on networks™

Easy, Reliable & Secure

N150 Wireless ADSL2+ Modem Router N150RM

User Manual

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 4 Security Settings

Chapter 5 Network Management

Chapter 6 Advanced Settings

Chapter 7 Troubleshooting

Hardware Setup

Getting to know your modem router

<div style="text-align: right">

1

</div>

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

This chapter contains the following sections:

- *Unpack Your Modem Router*
- *Position Your Modem Router*
- *Hardware Features*
- *Install the Modem Router*

Unpack Your Modem Router

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

The filter or splitter provided depends on the region.

Filter/splitter

Power adapter

N150 Modem Router

Phone cable

Ethernet cable
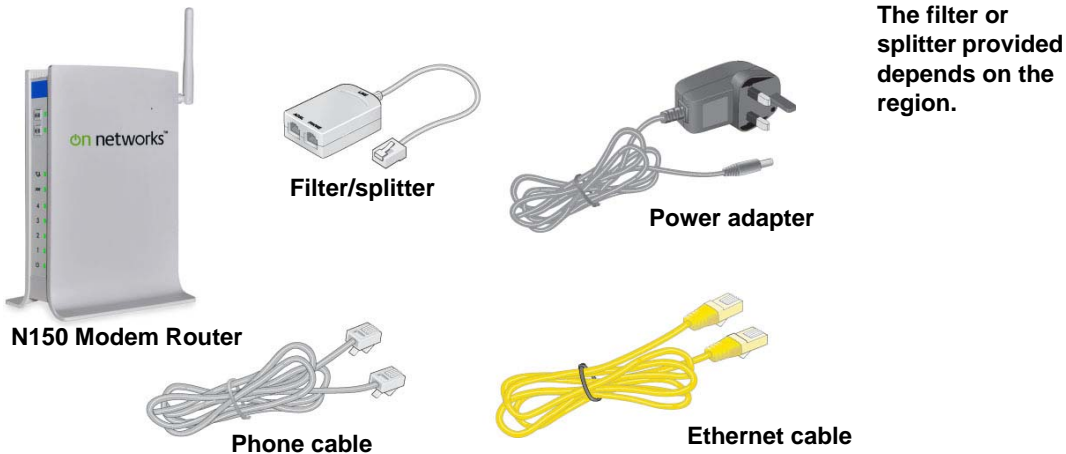
Figure 1. Check the package contents

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 Modem Router

The modem router lets you access your network from virtually anywhere within the operating range of your wireless network. This range can vary significantly depending on where you put the modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem 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 modem 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, computers, 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 modem 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 modem router front panel has buttons and status LEDs.
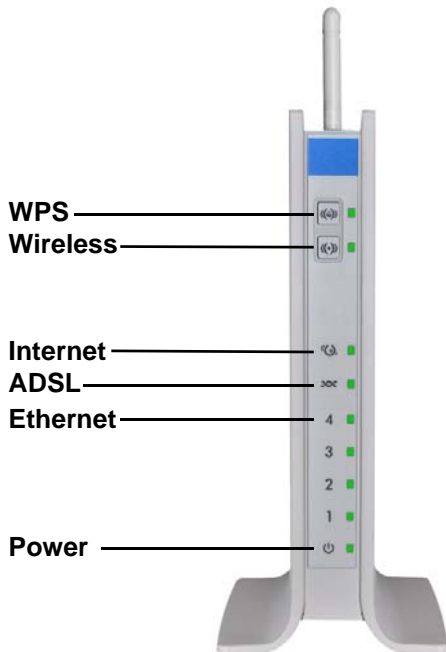
Figure 2. Modem router front panel

Table 1. Front panel LED descriptions

LED	Description
WPS	Wi-Fi Protected Setup (WPS) lets your use a wireless computer or device to join a secure wireless network without typing the password. See *WPS Method* on page 22. • **Solid green**. A WPS-capable device is connected to the router. • **Blinking green**. A WPS connection with a WPS-capable device is in process. • **Off**. No WPS connection is detected.
Wireless	You can press the Wireless button to turn the wireless radio off and on. • **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. • **Solid red**. The Internet (IP) connection failed. • **Off**. No Internet connection is detected.

Table 1. Front panel LED descriptions (continued)

LED	Description
ADSL	• **Solid green**. You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP's network-access device. • **Blinking green**. The modem router is negotiating the best possible speed on the DSL line. • **Off**. The unit is off or there is no DSL link established.
Ethernet (1-4)	• **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.
Power/ Check	• **Solid green**. Power is supplied to the modem router. • **Blinking green**. The router is starting up. • **Solid red**. The power-on self-test (POST) failed or the modem router has malfunctioned. • **Off**. Power is not supplied to the modem router.

Rear Panel

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

RJ-11 ADSL nternet port

RJ-45 Ethernet LAN ports (4)

Power On/Off
Power connector
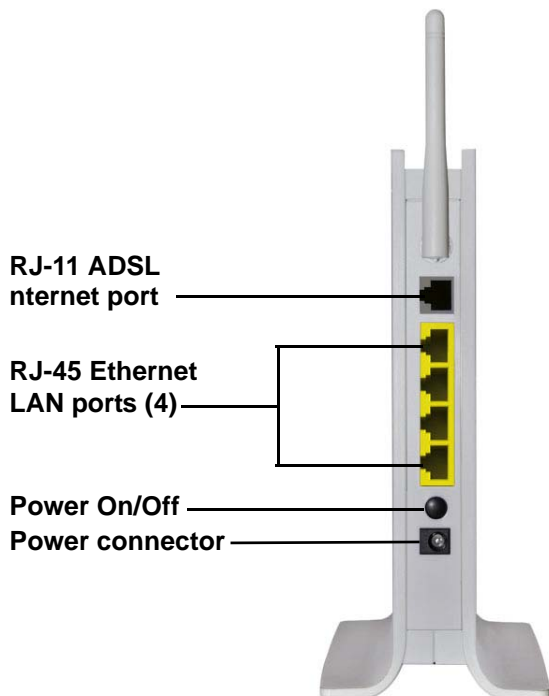
Figure 3. Modem router, rear panel

