



Wireless N Router

**DX-NRUTER**

**USER GUIDE**

# Dynex DX-NRUTER Wireless N Router

## Contents

Introduction .....	2
Product features .....	3
Setting up your wireless router.....	8
Troubleshooting .....	55
Legal notices .....	67
One-Year Limited Warranty .....	69

## Introduction

Thank you for purchasing the Dynex DX-NRUTER Wireless N Router. The easy installation and setup will have you networking wirelessly in minutes. Be sure to read through this User Guide completely, and pay special attention to the section entitled “Product features” on page 3.

## Benefits of a home network

Your home network will let you:

- Share one high-speed Internet connection with all the computers in your home
- Share resources, such as files, and hard drives among all the connected computers in your home
- Share a single printer with the entire family
- Share documents, music, video, and digital pictures
- Store, retrieve, and copy files from one computer to another
- Simultaneously play games online, check Internet e-mail, and chat

## Advantages of a wireless network

Here are some of the advantages of setting up a Dynex wireless network:

- **Mobility**—You will no longer need a dedicated “computer room” — now you can work on a networked laptop or desktop computer anywhere within your wireless range.
- **Easy installation**—Dynex’s Setup Assistant makes setup simple.
- **Flexibility**—Set up and access printers, computers, and other networking devices from anywhere in your home.
- **Easy expansion**—The wide range of Dynex networking products lets you expand your network to include devices such as printers and gaming consoles.
- **No cabling required**—You can spare the expense and hassle of retrofitting Ethernet cabling throughout the home or office.

- **Widespread industry acceptance**—Choose from a wide range of interoperable networking products.
- **N wireless technology**—Your router uses a new smart-antenna technology called Multiple Input Multiple Output (MIMO). N wireless complies with the IEEE draft 802.11n specification. It increases speed, range, reliability, and spectral efficiency for wireless networking systems.

## Product features

In minutes you will be able to share your Internet connection and network your computers. The following is a list of features that make your router an ideal solution for your home or small office network.

**Works with Both PCs and Mac® Computers**—Your router supports a variety of networking environments including Mac OS® X v10.x, Linux®, Windows® 98, Windows® 2000, Windows XP®, Windows Vista®, and others. All that is needed is an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

**Front-Panel LED Display**—Lighted LEDs on the front of your router indicate which functions are in operation. You'll know at-a-glance whether your router is connected to the Internet. This feature eliminates the need for advanced software and status-monitoring procedures.

**Web-Based Advanced User Interface**—You can set up your router's advanced functions easily through your Web browser, without having to install additional software onto the computer. There are no disks to install or keep track of and you can make changes and perform setup functions from any computer on the network quickly and easily.

**NAT IP Address Sharing**—Your router employs Network Address Translation (NAT) to share the single IP address assigned to you by your Internet Service Provider while saving the cost of adding IP addresses to your Internet service account.

**SPI Firewall**—Your router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect, and fragment flooding.

**Integrated 10/100 4-Port Switch**—Your router has a built-in, 4-port network switch to allow your wired computers to share printers, data and MP3 files, digital photos, and much more. The switch features automatic detection so it will adjust to the speed of connected devices. The switch will transfer data between computers and the Internet simultaneously without interrupting or consuming resources.

**Universal Plug-and-Play (UPnP) Compatibility**—UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant.

**Support for VPN Pass-Through**—If you connect to your office network from home using a VPN connection, your router will allow your VPN-equipped computer to pass through your router and to your office network.

**Built-In Dynamic Host Configuration Protocol (DHCP)**—Built-In Dynamic Host Configuration Protocol (DHCP) on-board makes for the easiest possible connection of a network. The DHCP server will assign IP addresses to each computer automatically so there is no need for a complicated networking setup.

**Setup Assistant**—The Setup assistant takes the guesswork out of setting up your router. This automatic software determines your network settings for you and sets up your router for connection to your Internet Service Provider (ISP). In a matter of minutes, your router will be up and running on the Internet.

*Note: Setup Assistant software is compatible with Windows 2000, Windows XP, Windows Vista, and Mac OS X 10.x. If you are using another operating system, your router can be set up using the Alternate Setup Method described in this User Guide (see "Alternative setup method" on page 16.*

**Integrated N Wireless Access Point**—N MIMO is an exciting new wireless technology based on the draft IEEE 802.11n specification. It employs MIMO (Multiple Input Multiple Output) smart-antenna technology that achieves data rates up to 300 Mbps. Actual throughput is typically lower than the connected data rate and will vary depending on your networking environment.

*Note: The standard transmission rate of 270 Mbps is the physical data rate. Actual data throughput will be lower.*

**MAC Address Filtering**—For added security, you can set up a list of MAC addresses (unique client identifiers) that are allowed access to your network. Every computer has its own MAC address. Simply enter these MAC addresses into a list using the Web-Based Advanced User Interface and you can control access to your network.

## Package contents

- Dynex N Wireless Router
- Quick Installation Guide
- Installation software CD
- RJ-45 Ethernet cable
- Power supply
- User Guide on Setup Assistant CD

## System requirements

- Broadband Internet connection such as a cable or DSL modem with RJ45 (Ethernet) connection
- At least one computer with an installed network interface adapter
- TCP/IP networking protocol installed on each computer
- RJ-45 Ethernet networking cable
- Internet browser



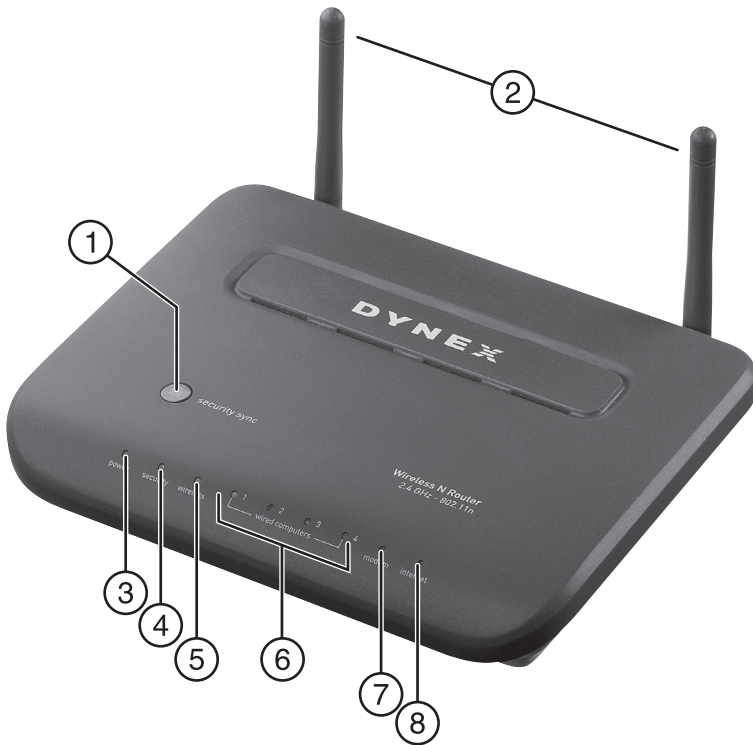
## Setup Assistant software system requirements

- A computer running Windows 2000, Windows XP, or Windows Vista or running Mac OS X v10.x
- Minimum 1 GHz processor and 128 MB RAM
- Internet browser

## Components

Your router has been designed to be placed on a desktop. All of the cables exit from the rear of your router for better organization and utility. The LED indicators are easily visible on the front of your router to provide you with information about network activity and status.

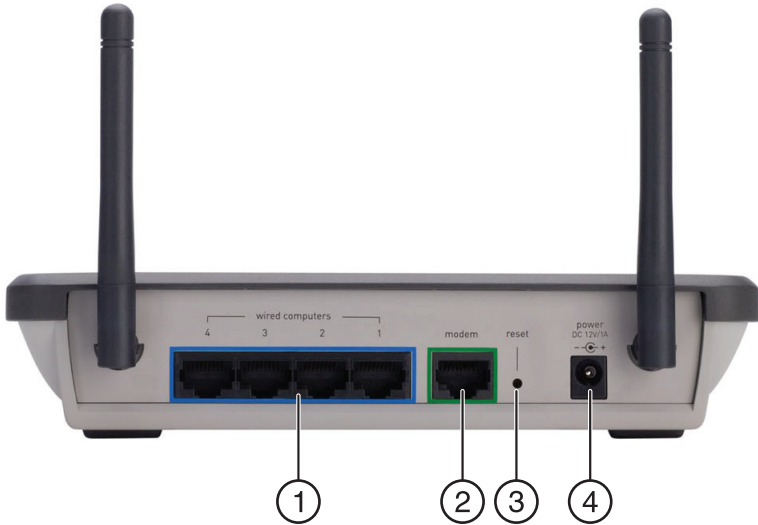
### Front panel



#	Component	Description
1	Security Sync button	Push and hold this button for three seconds, then initiate the Security Sync (WPS) procedure on the client device within two minutes. Your client will automatically exchange the security information and be added to your wireless network.
2	Antenna	Lets your router communicate with a wireless client (card or USB adapter).

#	Component	Description
3	Power/ready LED	<p>When you apply power to your router or restart it, a short period of time elapses while your router boots up. During this time, the Power/Ready LED blinks. When your router has completely booted up, the Power/Ready LED becomes a SOLID light, indicating your router is ready for use.</p> <p>Off—Router is off            Blinking Green—Router is booting up            Solid Green—Router is ready</p>
4	Security Sync LED	<p>Lights to indicate that WPS has been activated.</p> <p>Blinking Green—Your router is searching for a WPS client to connect with.            Solid Green—The secure connection has been established with the client.</p>
5	Wireless network LED	<p>Off—The wireless network is off            Solid Green—The wireless network is ready            Blinking Green—Network activity</p>
6	Wired computer status LEDs	<p>These LEDs are labeled 1-4 and correspond to the numbered ports on the rear of your router. When a computer is properly connected to one of the wired computer ports on the rear of your router, the LED will light.</p> <p>Off—The wireless network is off            Solid Green—A 10base-T device is connected            Solid Orange—A 100base-T device is connected            Blinking—Port activity</p>
7	Modem status LED	<p>This LED lights green to indicate that your modem is connected properly to your router. It blinks rapidly when information is being sent over the port between your router and the modem.</p> <p>Off—No WAN link            Solid Green—Good WAN link            Blinking Green—WAN activity</p>
8	Internet LED	<p>This unique LED shows you when your router is connected to the Internet. When the light is OFF, your router is not connected to the Internet. When the light is blinking, your router is attempting to connect to the Internet. When the light is solid green, your router is connected to the Internet. When using the “Disconnect after x minutes” feature, this LED becomes extremely useful in monitoring the status of your router’s connection.</p> <p>Off—Router is not connected to the Internet            Blinking Green—Router is attempting to connect to the Internet            Solid Green—Router is connected to the Internet</p>

### Back panel



#	Component	Description
1	Wired computer ports - Blue	Connect your wired (non-wireless) computers to these ports. These ports are RJ-45, 10/100 auto-negotiation, auto-uplinking ports for standard UTP category 5 or 6 Ethernet cable. The ports are labeled 1 through 4. These ports correspond to the numbered LEDs on the front of your router.
2	Modem port - Green	This port is for connection to your cable or DSL modem. Use the cable that was provided with the modem to connect the modem to this port. Use of a cable other than the cable supplied with the cable modem may not work properly.
3	Reset button	The <b>Reset</b> button is used in rare cases when your router may function improperly. Resetting your router restores your router's normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the Reset button. Use the restore option in instances where you may have forgotten your custom password. <b>Resetting your router</b> —Push and release the <b>Reset</b> button. The lights on your router will momentarily flash. The Power/Ready light will begin to blink. When the Power/Ready light becomes solid again, the reset is complete. <b>Restoring the Factory Defaults</b> —Press and hold the <b>Reset</b> button for at least 10 seconds, then release it. The lights on your router will momentarily flash. The Power/Ready light will begin to blink. When the Power/Ready light becomes solid again, the restore is complete.
4	Power jack	The 5 V DC power supply plugs into this jack.

# Setting up your wireless router

## Modem requirements

Your cable or DSL modem must be equipped with an RJ-45 Ethernet port. Many modems have both an RJ-45 Ethernet port and a USB connection. If you have a modem with both Ethernet and USB, and are using the USB connection at this time, you will be instructed to use the RJ-45 Ethernet port during the installation procedure. If your modem has only a USB port, you can request a different type of modem from your ISP, or you can, in some cases, purchase a modem that has an RJ-45 Ethernet port on it.

***Important:** Always install your router first! If you are installing numerous network devices for the first time, it is important that your router is connected and running before attempting to install other network components such as notebook cards and desktop cards.*

## Setup assistant

Dynex has provided our Setup Assistant software to make installing your router a simple and easy task. You can use it to get your router up and running in minutes. The Setup Assistant requires that your computer be connected directly to your cable or DSL modem and that the Internet connection is active and working at the time of installation. If it is not, you must use the "Alternative setup method" section on page 16 to configure your router. Additionally, if you are using an operating system other than Windows 2000, Windows XP, Windows Vista, or Mac OS X v10.x, you must set up your router using the "Alternative setup method" section on page 16.

## Hardware connections

### To connect the hardware:

- 1 Unplug your modem's power cord. Put your router next to the modem and raise your router's antenna.
- 2 Locate the networking cable that connects your modem and computer. Unplug that cable from your modem, and plug it into any gray port on the back of your router.
- 3 Find your new networking cable (included in the box with your router) and connect it to the yellow port on the back of your router. Connect the other end to your modem, in the port that is now free.
- 4 Plug in your modem's power cord. Wait 60 seconds for the modem to start up. Plug your router's power supply into the black port on the back of your router. Plug the other end into the wall outlet.
- 5 Wait 20 seconds for your router to start up. Look at the display on the front of your router and make sure the **Wired** and **Router** icons are lit up in green. If they are not, recheck your connections.

## Running the Setup Assistant

### To run the Setup Assistant:

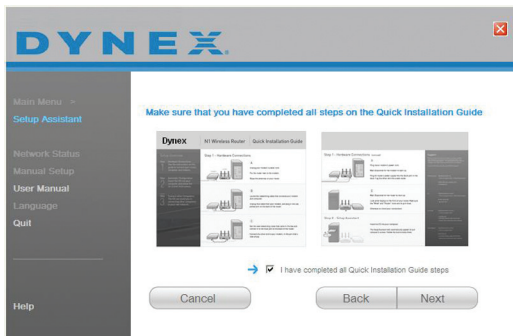
- 1 Shut down any programs that are running on your computer at this time.
- 2 Turn off any firewall or Internet-connection-sharing software on your computer.
- 3 Insert the included CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Click **GO** to run the Setup Assistant, then follow the on-screen instructions.



