on page 3-9
- “Setting the Time” on page 3-11

Protecting Access to Your Wireless Router

For security reasons, the wireless router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the wireless router user name and **password** for the wireless router password. You can use procedures in the following sections to change the wireless router password and the amount of time for the administrator’s login time-out.



Note: The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Built-In Password

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the wireless router.
2. From the main menu, under the Maintenance heading, select **Set Password** to display the Set Password screen:
3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.



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

Restricting Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WNR2000v3 router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

To restrict access based on MAC addresses:

1. Log in to the wireless router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin**, and default password of **password**, or using whatever password and LAN address you have chosen for the wireless router.



Note: If you configure the router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the wireless router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

- From the main menu, select Wireless Settings, and then click **Setup Access List** to display the Wireless Card Access List screen.



Figure 3-1

- Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

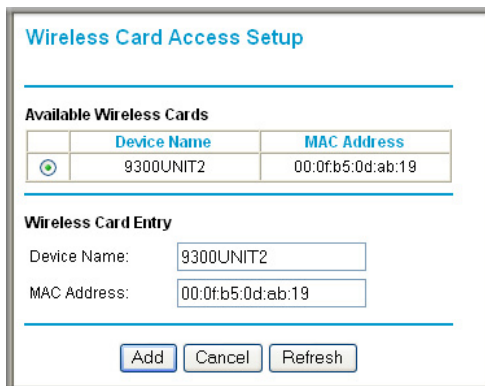
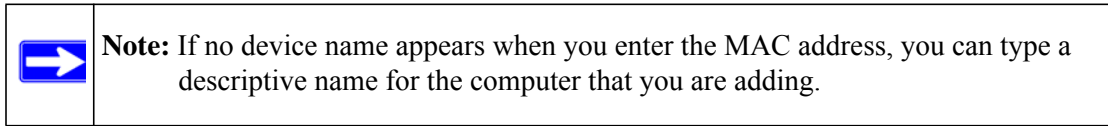


Figure 3-2

- Adjust the list as needed for your network. You can add devices using either of the following methods:
 - If the computer is in the Available Wireless Cards table, select the radio button of that computer to capture its MAC address.

- Use the **Add** button to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device.



5. Click **Add**, and then click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the router.

Blocking Access to Internet Sites

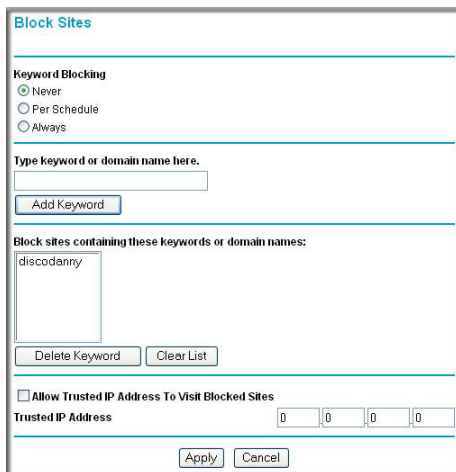
The WNR2000v3 router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL `www.zzzyyqq.com/xxx.html` is blocked.
- If the keyword **.com** is specified, only websites with other domain suffixes (such as `.edu`, `.org`, or `.gov`) can be viewed.

To block access to Internet sites:

1. Select **Block Sites** under Content Filtering in the main menu. The Block Sites screen displays.



Block Sites

Keyword Blocking

Never
 Per Schedule
 Always

Type keyword or domain name here.

Block sites containing these keywords or domain names:

Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address:

Figure 3-3

2. Enable keyword blocking by selecting either **Per Schedule** or **Always**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see “[Scheduling Blocking](#)” on page 3-8.

Block all access to Internet browsing during a scheduled period by entering a dot (.) as the keyword, and then set a schedule in the Schedule screen.

3. Add a keyword or domain by entering it in the keyword field and clicking **Add Keyword**. The keyword or domain name then appears the **Block sites containing these keywords or domain names** list.

Delete a keyword or domain name by selecting it from the list and clicking **Delete Keyword**.

4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer’s IP address in the **Trusted IP Address** fields.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

5. Click **Apply** to save all your settings in the Block Sites screen.

Blocking Access to Internet Services

The wireless router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. 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 your network sends a request for service to a server computer on the Internet, 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.

To block access to Internet services:

1. Select **Block Services** under Content Filtering in the main menu. The Block Services screen displays.

Block Services

Services Blocking

Never
 Per Schedule
 Always

Service Table

#	Service Type	Port	IP

Add Edit Delete

Apply Cancel

Figure 3-4

2. Enable service blocking by selecting either **Per Schedule** or **Always**, and then click **Apply**.

To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see “[Scheduling Blocking](#)” on page 3-8.

3. Specify a service for blocking by clicking **Add**. The Block Services Setup screen displays.

Block Services Setup

Service Type: AIM

Protocol: TCP

Starting Port: 5190 (1~65534)

Ending Port: 5190 (1~65534)

Service Type/User Defined: AIM

Filter Services For :

Only This IP Address: 192 . 168 . 1 .

IP Address Range: 192 . 168 . 1 . to 192 . 168 . 1 .

All IP Addresses

Add Cancel

Figure 3-5

4. From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.
5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields.

You can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

6. Click **Add** to enable your Block Services Setup selections.

Configuring a User-Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) 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. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

- Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.
- If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

Scheduling Blocking

To schedule blocking:

1. Select **Schedule** under Content Filtering in the main menu. The Schedule screen displays.

Figure 3-6

2. Configure the schedule for blocking keywords and services.
 - a. **Days to Block.** Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days. Click **Apply**.
 - b. **Time of Day to Block.** Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking. Click **Apply**.

Be sure to select your time zone in the E-mail screen as described in [“Setting the Time” on page 3-11](#).

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

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **Logs** under Content Filtering in the main menu. The Logs screen displays.

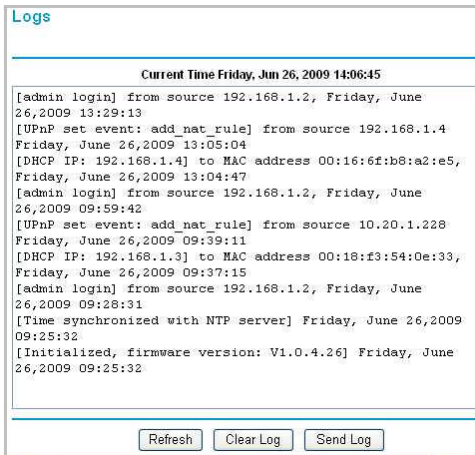


Figure 3-7

Table 3-1. Log Entry Descriptions

Field	Description
Date and time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the website or newsgroup visited or to which access was attempted.
Action	Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

To e-mail the log immediately, click the **Send Log** button.

Configuring E-mail Alert and Web Access Log Notifications

To receive logs and alerts by e-mail, you must provide your e-mail account information.

To configure e-mail alert and web access log notifications:

1. Select **E-mail** under Content Filtering in the main menu. The E-mail screen displays.

E-mail

Turn E-mail Notification On

Send Alerts and Logs Via E-mail

Your Outgoing Mail Server:

Send To This E-mail Address:

My Mail Server requires authentication

User Name:

Password:

Send Alert Immediately
When Someone Attempts To Visit A Blocked Site

Send Logs According to this Schedule

None

Day:

Time: a.m. p.m.

Time Zone

(GMT-08:00) Pacific Time (US Canada)

Automatically Adjust for Daylight Savings Time

Current Time: Monday, 24 Dec 2007 15:17:07

Figure 3-8

2. To receive e-mail logs and alerts from the router, select the **Turn E-mail Notification On** check box.
 - a. Enter the name of your ISP's outgoing (SMTP) mail server (such as **mail.myISP.com**) in the **Your Outgoing Mail Server** field. You might be able to find this information in the configuration screen of your e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail.
 - b. Enter the e-mail address to which logs and alerts are sent in the **Send To This E-mail Address** field. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by e-mail.
3. If your outgoing e-mail server requires authentication, select the **My Mail Server requires authentication** check box.
 - a. Enter your user name for the outgoing e-mail server in the **User Name** field.
 - b. Enter your password for the outgoing e-mail server in the **Password** field.
4. You can specify that logs are automatically sent by e-mail with these options:
 - **Send alert immediately.** Select this check box for immediate notification of attempted access to a blocked site or service.

- **Send Logs According to this Schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
 - **Day.** Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
 - **Time.** Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.

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

So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Setting the Time

The WNR2000v3 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. To localize the time for your log entries, you must specify your time zone:

- **Time Zone.** Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- **Automatically Adjust for Daylight Savings Time.** Select this check box if your region supports daylight savings time. When this check box is set, the router will adjust the time by adding one hour during the daylight savings time period. When daylight savings time ends, be sure to un-check this check box.

Chapter 4

Using Network Monitoring Tools

This chapter describes features to help you manage your N300 Wireless Router WNR2000v3.

This chapter includes the following sections:

- “Upgrading the Router Firmware”
- “Viewing Wireless Router Status Information” on page 4-5
- “Viewing a List of Attached Devices” on page 4-10
- “Managing the Configuration File” on page 4-11
- “Enabling Remote Management Access” on page 4-13
- “Traffic Meter” on page 4-15

Upgrading the Router Firmware

The routing software (also called firmware) of the WNR2000v3 router is stored in flash memory, and can be upgraded as NETGEAR releases new software. Your router can download and install the new software, or you can download upgrade files from the NETGEAR website and manually send the upgrade file to the router using your browser.



Tip: To ensure that you are always using the latest router firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability.

The Checking for Firmware Updates screen appears at login unless you clear the **Check for Updated Firmware Upon Log-in** check box.

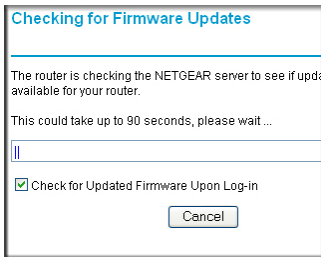


Figure 4-1

A screen is also provided for upgrading the router. From the main menu, under Maintenance, select **Router Upgrade** to display the Router Upgrade screen.

