on networks™
Easy, Reliable & Secure

N300 WiFi Router (N300R)

User Manual

August 2012
202-11001-01
v1.0

Trademarks

Brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice.

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

This symbol is placed in accordance with the European Union Directive 2002/96 on the Waste Electrical and Electronic Equipment (the WEEE Directive). If disposed of within the European Union, this product should be treated and recycled in accordance with the laws of your jurisdiction implementing the WEEE Directive.

Contents

Chapter 1 Hardware Setup

Chapter 2 Getting Started

Chapter 3 Router Setup

Chapter 4 Security Settings

Chapter 5 Network Management

Chapter 6 Advanced Settings

Chapter 7 Troubleshooting

Appendix A Supplemental Information

Appendix B Notification of Compliance

Index

1. Hardware Setup

1

Getting to know your router

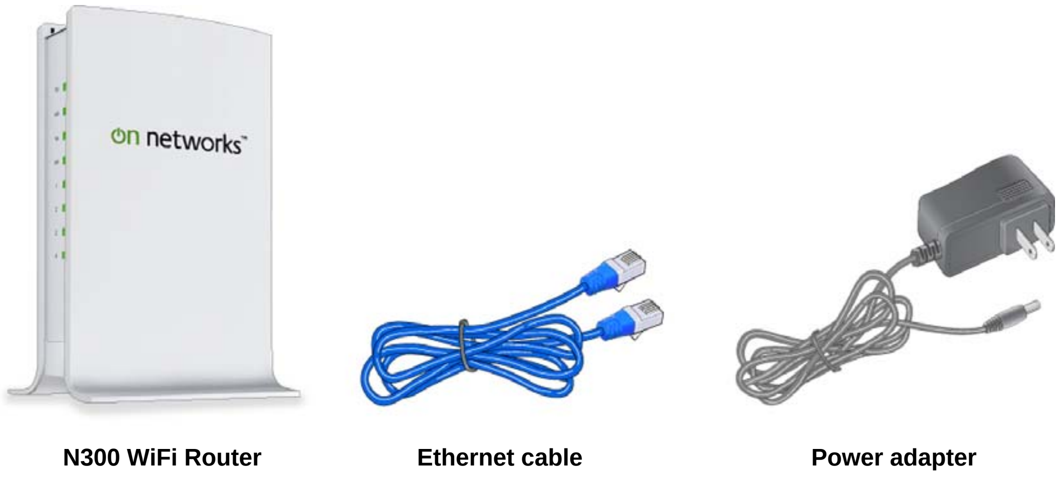
This chapter explains how to set up your hardware. If you have already set up your N300R router, you can skip this chapter. Chapter 2 explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Router*
- *Position Your Router*
- *Hardware Features*

Unpack Your Router

Open the box and remove the router, cables, and installation guide.



N300 WiFi Router

Ethernet cable

Power adapter

Figure 1. Check the package contents

Your box contains the following items:

- N300 WiFi Router (N300R)
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and router setup instructions

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

Position Your Router

The router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your router:

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.

- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, PCs, the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

When you use 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).

Hardware Features

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

Front Panel

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

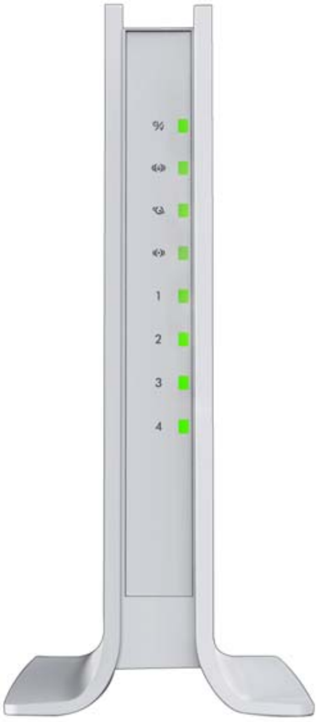


Figure 2. Router front view

Table 1. Front panel LED descriptions

LED	Description
Power/ Check	• **Solid green**. Power is supplied to the router. • **Blinking green**. The router is starting up. • **Off**. Power is not supplied to the router.
Wireless	• **Blinking green**. Data is being transmitted or received over the wireless link. • **Off**. The wireless radio is turned off.
Internet	• **Solid green**. The Internet connection has been established. • **Blinking green**. There is traffic on the Internet port. • **Off**. No Internet connection.
WPS	• **Solid green**. A WPS-capable device is connected to the router. • **Blinking green**. WPS connection with WPS-capable device is in process. • **Off**. No WPS connection.
Ethernet (1-4) 1	• **Solid green**. The LAN port has detected an Ethernet link with a device such as a computer. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on this port.

Back Panel

The back panel has the connections shown in the following figure.

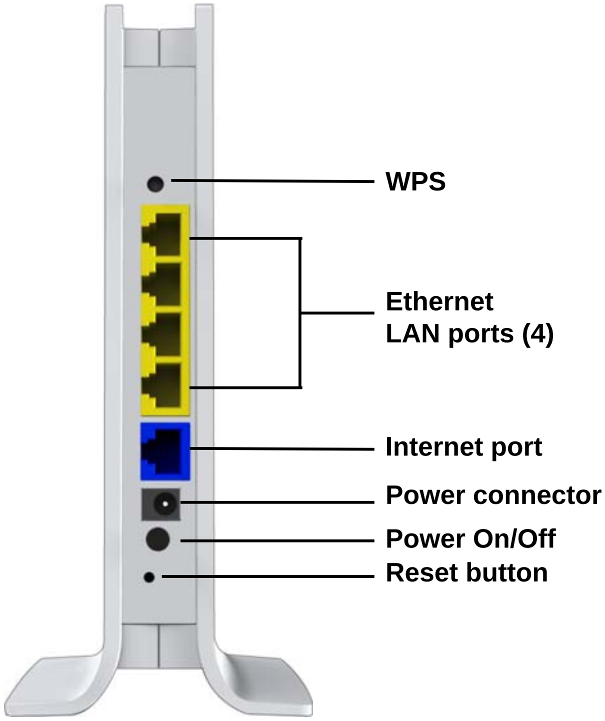
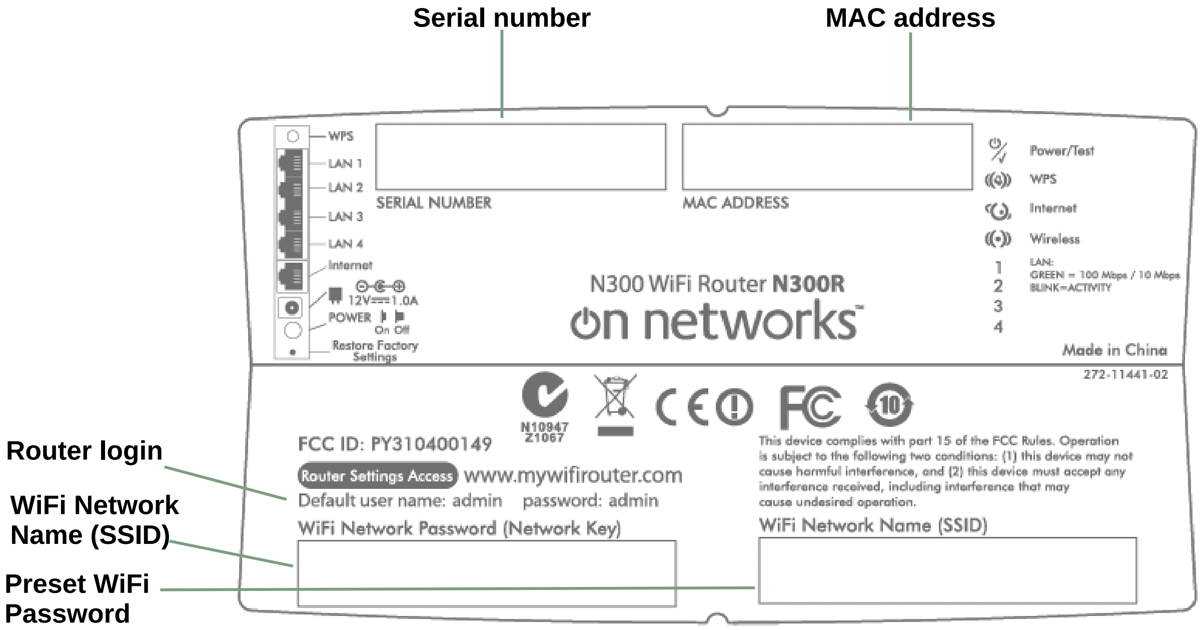


Figure 3. Router, rear view

See *Default Factory Settings* on page 85 for information about restoring factory settings.

Label

The label on the bottom of the router shows the preset WiFi network name and password, login informatioThe label on the bottom of the router shows the preset WiFi network name and password, login information, MAC address, and serial number.


Serial number
MAC address
WPS
LAN 1
LAN 2
LAN 3
LAN 4
Internet
12V⎓1.0A
POWER
On Off
Restore Factory Settings
SERIAL NUMBER
MAC ADDRESS
Power/Test
WPS
Internet
Wireless
1
2
3
4
LAN:
GREEN = 100 Mbps / 10 Mbps
BLINK=ACTIVITY
N300 WiFi Router N300R
on networks™
Made in China
272-11441-02
N10947
Z1067
FCC ID: PY310400149
Router Settings Access www.mywifirouter.com
Default user name: admin password: admin
WiFi Network Password (Network Key)
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
WiFi Network Name (SSID)
Router login
WiFi Network Name (SSID)
Preset WiFi Password

The label shows unique information about your router

Getting Started

2

Access your router

This chapter explains how to log in to your router to access the Home screen (Dashboard) to view or change the Internet settings and how to join your wireless network. This chapter contains the following sections:

- *Router Setup Preparation*
- *Log In to the Router*
- *Home Screen (Dashboard)*
- *EZ Setup Wizard*
- *Join Your Wireless Network*

Router Setup Preparation

You can set up your router with the Setup Wizard as described in *EZ Setup Wizard* on page 17, or manually as described in *Internet Setup (Basic Settings)*. However, before you start the setup process, you need to have your ISP information and to make sure the laptops, PCs, and other devices in the network have the settings described here.

Note: For a Macintosh or Linux system, you have to use manual setup.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you have to change the settings back so that it uses Dynamic Host Configuration Protocol (DHCP).

Replace an Existing Modem and Router

To replace an existing modem and router, disconnect them and set them aside before starting the router setup.

Gather ISP Information

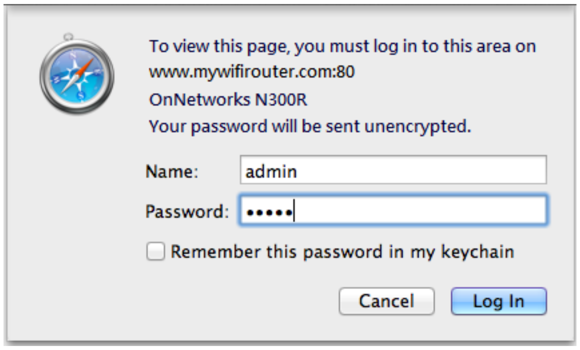
You need the following information to set up your router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it.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

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

Log In to the Router

➢ **Log in to the router to view or change settings or to set up the router.**

1. Type **http://192.168.1.1** in the address field of your browser and press **Enter** to display the login window. You can also enter the following address to access the router: **http://www.mywifirouter.com**.



To view this page, you must log in to this area on
www.mywifirouter.com:80
OnNetworks N300R
Your password will be sent unencrypted.

Name: admin
Password: •••••

□ Remember this password in my keychain

2. Enter **admin** for the user name and **admin** for the password, both in lowercase letters.

> **Note:** The router user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 15 for more information.

When you log in, if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest firmware.

A message displays telling you whether the router discovered a newer version of firmware.

3. To update to the new firmware, click **Yes** to allow the router to download and install the new firmware file from On Networks.

⚠ **WARNING:**

When uploading firmware to the N300R 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 firmware.

When the upload is complete, your Router restarts. The update process typically takes about 1 minute.

Unsuccessful Login

- **Do the following if you do not see the login prompt:**

1. Check the LEDs on the front of the router to make sure that the router is plugged in, its power is on, and the Ethernet cable between your computer and the router is connected to a LAN port.
2. If you connected the Ethernet cable and quickly launched your browser and typed in the router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the router wirelessly, On Networks recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the router.
4. If you cannot connect to the router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation.

Log Out Manually

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

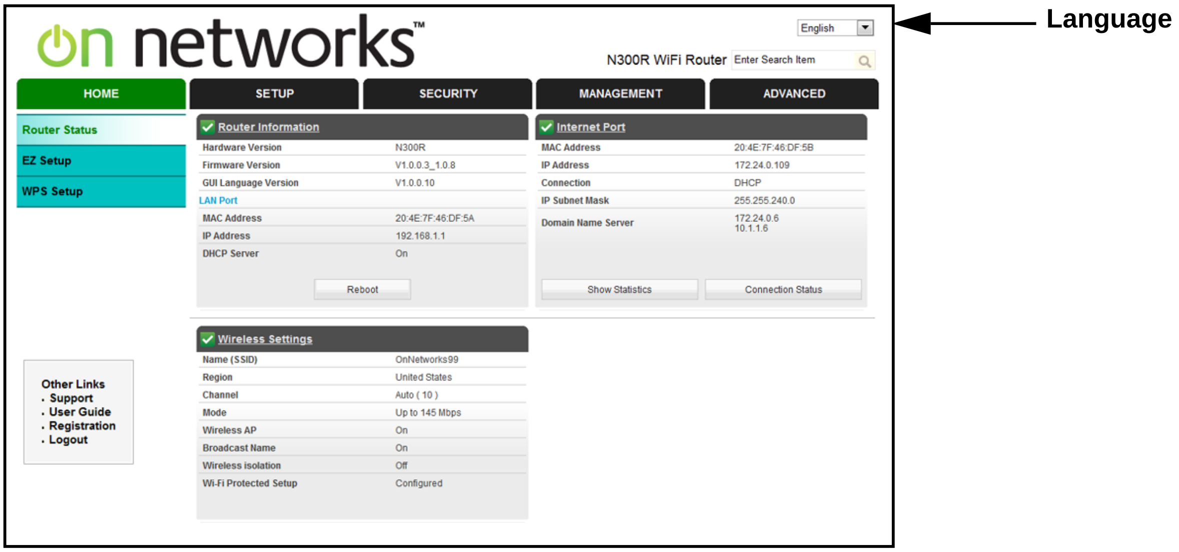
Types of Logins

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

- **Router login** logs you in to the router interface. See *Log In to the Router* on page 14 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **WiFi Network Name (SSID) and WiFi Network Password (network key)** logs you in to your wireless network. This login is preconfigured and can be found on the label on the bottom of your unit. See *WiFi Setup* on page 25, for more information.

Home Screen (Dashboard)

The router interface lets you view or change the router settings. The left column has menus, and the right column provides online help. The middle column is the screen for the current menu option.



