DYNEX®

Wireless Enhanced G Router

Routeur sans fil G amélioré

Enrutador inalámbrico G mejorado

DX-WEGRTR

USER GUIDE

GUIDE DE L'UTILISATEUR • GUÍA DEL USUARIO

Dynex DX-WEGRTR Wireless Enhanced G Router

Contents

Introduction

Thank you for purchasing the Dynex DX-WEGRTR Wireless Enhanced G 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 "Placement of your router for optimal performance" on page 47.

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 Easy Installation Wizard 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

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 new Dynex wireless enhanced G router an ideal solution for your home or small office network.

Works with Both PCs and Mac® Computers—The router supports a variety of networking environments including Mac OS®, X v10.x, Linux®, Windows® 2000, XP, 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 the 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 the 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—The 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 the 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.

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

> ***Note**: Easy Install Wizard software is compatible with Windows 2000, XP, Vista, and Mac OS Mac OSx 10.4.x. If you are using another operating system, the wireless router can be set up using the Alternate Setup Method described in this User Guide (see Alternate setup method on page 15.*

Enhanced G Mode*–Enhanced G Mode, a 54g performance enhancement, provides the fastest wireless connectivity for 802.11g-capable networks in real-world environments. It is designed for home networks that require additional bandwidth for applications such as sharing digital pictures. Enhanced G makes 802.11g WLANs more efficient without affecting the performance of neighboring networks, and is compatible at high speeds with leading brands.

> **When operating in 125 Enhanced G Mode, this Wi-Fi device achieves an actual throughput of up to 34.1 Mbps, which is the equivalent throughput of a system following 802.11g protocol and operating at a signaling rate of 125 Mbps. Actual throughput will vary depending on environmental, operational, and other factors.*

Integrated 802.11g Wireless Access Point—802.11g is an exciting new wireless technology that achieves data rates up to 54 Mbps, nearly five times faster than 802.11b.

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 Wireless Enhanced G Router
- Quick Installation Guide
- Installation software CD
- RJ-45 Ethernet cable
- Power supply
- User Guide

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

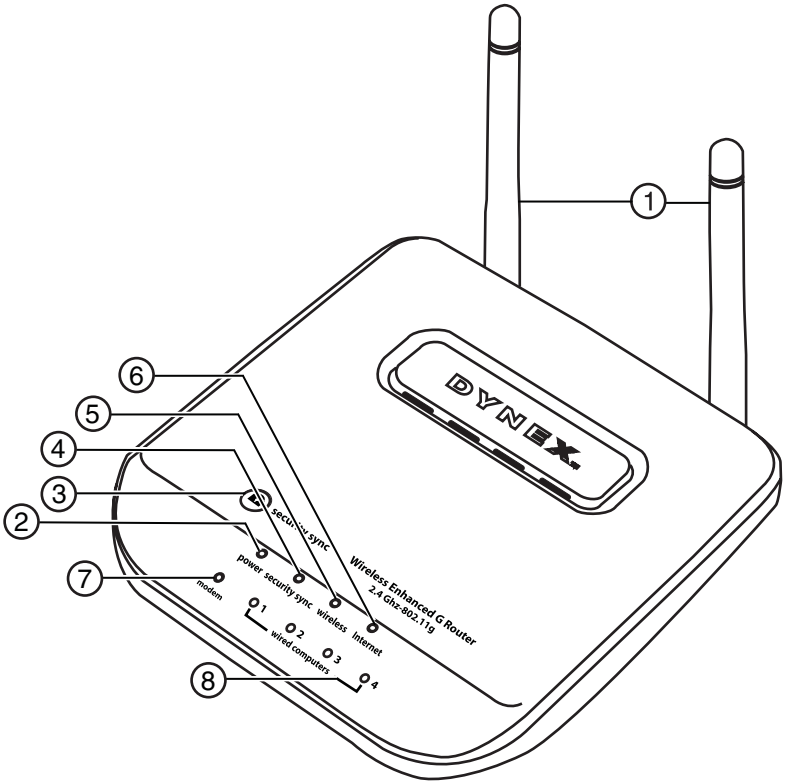
Easy Install Wizard Software System Requirements

- A PC running Windows 2000, XP, or Vista, or a Mac computer running Mac OSx 10.4x
- A minimum 64 MB RAM
- An Internet browser

Components

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

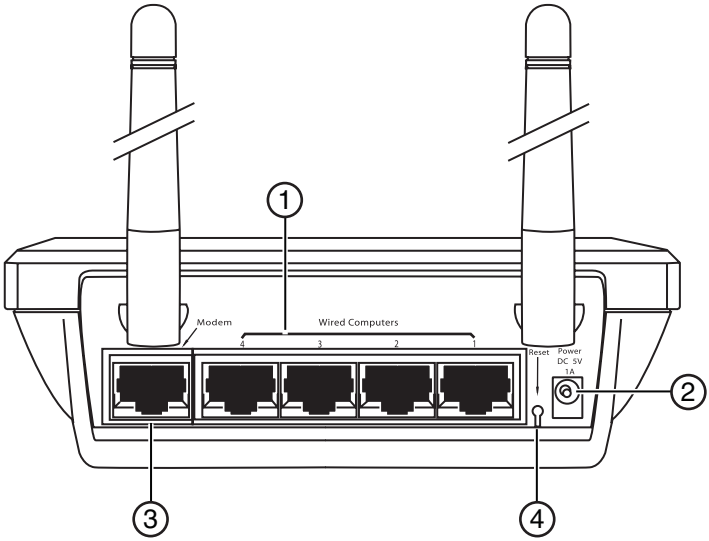
Front panel



#	Component	Description
1	Antennas	Lets the router communicate with a wireless client (card or USB adapter).
2	Power/ready LED	When you apply power to the router or restart it, a short period of time elapses while the router boots up. During this time, the Power/Ready LED blinks. When the Router has completely booted up, the Power/Ready LED becomes a SOLID light, indicating the router is ready for use. Off—Router is off Blinking Green—Router is booting up Solid Green—Router is ready

#	Component	Description
3	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. Pushing the Security Sync button will automatically enable WPS. See "Using Security Sync (Wi-Fi Protected Setup)" on page 28.
4	Security Sync LED	Lights to indicate that WPS has been activated. Blinking Green—The router is searching for a WPS client to connect with. Solid Green—The secure connection has been established with the client.
4	Wireless network LED	Off—The wireless network is off Solid Green—The wireless network is ready Blinking Green—Network activity
5	Internet LED	This unique LED shows you when the router is connected to the Internet. When the light is OFF, the router is not connected to the Internet. When the light is blinking, the router is attempting to connect to the Internet. When the light is solid green, the 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. 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
6	Modem status LED	This LED lights green to indicate that your modem is connected properly to the router. It blinks rapidly when information is being sent over the port between the router and the modem. Off—No WAN link Solid Green—Good WAN link Blinking Green—WAN activity
7	Wired computer status LEDs	These LEDs are labeled 1-4 and correspond to the numbered ports on the rear of the router. When a computer is properly connected to one of the wired computer ports on the rear of the router, the LED will light. green means a 10Base-T device is connected, orange means a 100Base-T device is connected. When information is being sent over the port, the LED blinks rapidly. 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

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 the router.
2	Power jack	The 5 V DC power supply plugs into this jack.
3	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.
4	Reset button	The **Reset** button is used in rare cases when the router may function improperly. Resetting the router restores the 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. **Resetting the router**—Push and release the **Reset** button. The lights on the router will momentarily flash. The Power/Ready light will begin to blink. When the Power/Ready light becomes solid again, the reset is complete. Restoring the Factory Defaults—Press and hold the **Reset** button for at least 10 seconds, then release it. The lights on the router will momentarily flash. The Power/Ready light will begin to blink. When the Power/Ready light becomes solid again, the restore is complete.

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 Windows 2000 or XP 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 "Alternate Setup Method" section of this User Guide to configure your router. Additionally, if you are using an operating system other than Windows 2000 or XP, you must set up the router using the "Alternate Setup Method" section of this User Guide.

Hardware connections

To connect the hardware:

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

Running the Setup Assistant software

To run the Setup Assistant software:

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 Installation CD into your computer. The Setup Assistant will automatically appear on your computer's screen within 15 seconds. Double-click the Setup Assistant to run it, then follow the on-screen instructions.

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

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

The 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). This is the name of your wireless network to which your computers or devices with wireless network adapters will connect.

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. The *Internet Account Info* screen opens.

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 the router and restarting it. Wait for the on-screen instructions.

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

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

This completes the 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**.

To troubleshoot the setup:

1 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 simply 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 this 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 take you back to the main menu.

Wireless Security Setup

Be sure to 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 the router, open up 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**.

3 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**.

4 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**.

5 Now go to each of your wireless computers. Use the wireless utility software on each to do the following (see you wireless adapter's user manual for more detailed instructions):

a. Find your wireless network and connect to it.

b. 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 wit h WPA/WPA2, return to Step 4 and choose WEP. See "WEP Setup" on page 30 for instructions on setting up WEP.

Alternate setup method

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

- View the router's current settings and status
- Configure the 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 the 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 the router's internal password
- Enable/Disable UPnP (Universal Plug-and-Play)
- Reset the router
- Back up your configuration settings
- Reset the router's default settings
- Update the router's firmware

To connect your router (step 1):

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 the 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 the router's power jack.
7. Make sure that your modem is connected to the router by checking the lights on the front of the router. The green light labeled **Modem** should be on if your modem is connected correctly to the router. If it is not, recheck your connections.
8. Make sure that your computer is connected properly to the 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 44 for directions.

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

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

   ***Note**: If you have difficulty accessing the router's Web-Based Advanced User Interface, go to the section entitled "Manually Configuring Network Settings".*

2. To make any changes to the router's settings, you have to log in. Click **Login**, or click on any one of the links on the home page to go to the login screen.
3. In the login screen, leave the password blank (the router ships with no password entered) and click **Submit** to log in.

   One computer at a time can log into the router for the purposes of making changes to the settings of the router.
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 -
5. 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 42.

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 the 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 the 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 on 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 the router. When the indicator says **connection OK** in green, the router is connected to the Internet. When the 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 the router.

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

Help Button—The **Help** button gives you access to the router's help pages. Help is also available on many pages by clicking **more info** next to certain sections of each page.

LAN Settings—Shows you the settings of the Local Area Network (LAN) side of the router. Changes can be made to the settings by clicking on 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 the router's NAT, firewall, and wireless features. Changes can be made to the settings by clicking on 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 the router that connects to the Internet. Changes to any of these settings can be made by clicking on the links or by clicking on 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 the 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). The router is capable of connecting to virtually any ISP's system provided you have correctly configured the router's settings for your ISP's connection type. Your ISP connection settings are provided to you by your ISP.

To configure the 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, clicking **DNS** lets you enter DNS address entries for ISPs that require specific settings.
3. Click **MAC address** to clone your computer's MAC address or type in a specific WAN MAC address, if required by your ISP.
4. 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 in 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; or
- You have to double-click on a desktop icon other than your browser to get on the Internet.

Enter the following:

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

Password–Type in your password and re-type 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 minutes...–This feature is used to automatically disconnect the 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 the 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 the 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 the 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 the 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 the router was installed. Click
2. Click **Clone**, then click **Apply Changes**. Your MAC address is now cloned to the router.

To enter a specific MAC Address:

- Type in a MAC address in the spaces provided, then click **Apply Changes** to save the changes. The 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 the router's Web-Based Advanced User Interface. Open your browser and enter **192.168.2.1** (do not type in anything else such as "http:// " or "www"), then press **Enter**. The router's home page opens in your browser window.

Viewing the LAN Settings

Clicking on the header of the **LAN Setup** tab 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 the router can be viewed and changed here.

IP Address–The *IP address* is the internal IP address of the 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 in 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 Dynex 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 the 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 on the header of the **Wireless** tab will take you to the *Wireless* page. Under the **Wireless** tab, there are links that allow you to make changes to the wireless network settings.

Changing the Wireless Network Name (SSID)

To identify your wireless network, an SSID (Service Set Identifier) is used. The default SSID of the router is "Dynex". You can change this to anything you want to or you can leave it unchanged. If there are other wireless networks operating in your area, you will want to make sure that your SSID is unique (does not match that of another wireless network in the area). To change the SSID, type in 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: "g and b", "g only", and "b only". The different modes are explained below.

g and b Mode–In this mode, the router is compatible with 802.11b and 802.11g wireless clients simultaneously. This is the factory default mode and ensures successful operation with all Wi-Fi-compatible devices. If you have a mix of 802.11b and 802.11g clients in your network, we recommend setting the router to g and b mode. This setting should only be changed if you have a specific reason to do so.

g only Mode–g only 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**.

b only Mode–We recommend you DO NOT use this mode unless you have a very specific reason to do so. This mode exists only to solve unique problems that may occur with some 802.11b client adapters and is NOT necessary for interoperability of 802.11g and 802.11b standards.

When to use b only Mode

In some cases, older 802.11b clients may not be compatible with 802.11g wireless. These adapters tend to be of inferior design and may use older drivers or technology. Switching to this mode can solve problems that sometimes occur with these clients. If you suspect that you are using a client adapter that falls into this category of adapters, first check with the adapter vendor to see if there is a driver update. If there is no driver update available, switching to b only mode may fix your problem. Please note that switching to b only mode will decrease 802.11g performance.

Enhanced G Mode*–The router supports two high-speed modes, 125 Enhanced G mode and frame-bursting mode.

Selecting 125 Enhanced G mode will result in all devices running in 125 Enhanced G mode if all devices are capable of 125 Mbps speeds. If any non-125 Enhanced G devices connect or associates with the network, the router will automatically shift the entire network back to frame-bursting mode.

Selecting **Frame Bursting** results in all devices capable of frame-bursting to function in frame-bursting mode, and all clients not capable, to operate in normal 802.11g modes. frame-bursting mode supports both frame-bursting-enabled devices and non-frame-bursting-enabled devices simultaneously. Frame-bursting mode is based on the unreleased 802.11e specification.

Selecting **Off** will disable Turbo mode.

**When operating in 125 Enhanced G Mode, this Wi-Fi device achieves an actual throughput of up to 34.1 Mbps, which is the equivalent throughput of a system following 802.11g protocol and operating at a signaling rate of 125 Mbps. Actual throughput will vary depending on environmental, operational, and other factors.*

QoS (Quality of Service) Configuration–QoS prioritizes important data on your network such as multimedia content and Voice over IP (VoIP) so it will not be interfered with by other data being sent over the network. Based on 802.11e, you can turn this feature on or off by selecting it from the drop-down menu (3) and choosing the acknowledgement mode you want to use. If you plan to stream multimedia content or use VoIP on your network, we recommend that you enable the QoS feature.

Changing the Wireless Channel

There are a number of operating channels you can choose from. 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 you reside in. The default channel is 11 (unless you are in a country that does not allow channel 11). 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. For best performance, use a channel that is at least five channels away from the other wireless network. For instance, if another network is operating on channel 11, then set your network to channel 6 or below. To change the channel, select the channel from the list, then click **Apply Changes**. The change is immediate.

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–As part of the 802.11g specification, Protected mode ensures proper operation of 802.11g clients and access points when there is heavy 802.11b traffic in the operating environment. When Protected mode is **ON**, 802.11g scans for other wireless network traffic before it transmits data. Therefore, using this mode in environments with HEAVY 802.11b traffic or interference achieves best performance results. If you are in an environment with very little-or no-other wireless network traffic, your best performance will be achieved with Protected mode **OFF**.

Securing your Wi-Fi® Network

Here are a few different ways you can maximize the security of your wireless network and protect your data from prying eyes and ears. This section is intended for the home, home office, and small office user.

At the time of this User Manual's publication, there are four encryption methods available.

Name	64-Bit Wired Equivalent Privacy	128-Bit Wired Equivalent Privacy	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronym	64-bit WEP	128-bit WEP	WPA-TKIP/AES (or just WPA)	WPA2-AES (or just WPA2)
Security	Good	Better	Best	Best
Features	Static keys	Static keys	Dynamic key encryption and mutual authentication	Dynamic key encryption and mutual authentication
	Encryption keys based on RC4 algorithm (typically 40-bit keys)	More secure than 64-bit WEP using a key length of 104 bits plus 24 additional bits of system generated data	TKIP (Temporal Key Integrity Protocol) added so that keys are rotated and encryption is strengthened	AES (Advanced Encryption Standard) does not cause any throughput loss

Wired Equivalent Privacy (WEP)

WEP is a common protocol that adds security to all Wi-Fi-compliant wireless products. WEP gives wireless networks the equivalent level of privacy protection as a comparable wired network.

64-Bit WEP—64-bit WEP was first introduced with 64-bit encryption, which includes a key length of 40 bits plus 24 additional bits of system-generated data (64 bits total). Some hardware manufacturers refer to 64-bit as 40-bit encryption. Shortly after the technology was introduced, researchers found that 64-bit encryption was too easy to decode.

128-Bit Encryption—As a result of 64-bit WEP's potential security weaknesses, a more secure method of 128-bit encryption was developed. 128-bit encryption includes a key length of 104 bits plus 24 additional bits of system-generated data (128 bits total). Some hardware manufacturers refer to 128-bit as 104-bit encryption. Most of the new wireless equipment in the market today supports both 64-bit and 128-bit WEP encryption, but you might have older equipment that only supports 64-bit WEP. All wireless products from Dynex will support both 64-bit and 128-bit WEP.

Encryption Keys—After selecting either the 64-bit or 128-bit WEP encryption mode, it is critical that you generate an encryption key. If the encryption key is not consistent throughout the entire wireless network, your wireless networking devices will be unable to communicate with one another. You can enter your key by typing in the hex key manually, or you can type a passphrase into the **Passphrase** field, then click **Generate** to create a key. A hex (hexadecimal) key is a combination of numbers and letters from A–F and 0–9. For 64-bit WEP, you need to enter 10 hex keys. For 128-bit WEP, you need to enter 26 hex keys.

For instance:

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

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

The WEP passphrase is NOT the same as a WEP key. Your card uses this passphrase to generate your WEP keys, but different hardware manufacturers might have different methods on generating the keys. If you have multiple vendors' equipment in your network, the easiest thing to do is to use the hex WEP key from your wireless router and enter it manually into the hex WEP key table in your card's configuration screen.

Security Sync (WPS)

Your router is equipped with the latest security standard, called *Wi-Fi Protected Access* (WPA2), and the legacy security standard, called *Wired Equivalent Privacy* (WEP). Your router also supports the *Wi-Fi Protected Setup* (WPS) specification, 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 enable users to automatically configure network names and strong WPA/WPA2 data encryption and authentication. By default, wireless security is disabled. 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 Security Sync (Wi-Fi Protected Setup)

Security Sync (WPS) uses WPA2 for encryption. It does not provide additional security, but rather, standardizes the method for securing your wireless network. You may use either the Push Button Configuration (PBC) method or PIN method to let a device access to your wireless network. Conceptually, the two methods work as follows:

PBC: Push and hold the Security Sync (WPS) button located on the top of your router 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. The client has now been securely added to your wireless network. Pushing the Security Sync button will automatically enable WPS. The PBC method can also be initiated from the notebook computer.

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

1. Wi-Fi Protected Setup (WPS): Enabled or Disabled.
2. Personal Identification Number (PIN) Method: In this method, a wireless client wishing to access your network must supply a 4- or 8-digit PIN to the router. After clicking "Enroll", you must start the WPS handshaking procedure from the client within two minutes.
3. Router PIN: If an external registrar is available, you can enter in the router's PIN to the registrar. Click **Generate New PIN** to change the PIN from the default value, or click **Restore Default PIN** to reset the PIN value.
4. Push Button Configuration (PBC) Method: PBC is an alternate method to connect to a WPS network. Push the Security Sync button located on the back of the router for three seconds, and then initiate the PBC on the client device. Alternatively, push the "Start PBC" soft button to start this process.
5. Manual Configuration Method: This section lists the default security settings if not using WPS.

Therouter features WPA2, which is the second generation of the WPA-based 802.11i standard. It offers a higher level of wireless security by combining advanced network authentication and stronger Advanced Encryption Standard (AES) encryption methods.