Reset Button on the Side Panel

You can use the Reset button to return the modem router to its factory settings.
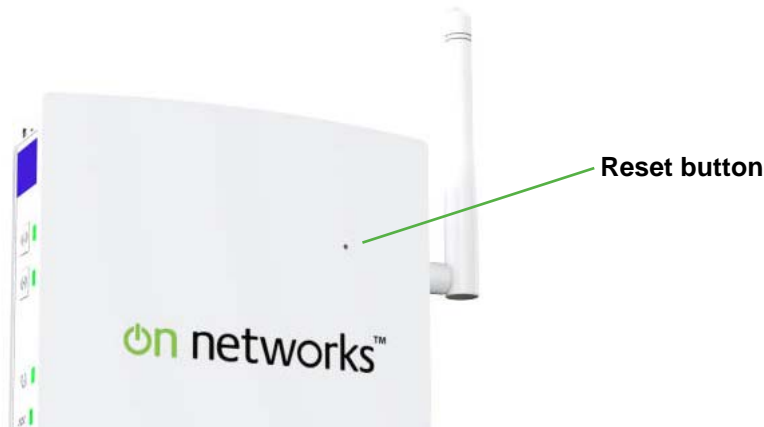
Figure 4. Reset button

➢ **To reset the modem router:**

Use a pin or paper clip to press and hold the **Reset** button for at least 7 seconds.

For information about the factory settings, see *Factory Settings* on page 72.

Label

The label on the bottom of the modem router shows the preset WiFi network name and password, login information, MAC address, and serial number.
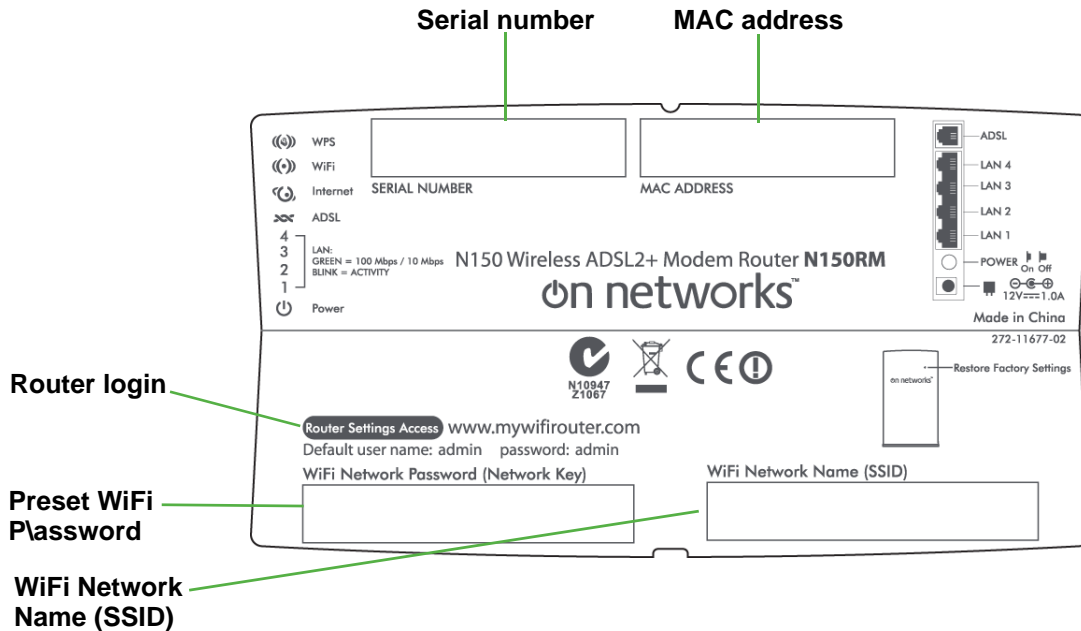
Figure 5. The label shows unique information about your modem router

Install the Modem Router

A microfilter filters DSL interference out of standard phone equipment that shares the line with DSL service. Examples of devices are telephones, fax machines, answering machines, and caller ID displays.

➢ **To install the modem router:**

1. Connect the ADSL.
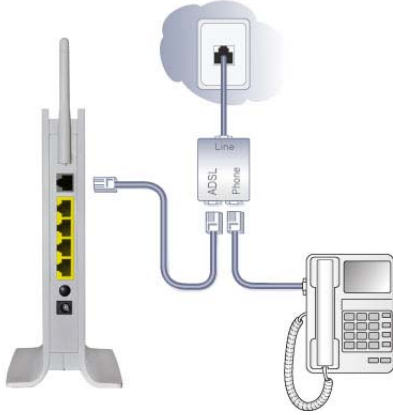
   a. Install an ADSL filter/splitter between the phone line and the phone.

   b. Connect the ADSL port of the modem router to the ADSL port of the filter/splitter.

   c. If your modem router and telephone connect to the same phone line, use an ADSL filter/splitter for every phone line in the house.

2. Add power to the modem router.
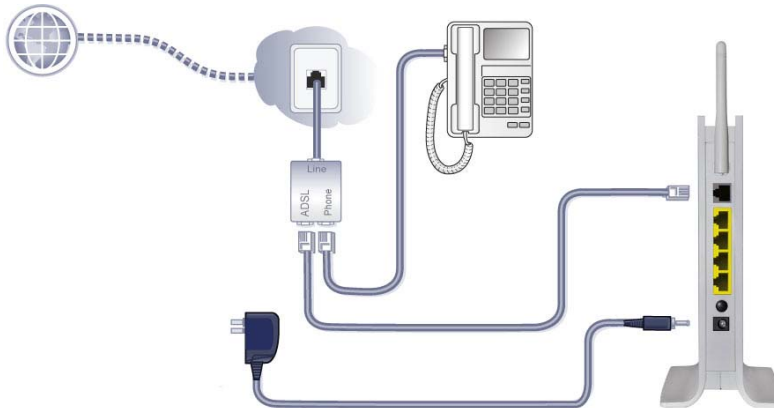
   a. Connect the power adapter to the modem router, and plug the power adapter into an outlet.

   b. Wait for the Wireless LED on the front panel to light. If none of the LEDs on the front panel are lit, press the **Power On/Off** button on the rear panel of the modem router.