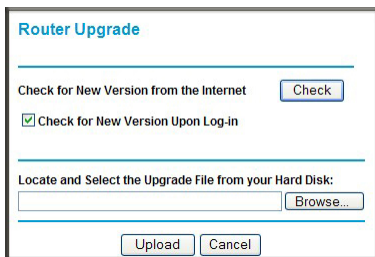


Figure 4-2

From this screen, you can check for new software versions by clicking the **Check** button. If a new version is found, you can download and install it in one step. To enable the Smart Wizard to automatically check for a new software version upon login, select the **Check for New Version Upon Log-in** check box.

Alternatively, you can manually install an upgrade file stored on your computer.



Tip: Before upgrading the router software, use the router Settings Backup screen to save your configuration settings. A router upgrade might cause the router settings to revert to the factory defaults. If this happens, after completing the upgrade, you can restore your settings from the backup.

Upgrading Automatically to New Router Software

If you have selected **Check for New Version Upon Log-in**, your router alerts you to the new software when you log in. Otherwise, you can click the **Check** button in the Router Upgrade screen to search for new software.

If the router discovers a newer version of software, the message on the left displays when you log in. If no new firmware is available, the message on the right displays.

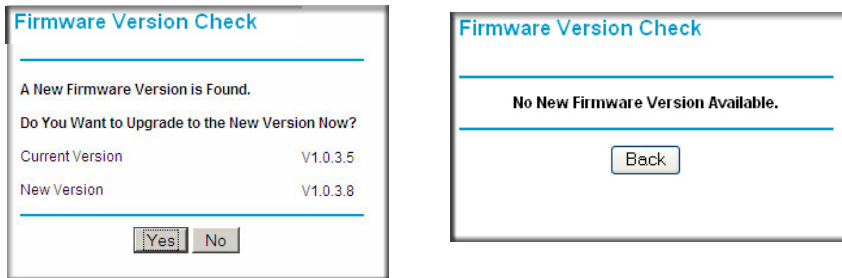



Figure 4-3

To automatically upgrade to the new software, click **Yes** to allow the router to download and install the new software file from NETGEAR.

	<p>Warning: When uploading software to the WNR2000v3 router, <i>do not</i> 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 software.</p>
---	--

When the upload is complete, your router automatically restarts. The upgrade process typically takes about three minutes. Read the new software release notes to determine whether you must reconfigure the router after upgrading.

Upgrading Manually to New Router Software

To manually select, download, and install new software to your router:

1. Under Maintenance on the main menu, select **Router Status**. Note the version number of your router firmware.
2. Go to the WNR2000v3 support page on the NETGEAR website at <http://www.netgear.com/support>.
3. Check the most recent firmware version offered against the firmware version shown in the Router Status screen.

4. If the version on the NETGEAR website is more recent, download the file to your computer.
5. Under Maintenance on the main menu, select **Router Upgrade**.
6. Click **Browse**, and locate the firmware image that you downloaded to your PC (the file ends in .img or .chk).
7. Click **Upload** to send the firmware to the router.



Warning: When uploading software to the WNR2000v3 router, *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 software.

When the upload is complete, your router automatically restarts. The upgrade process typically takes about three minutes. Read the new software release notes to determine whether you must reconfigure the router after upgrading.

Viewing Wireless Router Status Information

To view router status and usage information, from the main menu, under the Maintenance heading, select **Router Status**. The Router Status screen displays.

Router Status	
Hardware Version	WNDR3700
Firmware Version	V1.0.4.26NA
GUI Language Version	V1.0.0.1
Internet Port	
MAC Address	00:22:3F:8C:F8:C1
IP Address	10.1.10.150
DHCP	DHCPClient
IP Subnet Mask	255.255.255.0
Domain Name Server	10.1.1.6 10.1.1.7
LAN Port	
MAC Address	00:22:3F:8C:F8:C0
IP Address	192.168.1.1
DHCP	On
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Settings a/n	
Name (SSID)	NETGEAR-5G
Region	United States
Channel	36(P)+40(S)
Mode	Up to 300 Mbps
Wireless AP	On
Broadcast Name	On
Wireless Settings b/g/n	
Name (SSID)	NETGEAR
Region	United States
Channel	Auto (9)
Mode	Up to 130 Mbps
Wireless AP	On
Broadcast Name	On
Wi-Fi Protected Setup b/g/n	Not Configured
Wi-Fi Protected Setup a/n	Not Configured
<input type="button" value="Show Statistics"/> <input type="button" value="Connection Status"/>	

Figure 4-4

You can use the Show Statistics and Connection Status buttons to view additional status information, as described in “[Connection Status](#)” on page 4-8 and “[Statistics](#)” on page 4-9. The following table explains Router Status screen fields.

Table 4-1. Wireless Router Status Fields

Field		Description
Hardware Version		The router model.
Firmware Version		The version of the router firmware. It changes if you upgrade the router.
GUI Language Version		The localized language of the GUI.
Internet Port	MAC Address	The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the router.
	IP Address	The IP address being used by the Internet (WAN) port of the router. If no address is shown, or is 0.0.0.0, the router cannot connect to the Internet.
	DHCP	<ul style="list-style-type: none"> • None. The router uses a fixed IP address on the WAN. • DHCP Client. The router obtains an IP address dynamically from the ISP.
	IP Subnet Mask	The IP subnet mask being used by the Internet (WAN) port of the router. For an explanation of subnet masks and subnet addressing, click the link to the online document “ TCP/IP Networking Basics ” in Appendix B .
	Domain Name Server	The Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Table 4-1. Wireless Router Status Fields (continued)

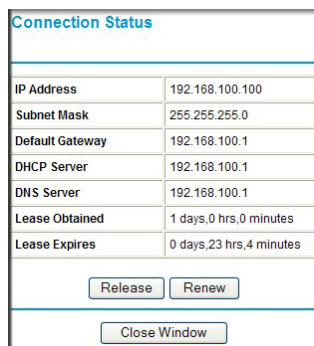
Field		Description
LAN Port	MAC Address	The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the router.
	IP Address	The IP address being used by the Ethernet (LAN) port of the router. The default is 192.168.1.1.
	DHCP	Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.
	IP Subnet Mask	The IP subnet mask being used by the Ethernet (LAN) port of the router. The default is 255.255.255.0.
Wireless Port	Wireless Settings a/n	Name (SSID): The wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
		Region: The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.
		Channel: Identifies the operating channel of the wireless port being used. The default channel is 36. If there is an Auto option in the channel list and you select it, the router will find the best operating channel available. If you notice interference from nearby devices, you can select a different channel.
		Mode: Indicates the wireless communication mode: <ul style="list-style-type: none"> • Up to 54Mbps • Up to 130Mbps • Up to 300Mbps (default)
		Wireless AP: Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless light on the front panel is off.
		Broadcast Name: Indicates whether the router is broadcasting its SSID.

Table 4-1. Wireless Router Status Fields (continued)

Field		Description
Wireless Settings b/g/n		Name (SSID): The 11N wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
		Region: The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.
		Channel: Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the router will find the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 will not interfere with each other.
		Mode: Indicates the wireless communication mode: <ul style="list-style-type: none"> • Up to 54Mbps • Up to 130Mbps (default) • Up to 300Mbps
		Wireless AP: Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless light on the front panel is off.
	Broadcast Name: Indicates whether the router is broadcasting its SSID.	
Wi-Fi Protected Setup b/g/n		Indicates whether Wi-Fi Protected Setup is configured for the b/g/n network.
Wi-Fi Protected Setup a/n		Indicates whether Wi-Fi Protected Setup is configured for the a/n network.

Connection Status

To view the connection status, on the Router Status screen, click **Connection Status**.



Connection Status	
IP Address	192.168.100.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DHCP Server	192.168.100.1
DNS Server	192.168.100.1
Lease Obtained	1 days, 0 hrs, 0 minutes
Lease Expires	0 days, 23 hrs, 4 minutes
<input type="button" value="Release"/> <input type="button" value="Renew"/>	
<input type="button" value="Close Window"/>	

Figure 4-5

The following table describes the connection status settings.

Table 4-2. Connection Status Settings

Item	Description
IP Address	The IP address that is assigned to the router.
Subnet Mask	The subnet mask that is assigned to the router.
Default Gateway	The IP address for the default gateway that the router communicates with.
DHCP Server	The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
DNS Server	The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
Lease Obtained	The date and time that the lease was obtained.
Lease Expires	The date and time that the lease will expire.

- Click the **Release** button to release the connection status items (that is, all items return to 0).
- Click the **Renew** button to renew to the connection status items (that is, all items are refreshed).
- Click the **Close Window** button to close the Connection Status screen.

Statistics

To view statistics, on the Router Status screen, click **Show Statistics**.

System Up Time 05:26:19							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	1000M/Full	5126	43441	0	26	474	05:25:22
LAN 1	1000M/Full	12144	13557	0	542	65	05:24:56
LAN 2	Link down						00:00:00
LAN 3	Link down						00:00:00
LAN 4	Link down						00:00:00
WLAN	130M	3580	5522	0	129	21	05:26:19

Poll Interval (secs)

Figure 4-6

The following table describes the router statistics.

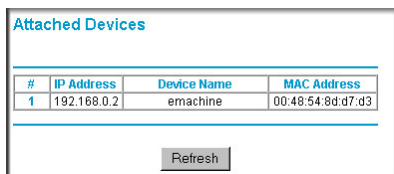
Table 4-3. Router Statistics

Item	Description
System Up Time	The time elapsed since the router was last restarted.
Port	The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	The intervals at which the statistics are updated in this screen.

- To change the polling frequency, enter a time in seconds in the **Poll Interval** field, and click **Set Interval**.
- To stop the polling entirely, click **Stop**.

Viewing a List of Attached Devices

The Attached Devices table lists all IP devices that the router has discovered on the local network. From the main menu, under Maintenance, select **Attached Devices** to view the table.



#	IP Address	Device Name	MAC Address
1	192.168.0.2	emachine	00:48:54:8d:d7:d3

Refresh

Figure 4-7

For each device, the table shows the IP address, NetBIOS host name or device name (if available), and the Ethernet MAC address. To force the router to look for attached devices, click **Refresh**.