Language

Router Information	
Hardware Version	N300R
Firmware Version	V1.0.0.3_1.0.8
GUI Language Version	V1.0.0.10
LAN Port	
MAC Address	20:4E:7F:46:DF:5A
IP Address	192.168.1.1
DHCP Server	On

Internet Port	
MAC Address	20:4E:7F:46:DF:5B
IP Address	172.24.0.109
Connection	DHCP
IP Subnet Mask	255.255.240.0
Domain Name Server	172.24.0.6 10.1.1.6

Wireless Settings	
Name (SSID)	OnNetworks99
Region	United States
Channel	Auto (10)
Mode	Up to 145 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

Figure 4. Dashboard (Home screen)

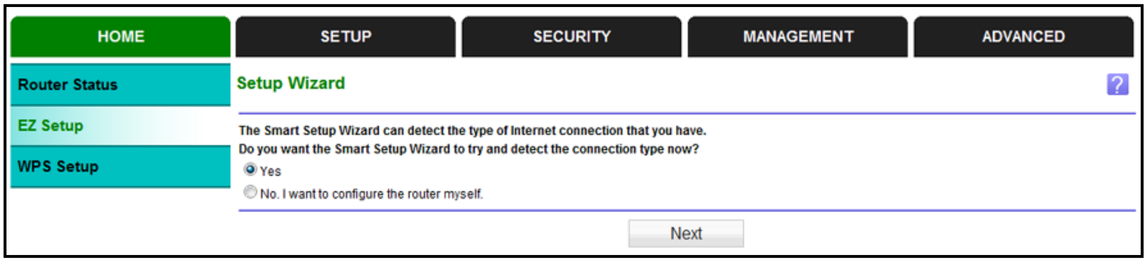
- **EZ Setup Wizard**. Specify the language and location, and automatically detect the Internet connection. See *EZ Setup Wizard* on page 17.
- **WPS Setup**. Join the secure WiFi network without typing the password. See *Join Your Wireless Network* .
- **Setup tab**. Set, upgrade, and check the ISP and wireless network settings of your router. See *Internet Setup (Basic Settings)*. See also *Chapter 3, Router Setup*, for information about preset and basic security settings.
- **Security tab**. View and configure the router firewall settings to prevent objectionable content from reaching your PCs. See *Chapter 4, Security Settings*.
- **Management tab**. Administer your router and network. See *Chapter 5, Network Management*.
- **Advanced tab**. Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 6, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.
- **Other Links**. Go to the support site to get information, help, and product documentation. These links work once you have an Internet connection.

EZ Setup Wizard

You can log in to the router and use EZ Setup to set up your Internet connection.

➢ **To use the setup wizard:**

1. From the top of the router menu, select **EZ Setup** to display the following screen:



Setup Wizard

The Smart Setup Wizard can detect the type of Internet connection that you have.
Do you want the Smart Setup Wizard to try and detect the connection type now?

● Yes

○ No. I want to configure the router myself.

2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, proceed to *Internet Setup (Basic Settings)* on page 21.
3. If you selected Yes, click **Next**.

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

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

➢ **To troubleshoot an unsuccessful Internet connection:**

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 7, Troubleshooting*. If problems persist, register your product and contact Technical Support.
4. If you cannot connect to the router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation.

Join Your Wireless Network

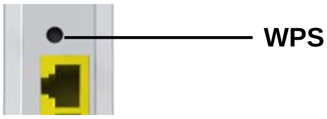
Choose either the WPS method or the manual method to join your wireless network.

WPS Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, you press a button or enter a PIN. Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

➢ **To use the WPS button on the router:**

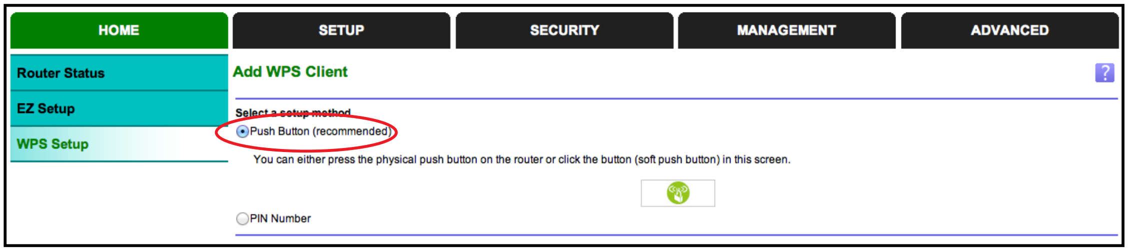
1. Press the **WPS** button on the rear panel of the router.
2. Within 2 minutes, use WPS to join the network using one of the following methods:



- If your computer or wireless device has a WPS button, press it.
- On your computer or wireless device, with the software you use to join wireless networks, select the **WPS** option, and follow the instructions to connect.

➢ **To use the WPS method when you are logged in to the router:**

1. Select **Home > WPS Setup**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



Add WPS Client

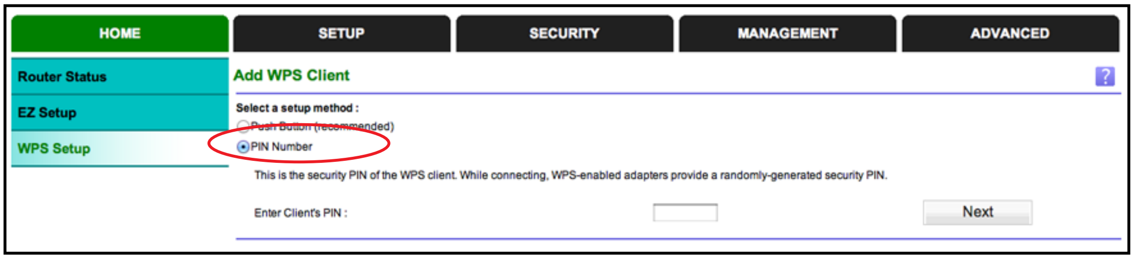
Select a setup method

● Push Button (recommended)

You can either press the physical push button on the router or click the button (soft push button) in this screen.

○ PIN Number

3. Select either **Push Button** or **PIN Number**. With either method, the router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.
4. When the PIN method screen displays, enter the client security PIN.



Add WPS Client

Select a setup method :

○ Push Button (recommended)

● PIN Number

This is the security PIN of the WPS client. While connecting, WPS-enabled adapters provide a randomly-generated security PIN.

Enter Client's PIN :

When the router establishes a WPS connection, the router WPS screen displays a confirmation message.

Manual Method

With the manual method, you choose the network that you want, and type its password to connect.

➢ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections. This software scans for all wireless networks in your area.
2. Look for your network and select it.

   The unique WiFi network name (SSID) and password is on the router label. If you changed these settings, then look for the network name that you used.

3. Enter the router password and click **Connect**.

3. Router Setup

3

Options on the Setup tab

This chapter contains the following sections:

- *Internet Setup (Basic Settings)*
- *Preset Security*
- *WiFi Security Basics*
- *WiFi Setup*
- *Internet Port*
- *LAN Ports*
- *Quality of Service (QoS) Setup*

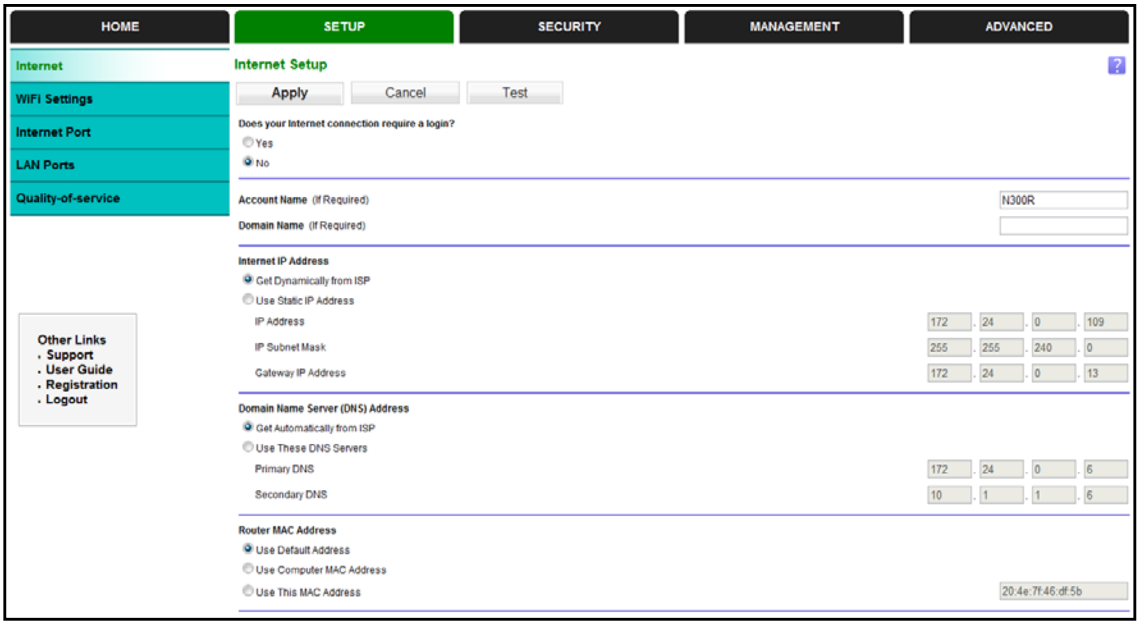
Internet Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Router myself in the Setup Wizard and is also available from the router menu. It is where you view or change ISP information. The fields that display vary depending on whether your Internet connection requires a login.

> **Note:** Check that the country is set as described *EZ Setup Wizard* on page 17 before proceeding with the manual setup.

➢ **To manually set up the Internet connection:**

1. Select **Setup > Internet,**



Internet Setup

Does your Internet connection require a login?
○ Yes
● No

Account Name (If Required) N300R
Domain Name (If Required)

Internet IP Address
● Get Dynamically from ISP
○ Use Static IP Address
IP Address 172 . 24 . 0 . 109
IP Subnet Mask 255 . 255 . 240 . 0
Gateway IP Address 172 . 24 . 0 . 13

Domain Name Server (DNS) Address
● Get Automatically from ISP
○ Use These DNS Servers
Primary DNS 172 . 24 . 0 . 6
Secondary DNS 10 . 1 . 1 . 6

Router MAC Address
● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address 20:4e:7f:46:df:5b

2. Select **Yes** or **No** depending on whether your ISP requires a login.
   - **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, as needed.
3. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the ISP settings.
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 you are not able to connect within 1 minute, see *Chapter 7, Troubleshooting*.

The following descriptions explain all of the possible fields in the Basic Settings screen. The fields that display in this screen depend on whether an ISP login is required.

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

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

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

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

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

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

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

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

  Service Name (If Required).

  Connection Mode.

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

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

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the 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.

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

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The router captures and uses 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.

Preset Security

The router comes with preset security. This means that the Wi-Fi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **WiFi Network Name (SSID)** identifies your network so devices can find it.
- **WiFi Network Password (Network Key)** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

Note: The preset SSID and passphrase are uniquely generated for every device to protect and maximize your wireless security.

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode, described in *Wireless Security Options* on page 24.

The Wireless Settings screen lets you view and change the preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

WiFi Security Basics

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

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Disable SSID Broadcast

By default, the router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to prevent the broadcast, wireless devices cannot find your router unless they are configured with the same SSID.

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

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific PCs based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the router. The Wireless Station MAC address filtering adds additional security protection to the wireless security option that you have in force. The Access list determines which wireless hardware devices are allowed to connect to the router by MAC address. See *Advanced WiFi Settings* on page 64 for the procedure.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the latest and most secure, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. It is possible to disable wireless security, but that is not recommended. You can view or change the wireless security options in the Wireless Settings screen. See *WiFi Setup* on page 25.

WiFi Setup

The Wireless Settings screen lets you view or change the wireless network settings. Your preset router has a unique network name and password on the product label. If you decide to change them, note the new settings and save them in a secure location.

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

Consider Every Device on Your Network

Before you begin, check the following:

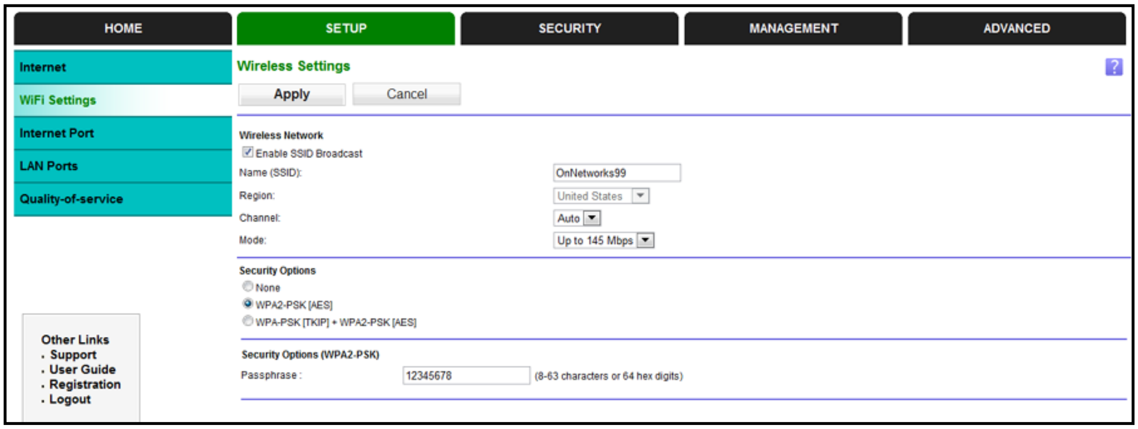
- Every wireless computer has to be able to obtain an IP address by DHCP from the router as described in *Use Standard TCP/IP Properties for DHCP* on page 13.
- Each computer or wireless adapter in your network must have the same SSID and wireless mode (bandwidth/data rate) as the router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network must match the router. For example, if you select a security option that requires a passphrase, be sure to use the same passphrase for each wireless computer in the network.

View or Change WiFi Settings

Your preset router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your router. You view or change these settings in the Wireless Settings screen.

➢ **To view or change wireless settings:**

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



Wireless Settings

Wireless Network

☑ Enable SSID Broadcast

Name (SSID): OnNetworks99

Region: United States

Channel: Auto

Mode: Up to 145 Mbps

Security Options

○ None

● WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA2-PSK)

Passphrase : 12345678 (8-63 characters or 64 hex digits)

2. Make any changes that are needed, and click **Apply** when done to save your settings.

> Note: The screen sections, settings, and procedures are explained in the following sections.

3. Set up and test your computers for wireless connectivity:

   a. Use your wireless computer or device to join your network. When prompted, enter the network password.

   b. From the wirelessly connected computer, make sure that you can access the Internet.

Wireless Settings Screen Fields

- **Enable SSID Broadcast**. This setting allows the router to broadcast its SSID so that a wireless station can display this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.
- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and there is typically no need to change it.
- **Region**. The location where the router is used. It might not be legal to operate the router in a region other than the regions listed.
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.
- **Mode**. Up to 145 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 300 Mbps supports up to 300 Mbps.