3. Connect a computer.

You can use an Ethernet cable or connect wirelessly.
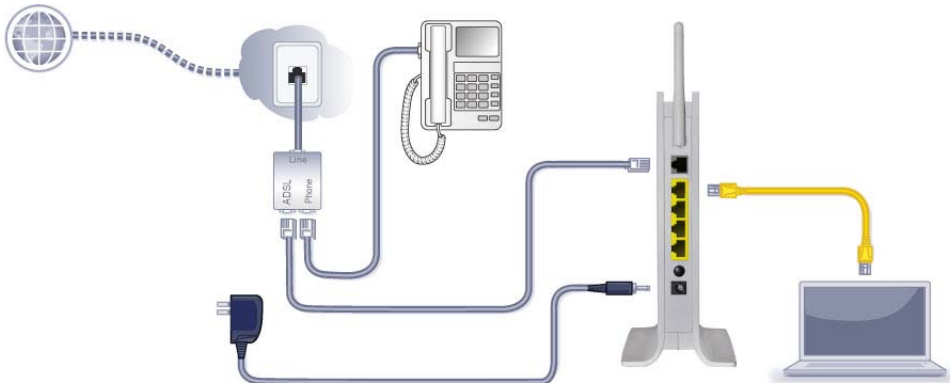
- Use the yellow Ethernet cable to connect your computer to an Ethernet port on your modem router.
- Or connect wirelessly by using the preset wireless security settings on the label on the bottom of the router.

4. Open a browser.

The first time that you connect to your modem router, the browser automatically displays a modem router screen to help you set up your Internet connection.
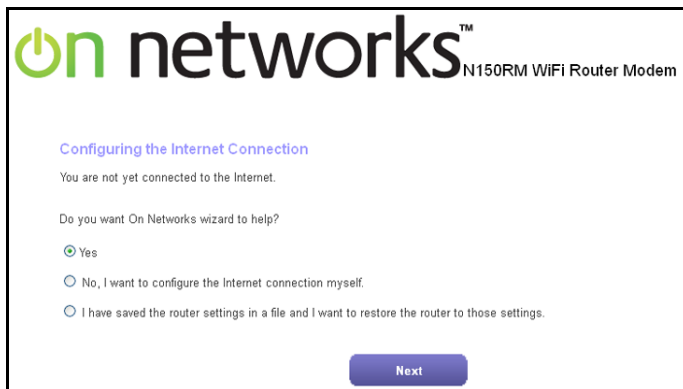
If this screen does not display, see the following section, *Tips for Connecting to the Modem Router* on page 13.

If you already connected to the modem router and used this screen, you are prompted to log in. See *Log In to the Modem Router* on page 19.

5. Connect any additional wired computers to your modem router by inserting an Ethernet cable from a computer into one of the three remaining LAN ports.

Tips for Connecting to the Modem Router

If the browser cannot display the web page:

* Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the modem router.

* Make sure that the modem router has full power, and that its Wireless LED is lit.

* Close and reopen the browser to make sure that the browser does not cache the previous page.

* Browse to **http://www.mywifirouter.com** (or **http://192.168.0.1/index.htm**).

* If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the modem router.

If the modem router does not connect to the Internet:

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.

Getting Started 2

This chapter contains the following sections:

- *Modem Router Setup Preparation*
- *Types of Logins and Access*
- *Log In to the Modem Router*
- *Home Screen (Dashboard)*
- *EZ Setup Wizard*
- *Join Your Wireless Network*

Modem Router Setup Preparation

You can set up your modem router with the Setup Wizard as described in *EZ Setup Wizard* on page 18, or manually as described in *Internet Setup (Basic Settings)* on page 22. However, before you start the setup process, you need to have your ISP information and to make sure the laptops, computers, 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 modem router setup.

Gather ISP Information

You need the following information to set up your modem 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 modem router Internet connection is set up, you no longer need to launch the ISP login program on your computer to access the Internet. When you start an Internet application, your modem 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

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.
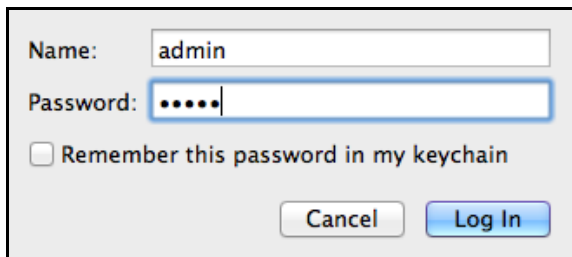
- **Modem router login** logs you in to the modem router interface.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your modem router.

Log In to the Modem Router

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

➢ **To log in to the modem router:**

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window. You can also enter **http://www.mywifirouter.com**.

Name:	admin
Password:	•••••

    ☐ Remember this password in my keychain

    Cancel   Log In

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

    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 modem router discovered newer firmware.

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

    ⚠ **WARNING:**

    To avoid corrupting the firmware, do not interrupt this process by closing the browser window, clicking a link, or loading a new page.

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

Unsuccessful Login

➤ **If you do not see the login prompt, do the following:**

1. Check the LEDs on the front of modem router to make sure that it is plugged in, its power is on. If you used an Ethernet cable between your computer and the modem router, make sure that it is connected to a LAN port.

2. If you connected the Ethernet cable and quickly launched your browser and typed in the modem 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 modem router wirelessly, during setup you can use an Ethernet cable to connect your computer so that you can log in to the modem router.

4. If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties. (For a Windows PC, see the Network Connections section of the Control Panel.) The computer should be set to obtain both IP and DNS server addresses automatically. See your computer documentation.