Note: If the router is rebooted, the table data is lost until the router rediscovers the devices.

Managing the Configuration File

The configuration settings of the WNR2000v3 router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings. From the main menu, under Maintenance, select Backup Settings.

The screenshot shows the 'Backup Settings' page with three main sections:

- Save a Copy of Current Settings:** A 'Backup' button.
- Restore Saved Settings from a File:** A text input field, a 'Browse...' button, and a 'Restore' button.
- Revert to Factory Default Settings:** An 'Erase' button.

Figure 4-8

The following sections describe the available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Backup Settings screen let you save and retrieve a file containing your router's configuration settings.

To save your settings, click **Back Up**. Your browser extracts the configuration file from the router and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as comcast.cfg.



Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

To restore your settings from a saved configuration file, enter the full path to the file on your computer, or click **Browse** to browse to the file. When you have located it, click **Restore** to send the file to the router. The router then reboots automatically.



Warning: Do not interrupt the reboot process.

Erasing the Configuration

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings. After an erase, the router's user name is **admin**, the password is **password**, the LAN IP address is **192.168.1.1** (or **www.routerlogin.net**), and its DHCP server is enabled.

- To erase the configuration, click the **Erase** button in the Backup Settings screen.
- To restore the factory default configuration settings when you do not know the login password or IP address, you must use the restore factory settings button on the bottom of the router (see [“Restoring the Default Configuration and Password”](#) on page 7-14).

Enabling Remote Management Access

The remote management feature allows you to upgrade or check the status of your WNR2000v3 router via the Internet. From the main menu, under Advanced, select **Remote Management**.

Figure 4-9



Note: Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for remote management:

1. Select the **Turn Remote Management On** check box.
2. Under Allow Remote Access By, specify what external IP addresses will be allowed to access the router's remote management.



Note: For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from any IP address on the Internet, select **Everyone**.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.

3. Specify the port number for accessing the management interface.

Normal Web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

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



Note: When accessing your router from the Internet, type your router's WAN IP address into your browser's address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter **http://134.177.0.123:8080** in your browser.

Traffic Meter

Traffic Metering allows you to monitor the volume of Internet traffic passing through your router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

To monitor traffic on your router, do the following:

1. On the Advanced menu, click **Traffic Meter**.

Traffic Meter

Internet Traffic Meter

Enable Traffic Meter

Traffic volume control by No limit

Monthly Limit Mbytes

Round up data volume for each connection by Mbytes

Connection time control

Monthly Limit hours

Traffic Counter

Restart traffic counter at : am On the day of each month

Traffic Control

Pop up a warning message

Mbytes/Minutes before the monthly limit is reached

When the monthly limit is reached

Turn the Internet LED to flashing green/amber

Disconnect and disable the Internet connection

Internet Traffic Statistics

start date / time: Wed Dec 31 16:00:00 1969

Current(s) Date / Time: Fri Dec 31 16:00:36 2009

Remaining data volume: 0 Bytes

Counting Period	Connection Time (hh:mm)	Traffic Volume (Mbytes)		
		Upload/Avg	Download/Avg	Total/Avg
Today	0.0	0.00	0.00	0.00
Yesterday	0.0	0.00	0.00	0.00
This week	0.0	0.00/0.00	0.00/0.00	0.00/0.00
This month	0.0	0.00/0.00	0.00/0.00	0.00/0.00
Last month	0.0	0.00/0.00	0.00/0.00	0.00/0.00

Figure 4-10

2. To enable the Traffic Meter, click the **Enable Traffic Meter** check box.

3. If you would like to record and restrict the volume of Internet traffic, click the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
 - No Limit – No restriction is applied when the traffic limit is reached.
 - Download only – The restriction is applied to incoming traffic only.
 - Both Directions – The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month:
 - By specifying how many Mbytes per month are allowed.
 - By specifying how many hours of traffic are allowed.
5. Set the **Traffic Counter** to begin at a specific time and date.
6. Set up **Traffic Control** to issue a warning message before the month limit of Mbytes or Hours is reached. You can select one of the following to occur when the limit is attained:
 - The Internet LED flashes green or amber.
 - The Internet connection is disconnected and disabled.
7. Set up **Internet Traffic Statistics** to monitor the data traffic.
8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.
9. Click **Apply** to save your settings.

Chapter 5

Customizing Your Network Settings

This chapter describes advanced features of the N300 Wireless Router WNR2000v3. This chapter includes the following sections:

- “Using the LAN Setup Options”
- “Using a Dynamic DNS Service” on page 5-5
- “Configuring the WAN Setup Options” on page 5-7
- “Configuring Static Routes” on page 5-9
- “Allowing Inbound Connections to Your Network” on page 5-11
- “Configuring Port Forwarding to Local Servers” on page 5-16
- “Configuring Port Triggering” on page 5-18
- “Wireless Repeating (Also Called WDS)” on page 5-22

Using the LAN Setup Options

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The router’s default LAN IP configuration is:

- LAN IP address: **192.168.1.1**
- Subnet mask: **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and should be suitable for 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.

To configure LAN IP settings, log in to the router, and under the Advanced heading, select **LAN Setup**. The following screen displays:

Figure 5-1

If you make changes you must click **Apply** in order for the changes to take effect.



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

The LAN Setup fields are explained in the following table.

Table 5-1. LAN Setup

Settings	Description
Device Name	A descriptive name for the router, which will be shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The Device Name field cannot be blank.

Table 5-1. LAN Setup

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the wireless router.
	IP Subnet Mask	The LAN subnet mask of the wireless router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or wireless router.
	RIP Direction	RIP (Router Information Protocol) allows a wireless router to exchange routing information with other routers. This setting controls how the wireless router sends and receives RIP packets. Both is the default. <ul style="list-style-type: none"> • Both or Out Only. The wireless router broadcasts its routing table periodically. • Both or In Only. The wireless router incorporates the RIP information that it receives.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the wireless router sends. It recognizes both formats when receiving. By default, the RIP function is disabled. <ul style="list-style-type: none"> • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information	Use Router as a DHCP Server	This check box is usually selected so that the wireless router functions as a Dynamic Host Configuration Protocol (DHCP) server. See “Using the Router as a DHCP Server” on page 5-4 .
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the wireless router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the wireless router.
Address Reservation For more information, see “Address Reservation” on page 5-4 .		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the router’s DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Using the Router as a DHCP Server

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

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

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

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

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

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

Address Reservation

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

To reserve an IP address:

1. Click **Add**.

2. In the **IP Address** field, type the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as **192.168.1.x**.)
3. Type the MAC address of the computer or server.



Tip: If the computer is already present on your network, you can 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 router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

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

Using a Dynamic DNS Service

If your Internet Service Provider (ISP) gave you 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 will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service, which allows you to register your domain to their IP address, and forwards traffic directed at your domain to your frequently changing IP address.

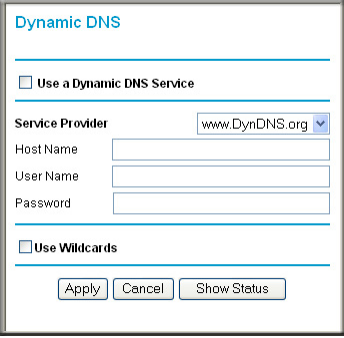


Note: If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service will not work because private addresses are not routed on the Internet.

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. You must first visit their website at www.dyndns.org and obtain an account and host name, which you configure in the router. Then, whenever your ISP-assigned IP address changes,

your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at hostname.dyndns.org.

From the main menu, under Advanced, select **Dynamic DNS** to display the Dynamic DNS screen.



Dynamic DNS

Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name:

User Name:

Password:

Use Wildcards

Apply Cancel Show Status

Figure 5-2

To configure Dynamic DNS:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the **Service Provider** list. For example, for DynDNS.org, select **www.dyndns.org**.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your Dynamic DNS service provider.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. 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.
8. Click **Apply** to save your configuration.

Configuring the WAN Setup Options

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the wireless router to respond to a ping on the WAN (Internet) port. From the main menu, under Advanced, click **WAN Setup** to view the WAN Setup screen.

Figure 5-3

The WAN Setup fields are described in the following table:

Table 5-2. WAN Setup Settings

Setting	Description
Disable SPI Firewall	The Stateful Packet Inspection (SPI) firewall protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The firewall should be disabled only in special circumstances, such as when you are troubleshooting application issues.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, Configuring Static Routes .
Respond to Ping on Internet Port	If you want the wireless router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your wireless router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. See “Changing the MTU Size” on page 6-6.

Table 5-2. WAN Setup Settings

Setting	Description
NAT Filtering	Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.
Disable SIP ALG	Select this feature if you have a SIP (Session Initiation Protocol) telephone or other SIP base devices, and you want them to communicate with other people. If you have been unable to build a successful SIP connection, selecting this check box allows for such a connection without compromising other SIP ALG (Application-level gateway) firewall settings, such as Disable SPI Firewall. If you are not using SIP devices, leave this check box unchecked.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router 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.



Warning: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

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

The WAN Setup screen lets you configure a default DMZ server.

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

1. Click the **Default DMZ Server** check box.
2. Type the IP address.

3. Click **Apply**.

Configuring Static Routes

Static routes provide additional routing information to your router. Under usual circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

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 router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router 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 must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100.

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 should be forwarded to the ISDN router at 192.168.1.100.
- A **Metric** value of 1 will work since the ISDN router is on the LAN.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

Select **Static Routes** under Advanced in the main menu. The Static Routes screen displays.

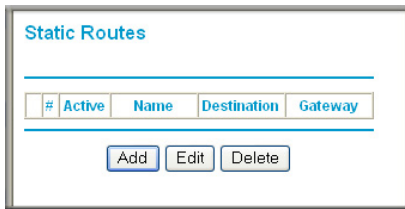


Figure 5-4

To add or edit a static route:

1. Click **Add** to open the Static Routes screen.

 A screenshot of the 'Static Routes' configuration form. The form has the following fields and controls:

- Route Name:** A text input field.
- Private:** A checkbox that is currently unchecked.
- Active:** A checkbox that is currently checked.
- Destination IP Address:** A dotted IP address input field.
- IP Subnet Mask:** A dotted IP address input field.
- Gateway IP Address:** A dotted IP address input field.
- Metric:** A numeric input field.