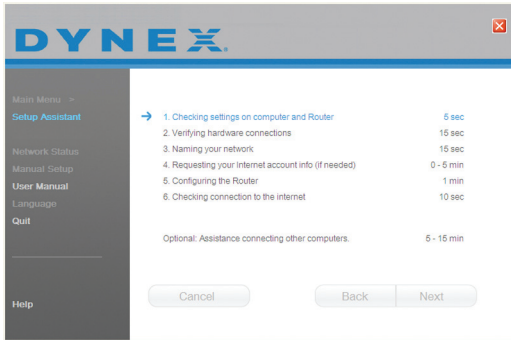
**Important:** Run the Setup Assistant from the computer that is directly connected to your router.

**Note for Windows users:** If the Setup Assistant does not start up automatically, select your CD drive from **My Computer** and double-click the file named **SetupAssistant** to start the Setup Assistant.

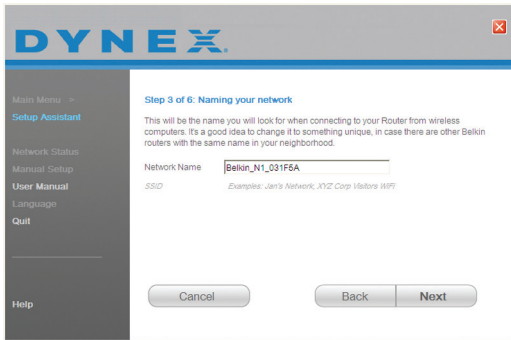
- 4 When the Confirmation screen opens, verify that you have completed all QIG steps by checking the box to the right of the arrow, then click **Next** to continue.



Setup Assistant will indicate each time a step in the setup has been completed.

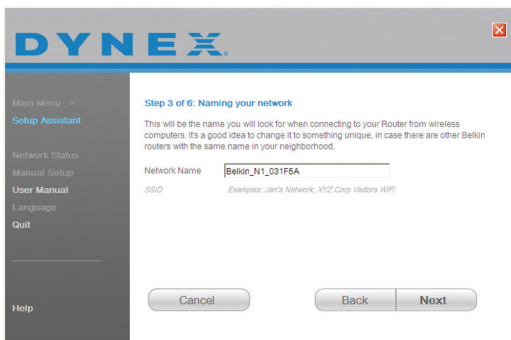


When it is time to name your network, the Setup Assistant will open the *Naming your network* screen.



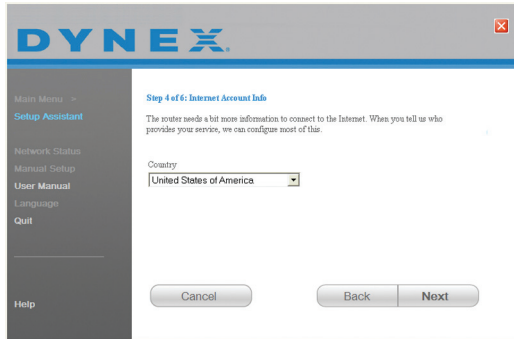
The default wireless network name or Service Set Identifier (SSID) is the name of your wireless network that your computers or devices with wireless network adapters will connect to.

- 5 You can either accept the default name or change it to something unique. If you change it, write down the name for future reference. Click **Next** to continue.

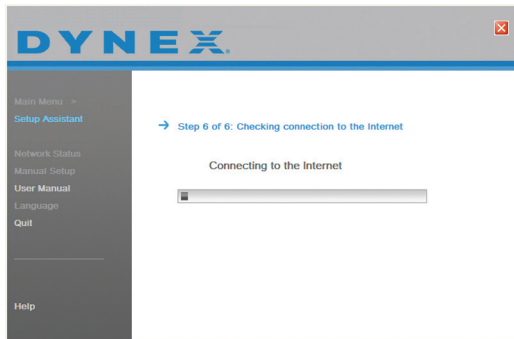


- 6 If your Internet account requires a login and password, you will be prompted with a screen similar to the illustration above. Select your country or ISP from the lists. The Setup Assistant will now configure your router by sending data to your router and restarting it. Wait for the on-screen instructions.

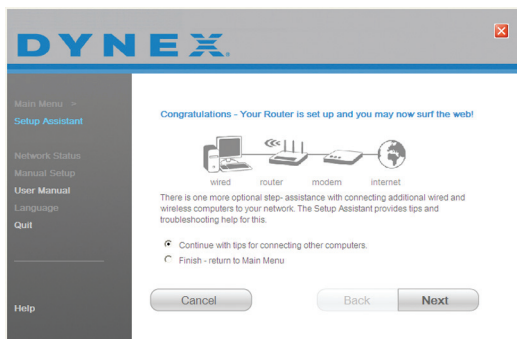
**Caution:** Do not disconnect any cable or power off your router while your router is rebooting. Doing so will render your router inoperable.



After configuring your router, the Setup Assistant checks your connection to the Internet.



This completes your router installation. You will see the *Congratulations* screen when your router can connect to the Internet. You can begin surfing by opening your browser and going to any Web site.

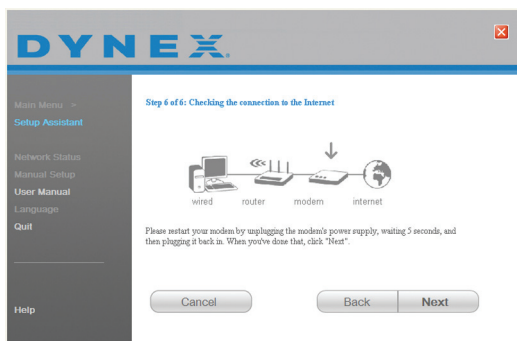


- 7 You can use the Setup Assistant to set up your other wired and wireless computers to connect to the Internet by clicking **Next**. If you decide to add computers to your router later, select **Exit the Assistant**, then click **Next**.

## Troubleshooting the setup

### To troubleshoot the setup:

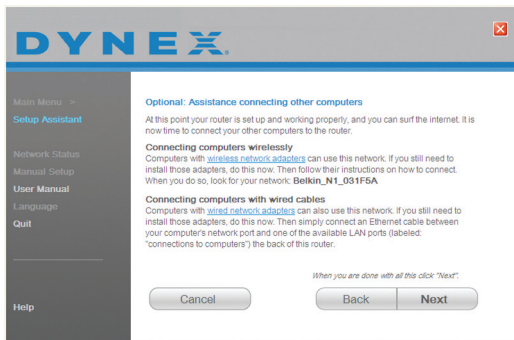
- If the Setup Assistant is not able to connect to the Internet, you will see the following screen. Follow the on-screen instructions to go through the troubleshooting steps.





**To use the optional assistance to connect to other computers:**

- 1 This optional step will help you to connect additional wired and wireless computers to your network. Follow the on-screen instructions.



At this point, your router is set up and working properly. It is now time to connect your other computers.

**Connecting computers wirelessly**

Computers with wireless network adapters can use this network. If you still need to install those adapters, do this now. Then follow their instructions on how to connect. When you do so, look for your network: John's Home Wi-Fi.

**Connecting computers with wired cables**

Computers with wired network adapters can use this network. If you still need to install those adapters, do this now. Then connect an Ethernet cable between your computer's network port and one of the available LAN ports (labeled **connections to computers**) on the back of your router.]

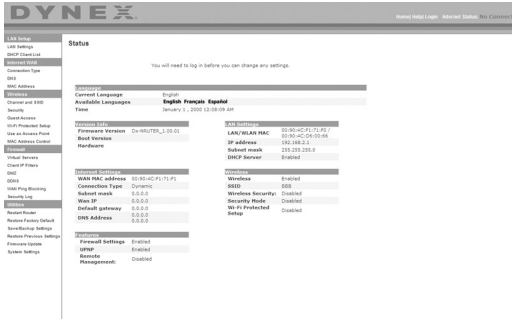
Once you have verified that your other wired and wireless computers are properly connected, your network is set up and working. You can now surf the Internet. Click **Next** to go back to the main menu.

## Wireless security setup

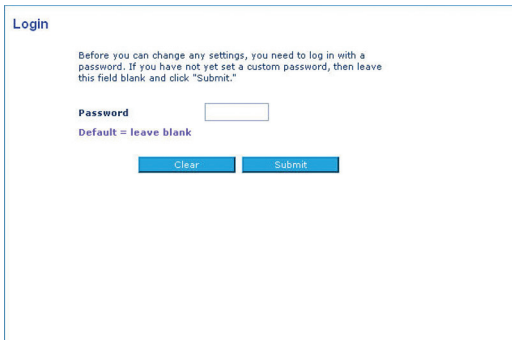
Make sure that you complete the basic setup of your router before setting up security. Make sure that all of your computers (wired and wireless) can successfully connect to the Internet through your router.

### To set up security:

- 1 On a computer that has a wired (cable) connection to your router, open a Web browser. In the address field, type 192.168.2.1 (or the IP address you customized), then click **Enter**.



- 2 In the menu at left, go to the wireless section and click **Security**. If asked to log in, enter your password. or if you have not yet set a custom password, leave this field blank. Then click, **Submit**.

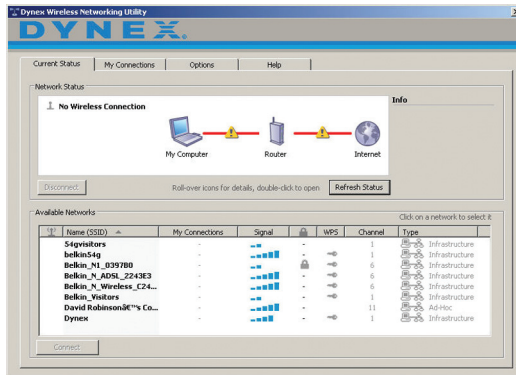


- You will be asked to pick a security type. We recommend WPA2-PSK as the security mode and then WPA-PSK+WPA2-PSK as the Authentication, as it is the most secure and easiest to use. Once you have made your choice, click **Apply Changes**.

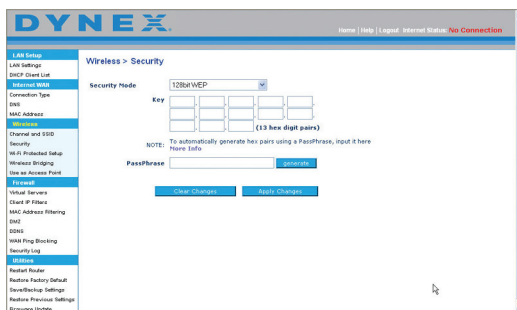


- In the Pre-shared key field, type a security key that is easy for you to remember. Using some punctuation will increase your network's security (for example, "My favorite team is the Tigers!"). Click **Apply Changes**.
- Now go to each of your wireless computers. Use the wireless utility software on each to do the following (see your wireless adapter's user manual for more detailed instructions):
  - Find your wireless network and connect to it.
  - When prompted, enter the phrase you created above.

**Note:** If a computer does not accept the phrase, it likely does not yet support WPA/WPA2. Go to your wireless adapter manufacturer's Web site and check for a driver update.



- 6 If you do not want to update your computer's wireless adapter to work with WPA/WPA2, return to Step 4 and choose WEP.



## Alternative setup method

The Web-Based Advanced User Interface is a Web-based tool that you can use to set up your router if you do not want to use the Setup Assistant. You can also use it to manage advanced functions of your router. From the Web-Based Advanced User Interface, you can perform the following tasks:

- View your router's current settings and status
- Configure your router to connect to your ISP with the settings that they provided you
- Change the current network settings such as the Internal IP address, the IP address pool, DHCP settings, and more
- Set your router's firewall to work with specific applications (port forwarding)
- Set up security features such as client restrictions, MAC address filtering, WEP, and WPA
- Enable the DMZ feature for a single computer on your network
- Change your router's internal password
- Enable/Disable UPnP (Universal Plug-and-Play)
- Reset your router
- Back up your configuration settings
- Reset your router's default settings
- Update your router's firmware

### To connect your router:

- 1 Turn off the power to your modem by unplugging the power supply from the modem.
- 2 Locate the network cable that is connected between your modem and your computer and unplug it from your computer, leaving the other end connected to your modem.
- 3 Plug the loose end of the cable you just unplugged into the port on the back of your router labeled **Modem**.
- 4 Connect a new network cable (not included) from the back of the computer to one of the wired computer ports labeled **1-4**.

**Note:** It does not matter which numbered port you choose.

- 5 Turn your cable or DSL modem on by reconnecting the power supply to the modem.
- 6 Plug the power cord into the wall, then plug the cord into your router's power jack.

- 7 Make sure that your modem is connected to your router by checking the lights on the front of your router. The green light labeled **Modem** should be on if your modem is connected correctly to your router. If it is not, recheck your connections.
- 8 Make sure that your computer is connected properly to your router by checking the lights labeled **1-4**. The light that corresponds to the numbered port connected to your computer should be on if your computer is connected properly. If it is not, recheck your connections.

**To set up your computer's network settings to work with a DHCP server:**

- See “Manually configuring network settings” on page 46 for directions.

**Configuring your router using the Web-Based Advanced User Interface:**

- 1 Open your Internet browser, then access your router's Web-Based Advanced User Interface by typing “192.168.2.1” in the address line (you do not need to type anything else such as “http://” or “www”), then press **Enter**. The router's home page opens.

**Note:** If you have difficulty accessing your router's Web-Based Advanced User Interface, go to “Manually configuring network settings” on page 46.

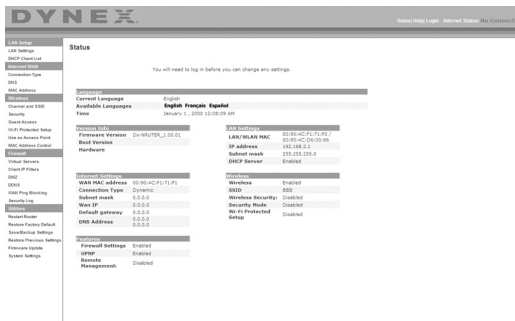
- 2 To make any changes to your router's settings, you have to log in. Click **Login**, or click any one of the links on the home page to go to the login screen.
- 3 In the login screen, leave the password blank (your router shipped with no password entered) and click **Submit** to log in.
- 4 After you have logged in to make changes, there are two ways that the computer can be logged out. Clicking **Logout** will log the computer out.

- OR -

The login will time out after a specified period of time. The default login time-out is 10 minutes. This can be changed from 1 to 99 minutes. For more information, see “Changing the Login Time-Out setting” on page 44.

## Using the Web-Based Advanced User Interface

The home page is the first page you will see when you access the Web-Based Advanced User Interface (UI). The home page shows you a quick view of your router's status and settings. All advanced setup pages can be reached from this page.