Wi-Fi Protected Areas (WPA)

WPA is a new Wi-Fi standard that improves upon the security features of WEP. To use WPA security, the drivers and software of your wireless equipment must be upgraded to support it. These updates will be found on your wireless vendor's Web site. There are three types of WPA security: WPA-PSK (no server), WPA (with radius server), and WPA2.

WPA-PSK (no server) uses what is known as a pre-shared key as the network key. A network key is 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 network key to access the network. Typically, this is the mode that will be used in a home environment.

WPA (with radius server) is a system where a radius server distributes the network key to the clients automatically. This is typically found in a business environment.

WPA2 requires Advanced Encryption Standard (AES) for encryption of data, which offers much greater security than WPA. WPA uses both Temporal Key Integrity Protocol (TKIP) and AES for encryption.

Most Wi-Fi products ship with security turned off. So once you have your network working, you need to activate WEP or WPA and make sure all your wireless devices are sharing the same network key.

***IMPORTANT**: You must now set all wireless network cards/adapters to match these settings.*

Sharing the Same Network Keys

Most Wi-Fi products ship with security turned off. So once you have your network working, you need to activate WEP or WPA and make sure your wireless networking devices are sharing the same network key.

The Wireless G Desktop Card cannot access the network because it is using a different network key than the network key that is configured on the wireless enhanced G router.

Using a Hexadecimal Key

A hexadecimal key is a combination of numbers and letters from A-F and 0-9. 64-bit keys are five two-digit numbers. 128-bit keys are 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

***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. Please check your product to see which version you are using. If you cannot configure your network with 128-bit encryption, try 64-bit encryption.*

WEP Setup

To set up 64-Bit WEP encryption:

1. Click **Security** under the **Wireless** heading on the left menu. The *Wireless > Security* page opens.
2. Select **64-bit WEP** from the **Security Mode** list.
3. Enter your key by typing in the hex key manually, or you can put a check mark in **Passphrase**, then type in your passphrase.
4. Click **Generate** to generate four different hex keys.

   A hex (hexadecimal) key is a combination of numbers and letters from A-F and 0-9. For 64-bit WEP, you need to enter 10 hex characters.

   For example: AF 0F 4B C3 D4 = 64-bit WEP key
5. Click **Apply Changes** to save the setting.

   ***Caution**: If you are configuring the wireless enhanced G router or access point from a computer with a wireless client, you will need to make sure that security is turned ON for this wireless client. If this is not done, your client will lose its wireless connection.*

To set up 128-Bit 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.*

1. Click **Security** under the **Wireless** heading on the left menu. The *Wireless Security* page opens.
2. Select **128-bit WEP** from the **Security Mode** list.
3. Enter your key by typing in the hex key manually, or you can put a check mark in **Passphrase**, then type in your passphrase.
4. Click **Generate** to generate four different hex keys.

   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 characters.

   For example: C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = 128-bit WEP key
5. Click **Apply Changes** to save the setting.

   ***Caution**: If you are configuring the wireless enhanced G router or access point from a computer with a wireless client, you will need to make sure that security is turned ON for this wireless client. If this is not done, your client will lose its wireless connection.*

Changing the Wireless Security Settings

Your router is equipped with WPA (Wi-Fi Protected Access), the latest wireless security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). By default, wireless security is disabled. To enable security, you must first determine which standard you want to use. To access the security settings, click **Security** under the **Wireless** heading on the left menu.

WPA Setup

***Note**: To use WPA security, all your clients must be upgraded to drivers and software that support it. At the time of this User Manual's publication, a security patch download is available, for free, from Microsoft®. This patch works only with the Windows XP operating system. You also need to download the latest driver for your Dynex Wireless Enhanced G 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 802.11g products.*

WPA uses a so-called pre-shared key as the security key. A pre-shared key is a password that is between eight and 63 characters long. It can be a combination of letters, numbers, and other characters. Each client uses the same key to access the network. Typically, this mode will be used in a home environment.

WPA2 is the second generation of WPA, offering a more advanced encryption technique over WPA.

To set up WPA/WPA2:

1. 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. Select **WPA-PSK** for just WPA authentication, or **WPA2-PSK** for just WPA2 authentication, or you may select **WPA-PSK + WPA2-PSK** for WPA and WPA2 as the authentication type.
4. 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. This pre-shared key will allow users full access to your network including shared files and printers.
5. 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.

   ***Note:** If your wireless card 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.*

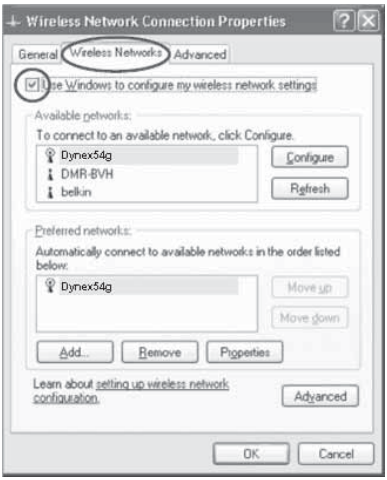
   The file that Microsoft has made available works only with Windows XP. Other operating systems are not supported at this time.

   ***Important**: 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.*

To set up Windows XP Wireless Network Utility to use WPA-PSK:

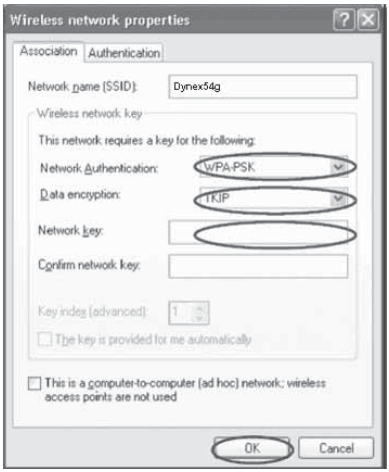
1. Under Windows XP, click **Start**, **Control Panel**, **Network Connections**.
2. Right-click **Wireless Network Connection Properties**, then click **Properties**.

3 Click the **Wireless Networks** tab. The following screen opens.



4 Make sure that the **Use Windows to configure my wireless network settings** box is checked.

5 Click the **Wireless Networks** tab, then click **Configure**. The following screen opens.



6 For a home or small business user, select **WPA-PSK** under **Network Authentication**.

***Note**: Select **WPA** 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.*

7 Select **TKIP** or **AES** under **Data Encryption**. This setting must be identical to the router that you set up.

8 Type in your encryption key in the **Network key** box.

***Important**: 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.*

9 Click **OK** to apply settings.

Using the Access Point Mode

***Note**: This advanced feature should be employed by advanced users only. The 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, the 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 the router to your existing network.

The router is now acting as an access point. To access the 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.

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

- Smurf Attack
- Fragment flooding
- TCP Null Scan

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*. 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 (e.g. [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 very quickly. It is recommended that you disable the settings when you are not using a specific application.

Setting Client IP Filters

The 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 wish 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**.

Setting MAC Address Filtering

The MAC address filter is a powerful security feature that allows you to specify which computers are allowed on the network. Any computer attempting to access the 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) on your network to allow network access to each.

To set MAC Address Filtering:

1. Open the *Firewall > MAC Address filters* page, then click **Enable MAC Address Filtering**.
2. Enter the MAC address of each computer on your network by clicking in the space provided and entering the MAC address of the computer you want to add to the list.
3. Click **Add**, then click **Apply Changes** to save the settings. You can have a MAC-address-filtering list of up to 32 computers.

***Note**: You will not be able to delete the MAC address of the computer you are using to access the router's administrative functions (the computer you are using now).*

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. If your ISP subscription provides you with additional public (WAN) IP addresses, additional computers can be placed outside the firewall provided each computer uses a different public (WAN) IP.

To set up a DMZ for a computer:

- Open the *Firewall > DMZ* page and 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.

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. The 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**. The router will not respond to an ICMP ping.

Utilities tab

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

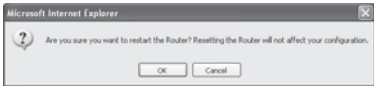
Restarting the router

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

To restart the 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 the router can take up to 25 seconds. It is important not to turn off the power to the router during the restart.

   A 25-second countdown will appear on the screen. When the countdown reaches zero, the router will be restarted. The router's home page should appear automatically. If not, type in the 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 the 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 the router. Restarting the router can take up to 25 seconds. It is important not to turn off the power to the router during the restart.

   A 25-second countdown will appear on the screen. When the countdown reaches zero, the router will be restarted. The router's home page should appear automatically. If not, type in the 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.

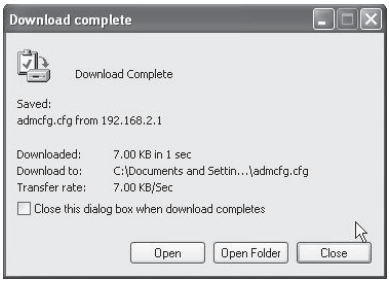
To save a current configuration:

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

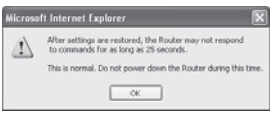
This option will let you restore a previously saved configuration.

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 ".bin". Locate the configuration file you want to restore, then double-click on it. The following message opens.

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



It will take up to 35 seconds for the configuration restoration to complete.

4 Click **OK**. A 35-second countdown will appear on the screen. When the countdown reaches zero, the router's configuration will be restored. The router's home page should appear automatically. If not, type in the 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 the 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:

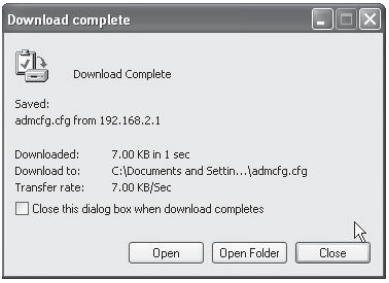
1 Under the **Utilities** heading on the left menu, click **Firmware Update**. The *Utilities > Firmware updates* page opens.

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.

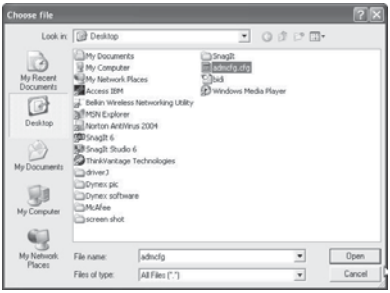


5 Click **Close**. The download is complete. To update the firmware, follow the steps in **To updating the router's firmware**.

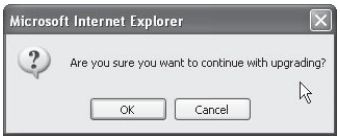
To update the router's firmware:

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

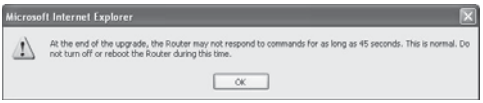
2 Browse to the firmware file you downloaded, then select the file by double-clicking on the file name.



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 the router may not respond for as long as one minute as the firmware is loaded into the router and the router is rebooted.



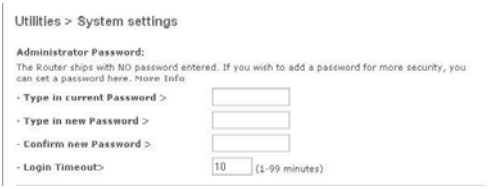
5 Click **OK**. A 60-second countdown will appear on the screen. When the countdown reaches zero, the router's firmware update will be complete. The router's home page should appear automatically. If not, type in the router's address (default = 192.168.2.1) into the navigation bar of your browser.

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 the router.

Setting or changing the Administrator Password



The router ships with NO password entered. If you wish 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 the 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

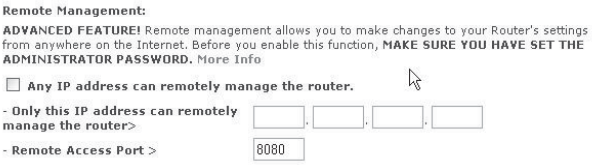
The login time-out option allows you to set the period of time that you can be logged into the router's Web-Based Advanced User Interface. The timer starts when there has been no activity. For example, you have made some changes in the Web-Based Advanced User Interface, then left your computer alone without clicking "Logout". Assuming the time-out is set to 10 minutes, then 10 minutes after you leave, the login session will expire. You will have to log into the 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 the router's Web-Based Advanced User Interface at one time.*

Setting the time and time zone

The router keeps time by connecting to a Simple Network Time Protocol (SNTP) server. This allows the router to synchronize the system clock to the global Internet. The synchronized clock in the 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 **Automatically Adjust Daylight Saving**. The system clock may not update immediately. Allow at least 15 minutes for the router to contact the time servers on the Internet and get a response. You cannot set the clock yourself.

Enabling Remote Management



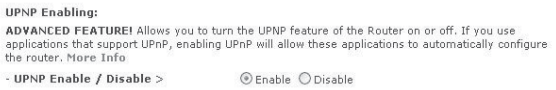
Before you enable this advanced feature of your router, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. Remote management allows you to make changes to your router's settings from anywhere on the Internet. There are two methods of remotely managing the router. The first is to allow access to the router 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 in the password of your router. The second method is to allow a specific IP address only to remotely manage the router. This is more secure, but less convenient. To use this method, enter the IP address you know you will be accessing the 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.*

NAT is the method by which the router shares the single IP address assigned by your ISP with the other computers on your network and is enabled by default. NAT should only be disabled 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 (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 the 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 the router, basically “telling” the router which way it needs the firewall configured. The router

ships with the UPnP feature disabled. If you are using any applications that are UPnP-compliant, and wish 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

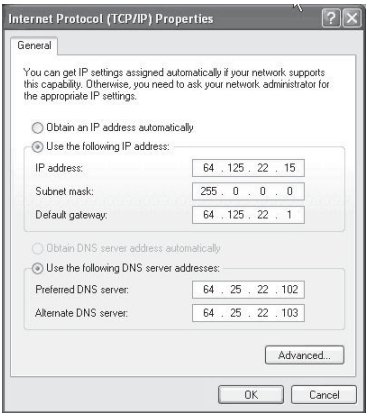
This innovation provides the router with the built-in capability to automatically check for a new version of firmware and alert you that the new firmware is available. When you log into the router's Web-Based Advanced User Interface, the router will perform a check to see if new firmware is available.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

Manually configuring network settings

In order for your computer to properly communicate with your router, you will need to change your PC's TCP/IP settings to DHCP.

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

1. Click **Start**, **Settings**, **Control Panel**.
2. Double-click the **Network and dial-up connections** icon (Windows 2000) or the **Network** icon (Windows XP or Vista).
3. Right-click the **Local Area Connection** associated with your network adapter, then select **Properties** from the list.
4. Click **Internet Protocol (TCP/IP)**, then click **Properties**. The following screen opens.



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

6 If not already selected, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, then click **OK**.

Your network adapter(s) are now configured for use with the router.

To manually configure network adapters in Windows 98SE or Me:

1 Right-click **My Network Neighborhood**, then select **Properties** from the list.

2 Select **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. You will need to enter this information into the router.

- Write in the IP address and subnet mask from the **IP Address** tab.
- Click the **Gateway** tab. Write the gateway address down in the chart.
- Click the **DNS Configuration** tab. Write the DNS address(es) in the chart.

4 If not already selected, click **Obtain IP address automatically** in the **IP Address** tab, then click **OK**.

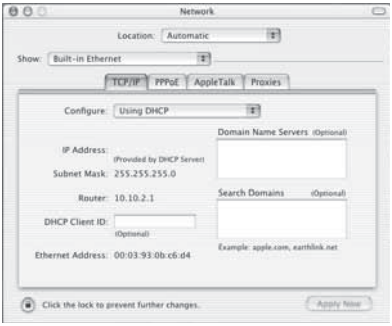
5 Restart the computer. When the computer restarts, your network adapter(s) are now configured for use with the router.

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 the 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. The *System Preferences* menu opens.

2 Click **Network**. The *Network* window opens.



3 Select **Built-in Ethernet** from the **Show** list.

4 Click the **TCP/IP** tab. Next to **Configure:**, you should see **Manually** or **Using DHCP**. If you do not, check the **PPPoE tab** 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.

***Note**: If **Manually** is selected in the **Configure** list, your router will need to be set up for a static IP connection type. Write down the address information. You will need to enter this information into the router.*

5 Select **Using DHCP** from the **Configure:** list, then click **Apply Now**.

Your network adapter(s) are now configured for use with the router.

Recommended Web browser settings

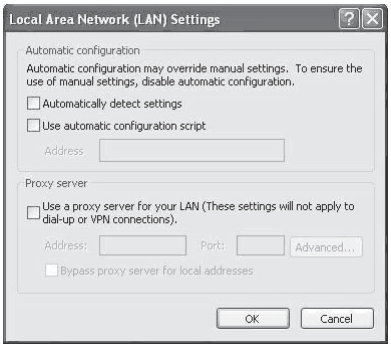
In most cases, you will not need to make any changes to your Web browser's settings. If you are having trouble accessing the Internet or the Web-Based Advanced User Interface, then change your browser's settings to the recommended settings in this section.

To change settings in Internet Explorer 4.0 or higher:

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

2 Click the **Connections** tab, then select **Never dial a connection**. If you cannot make a selection, go to the next step.

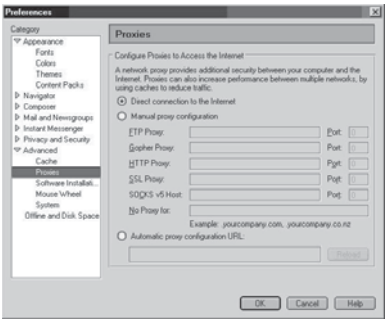
3 Click **LAN Settings…**. The *LAN Settings* page opens.



4 Make sure there are no check marks next to any of the displayed options. 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 Select **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 wireless 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 wireless router and connected devices increases. This may or may not be noticeable to you. As you move farther from your wireless 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 5 and 10 feet from the wireless 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 wireless router

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

2. Avoid obstacles and interference

Avoid placing your wireless 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 wireless 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 the wireless 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 wireless 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 wireless 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.

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 Enhanced 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 Websites
- Many commercial Websites 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: Installation CD does not automatically start.

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

1. If the Easy Install Wizard screen does not appear within 15-20 seconds, open up your CD drive by double-clicking the **My Computer** icon located on your desktop.

2. Next, double-click on the CD drive containing the Easy Install Wizard Software CD.

3. The Easy Install Wizard should start within a few seconds. If a window opens showing the files on the CD, double-click **EasyInstall.exe**.

4. If the Easy Install Wizard still does not start, see "Manually configuring network settings" on page 44 for an alternate setup method.

Problem: The Easy Install Wizard cannot find my router.

Solution: If the Easy Install Wizard is not able to find the router during the installation process, please check the following items:

1. If the Easy Install Wizard is not able to find the 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, please 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.

Please 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 r from the router for 10 seconds, and then plug the power back into the router. Make sure that the router's power light is on and solid green. If not, make sure that the AC adapter is correctly connected to the router and plugged into a wall outlet.

3. Make sure that you have a cable (use the cable included with the router) connected between (1) the network (Ethernet) port on the back of the computer and (2) one of the LAN ports, labeled "1" through "4", on the back of the router.

> ***Note**: The computer should NOT be connected to the port labeled "Internet/WAN" on the back of the router.*

4. Try shutting down and restarting your computer, then rerunning the Easy Install Wizard.

If the Easy Install Wizard is still unable to find the router, see "Manually configuring network settings" on page 44 for an alternate setup method.

Problem: The Easy Install Wizard cannot connect my router to the Internet.

Solution: If the Easy Install Wizard is not able to connect the router to the Internet, check the following items:

1. Use the troubleshooting suggestions within the Easy Install Wizard. If the troubleshooting screen does not open automatically, click the **Troubleshoot** button in the lower, right-hand corner of the Easy Install Wizard window.

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 44 for an alternate setup method.

Problem: The Easy Install Wizard completed installation, but my Web browser doesn't work.

- OR -

I am unable to connect to the Internet. The router's WAN light is off and the Connected light is blinking.

Solution: If you cannot connect to the Internet, the WAN light is off, and the Connected light is blinking, the problem may be that your modem and router are not connected properly.