 At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

Figure 5-5

2. In the **Route Name** field, type a name for this static route. (This is for identification purposes only.)
3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
4. Select the **Active** check box to make this route effective.
5. Type the destination IP address of the final destination.
6. Type the IP subnet mask for this destination.
If the destination is a single host, type 255.255.255.255.
7. Type the gateway IP address, which must be a router on the same LAN segment as the WNR2000v3 router.

8. Type a number between 1 and 15 as the metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to have the static route entered into the table.

Allowing Inbound Connections to Your Network

By default, the WNR2000v3 router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you might need to create exceptions to this rule for the following purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. This section explains how a normal outbound connection works, followed by two examples explaining how port forwarding and port triggering operate and how they differ.

How Your Computer Accesses a Remote Computer through Your Router

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must 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 Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.
2. You ask your browser to get a Web page from the Web server at www.example.com. Your computer composes a Web page request message with the following address and port information:
 - The source address is your computer's IP address.
 - The source port number is 5678, the browser session.

- The destination address is the IP address of `www.example.com`, which your computer finds by asking a DNS server.
- The destination port number is 80, the standard port number for a Web 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 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 source address is the IP address of `www.example.com`.
 - The source port number is 80, the standard port number for a Web server process.
 - The destination address is the public IP address of your router.
 - The destination port number is 33333.

The Web server then sends this reply message to your router.

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, restoring the original address information replaced by NAT. The message now contains the following address and port information:
 - The source address is the IP address of `www.example.com`.
 - The source port number is 80, the standard port number for a Web server process.
 - The destination address is your computer's IP address.
 - The destination port number is 5678, the browser session that made the initial request.

Your router then sends this reply message to your computer, which displays the Web page from www.example.com.

6. When you finish your browser session, your router eventually senses 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.

How Port Triggering Changes the Communication Process

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 will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering 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. Using port triggering, you can tell the router, “When you initiate a session with destination port 6667, you must 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 port triggering rule you have defined:

1. You open an IRC client program, beginning 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 port triggering 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 (as in the previous example, let’s say 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 port triggering, 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 user groups or newsgroups.



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

How Port Forwarding Changes the Communication Process

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 port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from our 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. Using port forwarding, 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 port forwarding rule you have defined:

1. The user of a remote computer opens Internet Explorer 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:

- The destination address is the IP address of `www.example.com`, which is the address of your router.
- The destination port number is 80, the standard port number for a Web server process.

The remote computer then 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 port forwarding 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 port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or user groups or newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

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

Configuring Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might make a local Web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. The DMZ server is configured in the WAN Setup screen, as discussed in [“Setting Up a Default DMZ Server” on page 5-8](#).

Before starting, you need to determine which type of service, application, or game you will provide, and the local IP address of the computer that will provide the service. Be sure the computer’s IP address never changes.



Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your WNR2000v3 router. See [“Address Reservation” on page 5-4](#) for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu.

Port Forwarding / Port Triggering

Please select the service type.

Port Forwarding
 Port Triggering

Service Name: FTP Server IP Address: 192.168.1. Add

#	Server Name	Start Port	End Port	Server IP Address

Edit Service Delete Service

Add Custom Service

Figure 5-6

2. Select the **Port Forwarding** radio button as the Service type.

3. From the **Service Name** list, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, “[Adding a Custom Service](#).”
4. In the corresponding **Server IP Address** box, enter the last digit of the IP address of your local computer that will provide this service.
5. Click **Add**. The service appears in the list in the screen.

Adding a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you must first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups. When you have the port number information, follow these steps:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu.
2. Select the **Port Forwarding** radio button as the Service type.
3. Click **Add Custom Service**.

Figure 5-7

4. In the **Service Name** field, enter a descriptive name.
5. In the **Protocol** field, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the **Starting Port** field, enter the beginning port number.
 - If the application uses only a single port, enter the same port number in the **Ending Port** field.

- If the application uses a range of ports, enter the ending port number of the range in the **Ending Port** field.
7. In the **Server IP Address** field, enter the IP address of your local computer that will provide this service.
 8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Editing or Deleting a Port Forwarding Entry

To edit or delete a port forwarding entry:

1. In the table, select the button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a Web server on your local network, you can use port forwarding to allow Web requests from anyone on the Internet to reach your Web server.

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP address reservation, as explained in [“Address Reservation” on page 5-4](#). In this example, your router will always give your Web server an IP address of 192.168.1.33.
2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your Web server at **192.168.1.33**.
HTTP (port 80) is the standard protocol for Web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in [“Using a Dynamic DNS Service” on page 5-5](#).
To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Configuring Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound “trigger” port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.



Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in [“Universal Plug and Play” on page 6-13](#).

To configure port triggering, 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 user groups or newsgroups.

To set up port triggering:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu. The Forwarding/Port Triggering screen displays.

- Select the **Port Triggering** radio button. The port triggering information displays.

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding
 Port Triggering

Disable Port Triggering

Port Triggering Timeout (in minutes)

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User
<input type="radio"/>	1	<input checked="" type="checkbox"/>	dialpad_1	TCP:51200	TCP/UDP:51200	ANY
<input type="radio"/>	2	<input checked="" type="checkbox"/>	dialpad_2	TCP:51201	TCP/UDP:51201	ANY
<input type="radio"/>	3	<input checked="" type="checkbox"/>	paltalk_1	TCP:2090	TCP/UDP:2090	ANY
<input type="radio"/>	4	<input checked="" type="checkbox"/>	paltalk_2	TCP:2091	TCP/UDP:2091	ANY
<input type="radio"/>	5	<input checked="" type="checkbox"/>	quicktime	TCP:554	TCP/UDP:6970..6990	ANY
<input type="radio"/>	6	<input checked="" type="checkbox"/>	starcraft	TCP:6112	TCP/UDP:6112	ANY

Figure 5-8

- Clear the **Disable Port Triggering** check box.



Note: If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

- In the **Port Triggering Timeout** field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add Service**.

Port Triggering - Services

Service

Service Name

Service User

. . .

Service Type

Triggering Port (1~65535)

Required Inbound Connection

Connection Type

Starting Port (1~65535)

Ending Port (1~65535)

Figure 5-9

6. In the **Service Name** field, type a descriptive service name.
7. In the **Service User** field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
9. In the **Triggering Port** field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
10. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.
11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Wireless Repeating (Also Called WDS)

The WNR2000v3 router can be used with a wireless access point (AP) to build large bridged wireless networks. Wireless repeating is a type of Wireless Distribution System (WDS).



Warning: If you use the wireless repeating function, your options for wireless security are limited to None or WEP. For more information about wireless security, see [Chapter 2, “Safeguarding Your Network.”](#)

The following figure shows a wireless repeating scenario:

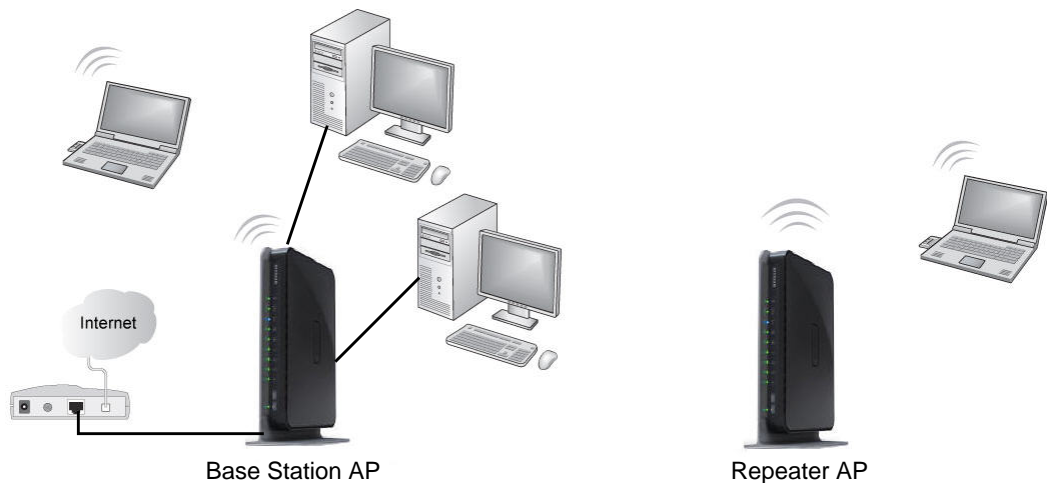


Figure 5-10

To set up a wireless network using WDS, the following conditions must be met for both APs:

- Both APs must use the same SSID, wireless channel, and encryption mode (see [“Manually Configuring Your Wireless Settings”](#) on page 2-4 or [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network”](#) on page 2-13).
- Both APs must be on the same LAN IP subnet. That is, all the AP LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the APs.

Wireless Repeating Function

You can view or change wireless repeater settings for the wireless router. From the main menu of the browser interface, under Advanced, click **Wireless Repeating Function** to display the Wireless Repeating Function screen.

Wireless Repeating Function

Enable Wireless Repeating Function(2.4GHz b/g/n)
Wireless MAC of this router 00:22:3F:8C:F8:C0

Wireless Repeater
Repeater IP Address: 192, 168, 1
 Disable Wireless Client Association
Base Station MAC Address:

Wireless Base Station
 Disable Wireless Client Association
Repeater MAC Address 1:
Repeater MAC Address 2:
Repeater MAC Address 3:
Repeater MAC Address 4:

Enable Wireless Repeating Function(5GHz a/n)
Wireless MAC of this router 00:22:3F:8C:F8:C2

Wireless Repeater
Repeater IP Address: 192, 168, 1
 Disable Wireless Client Association
Base Station MAC Address:

Wireless Base Station
 Disable Wireless Client Association
Repeater MAC Address 1:
Repeater MAC Address 2:
Repeater MAC Address 3:
Repeater MAC Address 4:

Apply Cancel

Figure 5-11

The wireless router supports two modes of the wireless repeating function, and allows you to control wireless client association:

- **Wireless Repeater.** The wireless router sends all traffic from its local wireless or wired computers to a remote AP. To configure this mode, you must know the MAC address of the remote parent AP.
- **Wireless Base Station.** The wireless router acts as the parent AP, bridging traffic to and from the child repeater AP, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater AP.
- **Disable Wireless Client Association.** Usually this check box is cleared so that the router is an access point for wireless computers.