**Quick-Navigation links**—You can go directly to any of your router's UI pages by clicking directly on these links. The links are divided into logical categories and grouped by tabs to make finding a particular setting easier to find. Clicking the purple header of each tab will show you a short description of the tab's function.

**Home button**—The **Home** button is available in every page of the UI. Pressing this button will take you back to the home page.

**Internet status indicator**—This indicator is visible in all pages of the UI, indicating the connection status of your router. When the indicator says **Connection OK** in green, your router is connected to the Internet. When your router is not connected to the Internet, the indicator will read **No Connection** in red. The indicator is automatically updated when you make changes to the settings of your router.

**Login/Logout button**—This button lets you log in and out of your router with the press of one button. When you are logged into your router, this button will change to read **Logout**. Logging into your router will take you to a separate login page where you will need to enter a password. When you are logged into your router, you can make changes to the settings. When you are finished making changes, you can log out of your router by clicking the **Logout** button.

**Help button**—The **Help** button gives you access to your router's help pages.

**LAN Settings**—Shows you the settings of the Local Area Network (LAN) side of your router. Changes can be made to the settings by clicking any one of the links (IP Address, Subnet Mask, DHCP Server) or by clicking the **LAN** quick-navigation link on the left side of the screen.

**Features**—Shows the status of your router's NAT, firewall, and wireless features. Changes can be made to the settings by clicking any one of the links or by clicking the quick-navigation links on the left side of the screen.

**Internet Settings**—Shows the settings of the Internet/WAN side of your router that connects to the Internet. Changes to any of these settings can be made by clicking the links or by clicking the **Internet/WAN** quick-navigation link on the left side of the screen.

**Version Info**—Shows the firmware version, boot-code version, hardware version, and serial number of your router.

**Page Name**—The page you are on can be identified by this name. This User Guide will sometimes refer to pages by name. For instance **LAN > LAN Settings** refers to the *LAN Settings* page.

## Configure your router for connection to your Internet Service Provider (ISP)

The **Internet/WAN** tab is where you will set up your router to connect to your Internet Service Provider (ISP). Your router is capable of connecting to virtually any ISP's system provided you have correctly configured your router's settings for your ISP's connection type. Your ISP connection settings are provided to you by your ISP.

**To configure your router with the settings that your ISP gave you:**

- 1 Click **Connection Type** on the left side of the screen, then select the connection type you use.
- 2 If your ISP gave you DNS settings, click **DNS** to enter DNS address entries for ISPs that require specific settings.
- 3 Click **MAC address** to clone your computer's MAC address or type a specific WAN MAC address, if required by your ISP.

When you have finished making settings, the **Internet Status** indicator will read **connection OK** if your router is set up properly.

**To set your Connection Type:**

- 1 Click **Connection Type** from the menu on the left side of the screen. The *Connection Type* page opens. From this page, you can select the type of connection you use by clicking the button next to your connection type and then clicking **Next**.

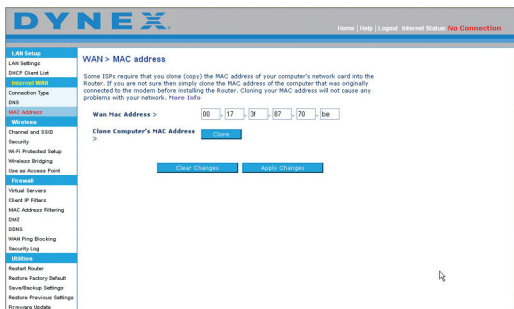


## Setting your Internet Service Provider (ISP) connection type to dynamic IP

A dynamic connection type is the most common connection type used with cable modems. Setting the connection type to **dynamic** in many cases is enough to complete the connection to your ISP. Some dynamic connection types may require a host name. You can enter your host name in the space provided if you were assigned one. Your host name is assigned by your ISP. Some dynamic connections may require that you clone the MAC address of the PC that was originally connected to the modem.

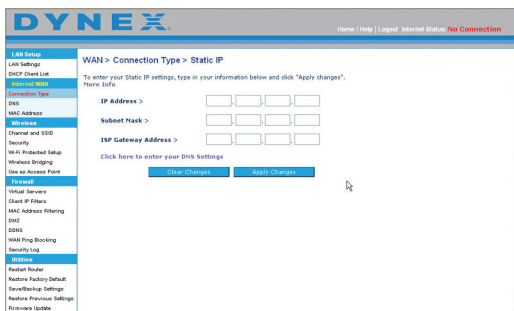
## Change WAN MAC Address

If your ISP requires a specific MAC address to connect to the service, you can enter a specific MAC address or clone the current computer's MAC address through this link.



## Setting your Internet Service Provider (ISP) connection type to static IP

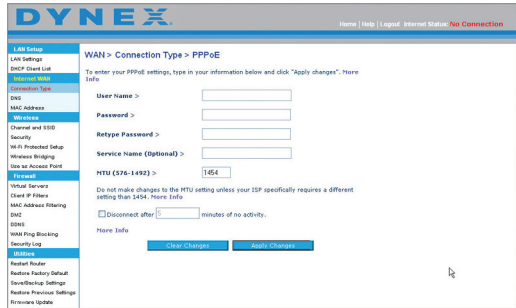
A static IP address connection type is less common than other connection types. If your ISP uses static IP addressing, you will need your IP address, subnet mask, and ISP gateway address. This information is available from your ISP or on the paperwork that your ISP left with you. Type your information, then click **Apply Changes**. After you apply the changes, the **Internet Status** indicator will read **connection OK** if your router is set up correctly.





## Setting your ISP connection type to PPPoE

Most DSL providers use PPPoE as the connection type. If you use a DSL modem to connect to the Internet, your ISP may use PPPoE to log you into the service. If you have an Internet connection in your home or small office that doesn't require a modem, you may also use PPPoE.



Your connection type is PPPoE if:

- Your ISP gave you a user name and password, which is required to connect to the Internet.
- Your ISP gave you software such as WinPOET or Enternet300 that you use to connect to the Internet.
- You have to double-click a desktop icon other than your browser to get on the Internet.

Enter the following:

**User Name**—This space is provided to type your user name that was assigned by your ISP.

**Password**—Type your password and retype it into the *Retype Password* box to confirm it.

**Service Name**—A service name is rarely required by an ISP. If you are not sure if your ISP requires a service name, leave this blank.

**MTU**—The MTU setting should never be changed unless your ISP gives you a specific MTU setting. Making changes to the MTU setting can cause problems with your Internet connection including disconnection from the Internet, slow Internet access, and problems with Internet applications working properly.

**Disconnect after X**—The Disconnect feature is used to automatically disconnect your router from your ISP when there is no activity for a specified period of time. For instance, placing a check mark next to this option and entering **5** into the minute field will cause your router to disconnect from the Internet after five minutes of no Internet activity. This option should be used if you pay for your Internet service by the minute.

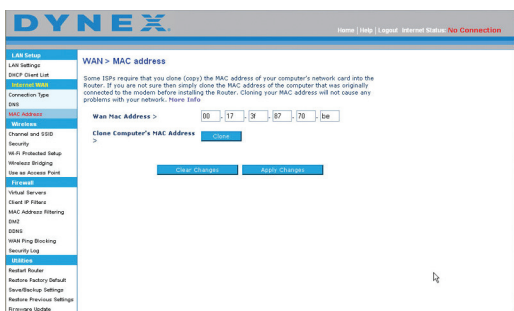
## Setting custom Domain Name Server (DNS) settings

A *Domain Name Server* is a server located on the Internet that translates Universal Resource Locators (URLs) like “www.dynex.com” into IP addresses. Many Internet Service Providers (ISPs) do not require you to enter this information into your router. The **Automatic from ISP** box should be checked if your ISP did not give you a specific DNS address. If you are using a static IP connection type, then you may need to enter a specific DNS address and secondary DNS address for your connection to work properly. If your connection type is dynamic or PPPoE, it is likely that you do not have to enter a DNS address. Leave the **Automatic from ISP** box checked. To enter the DNS address settings, uncheck the **Automatic from ISP** box and enter your DNS entries in the spaces provided. Click **Apply Changes** to save the settings.



## Configuring your WAN Media Access Controller (MAC) address

All network components including cards, adapters, and routers, have a unique *serial number* called a MAC address. Your Internet Service Provider may record the MAC address of your computer's adapter and only let that particular computer connect to the Internet service. When you install your router, its own MAC address will be “seen” by the ISP and may cause the connection not to work. Dynex has provided the ability to clone (copy) the MAC address of the computer into your router. This MAC address, in turn, will be seen by the ISP's system as the original MAC address and will allow the connection to work. If you are not sure whether your ISP needs to see the original MAC address, simply clone the MAC address of the computer that was originally connected to the modem. Cloning the address will not cause any problems with your network.



**To clone your MAC Address:**

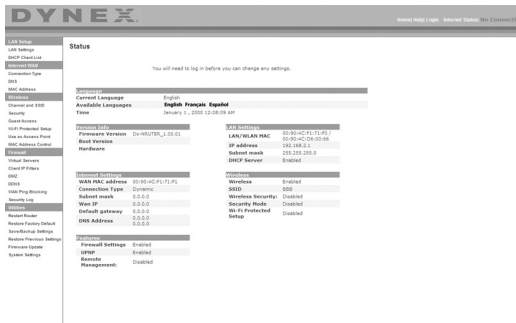
- 1 Make sure that you are using the computer that was **ORIGINALLY CONNECTED** to your modem before your router was installed. Click
- 2 Click **Clone**, then click **Apply Changes**. Your MAC address is now cloned to your router.

**To enter a specific MAC Address:**

- Type a MAC address in the spaces provided, then click **Apply Changes** to save the changes. Your router's WAN MAC address is changed to the MAC address you specified.

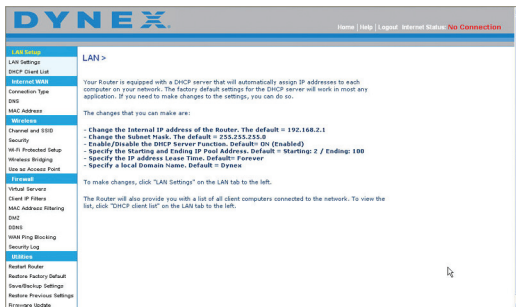
**Using the Web-Based Advanced User Interface**

Using your Internet browser, you can access your router's Web-Based Advanced User Interface. Open your browser and enter **192.168.2.1** (do not type anything else such as "http://" or "www"), then press **Enter**. Your router's home page opens in your browser window.



**Viewing the LAN settings**

Clicking the header of the **LAN Setup** will take you its header page. A quick description of the functions can be found here. To view the settings or make changes to any of the LAN settings, click **LAN Settings**, or to view the list of connected computers, click **DHCP client list**.



## Changing LAN settings

All settings for the internal LAN setup of your router can be viewed and changed here.

The screenshot shows the 'LAN > LAN settings' page on a DYNEX router. The page is divided into a left sidebar with navigation links and a main content area. The main content area includes a title 'LAN > LAN settings', a warning message, and several configuration sections: IP Address (192.168.2.1), Subnet Mask (255.255.255.0), DHCP server (On), IP Pool (Start: 192.168.0.2, End: 192.168.0.100), Lease Time (Forever), and Local Domain Name (Dynamic). At the bottom, there are two buttons: 'Apply Changes' and 'Cancel Changes'.

**IP Address**—The *IP address* is the internal IP address of your router. The default IP address is **192.168.2.1**. To access the Web-Based Advanced User Interface, type this IP address into the address bar of your browser. This address can be changed if needed. To change the IP address, type the new IP address and click **Apply Changes**. The IP address you choose should be a non-routable IP.

Examples of a non-routable IP are: 192.168.x.x (where x is anywhere between 0 and 255), and 10.x.x.x (where x is anything between 0 and 255).

**Subnet Mask**—There is no need to change the subnet mask. This is a unique, advanced feature of your router. It is possible to change the subnet mask if necessary; however, do NOT make changes to the subnet mask unless you have a specific reason to do so. The default setting is **255.255.255.0**.

**DHCP Server**—The DHCP server function makes setting up a network very easy by assigning IP addresses to each computer on the network automatically. The default setting is **On**. The DHCP server can be turned OFF if necessary; however, in order to do so you must manually set a static IP address for each computer on your network. To turn off the DHCP server, select **Off**, then click **Apply Changes**.

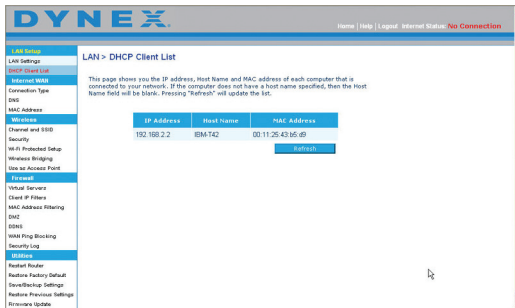
**IP Pool**—The range of IP addresses set aside for dynamic assignment to the computers on your network. The default is 2-100 (99 computers). If you want to change this number, you can do so by entering a new starting and ending IP address and clicking **Apply Changes**. The DHCP server can assign 100 IP addresses automatically. This means that you cannot specify an IP address pool larger than 100 computers. For example, starting at 50 means you have to end at 150 or lower so as not to exceed the 100-client limit. The starting IP address must be lower in number than the ending IP address.

**Lease Time**—The length of time the DHCP server will reserve the IP address for each computer. We recommend that you leave the lease time set to **Forever**. The default setting is **Forever**, meaning that any time a computer is assigned an IP address by the DHCP server, the IP address will not change for that particular computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer's IP address may change over time. If you have set any of the other advanced features of your router such as DMZ or client IP filters, these are dependent on the IP address. For this reason, you will not want the IP address to change.

**Local Domain Name**—The default setting is **Dynex**. You can set a local domain name (network name) for your network. There is no need to change this setting unless you have a specific advanced need to do so. You can name the network anything you want such as "MY NETWORK".

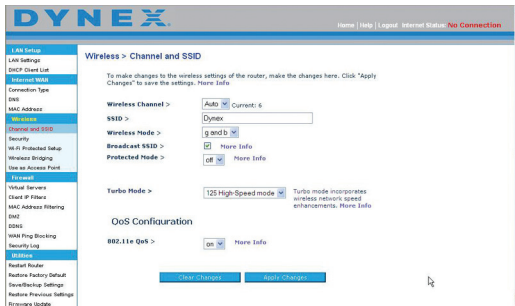
### Viewing the DHCP Client List page

You can view a list of the computers (known as clients), which are connected to your network. You are able to view the IP address of the computer, the host name (if the computer has been assigned one), and the MAC address of the computer's network interface card (NIC). Pressing the **Refresh** button will update the list. If there have been any changes, the list will be updated.