Log Out Manually

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

Home Screen (Dashboard)

The modem router interface lets you view or change the modem router settings. The left column has menus and their are tabs at the top.
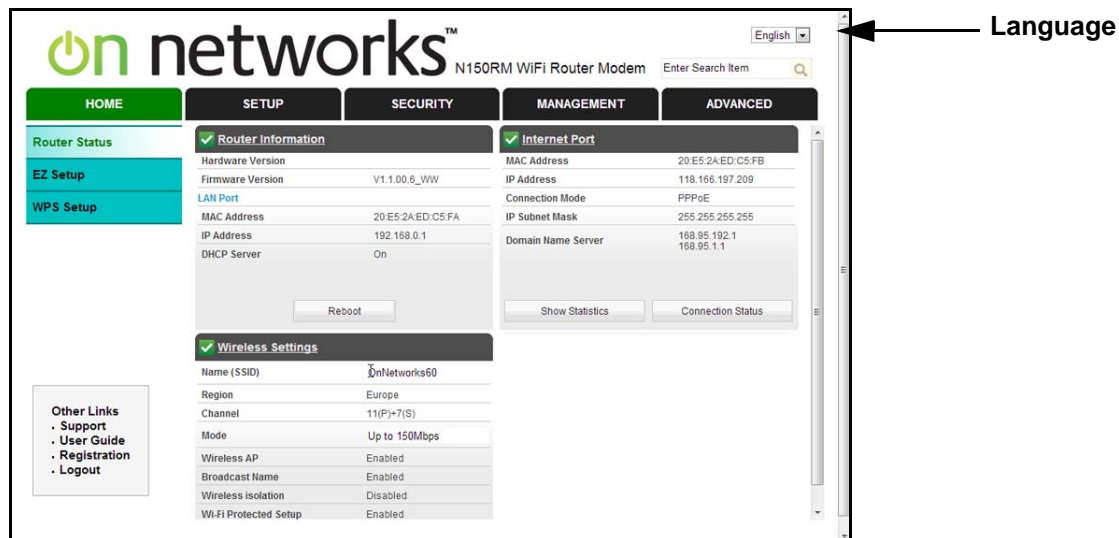
Figure 6. Dashboard (Home screen)

The Dashboard (Home screen) includes the following selections:

- **Router Status**. View the status of the modem router and its Internet connection.
- **EZ Setup Wizard**. Specify the language and location, and automatically detect the Internet connection. See *EZ Setup Wizard* on page 18.
- **WPS Setup**. Join the secure WiFi network without typing the password. See *Join Your Wireless Network* on page 19.
- **Setup tab**. Set, upgrade, and check the ISP and wireless network settings of your modem router. See *Internet Setup (Basic Settings)* on page 22. See also *Chapter 3, Modem Router Setup,* for information about preset and basic security settings.
- **Security tab**. View and configure the modem router firewall settings to prevent objectionable content from reaching your computers. See *Security Settings* on page 35.
- **Management tab**. Administer your modem router and network. See *Chapter 5, Network Management*.
- **Advanced tab**. Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Advanced Settings* on page 54. Using this menu requires a solid understanding of networking concepts.
- **Other Links**. For information, help, and product documentation, visit the support site. These links work once you have an Internet connection.

EZ Setup Wizard

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

➢ **To use the EZ Setup wizard:**

1. From the top of the modem router menu, select **EZ Setup**.

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 22.

3. If you selected Yes, click **Next**.
   - EZ Setup searches your Internet connection for servers and protocols to determine your ISP configuration.
   - EZ Setup 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 22.

➢ **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 modem router, check the Internet Protocol (TCP/IP) properties. For a Windows PC, this setting is in the Network Connections section of the Control Panel. The computer should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation.

Join Your Wireless Network

Select 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 method:**

1. Select **Home > WPS Setup**.

2. Click **Next**. The following screen lets you select the method for adding the WPS client.
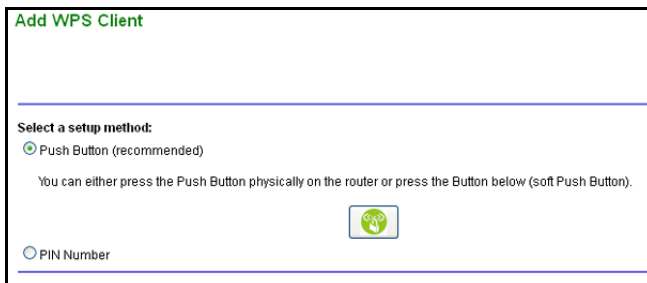
3. Select either **Push Button** or **PIN Number**. With either method, the modem router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.

4. When the PIN method screen displays, enter the client security PIN.

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

Manual Method

With the manual method, select 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 are on the modem router label. If you changed these settings, look for the network name that you used.

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

Modem Router Setup

3

This chapter contains the following sections:

- *Internet Setup (Basic Settings)*
- *Preset Security*
- *WiFi Security Basics*
- *Wireless Setup*
- *WAN Setup*
- *LAN Ports*

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 modem 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.

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

1. Select **Setup > Internet Setup**.

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, and 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 Internet Connection 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:

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

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

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

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

Internet IP Address.

When a login is required, these fields display:

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

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

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 modem router during login, select this option, and enter the IP address of your ISP primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). You can enable or disable NAT. If you disable NAT, you can also disable the firewall. The firewall cannot be disabled when NAT is enabled.

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 working. Open NAT provides a much less secured firewall, but allows almost all Internet applications to work.

Preset Security

The modem router comes with preset security. This means that the Wi-Fi network name (SSID) and the WiFi network password (network key) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **Wi-Fi network name (SSID)** identifies your network so devices can find it.
- **Passphrase** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.
- **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 25.

The Wireless Settings screen lets you view and change the preset security settings. If you 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 modem router has the security features described here and in *Security Settings* on page 35.

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

Disable SSID Broadcast

By default, the modem router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices cannot find your modem 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 computers based on their Media Access Control (MAC) addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the modem router. The wireless station MAC address filtering adds more 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 modem router by MAC address. See *Advanced Settings* on page 54 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 *Wireless Setup* on page 25.

Wireless Setup

The Wireless Settings screen lets you view or change the wireless network settings. Your preset modem router has a unique network name and password on the product label. If you 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 modem 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 modem router as described in *Use Standard TCP/IP Properties for DHCP* on page 15.
* Each computer or wireless adapter in your network must have the same SSID and wireless mode (bandwidth or data rate) as the modem 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 settings of the modem router. For example, if you select a security option that requires a passphrase, be sure to use same passphrase for each wireless computer in the network.