1. Make sure the network cable between the modem and the router is connected. We strongly recommend using the cable that was supplied with your cable or DSL modem for this purpose. The cable should be connected at one end to the router's Internet/WAN port, and at the other end to the network port on your modem.

2. Unplug the cable or DSL modem from its power source for three minutes. After three minutes, plug the modem back into its power source. This may force the modem to properly recognize the router.

3. Unplug the power to your router, wait 10 seconds, and then reconnect the power. This will cause the router to reattempt communication with the modem.

4. Try shutting down and restarting your computer.

Problem: The Easy Install Wizard completed installation, but my Web browser doesn't work.

-OR-

I am unable to connect to the Internet. The Router's WAN light is on and the Connected light is blinking.

Solution: If you cannot connect to the Internet, the WAN light is on, and the Connected light is blinking, the problem may be that your connection type may not match the ISP's connection.

- If you have a *static IP address* connection, your ISP must assign you the IP address, subnet mask, and gateway address. See"Alternate setup method" on page 15 for details on changing this setting.
- You may need to configure your router to meet the specific requirements of your ISP. To search our Knowledge Base for ISP-specific issues, go to: http://www.dynexsupport.com and type in "ISP."

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

Problem: The Easy Install Wizard completed, but my web browser doesn't work.

- OR -

I am unable to connect to the Internet. The WAN light on my router is blinking and the Connected light is solid.

Solution: If the WAN light is blinking and the Connected light 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, please 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.

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

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

1. Look at the lights on your router. They should be as follows:
   - The Power light should be on.
   - The Connected light should be on and not blinking.
   - The WAN light should be either on or blinking.

2. Open your wireless utility software by clicking on the icon in the system tray at the bottom, right-hand corner of the screen. If you are also using a Dynex wireless card or adapter with this router, the tray icon should look like this  (the icon may be red or green):

3. 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.

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, please follow the steps below to connect wirelessly:

1. Click on 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 "Securing your Wi-Fi® Network" on page 26.

3. Within a few seconds, the tray icon in the lower, left-hand 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, please attempt the following troubleshooting steps:

1. Temporarily move your computer, if possible, 5 to 10 feet away from the 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 47.

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

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. As a result, the typical indoor range of your wireless devices will be between 100 to 200 feet. Note also that connection speed may decrease as you move farther away from the router or access point.

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 the 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 the 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 25 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 on 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: How do I extend the range of my wireless network?

Solution: Dynex recommends using one of the following products to extend wireless network coverage throughout large homes or offices:

- Wireless Access Point: A wireless access point can effectively double the coverage area of your wireless network. An access point is typically placed in the area not currently covered by your wireless enhanced G router, and is connected to the router using either an Ethernet cable or through your home's power lines using two Powerline ethernet adapters.

Problem: I am having difficulty setting up Wired Equivalent Privacy (WEP) security on a Dynex wireless router or Dynex access point.

Solution:

1. Log into your wireless router or access point.

Open your web browser and type in the IP address of the wireless router or access point. (The router's default is 192.168.2.1, the access point's default is 192.168.2.254.) Log into your router by clicking on **Login** button in the top, right 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**.

Click the **Wireless** tab on the left of your screen. Select the **Encryption** or **Security** tab to get to the security settings page.

2. Select **128-bit WEP** from the list.

3. After selecting your WEP encryption mode, you can type in your hex WEP key manually, or you can type in 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 characters.

For example: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = 128-bit key

4. Click **Apply Changes** to finish. Encryption in the wireless 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 the wireless router or Access Point 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 the wireless enhanced G router or access point. For instance, if your wireless router or access point uses the key 00112233445566778899AABBCC, then the client card must be set to the exact same key.

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. The Wireless LAN Utility opens. This utility lets you manage all the advanced features of the 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. Select **WEP**, on the **Data Encryption** list.

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 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 wireless enhanced G router or access point.*
>
> *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, please consult the manufacturer's user manual for that wireless client card.

Problem: Do Dynex products support WPA?

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 802.11g 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 802.11g products.

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

Problem: I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Dynex wireless router or Dynex access point for a home network.

Solution:

1. Select **WPA-PSK (no server)** from the **Security Mode** list.

2. Select **TKIP** or **AES** for **Encryption Technique**. 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. Click **Apply Changes** to finish. You must now set all clients to match these settings.

Problem: I am having difficulty setting up Wi-Fi 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 the wireless enhanced G router or access point uses. For instance, if the key is "Smith Family Network Key" in the wireless enhanced G router or access point, the clients must also use that same key.

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 client card.

3. Click the **Wireless Network Properties** tab, then select a network name from the **Available Networks** list, then click the **Properties** button. The *Properties* page opens.

4. Select **WPA-PSK (no server)** from the **Network Authentication** list.

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 wireless enhanced G router or access point.*

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

Problem: I am having difficulty setting up Wi-Fi Protected Access (WPA) security on a Dynex client card (Wireless Network Card or Adapter) for a business.

Solution:

1. Double-click the **Signal Indicator** icon. The *Wireless Network Utility* screen opens.

2. Click the **Advanced** button is clicked, the Dynex Wireless LAN Utility opens. This Utility lets you manage all the advanced features of the Dynex client card.

3. Click the **Wireless Network Properties** tab, then select a network name from the **Available Networks** list, then click the **Properties** button. The *Properties* page opens.

4. Select **WPA** from the **Network Authentication** list.

5. Click the **Authentication** tab, then select the settings that are indicated by your network administrator.

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 WPA wireless desktop or wireless 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:

http://www.microsoft.com/downloads/search.aspx?displaylang=en

***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. 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**.

5. Select **TKIP** or **AES** on the **Date Encryption** list. This setting will have to be identical to the wireless enhanced G router or access point that you set up.

6. Type in your encryption key in the **Network key** box.

***Important:** 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.*

7. Click **OK** to apply settings.

What's the difference between 802.11b, 802.11g, 802.11a, and 802.11n?

Currently there are four levels of 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, 802.11b, transmits information at 11 Mbps; 802.11a and 802.11g work at 54 Mbps; and Pre-N works at 108 Mbps. 802.11n has speeds that exceed 802.11g, and up to twice the wireless coverage area. See the following chart for more detailed information.

Wireless Technology	802.11b	802.11g	802.11a	802.11n
Speed	11Mbps	54Mbps	54Mbps	600% faster than standard 802.11g*
Frequency	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz	5GHz- uncrowded band	Common household devices such as cordless phones and microwave ovens may interfere with the unlicensed band 2.4GHz
Compatibility	Compatible with 802.11g	Compatible with 802.11b	Incompatible with 802.11b or 802.11g	Compatible with 802.11g or 802.11b
Coverage*	Depends on interference-typically 100-200 ft. indoors	Depends on interference-typicall y 100-200 ft. indoors	Interference range is typically 50-100 ft.	Up to 800% wider coverage than standard 802.11g*
Advantage	Mature-legacy technology	Common-widespread use for Internet sharing	Less interference-great for multimedia application	Leading edge- best coverage and throughput

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

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-WEGRTR, 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 310 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-WEGRTR** ("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 a 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 and Canada.

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

Distributed by Best Buy Purchasing, LLC.
Dynex, 7601 Penn Avenue South, Richfield, Minnesota, U.S.A.

Routeur sans fil G amélioré Dynex DX-WEGRTR

Table des matières

Introduction

Merci d'avoir acheté le routeur sans fil G amélioré DX-WEGRTR de Dynex. La procédure aisée d'installation et de configuration permet de créer un réseau sans fil en quelques minutes. Veiller à lire complètement ce guide de l'utilisateur et à prêter une attention particulière à la section intitulée « Emplacement du routeur pour des performances optimales », à la page 114.

Avantages d'un réseau domestique

Un réseau domestique permet de :

- Partager une connexion Internet à haut débit avec tous les ordinateurs de la maison
- Partager des ressources, telles que des fichiers et des disques durs, entre tous les ordinateurs connectés dans la maison
- Partager une imprimante avec toute la famille
- Partager des documents, de la musique, des vidéos et des images numériques
- Enregistrer, lire et copier des fichiers d'un ordinateur à un autre
- Jouer à des jeux en ligne, consulter une messagerie électronique et bavarder en ligne, le tout simultanément

Avantages d'un réseau sans fil

Voici quelques-uns des avantages qu'offre un réseau sans fil Dynex :

- **Mobilité** – plus besoin de réserver une « pièce ordinateur » : il est maintenant possible de travailler sur un ordinateur de bureau ou portatif partout dans la zone de portée du réseau sans fil
- **Installation simple** – l'Assistant Installation facile de Dynex facilite la configuration
- **Souplesse** – permet de configurer et d'accéder à des imprimantes, à des ordinateurs et à d'autres périphériques en réseau depuis n'importe quel endroit de la maison
- **Expansion aisée** – la large gamme de produits de réseau de Dynex permet d'étendre le réseau pour inclure des périphériques tels que des imprimantes ou des consoles de jeux

- **Aucun câble nécessaire** – permet d'éviter les frais et les complications d'une installation de câbles Ethernet dans la maison ou le bureau
- **Acceptation répandue dans l'industrie** – offre le choix d'une large gamme de produits de réseau compatibles

Caractéristiques du produit

En quelques minutes, il est possible de partager une connexion Internet et de mettre plusieurs ordinateurs en réseau. Ci-dessous figure une liste de caractéristiques qui font du routeur sans fil G amélioré de Dynex une solution idéale pour un réseau domestique ou un réseau d'une petite entreprise.

Fonctionne avec ordinateurs PC et MacMD – Le routeur prend en charge divers environnements de réseau, y compris Mac OSMD X, v10.x, LinuxMD, WindowsMD 2000, XP, VistaMC, et autres. Tout ce qui est nécessaire est un navigateur Internet et une carte réseau compatible avec TCP/IP (le langage standard d'Internet).

Témoins DEL sur le panneau avant – Les témoins DEL qui s'allument sur le devant du routeur indiquent les fonctions actives. Il est possible de savoir d'un coup d'œil si le routeur est connecté à Internet. Cette fonctionnalité élimine le besoin de logiciels avancés et de procédures de contrôle d'état.

Interface utilisateur Web avancée – Les fonctions avancées du routeur peuvent être facilement configurées par l'intermédiaire d'un navigateur Web, sans avoir à installer aucun logiciel supplémentaire sur l'ordinateur. Aucun disque à installer ni à conserver et il est possible d'apporter des modifications et d'exécuter des fonctions de configuration rapidement et facilement à partir de n'importe quel ordinateur du réseau.

Partage d'adresse IP NAT – Le routeur utilise le protocole de traduction d'adresses réseau (Network Address Translation, ou NAT) pour partager l'adresse IP unique assignée par le fournisseur de service Internet, évitant ainsi le coût d'ajouter des adresses IP au compte Internet.

Pare-feu SPI – Le routeur est équipé d'un pare-feu qui protégera le réseau contre un grand nombre d'attaques habituelles de pirates, notamment l'usurpation d'adresse IP (IP Spoofing), attaque Land, ping de la mort (Ping of Death, ou PoD), déni de service (Denial of Service, ou DoS), IP de longueur nulle, attaque Smurf, TCP Null Scan, SYN flood, UDP flooding, attaque Teardrop, défaut ICMP, défaut RIP et fragment flooding.

Commutateur 10/100 à 4 ports intégré – Le routeur dispose d'un commutateur réseau à 4 ports intégré afin que les ordinateurs câblés puissent partager imprimantes, données, fichiers MP3, photos numériques et autres. Le commutateur dispose d'une fonction de détection automatique de manière à s'ajuster à la vitesse des périphériques connectés. Il transfère simultanément les données entre les ordinateurs et Internet sans interruption ni consommation de ressources.

Compatibilité Universal Plug-and-Play (UPnP) – L'UPnP (Universal Plug-and-Play) est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux et d'autres applications compatibles avec l'UPnP.

Prise en charge de l'interconnexion de réseaux privés virtuels (VPN Pass-Through) – En cas de connexion au réseau du bureau à partir de la maison, par l'intermédiaire d'une connexion VPN, le routeur autorisera l'ordinateur équipé du système VPN à traverser le routeur et à accéder au réseau du bureau.

DHCP (Dynamic Host Configuration Protocol) intégré – Le protocole DHCP (Dynamic Host Configuration Protocol) intégré rend la connexion au réseau aussi simple que possible. Le serveur DHCP attribue automatiquement des adresses IP à chaque ordinateur afin de simplifier la configuration de la mise en réseau.

Assistant Installation facile – Grâce à l'Assistant Installation facile, la configuration du routeur ne sera plus faite au hasard. Ce logiciel automatisé définit les paramètres du réseau et configure le routeur de manière à se connecter au fournisseur d'accès Internet (FSI). En quelques minutes, le routeur sans fil sera connecté à Internet.

> ***Remarque** : L'Assistant Installation facile est compatible avec Windows 2000, XP, Vista, ainsi que Mac OS X 10.4.x. En cas d'utilisation d'un autre système d'exploitation, il est possible de configurer le routeur sans fil à l'aide d'une autre méthode décrite dans ce Guide de l'utilisateur (voir « Autre méthode de configuration » à la page 77).*

Mode G amélioré* – Le mode G amélioré, une amélioration des performances de 54g, fournit la connectivité sans fil la plus rapide pour des réseaux compatibles 802.11g dans les environnements du monde réel. Il est conçu pour les réseaux à la maison qui nécessitent une largeur de bande additionnelle pour des applications telles que le partage de photos numériques. G amélioré rend les réseaux locaux sans fil (WLAN) 802.11g plus efficaces sans pour cela interférer avec les performances des réseaux du voisinage; il est également compatible aux produits à haut débit du marché.

> ** Lors d'un fonctionnement en G amélioré 125, ce dispositif Wi-Fi peut atteindre un débit réel égal ou supérieur à 34,1 Mbps, ce qui est le débit équivalent d'un système suivant le protocole 802.11g et fonctionnant à un débit de données de 125 Mbps. Le débit réel variera en fonction de l'environnement, des conditions d'utilisation et d'autres facteurs.*

Point d'accès sans fil 802.11g intégré – La nouvelle technologie sans fil 802.11g procure une vitesse réseau près de cinq fois supérieure à la norme Wi-Fi actuelle (802.11b), soit 54 Mbps.

Filtrage d'adresses MAC – Pour une plus grande sécurité, il est possible de créer une liste d'adresses MAC. Il s'agit des identificateurs uniques des clients qui sont autorisés à accéder au réseau. Chaque ordinateur a sa propre adresse MAC. Il suffit d'entrer ces adresses MAC dans une liste grâce à l'Interface utilisateur Web avancée pour pouvoir contrôler l'accès au réseau.

Contenu de la boîte

- Routeur sans fil G amélioré de Dynex
- Guide d'installation rapide
- CD avec logiciel d'installation
- Câble Ethernet RJ-45
- Alimentation
- Guide de l'utilisateur

Configuration système requise

- Connexion Internet à haut débit par modem câble ou DSL avec connexion RJ45 (Ethernet)
- Au moins un ordinateur avec un adaptateur d'interface réseau installé
- Protocole de gestion de réseau TCP/IP installé sur chaque ordinateur
- Câble réseau Ethernet RJ-45
- Navigateur Internet

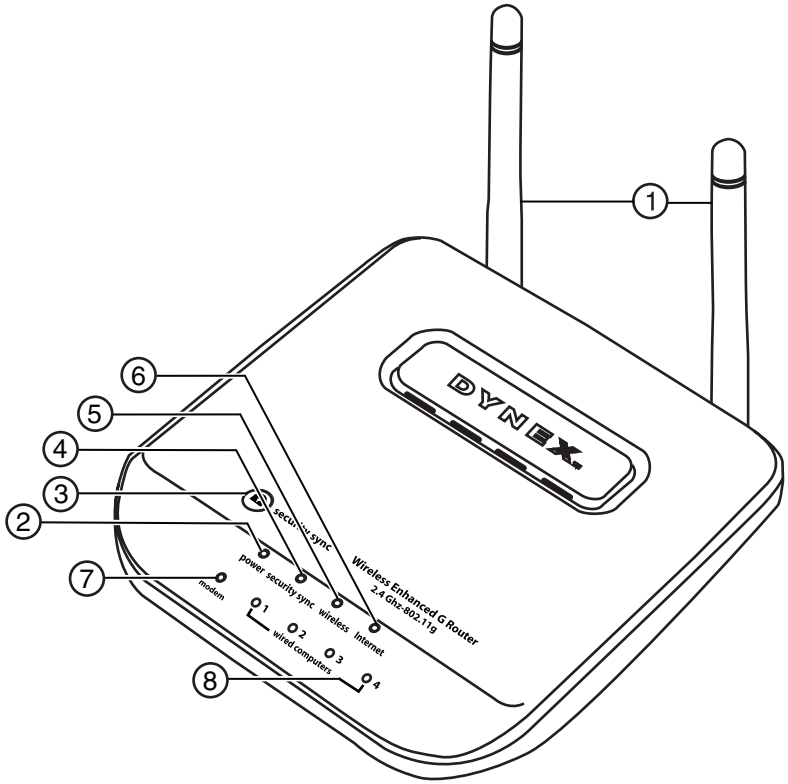
Configuration requise pour l'Assistant Installation facile

- Un PC fonctionnant sous Windows 2000, XP ou Vista, ou un ordinateur Mac fonctionnant sous Mac OS X 10.4x
- Un minimum de 64 Mo de RAM
- Navigateur Internet

Composants

Le routeur a été conçu pour être placé sur un bureau. Tous les câbles sont fixés à l'arrière afin de faciliter l'organisation et l'utilisation. Les témoins lumineux visibles à l'avant du routeur fournissent des informations sur l'activité et l'état du réseau.