### Configuring the wireless network settings

Clicking the header of the **Wireless** tab will take you to the *Wireless* page. Under the **Wireless** tab, there are links that let you make changes to the wireless network settings.



### Changing the Wireless Channel

There are a number of operating channels from which you can choose. In the United States, there are 11 channels. In Australia, the United Kingdom, and most of Europe, there are 13 channels. In a small number of other countries, there are other channel requirements. Your router is configured to operate on the proper channels for the country in which you reside. The channel can be changed, if needed. If there are other wireless networks operating in your area, your network should be set to operate on a channel that is different than the other wireless networks.

### Extension channel

The IEEE 802.11n draft specification allows the use of a secondary channel to double the bandwidth (see “Using the bandwidth switch” on page 27). An appropriate extension channel will be displayed when operating in 40 MHz mode (see “Using the wireless mode switch” on page 26). The channel can be changed, if needed.

### Changing the wireless network name (SSID)

To identify your wireless network, a name (SSID for Service Set Identifier) is used. The SSID is your network name. The default network name of your router is “Dynex” followed by six digits that are unique to your router. You can change this to anything you choose, or you can leave it unchanged. Keep in mind, if you decide to change your wireless network name, and there are other wireless networks operating in your area, your network name needs to be different from other wireless networks. To change the SSID, type the SSID that you want to use in the **SSID** field and click **Apply Changes**. The change is immediate. If you make a change to the SSID, your wireless-equipped computers may also need to be reconfigured to connect to your new network name. Refer to the documentation of your wireless network adapter for information on making this change.

### Using the wireless mode switch

Your router can operate in three different wireless modes: 802.11n&802.11g&802.11b, 802.11g and 802.11b. The different modes are explained below.

#### **802.11n&802.11g&802.11b**

Setting your router to this mode will allow 802.11n, 802.11g, and 802.11n-compliant devices to join the network. This is the factory default mode and ensures successful operation with all Wi-Fi-compatible devices.

#### **802.11g**

802.11g mode works with 802.11g clients only. This mode is recommended only if you want to prevent 802.11b clients from accessing your network. To switch modes, select the desired mode from the Wireless Mode list, then click **Apply Changes**.

#### **Off**

This mode will turn OFF your router's access point, so no wireless devices can join the network. Turning off the wireless function of your router is a great way to secure your network when you are away from home for a long period of time or don't want to use the wireless feature of your router at a certain time.

### Using the bandwidth switch

This switch let you set your router's wireless bandwidth modes. There are several modes available:

#### **20MHz only**

Setting your router to this mode allows only 20 MHz operation. This mode is compatible with N, draft 802.11n-, 802.11g-, and 802.11b-compliant devices, but will limit N, draft 802.11n-compliant devices' bandwidth by half. Reducing bandwidth to 20 MHz-only operation might solve some wireless problems.

#### **20MHz/40MHz auto**

Setting your router to this mode lets it switch automatically between 20 MHz and 40 MHz operation. This mode enables 40 MHz operation, to maximize speed for N, draft 802.11n-compliant devices when conditions permit. When a legacy 802.11g access point is presented and occupies an adjacent secondary channel, your router automatically reverts to 20 MHz operation to maximize compatibility. We recommend using this as the default mode.

### Using the Broadcast SSID feature

*Note: This advanced feature should be employed by advanced users only.*

For security, you can choose not to broadcast your network's SSID. Doing so will keep your network name hidden from computers that are scanning for the presence of wireless networks. To turn off the broadcast of the SSID, remove the check mark from the box next to **Broadcast SSID**, then click **Apply Changes**. The change is immediate. Each computer now needs to be set to connect to your specific SSID. An SSID of **ANY** will no longer be accepted. Refer to the documentation of your wireless network adapter for information on making this change.

**Protected mode switch**—Protected mode ensures proper operation of N, draft 802.11n-compliant devices on your wireless network when 802.11g or 802.11b devices are present or when there is heavy 802.11g or 802.11b traffic in the operating environment. Use protected mode if your network consists of a mix of Dynex N Wireless Cards and 802.11g or 802.11b cards on your network. If you are in an environment that includes little to no 802.11g or 802.11b wireless network traffic, you will achieve the best N wireless performance with protected mode OFF. Conversely, in an environment with HEAVY 802.11g or 802.11b traffic or interference, you will achieve the best N wireless performance with protected mode ON. This will ensure N wireless performance is not affected.

### Changing the Wireless Security Settings

Your router is equipped with the latest wireless security standard called Wi-Fi Protected Access™2 (WPA2™) and the legacy security standard called Wired Equivalent Privacy (WEP). Your router also supports the Wi-Fi Protected Setup (WPS), which simplifies the setup of a wireless network. WPS uses familiar methodologies, such as typing in a Personal Identification Number (PIN) or pushing a button, to let you automatically configure network names and strong WPA™/WPA2 data encryption and authentication. To enable security, you need to determine which standard you want to use. To access the security settings, click **Security** on the **Wireless** tab.

## Using Wi-Fi Protected Setup

WPS uses WPA2 for encryption. It does not provide additional security, but rather, standardizes the method for securing your wireless network. You can use either the Push Button Configuration (PBC) method or Personal Identification Number (PIN) method to let a device access your wireless network.

**PBC**—Push and hold the WPS button located on the back of your router for three seconds. Then, initiate the WPS procedure on the client device within two minutes. Refer to your client's documentation on this procedure. Pushing the PBC button will automatically enable WPS. The client has now been securely added to your wireless network.

**PIN**—The client device has a PIN number (either four or eight digits) that is associated with WPS. Enable WPS through the screen illustrated below. Enter the client's PIN into your router's internal registrar (accessed through this screen). The client will be automatically enrolled into your wireless network within two minutes.



**Wi-Fi Protected Setup (WPS)**—Enabled or Disabled.

**Personal Identification Number (PIN) Method**—In this method, a wireless client wanting to access your network must supply a 4- or 8-digit PIN to your router. After clicking **Enroll**, you must start the WPS handshaking procedure from the client within two minutes.

**Router PIN**—If an external registrar is available, you can enter in your router's PIN to the registrar. Click **Generate New PIN** to change the PIN from the default value. Click **Restore Default PIN** to reset the PIN value.

**Push Button Configuration (PBC) Method**—PBC is an alternate method to connect to a WPS network. Push the **PBC** button located on the back of your router for three seconds, then initiate the PBC on the client device. Alternatively, push the **Start PBC** soft button to start this process.

**Manual Configuration Method**—This section lists the default security settings to be set up if not using WPS.



## WPA2 Requirements

**IMPORTANT:** In order to use WPA2 security, all your computers and wireless client adapters must be upgraded with patches, driver, and client utility software that support WPA2. At the time of this User Manual's publication, a couple security patches are available, for free download, from Microsoft®. These patches work only with the Windows XP operating system. Other operating systems are not supported at this time.

For Windows XP computers that do not have Service Pack 2 (SP2), a file from Microsoft called "Windows XP Support Patch for Wireless Protected Access (KB 826942)" is available for free download at <http://support.microsoft.com/kb/826942>.

For Windows XP with Service Pack 2, Microsoft has released a free download to update the wireless client components to support WPA2 (KB971021). The update is available from <http://support.microsoft.com/kb/917021>.

**Important:** You also need to ensure that all your wireless client cards/adapters support WPA2, and that you have downloaded and installed the latest driver. Most of the Dynex wireless cards have driver updates available for download from the Dynex support site at [www.dynexsupport.com](http://www.dynexsupport.com).

## Setting WPA/WPA2-Personal (PSK)

Like WPA security, WPA2 is available in both WPA2-Personal (PSK) mode and WPA2-Enterprise (RADIUS) mode. Typically, WPA2-Personal (PSK) is the mode that will be used in a home environment, while WPA2-Enterprise (RADIUS) is implemented in a business environment where an external radius server distributes the network key to the clients automatically. Your router supports WPA2-Personal (PSK).

### To set up WPA/WPA2:

- 1 After you set up your router, click **Security** under the **Wireless** heading on the left menu. The *Wireless > Security* page opens.
- 2 Select **WPA/WPA2-Personal (PSK)** from the **Security Mode** list.
- 3 For **Authentication**, select **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK + WPA2-PSK**. This setting must be identical on the wireless clients that you set up. **WPS-PSK + WPA2-PSK** mode lets your router support clients running either WPA or WPA2 security.
- 4 For **Encryption Technique**, select **TKIP**, **AES**, or **TKIP + AES**. This setting must be identical on the wireless clients that you set up.
- 5 Enter your pre-shared key (PSK). This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up. For example, your PSK might be something like "Smith family network key."

- 6 Click **Apply Changes** to finish. You must now set all clients to match these settings depending on the type of access you want them to have.



**Important:** Make sure that your wireless computers are updated to work with WPA2 and have the correct settings to get proper connection to your router.

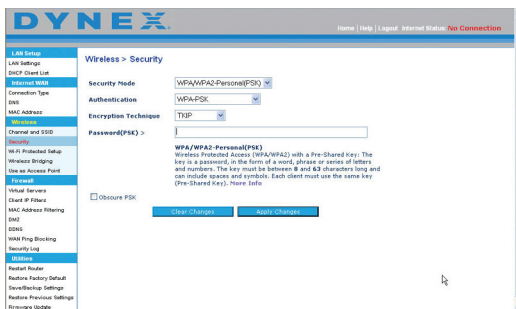
## Setting WPA Security

**Note:** To use WPA security, your wireless network cards must be equipped with software that supports WPA. At the time this User Manual was published, a security patch from Microsoft is available for free download. This patch works only with Windows XP.

Your router supports WPA-Personal (PSK), which uses a pre-shared key (PSK) as the security key. A pre-shared key is basically a password that is between eight and 63 characters long. It can be a combination of letters, numbers, or characters. Each client uses the same key to access the network. Typically this is the mode that will be used in a home environment.

### To set WPA-PSK security:

- 1 From the *Security Mode* drop-down menu, select **WPA/WPA-Personal (PSK)**.
- 2 For **Encryption Technique**, select **TKIP** or **AES**. This setting will have to be identical on the clients that you set up.
- 3 Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, or symbols. This same key must be used on all of the clients that you set up.
- 4 Click **Apply Changes** to finish. You must now set all clients to match these settings.

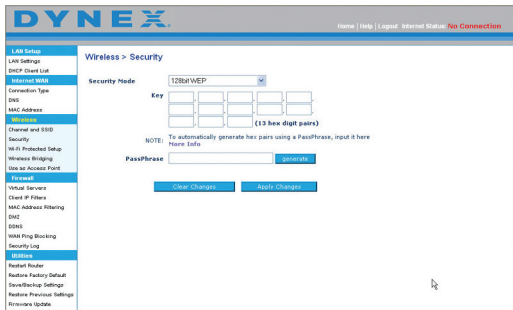


## Setting WEP encryption

**Note to Mac users:** The **Passphrase** option will not operate with Apple® AirPort®. To configure encryption for your Mac computer, set the encryption using the manual method described in the next section.

### To set WEP encryption:

- 1 From the **Security Mode** drop-down menu, select **128-bit WEP** or **64-bit WEP** from the.
- 2 After selecting your WEP encryption mode, enter you WEP key manually by typing the hex WEP key, or type a passphrase in the **PassPhrase** field, then click **Generate** to create a WEP key from the passphrase.
- 3 Click **Apply Changes** to finish. You must now set all of your clients to match these settings.



Encryption in your router is now set. Each of your computers on your wireless network will now need to be configured with the same passphrase. Refer to the documentation of your wireless network adapter for information on making this change.

## Using a Hexadecimal Key

A hexadecimal key is a mixture of numbers and letters from A-F and 0-9. 64-bit keys are 10 digits long and can be divided into five two-digit numbers. 128-bit keys are 26 digits long and can be divided into 13 two-digit numbers.

For instance:

**AF 0F 4B C3 D4** = 64-bit key

**C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7** = 128-bit key

In the table below, make up your key by writing in two characters between A-F and 0-9. You will use this key to program the encryption settings on your router and your wireless computers.

Example: 

AF	0F	4B	C3	D4
----	----	----	----	----

64-bit: 

--	--	--	--	--

128-bit: 

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

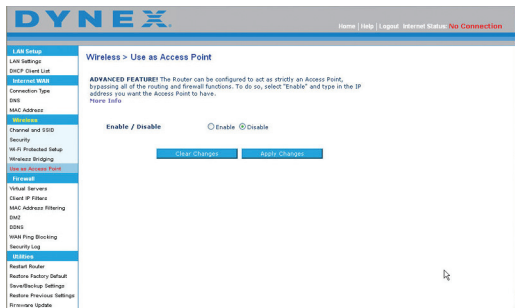
**Note to Mac users:** Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.

## Using the Access Point mode

**Note:** This advanced feature should be employed by advanced users only. Your router can be configured to work as a wireless network access point. Using this mode will defeat the NAT IP sharing feature and DHCP server. In Access Point (AP) mode, your router will need to be configured with an IP address that is in the same subnet as the rest of the network that you will bridge to. The default IP address is 192.168.2.254 and subnet mask is 255.255.255.0. These can be customized for your needs.

### To use the Access Point mode:

- 1 Click **Use as access point** under the **Wireless** heading on the left menu. The *Wireless > Use as Access Point* page opens.



- 2 Select **Enable**. When you select this option, you will be able to change the IP settings.
- 3 Set your IP settings to match your network, then click **Apply Changes**.
- 4 Connect a cable from the Modem port on your router to your existing network. Your router is now acting as an access point. To access your router's Web-Based Advanced User Interface again, type the IP address you specified into your browser's navigation bar. You can set the encryption settings, MAC address filtering, SSID, and channel normally.

## Setting MAC Address Control

The MAC address filter is a powerful security feature that lets you specify which computers are allowed on the wireless network.

*Note: This list applies only to wireless computers.*

This list can be configured so any computer attempting to access the wireless network that is not specified in the filter list will be denied access. When you enable this feature, you must enter the MAC address of each client (computer) to which you want to allow network access. The **Block** feature lets you turn on and off access to the network easily for any computer without having to add and remove the computer's MAC address from the list.



## Setting up an Allow Access list

To set up an Allow Access list:

- 1 Click the **Allow** radio button to begin setting up a list of computers allowed to connect to the wireless network.
- 2 In the **MAC Address** field that is blank, type the MAC address of the wireless computer you want to be able to access the wireless network, then click **<<Add**.
- 3 Repeat Step 2 until all of the computers you want to add have been entered.
- 4 Click **Apply Changes** to finish.

## Setting up a Deny Access list

The Deny Access list lets you specify computers that you DO NOT want to access the network. Any computer in the list will not be allowed access to the wireless network. All others will.