If this check box is selected, the router communicates wirelessly only with other APs whose MAC addresses are listed in this screen. The router still communicates with wire-connected LAN devices.



Note: The WNR2000v3 router is always in dual band concurrent mode, unless you turn off one radio. Be aware that if you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless router or wireless base station, dual band concurrent mode is not affected.

Setting Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy chained. You must know the wireless settings for both units. You must know the MAC address of the remote unit. First, set up the base station, and then set up the repeater. To set up the base station:

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option must be set to **None** or **WEP**.

2. Log into the wireless router base unit, under the Advanced heading, select **Wireless Repeating Function** to display the Wireless Repeating Function screen.

Wireless Repeating Function

Enable Wireless Repeating Function(2.4GHz b/g/n)
Wireless MAC of this router 00:22:3F:8C:F8:C0

Wireless Repeater
Repeater IP Address: 192 | 168 | 1 | 1
 Disable Wireless Client Association
Base Station MAC Address: _____

Wireless Base Station
 Disable Wireless Client Association
Repeater MAC Address 1: _____
Repeater MAC Address 2: _____
Repeater MAC Address 3: _____
Repeater MAC Address 4: _____

Enable Wireless Repeating Function (5GHz a/n)
Wireless MAC of this router 00:22:3F:8C:F8:C2

Wireless Repeater
Repeater IP Address: 192 | 168 | 1 | 1
 Disable Wireless Client Association
Base Station MAC Address: _____

Wireless Base Station
 Disable Wireless Client Association
Repeater MAC Address 1: _____
Repeater MAC Address 2: _____
Repeater MAC Address 3: _____
Repeater MAC Address 4: _____

Apply Cancel

Figure 5-12

3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Setting Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.



Note: If you are using the WNR2000v3 base station with a non-NETGEAR wireless router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

To configure a WNR2000v3 router as a repeater unit:

1. Log in to the router that will be the repeater. Check the Wireless Settings screen, and verify that the wireless settings match the base unit exactly. The wireless security option must be set to **WEP** or **None**.
2. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
3. Fill in the **Repeater IP Address** field. This IP address must be in the same subnet as the base station, but different from the LAN IP of the base station
4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

A computer on any wireless or wired LAN segment of the wireless router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other AP.

Chapter 6

Fine-Tuning Your Network

This chapter describes features to help you manage your N300 Wireless Router WNR2000v3.

This chapter includes the following sections:

- “Assessing Your Speed Requirements” on page 6-2
- “Optimizing Your Network Bandwidth” on page 6-3
- “Optimizing Wireless Performance” on page 6-5
- “Changing the MTU Size” on page 6-6
- “Quality of Service (QoS)” on page 6-7

Common connection types and their speed and security considerations are:

- **Broadband Internet.** Your Internet connection speed is determined by your modem type, such as ADSL or cable modem, as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL and cable modem connections are asymmetrical, meaning they have a lower data rate *to* the Internet (upstream) than *from* the Internet (downstream). Keep in mind that when you connect to another site that also has an asymmetrical connection, the data rate between your sites is limited by each side’s upstream data rate. A typical residential ADSL or cable modem connection provides a downstream throughput of about 1 to 3 megabits per second (Mbps). Newer technologies such as ADSL2+ and Fiber to the Home (FTTH) will increase the connection speed to tens of Mbps.
- **Wireless.** Your N300 Wireless Router WNR2000v3 provides a wireless data throughput of up to 300 Mbps using technology called multiple input, multiple output (MIMO), in which multiple antennas transmit multiple streams of data. The use of multiple antennas also provides excellent range and coverage. With the introduction of the newer WPA and WPA2 encryption and authentication protocols, wireless security is extremely strong.

To get the best performance, use RangeMax adapters, such as the WNDA3100, for your computers. Although the RangeMax router is compatible with older 802.11b and 802.11g adapters, the use of these older wireless technologies in your network can result in lower throughput overall (typically less than 10 Mbps for 802.11b and less than 40 Mbps for 802.11g). In addition, many older wireless products do not support the latest security protocols, WPA and WPA2.

- **Powerline.** For connecting rooms or floors that are blocked by obstructions or are distant vertically, consider networking over your building's AC wiring. NETGEAR's Powerline HD family of products delivers up to 200 Mbps to any outlet, while the older-generation XE family of products delivers 14 Mbps or 85 Mbps. Data transmissions are encrypted for security, and you can configure an individual network password to prevent neighbors from connecting.

The Powerline HD family of products can coexist on the same network with older-generation XE family products or HomePlug 1.0 products, but they are not interoperable with these older products.

- **Wired Ethernet.** As gigabit-speed Ethernet ports (10/100/1000 Mbps) become common on newer computers, wired Ethernet remains a good choice for speed, economy, and security. Gigabit Ethernet can extend up to 100 meters with twisted-pair wiring of CAT-5e or better. A wired connection is not susceptible to interference, and eavesdropping would require a physical connection to your network.



Note: Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

Assessing Your Speed Requirements

Because your Internet connection is likely to operate at a much lower speed than your local network, faster local networking technologies might not improve your Internet experience. However, many emerging home applications require high data rates. For example:

- Streaming HD video requires 10 to 30 Mbps per stream. Because latency and packet loss can disrupt your video, plan to provide at least twice the capacity you need.
- Streaming MP3 audio requires less than 1 Mbps per stream and does not strain most modern networks. Like video, however, streaming audio is also sensitive to latency and packet loss, so a congested network or a noisy link can cause problems.

- Backing up computers over the network has become popular due to the availability of inexpensive mass storage. [Table 6-1](#) shows the time to transfer 1 gigabyte (GB) of data using various networking technologies.

Table 6-1. Theoretical Transfer Time for 1 Gigabyte

Network Connection	Theoretical Raw Transfer Time
Gigabit wired Ethernet	8 seconds
RangeMax NEXT Wireless-N	26 seconds
Powerline HD	40 seconds
100 Mbps wired Ethernet	80 seconds
802.11n wireless	45 seconds
802.11g wireless	150 seconds
802.11b wireless	700 seconds
10 Mbps wired Ethernet	800 seconds
Cable modem (3 Mbps)	2700 seconds
Analog modem (56 kbps)	144,000 seconds (40 hours)

Optimizing Your Network Bandwidth

As your network grows, it might consist of several segments of different networking technologies, each providing different throughput. In planning your network, you should first consider which devices will have the heaviest traffic flow between them. Examples are:

- A media center in one room streaming high-definition video from a server in another room
- A storage device that is used for backing up your computers

Next, consider the throughput of your network devices. Where possible, make the heaviest-traffic connections using higher-speed technologies, with no lower-speed bottlenecks in the path.

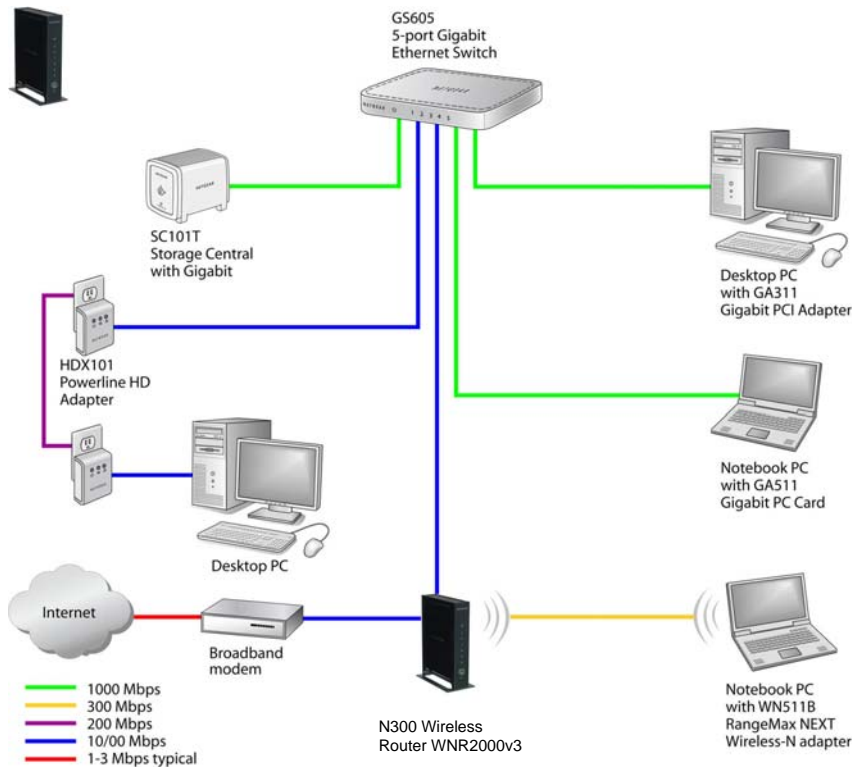


Figure 6-1

Figure 6-1 shows a sample network using multiple networking technologies. In this network, the two PCs with Gigabit (1000 Mbps) Ethernet adapters have a gigabit connection through the GS605 switch to the storage server. This connection should allow for extremely fast backups or quick access to large files on the server. The PC connected through a pair of Powerline HD adapters is limited to the 200 Mbps speed of the Powerline HD connection. Although any of the links in this example would be sufficient for high-traffic applications such as streaming HD video, the use of older devices such as 10 Mbps Ethernet or 802.11b wireless would create a significant bottleneck.

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, click the link to the online document “[Wireless Networking Basics](#)” in Appendix B.

The following list describes how to optimize wireless router performance.