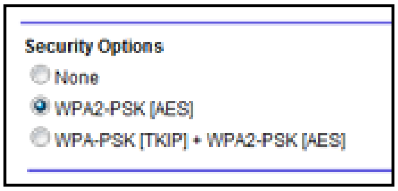
Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. Your preset router is already set up with WPA2 and WPA security. For information about changing these settings, see the following section, *Change WPA Security Option and Passphrase*.

Change WPA Security Option and Passphrase

➢ **To change WPA security:**

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

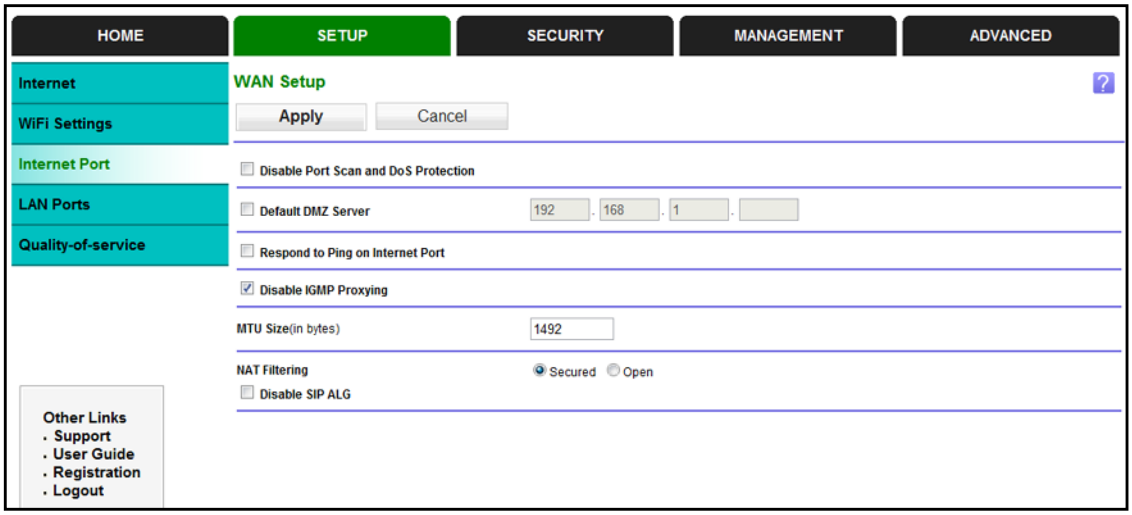


Security Options
○ None
● WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]

2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.
3. Click **Apply**.

Internet Port

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the router to respond to a ping on the WAN (Internet) port. Select **Setup > Internet Port** to view the following screen:



WAN Setup

□ Disable Port Scan and DoS Protection

□ Default DMZ Server 192 . 168 . 1 .

□ Respond to Ping on Internet Port

☑ Disable IGMP Proxying

MTU Size(in bytes) 1492

NAT Filtering ● Secured ○ Open
□ Disable SIP ALG

- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.

- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the router to respond to a ping from the Internet, select this check box. Use this setting only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.
- **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. You should only reduce the MTU if you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 29.
- **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.

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.

The router usually detects and discards Incoming traffic from the Internet that is not 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 the router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the Internet Port screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change 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 a device in the data path has a lower MTU setting than the other devices, the data packets have to be split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for On Networks equipment is often just the default value. In some situations, changing the value fixes one problem but causes another. Leave the 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 On Networks recommends changing the MTU setting. These web-based applications might require an MTU change:
    - A secure website that does not open or displays only part of a web page
    - Yahoo email
    - MSN portal
    - 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. For instance, you might not be able to access certain websites, frames within websites, 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. The following table describes common MTU sizes and applications.

Table 2. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for On Networks 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 do not have large email 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:**

1. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a value from 64 to 1500.
3. Click **Apply** to save the settings.

LAN Ports

The LAN Ports 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:

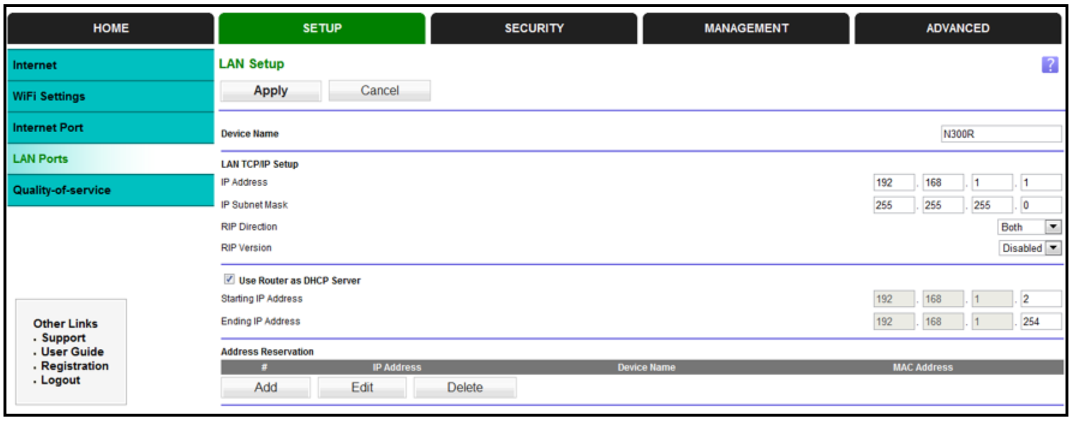
- LAN IP address. **192.168.1.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings in the LAN Setup screen.

➢ **To change the LAN settings:**

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

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



LAN Setup

Device Name: N300R

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disabled

☑ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

2. Enter the settings that you want to customize. These settings are described in the following section, *LAN TCP/IP Setup*.
3. Click **Apply** to save your changes.

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or router.
- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **RIP Version**. This setting controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.

  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.

Use Router as a DHCP Server

This check box is selected by default so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the router.

Address Reservation

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

Use the Router as a DHCP Server

By default, the router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the 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.

You can 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, define a range between 192.168.1.2 and 192.168.1.254, although you might want 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 Internet Setup screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Setup screen)

To use another device on your network as the DHCP server, or to specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, 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. Assign reserved IP addresses to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the 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 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.

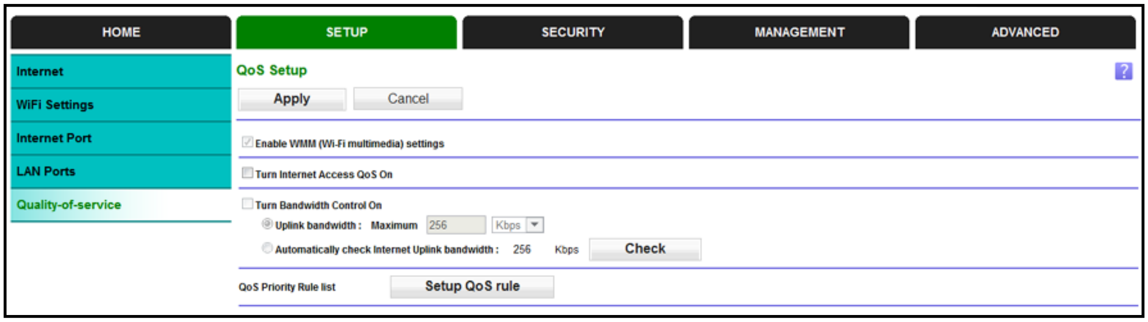
   The reserved address is not assigned until the next time the computer contacts the router’s DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The N300R router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

Select **Setup > Quality of Service** to display the following screen:



QoS Setup

☑ Enable WMM (Wi-Fi multimedia) settings

□ Turn Internet Access QoS On

□ Turn Bandwidth Control On

● Uplink bandwidth : Maximum 256 Kbps

○ Automatically check Internet Uplink bandwidth : 256 Kbps

QoS Priority Rule list

Enable WMM QoS for Wireless Multimedia Applications

The N300R 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 have to have 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 by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for Internet Access

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

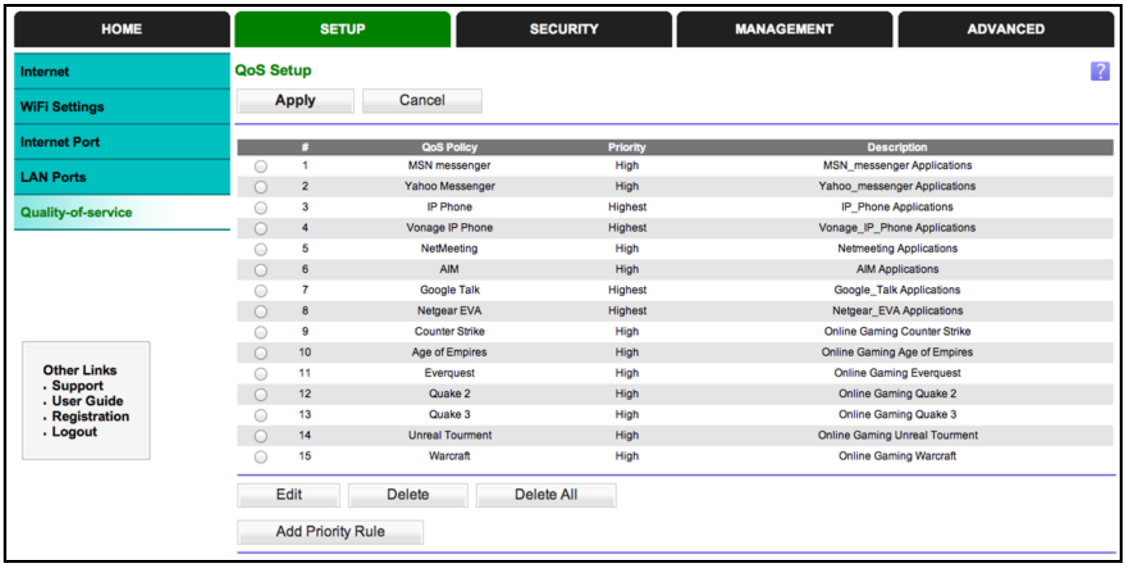
- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific device by MAC address

To specify prioritization of traffic, 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:**

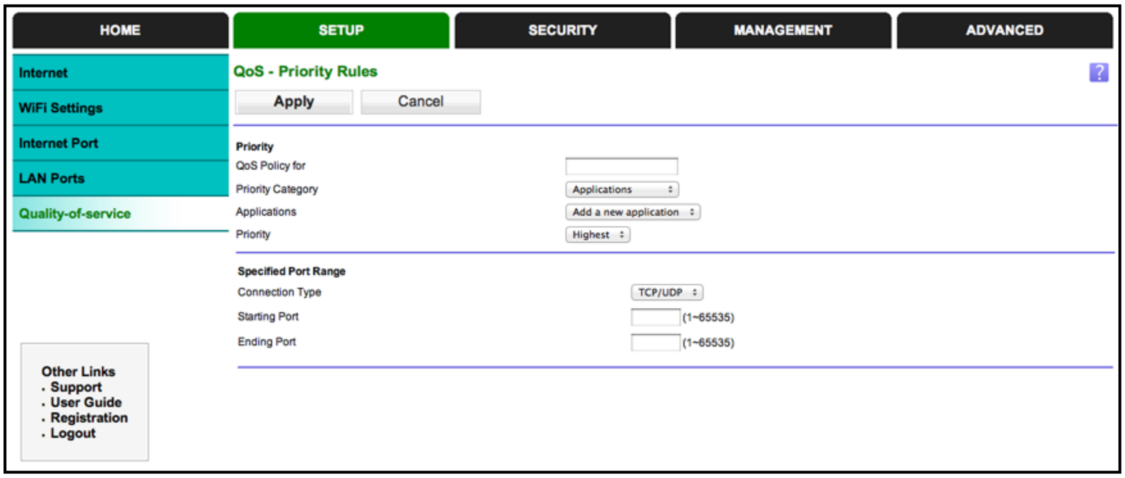
1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button to see the existing priority rules.



	#	QoS Policy	Priority	Description
○	1	MSN messenger	High	MSN_messenger Applications
○	2	Yahoo Messenger	High	Yahoo_messenger Applications
○	3	IP Phone	Highest	IP_Phone Applications
○	4	Vonage IP Phone	Highest	Vonage_IP_Phone Applications
○	5	NetMeeting	High	Netmeeting Applications
○	6	AIM	High	AIM Applications
○	7	Google Talk	Highest	Google_Talk Applications
○	8	Netgear EVA	Highest	Netgear_EVA Applications
○	9	Counter Strike	High	Online Gaming Counter Strike
○	10	Age of Empires	High	Online Gaming Age of Empires
○	11	Everquest	High	Online Gaming Everquest
○	12	Quake 2	High	Online Gaming Quake 2
○	13	Quake 3	High	Online Gaming Quake 3
○	14	Unreal Tourment	High	Online Gaming Unreal Tourment
○	15	Warcraft	High	Online Gaming Warcraft

You can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all of the rules by simply clicking the **Delete All** button.

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:



QoS - Priority Rules

Priority

QoS Policy for

Priority Category: Applications

Applications: Add a new application

Priority: Highest

Specified Port Range

Connection Type: TCP/UDP

Starting Port (1~65535)

Ending Port (1~65535)

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 applications or games displays in the list.
6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.

   If you add an entry, the Priority Rules screen expands.

   a. In the QoS Policy for field, enter a name for the new application or game.

   b. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**). Specify the port number or range of port numbers that the application or game uses.
7. From the Priority list, select the priority for Internet access for this traffic relative to other applications and traffic. 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.

QoS for a Router LAN Port

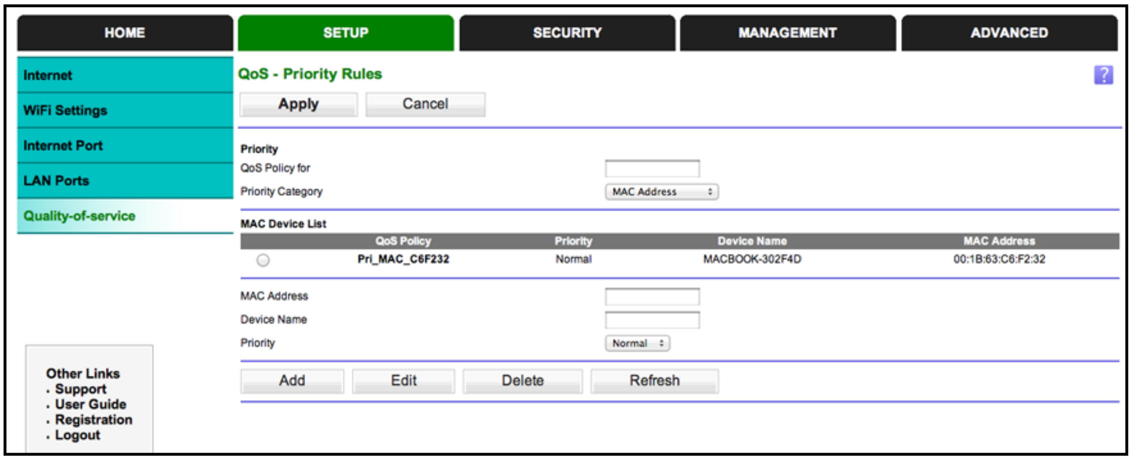
➢ **To create a QoS policy for a device connected to one of the router's LAN ports:**

1. Select **Setup > Quality of Service** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button.
3. Click the **Add Priority Rule** button.
4. From the Priority Category list, select **Ethernet LAN Port**.
5. From the LAN port list, select the LAN port.
6. From the Priority list, select the priority for Internet access for this port's traffic relative to other applications. The options are Low, Normal, High, and Highest.
7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **Setup > Quality of Service** and click the **Setup QoS Rule** button. The QoS Setup screen displays.
2. Click **Add Priority Rule**.
3. From the Priority Category list, select **MAC Address**:



QoS - Priority Rules

Priority

QoS Policy for

Priority Category: MAC Address

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
○	Pri_MAC_C6F232	Normal	MACBOOK-302F4D	00:1B:63:C6:F2:32

MAC Address

Device Name

Priority: Normal

4. If the device is the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device is not in the list, click **Refresh**. If it still does not appear, fill in these fields manually.
5. From the Priority list, select the priority for Internet access for this device’s traffic relative to other applications and traffic. The options are Low, Normal, High, and Highest.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Editing or Deleting an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **Setup > Quality of Service** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy that you want to edit or delete, 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.
3. Click **Apply** in the QoS Setup screen to save your changes.