To set up a Deny Access list:

- 1 Click the **Deny** radio button to begin setting up a list of computers to be denied access to the wireless network.
- 2 In the **MAC Address** field that is blank, type the MAC address of the wireless computer you want to deny access to the wireless network, then click **<<Add**.
- 3 Repeat Step 2 until all of the computers you want to deny access to have been entered.
- 4 Click **Apply Changes** to finish.

## Configuring the firewall

Your router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

- IP Spoofing
- Land Attack Ping of Death (PoD)
- Denial of Service (DoS)
- IP with zero length
- Smurf Attack
- TCP Null Scan
- SYN flood
- UDP flooding
- Tear Drop Attack
- ICMP defect
- RIP defect
- Fragment flooding

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be *stealth*, meaning that for all intents and purposes, they do not exist to a would-be hacker. You can turn the firewall function off if needed, however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.



## Configuring Internal Forwarding settings

The *Virtual Servers* function lets you route external (Internet) calls for services such as a Web server (port 80), FTP server (Port 21), or other applications through your router to your internal network. Since your internal computers are protected by a firewall, computers outside your network (over the Internet) cannot get to them because they cannot be *seen*. A list of common applications has been provided in case you need to configure the Virtual Server function for a specific application. If your application is not listed, you will need to contact the application vendor to find out which port settings you need.



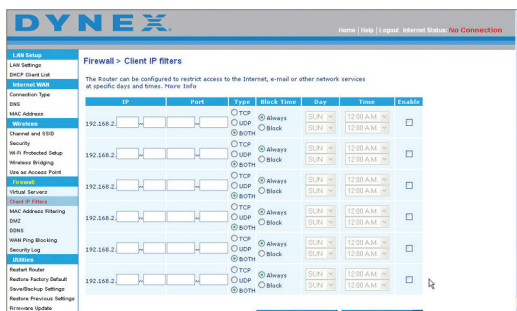
### To enter settings into the virtual server:

- 1 Open the *Virtual Servers* page, then enter the IP address in the space provided for the internal (server) machine, and the port(s) required to pass.
- 2 Select the port type (TCP or UDP), check the **Enable** box, then click **Apply Changes**.

Each inbound port entry has two fields with five characters maximum per field that allows a start and end port range, for example [xxxxx]-[xxxxx]. For each entry, you can enter a single port value by filling in the two fields with the same value (for example, [7500]-[7500]) or a wide range of ports (for example [7500]-[9000]). If you need multiple single port values or a combination of ranges and a single value, you must use multiple entries up to the maximum of 20 entries (for example, 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings quickly. It is recommended that you disable the settings when you are not using a specific application.

## Setting Client IP filters

Your router can be configured to restrict access to the Internet, e-mail, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.

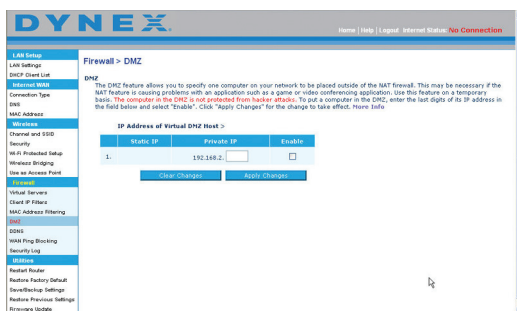


**To restrict Internet access to a single computer:**

- 1 Open the *Firewall > Client IP filters* page, then enter the IP address of the computer you want to restrict access to in the IP fields.
- 2 Enter **80** in both the port fields, select **Both**, then select **Block**. You can also select **Always** to block access all of the time.
- 3 Select the day to start on top, the time to start on top, the day to end on the bottom, and the time to stop on the bottom.
- 4 Select **Enable**, then click **Apply Changes**. The computer at the IP address you specified will now be blocked from Internet access at the times you specified. Be sure you have selected the correct time zone under **Utilities > System Settings > Time Zone**.

## Enabling the Demilitarized Zone (DMZ)

The DMZ feature lets you specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is NOT protected from hacker attacks.





**To set up a DMZ for a computer:**

- Enter the last digits of the computer's IP address in the **IP field**, click **Enable**, then click **Apply Changes** for the change to take effect.

**Using Dynamic DNS**

The Dynamic DNS service lets you alias a dynamic IP address to a static host name in any of the many domains DynDNS.org offers, allowing your network computers to be more easily accessed from various locations on the Internet. DynDNS.org provides this service, for up to five host names, free to the Internet community.

The Dynamic DNSSM service is ideal for a home Web site, file server, or to make it easy to access your home PC and stored files while you're at work. Using the service can ensure that your host name always points to your IP address, no matter how often your ISP changes it. When your IP address changes, your friends and associates can always locate you by visiting yourname.dyndns.org instead.

To register free for your Dynamic DNS host name, *visit <http://www.dyndns.org>.*

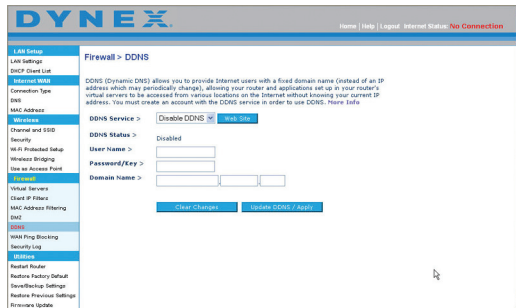
**Setting up your router's Dynamic DNS Update Client**

You must register with DynDNS.org's free update service before using this feature. Once you have your registration, follow the directions below.

**To set up your router's Dynamic DNS Update Client:**

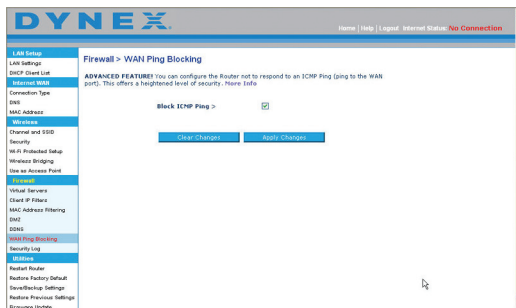
- 1 Select **DynDNS** as the **DDNS Service**.
- 2 Enter your DynDNS.org user name in the **User Name** field.
- 3 Enter your DynDNS.org password in the **Password** field.
- 4 Enter the DynDNS.org domain name you set up with DynDNS.org in the **Domain Name** field.
- 5 Click **Update Dynamic DNS** to update your IP address.

Whenever your IP address assigned by your ISP changes, your router will automatically update DynDNS.org's servers with your new IP address. You can also do this manually by clicking **Update Dynamic DNS**.



## WAN ping blocking

Computer hackers use what is known as *pinging* to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. Your router can be set up so it will not respond to an ICMP ping from the outside. This heightens the level of security of your router.

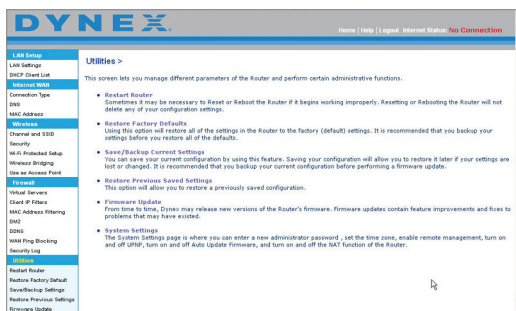


### To turn off the ping response

- Open the *Firewall > WAN Ping Blocking* page and select **Block ICMP Ping**, then click **Apply Changes**. Your router will not respond to an ICMP ping.

## Utilities tab

This screen lets you manage different parameters of your router and perform certain administrative functions.

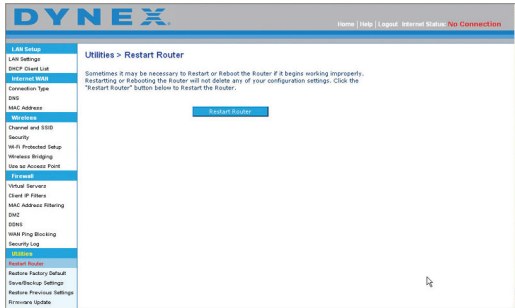


## Restarting your router

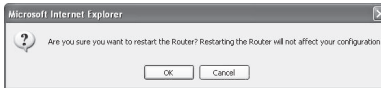
Sometimes it may be necessary to restart or reboot your router if it begins working improperly. Restarting or rebooting your router will NOT delete any of your configuration settings.

**To restart your router to restore normal operation:**

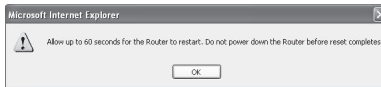
- 1 Under the **Utilities** heading on the left menu, click **Restart Router**. The *Restart Router* page opens.



- 2 Click the **Restart Router** button. The following message appears.



- 3 Click **OK**. The following message appears.



- 4 Click **OK**. Restarting your router can take up to 60 seconds. It is important not to turn off the power to your router during the restart.

A 60-second countdown will appear on the screen. When the countdown reaches zero, your router will be restarted. Your router's home page should appear automatically. If not, type your router's address (default = 192.168.2.1) into the navigation bar of your browser.

## Restoring factory default settings

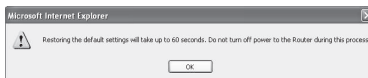
Using this option will restore all of the settings in your router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

### To restore factory default settings:

- 1 Under the **Utilities** heading on the left menu, click **Restore Defaults**. The following warning will appear.



- 2 Click **OK**. The following message appears.



- 3 Click **OK**. Restoring the defaults includes restarting your router. Restarting your router can take up to 60 seconds. It is important not to turn off the power to your router during the restart.

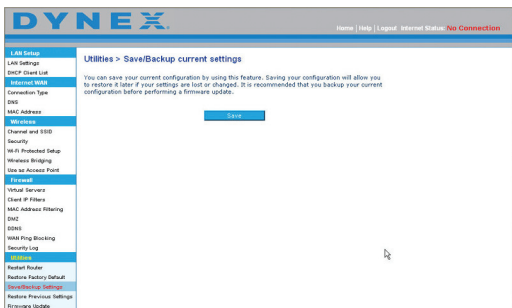
A 60-second countdown will appear on the screen. When the countdown reaches zero, your router will be restarted. Your router's home page should appear automatically. If not, type your router's address (default = 192.168.2.1) into the navigation bar of your browser.

## Saving a current configuration

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.

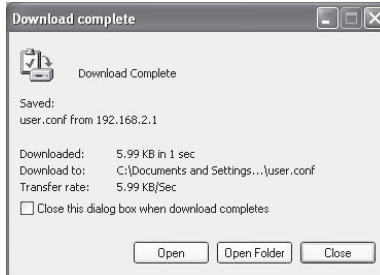
### To save a current configuration:

- 1 Under the **Utilities** heading on the left menu, click **Save/Backup Settings**. The *Save/Backup Settings* page opens.
- 2 Click **Save**. The *File Download* window opens.



- 3 Click **Save**. A window will open that lets you select the location where you want to save the configuration file.

- 4 Select a location. You can name the file anything you want, or use the default name "Config." Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file, click **Save**.
- 5 When the save is complete, you will see the following window.



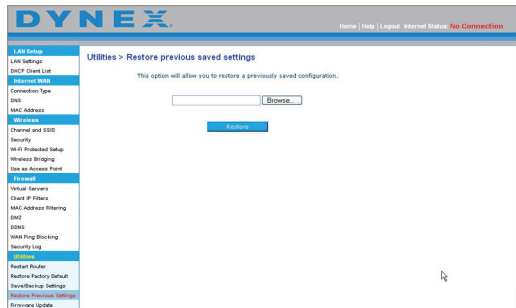
- 6 Click **Close**. The configuration is now saved.

## Restoring a previous configuration

This option will let you restore a previously saved configuration.

**To restore a previously saved configuration:**

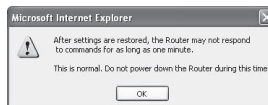
- 1 Under the **Utilities** heading on the left menu, click **Restore Previous Settings**. The *Restore Previous Settings* page opens.



- 2 Click **Browse**. A window opens that lets you select the location of the configuration file. All configuration files end with a ".conf". Locate the configuration file you want to restore, then double-click it. The following message opens.



- 3 Click **OK**. A reminder window appears.



It will take up to 60 seconds for the configuration restoration to complete.

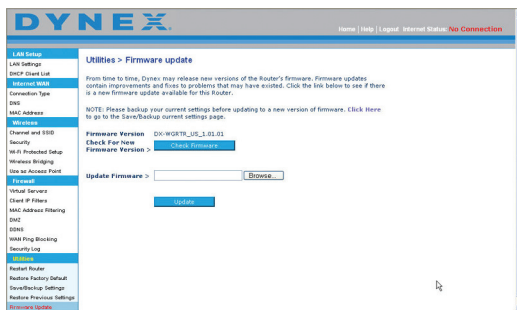
- 4 Click **OK**. A 60-second countdown will appear on the screen. When the countdown reaches zero, your router's configuration will be restored. The router's home page should appear automatically. If not, type your router's address (default = 192.168.2.1) into the navigation bar of your browser.

## Updating the firmware

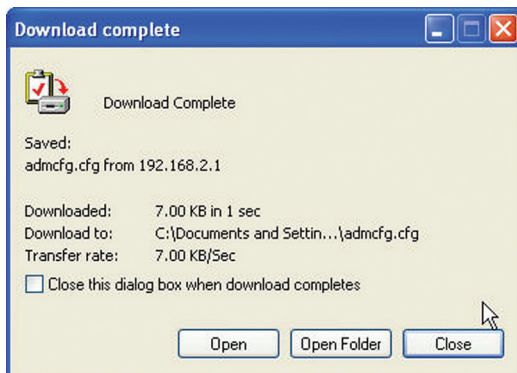
From time to time, Dynex may release new versions of your router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. When Dynex releases new firmware, you can download the firmware from the Dynex update Web site and update your router's firmware to the latest version.

**To search for and download a new version of the firmware:**

- 1 Under the **Utilities** heading on the left menu, click **Firmware Update**. The *Utilities > Firmware updates* page opens.

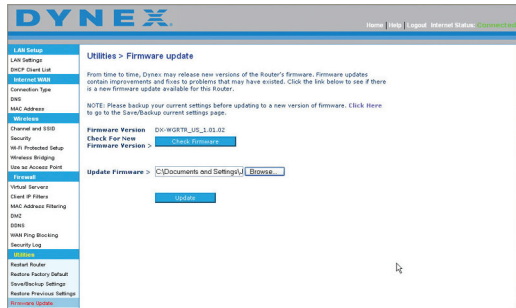


- 2 Click **Check Firmware**. The utility checks to see if there is an updated version of the firmware available.
- 3 If a new version of the firmware is available, a window will open that lets you select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to save the file in a place where you can locate it yourself later. When you have selected the location, click **Save**.  
*Note: We suggest saving this to your desktop to make it easy to locate the file.*
- 4 When the save is complete, you will see the following window.