- **Identify critical wireless links.**
If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without loss of connectivity. This also means that devices that are farther away might be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.
- **Choose placement carefully.**
For best results, place your router:
 - Near the center of the area in which your computers will operate.
 - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
 - Avoid obstacles to wireless signals.
 - Keep wireless devices at least 2 feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
 - Keep away from large amounts of water such as fish tanks and water coolers.
- **Reduce interference.**
 - Avoid windows unless communicating between buildings.
 - Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
 - Computers and fax machines (no closer than 1 foot)
 - Copying machines, elevators, and cell phones (no closer than 6 feet)

- Microwave ovens (no closer than 10 feet)
- **Choose your settings.**
 - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.
 - Turn off SSID broadcast, and change the default SSID. Other nearby devices might automatically try to connect to your network several times a second, which can cause significant performance reduction.
- Set WPA2-PSK (AES) security to achieve the best wireless performance and the best security.
- Use WMM to improve the performance of voice and video traffic over the wireless link.

Changing the MTU Size

The Maximum Transmission Unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets must be split or “fragmented” to accommodate the one with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These might require an MTU change:
 - A secure website that won’t open, or displays only part of a Web page
 - Yahoo e-mail
 - MSN
 - America Online’s DSL service
- You use VPN and have severe performance problems.

- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.



Note: An incorrect MTU setting can cause Internet communication problems such as the inability to access certain Web sites, frames within Web sites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. [Table 6-2](#) describes common MTU sizes and applications.

Table 6-2. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you don't have large e-mail attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

To change the MTU size:

- In the main menu, under Advanced, select WAN Setup.
- In the **MTU Size** field, enter a new size between 64 and 1500.
- Click **Apply** to save the new configuration.

Quality of Service (QoS)

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The WNR2000v3 router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays:

QoS Setup

Enable WMM (Wi-Fi multimedia) settings (2.4GHz b/g/n)

Enable WMM (Wi-Fi multimedia) settings (5GHz a/n)

Turn Internet Access QoS On

Turn Bandwidth Control On

Uplink bandwidth Maximum

QoS Priority Rule list

Figure 6-2

Using WMM QoS for Wireless Multimedia Applications

The WNR2000v3 router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen, shown in [Figure 6-2 on page 6-8](#), by clearing the **Enable WMM** check box and clicking **Apply**.

Configuring QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- For specific applications
- For specific online games
- On individual Ethernet LAN ports of the router
- From a specific device by MAC address

To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

To create a QoS policy for applications and online games:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in [Figure 6-2](#) on page 6-8.
2. Click **Setup QoS Rule**. The QoS Setup screen then displays the existing priority rules.

Figure 6-3

3. Click **Add Priority Rule**.

Figure 6-4

4. In the **QoS Policy for** field, type the name of the application or game.
5. In the **Priority Category** list, select either **Applications** or **Online Gaming**. In either case, a list of predefined applications or games displays in the **Applications** drop-down list.

6. From the **Applications** list, you can select an existing item, or you can scroll to the bottom of the list and select **Add a New Application** or **Add a New Game**.
 - a. If you add a new entry, the screen expands as shown:

The screenshot shows a web-based configuration interface for QoS Priority rules. It features a title bar 'QoS - Priority rules' and a form with the following elements:

- Priority**: A text input field for the QoS Policy name.
- Priority Category**: A dropdown menu currently set to 'Applications'.
- Applications**: A dropdown menu currently set to 'Add a new Application'.
- Priority**: A dropdown menu currently set to 'Normal'.
- Specified port range**: A section containing:
 - Connection Type**: A dropdown menu set to 'TCP/UDP'.
 - Starting Port**: A text input field with '(1-65535)' as a hint.
 - Ending Port**: A text input field with '(1-65535)' as a hint.
- Buttons**: 'Apply' and 'Cancel' buttons at the bottom.

Figure 6-5

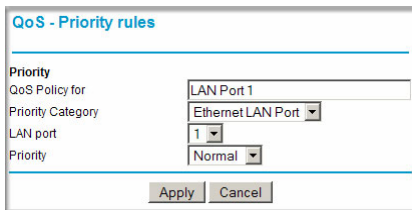
- b. In the **QoS Policy for** field, enter a descriptive name for the new application or game.
 - c. Select the packet type, either **TCP**, **UDP**, or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.
7. From the **Priority** drop-down list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
9. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
10. Click **Apply**.

QoS for a Router LAN Port

To create a QoS policy for a device connected to one of the router's LAN ports:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in [Figure 6-2](#) on [page 6-8](#).
2. Click the **Setup QoS Rule** button.
3. Click **Add Priority Rule**.

- From the **Priority Category** list, select **Ethernet LAN Port**. The QoS - Priority Rules screen changes:



The screenshot shows a web interface titled "QoS - Priority rules". It contains a form with the following fields and values:

- QoS Policy for: LAN Port 1
- Priority Category: Ethernet LAN Port
- LAN port: 1
- Priority: Normal

At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 6-6

- From the **LAN port** list, select the LAN port that will have a QoS policy.
- From the **Priority** drop-down list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
- Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
- In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
- Click **Apply**.

QoS for a MAC Address

To create a QoS policy for traffic from a specific MAC address, follow these steps:

- From the main menu, under Advanced, select **QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays, as shown in [Figure 6-2 on page 6-8](#).
- Click **Add Priority Rule**.

- From the **Priority Category** list, select **MAC Address**. The QoS - Priority Rules screen changes:

QoS - Priority rules

Priority
QoS Policy for
Priority Category: **MAC Address**

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
C	Pri_MAC_59F408	Normal	DELL	00:0D:56:59:F4:08

MAC Address:
Device Name:
Priority: **Normal**

Figure 6-7

- If the device to be prioritized appears in the MAC Device List, select it. The information from the MAC Device List will be used to populate the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you must complete these fields manually.
- From the **Priority** drop-down list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
- Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
- In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
- Click **Apply**.

Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

- From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays, as shown in [Figure 6-2 on page 6-8](#).
- Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:
 - Click **Delete** to remove the QoS policy.
 - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

- Click **Apply** in the QoS Setup screen to save your changes.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to 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.



Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should enable UPnP.

To turn on Universal Plug and Play:

- From the main menu, under Advanced, click **UPnP**. The UPnP screen displays.

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Figure 6-8

- The available settings and information in this screen are:
 - Turn UPnP On.** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.
 - Advertisement Period.** The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period 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 freshness of the device status but can significantly reduce network traffic.

- **Advertisement Time To Live.** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.
 - **UPnP Portmap Table.** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.
3. Click **Apply** to save your settings.

Chapter 7

Troubleshooting

This chapter provides information about troubleshooting your N300 Wireless Router with USB WNR2200. After each problem description, instructions are provided to help you diagnose and solve the problem. As a first step, review the Quick Tips.



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

This chapter includes the following sections:

- “Quick Tips”
- “Troubleshooting Basic Functions” on page 7-3
- “Cannot Access the Internet” on page 7-5
- “Troubleshooting a Network Using the Ping Utility” on page 7-6
- “Problems with Date and Time” on page 7-8
- “Wireless Connectivity” on page 7-9
- “Restoring the Default Configuration and Password” on page 7-14

Quick Tips

This section describes tips for troubleshooting some common problems.

Table 7-1. Quick Tips


Recommendation	Instructions
Be sure to restart your network in this sequence.	<ol style="list-style-type: none"> 1. Turn off <i>and</i> unplug the modem. 2. Turn off the wireless router and computers. 3. Plug in the modem and turn it on. Wait 2 minutes. 4. Turn on the wireless router and wait 2 minutes. 5. Turn on the computers.

Table 7-1. Quick Tips (continued)

Recommendation	Instructions
Make sure that the Ethernet cables are securely plugged in.	<ul style="list-style-type: none"> • The Internet status light on the wireless router is on if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on. • For each powered-on computer connected to the wireless router by an Ethernet cable, the corresponding numbered router LAN port light is on.
Make sure that the wireless settings in the computer and router match exactly.	<ul style="list-style-type: none"> • For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer must match exactly. • If you set up an Access List in the Advanced Wireless Settings screen, you must add each wireless computer's MAC address to the router's access list.
Make sure that the network settings of the computer are correct.	<ul style="list-style-type: none"> • Wired and wirelessly connected computers <i>must</i> have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Click the link to the online document "Preparing Your Network" in Appendix B, or see the documentation that came with your computer. • Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.
Check the Power light to verify correct router operation.	If the Power light does not turn off within 2 minutes after you turn the router on, reset the router according to the instructions in " Restoring the Default Configuration and Password " on page 7-14.

Troubleshooting Basic Functions

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

1. When power is first applied, verify that the Power light  is on.
2. After approximately 2 minutes, verify that:
 - The Power light is solid green.
 - The Internet light is on.
 - A numbered Ethernet port light is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

If any of the above conditions does not occur, see the following table.

Table 7-2. Troubleshooting Basic Functions

Situation	Recommended Action
Power light is off or is blinking.	<ul style="list-style-type: none"> • Make sure that the power cord is properly connected to your router and that the power adapter is properly connected to a functioning power outlet. • Check that you are using the 12V DC, 2.5A power adapter that NETGEAR supplied for this product. • If the Power light alternately blinks green every second, the router software is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact Technical Support at www.netgear.com/support.
Lights never turn off.	<p>When the router is turned on, the lights turns on for about 10 seconds and then turn off. If all the lights stay on, there is a fault within the router.</p> <p>If all lights are still on 1 minute after power up:</p> <ul style="list-style-type: none"> • Cycle the power to see if the router recovers. • Clear the router's configuration to factory defaults as explained in "Restoring the Default Configuration and Password" on page 7-14. <p>If the error persists, you might have a hardware problem and should contact Technical Support at www.netgear.com/support.</p>


Table 7-2. Troubleshooting Basic Functions

Situation	Recommended Action
The Internet or Ethernet port lights are off.	<p>If either the Ethernet port lights or the Internet light does not light when the Ethernet connection is made, check the following:</p> <ul style="list-style-type: none"> • Make sure that the Ethernet cable connections are secure at the router and at the modem or computer. • Make sure that power is turned on to the connected modem or computer. • Be sure that you are using the correct cable: When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.
Wireless light is off.	<p>If the Wireless light does not come on, verify that the Enable Wireless Router Radio check box is selected in the Advanced Wireless Settings screen (see "Restricting Access to Your Router" on page 2-19). Or, you can press the Wi-Fi on/off button on the wireless router to enable the Wireless function. The wireless light will be lit when the Wireless function is turned on.</p>

Cannot Access the Router Main Menu

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

- If you are connecting from a wireless computer, try connecting from a wired computer.
- Check the Ethernet connection between the wired computer and the router. Make sure that the cable connections are secure, and that you are using the correct cable.
- Make sure that your computer's IP address is on the same subnet as the router. For instructions, click the link to the online document ["Preparing Your Network"](#) in Appendix B to configure your computer.