4

Security Settings

Security tab (firewall) details

You can customize many of the firewall settings based on your needs. This chapter contains the following sections:

Firewall Rules to Control Network Access

Your router has a firewall that blocks unauthorized access to your wireless network and permits authorized inbound and outbound communications. Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

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

Inbound Rules (Port Forwarding)

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

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

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

Outbound Rules (Service Blocking)

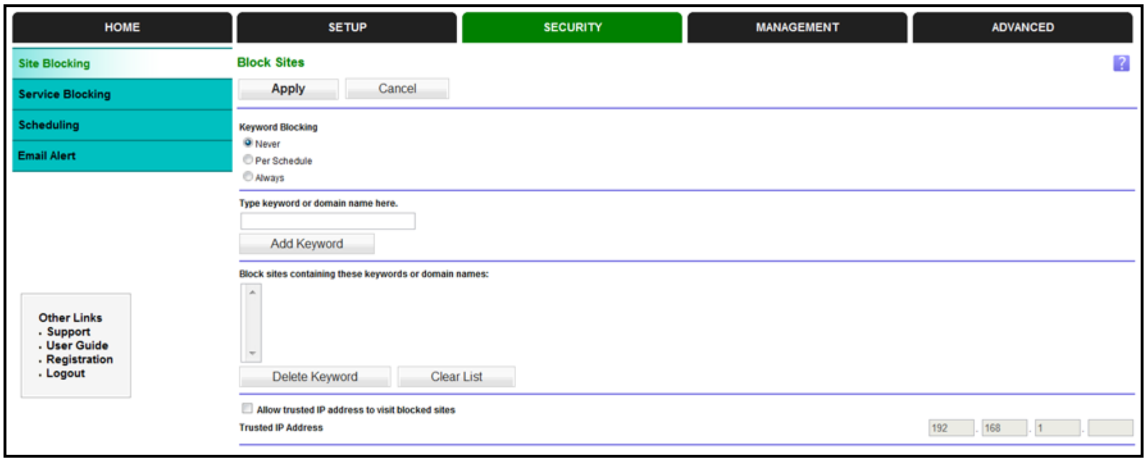
You can block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can add an outbound rule to block Internet access from a local computer based on the computer, Internet site, time of day, and type of service.

Set Up Site Blocking

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

➢ **To block traffic:**

1. Select **Security > Site Blocking**.



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 192 . 168 . 1 .

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

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

Delete Keyword or Domain

➢ **To delete keywords:**

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

Specify Trusted Computer

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

➢ **To specify a trusted computer:**

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

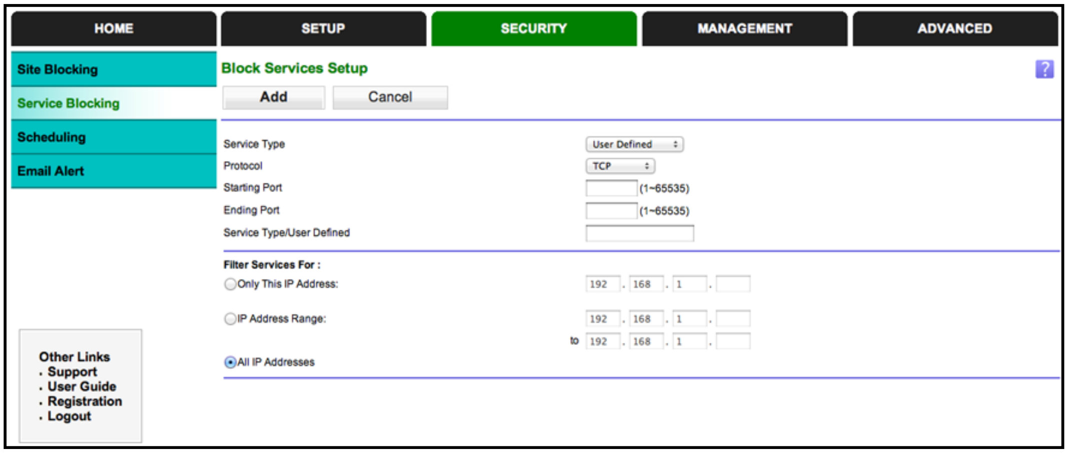
Set Up Service Blocking

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

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

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

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



Block Services Setup

Service Type: User Defined
Protocol: TCP
Starting Port: (1~65535)
Ending Port: (1~65535)
Service Type/User Defined:

Filter Services For :
○ Only This IP Address: 192 . 168 . 1 .
○ IP Address Range: 192 . 168 . 1 . to 192 . 168 . 1 .
● All IP Addresses

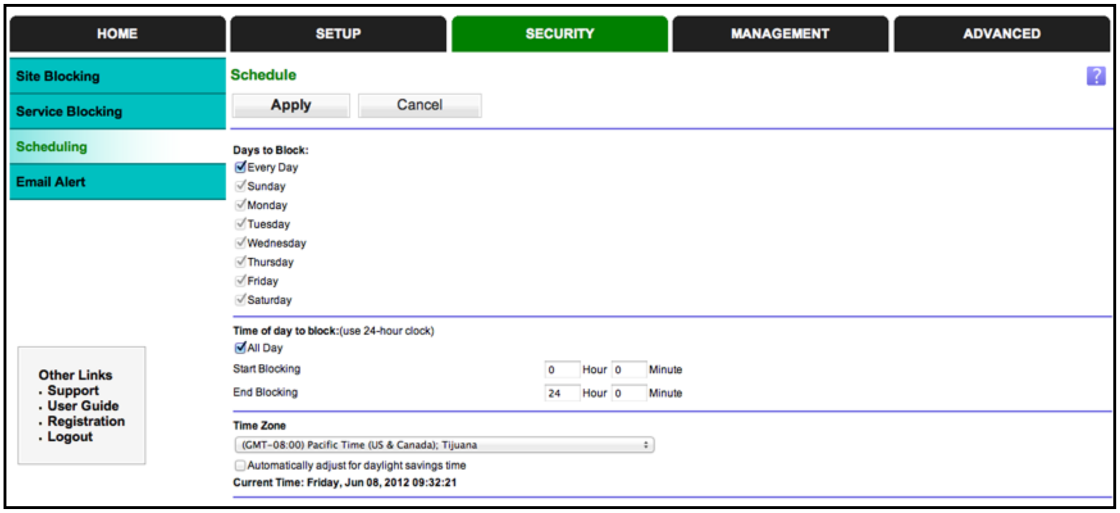
2. To create a service, click the **Add** button. If you want to change a service, select it and click **Edit**.
3. Define or edit a service by specifying the following.
   - **Name**. Enter a meaningful name for the service.
   - **Type**. Select the correct type for this service. If in doubt, select **TCP/UDP**. The options are TCP, UDP, and TCP/UDP.
   - **Start Port** and **Finish Port**. If a port range is required, enter the range here. If a single port is required, enter the same value in both fields.
4. Click **Apply** to save your changes.

Set the Time Zone

The 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 set the time zone:**

1. Select **Security > Schedule**.



Schedule

Days to Block:
☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day to block:(use 24-hour clock)
☑ All Day
Start Blocking 0 Hour 0 Minute
End Blocking 24 Hour 0 Minute

Time Zone
(GMT-08:00) Pacific Time (US & Canada); Tijuana
□ Automatically adjust for daylight savings time
Current Time: Friday, Jun 08, 2012 09:32:21

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

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

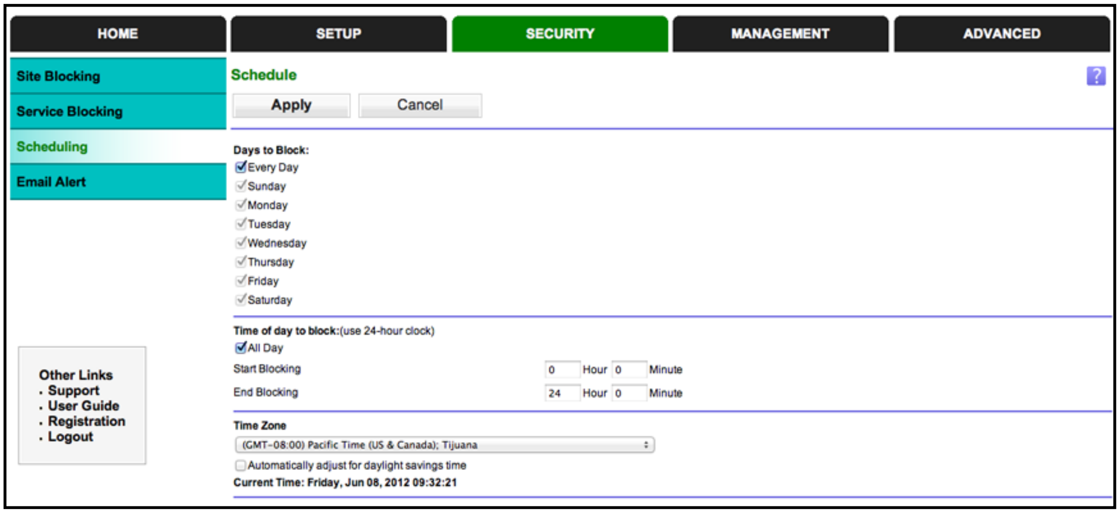
4. Click **Apply** to save your settings.

Schedule Services

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

➢ **To schedule services:**

1. Select **Security > Schedule**.



Schedule

Days to Block:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day to block:(use 24-hour clock)

☑ All Day

Start Blocking 0 Hour 0 Minute

End Blocking 24 Hour 0 Minute

Time Zone

(GMT-08:00) Pacific Time (US & Canada); Tijuana

□ Automatically adjust for daylight savings time

Current Time: Friday, Jun 08, 2012 09:32:21

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

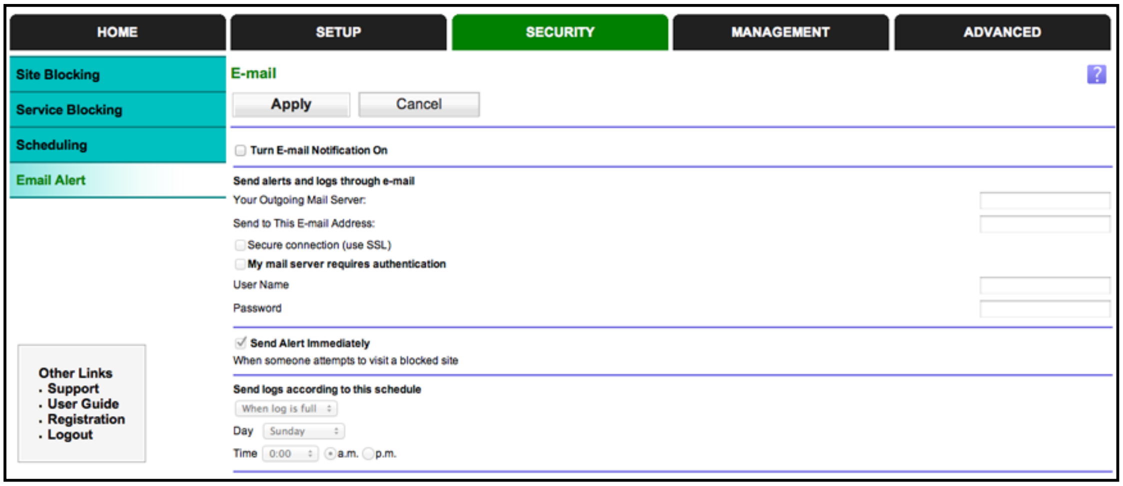
   Note: *Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.*

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

Set Up Email Alerts

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

Select **Security > Email Alert** to display the following screen:



□ Turn E-mail Notification On

Send alerts and logs through e-mail

Your Outgoing Mail Server:

Send to This E-mail Address:

□ Secure connection (use SSL)

□ 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

When log is full

Day Sunday

Time 0:00 ● a.m. ○ p.m.

Figure 5. E-Mail screen

- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the router.
- **Send to This E-mail Address**. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **Your Outgoing Mail Server**. Enter the name or IP address of your ISP’s outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **My mail server requires authentication**. If you use an outgoing mail server that your current ISP provided, you do not need to select this field. If you use an email account that is not provided by your ISP, select this field, and enter the required user name and password information.
- **Send Alerts Immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - **Days**. Specify which day of the week to send the log. This is relevant when the log is sent weekly.

- **Time**. Specify the time of day to send the log. This is relevant when the log is sent daily or weekly.

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

Port Forwarding and Triggering

By default, the router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these 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 your router does not recognize their replies.

Your router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

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

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

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

   Source address. Your computer’s IP address.

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

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

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

3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

   - The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
   - The source port number is changed to a number assigned by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

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

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

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

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

   Destination address. The public IP address of your router.

   Destination port number. 33333.

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

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

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

   Destination address. Your computer's IP address.

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

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

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number. Replies from the remote computer to your router are directed to that port number. If the remote server sends a reply to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies 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 have to also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your 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, 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.

Port Forwarding to Permit External Host Communications

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

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. 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. A person using a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

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

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

   The remote computer 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 is 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 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 the relevant user groups and 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 require that you 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 can 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.

Set Up 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 want to make a local web server, FTP server, or game server visible and available to the Internet.