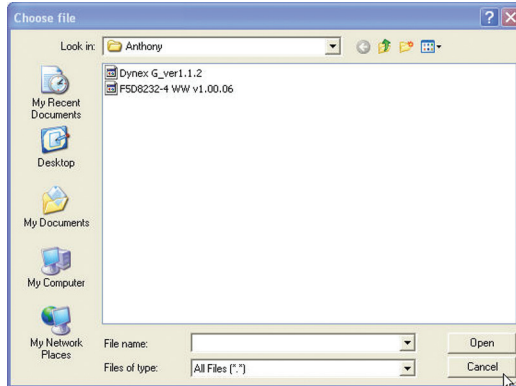


**To update your router's firmware:**

- 1 On the *Firmware Update* page, click **Browse**. A window will open that lets you select the location of the firmware update file.



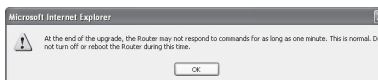
- 2 Browse to the firmware file you downloaded, then select the file by double-clicking the file name.



- 3 The **Update Firmware** box will now display the location and name of the firmware file you just selected. Click **Update**. You will be asked if you are sure you want to continue.



- 4 Click **OK**. You will see one more message. This message tells you that your router may not respond for as long as one minute as the firmware is loaded into your router and your router is rebooted.



- 5 Click **OK**. A 60-second countdown will appear on the screen. When the countdown reaches zero, your router's firmware update will be complete. Your router's home page should appear automatically. If not, type your router's address (default = 192.168.2.1) into the navigation bar of your browser.

The firmware update is complete.

## Changing system settings

The *System Settings* page is where you can enter a new administrator password, set the time zone, enable remote management, and turn on and off the NAT function of your router.

### Setting or changing the Administrator Password

Utilities > System settings

**Administrator Password:**  
The Router ships with NO password entered. If you wish to add a password for more security, you can set a password here. [More Info](#)

- Type in current Password >
- Type in new Password >
- Confirm new Password >
- Login Timeout>  (1-99 minutes)

Your router shipped with NO password entered. If you want to add a password for greater security, you can set a password here. Write down your password and keep it in a safe place, as you will need it if you need to log into your router in the future. It is also recommended that you set a password if you plan to use the remote management feature of your router.

### Changing the Login Time-Out setting

The login time-out option lets you set the period of time that you can be logged into your router's advanced setup interface. For example, if you have made some changes in the advanced setup interface, then left your computer alone without clicking **Logout**, and the time-out is set to 10 minutes, 10 minutes after you leave, the login session will expire. You will have to log into your router again to make any more changes. The login time-out option is for security purposes and the default is set to 10 minutes.

**Note:** Only one computer can be logged into your router's advanced setup interface at one time.

### Setting the time and time zone

**Time and Time Zone:** July 25, 2007 1:58:23 PM

Please set your time Zone. If you are in an area that observes daylight saving check this box. [More Info](#)

- Time Zone > (GMT-08:00) Pacific Time(US, Canada), Tijuana ▾
- Daylight Savings >  Automatically Adjust Daylight Saving
- Primary NTP Server > 192.43.244.18-NorthAmerica ▾
- Backup NTP Server > 132.163.4.102-NorthAmerica ▾

Your router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows your router to synchronize the system clock to the global Internet. The synchronized clock in your router is used to record the security log and control client filtering. Select the time zone that you reside in. If you reside in an area that observes daylight saving, then place a check mark in the box next to **Enable Daylight Saving**. The system clock may not update immediately. Allow at least 15 minutes for your router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.



## Enabling remote management

### Remote Management:

**ADVANCED FEATURE!** Remote management allows you to make changes to your Router's settings from anywhere on the Internet. Before you enable this function, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD.** [More Info](#)

Any IP address can remotely manage the router.

- Only this IP address can remotely manage the router >

- Remote Access Port >

8080

Before you enable this advanced feature of your router, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD.** Remote management allows you to make changes to your router's settings from anywhere on the Internet. There are two methods of remotely managing your router. The first is to allow access to your router from anywhere on the Internet by selecting **Any IP address can remotely manage the Router**. By typing in your WAN IP address from any computer on the Internet, you will be presented with a login screen where you need to type the password of your router. The second method is to allow a specific IP address only to remotely manage your router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing your router from in the space provided and select **Only this IP address can remotely manage the Router**. Before you enable this function, it is **STRONGLY RECOMMENDED** that you set your administrator password. Leaving the password empty will potentially open your router to intrusion.

## Enabling/Disabling Network Address Translation (NAT)

*Note: This feature should only be modified by advanced users.*

Before you enable this advanced feature of your router, **MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD.**

### NAT Enabling:

**ADVANCED FEATURE!** Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. [More Info](#)

- NAT Enable / Disable >

Enable  Disable

NAT is the method by which your router shares the single IP address assigned by your ISP with the other computers on your network. NAT should only be used if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration. If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.

## Enabling/Disabling UPnP

### UPnP Enabling:

**ADVANCED FEATURE!** Allows you to turn the UPnP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. [More Info](#)

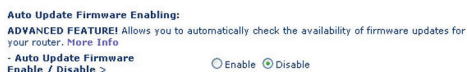
- UPnP Enable / Disable >

Enable  Disable

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require your router's firewall to be configured in a specific way to operate properly. This usually requires opening TCP and UDP ports. An application that is UPnP-compliant has the ability to communicate with your router, basically "telling" your router which way it needs the firewall configured. Your router shipped with the UPnP feature disabled. If you are using any applications that are

UPnP-compliant, and want to take advantage of the UPnP features, you can enable the UPnP feature. Select **Enable** in the **UPnP Enabling** section of the *Utilities* page, then click **Apply Changes** to save the change.

### Enabling/Disabling Auto Firmware Update



Auto Update Firmware Enabling:  
**ADVANCED FEATURE!** Allows you to automatically check the availability of firmware updates for your router. [More Info](#)  
- Auto Update Firmware  
Enable / Disable >       Enable  Disable

This innovation provides your router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into your router's advanced user interface, your router will perform a check to see if new firmware is available. If so, you will be notified. You can choose to download the new version or ignore it. Your router shipped with this feature enabled. If you want to disable it, select **Disable**, then click **Apply Changes**.

## Manually configuring network settings

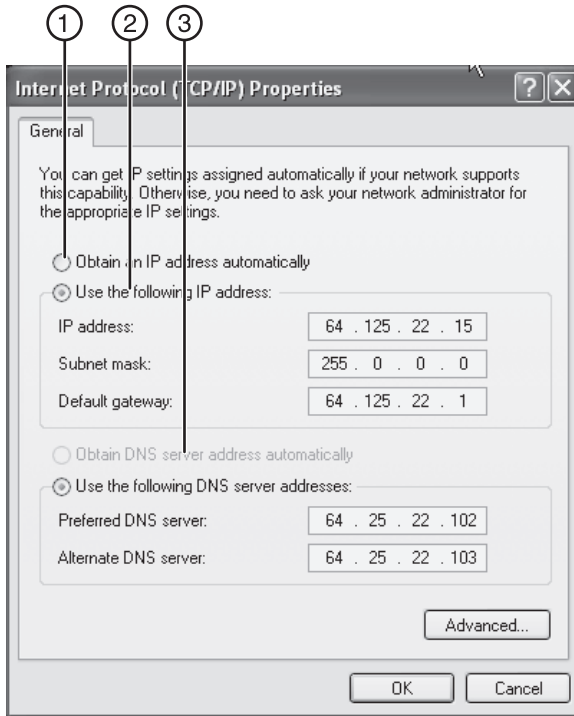
Set up the computer that is connected to the cable or DSL modem **FIRST** using these steps. You can also use these steps to add computers to your router after it has been set up to connect to the Internet.

### Windows 2000 or Windows XP

To manually configure network adapters in Windows 2000, NT, XP, or Vista:

- 1 Click **Start**, **Settings**, then click **Control Panel**.
- 2 Double-click the **Network and dial-up connections** icon (Windows 2000) or the **Network** icon (Windows XP).
- 3 Right-click the **Local Area Connection** associated with your network adapter, then click **Properties** in the list.

- 4 In the *Local Area Connection Properties* window, click **Internet Protocol (TCP/IP)**, then click **Properties**. The following screen opens.



- 5 If **Use the following IP address** (2) is selected, your router will need to be set up for a static IP connection type. Write the address information down in the table below. You will need to enter this information into your router.

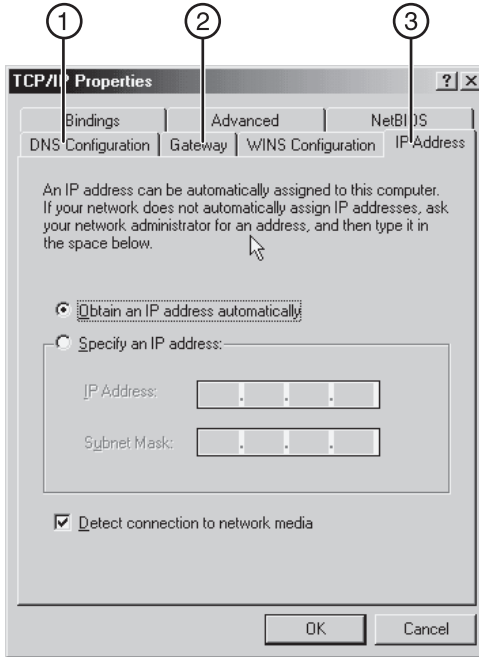
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

- 6 If not already selected, select **Obtain an IP address automatically** (1) and **Obtain DNS server address automatically** (3), then click **OK**. Your network adapter(s) are now configured for use with your router.

## Windows 98

### To manually configure network adapters in Windows 98SE:

- 1 Right-click **My Network Neighborhood**, then select **Properties** from the list.
- 2 Click **TCP/IP**, then **settings** for your installed network adapter. You will see the following window.



- 3 If **Specify an IP address** is selected, your router will need to be set up for a static IP connection type. Write down the address information in the table below. You will need to enter this information into your router.

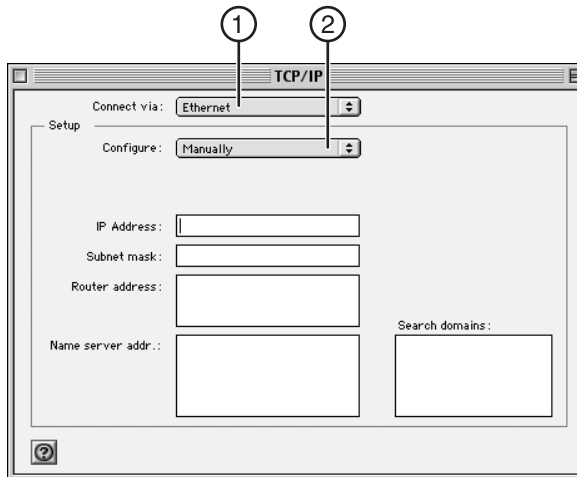
IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Default gateway:	<input type="text"/>
Preferred DNS server:	<input type="text"/>
Alternate DNS server:	<input type="text"/>

- Write in the IP address and subnet mask from the **IP Address** tab (3).
  - Click the **Gateway** tab (2). Write the gateway address down in the table.
  - Click the **DNS Configuration** tab (1). Write the DNS address(es) in the table.
- 4 If not already selected, click **Obtain IP address automatically** in the **IP Address** tab, then click **OK**.
- 5 Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with your router.

## Mac OS up to 9.x

### To manually configure network adapters in Mac OS up to 9.x:

- 1 Pull down the Apple menu. Select **Control Panels** and select **TCP/IP**. The TCP/IP control panel opens.

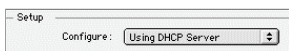


- 2 Select **Ethernet Built-In** or **Ethernet** in the **Connect via** drop-down menu (1).

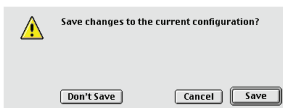
- Next to **Configure** (2), if **Manually** is selected, your router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into your router.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

- If not already set, at **Configure**, select **Using DHCP Server**. This will tell the computer to obtain an IP address from your router.



- Close the window. If you made any changes, the following window appears.



- Click **Save**.
- Restart the computer. When the computer restarts, your network settings are now configured for use with your router.

## Mac OS X

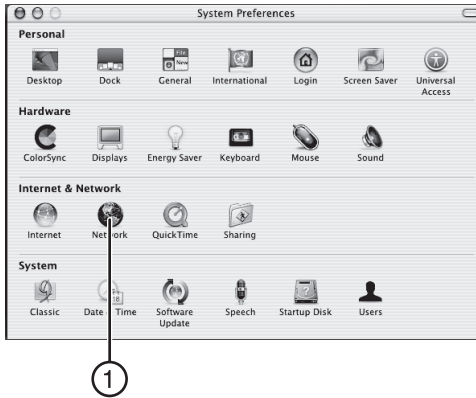
Set up the computer that is connected to the cable or DSL modem **FIRST** using these steps. You can also use these steps to add computers to your router after your router has been set up to connect to the Internet.

**To manually configure network adapters in Mac OS X:**

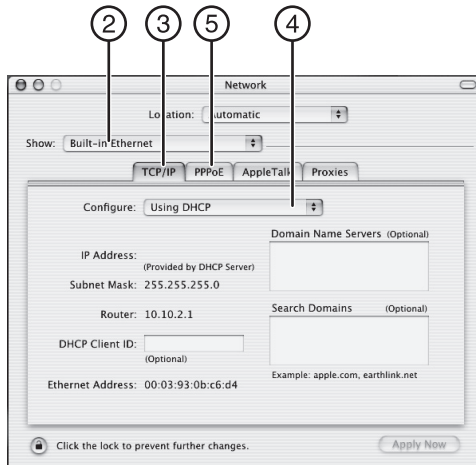
- 1 Click the **System Preferences** icon.



- 2 Select **Network** (1) from the *System Preferences* menu.



- 3 Select **Built-in Ethernet** (2) next to **Show** in the **Network** menu.



- 4 Select the **TCP/IP** tab (3). Next to **Configure** (4), you should see **Manually** or **Using DHCP**. If you do not, check the **PPPoE** tab (5) to make sure that **Connect using PPPoE** is NOT selected. If it is, you will need to configure your router for a PPPoE connection type using your user name and password.
- 5 If **Manually** is selected, your router will need to be set up for a static IP connection type. Write the address information in the table below. You will need to enter this information into your router.

IP address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Router Address:	<input type="text"/>
Name Server Address:	<input type="text"/>

- 6 If not already selected, select **Using DHCP** next to **Configure** (4), then click **Apply Now**. Your network settings are now configured for use with your router.