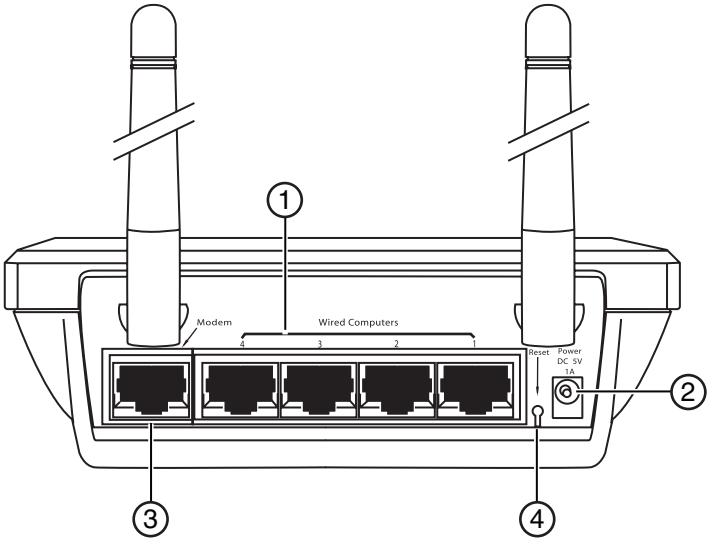
Panneau avant



#	Composant	Description
1	Antennes	Permet au routeur de communiquer avec un client sans fil (carte ou adaptateur USB).
2	DEL Alimentation/ Marche	Lors de la mise sous tension ou d'un redémarrage du routeur, il s'écoule un petit laps de temps nécessaire à son amorçage. Pendant ce temps, la DEL Alimentation/ Marche clignote. Lorsque le routeur est entièrement amorcé, la DEL Alimentation/ Marche s'allume en continu pour indiquer que le routeur est prêt à être utilisé. Éteint – Le routeur est éteint Vert clignotant – Le routeur est en cours d'amorçage Vert continu – Le routeur est prêt

#	Composant	Description
3	Touche de synchronisation de sécurité	Appuyer sur cette touche pendant trois secondes, puis initier la procédure de synchronisation de sécurité (WPS) sur le périphérique client dans les deux minutes suivantes. Le client échangera automatiquement les informations de sécurité et sera ajouté au réseau sans fil. Le fait d'appuyer sur la touche de synchronisation de sécurité activera automatiquement WPS. Voir « Utilisation de la synchronisation de sécurité (WPS) » à la page 90.
4	DEL de synchronisation de sécurité	S'allume pour indiquer que WPS a été activé. Vert clignotant – Le routeur cherche un client WPS pour établir une connexion. Vert continu – La connexion sécurisée a été établie avec le client.
4	DEL du réseau sans fil	Éteint – Le réseau sans fil est éteint Vert continu – Le réseau sans fil est prêt Vert clignotant – Activité du réseau
5	DEL Internet	Cette DEL unique indique lorsque le routeur est connecté à l'Internet. Lorsque le témoin est éteint, le routeur n'est pas connecté à l'Internet. Lorsque le témoin clignote, le routeur essaye de se connecter à l'Internet. Lorsque le témoin reste allumé en vert, sans clignoter, le routeur est connecté à l'Internet. Lors de l'utilisation de la fonction « Disconnect after x minutes » (Déconnecter après x minutes), cette DEL devient très utile pour surveiller l'état de la connexion du routeur. Éteint – Le routeur n'est pas connecté à l'Internet Vert clignotant – Le routeur essaye de se connecter à l'Internet Vert continu – Le routeur est connecté à l'Internet
6	DEL d'état du modem	Cette DEL s'allume en vert pour indiquer que le modem est correctement connecté au routeur. Elle clignote rapidement lorsque des informations transitent par le port entre le routeur et le modem. Éteint – Aucune liaison WAN Vert continu – Bonne liaison WAN Vert clignotant – Activité WAN
7	DEL d'état des ordinateurs câblés	Ces DEL portent les numéros 1 à 4 et correspondent aux numéros des ports à l'arrière du routeur. Lorsqu'un ordinateur est correctement connecté à l'un des ports pour ordinateurs câblés à l'arrière du routeur, la DEL correspondante s'allume : vert signifie qu'un périphérique 10Base-T est connecté, ORANGE signifie qu'un périphérique 100Base-T est connecté. Lorsque des informations sont envoyées par le port, la DEL clignote rapidement. Éteint – Le réseau sans fil est éteint Vert continu – Un périphérique 10base-T est connecté Orange continu – Un périphérique 100base-T est connecté Clignotement – Activité du port

Panneau arrière



#	Composant	Description
1	Ports pour ordinateurs câblés - Bleus	Connecter les ordinateurs câblés (et non pas sans fil) sur ces ports. Ces ports sont des ports 10/100 RJ45 à négociation automatique et à liaison ascendante automatique pour un câble Ethernet UTP standard de catégorie 5 ou 6. Ces ports portent les numéros 1 à 4 et correspondent aux DEL numérotées à l'avant du routeur.
2	Prise d'alimentation	Le bloc d'alimentation 5 V CC fourni se branche sur cette prise.
3	Port modem - Vert	Ce port permet de brancher un modem câble ou DSL. Utiliser le câble fourni avec le modem pour connecter le modem à ce port. L'utilisation d'un autre câble que celui fourni avec le modem câble risque de ne pas fonctionner correctement.
4	Touche de réinitialisation	La touche de réinitialisation (**Reset**) s'utilise dans les rares cas où le routeur peut fonctionner de façon incorrecte. La réinitialisation du routeur rétablit son fonctionnement normal tout en conservant les paramètres programmés. Il est également possible de rétablir les paramètres d'usine en utilisant la touche de réinitialisation. Utiliser l'option de rétablissement en cas d'oubli du mot de passe. **Réinitialisation du routeur** – Appuyer sur la touche de réinitialisation (**Reset**), puis la relâcher. Les témoins du routeur clignotent momentanément. Le témoin Alimentation/Marche clignote. Lorsque le témoin Alimentation/Marche reste allumé sans clignoter, la réinitialisation est terminée. Rétablissement des paramètres par défaut du fabricant – Appuyer sur la touche de réinitialisation (**Reset**) pendant au moins 10 secondes, puis la relâcher. Les témoins du routeur clignotent momentanément. Le témoin Alimentation/Marche clignote. Lorsque le témoin Alimentation/Marche reste allumé sans clignoter, le rétablissement est terminé.

Installation du routeur sans fil

Configuration requise pour le modem

Le modem câble ou DSL doit être équipé d'un port Ethernet RJ45. De nombreux modems possèdent à la fois un port Ethernet RJ45 et une connexion USB. Si le modem en service est à la fois Ethernet et USB, et que la connexion USB est celle qui est utilisée à ce moment-là, un message demandera d'utiliser le port Ethernet RJ45 pendant la procédure d'installation. Si le modem est équipé uniquement d'un port USB, il faudra demander un autre type de modem au FSI ou, dans certains cas, acheter un modem équipé d'un port Ethernet RJ45.

***Important** : Toujours installer d'abord le routeur! En cas d'installation de plusieurs dispositifs réseau pour la première fois, il est important que le routeur soit connecté et fonctionne avant d'essayer d'installer d'autres composants réseau, tels que les cartes pour ordinateurs portatifs ou pour ordinateurs de bureau.*

Assistant Configuration

Dynex propose un Assistant Configuration pour rendre l'installation du routeur simple et facile. Grâce à lui, le routeur peut être prêt à fonctionner en quelques minutes. L'Assistant Configuration requiert que l'ordinateur sous Windows 2000 ou XP soit connecté directement au modem câble ou DSL et que la connexion à l'Internet soit active et qu'elle fonctionne au moment de l'installation. Si ce n'est pas le cas, il faudra utiliser la section « Autre méthode de configuration » de ce Guide de l'utilisateur pour configurer le routeur. En outre, si le système d'exploitation utilisé n'est pas Windows 2000 ou XP, il faudra configurer le routeur en utilisant également la section « Autre méthode de configuration » de ce Guide de l'utilisateur.

Connexion du matériel

Pour connecter le matériel :

1. Débrancher le cordon d'alimentation du modem. Placer le routeur à côté du modem et relever les antennes du routeur.
2. Repérer le câble réseau qui permet de connecter le modem et l'ordinateur. Débrancher ce câble du modem et le connecter à l'un des ports de couleur bleue à l'arrière du routeur.
3. Prendre le nouveau câble réseau (inclus dans la boîte avec le routeur) et le connecter au port de couleur verte à l'arrière du routeur. Connecter l'autre extrémité au modem, dans le port qui est maintenant libre.
4. Brancher le cordon d'alimentation du modem. Attendre 60 secondes pour permettre au modem de s'initialiser. Brancher l'alimentation du routeur sur le port de couleur noire situé à l'arrière du routeur. Brancher l'autre extrémité sur une prise secteur.
5. Attendre 20 secondes pour permettre au routeur de s'initialiser. Vérifier que le témoin **Modem** et l'un des témoins **Wired Computers** (Ordinateurs connectés) sont allumés en vert sur la face avant du routeur. Si ce n'est pas le cas, vérifier de nouveau les connexions.

Exécution de l'Assistant Configuration

Pour exécuter l'Assistant Configuration :

1. Fermer tous les programmes en cours d'exécution sur l'ordinateur.
2. Désactiver tout pare-feu ou logiciel de partage de connexion Internet sur l'ordinateur.
3. Insérer le CD d'installation dans l'ordinateur. L'Assistant Configuration (Setup Assistant) s'affichera automatiquement sur l'écran de l'ordinateur en moins de 15 secondes. Double-cliquer sur l'Assistant Configuration pour l'exécuter, puis suivre les instructions à l'écran.

***Important** : Exécuter l'Assistant Configuration à partir de l'ordinateur qui est directement connecté au routeur.*

***Remarque** : Pour les utilisateurs de Windows : Si l'Assistant Configuration ne démarre pas automatiquement, sélectionner le lecteur CD/DVD à partir de **My Computer** (Poste de travail) et double-cliquer sur le fichier appelé **Setup Assistant** (Assistant Configuration) pour démarrer l'Assistant Configuration.*

4. Lorsque l'écran de confirmation s'affiche, confirmer que toutes les étapes du guide d'installation rapide ont été effectuées en cochant la case à droite de la flèche, puis cliquer sur **Next** (Suivant) pour continuer.

L'Assistant Configuration indiquera la fin de chaque étape de la configuration.

Lorsqu'il convient de donner un nom au réseau, l'Assistant Configuration ouvre l'écran *Naming your network* (Donner un nom au réseau).

Nom du réseau sans fil ou SSID (Service Set Identifier) par défaut. Il s'agit du nom du réseau sans fil auquel les ordinateurs ou périphériques munis d'un adaptateur réseau sans fil se connecteront.

5 Il est possible soit d'accepter le nom par défaut, soit de le remplacer par un nom personnalisé. En cas de modification du nom, le noter par écrit pour référence ultérieure. Cliquer sur **Next** (Suivant) pour continuer. L'écran *Internet Account Info* (Informations relatives au compte Internet) s'affiche.

6 Si le compte Internet exige un nom d'utilisateur et un mot de passe, un écran similaire à l'illustration ci-dessus s'affichera. Sélectionner un pays ou un FSI dans les listes.

L'Assistant Configuration configure alors le routeur en lui envoyant des données et en le redémarrant. Attendre les instructions à l'écran.

***Remarque** : Ne déconnecter aucun câble et ne pas mettre le routeur hors tension pendant que celui-ci redémarre. Cela rendrait le routeur inutilisable.*

Une fois le routeur configuré, l'Assistant Configuration vérifie la connexion à l'Internet.

Ceci termine l'installation du routeur. L'écran *Congratulations* (Félicitations) s'affiche lorsque le routeur peut se connecter à l'Internet. Il est alors possible de commencer à surfer en ouvrant un navigateur Web et en se rendant sur n'importe quel site Web.

7 L'Assistant Configuration peut être utilisé pour configurer les autres ordinateurs câblés et sans fil, afin de les connecter à l'Internet, en cliquant sur **Next** (Suivant). Pour ajouter ultérieurement des ordinateurs au routeur, sélectionner **Exit the Assistant** (Quitter l'assistant), puis cliquer sur **Next** (Suivant).

Pour identifier et résoudre les problèmes de configuration :

1 Si l'Assistant Configuration ne parvient pas à établir une connexion Internet, l'écran suivant s'affichera. Suivre les instructions à l'écran pour procéder à l'identification et à la résolution des problèmes.

Pour utiliser l'aide optionnelle pour connecter d'autres ordinateurs :

1 Cette étape optionnelle aide à connecter des ordinateurs câblés ou sans fil supplémentaires au réseau. Suivre les instructions affichées à l'écran.

À ce stade, le routeur est configuré et fonctionne correctement. Il est temps maintenant de connecter les autres ordinateurs.

Connexion d'ordinateurs sans fil

Des ordinateurs munis d'un adaptateur réseau sans fil peuvent utiliser ce réseau. Si ces adaptateurs n'ont pas encore été installés, le faire maintenant. Ensuite, suivre leurs instructions pour les connecter. Ce faisant, rechercher le réseau défini : domicile de Jean Wi-Fi.

Connexion d'ordinateurs câblés

Les ordinateurs munis d'un adaptateur réseau câblé peuvent utiliser ce réseau. Si ces adaptateurs n'ont pas encore été installés, le faire maintenant. Ensuite, connecter simplement un câble Ethernet du port réseau de l'ordinateur à un des ports LAN disponibles (étiquetés **connections to computers** [connexions aux ordinateurs]) au dos de ce routeur.

Une fois établi que les autres ordinateurs câblés et sans fil sont correctement connectés, le réseau est configuré et prêt à fonctionner. Il est maintenant possible de surfer sur Internet. Cliquer sur **Next** (Suivant) pour revenir au menu principal.

Configuration de la sécurité sans fil

Veiller à effectuer la configuration de base du routeur avant de configurer la sécurité. Vérifier que tous les ordinateurs (câblés et sans fil) peuvent se connecter sans problème à l'Internet par l'intermédiaire du routeur.

Pour configurer la sécurité :

1. Sur un ordinateur qui a une connexion câblée avec le routeur, ouvrez un navigateur Web. Dans le champ de l'adresse, saisir 192.168.2.1 (ou une autre adresse IP personnalisée), puis cliquer sur **Enter** (Entrée).

2. Dans le menu de gauche, aller à la section sans fil et cliquer sur **Security** (Sécurité). S'il est demandé d'ouvrir une session, saisir le mot de passe; si aucun mot de passe personnalisé n'a encore été configuré, laisser ce champ en blanc. Ensuite, cliquer sur **Submit** (Soumettre).

3. Il sera demandé de choisir le type de sécurité. Dynex recommande WPA2-PSK comme mode de sécurité et ensuite WPA-PSK+WPA2-PSK pour l'authentification, car c'est le mode le plus sûr et le plus facile à utiliser. Une fois le choix effectué, cliquer sur **Apply Changes** (Appliquer les modifications).

4 Dans le champ de la clé pré-partagée (PSK), saisir une clé de sécurité dont il sera facile de se souvenir. L'utilisation de ponctuation permettra d'améliorer la sécurité du réseau (par exemple, « Mon équipe favorite est celle des Canadiens de Montréal! »). Cliquer sur **Apply Changes** (Appliquer les modifications).

5 Maintenant, aller à chaque ordinateur sans fil. Utiliser l'utilitaire sans fil sur chacun d'entre eux pour effectuer les opérations suivantes (se reporter au manuel de l'utilisateur de l'adaptateur sans fil pour des instructions détaillées) :

a. Repérer le réseau sans fil et s'y connecter.

b. À l'invite, saisir la clé de sécurité créée à l'étape ci-dessus.

***Remarque** : Si un ordinateur n'accepte pas cette clé, il est probable qu'il ne prenne pas encore en charge le mode WPA/WPA2. Aller sur le site Web du fabricant de l'adaptateur sans fil et vérifier s'il existe une mise à jour pour le pilote.*

6 Si la mise à jour de l'adaptateur sans fil de l'ordinateur pour qu'il prenne en charge le mode WPA/WPA2 n'est pas souhaitée, retourner à l'étape 4 et choisir WEP. Voir « Configuration du WEP » à la page 93 pour les instructions relatives à une configuration WEP.

Autre méthode de configuration

L'Interface utilisateur Web avancée est un outil qui peut être utilisé pour configurer le routeur sans utiliser l'Assistant Installation facile. Elle peut également être utilisée pour gérer les fonctions avancées du routeur. À partir de l'Interface utilisateur Web avancée, les tâches suivantes peuvent être réalisées :

- Visualiser les paramètres et l'état actuel du routeur
- Configurer le routeur afin qu'il se connecte au FSI, à l'aide des paramètres fournis par celui-ci
- Modifier les paramètres réseau en cours comme l'adresse IP interne, le pool d'adresses IP, les paramètres DHCP et bien plus encore
- Configurer le pare-feu du routeur afin qu'il fonctionne avec des applications spécifiques (réacheminement de port)
- Configurer des fonctions de sécurité, telles que la restriction des clients, le filtrage d'adresses MAC, le WEP et le WPA
- Activer la fonction DMZ (zone démilitarisée) pour un ordinateur unique du réseau
- Changer le mot de passe interne du routeur
- Activer/désactiver l'UPnP (Universal Plug-and-Play)
- Réinitialiser le routeur
- Sauvegarder les paramètres de configuration
- Rétablir les paramètres par défaut du routeur
- Mettre à jour le microprogramme du routeur.

Pour connecter le routeur (étape 1) :

1 Mettre le modem hors tension en débranchant le bloc d'alimentation du modem.

2 Repérer le câble réseau qui relie le modem à l'ordinateur. Le débrancher de l'ordinateur et laisser l'autre extrémité branchée sur le modem.

3 Brancher l'extrémité du câble ainsi débranchée sur le port marqué **Modem** à l'arrière du routeur.

4 Brancher un nouveau câble réseau (non fourni) pour connecter l'ordinateur à un des ports **1 à 4** sur le routeur. Remarque : Le numéro du port n'a pas d'importance.

5 Rebrancher le bloc d'alimentation du modem câble ou DSL pour l'allumer.

6 Brancher le cordon d'alimentation sur la prise secteur, puis sur la prise d'alimentation du routeur.

7 Vérifier que le modem est connecté au routeur en vérifiant les témoins lumineux à l'avant du routeur. Le témoin vert marqué **Modem** devrait être allumé si le modem est correctement branché sur le routeur. Si ce n'est pas le cas, vérifier de nouveau les connexions.

8 Vérifier que l'ordinateur est correctement connecté au routeur en vérifiant les témoins **1 à 4**. Le témoin correspondant au port connecté à l'ordinateur devrait être allumé si l'ordinateur est correctement connecté. Si ce n'est pas le cas, vérifier de nouveau les connexions.

Pour configurer les paramètres réseau de l'ordinateur de manière à ce qu'il fonctionne avec un serveur DHCP :

- Voir « Configuration manuelle des paramètres réseau » à la page 109 pour plus d'informations.

Configuration du routeur au moyen de l'Interface utilisateur Web avancée :

1 Ouvrir le navigateur Internet, puis accéder à l'Interface utilisateur Web avancée en saisissant « 192.168.2.1 » dans la barre d'adresse (il n'est pas nécessaire de taper autre chose, tel que « http:// » ou « www »). Ensuite, appuyer sur **Enter** (Entrée). La page d'accueil du routeur s'affiche.

***Remarque**: En cas de difficulté à accéder à l'Interface utilisateur Web avancée du routeur, aller à la section intitulée « Configuration manuelle des paramètres du réseau ».*

2 Pour apporter des modifications aux paramètres du routeur, il est nécessaire de se connecter. Cliquer sur **Login** (Connexion) ou sur tout autre lien sur la page d'accueil pour passer à l'écran de connexion.

3 Dans l'écran de connexion, laisser le mot de passe vide (aucun mot de passe n'est entré avant la livraison du routeur) et cliquer sur **Submit** (Soumettre) pour se connecter.

Un seul ordinateur à la fois peut se connecter au routeur pour en modifier les paramètres.

4 Une fois l'utilisateur connecté pour apporter des modifications, il existe deux méthodes de déconnexion de l'ordinateur. Le fait de cliquer sur **Logout** (Déconnexion) déconnectera l'ordinateur.

- OU -

5 La connexion se fermera automatiquement après une durée déterminée. Le délai avant déconnexion est par défaut de 10 minutes. Cette valeur peut être modifiée en choisissant une durée de 1 à 99 minutes. Pour plus d'informations, voir « Modification du paramètre de délai avant déconnexion » à la page 107.

Utilisation de l'Interface utilisateur Web avancée

La page d'accueil est la première page qui s'affiche lors de l'accès à l'interface utilisateur (IU) Web avancée. Cette page offre un aperçu rapide de l'état et des paramètres du routeur. Il est possible d'accéder à toutes les pages de configuration avancée depuis cette page.

Quick-Navigation Links (Liens de navigation rapide) – Il est possible de se rendre directement à n'importe laquelle des pages de l'IU du routeur en cliquant directement sur l'un de ces liens. Ils sont divisés en catégories logiques et groupés par onglets afin de faciliter la recherche d'un paramètre particulier. Pour obtenir une brève description de la fonction d'un onglet, cliquer sur l'en-tête violet de l'onglet.

Touche Home (Accueil) – La touche **Home** est disponible sur chaque page de l'IU. Appuyer sur cette touche pour revenir à la page d'accueil.

Internet Status Indicator (Témoin d'état Internet) – Ce témoin est visible sur toutes les pages de l'IU. Il indique l'état de la connexion du routeur. Lorsqu'il indique **connection OK** (Connexion OK) en vert, le routeur est connecté à l'Internet. Lorsque le routeur n'est pas connecté à l'Internet, l'indicateur affiche **no connection** (Pas de connexion) en rouge. L'indicateur est automatiquement mis à jour lors d'une modification des paramètres du routeur.

Touche Login/Logout (Connexion/Déconnexion) – Cette touche permet de se connecter et de se déconnecter du routeur en appuyant simplement sur une touche. Lorsque l'utilisateur est connecté au routeur, cette touche indique **Logout** (Déconnexion). Lors de la connexion au routeur, l'utilisateur accède à une page distincte où il doit entrer un mot de passe. Une fois connecté au routeur, il est possible de modifier les paramètres. Une fois les modifications apportées, l'utilisateur peut se déconnecter du routeur en cliquant sur **Logout** (Déconnexion).

Touche Help (Aide) – La touche **Help** permet d'accéder aux pages d'aide du routeur. Il est également possible d'obtenir de l'aide sur de nombreuses pages en cliquant sur **more info** (Plus d'infos) en regard de certaines sections de chaque page.