	<p>Note: If your computer's IP address is shown as 169.254.x.x: Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in subnet 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.</p>
---	---

- 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 opening it again, or try a different browser.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the router does not save configuration changes that you have made, check the following:

- When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.
- Click **Refresh** or **Reload** in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet Service Provider (ISP). Unless your ISP provides a fixed IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

To check the WAN IP address:

1. Start your browser, and select an external site such as <http://www.netgear.com>.
2. Access the main menu of the router's configuration at <http://www.routerlogin.net>.
3. Under Maintenance, select **Router Status**.
4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in [Table 7-1 on page 7-1](#).

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your ISP might require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.

- Your ISP might check for your computer's host name.
Assign the computer host name of your ISP account as the account name in the Basic Settings screen.
- Your ISP allows only one Ethernet MAC address to connect to 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 router's MAC address.
 - Configure your router to spoof your computer's MAC address.

If your router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- 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 router's configuration, reboot your computer, and verify the DNS address as described in the online document you can access from [“Preparing Your Network” in Appendix B](#). You can also configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer might not have the router configured as its TCP/IP gateway.
If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address as described in the online document you can access from [“Preparing Your Network” in Appendix B](#).
- You might be running login software that is no longer needed.
If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the Connections tab, and select **Never dial a connection**.

Troubleshooting a Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network by using the ping utility in your computer or workstation.

Testing the LAN Path to Your Router

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

To ping the router from a running Windows PC:

1. From the Windows toolbar, click the Start button, and then select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:
ping www.routerlogin.net
3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
 - For a wired connection, make sure the numbered Ethernet port light is on for the port to which you are connected. If the light is off, follow the instructions in [Table 7-2 on page 7-3](#).
 - Check that the corresponding Link lights are on for your network interface card. If your router and computer are connected to a separate Ethernet switch, make sure the Link lights are on for the switch ports that are connected to your computer and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
 - Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the Start button, and then select **Run**.
2. In the Windows Run window, 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 like those shown in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in the online document you can access from "[Preparing Your Network](#)" in [Appendix B](#).
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) 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 computer, 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 computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer.

Problems with Date and Time

Under Content Filtering in the main menu, select **E-mail** to display a screen that shows the current date and time of day. The WNR2000v3 router 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.
Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
Cause: The router does not adjust for daylight savings time. In the E-mail screen, select the **Adjust for Daylight Savings Time** check box.

Wireless Connectivity

The first steps in solving wireless connection problems are these:

1. Using your wireless card's setup utility program, make sure that your wireless card can find your wireless router.
2. Configure and test with the simplest wireless connection possible, and then add security.

The topics in this section describe these steps.

Using Your Wireless Card Setup Program

When you install a NETGEAR wireless card in your computer, a Smart Wizard utility program is installed that can provide helpful information about your wireless network. You can find this program in your Windows Program menu or as an icon in your system tray. Other wireless card manufacturers might include a similar program.

If you have no specific wireless card setup program installed, you can use the basic setup utility in Windows by following these steps:

1. Open the Windows Control Panel, and double-click **Network Connections**.
2. In the LAN section, double-click **Wireless Network Connection**.

Use the setup program to scan for available wireless networks. Look for a network name (SSID) of NETGEAR or your custom SSID if you have changed it. If your wireless network does not appear, check these conditions:

- Is your router's wireless radio enabled? See ["Restricting Access to Your Router"](#) on page 2-19.
- Is your router's SSID broadcast enabled? See ["Restricting Access to Your Router"](#) on page 2-19.
- Is your router set to a wireless standard that is not supported by your wireless card? Check the Mode setting, as described in ["Manually Configuring Your Wireless Settings"](#) on page 2-4.

If your wireless network appears, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal obstructed by objects between the router and your computer? See [“Wireless Placement and Range Guidelines”](#) on page 2-2.

If your wireless network appears and has good signal strength, configure your wireless card and router for the simplest possible connection, as described in the next section.

Setting Up and Testing Basic Wireless Connectivity



Note: If you use a wireless computer to change wireless settings, you might be disconnected when you click **Apply**. Reconfigure your wireless adapter to match the new settings, or access the wireless router from a wired computer to make any further changes.

Follow these instructions to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Select **Wireless Settings** under Setup in the main menu of the WNR2000v3 router.

The screenshot shows the 'Wireless Settings' page. It is divided into three main sections: 'Region Selection', 'Wireless Network(2.4GHz b/g/n)', and 'Wireless Network(5GHz a/n)'. Each section has its own 'Security Options'.

Region Selection
Region: United States

Wireless Network(2.4GHz b/g/n)
 Enable SSID Broadcast
Name (SSID): NETGEAR
Channel: Auto
Mode: Up to 130 Mbps

Security Options
 None
 WEP
 WPA-PSK (TKIP)
 WPA2-PSK (AES)
 WPA-PSK (TKIP) + WPA2-PSK (AES)
 WPA/WPA2 Enterprise

Wireless Network(5GHz a/n)
 Enable SSID Broadcast
 Enable Video Network
Name (SSID): NETGEAR-5G
Channel: 36
Mode: Up to 300 Mbps

Security Options
 None
 WEP
 WPA-PSK (TKIP)
 WPA2-PSK (AES)
 WPA-PSK (TKIP) + WPA2-PSK (AES)
 WPA/WPA2 Enterprise

Buttons: Apply, Cancel

Figure 7-1

2. Make sure the **Enable SSID Broadcast** check box is selected.

3. For the wireless network name (SSID), use the default name, or choose a suitable descriptive name. In the **Name (SSID)** field, you can enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.



Note: The SSID is case-sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you configure in the N300 Wireless Router with USB WNR2200. If they do not match, you will not get a wireless connection to the WNR2000v3 router.

4. Select the region in which the wireless interface will operate.
5. Set the channel. The default channel is **Auto**.

This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information about the wireless channel frequencies, click the link to the online document “[Wireless Networking Basics](#)” in [Appendix B](#).

6. Set the mode to **Up to 130 Mbps**.
7. For Security Options, select **None**.
8. Click **Apply** to save your changes.



Note: If you are configuring the router from a wireless computer and you change the router’s SSID, channel, or security settings, you will lose your wireless connection when you click **Apply**. You must then change the wireless settings of your computer to match the router’s new settings.

9. Select **Advanced Wireless Settings** under Advanced in the main menu of the WNR2000v3 router.

Advanced Wireless Settings

Advanced Wireless Settings (2.4GHz b/g/n)

Enable Wireless Router Radio

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

Advanced Wireless Settings (5GHz a/n)

Enable Wireless Router Radio

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

WPS Settings

Router's PIN **10000151**

Disable Router's PIN

Keep Existing Wireless Settings (2.4G-hz b/g/n)

Keep Existing Wireless Settings (5GHz a/n)

Wireless Card Access List

Figure 7-2

10. Make sure the **Enable Wireless Router Radio** check box is selected.
11. Click **Setup Access List**.
12. Make sure that the **Turn Access Control On** check box is *not* selected.
13. Configure and test your wireless computer for wireless connectivity.

Program the wireless adapter of your computer to have the same SSID and channel that you configured in the router, and disable encryption. Check that your computer has a wireless link and can obtain an IP address by DHCP from the router.

Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router (for more information about security, see [Chapter 2, “Safeguarding Your Network”](#)).

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see “Erasing the Configuration” on page 4-12).
- Use the Reset button on the bottom of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the restore settings button on the bottom of the router.

1. Press and hold the restore settings button for over 5 seconds until the Power light turns to blinking amber.
2. Release the restore settings button, and wait for the router to reboot.

If the wireless router fails to restart, or the green Power light continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact Technical Support at <http://www.netgear.com/support>.

Appendix A

Default Configuration and Technical Specifications

This appendix provides factory default settings and technical specifications for the N300 Wireless Router with USB WNR2200.

Restoring the Default Factory Configuration Settings

You can restore the factory default configuration settings to reset the router's user name to **admin**, the password to **password**, and the IP address to **www.routerlogin.net**. This procedure erases your current configuration, including your wireless security settings, and restores the factory defaults. When you log in after resetting, the Smart Wizard configuration assistant prompts you to configure these settings.

To restore the factory default configuration settings:

1. Use a sharp object such as a pen or a paper clip to press and hold the restore factory settings button, located on the bottom of the router, for over 5 seconds until the Power light turns to blinking amber.
2. Release the restore factory settings button, and wait for the router to reboot.

The factory default settings are restored so that you can access the router from your Web browser using the factory defaults.

Table A-1. WNDR3700 Router Default Configuration Settings

Feature	Default Setting
Router login	
Router login URL	http://www.routerlogin.net or http://www.routerlogin.com
User name (case-sensitive) printed on product label	admin
Password (case-sensitive) printed on product label	password

Table A-1. WNDR3700 Router Default Configuration Settings (continued)

Feature		Default Setting
Internet connection		
	MAC Address	Use default hardware address
	MTU Size	1500
Local network		
	Router LAN IP address printed on product label (gateway IP address)	192.168.1.1
	Router subnet	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	Time zone Daylight Saving time	Disabled
	Allow a registrar to configure this router	Enabled
Wireless		
	Wireless communication	Enabled
	SSID names	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 130 Mbps
	Data rate	Best
	Output power	Full
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

*. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Table A-1. WNDR3700 Router Specifications

Feature	General
Network Protocol and Standards Compatibility	
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power Adapter	
North America	120V, 60 Hz, input
UK, Australia	240V, 50 Hz, input
Europe	230V, 50 Hz, input
All regions (output)	12V DC @ 2.5A, output
Physical	
Dimensions	1.1" x 6.89" x 4.68" (28 x 175 x 119 mm)
Weight	1.2 lbs. (0.5 kg)
Environmental	
Operating temperature	0° to 40° C (32° to 104° F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B C-Tick N10947

Table A-1. WNDR3700 Router Specifications (continued)

Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx
	WAN	10BASE-T or 100BASE-Tx
	Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for this table.
	Radio data rates	Auto Rate Sensing
	Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz
	Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
	Operating frequency ranges 2.4 Ghz	2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI)
	802.11 security	40-bit (also called 64-bit) and 128-bit WEP, WPA-PSK, WPA2-PSK, and WPA/WPA2 Enterprise.