View or Change Wireless Settings

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

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

1. Select **Setup > Wireless Settings**.

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

Wireless Network

- **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 modem router is used. It might not be legal to operate the modem 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 150 Mbps is the default (11n supports up to 150 Mbps) and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps.

Wireless Access Point

- **Enable Wireless Access Point**. Allow the unit to work as a wireless acces point.

- **Allow Broadcast of Name (SSID)**. This feature allows the modem 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**.

- **Wireless Isolation**. If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.

Wireless Station 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. See *Restrict Access by MAC Address* on page 25.

Security Options

You can view or change the security option and passphrase. Your preset modem router is already set up with WPA2 and WPA security.

➢ **To change WPA security:**

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

   ```
   Security Options
   ○ Disable
   ○ WEP (Wired Equivalent Privacy)
   ○ WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
   ○ WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)
   ◉ Mixed WPA-PSK+WPA2-PSK
   ○ WPA-802.1x
   ```
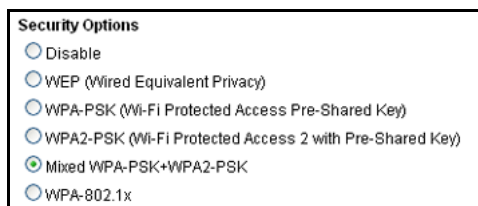
2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.

3. Click **Apply**.

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 wireless card or 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). The MAC address is typically on a label on the wireless card or 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 > Wireless Settings**, and click the **Setup Access List** to display the Wireless Card Access List.

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.

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 Attached Devices screen into the MAC Address field of this screen. Each computer that joins the wireless network is listed in the Attached Devices screen.
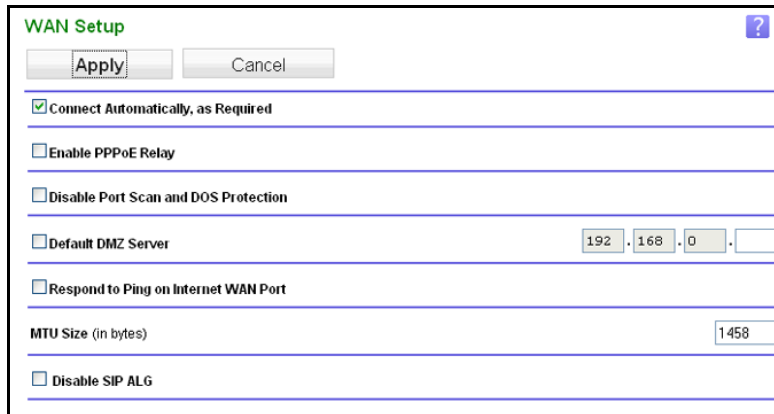
4. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

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**.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the modem router to respond to a ping on the WAN (Internet) port.

Select **Setup > WAN Setup**.

The following information is displayed:

- **Connect Automatically, as Required**. The modem router connects to the Internet automatically.

- **Enable PPPoE Relay**. When enabled, this feature allows a PPPoE client on a local computer to connect to a remote PPPoE server with the modem router acting as a relay agent.

- **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 WAN Port**. If you want the modem 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 modem router to be discovered. Do not select this check box unless you have a specific reason.

- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure that it is necessary for your ISP connection. See *MTU Size* on page 30.

- **Disable SIP ALG**. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. You can select this check box to disable the SIP ALG, which might be useful when running certain applications.

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 modem router is programmed to recognize some of these applications and to work correctly with them, but other applications 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. 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. Select **Setup > WAN Setup**.
2. Select the **Default DMZ Server** check box.
3. Type the IP address.
4. Click **Apply**.

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 example, 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 modem 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.
1458	Used in PPPoA environments.
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 **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 modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is:

- LAN IP address. **192.168.0.1**
- 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 modem 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**.

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 modem router.

- **IP Subnet Mask**. The LAN subnet mask of the modem 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 modem 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 modem 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 modem 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 modem router.

- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the modem 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 modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings. See *Address Reservation* on page 34.

Use the Modem Router as a DHCP Server

By default, the modem 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 modem router. The modem 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 modem router are satisfactory.

You can specify the pool of IP addresses that the modem router assigns by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the modem router's LAN IP address. Using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

The modem 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 modem router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Internet Setup screen; otherwise, the modem 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 you clear this check box and no other DHCP server is on your network, you need to set your computers' IP addresses manually so that they can access the modem 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 modem 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 modem router's LAN subnet, such as 192.168.0.x.)
3. Type the MAC address of the computer or server.

   Tip: If the computer is already 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 modem 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**.

Security Settings

4

This chapter contains the following sections:

- *Block Internet Sites*
- *Block Services*
- *Firewall Rules to Control Network Access*
- *Set the Time Zone*
- *Schedule Services*
- *Set Up Email Alerts*

Block Internet Sites

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

➢ **To block traffic:**

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

2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.

3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

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

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

➢ **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.

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.

Block Services

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

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

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

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

2. Click the **Add Services** button. If you want to change a service, select it and click **Edit Service**.
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.

Firewall Rules to Control Network Access

Your modem 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.

Set Up Firewall Rules

The Firewall Rules screen lets you add custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence.

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

➢ **To set up firewall rules:**

1. Select **Security > Firewall Rules**.

2. To add an outbound rule, click **Add** under Outbound Services. To edit or delete a rule, select its button on the left side and click **Edit** or **Delete**.

3. To change the order of precedence:

    a. Select the button on the left side of the rule and click **Move**.

    b. At the prompt, enter the number of the new position and click **OK**.

4. To open or close instant messaging, select one of the following radio buttons:

    •   **Close IM Ports**. Disables instant messaging traffic.

    •   **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.

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

Set the Time Zone

The modem 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**.

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 **Automatically Adjust for daylight savings time** check box to add one hour to standard time.

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

Schedule Services

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

➢ **To schedule services:**

1. Select **Security > Schedule**.

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 > E-mail** to display the following screen:

Figure 7. E-Mail screen

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

- **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.

- **My mail server requires authentication**. If you use an outgoing mail server provided by your current ISP, you do not need to select this check box. If you use an email account that your ISP did not provide, select this check box, 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**. This setting specifies which day of the week to send the log. This is relevant when the log is sent weekly.