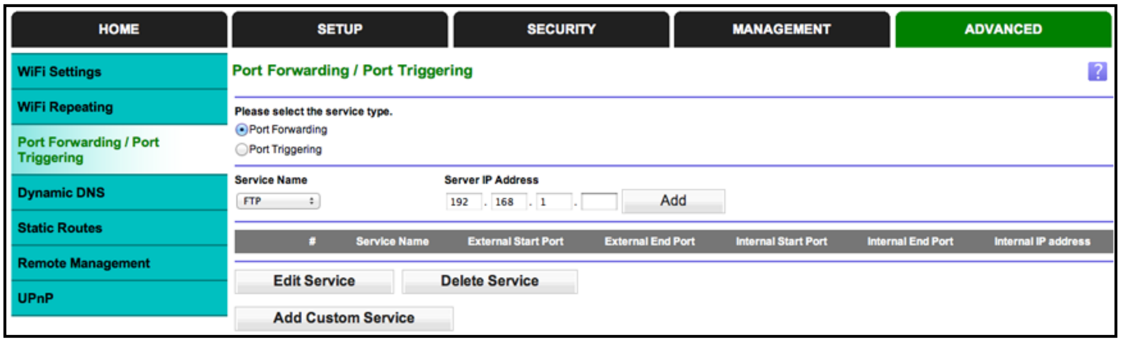
Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, determine which type of service, application, or game you want to provide. Find out the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your N300R router.

1. Select **Advanced > Port Forwarding/Port Triggering** to display the following screen:



Port Forwarding / Port Triggering

Please select the service type.

● Port Forwarding

○ Port Triggering

Service Name: FTP

Server IP Address: 192 . 168 . 1 .

#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address

Port Forwarding is selected as the service type.

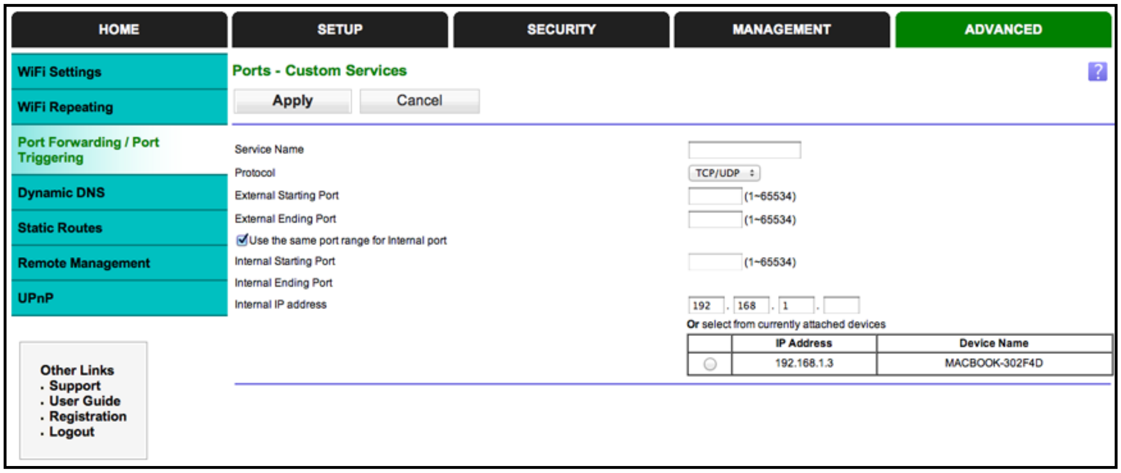
2. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 49.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
4. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, first determine which port number or range of numbers the application uses. You can usually get this information by contacting the publisher of the application or user groups or newsgroups.

To add a custom service:

1. Select **Advanced > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button to display the following screen:



Ports - Custom Services

Service Name:

Protocol: TCP/UDP

External Starting Port: (1~65534)

External Ending Port: (1~65534)

☑ Use the same port range for Internal port

Internal Starting Port: (1~65534)

Internal Ending Port:

Internal IP address: 192 . 168 . 1 .

Or select from currently attached devices

	IP Address	Device Name
○	192.168.1.3	MACBOOK-302F4D

4. In the Service Name field, enter a descriptive name.
5. In the Protocol list, 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 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.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the radio 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. In this example, your router always gives 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 *Dynamic DNS* on page 70. To access your web server from the Internet, a remote user has to know the IP address that your ISP assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetwork.dyndns.org.

Set Up 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.

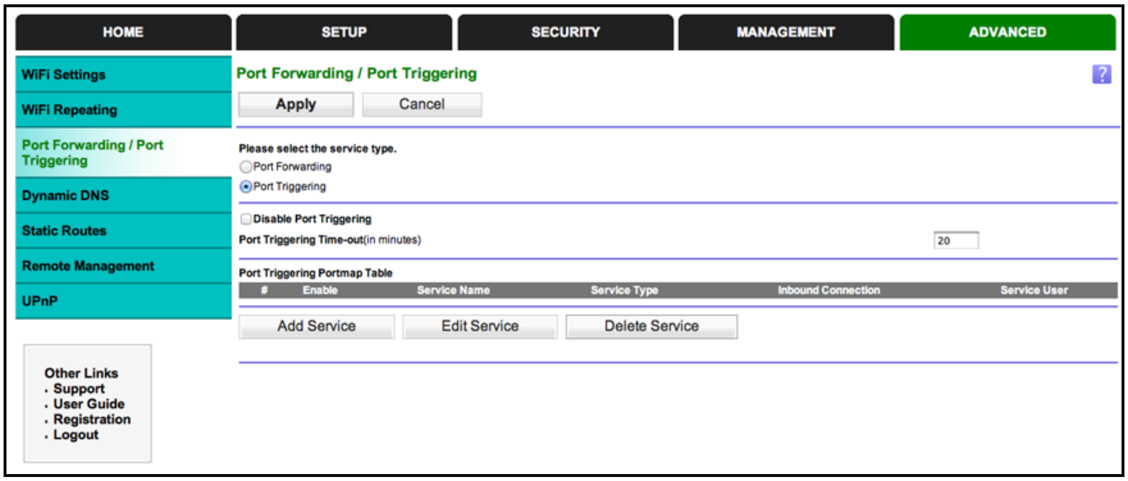
Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

> **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 74.

To set up port triggering, you need to know which inbound ports the application needs and the number of the outbound port that will trigger the opening of the inbound ports. You can usually get this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To set up port triggering:**

1. Select **Advanced > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.



Port Forwarding / Port Triggering

Please select the service type.
○ Port Forwarding
● Port Triggering

□ Disable Port Triggering
Port Triggering Time-out(in minutes) 20

Port Triggering Portmap Table

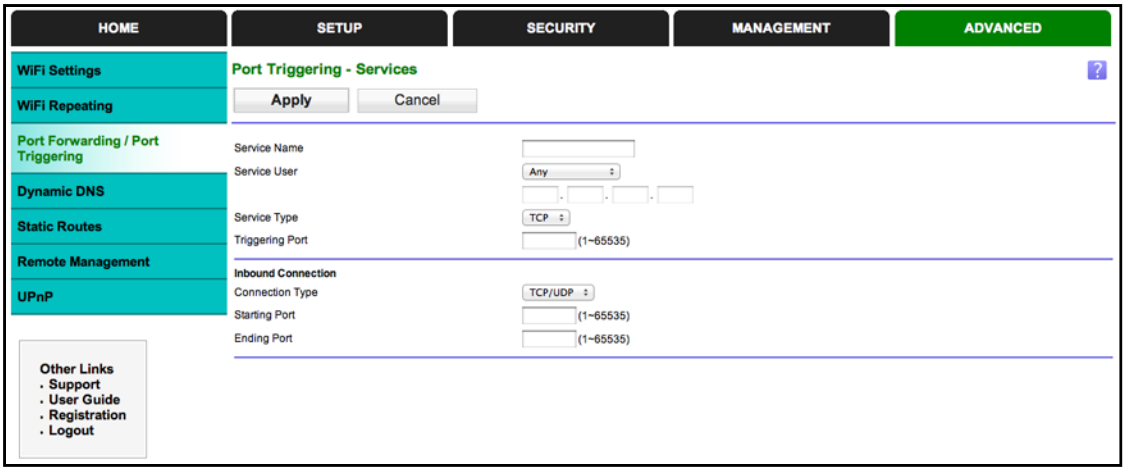
#	Enable	Service Name	Service Type	Inbound Connection	Service User

3. Clear the **Disable Port Triggering** check box if it is selected.

> **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.*

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes.

5. 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.
6. Click **Add Service** to display the following screen:



Port Triggering - Services

Service Name
Service User: Any
Service Type: TCP
Triggering Port (1~65535)

Inbound Connection
Connection Type: TCP/UDP
Starting Port (1~65535)
Ending Port (1~65535)

7. In the Service Name field, type a descriptive service name.
8. In the Service User list, 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.
9. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
10. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
11. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
12. Click **Apply**. The service appears in the Port Triggering Portmap table.

5. Network Management

Management tab options

5

This chapter contains the following sections:

- *Upgrade the Router Firmware*
- *Manually Check for Firmware Upgrades*
- *Backup Settings*
- *Change Password*
- *View Router Status*
- *View Attached Devices*
- *Logs*

Upgrade the Router Firmware

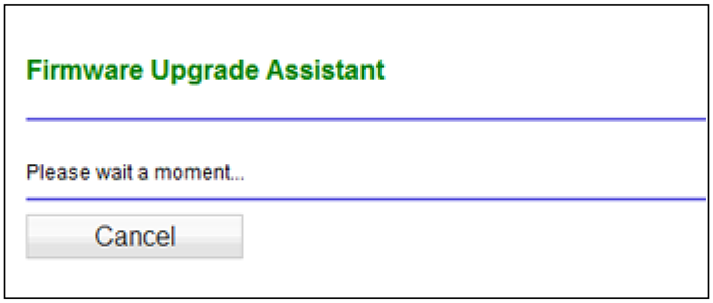
The router firmware (routing software) is stored in flash memory. By default, when you log in to your router, it checks the On Networks website for new firmware and alerts you if there is a newer version.

⚠ WARNING:

When uploading firmware to the 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 firmware.

Automatic Firmware Check

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



Firmware Upgrade Assistant

Please wait a moment...

➢ **To check the firmware automatically:**

1. Click **Yes** to allow the router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your router restarts.
2. Go to the N300R support page and read the new firmware release notes to determine whether you need to reconfigure the router after upgrading.

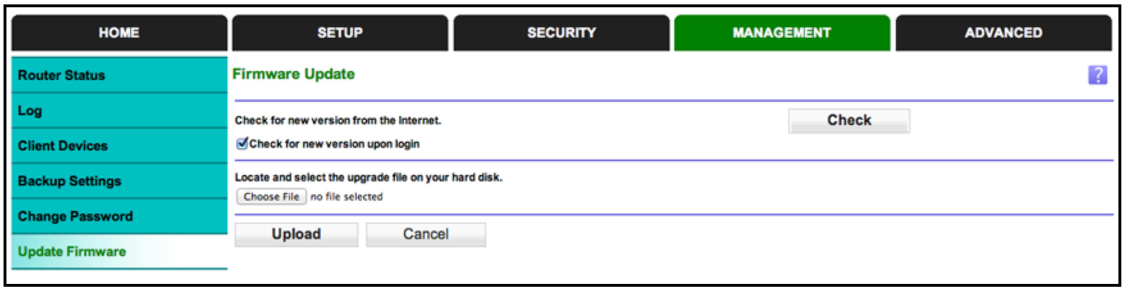
Note: If you get a “Firmware needs to be reloaded” message, it means that a problem has been detected with the router’s firmware. Follow the prompts to correct the problem.

Stop the Automatic Firmware Check

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See *Manually Check for Firmware Upgrades* on page 55. To turn off the automatic firmware check at login:

➢ **To stop automatic firmware check:**

1. Select **Manage > Update Firmware**.
2. Clear the **Check for new version upon login** check box.



Firmware Update

Check for new version from the Internet.

☑ Check for new version upon login

Locate and select the upgrade file on your hard disk.

no file selected

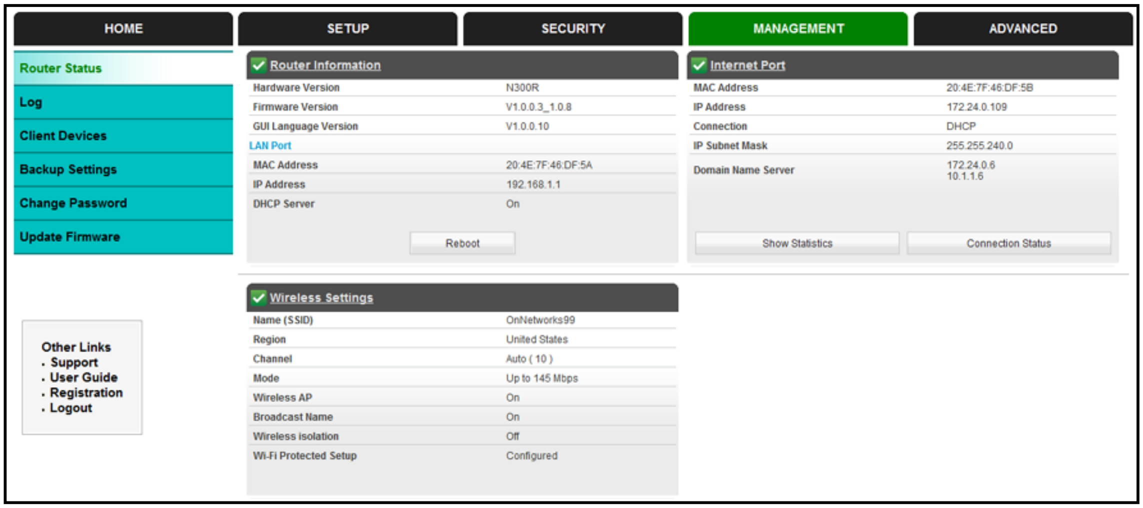
Manually Check for Firmware Upgrades

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

WARNING:

When uploading firmware to the 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 firmware.

1. Log in to your router, select **Manage > Router Status**, and make note of the firmware version of your router.



✓ Router Information	
Hardware Version	N300R
Firmware Version	V1.0.0.3_1.0.8
GUI Language Version	V1.0.0.10
LAN Port	
MAC Address	20:4E:7F:46:DF:5A
IP Address	192.168.1.1
DHCP Server	On

✓ Internet Port	
MAC Address	20:4E:7F:46:DF:5B
IP Address	172.24.0.109
Connection	DHCP
IP Subnet Mask	255.255.240.0
Domain Name Server	172.24.0.6 10.1.1.6

✓ Wireless Settings	
Name (SSID)	OnNetworks99
Region	United States
Channel	Auto (10)
Mode	Up to 145 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

2. Go to the N300R support page on the On Networks website at *http://www.on-networks.com/support*.

3. Compare the version number of the most recent firmware offered to the firmware version of your router. If the version on the On Networks website is more recent, download the file from the N300R support page to your computer.
4. Log in to your router and select **Manage > Update Firmware**.
5. Click **Browse**, and locate the firmware image that you downloaded to your computer (the file ends in .img or .chk).
6. Click **Upload** to send the firmware to the router.

   When the upload is complete, your router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether you need to reconfigure the router after upgrading.