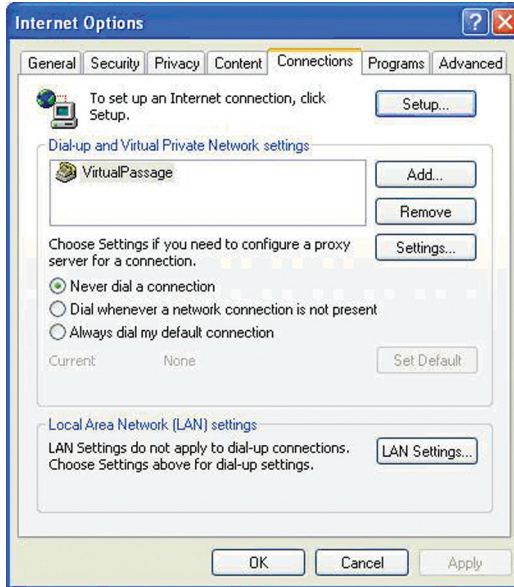
### Recommended Web browser settings

In most cases, you will not need to make any changes to your Web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

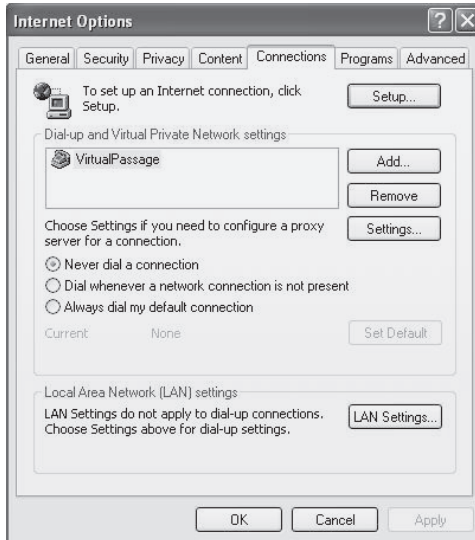


**To change settings in Internet Explorer 4.0 or higher:**

- 1 Start your Web browser. Open the *Tools* menu, then click **Internet Options**. The *Internet Options* page opens.

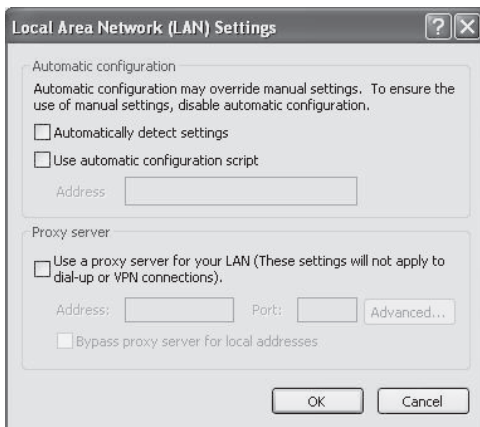


- 2 Click the **Connections** tab.



- 3 Select **Never dial a connection**. If you cannot make a selection, go to the next step.

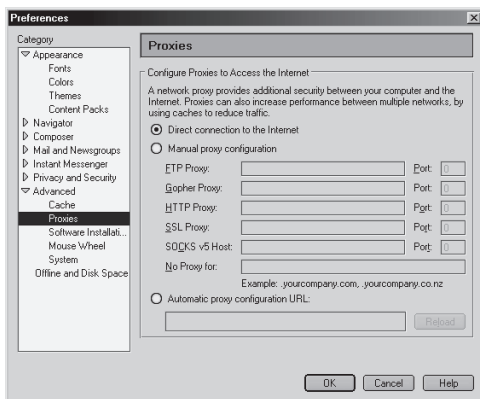
- 4 Click **LAN Settings**. The *LAN Settings* page opens.



- 5 Make sure there are no check marks next to any of the displayed options: **Automatically detect settings**, **Use automatic configurational script**, **Use a proxy server**. Click **OK** to close the page, then click **OK** again in the *Internet Options* page to exit.

To change settings in Netscape® Navigator® 4.0 or higher:

- 1 Start Netscape, then open the **Edit** menu and click **Preferences**. The *Preferences* page opens.



- 2 Click **Advanced**, then click **Proxies**.
- 3 In the **Proxies** area, click **Direct connection to the Internet**, then click **OK** to exit.

# Troubleshooting

## Placement of your router for optimal performance

Your wireless connection will be stronger the closer your computer is to your router. Typical indoor operating range for your wireless devices is between 100 and 200 feet. In the same way, your wireless connection and performance will degrade somewhat as the distance between your router and connected devices increases. This may or may not be noticeable to you. As you move farther from your router, connection speed may decrease.

Factors that can weaken signals simply by getting in the way of your network's radio waves are metal appliances or obstructions, and walls.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between five and 10 feet from the router in order to see if distance is the problem.

***Note:** While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning. If you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.*

### 1. Placement of your router

Place your router, the central connection point of your network, as close as possible to the center of your wireless network devices.

To achieve the best wireless network coverage for your "wireless clients," (for example, computers enabled by Wireless Notebook Cards, Wireless Desktop Cards, and Wireless USB Adapters):

- Make sure that your router's antennas are parallel to each other, and are positioned vertically (toward the ceiling). If your router itself is positioned vertically, point the antennas as much as possible in an upward direction.
- In multistory homes, place the router on a floor that is as close to the center of the home as possible. This may mean placing your router on an upper floor.
- Try not to place your router near a cordless 2.4 GHz phone.

### 2. Avoid obstacles and interference

Avoid placing your router near devices that may emit radio "noise", such as microwave ovens. Other objects that can inhibit wireless communication can include:

- Refrigerators
- Washers or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path between your computers and router.

### 3. Cordless phone placement

If the performance of your wireless network is impaired after attending to the above issues, and you have a cordless phone:

- Try moving cordless phones away from your router and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4 GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network as possible. For example, change the phone to channel 1 and move your router to channel 11. (Your channel selection will vary depending on your region.) See your phone's user guide for detailed instructions.
- If necessary, consider switching to a 900 MHz or 5 GHz cordless phone.

### 4. Choose the "quietest" channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with yours. Use the Site Survey capabilities of your Wireless Networking Utility to locate any other wireless networks, and move your router and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices.

For more wireless networking products from Dynex, use the detailed Site Survey and wireless channel information included in your User Guide.

These guidelines should let you cover the maximum possible area with your router. If you need to cover an even wider area, we suggest the Dynex Wireless G Range Extender/Access Point.

### 5. Secure connections, VPNs, and AOL

Secure connections typically require a user name and password, and are used where security is important. Secure connections include:

- Virtual Private Network (VPN) connections, often used to connect remotely to an office network
- The "Bring Your Own Access" program from America Online (AOL), which lets you use AOL through broadband provided by another DSL or cable service
- Most online banking Web sites
- Many commercial Web sites that require a user name and password to access your account Secure connections can be interrupted by a computer's power management setting, which causes it to "go to sleep." The simplest solution to avoid this is to simply reconnect by re-running the VPN or AOL software, or by re-logging into the secure Web site.

A second alternative is to change your computer's power management settings so it does not go to sleep. However, this may not be appropriate for portable computers. To change your power management setting in Windows, see the **Power Options** item in the **Control Panel**.

If you continue to have difficulty with Secure Connections, VPNs, and AOL, review the items above to be sure you have addressed these issues.

**Problem: Setup Assistant CD does not automatically start.**

**Solution:** If the CD does not start the Setup Assistant automatically, it could be that the computer is running other applications that are interfering with the CD drive.

**To solve the problem:**

- 1 If the Setup Assistant screen does not appear within 15-20 seconds, open your CD drive by double-clicking the **My Computer** icon located on your desktop.
- 2 Double-click the CD drive containing the Setup Assistant Software CD.
- 3 The Setup Assistant should start within a few seconds. If a window opens showing the files on the CD, double-click the icon labeled SetupAssistant.
- 4 If the Setup Assistant still does not start, see "Manually configuring network settings" on page 46 for an alternate setup method.

**Problem: The Setup Assistant cannot find my router.**

**Solution:** If the Setup Assistant is not able to find your router during the installation process, check the following items:

**To solve the problem:**

- 1 If the Setup Assistant is not able to find your router during the installation process, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

If you do have firewall software installed on your computer, make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled, Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

Refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

- 2 Unplug the AC adapter from your router for 10 seconds, and then plug the adapter back into your router. Make sure that your router's LED is on and solid blue. If not, make sure that the AC adapter is correctly connected to your router and plugged into a power outlet.
- 3 Make sure that you have a cable (use the cable included with your router) connected between the network (Ethernet) port on the back of the computer and one of the LAN ports, labeled "1" through "4," on the back of your router.

**Note:** The computer should NOT be connected to the port labeled "to Modem" on the back of your router.

- 4 Try shutting down and restarting your computer, then rerunning the Setup Assistant.

If the Setup Assistant is still unable to find your router, see "Manually configuring network settings" on page 46 for an alternate setup method.

**Problem: The Setup Assistant cannot connect my router to the Internet.**

**Solution:** If the Setup Assistant is not able to connect your router to the Internet, check the following items:

**To solve the problem:**

- 1 Use the troubleshooting suggestions within the Setup Assistant.
- 2 If your ISP requires a user name and password, make sure that you have typed in your user name and password correctly. Some user names require that the ISP's domain be at the end of the name. For example: **myname@myisp.com**. The **@myisp.com** part of the user name may need to be typed as well as your user name.

If you continue to have no Internet connection, see "Manually configuring network settings" on page 46 for an alternate setup method.

**Problem: The Setup Assistant completed installation, but my Web browser doesn't work.****I am unable to connect to the Internet. My router's modem LED is off and the internet LED is blinking.**

**Solution:** If you cannot connect to the Internet, the MODEM led is off, and the internet LED is blinking, the problem may be that your modem and router are not connected properly.

**To solve the problem:**

- 1 Make sure that the network cable between the modem and your router is connected. The cable should be connected to your router's modem port and to the network port on your modem.
- 2 Unplug the cable or DSL modem from its power outlet for three minutes. After three minutes, plug the modem back into its power outlet. This may force the modem to properly recognize your router.
- 3 Unplug the power to your router, wait 10 seconds, and then reconnect the power. This will cause your router to reattempt communication with the modem. If the modem LED on your router is not lit after completing these steps, contact Dynex Technical Support.
- 4 Try shutting down and restarting your computer.

**Problem: The Setup Assistant completed installation, but my Web browser doesn't work.****I am unable to connect to the Internet. The router's modem led is on and the internet LED is blinking.**

**Solution:** If you cannot connect to the Internet, the modem LED is on, and the internet LED is blinking, the problem may be that your connection type may not match the ISP's connection.

**To solve the problem:**

- 1 If you have a *static IP address* connection, your ISP must assign you the IP address, subnet mask, and gateway address. See "Alternative setup method" on page 16 for details on changing this setting.
- 2 If you have a PPPoE connection, your ISP will assign you a user name and password and sometimes a service name. Make sure that your router's connection type is configured to PPPoE and the settings are entered properly. Refer to "Alternative setup method" on page 16 for details on changing this setting. You may need to configure your router to meet the specific requirements of your ISP.

If you are still unable to access the Internet after verifying these settings, contact Dynex Technical Support.

**Problem: The Setup Assistant completed, but my Web browser doesn't work.****I am unable to connect to the Internet. The modem LED on my router is blinking and the internet LED is solid.**

**Solution:** If the modem LED is blinking and the internet LED is solid, but you are unable to access the Internet, there may be third-party firewall software installed on the computer attempting to access the Internet. Examples of third-party firewall software are ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, and Norton Personal Firewall.

If you do have firewall software installed on your computer, make sure that you properly configure it. You can determine if the firewall software is preventing Internet access by temporarily turning it off. If, while the firewall is disabled and Internet access works properly, you will need to change the firewall settings to function properly when it is turned on.

Refer to the instructions provided by the publisher of your firewall software for instructions on configuring the firewall to allow Internet access.

If you are still unable to access the Internet after disabling any firewall software, please contact Dynex Technical Support.

**Problem: I can't connect to the Internet wirelessly.**

**Solution:** If you are unable to connect to the Internet from a wireless computer, do the following.

**To solve the problem:**

- 1 Look at the lights on your router. They should be as follows:
  - The "router" LED should be on.
  - The "modem" light should be on, and not blinking.
  - The "internet" LED should be on, and not blinking.
  - The "Wireless" light should be on, and not blinking.
- 2 Open your wireless utility software by clicking the icon in the system tray at the bottom, right-hand corner of the screen.

The exact window that opens will vary depending on the model of wireless card you have; however, any of the utilities should have a list of **Available Networks**—those wireless networks it can connect to.
- 3 Does the name of your wireless network appear in the results?
  - Yes, my network name is listed—Go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, but my network name is listed."
  - No, my network name is not listed—Go to the troubleshooting solution titled "I can't connect to the Internet wirelessly, and my network name is not listed."

**Problem: I can't connect to the Internet wirelessly, but my network name is listed.**

**Solution:** If the name of your network is listed in the **Available Networks** list, follow the steps below to connect wirelessly.

**To solve the problem:**

- 1 Click the correct network name in the **Available Networks** list.
- 2 If the network has security (encryption) enabled, you will need to enter the network key. For more information regarding security, see "Changing system settings" on page 44.

Within a few seconds, the tray icon in the lower, right corner of your screen should turn green, indicating a successful connection to the network.

**Problem: I can't connect to the Internet wirelessly, and my network name is not listed.**

**Solution:** If the correct network name is not listed under **Available Networks** in the wireless configuration utility, attempt the following troubleshooting steps:

**To solve the problem:**

- 1 Temporarily move your computer, if possible, 5 to 10 feet away from your router. Close the wireless configuration utility, and reopen it. If the correct network name now appears under **Available Networks**, you may have a range or interference problem. See the suggestions discussed in "Placement of your router for optimal performance" on page 55.



- 2 Using a computer that is connected to your router through a network cable (as opposed to wirelessly), make sure that **Broadcast SSID** is enabled. This setting is found on your router's wireless *Channel and SSID* configuration page.

If you are still unable to access the Internet after disabling any firewall software, please contact Dynex Technical Support.

**Problem: My wireless network performance is inconsistent.**

**Data transfer is sometimes slow.**

**Signal strength is poor.**

**I am having difficulty establishing and/or maintaining a Virtual Private Network (VPN) connection.**

**Solution:** Wireless technology is radio-based, which means connectivity and the throughput performance between devices decreases when the distance between devices increases. Other factors that will cause signal degradation (metal is generally the worst culprit) are obstructions such as walls and metal appliances. Note also that connection speed may decrease as you move farther away from your router.