LAN Settings (Paramètres du réseau local) – Indique les paramètres du côté réseau local (LAN) du routeur. Pour modifier ces paramètres, cliquer sur l'un des liens (Adresse IP, Masque de sous-réseau, serveur DHCP) ou cliquer sur le lien **LAN - Quick Navigation** (LAN - Navigation rapide) sur le côté gauche de l'écran.

Features (Caractéristiques) – Indique l'état des fonctions NAT, pare-feu et sans fil du routeur. Pour modifier ces paramètres, cliquer sur l'un des liens ou sur les liens **Quick Navigation** (Navigation rapide) sur le côté gauche de l'écran.

Internet Settings (Paramètres Internet) – Affiche les paramètres du côté Internet/WAN du routeur qui se connecte à l'Internet. Pour modifier ces paramètres, cliquer sur l'un des liens ou sur le lien **Internet/WAN** - **Quick Navigation** (Internet/WAN - Navigation rapide) sur le côté gauche de l'écran.

Version Info (Informations sur la version) – Affiche la version du microprogramme, la version du code d'amorçage, la version du matériel ainsi que le numéro de série du routeur.

Page Name (Nom de la page) – La page sur laquelle se trouve l'utilisateur peut être identifiée par son nom. Ce guide de l'utilisateur fait parfois référence aux pages par leur nom. Par exemple, **LAN > LAN Settings** (LAN > Paramètres du réseau local) fait référence à la page LAN Settings (Paramètres LAN).

Configuration du routeur pour la connexion au fournisseur de service Internet (FSI)

L'onglet **Internet/WAN** est l'endroit où l'utilisateur doit configurer le routeur pour qu'il se connecte à son fournisseur de service Internet (FSI). Le routeur peut se connecter pratiquement à n'importe quel système offert par un FSI, si bien sûr les paramètres du routeur ont été correctement configurés pour le type de connexion du FSI. Les paramètres de connexion au FSI sont fournis par ce dernier.

Pour configurer le routeur avec les paramètres fournis par le FSI :

1. Cliquer sur **Connection Type** (Type de connexion) sur le côté gauche de l'écran, puis sélectionner le type de connexion à employer.
2. Si le FSI a donné des paramètres DNS, cliquer sur **DNS** pour entrer l'adresse DNS pour les FSI qui nécessitent des paramètres particuliers.
3. Cliquer sur **MAC address** (Adresse MAC) pour cloner l'adresse MAC de l'ordinateur ou entrer une adresse WAN MAC spécifique, si cela est requis par le FSI.
4. Une fois les paramètres entrés, le témoin **Internet Status** (État Internet) affiche **connection OK** (Connexion OK) si le routeur est correctement configuré.

Pour définir le type de connexion :

1. Cliquer sur **Connection Type** (Type de connexion) dans le menu qui figure sur le côté gauche de l'écran. La page *Connection Type* (Type de connexion) s'affiche. À partir de cette page, sélectionner le type de connexion à utiliser en cliquant sur la touche qui se trouve en face du type de connexion, puis en cliquant sur **Next** (Suivant).

Réglage du type de connexion FSI comme « IP Dynamique »

La connexion dynamique est le type le plus répandu sur les modems câble. Dans de nombreux cas, le simple fait de définir le type de connexion sur **dynamic** (Dynamique) suffit à effectuer la connexion avec le FSI. Certains types de connexion dynamique peuvent nécessiter un nom d'hôte. L'utilisateur peut entrer un nom d'hôte dans l'espace fourni à cet effet si un nom lui a été attribué. Le nom d'hôte est attribué par le FSI. Certaines connexions dynamiques peuvent nécessiter le clonage de l'adresse MAC du PC qui était, à l'origine, connecté au modem.

Modification de l'adresse MAC WAN

Si le FSI a besoin d'une adresse MAC spécifique pour la connexion au service, l'utilisateur peut entrer une adresse MAC particulière ou cloner l'adresse MAC de l'ordinateur en cours via ce lien.

Réglage du type de connexion FSI comme « IP Statique »

Le type de connexion à adresse IP statique est moins répandu que les autres. Si le FSI utilise ce type d'adressage, il est nécessaire de connaître l'adresse IP, le masque de sous-réseau ainsi l'adresse de la passerelle du FSI. Ces informations sont disponibles auprès du FSI ou sur les documents qu'il distribue à ses abonnés. Entrer les informations, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Une fois les modifications effectuées, le témoin **Internet Status** (État Internet) affiche **connection OK** (Connexion OK) si le routeur est correctement configuré.

Réglage du type de connexion FSI comme « PPPoE »

La plupart des fournisseurs de services DSL utilisent une connexion de type PPPoE. Si la connexion à l'Internet s'effectue au moyen d'un modem DSL, il est possible que le FSI utilise le protocole PPPoE pour fournir le service. Si une connexion Internet, à la maison ou dans une petite entreprise, n'utilise pas de modem, il est possible qu'elle utilise également le protocole PPPoE.

La connexion est de type PPPoE si :

- Le FSI a attribué un nom d'utilisateur et un mot de passe, qui sont requis pour se connecter à l'Internet;
- Le FSI a donné un logiciel tel que WinPOET ou Enternet300 à utiliser pour accéder à l'Internet; ou
- Il faut double-cliquer sur une icône du bureau, autre que celle du navigateur, pour accéder à l'Internet.

Saisir ce qui suit :

User Name (Nom d'utilisateur) – Cet espace est prévu pour saisir le nom d'utilisateur qui a été attribué par le FSI.

Password (Mot de passe) – Entrer le mot de passe et le retaper dans la zone *Retype Password* (Confirmer le mot de passe) pour le confirmer.

Service Name (Nom du service) – Un nom de service est rarement requis par un FSI. À moins d'avoir établi avec certitude que le FSI exige un nom de service, laisser ce champ vide.

MTU – Le paramètre MTU ne devrait jamais être modifié, à moins que le FSI ne fournisse un paramètre MTU spécifique. Apporter des modifications aux valeurs MTU peut causer des problèmes pour la connexion à l'Internet, y compris déconnexion de l'Internet, accès lent à l'Internet et difficultés avec des applications Internet qui fonctionnaient correctement auparavant.

Disconnect after X minutes… (Déconnecter après X minutes...) – Cette fonction permet de déconnecter automatiquement le routeur du FSI en l'absence d'activité pendant une durée déterminée. Par exemple, si cette option est cochée et que la valeur **5** est entrée dans le champ des minutes, le routeur se déconnectera de l'Internet après 5 minutes d'inactivité Internet. Cette option devrait être utilisée si le service Internet est facturé à la minute.

Définition des paramètres personnalisés du serveur de noms de domaine (DNS)

Un serveur de noms de domaine (*Domain Name Server*) est un serveur situé sur Internet qui traduit les URL (Universal Resource Locators), telles que « www.dynex.com », en adresses IP. La plupart des FSI n'exigent pas que cette information soit entrée dans le routeur. La case **Automatic from ISP** (Obtenir automatiquement du FSI) doit être cochée si le FSI n'a pas fourni d'adresse DNS particulière. En cas d'utilisation d'un type de connexion avec adresse IP statique, il pourra être nécessaire d'entrer une adresse DNS particulière, ainsi qu'une adresse DNS secondaire, pour que la connexion fonctionne correctement. Si la connexion est de type dynamique ou PPPoE, il ne sera probablement pas nécessaire d'entrer une adresse DNS. Laisser la case **Automatic from ISP** (Obtenir automatiquement du FSI) cochée. Pour entrer les paramètres d'adresse DNS, désélectionner la case **Automatic from ISP** (Obtenir automatiquement du FSI) et entrer les numéros DNS dans les espaces fournis à cet effet. Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.

Configuration de l'adresse MAC (Media Access Controller) WAN

Tous les composants réseau, y compris les cartes, les adaptateurs et les routeurs, possèdent un « numéro de série » unique appelé une adresse MAC. Il est possible qu'un FSI enregistre l'adresse MAC de l'adaptateur d'un ordinateur et n'autorise que cet ordinateur à accéder à l'Internet. Après l'installation du routeur, c'est sa propre adresse MAC qui sera « vue » par le FSI, ce qui risque de faire échouer la connexion. Dynex permet de cloner (copier) l'adresse MAC de l'ordinateur sur le routeur. Cette adresse MAC, à son tour, sera vue par le système du FSI comme l'adresse MAC d'origine et permettra la connexion. Si la politique du FSI à l'égard de l'adresse MAC d'origine n'est pas connue, cloner simplement l'adresse MAC de l'ordinateur qui était au départ connecté au modem. Le clonage de l'adresse ne causera aucun problème au niveau du réseau.

Pour cloner l'adresse MAC :

1. Veiller à utiliser l'ordinateur qui était CONNECTÉ À L'ORIGINE au modem avant que le routeur ne soit installé.

2 Cliquer sur **Clone** (Cloner), puis sur **Apply Changes** (Enregistrer les modifications). L'adresse MAC est désormais clonée sur le routeur.

Pour entrer une adresse MAC spécifique :

- Entrer une adresse MAC dans les espaces fournis à cet effet, puis cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les changements. L'adresse MAC WAN du routeur est alors remplacée par l'adresse MAC spécifiée.

Utilisation de l'Interface utilisateur Web avancée

Grâce au navigateur Internet, il est possible d'accéder à l'Interface utilisateur Web avancée du routeur. Ouvrir le navigateur et entrer **192.168.2.1** (n'entrer aucun autre élément, comme « http:// » ou « www »), puis appuyer sur **Enter** (Entrée). La page d'accueil du routeur s'affiche dans le navigateur.

Affichage des paramètres LAN

Cliquer sur l'onglet intitulé **LAN Setup** (Configuration du réseau local) pour accéder à la page d'accueil correspondante. Celle-ci contient une brève description des fonctions. Pour afficher les paramètres ou modifier un des paramètres du réseau local, cliquer sur **LAN Settings** (Paramètres du réseau local) ou, pour afficher la liste des ordinateurs connectés, cliquer sur **DHCP Client List** (Liste des clients DHCP).

Modifications des paramètres LAN

Tous les paramètres de configuration du réseau local interne du routeur peuvent être affichés ou modifiés sur cette page.

IP Address (Adresse IP) – *IP address* représente l'adresse IP interne du routeur. L'adresse IP par défaut est **192.168.2.1**. Pour accéder à l'Interface utilisateur Web avancée, entrer cette adresse IP dans la barre d'adresse du navigateur. Si besoin, cette adresse peut être modifiée. Pour modifier l'adresse IP, entrer la nouvelle adresse, puis cliquer sur **Apply Changes** (Enregistrer les modifications). L'adresse IP choisie doit être une adresse IP non-acheminable.

Exemples d'IP non-acheminables : 192.168.x.x (où x est un nombre compris entre 0 et 255) et 10.x.x.x (où x est un nombre compris entre 0 et 255).

Subnet Mask (Masque de sous-réseau) – Il est inutile de modifier le masque de sous-réseau. Il s'agit d'une fonctionnalité unique et avancée du routeur Dynex. Il est possible de changer le masque de sous-réseau, si nécessaire. Toutefois, ne PAS le modifier à moins d'avoir une raison particulière de le faire. La valeur par défaut est **255.255.255.0**.

DHCP Server (Serveur DHCP) – La fonction de serveur DHCP facilite grandement la configuration du réseau grâce à l'attribution automatique d'adresses IP à tous les ordinateurs du réseau. La valeur par défaut est **On** (Activé). Le serveur DHCP peut être désactivé, si nécessaire. Toutefois, pour le désactiver, il faut définir manuellement une adresse IP statique pour chaque ordinateur du réseau. Pour désactiver le serveur DHCP, sélectionner l'option **Off** (Désactivé), puis cliquer sur **Apply Changes** (Enregistrer les modifications).

IP Pool (Pool d'adresses IP) – Plage d'adresses IP mises de côté pour l'affectation dynamique aux ordinateurs du réseau. La valeur par défaut est 2–100 (99 ordinateurs). Pour changer ce nombre, entrer de nouvelles adresses IP de début et de fin, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le serveur DHCP peut attribuer automatiquement 100 adresses IP. Cela signifie qu'il n'est pas possible de spécifier un pool d'adresses IP supérieur à 100 ordinateurs. Par exemple, si on commence à 50, cela signifie qu'il faut terminer à 150 ou à moins, de manière à ne pas dépasser la limite des 100 clients. L'adresse IP de début doit avoir un numéro inférieur à celui de l'adresse IP de fin.

Lease Time (Durée du bail) – Durée pendant laquelle le serveur DHCP réserve l'adresse IP de chaque ordinateur. Dynex conseille de laisser la durée du bail à **Forever** (Toujours). La valeur par défaut est **Forever** (Toujours), ce qui signifie que chaque fois que le serveur DHCP attribue une adresse IP à un ordinateur, cette adresse ne changera pas pour l'ordinateur. L'affectation en tant que durées de bail d'intervalles plus courts, comme un jour ou une heure, permet de libérer les adresses IP une fois la durée écoulée. Cela signifie également que l'adresse IP d'un ordinateur peut changer. Si d'autres fonctionnalités avancées du routeur ont été définies, comme la DMZ ou les filtres IP de clients, elles dépendent de l'adresse IP. Pour cette raison, il n'est pas recommandé que l'adresse IP change.

Local Domain Name (Nom du domaine local) – Le paramètre par défaut est **Dynex**. Il est possible de définir un nom de domaine local (nom de réseau) pour le réseau. Il est inutile de changer ce paramètre à moins d'avoir un réel besoin de le faire. Il est possible de donner n'importe quel nom au réseau (« MON RÉSEAU », par exemple).

Affichage de la liste des clients DHCP

Il est possible d'afficher la liste des ordinateurs (appelés des clients) qui sont connectés au réseau. Il est possible d'afficher l'adresse IP de l'ordinateur, le nom d'hôte (si l'ordinateur en a un) ainsi que l'adresse MAC de la carte d'interface réseau (NIC) de l'ordinateur. Cliquer sur **Refresh** (Actualiser) pour mettre la liste à jour. Si des changements ont eu lieu, la liste sera mise à jour.

Configuration des paramètres du réseau sans fil

Cliquer sur l'onglet intitulé **Wireless** (Sans fil) pour accéder à la page *Wireless* (Sans fil). Sous l'onglet **Wireless** (Sans fil) se trouvent des liens qui permettent de modifier les paramètres du réseau sans fil.

Modification du nom du réseau sans fil (SSID)

Un SSID (Service Set Identifier) est utilisé pour identifier le réseau sans fil. Le SSID par défaut du routeur est « Dynex ». L'utilisateur est libre de choisir ce qu'il veut ou de le laisser inchangé. Si d'autres réseaux sans fil fonctionnent dans le secteur, il faudra s'assurer que le SSID est unique (qu'il ne correspond pas à celui d'un autre réseau sans fil de la zone). Pour modifier le SSID, entrer le SSID souhaité dans le champ **SSID** et cliquer sur **Apply Changes** (Enregistrer les informations). Le changement est immédiat. En cas de changement du SSID, les ordinateurs sans fil devront également être reconfigurés pour se connecter au nouveau nom du réseau. Se reporter à la documentation de l'adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Utilisation du commutateur de mode sans fil

Le routeur est en mesure de fonctionner sous trois modes sans fil différents : « g and b », « g only » et « b only ». Ces différents modes sont décrits ci-dessous.

Mode « g and b » – Dans ce mode, le routeur est compatible avec des clients sans fil 802.11b et 802.11g, de façon simultanée. Ce mode est le mode par défaut, et il assure un bon fonctionnement avec tous les dispositifs Wi-Fi compatibles. Si le réseau comprend à la fois des clients 802.11b et 802.11g, Dynex recommande le mode « g and b » pour le routeur. Ne pas modifier ce paramètre à moins d'avoir une raison particulière de le faire.

Mode « g only » – Ce mode ne fonctionne qu'avec des clients 802.11g. Ce mode n'est recommandé que pour empêcher les clients 802.11b d'accéder au réseau. Pour changer de mode, sélectionner le mode souhaité dans la liste **Wireless Mode** (Mode sans fil), puis cliquer sur **Apply Changes** (Enregistrer les modifications).

Mode « b only » – Il n'est PAS recommandé d'utiliser ce mode à moins d'avoir une raison très particulière de le faire. Ce mode existe dans l'unique but de résoudre les problèmes pouvant survenir avec certains adaptateurs 801.11b et n'est PAS nécessaire pour assurer l'interopérabilité entre les normes 802.11b et 802.11g.

Quand utiliser le mode « b only »

Parfois, des clients 802.11b plus anciens peuvent ne pas être compatibles avec le sans fil 802.11g. Ces adaptateurs sont généralement de qualité inférieure et peuvent utiliser des pilotes ou des technologies plus anciennes. Le choix de ce mode peut résoudre certains problèmes rencontrés avec ces clients. Si le client utilisé semble faire partie de cette catégorie d'adaptateurs, vérifier d'abord auprès du fabricant de l'adaptateur s'il existe une mise à jour des pilotes. En l'absence de mise à jour disponible, il se peut que l'utilisation du mode « b only » puisse résoudre le problème. Noter que l'utilisation du mode « b only » diminuera les performances du réseau 802.11g.

Mode G amélioré* – Le routeur prend en charge deux modes à haut débit, le mode G amélioré 125 et le mode d'émission de salves de petites trames (frame-bursting).

La sélection du mode G amélioré 125 aura pour effet que tous les dispositifs fonctionneront en mode G amélioré 125 s'ils peuvent prendre en charge des débits de 125 Mbps. Si des dispositifs ne prenant pas en charge le mode G amélioré 125 sont connectés ou associés au réseau, le routeur basculera automatiquement tout le réseau sur le mode d'émission par salves de petites trames (frame-bursting).

La sélection de **Frame Bursting** signifie que tous les dispositifs prenants en charge cette technologie utiliseront ce mode; les clients qui ne le prenne pas en charge fonctionneront sur le mode normal 802.11g. Le mode d'émission par salves de petites trames prend en charge à la fois les dispositifs compatibles avec cette technologie est ce qui ne le sont pas de façon simultanée. Le mode d'émission par salves de petites trames est fondé sur la spécification 802.11e non publiée.

Si **Off** est sélectionné le mode Turbo sera désactivé.

** Lors d'un fonctionnement en G amélioré 125, ce dispositif Wi-Fi peut atteindre un débit réel égal ou supérieur à 34,1 Mbps, ce qui est le débit équivalent d'un système suivant le protocole 802.11g et fonctionnant à un débit de données de 125 Mbps. Le débit réel variera en fonction de l'environnement, des conditions d'utilisation et d'autres facteurs.*

Configuration QoS (Quality of Service) – QoS établit la priorité des données sur le réseau, telles que le contenu multimédia et la téléphonie Internet (VoIP), de manière à éviter les interférences avec d'autres données transmises sur le réseau. Basé sur 802.11e, il est possible d'activer ou de désactiver cette fonction en la sélectionnant dans le menu déroulant (3) et en choisissant le mode d'accusé de réception souhaité. S'il est prévu d'accéder en flux continu à du contenu multimédia ou d'utiliser la téléphonie Internet sur le réseau, Dynex recommande d'activer la fonction QoS.

Modification du canal sans fil

Il est possible de choisir entre plusieurs canaux de fonctionnement. Aux États-Unis, il existe 11 canaux. En Australie, au Royaume-Uni et dans la plupart des pays européens, il existe 13 canaux. Dans un petit nombre d'autres pays, les exigences concernant les canaux sont différentes. Le routeur est configuré de façon à fonctionner sur les canaux appropriés pour le pays de résidence de l'utilisateur. Le canal par défaut est 11 (à moins que l'utilisateur ne réside dans un pays où le canal 11 est interdit). Si besoin est, le canal peut être modifié. Si d'autres réseaux sans fil fonctionnent dans le secteur, le réseau doit être configuré de manière à fonctionner sur un canal différent de celui des autres réseaux sans fil. Pour un bon fonctionnement, utiliser un canal qui se trouve au moins à cinq canaux d'écart d'un autre réseau sans fil. Par exemple, si un autre réseau fonctionne sur le canal 11, choisir le canal 6 ou inférieur pour celui-ci. Pour changer de canal, sélectionner le canal souhaité dans la liste, puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le changement est immédiat.