Appendix B Related Documents

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

Document	Link
TCP/IP Networking Basics	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Networking Basics	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing Your Network	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking Basics	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

In addition, you can find initial setup instructions for your wireless router in the *NETGEAR Wireless Router Setup Manual*.

A

- access
 - blocking 3-4
 - remote 4-13
 - restricting by MAC address 3-2
 - viewing logs 3-8
- access control
 - turning off 7-13
- access points 5-22
- accessing remote computer 5-11
- adding
 - custom service 5-17
 - priority rules 6-9
- address reservation 5-4
- advertisement period 6-13
- applications
 - QoS for 6-9
- attached devices 4-10
- authentication, required by mail server 3-10
- autogenerated IP addresses 7-4
- automatic software upgrade 4-3

B

- backing up configuration file 4-11
- backing up, transfer time 6-3
- bandwidth, optimizing 6-3
- base station, setting up 5-24
- Basic Settings screen 1-7
- basic wireless connectivity 7-10
- blocking
 - access 3-4
 - inbound traffic 5-11

- bold text *xi*
- broadband Internet 6-1

C

- cables, checking 7-2
- compatibility, protocol and standards A-3
- configuration file 4-11
 - backing up 4-11
 - erasing 4-12
- configuring
 - DMZ server 5-8
 - dynamic DNS 5-6
 - NAT 5-8
 - port forwarding 5-16
 - port triggering 5-18
 - QoS 6-8
 - repeater unit 5-26
 - user-defined services 3-7
- connection status settings 4-9
- connection types 6-1
- crossover cable 7-4
- CTS/RTS Threshold 2-20
- custom service (port forwarding) 5-17
- customer support *ii*

D

- data packets, fragmented 6-6
- date and time, troubleshooting 7-8
- daylight savings time 3-11, 7-9
- default DMZ server 5-8
- default factory settings
 - listed A-1
 - restoring 4-12, 7-14, A-1

default gateway 4-9
deleting configuration 4-12
device name 4-11
DHCP server 4-9, 5-4
DHCP setting 4-6
Disable SIP ALG 5-8
disabling
 firewall 5-7
 wireless client association 5-23
DMZ server 5-8
DNS addresses
 troubleshooting 7-6
DNS server
 primary 1-9
 secondary 1-9
DNS servers 5-12
documents, reference B-1
Domain Name Server (DNS) addresses 4-6
dynamic DNS 5-5
DynDNS.org 5-5

E

electromagnetic emissions A-3
e-mailing logs 3-9
environmental specifications A-3
erasing configuration 4-12
Ethernet cables, checking 7-2
Ethernet light, troubleshooting and 7-3, 7-4
Ethernet MAC address. *See* MAC addresses

F

factory default settings
 listed A-1
 restoring 4-12, 7-14, A-1
firewalls
 default settings A-2
 disabling 5-7
Firmware Upgrade Assistant 1-3, 4-1
firmware version 4-6

fixed font text *xi*
Fragmentation Threshold 2-20
fragmented data packets 6-6

G

games, online, QoS for 6-9
general specifications A-3
Gigabit Ethernet 6-2

H

host name 1-8, 4-11

I

inbound connections 5-11
inbound traffic, allowing or blocking 5-11
Interface specifications A-3
interference, reducing 6-5
Internet connection
 default settings A-2
 troubleshooting 7-5
Internet light, troubleshooting and 7-3, 7-4
Internet port, status 4-6
Internet Relay Chat (IRC) 5-13
Internet services, blocking access 3-5
interval, poll 4-10
IP addresses
 autogenerated 7-4
 current 4-6
 dynamic 5-5
 reserved 5-4
IP subnet mask 4-6
italic text *xi*

K

keywords, blocking by 3-4

L

- LAN path, troubleshooting 7-7
- LAN port
 - QoS for 6-10
 - settings 4-7
- LAN setup 5-1, 5-2
 - default LAN IP configuration 5-1
 - LAN IP 5-2
- language, screen display 1-4
- lease, DHCP 4-9
- LEDs. *See* lights, troubleshooting and
- local network, default settings A-2
- local servers, port forwarding to 5-16
- logging in 1-2
- logging out 1-4
- login settings A-1
- logs
 - sending 3-9
 - time-stamping entries 3-11
 - viewing 3-8

M

- MAC address
 - location of 3-4
 - restricting access by 3-2
 - spoofing 1-9
- MAC addresses
 - attached devices 4-11
 - current 4-6
 - QoS for 6-11
 - troubleshooting 7-8
- mail server, outgoing 3-10
- managing router remotely 4-13
- manual software upgrade 4-3
- metric value 5-11
- MTU size 6-6
- multicasting 5-3
- multiple input, multiple output (MIMO) 6-1

N

- NAT (Network Address Translation) 5-8, 5-12
 - network
 - correct settings, checking 7-2
 - restarting 7-2
- Network Time Protocol (NTP) 3-11, 7-8

O

- obstructions, connecting through 6-2
- online gaming, QoS for 6-9
- optimizing bandwidth 6-3
- optimizing performance 6-5
- outgoing mail server 3-10

P

- packets, fragmented 6-6
- password
 - restoring 7-14
- path, testing 7-8
- performance, optimizing 6-5
- physical specifications A-3
- ping 7-6
- placement, router 6-5
- poll interval 4-10
- port filtering 3-5
- port forwarding 5-14, 5-15, 5-16
 - configuring 5-16
 - example 5-14
- port numbers 3-5
- port status 4-10
- port triggering 5-13, 5-15, 5-18
 - configuring 5-18
 - example 5-13
- power adapter specifications A-3
- Power light, troubleshooting and 7-3
- Powerline HD products 6-2
- PPPoE (PPP over Ethernet) 1-8, 7-5

Preamble mode [2-20](#)
primary DNS server [1-9](#)
prioritizing traffic [6-7](#)
product and publication details [vii](#)
protocols, compatibility [A-3](#)

Q

QoS (Quality of Service) [6-7](#)

R

radio, wireless [2-20](#)
range, router [6-5](#)
reducing interference [6-5](#)
reference documents [B-1](#)
releasing connection status [4-9](#)
remote devices, testing path [7-8](#)
remote management [4-13](#)
renewing connection status [4-9](#)
repeater units [5-26](#)
requirements, speed [6-2](#)
reserved IP addresses [5-4](#)
restarting network [7-2](#)
restoring
 configuration [4-11](#)
 default factory settings [4-12, 7-14, A-1](#)
Restrict Wireless Access by MAC Address [2-11](#)
RIP (Router Information Protocol) [5-3](#)
router status, viewing [4-5](#)

S

sample network, figure [6-4](#)
screen display language [1-4](#)
 selecting [1-4](#)
service numbers [3-7](#)
services, blocking [3-5](#)
setting time [3-11](#)
settings, default. *See* default factory settings

SMTP server [3-10](#)
software, upgrading [4-1](#)
specifications
 general [A-3](#)
 technical [A-1](#)
speed requirements [6-2](#)
SPI (Stateful Packet Inspection) firewall [5-7](#)
SSID [7-12](#)
SSID broadcast [7-13](#)
standards, compatibility [A-3](#)
static routes [5-9](#)
status, router, viewing [4-5](#)
streaming video and audio [6-2](#)
subnet mask [4-6](#)
system up time [4-10](#)

T

TCP/IP network, troubleshooting [7-6](#)
technical specifications [A-1](#)
testing wireless connections [7-10](#)
time of day, troubleshooting [7-8](#)
time to live, advertisement [6-14](#)
time, setting [3-11](#)
time-out
 port triggering [5-20](#)
trademarks [ii](#)
traffic metering [4-15](#)
troubleshooting [7-1](#)
trusted user [3-5](#)
typographical conventions [xi](#)

U

Universal Plug and Play (UPnP) [6-13](#)
up time, system [4-10](#)
updating firmware [1-3](#)
upgrading router software [4-1](#)
URLs, typography for [xi](#)
user-defined services [3-7](#)

V

- viewing
 - attached devices [4-10](#)
 - logs [3-8](#)
 - router status [4-5](#)

W

- WAN IP address, troubleshooting [7-5](#)
- WAN setup [5-7](#)
- WDS [5-23](#)
- WDS (see Wireless Repeating) [5-22](#)
- Web Configuration Interface, troubleshooting [7-4](#)
- WEP, configuring [2-9](#)
- wireless
 - manually configuring settings [2-4](#)
 - range and interference [2-2](#)
- wireless card, setting up [7-9](#)
- wireless connection type [6-1](#)
- wireless connection, troubleshooting [7-9](#)
- Wireless Distribution System (WDS) [5-22](#)
- Wireless light, troubleshooting and [7-4](#)
- wireless network name [7-12](#)
- Wireless port settings [4-7](#)
- wireless radio [2-20, 7-13](#)
- Wireless Repeating [5-22](#)
- wireless repeating [5-22, 5-23](#)
 - base station [5-24](#)
 - repeater unit [5-26](#)
- wireless repeating function [5-22, 5-23](#)
- wireless security [2-16](#)
- wireless settings
 - checking for correct [7-2](#)
 - default, listed [A-2](#)
 - testing [7-10](#)
- WMM (Wi-Fi Multimedia) [6-8](#)
- WPA, configuring [2-11](#)