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

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

Network Management

5

This chapter contains the following sections:

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

Upgrade the Firmware

The modem router firmware (routing software) is stored in flash memory. By default, when you log in to your modem 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 modem 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 modem router performs the check and notifies you if an upgrade is available or not.

Firmware Upgrade Assistant

Please wait a moment...

Cancel
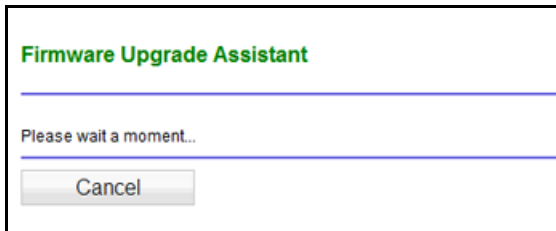
➢ **To check the firmware automatically:**

1. Click **Yes** to allow the modem router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your modem router restarts.

2. Go to the N150R support page and read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

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

Check for Firmware Upgrades

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

➢ **To check for newer versions of firmware:**

⚠️ **WARNING:**

> **When uploading firmware to the modem 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 and select **Management > Upgrade Firmware**.

```
Firmware Upgrade                                    [?]


Check for New Version from the Internet           [ Check ]

Locate and Select the Upgrade File from your Hard Disk:
[                              ] [ Browse... ]

[  Upload  ]        [  Cancel  ]
```

2. Click **Browse**, and locate the firmware image that you downloaded to your computer (the file ends in .img or .chk).

3. Click **Upload** to send the firmware to the router.

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

Backup Settings

The modem 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 **Management > 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 modem router.

Upon completion, the modem router reboots.

Erase

Click the **Erase** button to reset the modem router to its factory default settings. Erase sets the password to **admin** and the LAN IP address to **192.168.0.1**, and enables the modem router's DHCP.

Set the Password

For security reasons, the modem router has its own user name of admin. The password defaults to admin. You can and should change the password to one that is secure but also easy to remember. The ideal password contains no dictionary words from any language and is a mixture of uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

The modem 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 and Access* on page 16 for more information about login types.

➢ **To change the password:**

1. Select **Management > Set Password**.

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 modem router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Backup Settings* on page 46 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 screen:**

Select **Management > Router Status**.

ADSL Port Settings

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

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

Network Type. The value (such as PPPoA) depends on your ISP.

IP Subnet Mask. The DSL port IP subnet mask.

Gateway IP Address. The IP address assigned to the modem router.

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

LAN Port (Local Ports)

MAC Address. The modem router LAN port Ethernet MAC address.

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

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

IP Subnet Mask. The subnet mask associated with the LAN IP address.

Modem Settings

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

Modem Status. The status of the modem connection on the DSL line.

Downstream Connection Speed. The connection speed of the ADSL connection from the phone company to your Router.

Upstream Connection Speed. The connection speed of the ADSL connection from your Router to the phone company.

VPI. The VPI setting.

VCI. The VCI setting.

Wireless Port Settings

See *Wireless 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 modem 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 00:14:43							
Port	**Status**	**TxPkts**	**RxPkts**	**Collisions**	**Tx B/s**	**Rx B/s**	**Up Time**
WAN	PPPoE	874	732	0	99	196	00:13:05
LAN	10M/100M	4630	4327	0	3264	516	00:14:23
WLAN	54M/65M/150M	408	0	0	52	0	00:14:26

ADSL Link	**Downstream**	**Upstream**
Connection Speed	8512 Kbps	768 Kbps
Line Attenuation	28.6 dB	15.5 dB
Noise Margin	9.1 dB	16.0 dB

Poll Interval : [10] (secs)   Set Interval   Stop

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.

Connection Status

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

- • **Connection Time**. The time elapsed since the last connection to the Internet through the DSL port.
- • **Connecting to server**. The connection status.
- • **Negotiation**. On or Off.
- • **Authentication**. On or Off.
- • **Getting IP Address**. The IP address assigned to the WAN port by the ISP.
- • **Betting Network Mask**. The subnet mask assigned to the WAN port by the ISP.

View Attached Devices

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

➢ **To view attached devices:**

Select **Management > Attached Devices**.

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

Logs

The modem 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 shows you when someone on your network tries to access a blocked site. If you enable email notification, you receive these logs in an email message.

➢ **To view the log:**

Select **Management > Logs**. A screen similar to the following displays:
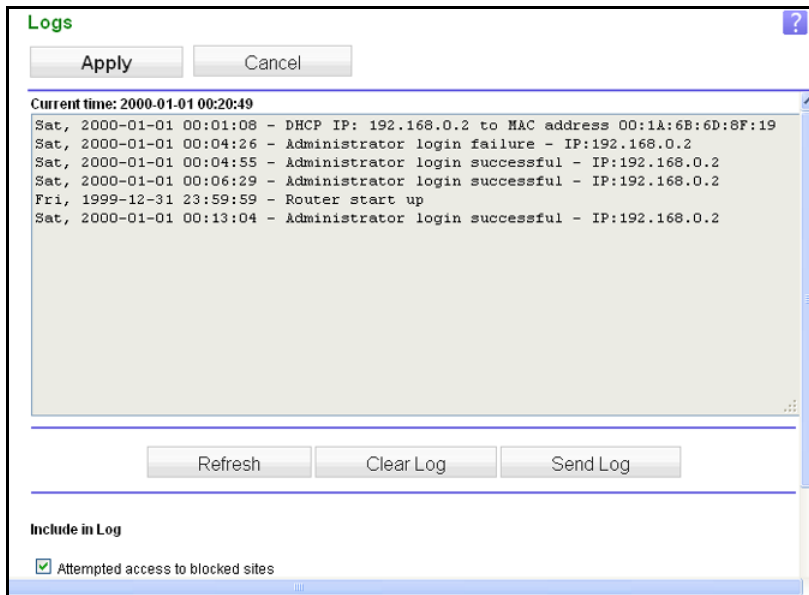
The Include in Log check boxes allow you to select which events are logged. The security log entries include the following information:

- **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.

Diagnostics

During normal operation, you do not need to use diagnostics.