Utilisation de la fonction Broadcast SSID (Diffusion du SSID)

Remarque : *Cette fonctionnalité avancée doit uniquement être employée par des utilisateurs expérimentés.*

Pour plus de sécurité, choisir de ne pas diffuser le SSID du réseau. Ainsi, le nom du réseau demeurera caché pour les ordinateurs qui recherchent la présence de réseaux sans fil. Pour désactiver la diffusion du SSID, désélectionner la case en regard de **Broadcast SSID** (Diffusion du SSID), puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le changement est immédiat. Chaque ordinateur doit maintenant être configuré pour se connecter au SSID spécifique. Le paramètre **ANY** (TOUS) pour le SSID ne sera plus accepté. Se reporter à la documentation de l'adaptateur réseau sans fil pour obtenir des informations sur la procédure à suivre pour effectuer cette modification.

Protected Mode Switch (Commutateur en mode protégé) – Faisant partie de la spécification 802.11g, le mode protégé assure un fonctionnement satisfaisant des clients et points d'accès 802.11g en présence d'un trafic 802.11b dense dans l'environnement d'exploitation. Lorsque le mode protégé est **ON** (Activé), le 802.11g effectue un balayage pour détecter le trafic d'autres réseaux sans fil avant de transmettre les données. Par conséquent, l'utilisation de ce mode dans un environnement avec un trafic 802.11b DENSE ou comportant des interférences permet d'obtenir les meilleurs résultats. Dans un environnement avec très peu, voire pas du tout, de trafic issu d'autres réseaux sans fil, les meilleures performances seront obtenues en désactivant le mode protégé (**OFF**).

Sécurisation du réseau Wi-Fi[MD]

Voici quelques façons d'optimiser la sécurité du réseau sans fil et de protéger les données des yeux et oreilles indiscrets. Cette section est destinée aux utilisateurs de réseaux sans fil à domicile ou dans de petites entreprises.

À la date de publication de ce manuel, quatre méthodes de cryptage sont disponibles.

Nom	Wired Equivalent Privacy 64 bits	Wired Equivalent Privacy 128 bits	Wi-Fi Protected Access-TKIP	Wi-Fi Protected Access 2
Acronyme	WEP 64 bits	WEP 128 bits	WPA-TKIP/AES (ou juste WPA)	WPA2-AES (ou juste WPA2)
Sécurité	Bonne	Meilleure	Optimale	Optimale
Fonctionnalités	Clés statiques	Clés statiques	Cryptage à clé dynamique et authentification réciproque.	Cryptage à clé dynamique et authentification réciproque.
	Clés de cryptage basées sur l'algorithme RC4 (généralement clés de 40 bits).	Plus sûr que le WEP 64 bits en utilisant une longueur de clé de 104 bits plus 24 bit supplémentaires de données générées par le système.	TKIP (Temporal Key Integrity Protocol) ajouté afin que les clés soient permutées et le cryptage renforcé.	AES (Advanced Encryption Standard) ne cause aucune perte de débit.

WEP (Wired Equivalent Privacy)

Le WEP est un protocole courant qui fournit une sécurité à tous les produits sans fil compatibles Wi-Fi. Le WEP donne aux réseaux sans fil un niveau de protection équivalent à celui d'un réseau câblé comparable.

WEP 64 bits – Le WEP 64 bits a été introduit la première fois avec un cryptage sur 64 bits, ce qui comprend une clé de 40 bits plus 24 bits supplémentaires composés de données générées par le système (64 bits au total). Certains fabricants parlent de cryptage sur 40 bits lorsqu'ils font référence au cryptage sur 64 bits. Peu après le lancement de la technologie, des chercheurs ont découvert que le cryptage sur 64 bits était trop simple à décoder.

Cryptage 128 bits – Pour contrer la faille de sécurité du WEP 64 bits, une méthode de cryptage plus sécurisée, le WEP 128 bits, a été créée. Le WEP 128 bits comprend une clé de 104 bits plus 24 bits supplémentaires composés de données générées par le système (128 bits au total). Certains fabricants parlent de cryptage sur 104 bits lorsqu'ils font référence au cryptage sur 128 bits. La plupart des nouveaux dispositifs sans fil disponibles sur le marché aujourd'hui prennent en charge le cryptage WEP 64 bits et 128 bits, mais il se peut que des dispositifs plus anciens ne prennent en charge que le WEP 64 bits. Tous les produits sans fil de Dynex prennent en charge le WEP 64 bits et 128 bits.

Encryption Keys (Clés de cryptage) – Après avoir sélectionné le mode de cryptage WEP 64 bits ou 128 bits, il est essentiel de générer une clé de cryptage. Si la clé de cryptage n'est pas la même dans tout le réseau sans fil, les dispositifs du réseau sans fil ne pourront pas communiquer les uns avec les autres. La clé peut être saisie en tapant manuellement la clé hexadécimale, ou en tapant un mot de passe dans le champ **Passphrase** (Mot de passe), puis en cliquant sur **Generate** (Générer) pour créer une clé. Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 64 bits, il faut entrer 10 clés hexadécimales. Pour le mode WEP 128 bits, il faut entrer 26 caractères hexadécimaux.

Par exemple :

AF 0F 4B C3 D4 = clé pour WEP 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé pour WEP 128 bits

Le mot de passe WEP n'est PAS la même chose que la clé WEP. La carte utilise ce mot de passe pour générer les clés WEP, mais différents fabricants de matériel peuvent avoir différentes méthodes pour générer les clés. Si le réseau comporte des équipements de différentes marques, le plus simple est d'utiliser la clé WEP hexadécimale du routeur sans fil et de l'entrer manuellement dans le tableau des clés WEP hexadécimales de l'écran de configuration de la carte.

Synchronisation de sécurité (WPS)

La routeur est équipé de la dernière norme de sécurité, appelée *Wi-Fi Protected Access* (WPA2), et de l'ancienne norme de sécurité, appelée *Wired Equivalent Privacy* (WEP). Il prend également en charge la spécification *Wi-Fi Protected Setup* (WPS), qui simplifie la configuration d'un réseau sans fil. WPS utilise des méthodologies familières, comme saisir un *numéro d'identification personnel* (NIP) ou appuyer sur une touche, pour permettre aux utilisateurs de configurer automatiquement les noms des réseaux et les protocoles WPA/WPA2 de cryptage et d'authentification des données. Par défaut, la sécurité sans fil est désactivée. Pour activer la sécurité, il faut d'abord déterminer quelle norme sera utilisée. Pour accéder aux paramètres de sécurité de la carte, cliquer sur **Security** (Sécurité) sous l'onglet **Wireless** (Sans fil).

Utilisation de la synchronisation de sécurité (WPS)

La synchronisation de sécurité (WPS) utilise WPA2 pour le cryptage. Elle ne fournit aucune sécurité supplémentaire, mais standardise la méthode de sécurisation du réseau sans fil. Il est possible d'utiliser soit la méthode de configuration du bouton-poussoir (PBC), soit la méthode NIP pour permettre à un dispositif d'accéder au réseau sans fil. Conceptuellement, les deux méthodes fonctionnent comme suit :

PBC : Appuyer sur la touche de synchronisation de sécurité (WPS), située sur le dessus du routeur, sans la relâcher pendant trois secondes. Entamer ensuite la procédure de synchronisation de sécurité (WPS) sur le client au cours des deux minutes suivantes. Le client échangera automatiquement les informations de sécurité et sera ajouté au réseau sans fil. Le client a maintenant été ajouté de façon sécurisée au réseau sans fil. Le fait d'appuyer sur la touche de synchronisation de sécurité activera automatiquement WPS. La méthode PBC peut également être lancée depuis un ordinateur portatif.

NIP : Le périphérique client est doté d'un numéro NIP (de quatre ou huit caractères) qui est associé à WPS. Activer WPS au moyen de l'interface utilisateur illustrée ci-dessous. Entrer le NIP du client dans le registre interne du routeur (accessible au moyen de cette IU). Le client sera automatiquement admis dans le réseau sans fil en moins de deux minutes.

1. Wi-Fi Protected Setup (WPS) : Enabled (Activé) ou Disabled (Désactivé).
2. Méthode du numéro d'identification personnel (NIP) : Avec cette méthode, un client sans fil souhaitant accéder au réseau doit fournir au routeur un NIP de 4 ou 8 caractères. Après avoir cliqué sur « Enroll » (Inscription), il faut démarrer le protocole de transfert WPS à partir du client au cours des deux minutes suivantes.
3. NIP du routeur : Si un registre externe est disponible, il est possible d'entrer le NIP du routeur dans le registre. Cliquer sur **Generate New PIN** (Générer nouveau NIP) pour remplacer la valeur par défaut du NIP, ou cliquer sur **Restore Default PIN** (Rétablir NIP par défaut) pour réinitialiser la valeur du NIP.
4. Méthode de configuration du bouton-poussoir (PBC) : PBC est une autre méthode permettant de se connecter à un réseau WPS. Appuyer sur la touche de synchronisation de sécurité, située au dos du routeur, pendant trois secondes, puis initier la configuration PBC sur le périphérique client. Il est également possible de cliquer sur « Start PBC » (Démarrer PBC) pour démarrer ce processus.
5. Méthode de configuration manuelle : Cette section indique les paramètres de sécurité par défaut si WPS n'est pas utilisé.

Le routeur est équipé de WPA2, qui est la deuxième génération de la norme 802.11i basée sur le WPA. Elle offre un niveau plus élevé de sécurité sans fil en combinant des méthodes avancées d'authentification de réseau et des méthodes de cryptage AES (Advanced Encryption Standard) plus robustes.

WPA (Wi-Fi Protected Access)

Le WPA est une nouvelle norme Wi-Fi qui apporte des améliorations aux caractéristiques de sécurité du WEP. Pour utiliser la sécurité WPA, les pilotes et le logiciel des appareils sans fil doivent être mis à niveau pour en assurer la prise en charge. Ces mises à niveau se trouvent sur le site Web du fournisseur des appareils sans fil. Il existe trois types de sécurité WPA : WPA-PSK (pas de serveur), WPA (avec serveur RADIUS) et WPA2.

WPA-PSK (pas de serveur) utilise en tant que clé de réseau ce que l'on appelle une clé pré-partagée. Une clé de réseau est un mot de passe qui comporte de 8 à 63 caractères. Cela peut être une combinaison de lettres, de chiffres ou de caractères. Chaque client utilise la même clé de réseau pour accéder au réseau. Généralement, il s'agit du mode utilisé dans un environnement familial.

WPA (avec serveur RADIUS) est un système dans lequel un serveur RADIUS distribue automatiquement la clé du réseau aux clients. Ceci se trouve généralement dans un environnement professionnel.

WPA2 utilise AES (Advanced Encryption Standard) pour le cryptage des données, offrant ainsi une sécurité bien supérieure à WPA. Le WPA utilise à la fois le protocole TKIP (Temporal Key Integrity Protocol) et AES pour le cryptage.

La plupart des produits Wi-Fi sont expédiés sans qu'aucune sécurité ne soit activée. Aussi, une fois que le réseau fonctionne, il faut activer le WEP ou le WPA et vérifier que tous les dispositifs sans fil partagent la même clé de réseau.

***IMPORTANT**: Il faut maintenant configurer toutes les cartes réseau pour qu'elles correspondent à ces paramètres.*

Partage des clés réseau

La plupart des produits Wi-Fi sont expédiés sans qu'aucune sécurité ne soit activée. Aussi, une fois que le réseau fonctionne, il faut activer le WEP ou le WPA et vérifier que tous les dispositifs de réseau sans fil partagent la même clé de réseau.

La carte réseau sans fil G pour ordinateur de bureau ne peut pas accéder au réseau parce qu'elle utilise une clé réseau différente de celle configurée sur le routeur sans fil G amélioré.

Utilisation d'une clé hexadécimale

Une clé hexadécimale est un mélange de chiffres et de lettres de A à F et de 0 à 9. Les clés de 64 bits sont constituées de cinq nombres de deux chiffres. Les clés de 128 bits sont constituées par 13 nombres de deux chiffres.

Par exemple :

AF 0F 4B C3 D4 = clé 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé 128 bits

Remarque pour les utilisateurs de Mac : *Les produits AirPort*[MD] *d'Apple*[MD] *de première génération ne prennent en charge que le cryptage sur 64 bits. Les produits Apple AirPort 2 prennent en charge le cryptage sur 64 bits ou 128 bits. Vérifier le produit pour savoir quelle est la version utilisée. S'il n'est pas possible de configurer le réseau avec le cryptage sur 128 bits, essayer le cryptage sur 64 bits.*

Configuration du WEP

Pour configurer le cryptage WEP 64 bits :

1. Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless* > *Security* (Sans fil > Sécurité) s'affiche.
2. Sélectionner **64-bit WEP** (WEP 128 bits) dans la liste **Security Mode** (Mode de sécurité).
3. Entrer la clé en saisissant manuellement la clé hexadécimale, ou cocher la case **Passphrase** (Mot de passe), puis saisir le mot de passe.
4. Cliquer sur **Generate** (Générer) pour générer quatre clés hexadécimales différentes.

   Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 64 bits, il faut entrer 10 caractères hexadécimaux.

   Par exemple : AF 0F 4B C3 D4 = clé pour WEP 64 bits
5. Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.

   Attention *: Si le routeur sans fil ou le point d'accès sans fil G amélioré est configuré à partir d'un ordinateur doté d'un client sans fil, il faut s'assurer que la sécurité est activée (ON) pour ce client sans fil. Sinon, le client perdra sa connexion sans fil.*

Pour configurer le cryptage WEP 128 bits :

Remarque pour les utilisateurs de Mac : *L'option de mot de passe ne fonctionne pas avec Apple AirPort. Pour configurer le cryptage sur un ordinateur Mac, utiliser la méthode manuelle décrite dans la section suivante.*

1. Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless Security* (Sécurité sans fil) s'affiche.
2. Sélectionner **128-bit WEP** (WEP 128 bits) dans la liste **Security Mode** (Mode de sécurité).
3. Entrer la clé en saisissant manuellement la clé hexadécimale, ou cocher la case **Passphrase** (Mot de passe), puis saisir le mot de passe.
4. Cliquer sur **Generate** (Générer) pour générer quatre clés hexadécimales différentes.

   Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 128 bits, il faut entrer 26 caractères hexadécimaux.

   Par exemple : C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = clé pour WEP 128 bits
5. Cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres.

***Attention** : Si le routeur sans fil ou le point d'accès sans fil G amélioré est configuré à partir d'un ordinateur doté d'un client sans fil, il faut s'assurer que la sécurité est activée (ON) pour ce client sans fil. Sinon, le client perdra sa connexion sans fil.*

Modification des paramètres de sécurité sans fil

Le routeur comprend la toute dernière norme de sécurité, appelée WPA (Wi-Fi Protected Access). En outre, il prend en charge les normes de sécurité plus anciennes telles que le WEP (Wired Equivalent Privacy). Par défaut, la sécurité sans fil est désactivée. Pour activer la sécurité, il faut d'abord déterminer quelle norme sera utilisée. Pour accéder aux paramètres de sécurité, cliquer sur **Security** (Sécurité) sous l'onglet **Wireless** (Sans fil).

Configuration du WPA

***Remarque** : Pour utiliser la sécurité WPA, tous les clients doivent être mis à jour avec les logiciels et les pilotes qui la prennent en charge. À la date de publication de ce manuel, un correctif de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft*[MD]*. Ce correctif ne fonctionne qu'avec Windows XP. Il faudra également télécharger sur le site d'assistance technique de Dynex le pilote le plus récent pour la carte réseau sans fil G amélioré de Dynex pour ordinateur de bureau ou portatif. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge. Le correctif de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Dynex.*

Le WPA utilise ce qu'on appelle une « clé pré-partagée » en tant que clé de sécurité. Une clé pré-partagée est un mot de passe qui comporte de 8 à 63 caractères. Cela peut être une combinaison de lettres, de chiffres ou d'autres caractères. Chaque client utilise la même clé pour accéder au réseau. Généralement, ce mode est utilisé dans un environnement familial.

Le WPA2, c'est le WPA de seconde génération. Il offre une technique de cryptage plus avancée que le WPA.

Pour configurer le WPA/WPA2 :

1. Cliquer sur **Security** (Sécurité) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless* > *Security* (Sans fil > Sécurité) s'affiche.
2. Sélectionner **WPA/WPA2-Personal (PSK)** dans la liste **Security Mode** (Mode de sécurité).
3. Sélectionner **WPA-PSK** pour une simple authentification WPA, ou **WPA2-PSK** pour une simple authentification WPA2; il est également possible de sélectionner **WPA-PSK + WPA2-PSK** pour choisir WPA et WPA2 comme type d'authentification.
4. Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres ou des symboles. Cette même clé doit être utilisée sur tous les clients qui seront configurés. Cette clé pré-partagée donnera aux utilisateurs un accès complet au réseau, y compris aux fichiers et imprimantes partagés.
5. Cliquer sur **Apply Changes** (Appliquer les modifications) pour terminer. Il faut maintenant configurer tous les clients avec ces paramètres, suivant le type d'accès souhaité pour chacun d'eux.

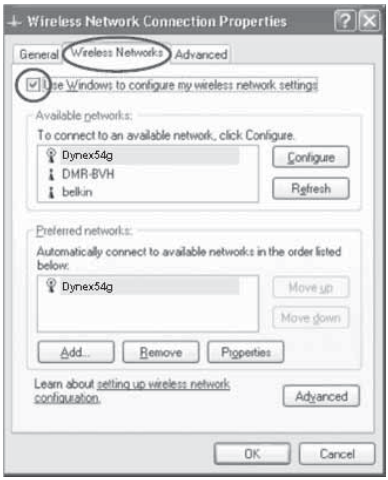
***Remarque :** Si une carte sans fil n'est pas équipée d'un logiciel compatible WPA, un fichier de Microsoft, appelé **Windows XP Support Patch for Wireless Protected Access**, peut être téléchargé gratuitement.*

Le fichier mis à disposition par Microsoft fonctionne uniquement avec Windows XP. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge.

***Important** : Il faudra également vérifier que le fabricant de la carte sans fil prend en charge le WPA et que le pilote le plus récent a été téléchargé à partir de son site Web et installé.*

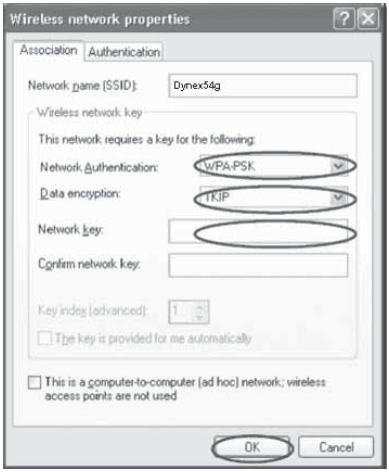
Configuration de l'utilitaire réseau sans fil de Windows XP pour utiliser le WPA-PSK :

1. Sous Windows XP, cliquer sur **Start** (Démarrer), **Control Panel** (Panneau de configuration) et **Network Connections** (Connexions réseau).
2. Cliquer à l'aide du bouton droit de la souris sur **Wireless Network Connection** (Connexion réseau sans fil), puis sur **Properties** (Propriétés).
3. Cliquer sur l'onglet **Wireless Networks** (Réseaux sans fil). L'écran suivant s'affiche.



4. Vérifier que la case **Use Windows to configure my wireless network settings** (Utiliser Windows pour configurer mes paramètres réseau sans fil) est cochée.

5 Cliquer sur l'onglet **Wireless Networks** (Réseaux sans fil), puis sur **Configure** (Configurer). L'écran suivant s'affiche.



6 Pour un utilisateur de réseau familial ou de petite entreprise, sélectionner **WPA-PSK** sous **Network Authentication** (Authentification de réseau).

***Remarque** : Sélectionner **WPA** si cet ordinateur est utilisé pour se connecter à un réseau d'entreprise qui prend en charge un serveur d'authentification tel qu'un serveur RADIUS. Consulter l'administrateur réseau pour de plus amples informations.*

7 Sélectionner **TKIP** ou **AES** sous **Data Encryption** (Cryptage des données). Ce paramètre doit être identique à celui configuré sur le routeur.