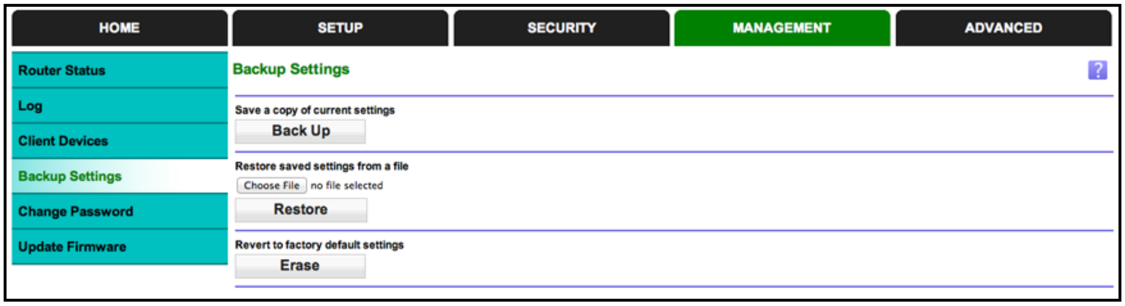
Backup Settings

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

Back Up

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

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



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

Restore

➢ **To restore the configuration file:**

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

   Upon completion, the router reboots.

Erase

Click the **Erase** button to reset the router to its factory default settings. Erase sets the password to **password**, the LAN IP address to **192.168.1.1**, and enables the router's DHCP.

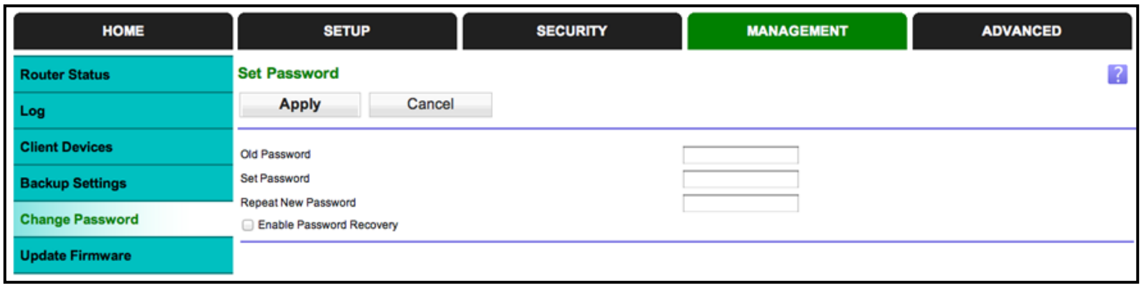
Change Password

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

> **Note:** The router user name and password are not the same as the user name and password for logging in to your Internet connection. See *Types of Logins* on page 15 for more information about login types.

➢ **To change the password and login time-out:**

1. Select **Management > Change Password** to display the following screen:.



Old Password
Set Password
Repeat New Password
□ Enable Password Recovery

2. Enter the old password.
3. Enter the new password twice.
4. Click **Apply** to save your changes.

After changing the password, you are required to log in again to continue the configuration. If you have backed up the router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Back Up* on page 56 for information about backing up your network configuration.

Password Recovery

On Networks recommends that you enable password recovery if you change the password for the router's user name of admin. Then if the password is forgotten, you can recover it. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

- **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.
3. Click **Apply** to save your changes.

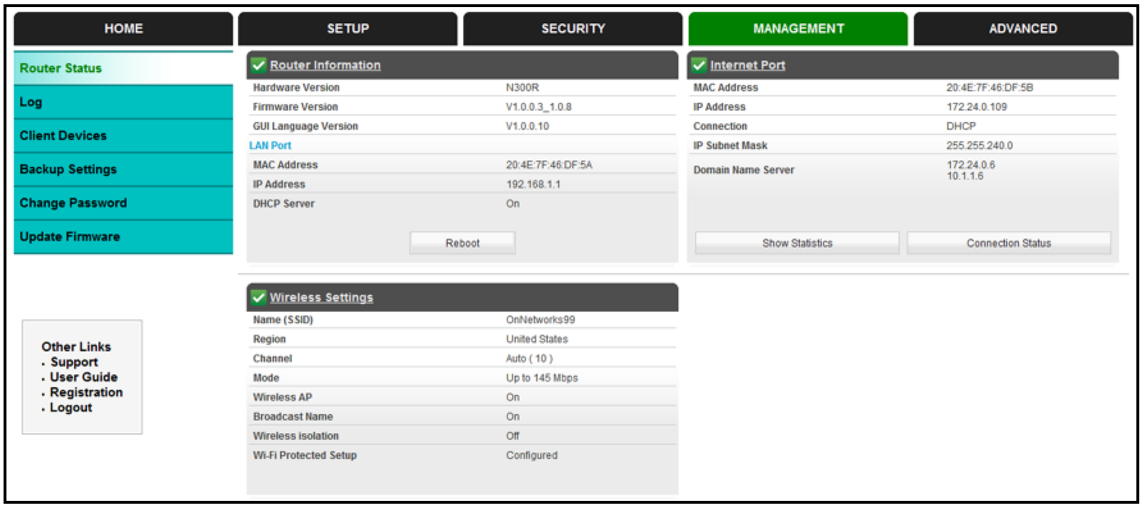
When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

View Router Status

The Router Status screen provides status and usage information.

- **To view the router status:**

Select **Manage > Router Status** to display this screen.



✓ Router Information

Hardware Version	N300R
Firmware Version	V1.0.0.3_1.0.8
GUI Language Version	V1.0.0.10
LAN Port	
MAC Address	20:4E:7F:46:DF:5A
IP Address	192.168.1.1
DHCP Server	On

✓ Internet Port

MAC Address	20:4E:7F:46:DF:5B
IP Address	172.24.0.109
Connection	DHCP
IP Subnet Mask	255.255.240.0
Domain Name Server	172.24.0.6 10.1.1.6

✓ Wireless Settings

Name (SSID)	OnNetworks99
Region	United States
Channel	Auto (10)
Mode	Up to 145 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

The following information is displayed:

Hardware and Firmware Version. The model of the hardware and the currently running firmware version.

GUI Language Version. The currently selected language.

Internet Port Settings

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

IP Address. The Internet port IP address. If no address is shown, the router cannot connect to the Internet.

Connection. The value depends on your ISP.

IP Subnet Mask. The Internet port IP subnet mask.

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

LAN Port (Local Ports)

MAC Address. The router LAN port Ethernet MAC address.

IP Address. The router LAN port IP address. The default is 192.168.1.1.

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

Wireless Port

See *WiFi Setup* on page 25 for a more detailed description of these settings.

Name (SSID). The Wi-Fi network name (service set ID) for the wireless network.

Region. The country where the unit is set up for use.

Channel. The current channel, which determines the operating frequency.

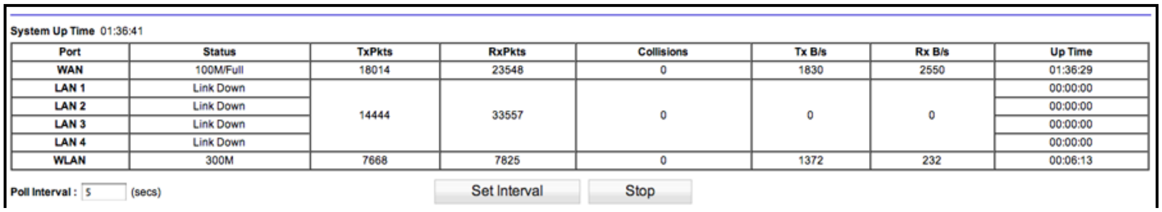
Mode. The current mbps setting.

Wireless AP. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates if the router is configured to broadcast its SSID.

Show Statistics

Click the **Show Statistics** button on the Router Status screen to display a screen similar to the following:



System Up Time 01:36:41

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	18014	23548	0	1830	2550	01:36:29
LAN 1	Link Down	14444	33557	0	0	0	00:00:00
LAN 2	Link Down						00:00:00
LAN 3	Link Down						00:00:00
LAN 4	Link Down						00:00:00
WLAN	300M	7668	7825	0	1372	232	00:06:13

Poll Interval : 5 (secs)

Port

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

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted since reset or manual clear.
- **RxPkts**. The number of packets received since reset or manual clear.
- **Collisions**. The number of collisions since reset or manual clear.

- **Tx B/s**. The current line utilization—percentage of current bandwidth used.
- **Rx B/s**. The average line utilization.
- **Up Time**. The time elapsed since the last power cycle or reset.

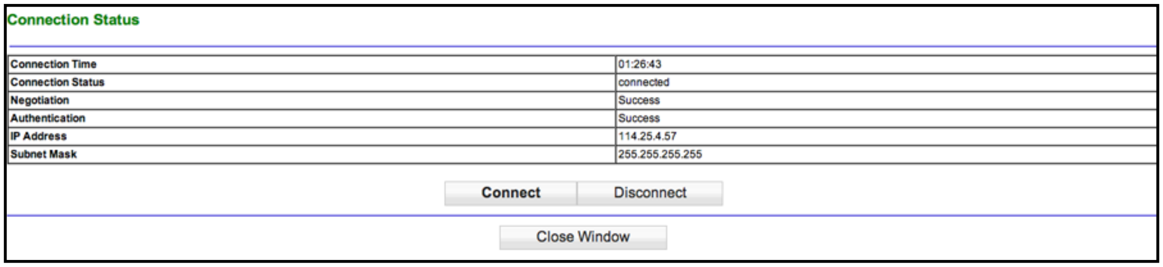
ADSL Link Downstream or Upstream

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

- **Connection Speed**. Typically, the downstream speed is faster than the upstream speed.
- **Line Attenuation**. The line attenuation increases the farther you are physically located from your ISP's facilities.
- **Noise Margin**. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.
- **Poll Interval**. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

Connection Status

In the Router Status screen, click the **Connection Status** button:



Connection Status

Connection Time	01:26:43
Connection Status	connected
Negotiation	Success
Authentication	Success
IP Address	114.25.4.57
Subnet Mask	255.255.255.255

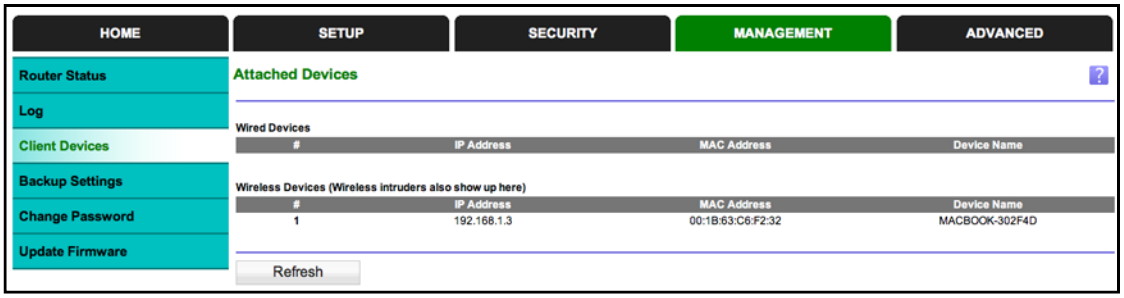
- **Connection Time**. The time elapsed since the last connection to the Internet through the Internet port.
- **Connection Status**. The connection status.
- **Negotiation**. On or Off.
- **Authentication**. On or Off.
- **IP Address**. The IP address assigned to the WAN port by the ISP.
- **Subnet Mask**. The network mask assigned to the WAN port by the ISP.

View Attached Devices

The Attached Devices screen shows all IP devices that the router has discovered on the local network.

- **To view attached devices:**

Select **Management > Client Devices**.



Attached Devices

Wired Devices

#	IP Address	MAC Address	Device Name

Wireless Devices (Wireless intruders also show up here)

#	IP Address	MAC Address	Device Name
1	192.168.1.3	00:1B:63:C6:F2:32	MACBOOK-302F4D

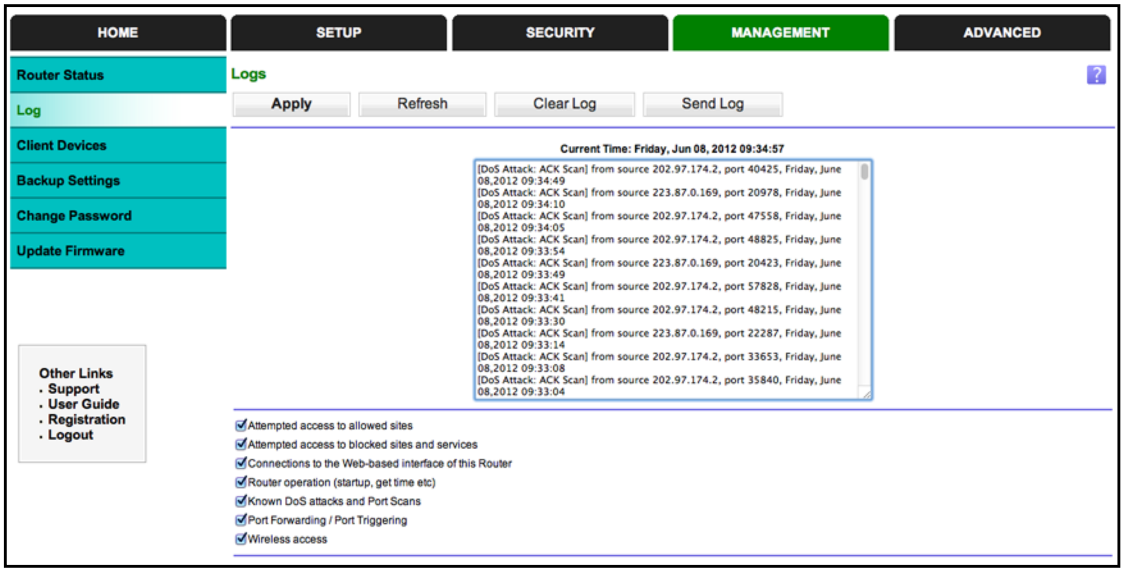
For each device, the table shows the IP address, the device name if available, and the Ethernet MAC address. If the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the **Refresh** button.

Logs

The router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites screen, the Logs screen show you when someone on your network tries to access a blocked site. If you enable email notification, you will receive these logs in an email message.