In order to determine if wireless issues are related to range, we suggest temporarily moving the computer, if possible, five to 10 feet away from your router.

**Changing the Wireless Channel**

Depending on local wireless traffic and interference, switching the wireless channel of your network can improve performance and reliability. The default channel your router is shipped with is channel 11. You may choose from several other channels depending on your region (see "Changing the Wireless Channel" on page 26 for instructions on how to choose other channels).

**Limiting the Wireless Transmit Rate**

Limiting the wireless transmit rate can help improve the maximum wireless range, and connection stability. Most wireless cards have the ability to limit the transmission rate. To change this property, go to the *Windows Control Panel*, open **Network Connections**, and double-click your wireless card's connection. In the *Properties* dialog box, select the **Configure** button on the **General** tab (Windows 98 users will have to select the wireless card in the list box and then click **Properties**), then choose the **Advanced** tab and select the rate property.

Wireless client cards are usually set to automatically adjust the wireless transmit rate for you, but doing so can cause periodic disconnects when the wireless signal is too weak. As a rule, slower transmission rates are more stable. Experiment with different connection rates until you find the best one for your environment. Note that all available transmission rates should be acceptable for browsing the Internet. For more assistance, see your wireless card's user manual.

## **Problem: I am having difficulty setting up Wired Equivalent Privacy (WEP) security on your router.**

### **To solve the problem:**

- 1** Log into your router.
- 2** Open your Web browser and type the IP address of your router. (Your router's default is 192.168.2.1.) Log into your router by clicking the **Login** button in the top, right-hand corner of the screen. You will be asked to enter your password. If you never set a password, leave the password field blank, then click **Submit**.
- 3** Click the **Wireless** tab on the left of your screen. Select the **Encryption or Security** tab to go to the security settings page.
- 4** Select **128-bit WEP** from the drop-down menu.
- 5** After selecting your WEP encryption mode, you can type your hex WEP key manually, or you can type a passphrase in the **Passphrase** field, then click **Generate** to create a WEP key from the passphrase. Click **Apply Changes** to finish. You must now set all of your clients to match these settings. A hex (hexadecimal) key is a combination of numbers and letters from A-F and 0-9. For 128-bit WEP, you need to enter 26 hex keys. For example: **C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4** = 128-bit key
- 6** Click **Apply Changes** to finish. Encryption in your router is now set. Each of your computers on your wireless network will now need to be configured with the same security settings.

**Caution:** *If you are configuring your router from a computer with a wireless client, you will need to ensure that security is turned on for this wireless client. If this is not done, you will lose your wireless connection.*

**Note to Mac users:** *Original Apple AirPort products support 64-bit encryption only. Apple AirPort 2 products can support 64-bit or 128-bit encryption. Check your Apple AirPort product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.*

**Problem: I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Dynex client card (wireless network card or adapter).**

**Solution:** The client card must use the same key as your router. For instance, if your router uses the key 00112233445566778899AABBCC, then the client card must be set to the exact same key.

**To solve the problem:**

- 1 Double-click the **Signal Indicator** icon to bring up the *Wireless Network Utility* screen. Click the **Advanced** button to view and configure more options of your client card.
- 2 Click the **Wireless Network Properties** tab, then select a network name from the **Available Networks** list and click the **Properties** button.
- 3 Under **Data Encryption**, select **WEP**.
- 4 Make sure that the **The key is provided for me automatically** box at the bottom is unchecked. If you are using this computer to connect to a corporate network, consult your network administrator to see if this box needs to be checked.
- 5 Type your WEP key in the **Network key** box.

**Important:** A WEP key is a combination of numbers and letters from A-F and 0-7. For 128-bit WEP, you need to enter 26 keys. This network key needs to match the key you assign to your router.

For example: **C3030FAF4BB2C3D44BC3D4E7E4** = 128-bit key

- 6 Click **OK**, then click **Apply** to save the settings.

If you are NOT using a Dynex wireless client card, consult the manufacturer's user manual for that wireless client card.

**Problem: Do Dynex products support WPA/WPA2?****Solution:**

**Note:** To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this publication, a security patch download is available, for free, from Microsoft. This patch works only with the Windows XP operating system.

Download the patch here:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&displaylang=en>

You also need to download the latest driver for your Dynex wireless 802.11n desktop or notebook network card from the Dynex support site. Other operating systems are not supported at this time. Microsoft's patch only supports devices with WPA-enabled drivers such as Dynex 802.11n products.

Download the latest driver at <http://www.dynexproducts.com>.

**Problem: I am having difficulty setting up Wireless Protected Access (WPA) security on my router for a home network.****To solve the problem:**

- 1 Select **WPA-PSK (no server)** from the **Security Mode** drop-down menu.
- 2 For **Encryption Technique**, select **TKIP** or **AES**. This setting will have to be identical on the clients that you set up.
- 3 Enter your pre-shared key. This can be from eight to 63 characters and can be letters, numbers, symbols, or spaces. This same key must be used on all of the clients that you set up. For example, your PSK might be something like: "Smith family network key".
- 4 4. Click **Apply Changes** to finish. You must now set all clients to match these settings.

**Problem: I am having difficulty setting up Wireless Protected Access (WPA) security on a Dynex client card (wireless network card or adapter) for a home network.**

**Solution:** Clients must use the same key that your router uses. For instance, if the key is "Smith Family Network Key" in your router, the clients must also use that same key.

**To solve the problem:**

- 1 Double-click the **Signal Indicator** icon to bring up the *Wireless Network Utility* screen.
- 2 Click the **Advanced** button. The Dynex Wireless LAN Utility will open. This Utility lets you manage all the advanced features of the Dynex wireless card.
- 3 Click the **Wireless Network Properties** tab, select a network name from the **Available Networks** list, then click the **Properties** button. The *Properties* page opens.
- 4 Under Network Authentication, select **WPA-PSK (no server)**.
- 5 Type your WPA key in the **Network key** box.

**Important:** WPA-PSK is a combination of numbers and letters from A-Z and 0-9. For WPA-PSK, you can enter eight to 63 characters. This network key needs to match the key you assign to your router.

6. Click **OK**, then **Apply** to save the settings.

**Problem: I am having difficulty setting up Wi-Fi Protected Access (WPA) security and I am NOT using a Dynex client card for a home network.**

**Solution:** If you are NOT using a Dynex wireless N USB or wireless N notebook network card and it is not equipped with WPA-enabled software, a file from Microsoft called “Windows XP Support Patch for Wireless Protected Access” is available for free download:

Download the patch from Microsoft by searching the knowledge base for “Windows XP WPA.”

***Note:** The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time. You also need to ensure that the wireless card manufacturer supports WPA and that you have downloaded and installed the latest driver from their support site.*

Supported Operating Systems:

- Windows XP Professional
- Windows XP Home Edition

**To enable WPA-PSK (no server):**

- 1** 1. In systems running Windows XP, click **Start, Control Panel, Network Connections**.
- 2** Right-click the **Wireless Networks** tab. The *Wireless Network Connection Properties* screen opens. Make sure that the **Use Windows to configure my wireless network settings** box is checked.
- 3** Back on the **Wireless Networks** tab, click the **Configure** button. The *Client Card Properties* screen opens.
- 4** For a home or small business user, select **WPA-PSK** under **Network Administration**.  
***Note:** Select WPA (with radius server) if you are using this computer to connect to a corporate network that supports an authentication server such as a radius server. Consult your network administrator for further information.*
- 5** Select **TKIP** or **AES** under **Date Encryption**. This setting will have to be identical to your router that you set up.
- 6** Type your encryption key in the **Network key** box.  
***Important:** Enter your pre-shared key. This can be from eight to 63 characters (letters, numbers, or symbols). The same key must be used on all of the clients that you set up.*
- 7** Click **OK** to apply settings.

## What's the difference between 802.11g and draft 802.11n?

Currently there are three commonly used wireless networking standards, which transmit data at very different maximum speeds. Each is based on the designation for certifying network standards. The most common wireless networking standard, 802.11g, can transmit information up to 54 Mbps. 802.11a also supports up to 54 Mbps, but in the 5 GHz frequency. 802.11n draft specification can connect at up to 300 Mbps. See the following table for more detailed information.

Wireless Technology	<b>G (802.11g)</b>	<b>Enhanced G (802.11g)</b>	<b>N (draft 802.11n)</b>	<b>N1 MIMO (draft 802.11n with MIMO)</b>
Speed/data rate	Up to 54 Mbps*	Up to 54 Mbps*	Up to 300 Mbps*	Up to 300 Mbps*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4 GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4 GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4 GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4 GHz
Compatibility	Compatible with 802.11b/g	Compatible with 802.11b/g	Compatible with draft 802.11n** and 802.11b/g	Compatible with draft 802.11n** and 802.11b/g
Coverage*	Up to 400 feet (121.9 m)*	Up to 1,000 feet (304.8 m)*	Up to 1,200 feet (365.8 m)*	Up to 1,400 feet (426.7 m)*
Advantage	Common—widespread use for Internet sharing	Better coverage and consistent speed and range	Enhanced speed and coverage	Leading edge—best coverage and throughput

*\*Distance and connection speeds will vary depending on your networking environment.*

*\*\*\*\*This Router is compatible with products based on the same version of the draft 802.11n specifications and may require a software upgrade for best results.*

# Legal notices

## FCC Statement

### **Declaration of Conformity with Fcc Rules for Electromagnetic Compatibility**

We, the Dynex Corporation, of 7601 Penn Avenue South, Richfield, Minnesota, U.S.A., declare under our sole responsibility that the product, DX-WGRTR, to which this declaration relates, 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.

### **Caution: Exposure to Radio Frequency Radiation.**

The radiated output power of this device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized. When connecting an external antenna to the device, the antenna shall be placed in such a manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

### **FCC warning**

Changes or modifications not expressly approved by the party responsible for compliance with the FCC Rules could void the user's authority to operate this equipment.

### **DHHS and FDA safety certification**

This product is made and tested to meet safety standards of the FCC, requirements and compliance with safety performance of the U.S. Department of Health and Human Services, and also with FDA Radiation Performance Standards 21 CFR Subchapter J.

### **Canada ICES-003 statement**

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

### **FCC Part 15**

This device complies with Part 15 of the FCC Rules. Operation of this product 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.

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

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

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

**RSS 210 statement**

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.



# One-Year Limited Warranty

Dynex Products ("Dynex") warrants to you, the original purchaser of this new **DX-NRUTER** ("Product"), that the Product shall be free of defects in the original manufacture of the material or workmanship for a period of one (1) year from the date of your purchase of the Product ("Warranty Period"). This Product must be purchased from an authorized dealer of Dynex brand Products and packaged with this warranty statement. This warranty does not cover refurbished product. If you notify Dynex during the Warranty Period of a defect covered by this warranty that requires service, terms of this warranty apply.

## How long does the coverage last?

The Warranty Period lasts for one year (365 days) from the date you purchased the Product. The purchase date is printed on the receipt you received with the Product.

## What does this warranty cover?

During the Warranty Period, if the original manufacture of the material or workmanship of the Product is determined to be defective by an authorized Dynex repair center or store personnel, Dynex will (at its sole option): (1) repair the Product with new or rebuilt parts; or (2) replace the Product at no charge with new or rebuilt comparable products or parts. Products and parts replaced under this warranty become the property of Dynex and are not returned to you. If service of products and parts are required after the Warranty Period expires, you must pay all labor and parts charges. This warranty lasts as long as you own your Dynex Product during the Warranty Period. Warranty coverage terminates if you sell or otherwise transfer the Product.

## How to obtain warranty service?

If you purchased the Product at a retail store location, take your original receipt and the Product to the store you purchased it from. Make sure that you place the Product in its original packaging or packaging that provides the same amount of protection as the original packaging. If you purchased the Product from an online web site, mail your original receipt and the Product to the address listed on the web site. Make sure that you put the Product in its original packaging or packaging that provides the same amount of protection as the original packaging.

To obtain in-home warranty service for a television with a screen 25 inches or larger, call 1-888-BESTBUY. Call agents will diagnose and correct the issue over the phone or will have an Dynex-approved repair person dispatched to your home.

## Where is the warranty valid?

This warranty is valid only to the original purchaser of the Product in the United States, Canada, and Mexico.

## What does the warranty not cover?

This warranty does not cover:

- Customer instruction
- Installation
- Set up adjustments
- Cosmetic damage
- Damage due to acts of God, such as lightning strikes
- Accident
- Misuse
- Abuse
- Negligence
- Commercial use
- Modification of any part of the Product
- Plasma display panel damaged by static (non-moving) images applied for lengthy periods (burn-in).

This warranty also does not cover:

- Damage due to incorrect operation or maintenance
- Connection to an incorrect voltage supply
- Attempted repair by anyone other than a facility authorized by Dynex to service the Product
- Products sold as is or with all faults
- Consumables, such as fuses or batteries
- Products where the factory applied serial number has been altered or removed

REPAIR REPLACEMENT AS PROVIDED UNDER THIS WARRANTY IS YOUR EXCLUSIVE REMEDY. DYNEX SHALL NOT BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR THE BREACH OF ANY EXPRESS OR IMPLIED WARRANTY ON THIS PRODUCT, INCLUDING, BUT NOT LIMITED TO, LOST DATA, LOSS OF USE OF YOUR PRODUCT, LOST BUSINESS OR LOST PROFITS. DYNEX PRODUCTS MAKES NO OTHER EXPRESS WARRANTIES WITH RESPECT TO THE PRODUCT, ALL EXPRESS AND IMPLIED WARRANTIES FOR THE PRODUCT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO THE WARRANTY PERIOD SET FORTH ABOVE AND NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WILL APPLY AFTER THE WARRANTY PERIOD. SOME STATES, PROVINCES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE OR PROVINCE TO PROVINCE.

Contact Dynex:

For customer service please call 1-800-305-2204

[www.dynexproducts.com](http://www.dynexproducts.com)

Distributed by Best Buy Purchasing, LLC

7601 Penn Avenue South, Richfield, Minnesota, U.S.A. 55423-3645

© 2008 Best Buy Enterprise Services, Inc.

All rights reserved. DYNEX is a trademark of Best Buy Enterprise Services, Inc. Registered in some countries. All other products and brand names are trademarks of their respective owners.

**DYNEX**™

ENGLISH  
08-1501  
PM01437

[www.dynexproducts.com](http://www.dynexproducts.com) (800) 305-2204

© 2008 Best Buy Enterprise Services, Inc. All rights reserved.  
DYNEX is a trademark of Best Buy Enterprise Services, Inc. Registered in some countries. All other  
products and brand names are trademarks of their respective owners.  
Distributed by Best Buy Purchasing, LLC  
7601 Penn Ave. South, Richfield, MN 55423 U.S.A.