8 Entrer la clé de cryptage dans la boîte **Network Key** (Clé de réseau).

***Important** : Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres ou des symboles. Cette même clé doit être utilisée sur tous les clients qui seront configurés.*

9 Cliquer sur **OK** pour enregistrer les modifications.

Utilisation du mode Point d'accès

***Remarque** : Cette fonctionnalité avancée doit uniquement être employée par des utilisateurs expérimentés. Il est possible de configurer le routeur pour qu'il fonctionne comme un point d'accès réseau sans fil. L'utilisation de ce mode bloque la fonction de partage IP NAT et de serveur DHCP. En mode « Point d'Accès » (AP), le routeur doit être configuré avec une adresse IP qui doit se trouver dans le même sous-réseau que le reste du réseau vers lequel une passerelle sera établie. L'adresse IP par défaut est 192.168.2.254 et le masque de sous-réseau est 255.255.255.0. Ces adresses peuvent être modifiées au besoin.*

Pour utiliser le mode Point d'accès :

1. Cliquer sur **Use as Access Point only** (Utiliser uniquement comme point d'accès) sous l'en-tête **Wireless** (Sans fil) du menu de gauche. La page *Wireless > Use as Access Point* (Sans fil > Utiliser comme point d'accès) s'affiche.

2. Sélectionner **Enable** (Activer). Lorsque cette option est sélectionnée, elle permet de modifier les paramètres IP.
3. Configurer les paramètres IP de manière à ce qu'ils correspondent à ceux du réseau, puis cliquer sur **Apply Changes** (Enregistrer les Modifications).
4. Connecter un câble depuis le port modem du routeur sur le réseau existant.

   Le routeur joue maintenant le rôle de point d'accès. Pour accéder de nouveau à l'Interface utilisateur Web avancée du routeur, taper l'adresse IP spécifiée dans la barre d'adresse du navigateur. Les paramètres de cryptage, le filtrage des adresses MAC, le SSID et le canal peuvent être configurés normalement.

Configuration du pare-feu

Le routeur est équipé d'un pare-feu qui protégera le réseau contre un grand nombre d'attaques habituelles de pirates, notamment :

- Usurpation d'adresse IP (IP Spoofing)
- SYN flood
- Attaque Land
- UDP flooding
- Ping de la mort (PoD)
- Attaque Teardrop
- Déni de service (DoS)
- Défaut ICMP
- IP de longueur nulle
- Défaut RIP
- Attaque Smurf
- Fragment flooding
- TCP Null Scan

Le pare-feu masque également les ports habituels qui sont fréquemment utilisés pour attaquer les réseaux. Ces ports apparaissent en tant que *stealth* (furtifs), ce qui veut dire en d'autres termes qu'ils n'existent pas pour un pirate potentiel. Si nécessaire, la fonction de pare-feu peut-être désactivée. Toutefois, Dynex conseille de la laisser activée. La désactivation de la protection par pare-feu ne laissera pas le réseau complètement vulnérable aux attaques des pirates, mais il est conseillé de laisser le pare-feu activé.

Configuration des paramètres de retransmission interne

La fonction *Virtual Servers* (Serveurs virtuels) permet de diriger les appels de service externes (Internet) tels qu'un serveur Web (port 80), un serveur FTP (port 21) ou toute autre application via le routeur vers le réseau interne. Étant donné que les ordinateurs internes sont protégés par un pare-feu, les ordinateurs situés hors du réseau (sur Internet) ne peuvent pas y accéder parce qu'ils ne sont pas *visibles*. Contacter le fournisseur de l'application pour déterminer quels paramètres de ports sont nécessaires.

Pour entrer des paramètres dans le serveur virtuel :

1. Ouvrir la page *Virtual Servers* (Serveurs virtuels), puis entrer l'adresse IP dans le champ prévu pour la machine (serveur) interne et les ports requis pour la transmission.
2. Sélectionner le type de port (TCP ou UDP), cliquer sur la case **Enable** (Activer), puis sur **Apply Changes** (Enregistrer les Modifications).

   Chaque entrée de port d'entrée possède deux champs, pouvant contenir cinq caractères maximum. Ces champs délimitent le début et la fin de la plage, soit [xxxxx]-[xxxxx]. Pour chaque entrée, il est possible d'entrer une seule valeur de port en remplissant les deux champs avec la même valeur (par exemple, [7500]-[7500]) ou une plage étendue (par exemple, [7500]-[9000]). Pour sélectionner plusieurs ports uniques, ou plusieurs plages et une valeur unique, il faut utiliser plusieurs entrées, jusqu'à un maximum de 20 (par exemple : 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Il est possible de transmettre un seul port par adresse IP interne.

L'ouverture de ports dans le pare-feu risque de créer un problème de sécurité. Les paramètres peuvent être activés ou désactivés très rapidement. Aussi, Dynex recommande de les désactiver lorsqu'une application particulière n'est pas utilisée.

Configuration des filtres IP de clients

Il est possible de configurer le routeur de manière à limiter l'accès à l'Internet, à la messagerie électronique ou à d'autres services réseau certains jours et à certaines heures. La restriction peut être définie pour un seul ordinateur, une plage d'ordinateurs ou plusieurs ordinateurs.

Pour limiter l'accès à l'Internet à un seul ordinateur :

1. Ouvrir la page *Firewall* > *Client IP filters* (Pare-feu > Filtres IP de clients), puis entrer l'adresse IP de l'ordinateur auquel sera limité l'accès dans les champs IP.
2. Entrer **80** dans chaque champ de port, sélectionner **Both** (Les deux), puis sélectionner **Block** (Bloquer). Il est aussi possible de sélectionner **Always** (Toujours) pour bloquer l'accès en permanence.
3. Sélectionner le jour de début en haut, l'heure de début en haut, le jour de fin en bas et l'heure de fin en bas.
4. Sélectionner **Enable** (Activer), puis cliquer sur **Apply Changes** (Enregistrer les modifications). L'ordinateur répondant à l'adresse IP indiquée sera désormais bloqué et ne pourra plus accéder à l'Internet aux heures mentionnées. Veiller à avoir sélectionné le fuseau horaire approprié dans **Utilities**> **System Settings**> **Time Zone** (Utilitaires > Paramètres système > Fuseau horaire).

Configuration du filtrage d'adresses MAC

Le filtrage d'adresses MAC est une fonction de sécurité puissante qui permet de spécifier les ordinateurs autorisés sur le réseau. Tout ordinateur qui tente d'accéder au réseau alors qu'il ne figure pas dans la liste ne pourra pas y accéder. Lorsque cette fonction est activée, il faut entrer l'adresse MAC de chaque client (ordinateur) du réseau pour permettre à chacun d'accéder au réseau.

Pour activer le filtrage d'adresses MAC :

1. Ouvrir la page *Firewall > MAC Address filters* (Pare-feu > Filtres d'adresses MAC), puis cliquer sur **Enable MAC Address Filtering** (Activer le filtrage d'adresses MAC).
2. Entrer l'adresse MAC de chaque ordinateur du réseau en cliquant sur le champ prévu et en entrant l'adresse MAC de l'ordinateur à ajouter à la liste.
3. Cliquer sur **Add** (Ajouter), puis sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les paramètres. La liste de filtrage d'adresses MAC peut comprendre jusqu'à 32 ordinateurs.

   ***Remarque** : Il n'est pas possible de supprimer l'adresse MAC de l'ordinateur qui est utilisé pour accéder aux fonctions d'administration du routeur (celui qui est actuellement en cours d'utilisation).*

Activation de la zone démilitarisée (DMZ)

La fonctionnalité DMZ permet de désigner un ordinateur du réseau qui sera placé hors du pare-feu. Ceci peut être nécessaire si le pare-feu cause des problèmes avec une application telle qu'un jeu ou une application de vidéoconférence. Cette fonctionnalité doit être utilisée de façon temporaire. L'ordinateur de la DMZ n'est PAS protégé contre les attaques de pirates. Si l'abonnement auprès du FSI prévoit des adresses IP publiques (WAN) supplémentaires, des ordinateurs supplémentaires peuvent être placés en dehors du pare-feu à condition que chaque ordinateur utilise une adresse IP publique (WAN) différente.

Pour établir une DMZ pour un ordinateur :

- Ouvrir la page *Firewall* > *DMZ* (Pare-feu > DMZ) et entrer les derniers chiffres de l'adresse IP de l'ordinateur dans le champ **IP**, cliquer sur **Enable** (Activer), puis sur **Apply Changes** (Enregistrer les modifications) pour que le changement entre en vigueur.

Blocage du ping WAN

Les pirates informatiques utilisent l'envoi de *ping* pour trouver des victimes potentielles sur Internet. En émettant un ping sur une certaine adresse IP et en recevant une réponse de celle-ci, un pirate informatique peut décider de s'intéresser à ce qui se trouve derrière cette adresse. Le routeur peut être défini de façon à ne pas répondre à un ping ICMP provenant de l'extérieur. Ceci accroît le niveau de sécurité du routeur.

Pour désactiver la réponse au ping

- Ouvrir la page *Firewall* > *WAN Ping Blocking* (Pare-feu > Blocage de ping WAN) et sélectionner Block ICMP Ping (Bloquer le ping ICMP), puis cliquer sur **Apply Changes** (Enregistrer les modifications). Le routeur ne répondra pas à un ping ICMP.

Onglet Utilities (Utilitaires)

Cet écran permet de gérer divers paramètres du routeur et de réaliser certaines fonctions d'administration.

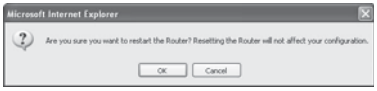
Redémarrage du routeur

Il est parfois nécessaire de redémarrer ou de réamorcer le routeur s'il commence à fonctionner de façon incorrecte. Le redémarrage ou le réamorçage du routeur ne supprimera AUCUN des paramètres de configuration.

Pour redémarrer le routeur afin de rétablir un fonctionnement normal :

1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restart Router** (Redémarrer le routeur). La page *Restart Router* (Redémarrer le routeur) s'affiche.

2. Cliquer sur **Restart Router** (Redémarrer le routeur). Le message suivant s'affiche.



3. Cliquer sur **OK**. Le message suivant s'affiche.

4. Cliquer sur **OK**. Le redémarrage du routeur peut prendre jusqu'à 25 secondes. Il est important de ne pas mettre le routeur hors tension pendant le redémarrage.

   Un compte à rebours de 25 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, le routeur est redémarré. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

Rétablissement des paramètres par défaut du constructeur

Cette option permet de rétablir tous les paramètres d'usine (par défaut) du routeur. Il est recommandé de sauvegarder les paramètres avant de rétablir les valeurs par défaut.

Pour rétablir les paramètres par défaut du constructeur :

1. Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restore Defaults** (Rétablir les paramètres par défaut). L'avertissement suivant s'affiche.

2 Cliquer sur **OK**. Le message suivant s'affiche.

3 Cliquer sur **OK**. Le rétablissement des paramètres par défaut exige un redémarrage du routeur. Le redémarrage du routeur peut prendre jusqu'à 25 secondes. Il est important de ne pas mettre le routeur hors tension pendant le redémarrage.

Un compte à rebours de 25 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, le routeur est redémarré. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

Enregistrement de la configuration en cours

Il est possible d'enregistrer la configuration en cours en utilisant cette fonction. L'enregistrement de la configuration permettra de la rétablir ultérieurement si les paramètres sont perdus ou modifiés. Il est recommandé de sauvegarder la configuration en cours avant d'effectuer une mise à jour du microprogramme.

Pour enregistrer une configuration en cours :

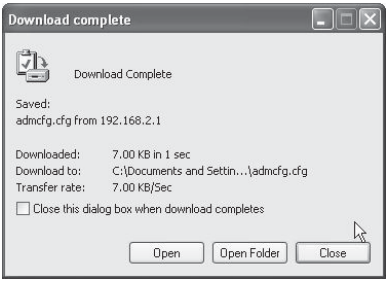
1 Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Save/ Backup Settings** (Enregistrer/sauvegarder les paramètres). La page *Save/Backup Settings* (Enregistrer/sauvegarder les paramètres) s'affiche.

2 Cliquer sur **Save** (Enregistrer). La fenêtre File Download (Téléchargement de fichier) s'affiche.

3 Cliquer sur **Save** (Enregistrer). Une fenêtre s'affiche, permettant de sélectionner l'emplacement où sera enregistré le fichier de configuration.

4 Choisir un emplacement. Il est possible de donner n'importe quel nom au fichier, ou d'utiliser le nom par défaut : « Config. ». Veiller à donner au fichier un nom qui permettra de le retrouver ultérieurement. Après la sélection de l'emplacement et du nom du fichier, cliquer sur **Save** (Enregistrer).

5 Une fois l'enregistrement terminé, la fenêtre ci-dessous s'affiche.



6 Cliquer sur **Close** (Fermer). La configuration est maintenant enregistrée.

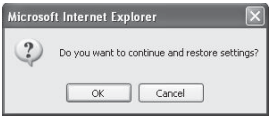
Rétablissement d'une configuration antérieure

Cette option permet de rétablir une configuration enregistrée préalablement.

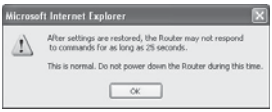
Pour rétablir une configuration enregistrée préalablement :

1 Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Restore Previous Settings** (Rétablir des paramètres antérieurs). La page *Restore Previous Settings* (Rétablir des paramètres antérieurs) s'affiche.

2 Cliquer sur **Browse** (Parcourir). Une fenêtre s'affiche, permettant de sélectionner l'emplacement du fichier de configuration. Tous les fichiers de configuration se terminent par l'extension « .bin ». Rechercher le fichier de configuration à rétablir, puis double-cliquer sur celui-ci. Le message suivant s'affiche à l'écran.



3 Cliquer sur **OK**. Une fenêtre de rappel s'affiche.



Le rétablissement de la configuration peut prendre jusqu'à 35 secondes.

4 Cliquer sur **OK**. Un compte à rebours de 35 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, la configuration du routeur est rétablie. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

Mise à jour du microprogramme

De temps en temps, Dynex peut publier de nouvelles versions du microprogramme du routeur. Ces mises à jour peuvent contenir des améliorations et des solutions aux problèmes existants. Lorsque Dynex publie un nouveau microprogramme, il est possible de le télécharger depuis le site Web des mises à jour de Dynex et d'actualiser le microprogramme du routeur avec la toute dernière version.

Pour rechercher et télécharger une nouvelle version du microprogramme :

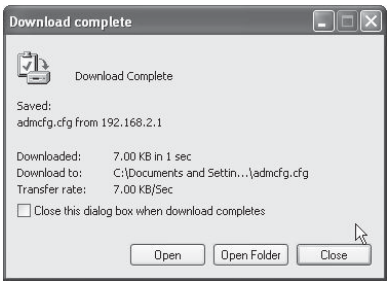
1 Sous l'en-tête **Utilities** (Utilitaires) dans le menu de gauche, cliquer sur **Firmware Update** (Mise à jour du microprogramme). La page *Utilities > Firmware updates* (Utilitaires > Mises à jour du microprogramme) s'affiche.

2 Cliquer sur **Check Firmware** (Vérifier le microprogramme). L'utilitaire vérifie si une mise à jour du microprogramme est disponible.

3 Si une nouvelle version du microprogramme est disponible, une fenêtre s'affiche, permettant de sélectionner l'emplacement où sera enregistré le fichier du microprogramme. Choisir un emplacement. Il est possible de donner n'importe quel nom au fichier, ou d'utiliser le nom par défaut. Veiller à enregistrer le fichier à un endroit où il sera possible de le retrouver ultérieurement. Une fois l'emplacement sélectionné, cliquer sur **Save** (Enregistrer).

***Remarque** : Dynex suggère de l'enregistrer sur le bureau afin de le retrouver facilement.*

4 Une fois l'enregistrement terminé, la fenêtre ci-dessous s'affiche.

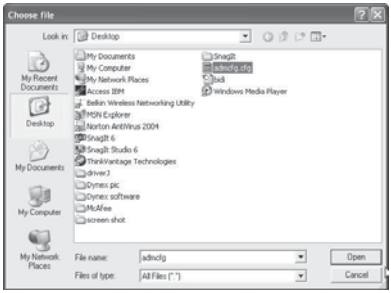


5 Cliquer sur **Close** (Fermer). Le téléchargement est terminé. Pour mettre le microprogramme à jour, procéder comme indiqué dans la section **Pour mettre à jour le microprogramme du routeur**.

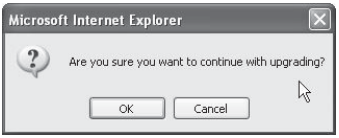
Pour mettre à jour le microprogramme du routeur :

1 Sur la page *Firmware Update* (Mise à jour du microprogramme), cliquer sur **Browse** (Parcourir). Une fenêtre s'affiche, permettant de sélectionner l'emplacement du fichier de mise à jour du microprogramme.

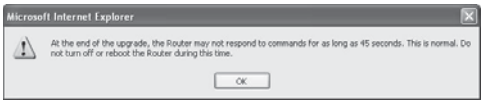
2 Accéder au fichier du microprogramme qui a été téléchargé, puis le sélectionner en double-cliquant sur son nom.



3 La boîte de dialogue **Update Firmware** (Mise à jour du microprogramme) affiche maintenant l'emplacement et le nom du fichier sélectionné. Cliquer sur **Update** (Mettre à jour). Un message demande confirmation avant de continuer.



4 Cliquer sur **OK**. Un autre message s'affiche. Ce message indique que le routeur peut ne pas répondre pendant une minute, car le microprogramme est en cours de chargement et que le routeur doit être redémarré.



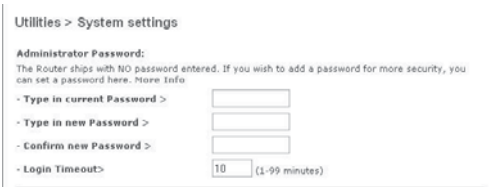
5 Cliquer sur **OK**. Un compte à rebours de 60 secondes s'affiche à l'écran. Lorsqu'il parvient à zéro, la mise à jour du microprogramme du routeur est terminée. La page d'accueil du routeur doit s'afficher automatiquement. Dans le cas contraire, taper l'adresse du routeur (par défaut = 192.168.2.1) dans la barre de navigation du navigateur.

La mise à jour du microprogramme est terminée.

Modifications des paramètres du système

La page *System Settings* (Paramètres du système) est l'endroit où il est possible d'entrer un nouveau mot de passe d'administrateur, définir le fuseau horaire, activer la gestion à distance et activer ou désactiver la fonction NAT du routeur.

Définition ou modification du mot de passe d'administrateur



AUCUN mot de passe n'est entré avant la livraison du routeur. Si l'utilisateur souhaite ajouter un mot de passe pour plus de sécurité, il peut en définir un ici. Noter le mot de passe et le garder en lieu sûr car il sera indispensable pour se connecter au routeur à l'avenir. Il est également recommandé de définir un mot de passe s'il est prévu d'utiliser la fonction de gestion du routeur à distance.

Modification du paramètre de délai avant déconnexion

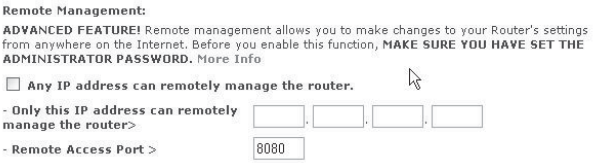
L'option de délai avant déconnexion permet de définir la durée pendant laquelle l'utilisateur peut rester connecté à l'Interface utilisateur Web avancée du routeur. Le temporisateur démarre lorsqu'il n'y a plus d'activité. Par exemple, des modifications ont été apportées au moyen de l'Interface utilisateur Web avancée, puis l'utilisateur a quitté l'ordinateur sans cliquer sur « Logout » (Déconnexion). Si le délai de déconnexion est de 10 minutes, 10 minutes après le départ de l'utilisateur, la session prendra fin. L'utilisateur devra de nouveau se connecter au routeur pour procéder à d'autres modifications. L'option de délai de déconnexion a été créée dans un but de sécurité. La valeur par défaut est de 10 minutes.