➢ To view the log:

Select **Management > Logs**. A screen similar to the following displays:



Current Time: Friday, Jun 08, 2012 09:34:57

```
[DoS Attack: ACK Scan] from source 202.97.174.2, port 40425, Friday, June
08,2012 09:34:49
[DoS Attack: ACK Scan] from source 223.87.0.169, port 20978, Friday, June
08,2012 09:34:10
[DoS Attack: ACK Scan] from source 202.97.174.2, port 47558, Friday, June
08,2012 09:34:05
[DoS Attack: ACK Scan] from source 202.97.174.2, port 48825, Friday, June
08,2012 09:33:54
[DoS Attack: ACK Scan] from source 223.87.0.169, port 20423, Friday, June
08,2012 09:33:49
[DoS Attack: ACK Scan] from source 202.97.174.2, port 57828, Friday, June
08,2012 09:33:41
[DoS Attack: ACK Scan] from source 202.97.174.2, port 48215, Friday, June
08,2012 09:33:30
[DoS Attack: ACK Scan] from source 223.87.0.169, port 22287, Friday, June
08,2012 09:33:14
[DoS Attack: ACK Scan] from source 202.97.174.2, port 33653, Friday, June
08,2012 09:33:08
[DoS Attack: ACK Scan] from source 202.97.174.2, port 35840, Friday, June
08,2012 09:33:04
```

☑ Attempted access to allowed sites
☑ Attempted access to blocked sites and services
☑ Connections to the Web-based interface of this Router
☑ Router operation (startup, get time etc)
☑ Known DoS attacks and Port Scans
☑ Port Forwarding / Port Triggering
☑ Wireless access

The Include in Log check boxes allow you to select which events are logged. You can write the logs to a computer running a syslog program. To activate this feature, select **Broadcast on LAN**, or enter the IP address of the server where the syslog file will be written. The security log entries include the following information:

- **Date and time**.The date and time the log entry was recorded.
- **Description or action**. The type of event and what action was taken, if any.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Source port and interface**. The service port number of the initiating device, and whether it originated from the LAN or WAN.
- **Destination**. The name or IP address of the destination device or website.
- **Destination port and interface**. The service port number of the destination device, and whether it is on the LAN or WAN.

6. Advanced Settings

6

Advanced tab settings for unique situations

This chapter describes the advanced features of your router. The information is for readers with advanced networking knowledge who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

Note: For information about port forwarding and port triggering, see *Chapter 4, Security Settings*.

This chapter includes the following sections:

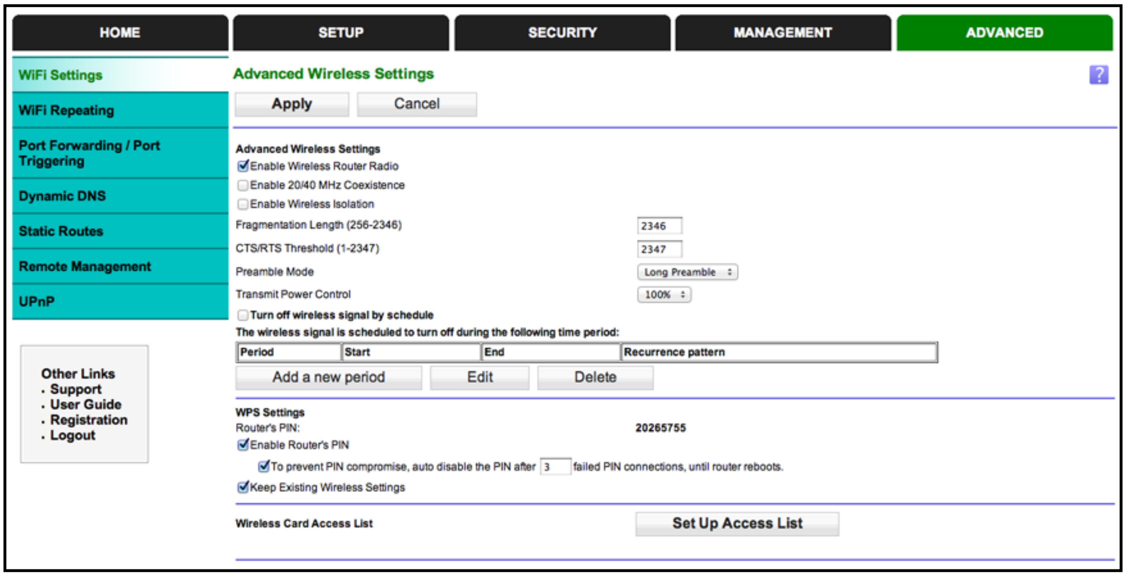
- *Advanced WiFi Settings*
- *WiFi Repeating (WDS)*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*

Advanced WiFi Settings

By default, the N300R router is set up with wireless settings that work in most situations. You can use this screen to control the wireless router radio and select advanced settings that specifically fit your environment.

➢ **To view or change the advanced wireless settings:**

Select **Advanced > WiFi Settings** to display the following screen:



Advanced Wireless Settings

Advanced Wireless Settings

☑ Enable Wireless Router Radio

□ Enable 20/40 MHz Coexistence

□ Enable Wireless Isolation

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Long Preamble

Transmit Power Control 100%

□ Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period	Start	End	Recurrence pattern

WPS Settings

Router's PIN: 20265755

☑ Enable Router's PIN

☑ To prevent PIN compromise, auto disable the PIN after 3 failed PIN connections, until router reboots.

☑ Keep Existing Wireless Settings

Wireless Card Access List

The following settings are available in this screen:

Enable Wireless Router Radio. You can completely turn off the wireless portion of the wireless router by clearing this check box. Select this check box again to enable the wireless portion of the router. When the wireless radio is disabled, other members of your household can use the router by connecting their computers to the router with an Ethernet cable.

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

Turn off wireless signal by schedule. You can use this feature to turn off the wireless signal from your router at times when you do not need a wireless connection. For instance, you could turn it off for the weekend if you leave town.

WPS Settings.You can add WPS devices to your network.

Wireless Card Access List. Click the **Set Up Access List** button display the Wireless Card Access List screen. You can restrict access to your network to specific devices based on their MAC address.

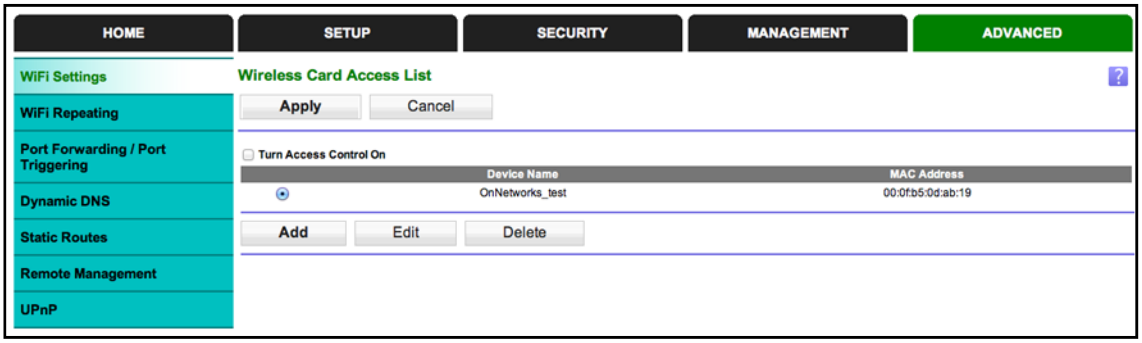
Restrict Wireless Access by MAC Address

You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

➤ **To restrict access based on MAC addresses:**

1. Select **Advanced > WiFi Setting** and click the **Setup Access List** to display the Wireless Card Access List.



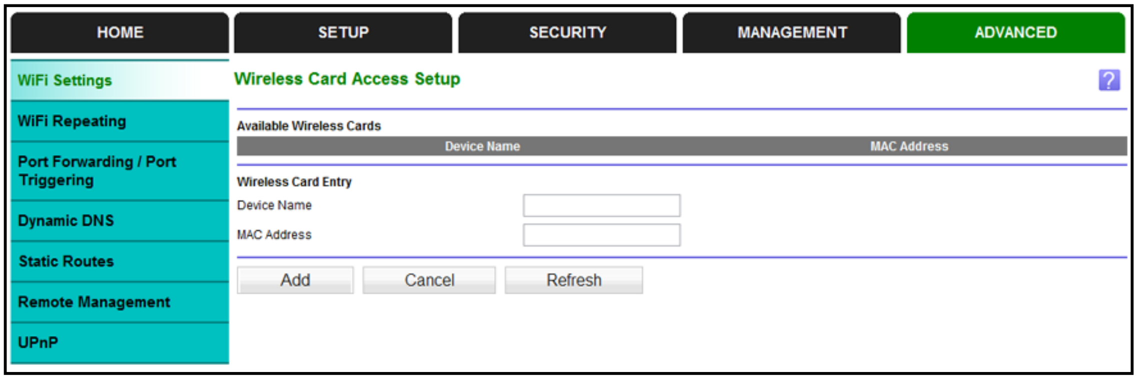
Wireless Card Access List

☐ Turn Access Control On

	Device Name	MAC Address
●	OnNetworks_test	00:0f:b5:0d:ab:19

2. 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.



Wireless Card Access Setup

Available Wireless Cards

Device Name	MAC Address

Wireless Card Entry

Device Name

MAC Address

3. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address. You can usually find the MAC address on the bottom of the wireless device.

Tip: You can copy and paste the MAC addresses from the router’s Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should then appear in the Attached Devices screen.

4. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.
5. Add each computer or device you want to allow to connect wirelessly.
6. Select the **Turn Access Control On** check box.
7. Click **Apply**.

WiFi Repeating (WDS)

You can set the N300R router up to be used as a wireless access point (AP). Doing this enables the router to act as a wireless repeater. A wireless repeater connects to another wireless router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

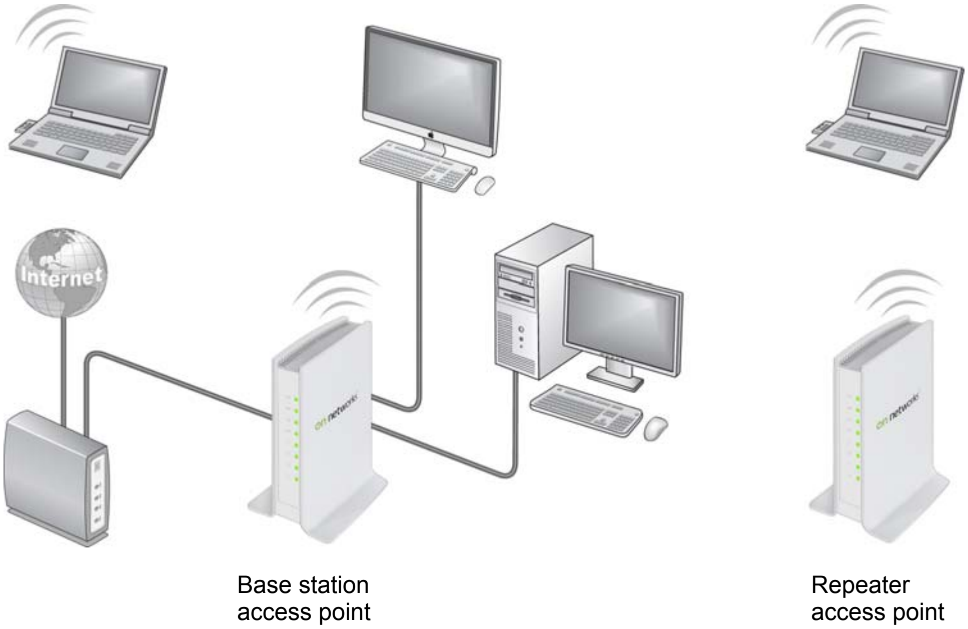


Figure 6. Wireless repeating scenario

If you use the wireless repeating function, you need to select either WEP or None as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode Up to 54 Mbps in the Wireless Settings screen.

Wireless Base Station. The router acts as the parent access point by bridging traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point.

Wireless Repeater. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

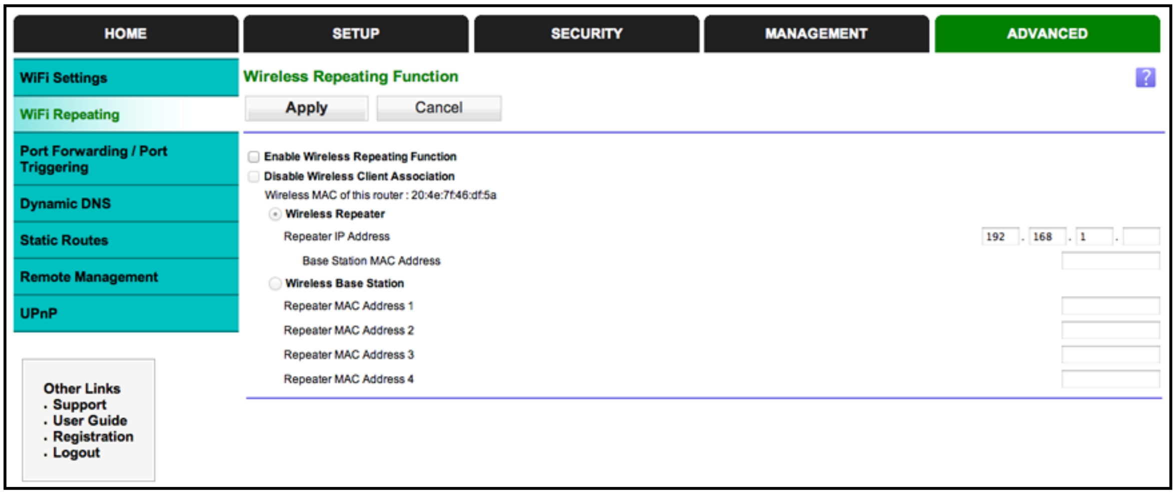
The N300R router is always in dual band concurrent mode, unless you turn off one radio.If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless router or wireless base station, dual band concurrent mode is not affected.

For you to set up a wireless network with WDS, both access points have to meet the following conditions:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

WiFi Repeating

Select **Advanced > WiFi Repeating** to view or change wireless repeater settings for the router.



Wireless Repeating Function

☐ Enable Wireless Repeating Function

☐ Disable Wireless Client Association

Wireless MAC of this router : 20:4e:7f:46:df:5a

● Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

Base Station MAC Address

○ Wireless Base Station

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

- **Enable Wireless Repeating Function**. Select this check box to use the wireless repeating function.

Disable Wireless Client Association. If your router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- If you are setting up a point-to-point bridge, select this check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- **Wireless MAC of this router**. This field displays the MAC address for your router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your router is the repeater, select this check box.

  Repeater IP Address. If your router is the repeater, enter the IP address of the other access point.

  Base Station MAC Address. If your router is the repeater, enter the MAC address for the access point that is the base station.
- **Wireless Base Station**. If your router is the base station, select this check box.

  Disable Wireless Client Association. If your router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

  Repeater MAC Address (1 through 4). If your router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

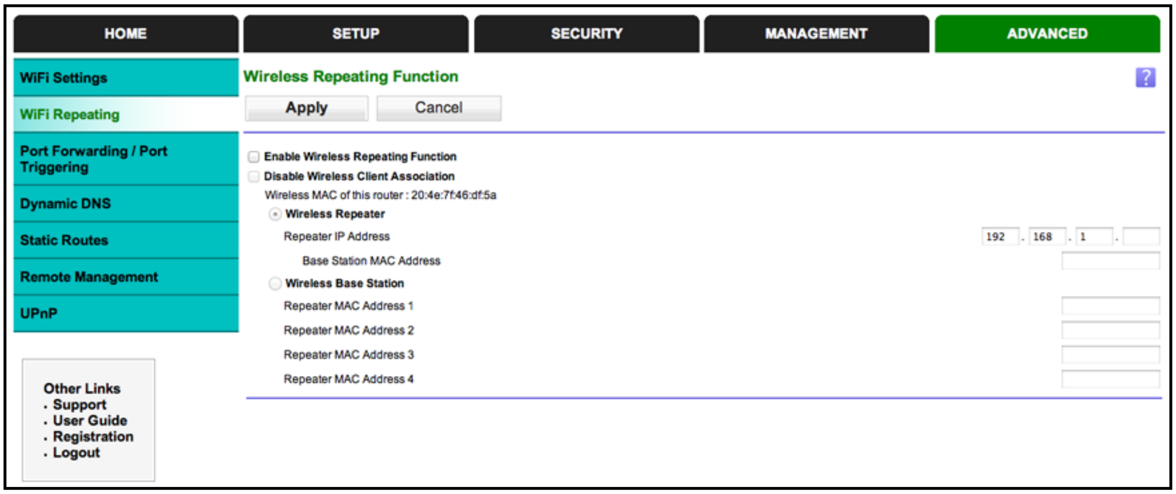
Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to 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 the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to None or WEP.