➢ **To use diagnostics:**

Select **Management > Diagnostics**.

The following features are available on the Diagnostics screen.

- **Ping an IP address**. Use this to send a ping packet request to the specified IP address. Ping can be used to test a connection. If the request times out (no reply is received), this usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping.

- **Perform a DNS Lookup**. A Domain Name Server (DNS) converts Internet names to IP addresses. If you need the IP address of a server on the Internet, you can do a DNS lookup to find the IP address.

- **Display the Routing Table**. View the internal routing table. This information is used by technical support and other staff who understand routing tables.

- **Reboot the Router**. Perform a remote reboot (restart). You can do this if the modem router seems to have become unstable or is not operating normally.

Note: Rebooting stops any network connections to the modem router or through the modem router. Connections to the Internet are automatically reestablished when possible.

Advanced Settings

6

This chapter describes the advanced features of your modem router. The information is for readers with advanced networking knowledge who want to set the modem 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 Wireless Settings*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*

Advanced Wireless Settings

➢ **To view the Advanced Wireless Settings screen:**

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

The following settings are available in this screen:

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

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 modem 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.

WLAN.

Name (SSID). The service set ID, also known as the wireless network name.

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

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

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

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

Security. Indicates if security is configured on the wireless modem router, and if so, what type of security is configured.

WPS Settings.

Router's PIN. The number that you can use from a wireless computer or device to join the wireless network through WPS. If the modem router detects attempts to use the PIN to break into the network, the PIN is disabled. To enable the PIN, clear the **Disable Router PIN** check box and click **Apply**.

Keep Existing Wireless Settings. By default, this check box is selected so that the SSID and wireless security settings stay the same when a new wireless computer or device uses WPS to join the wireless network.

If you clear the Keep Existing Wireless Settings check box, the next time a someone uses WPS to join the wireless network, the modem router generates a new random SSID and WPA/WPA2 passphrase.

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). Most Internet accounts use dynamically assigned IP addresses. 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 modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. If you register for an account and set up the modem router, whenever your ISP-assigned IP address changes, your modem 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 modem router at http://hostname.dyndns.org.

➢ **To set up Dynamic DNS:**

1. Register for an account with one of the Dynamic DNS service providers whose web addresses are in the Service Provider list.

2. Select **Advanced > Dynamic DNS**.

3. Select the **Use a Dynamic DNS Service** check box.

4. Enter the web address of your Dynamic DNS service provider. For example, for DynDNS.org, type **www.dyndns.org**.

5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.

6. 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.

7. Type the password (or key) for your Dynamic DNS account.

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

Static Routes

Static routes provide additional routing information to your modem router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple modem 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 modem router on your home network for connecting to the company where you are employed. This modem router's address on your LAN is 192.168.0.100.

*   Your company's network address is 134.177.0.0.

When you first configured your modem 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 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem 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 modem router that 134.177.0.0 should be accessed through the ISDN modem router at 192.168.0.100. In this example:

*   The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.

*   The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN modem router at 192.168.0.100.

*   A metric value of 1 will work since the ISDN modem 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:

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 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 modem router on the same LAN segment as the N150RM modem router.

8. Type a number from 1 through 15 as the metric value.

   This value represents the number of modem 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 N150RM modem router over the Internet.

➢ **To set up remote management:**

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

> **Note:** *Be sure to change the modem router's default login password to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase 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 that are allowed to access the modem router management interface remotely

> **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 of the computer that is allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP addresses 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 web 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 modem router from the Internet, type your modem 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.

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 modem router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the modem router.

Advertisement Period. The advertisement period is how often the modem 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 more 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, 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 accessing the modem 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.

Troubleshooting

7

Diagnose and solve problems

This chapter provides information about troubleshooting your modem router. After each problem description, instructions are provided to help you diagnose and solve the problem.

This chapter contains the following sections:

Troubleshoot with the LEDs

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

1. When power is first applied, the Power LED lights.

2. After approximately 10 seconds, the Ethernet and ADSL LEDs light as follows:

   a. The Ethernet port LEDs light for any local ports that are connected.

   b. The ADSL LED lights to indicate that there is a link to the connected device.

   c. If a LAN port is connected to a 100 Mbps device, verify that the LAN port's LED is green. If the LAN port is 10 Mbps, the LED is amber.
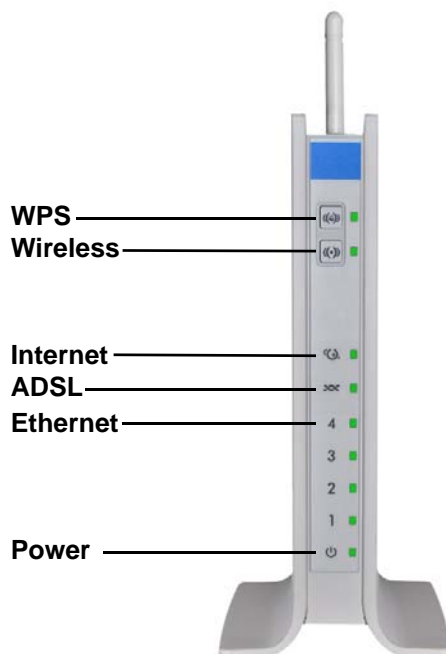
Figure 8. Front panel LEDs

Power LED Is Off

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

- Check that the power cord is correctly connected to your modem router and the power supply adapter is correctly connected to a functioning power outlet.

- Check that you are using the power adapter supplied in the package with this product.

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

Power LED Is Red

When the modem router is turned on, it performs a power-on self-test during which time the Power LED turns red. If the Power LED does not turn green within a minute or so or if it turns red at any other time during normal operation, there is a fault within the modem router.

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

- Turn the power off and on one more time to see if the modem router recovers.
- Clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 72. This sets the modem router's IP address to 192.168.0.1.

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

Ethernet LED Is Off for a Connected Port

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

- The Ethernet cable connections are secure at the modem router and at the hub or workstation.
- The power is turned on to the connected hub or workstation.
- You are using the correct cable.

Cannot Log In to the Modem Router

If you are unable to log in to the modem 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 modem router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router, and reboot your computer.
- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Factory Settings* on page 72.