2. Select **Advanced > WiFi Repeating** to display the Wireless Repeating Function screen.



Wireless Repeating Function

□ Enable Wireless Repeating Function

□ Disable Wireless Client Association

Wireless MAC of this router : 20:4e:7f:46:df:5a

● Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

Base Station MAC Address

○ Wireless Base Station

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

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

Set 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 N300R base station with a different router product 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 the router as a repeater unit:**

1. Log in to the router that will be the repeater.
2. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
3. Select **Advanced > Wireless Repeating Function**.
4. Select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
5. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
6. Click **Apply** to save your changes.
7. Verify connectivity across the LANs.

A computer on any wireless or wired LAN segment of the 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 access point.

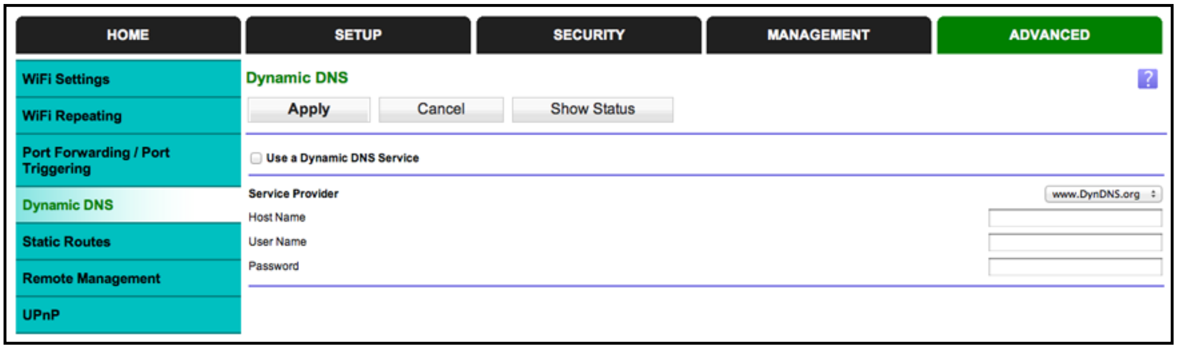
Dynamic DNS

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. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does 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. First visit their website at *http://www.dyndns.org* and obtain an account and host name that 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 *http://hostname.dyndns.org*.

Select **Advanced > Dynamic DNS** to display the following screen:



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name

User Name

Password

Figure 7. Forward traffic to a changing IP address

➢ To set up 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**.

Static Routes

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets 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.

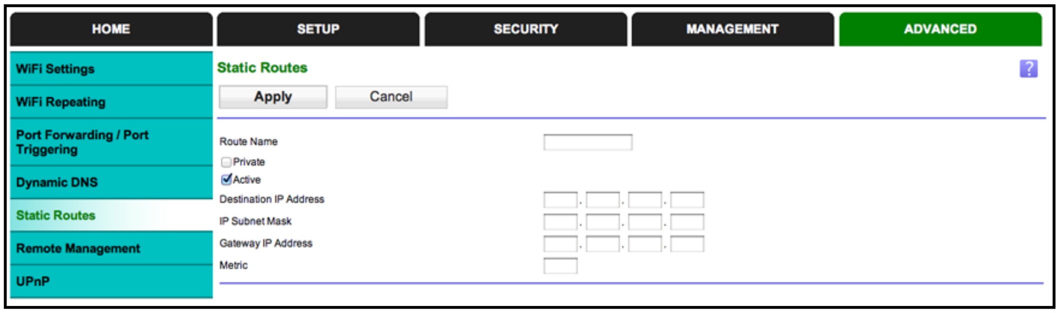
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 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 have to define a static route, telling your router to access 134.177.0.0 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 works since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➢ To set up a static route:

1. Select **Advanced > Static Routes**, and click **Add** to display the following screen:



Static Routes

Route Name

□ Private

☑ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

2. In the Route Name field, type a name for this static route (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 has to be a router on the same LAN segment as the N300R router.
8. Type a number from 1 through 15 as the metric value.

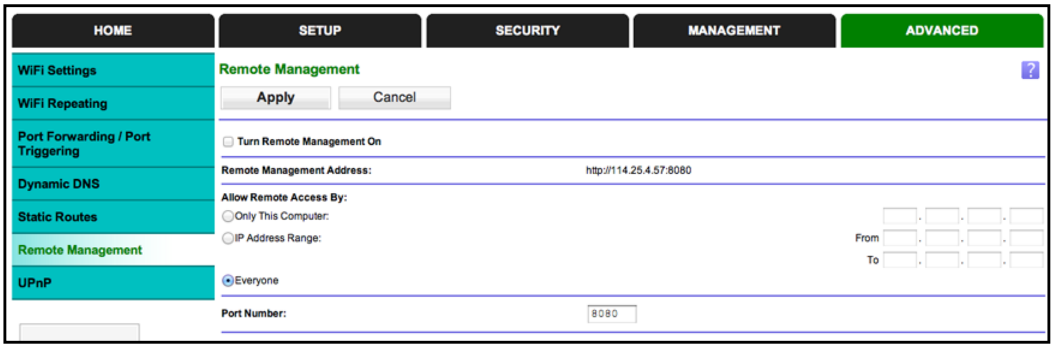
   This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your N300R router over the Internet.

➢ To set up remote management:

1. Select **Advanced > Remote Management**.



Remote Management

□ Turn Remote Management On

Remote Management Address: http://114.25.4.57:8080

Allow Remote Access By:

○ Only This Computer:

○ IP Address Range: From . . . To . . .

● Everyone

Port Number: 8080

> **Note:** *Be sure to change the router's default login password to a secure password. The ideal password contains no dictionary words from any language and contains upper-case and lower-case letters, numbers, and symbols. It can be up to 30 characters.*

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses to 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 a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
- 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 specify IP addresses, select **IP Address List** and type in the allowed IP addresses.
- To allow access from any IP address on the Internet, select **Everyone**.

4. 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 web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.
6. 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, enter **http://134.177.0.123:8080** in your browser.

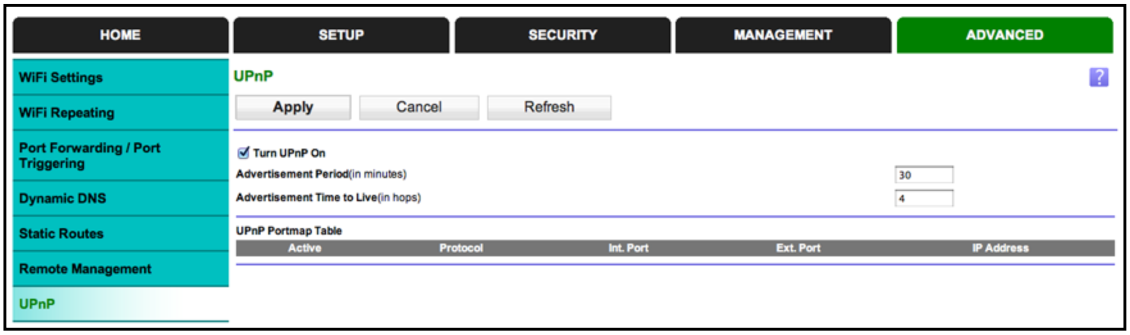
Universal Plug and Play

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.

If you use applications such as multiplayer gaming, peer-to-peer connections, or 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:**

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



☑ Turn UPnP On

Advertisement Period(in minutes) 30

Advertisement Time to Live(in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

2. 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 can 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 is 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.

7. Troubleshooting

Diagnose and solve problems

7

This chapter provides information about troubleshooting your N300 WiFi Router (N300R). After each problem description, instructions are provided to help you diagnose and solve the problem

Tip: On Networks provides helpful articles, documentation, and the latest software updates at *http://www.on-networks.com/support*.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Restore the Factory Settings and Password*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems

Sequence to Restart Your Network

If you need to restart your network, use the following sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router and computers.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the router and wait 2 minutes.
5. Turn on the computers.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

- The Internet LED on the router is on if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.
- For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is on.

Wireless Settings

If you are having trouble joining the wireless network, make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you have to add each wireless computer’s MAC address to the router’s access list.

Network Settings

If you cannot access the network, make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers need to 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.
- 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.

Troubleshooting with the LEDs

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

1. When power is first applied, verify that the Power/Test LED is on.
2. Verify that the Power/Test LED starts blinking green, indicating that the self-test is running.
3. After approximately 30 seconds, verify the following:
   - The Power/Test LED is solid green.
   - The Internet LED is on.
   - A numbered Ethernet port LED is on for any local port that is connected to a computer. This indicates that a link has been established to the connected device.

The LEDs on the front panel of the router can be used for troubleshooting.

Power/Test LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the power adapter that came in the package with your product.
- If the Power/Test LED blinks slowly and continuously, the router firmware 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 *http://www.on-networks.com/support*.

Internet or Ethernet Port LEDs Are Off

If either the Ethernet port LEDs or the Internet LED does not light when the Ethernet connection is made, check the following:

- 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.

Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 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.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. This procedure is explained in *Default Factory Settings* on page 85.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **admin**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your router as an additional router behind an existing router in your network, consider replacing the existing router.
- If you are attempting to set up your router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert ADSL or cable data into Ethernet networking information.

Cannot Access the Internet

If you can access your router but not the Internet, check to see if the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests 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 www.on-networks.com.
2. Access the router interface at **www.mywifirouter.com**.
3. Select **Management > 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 *Sequence to Restart Your Network* on page 76.

If your router is still unable to obtain an IP address from the Internet service provider (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 Internet Setup screen.
- Your ISP allows only one Ethernet MAC address to connect to the Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device and ask them to use the router's MAC address.
  - Configure your router to clone 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. You can 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.
- 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 PPPoE

If you are using PPPoE, you can troubleshoot your Internet connection over the PPPoE connection.

➢ **To troubleshoot a PPPoE connection:**

1. Log in to the router.
2. Select **Management > Router Status**.
3. Click **Connection Status**. If all of the steps indicate OK, then your PPPoE connection is up and working.

If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**. The router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshooting Internet Browsing

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

- 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, restart your computer.

  Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- Your computer might not have the router configured as its default gateway.

  Reboot the computer and verify that the router address (www.mywifirouter.com) is listed by your computer as the default gateway address.

- 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.

Changes Not Saved

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

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

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

- Does the wireless device or computer that you are using find your wireless network?

  If not, check the WiFi LED on the front of the router. It should be lit.

  If you disabled the router's SSID broadcast, then your wireless network is hidden and does not show up in your wireless client's scanning list. (By default, SSID broadcast is enabled.)
- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **Setup > WiFi Settings** (see *WiFi Setup* on page 25).

Note: *Be sure to click **Apply** if you make changes.*

Wireless Signal Strength

If your wireless device finds your network, 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 blocked by objects between the router and your computer?

Restore the Factory Settings and Password

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

- Use the Erase function of the router (see *Backup Settings* on page 56).

- Use the Reset button on the back of the router. See *Default Factory Settings* on page 85. If you restore the factory settings and the router fails to restart, or the green Power/Test LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support.

Troubleshoot Your 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. Troubleshooting a network is made easy by using the ping utility in your computer or workstation.

Test 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 Windows PC:**

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

   ping www.mywifirouter.com

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 that the numbered LAN port LED is on for the port to which you are connected.

  Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs 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.

Test 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.

➢ **To use ping:**

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.
- 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 Internet Setup 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. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your router to clone or spoof the MAC address from the authorized computer.

A. Supplemental Information

A

This appendix covers the following topics:

- *Default Factory Settings*
- *Technical Specifications*

Default Factory Settings

Table 1. N300R Router Default Factory Settings

Feature	Default Setting
Routerr login URL	http://www.mywifirouter.com
Router login (case-sensitive) printed on product label	User name: admin Password: admin
WAN MAC Address	Default hardware address (on label)
MTU Size	1500
Router LAN IP address printed on product label (also known as 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	GMT
Time zone adjusted for daylight saving time	Disabled
Allow a registrar to configure this router	Enabled
Wireless Communication	Enabled
SSID Name (on product label)	OnNetworks*XX* (where XX is two random digits)
Security	*XXXXXXXX* (8 random digits) See the product label.
Wireless Access List (MAC Filtering)	All wireless stations allowed
Broadcast SSID	Enabled
Transmission Speed	Auto*
Country/Region	United States (North America only; otherwise varies by country and region)
RF Channel	Auto
Operating mode	Up to 300 Mbps
Data rate	Best
Output power	Full

Table 1. N300R Router Default Factory Settings (continued)

Feature	Default Setting
Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests except for traffic on port 80, the http port)
Outbound (communications going out to the Internet)	Enabled (all)

**. 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 2. N300R Router Technical Specifications

Feature	Description
Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, and UPnP
AC plug is localized	110V 60 Hz or 220V50 Hz, input (localized to country of sale)
Dimensions	200 x 113 x 86.2 mm (7.9 x 4.5 x 3.4 in)
Weight	0.22 kg (0.49 lb)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Designed to conform to the following standards	FCC Part 15 Class B EN 55022/24 (CISPR 22/24) Class B EN 60950 (CE LVD) Class B EN 301 489-17 V.2.1.1 (2009) EN 301 489-1 V1.9.2 (2011) EN 300 328 V.1.7.1 (2006) EN 62311: 2008 R&TTE Directive 99/5/EC ErP 2009/125/EC

B.

Notification of Compliance

B

Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: 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

CE (!)

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 (2.4Ghz), EN301 489-17 EN60950-1

For complete DoC, visit the On Networks EU Declarations of Conformity website at:

http://www.on-networks.com/do

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*On Networks* tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *On Networks* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *On Networks* 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 *On Networks* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *On Networks* 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 *On Networks* 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 *On Networks* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *On Networks* 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 *On Networks* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *On Networks* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *On Networks* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *On Networks* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *On Networks* jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *On Networks* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym On Networks oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*On Networks* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	On Networks izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*On Networks* týmto vyhlasuje, že Radiolan spÍňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*On Networks* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *On Networks* 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 *On Networks* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*On Networks* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

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, On Networks 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 WiFi Router (N300R) complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 WiFi Router (N300R)) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

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

Industry Canada

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 & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

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

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

Index