- 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 you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

Troubleshoot the Internet Connection

If your modem router is unable to access the Internet, check the ADSL connection, then the WAN TCP/IP connection.

ADSL Link

If your modem router is unable to access the Internet, first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

ADSL Link LED Is Green

If your ADSL link LED is green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

ADSL Link LED Is Blinking Green

If your ADSL link LED is blinking green, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

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

ADSL Link LED Is Off

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

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

- Check that the telephone company has made the connection to your line and tested it.

- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings are correct.
- Check if your ISP has a problem—it might not be that the modem router cannot connect to the Internet, but rather that your ISP that cannot provide an Internet connection.

Obtaining an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green, see if the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router requests an IP address from the ISP. You can determine whether the request was successful using the browser interface.

➢ **To check the Internet IP address from the browser interface:**

1. Launch your browser, and select an external website.
2. Access the modem router's configuration at http://192.168.0.1.
3. On the Home screen (Router Status), check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

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

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, *PPPoE or PPPoA* .
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the modem router's MAC address.
  - Configure your modem router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

PPPoE or PPPoA

➢ **To debug the PPPoE or PPPoA connection:**

1. Log in to the modem router.

2. On the Home screen (Router Status), click the **Connection Status** button.

3. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.

4. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The modem 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 modem router does not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Internet Browsing

If your modem 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 when you set up the modem router, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

• Your computer might not have the modem router configured as its TCP/IP modem router.

If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

TCP/IP Network Does Not Respond

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

Test the LAN Path to Your Modem Router

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

➢ **To ping the modem router from a PC running Windows 95 or later:**

1. From the Windows task bar, click the **Start** button, and select **Run**.

2. In the field provided, type **ping** followed by the IP address of the modem router, as in this example:

   ping 192.168.0.1

3. Click **OK**.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   `Request timed out`

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

   - Wrong physical connections
     - Make sure that the Ethernet port LED is on. If the LED is off, follow the instructions in *Ethernet LED Is Off for a Connected Port* on page 64.
     - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and modem router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
     - Verify that the IP address for your modem router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

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

```
ping -n 10 IP address
```

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

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Modem Router* on page 68 display. If you do not receive replies:

- Check that your PC has the IP address of your modem router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the modem router is listed as the default router.

- Check that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single PC connected to that modem. In this case, configure your modem router to clone or spoof the MAC address from the authorized PC.

Changes Not Saved

If the modem router does not save the changes you make in the modem 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.

Incorrect Date or Time

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

- Date shown is January 1, 2000. This means the modem router has not yet reached a network time server. Check that your Internet access is configured correctly. If you have

just finished setting up the modem router, wait at least 5 minutes, and check the date and time again.

- Time is off by one hour. This modem has automatic DST adjustment. To use this feature, in the Schedule screen, select the **Automatically adjust for daylight savings time** check box and click **Apply**.

Supplemental Information

A

This appendix covers the following topics:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the modem router to its factory settings. Use the end of a paper clip or some other similar object to press and hold the **Reset** button for at least 7 seconds.
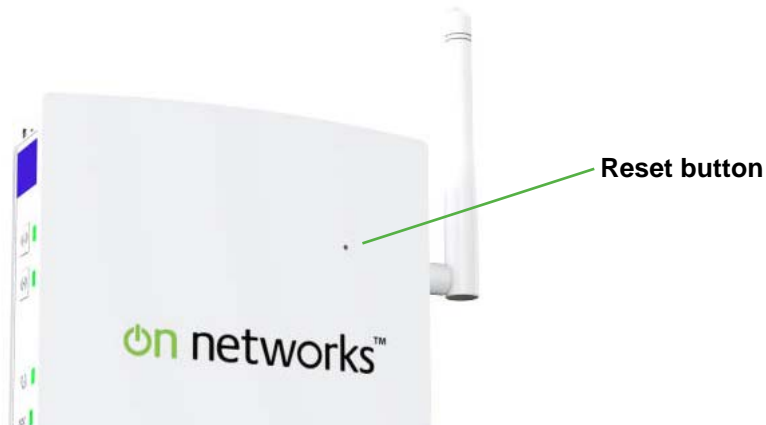
Reset button

Figure 1. Reset button

The modem router resets, and returns to the factory settings, as shown in the following table.

Table 1. Factory default settings

Feature		Default Behavior
Router Login	User login URL	http://www.mywifirouter.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	admin
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1458
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled

Table 1. Factory default settings (continued)

Feature		Default Behavior
Local network (LAN) continued	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID name	*OnNetworksXX* (where XX are two random digits) Can be found on the label on the bottom of the unit.
	WiFi password	*XXXXXXXX* (8 random digits)
	Security	Mixed WPA-PSK + WPA2-PSK
	Broadcast SSID	Enabled
	Country/region	Europe
	RF channel	Auto
	Operating mode	Up to 150 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Pre-Shared Key
	Wireless card access list	All wireless stations allowed

Technical Specifications

Table 2. Technical specifications

Feature	Description
Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
AC plug is localized	110V-220V, 50/60 Hz, input
Dimensions	200 x 113.4 x 86.2 mm (7.9 x 4.5 x 3.4 in.)
Weight	0.28 kg (0.62 lb)
Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	90% maximum relative humidity, noncondensing
Regulatory compliance	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 V1.7.1 (2006) K21:ITU-T K.21- 07/2003 TBR21: TBR21 January 1998
Interface specifications	LAN: 10BASE-T or 100BASE-Tx, RJ-45 WAN: ADSL, dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A hardware or Annex B hardware ITU G.992.5 (ADSL2+)

Notification of Compliance

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

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 the complete EU Declarations of Conformity, visit *http://www.on-networks.com/doc.*

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*On Networks* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *On Networks Inc.* 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 Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *On Networks Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *On Networks Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *On Networks Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *On Networks Inc.* 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 Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *On Networks Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *On Networks Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *On Networks Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *On Networks Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *On Networks Inc.*, 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 Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym On Networks Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*On Networks Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	On Networks Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*On Networks Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*On Networks Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *On Networks Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *On Networks Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*On Networks Inc.* 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, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N150 WiFi Router (N150R) 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 (N150 WiFi Router (N150R)) 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