***Remarque** : Un seul ordinateur à la fois peut être connecté à l'Interface utilisateur Web avancée du routeur.*

Réglage de l'heure et choix d'un fuseau horaire

Le routeur marque l'heure en se connectant à un serveur SNTP (Simple Network Time Protocol). Cela lui permet de synchroniser l'horloge système du routeur avec Internet. L'horloge synchronisée du routeur est employée pour enregistrer le journal de sécurité et contrôler le filtrage des clients. Sélectionner un fuseau horaire. Si l'utilisateur vit dans une région qui passe à l'heure d'été, cocher la case située à côté de **Automatically Adjust Daylight Saving** (Régler automatiquement à l'heure d'été). Il se peut que l'horloge système ne soit pas mise à jour immédiatement. Laisser au minimum 15 minutes au routeur pour contacter les serveurs horaires sur Internet et obtenir une réponse. Il n'est pas possible de régler l'horloge manuellement.

Activation de la gestion à distance



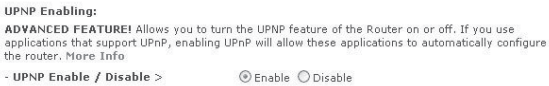
Avant d'activer cette fonctionnalité avancée du routeur, VÉRIFIER QU'UN MOT DE PASSE D'ADMINISTRATEUR A BIEN ÉTÉ DÉFINI. La gestion à distance permet de modifier les paramètres du routeur depuis Internet. Il existe deux méthodes de gestion à distance du routeur. La première consiste à accéder au routeur depuis un endroit quelconque d'Internet en sélectionnant **Any IP address can remotely manage the Router** (Toute adresse IP peut gérer le routeur à distance). Après avoir tapé l'adresse IP WAN depuis un ordinateur quelconque relié à l'Internet, un écran de connexion s'affichera, demandant d'entrer le mot de passe du routeur. La seconde méthode consiste à autoriser une seule adresse IP spécifique à gérer le routeur à distance. Cette méthode est plus sûre, mais moins pratique. Pour utiliser cette méthode, entrer l'adresse IP autorisée à accéder au routeur dans le champ fourni à cet effet, puis sélectionner **Only this IP address can remotely manage the Router** (Seule cette adresse IP est autorisée à gérer le routeur à distance). Avant d'activer cette fonction, Dynex CONSEILLE VIVEMENT de définir un mot de passe d'administrateur. Si le mot de passe reste vide, le routeur sera potentiellement vulnérable à des intrusions.

Activation/Désactivation de la traduction d'adresses réseau (NAT)

***Remarque** : Cette fonctionnalité doit uniquement être modifiée par des utilisateurs expérimentés.*

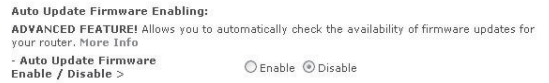
La traduction d'adresses réseau (Network Address Translation, ou NAT) est la méthode selon laquelle le routeur partage l'adresse IP unique attribuée par le FSI avec les autres ordinateurs du réseau. Cette fonction est activée par défaut. Elle ne doit être désactivée que si le FSI attribue plusieurs adresses IP ou s'il est nécessaire de la désactiver pour une configuration système avancée. Si l'utilisateur dispose d'une seule adresse IP et que la fonction NAT est désactivée, les ordinateurs du réseau ne pourront pas accéder à l'Internet. D'autres problèmes risquent également de survenir. La désactivation de NAT désactive les fonctions du pare-feu.

Activation/Désactivation de l'UPnP



UPnP (Universal Plug-and-Play) est une autre fonctionnalité avancée offerte par ce routeur. C'est une technologie qui offre un fonctionnement transparent de la messagerie vocale et vidéo, des jeux et d'autres applications compatibles avec l'UPnP. Certaines applications exigent que le pare-feu du routeur soit configuré d'une certaine manière pour fonctionner correctement. Ceci demande habituellement l'ouverture des ports TCP et UDP. Une application compatible UPnP peut communiquer avec le routeur en lui « disant » comment le pare-feu doit être configuré. Au départ, la fonction UPnP du routeur est désactivée. Lors de l'utilisation d'applications compatibles UPnP, activer la fonction UPnP pour profiter de leurs fonctionnalités UPnP. Sélectionner **Enable** (Activer) dans la section **UPnP Enabling** (Activation UPnP) de la page *Utilities* (Utilitaires), puis cliquer sur **Apply Changes** (Enregistrer les modifications) pour enregistrer les modifications.

Activation/Désactivation de la mise à jour automatique du microprogramme



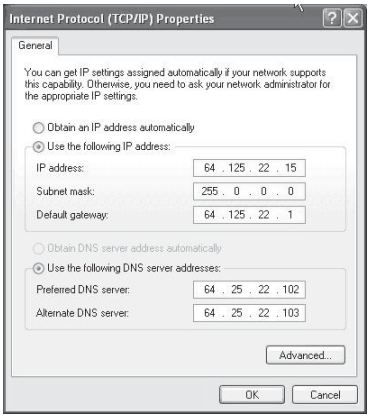
Cette innovation permet au routeur, grâce à une fonction intégrée, de vérifier automatiquement l'existence d'une nouvelle version du microprogramme et d'avertir l'utilisateur lorsqu'elle est disponible. Lors de la connexion à l'Interface utilisateur Web avancée du routeur, ce dernier effectue une vérification pour savoir s'il existe une nouvelle version du microprogramme. Si tel est le cas, l'utilisateur en est informé. Il est alors possible de télécharger la nouvelle version ou d'ignorer le message. Au départ, cette fonction du routeur est activée. Pour la désactiver, sélectionner **Disable** (Désactiver), puis cliquer sur **Apply Changes** (Enregistrer les modifications).

Configuration manuelle des paramètres réseau

Afin que l'ordinateur puisse communiquer efficacement avec le routeur, il faut modifier les paramètres TCP/IP de l'ordinateur à DHCP.

Pour configurer manuellement les adaptateurs réseau sous Windows 2000, NT, XP ou Vista :

1. Cliquer sur **Start** (Démarrer), **Settings** (Paramètres), puis sur **Control Panel** (Panneau de configuration).
2. Double-cliquer sur l'icône **Network and dial-up connections** (Connexions réseau et accès à distance) (Windows 2000) ou sur l'icône **Network** (Réseau) (Windows XP ou Vista).
3. Cliquer avec le bouton droit de la souris sur la connexion au réseau local (**Local Area Connection**) associée à l'adaptateur réseau, puis sélectionner **Properties** [Propriétés] dans la liste.
4. Cliquer sur **Internet Protocol (TCP/IP)** (Protocole Internet [TCP/IP]), puis cliquer sur **Properties** (Propriétés). L'écran suivant s'affiche.



5. Si l'option **Use the following IP address** (Utiliser l'adresse IP suivante) est sélectionnée, le routeur devra être configuré pour un type de connexion IP statique. Noter par écrit les informations de l'adresse. Il faudra entrer ces informations dans le routeur.
6. Si ce n'est pas déjà fait, sélectionner **Obtain an IP address automatically** (Obtenir automatiquement une adresse IP) et **Obtain DNS server address automatically** (Obtenir les adresses des serveurs DNS automatiquement), puis cliquer sur **OK**.

   Les adaptateurs réseau sont maintenant configurés pour fonctionner avec le routeur.

Pour configurer manuellement les adaptateurs réseau sous Windows 98SE ou Me :

1. Cliquer avec le bouton droit de la souris sur **My Network Neighborhood** (Voisinage réseau), puis sélectionner **Properties** (Propriétés) dans la liste.
2. Sélectionner **TCP/IP**, puis sur **settings** (paramètres) pour l'adaptateur installé. La fenêtre suivante s'affiche.
3. Si l'option **Specify an IP address** (Spécifier une adresse IP) est sélectionnée, le routeur devra être configuré pour un type de connexion IP statique. Noter par écrit les informations de l'adresse. Il faudra entrer ces informations dans le routeur.

- Écrire l'adresse IP et le masque de sous-réseau de l'onglet **IP Address** (Adresse IP).
- Cliquer sur l'onglet **Gateway** (Passerelle). Écrire l'adresse de passerelle au bas du tableau.
- Cliquer sur l'onglet **DNS Configuration** (Configuration DNS). Écrire l'adresse (ou les adresses) DNS dans le tableau.

4 Si elle n'est pas déjà sélectionnée, cliquer sur l'option **Obtain IP address automatically** (Obtenir automatiquement une adresse IP) sous l'onglet **IP Address** (Adresse IP), puis cliquer sur **OK**.

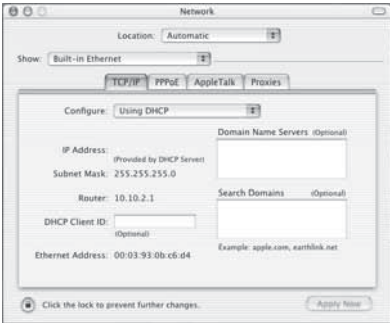
5 Redémarrer l'ordinateur. Quand l'ordinateur redémarre, les adaptateurs réseau sont maintenant configurés de manière à fonctionner avec le routeur.

Procéder comme suit pour configurer D'ABORD l'ordinateur connecté au modem câble ou DSL. Il est également possible de suivre cette procédure pour ajouter des ordinateurs au routeur une fois que ce dernier a été configuré pour l'accès à l'Internet.

Pour configurer manuellement les adaptateurs réseau sous Mac OS X :

1 Cliquer sur l'icône **System Preferences** (Préférences système). Le menu *System Preferences* (Préférences système) s'affiche.

2 Cliquer sur **Network** (Réseau). La fenêtre *Network* (Réseau) s'ouvre.



3 Sélectionner **Built-in Ethernet** (Ethernet intégré) dans la liste **Show** (Afficher).

4 Cliquer sur l'onglet **TCP/IP**. À côté de **Configure:** (Configurer :) devrait figurer **Manually** (Manuellement) ou **Using DHCP** (Utiliser DHCP). Si tel n'est pas le cas, vérifier sous l'onglet **PPPoE** que l'option **Connect using PPPoE** (Se connecter via PPPoE) n'est PAS sélectionnée. Si elle l'est, il faudra configurer le routeur pour une connexion de type PPPoE en utilisant le nom d'utilisateur et le mot de passe de l'utilisateur.

***Remarque** : Si l'option **Manually** (Manuellement) est sélectionnée dans la liste **Configure** (Configurer), le routeur devra être configuré pour un type de connexion IP statique. Noter par écrit les informations de l'adresse. Il faudra entrer ces informations dans le routeur.*

5 Sélectionner **Using DHCP** (Utiliser DHCP) dans la liste **Configure** (Configurer), puis cliquer sur **Apply Now** (Appliquer).

Les adaptateurs réseau sont maintenant configurés pour fonctionner avec le routeur.

Paramètres recommandés pour le navigateur Web

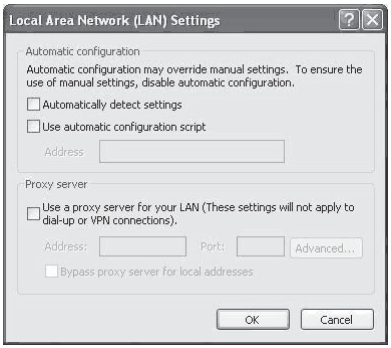
Dans la majorité des cas, il sera inutile de modifier les paramètres du navigateur Web. En cas de problème pour accéder à l'Internet ou avec l'Interface utilisateur Web avancée, modifier les paramètres du navigateur et choisir ceux recommandés dans cette section.

Pour changer les paramètres dans Internet Explorer 4.0 ou version ultérieure :

1 Lancer le navigateur Web. Ouvrir le menu *Tools* (Outils), puis sélectionner **Internet Options** (Options Internet). La page *Internet Options* (Options Internet) s'affiche.

2 Cliquer sur l'onglet **Connections** (Connexions), puis sélectionner **Never dial a connection** (Ne jamais établir de connexion). S'il n'est pas possible d'effectuer une sélection, passer à l'étape suivante.

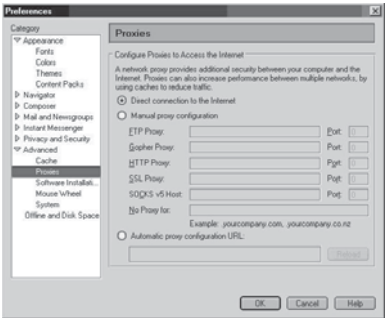
3 Cliquer sur **LAN Settings...** (Paramètres du réseau local...). La page *LAN Settings* (Configuration du réseau local) s'affiche.



4 Vérifier qu'aucune des options affichées n'est cochée. Cliquer sur **OK** pour fermer la page, puis de nouveau sur **OK** dans la page *Internet Options* (Options Internet) pour quitter.

Pour changer les paramètres dans Netscape^{MD} Navigator^{MD} 4.0 ou version ultérieure :

1 Lancer Netscape, puis ouvrir le menu **Edit** (Édition) et cliquer sur **Preferences** (Préférences). La page *Preferences* (Préférences) s'affiche à l'écran.



2 Cliquer sur **Advanced** (Avancé), puis sur **Proxies** (Serveurs proxy).

3 Sélectionner **Direct connection to the Internet** (Connexion directe à l'Internet), puis cliquer sur **OK** pour quitter.

Problèmes et solutions

Emplacement du routeur pour des performances optimales

Plus l'ordinateur est proche du routeur sans fil, meilleure est la connexion sans fil. La portée normale des dispositifs sans fil, en intérieur, est comprise entre 30 et 60 mètres. De la même manière, la connexion sans fil et les performances se dégradent quelque peu lorsque la distance entre le routeur sans fil et les dispositifs connectés augmente. Ceci peut ne pas être perceptible. À mesure que l'on s'éloigne du routeur sans fil, la vitesse de connexion peut diminuer.

Parmi les facteurs qui peuvent affaiblir les signaux simplement en faisant obstacle aux ondes radio du réseau figurent les appareils ou les obstructions métalliques et les murs.

En cas de difficultés concernant les performances du réseau et pouvant avoir trait à des facteurs de portée ou d'obstruction, essayer d'approcher l'ordinateur du routeur sans fil, à une distance de 2 à 3 mètres (5 à 10 pi), pour voir si la distance constitue la source du problème.

> ***Remarque** : Bien que certains des éléments indiqués ci-dessous puissent affecter les performances du réseau, ils n'empêcheront pas le réseau sans fil de fonctionner. S'il semble que le réseau ne fonctionne pas de façon optimale, cette liste de vérification peut être utile.*

1. Emplacement du routeur sans fil

Placer le routeur sans fil, le point de connexion central du réseau, aussi près que possible du centre des périphériques du réseau sans fil.

Afin d'assurer une couverture optimale du réseau sans fil pour les « clients sans fil » (par exemple, les ordinateurs dotés d'une carte sans fil pour ordinateur portatif ou de bureau ou d'un adaptateur USB) :

- Veiller à ce que les antennes du routeur sans fil soient parallèles et disposées à la verticale (en pointant vers le plafond). Si le routeur est lui-même en position verticale, essayer autant que possible de disposer les antennes de façon à ce qu'elles pointent vers le haut.
- Dans des habitations à plusieurs étages, placer le routeur à l'étage le plus central de la maison. Ceci peut signifier qu'il faudra placer le routeur sans fil à un étage supérieur.
- Éviter de placer le routeur sans fil près d'un téléphone sans fil 2,4 GHz.

2. Éviter les obstacles et les interférences

Éviter de placer le routeur sans fil près d'un appareil susceptible d'émettre des parasites radio, comme un four à micro-ondes. D'autres objets qui peuvent empêcher la communication sans fil sont les suivants :

- Réfrigérateur
- Lave-linge ou sèche-linge
- Armoire métallique
- Grand aquarium
- Fenêtre avec teinture anti-UV métallique

Si le signal sans fil semble faible à certains endroits, vérifier qu'aucun de ces objets ne peut faire obstruction au signal entre les ordinateurs et le routeur sans fil.

3. Emplacement des téléphones sans fil

Si les performances du réseau sans fil sont toujours affectées malgré les solutions susmentionnées et si un téléphone sans fil se trouve à proximité :

- Éloigner les téléphones sans fil du routeur sans fil ainsi que des ordinateurs sans fil.
- Débrancher et retirer la batterie de tout téléphone sans fil fonctionnant sur la bande de 2,4 GHz (consulter la documentation du fabricant). Si cela résout le problème, il est possible que le téléphone interfère avec les signaux du réseau sans fil.
- Si le téléphone prend en charge la sélection du canal, modifier le canal du téléphone en choisissant le canal le plus éloigné possible du canal du réseau sans fil. Par exemple, choisir le canal 1 pour le téléphone et sélectionner le canal 11 pour le routeur sans fil (les canaux disponibles varient en fonction de la région). Voir le guide de l'utilisateur du téléphone pour des instructions détaillées.
- Le cas échéant, envisager de remplacer le téléphone sans fil par un téléphone sans fil 900 MHz ou 5 GHz.

4. Choisir le canal le moins « fréquenté » pour le réseau sans fil

Dans les endroits où les domiciles ou les bureaux sont rapprochés, tels que les appartements et les immeubles à bureaux, il se peut que d'autres réseaux sans fil à proximité créent un conflit avec celui-ci. Utiliser la fonction d'analyse de site de l'utilitaire de réseau sans fil pour localiser les autres réseaux sans fil et choisir pour le routeur et les ordinateurs sans fil un canal aussi éloigné que possible du canal utilisé par ces autres réseaux.

Essayer plusieurs canaux parmi ceux disponibles afin de déterminer la connexion la plus claire et éviter les interférences de la part de téléphones sans fil ou d'autres dispositifs sans fil se trouvant dans le voisinage.

Ces solutions devraient permettre d'obtenir une zone de couverture maximale avec le routeur. S'il est nécessaire d'étendre davantage la zone de couverture, Dynex suggère le Point d'accès/Module d'extension de portée sans fil G de Dynex.

5. Connexions sécurisées, VPN et AOL

Les connexions sécurisées requièrent généralement un nom d'utilisateur et un mot de passe, et sont utilisées là où la sécurité revêt une grande importance. Parmi les connexions sécurisées figurent :

- Les connexions de type Virtual Private Network (VPN – réseau privé virtuel), souvent utilisées pour accéder à distance à un réseau d'entreprise.
- Le programme « Bring Your Own Access » d'America Online (AOL), qui permet d'utiliser AOL via une connexion à haut débit (DSL ou câble) offerte par un autre fournisseur de service Internet.
- La plupart des sites Web offrant des services bancaires en ligne.
- De nombreux sites Web commerciaux qui requièrent un nom d'utilisateur et un mot de passe afin d'accéder au compte Connexions sécurisées peuvent être interrompus par la configuration de la gestion de l'alimentation d'un ordinateur, l'amenant à se mettre en « pause ». La solution la plus simple face à cette situation est de se reconnecter en lançant de nouveau le logiciel de VPN ou d'AOL ou en se reconnectant au site Web sécurisé.

Une autre solution consiste à modifier les paramètres de gestion de l'alimentation afin que l'ordinateur ne soit plus mis en pause, toutefois cela peut ne pas être approprié pour les ordinateurs portatifs. Pour modifier les paramètres de gestion de l'alimentation sous Windows, voir la rubrique **Power Options** (Options d'alimentation), dans le **Control Panel** (Panneau de configuration).

Si les difficultés ayant trait aux connexions sécurisées, aux VPN et à AOL persistent, lire les paragraphes qui précèdent afin de s'assurer d'avoir tenté les solutions proposées.

Problème : Le CD d'installation ne démarre pas automatiquement.

Solution : Si le CD ne lance pas automatiquement l'Assistant Installation facile, il se peut qu'un autre programme utilisé par l'ordinateur interfère avec le lecteur de CD.

1. Si l'écran de l'Assistant Installation facile ne s'affiche pas au bout de 15 à 20 secondes, ouvrir le lecteur de CD en double-cliquant sur l'icône **My Computer** (Poste de travail) qui se trouve sur le bureau.

2. Ensuite, double-cliquer sur le lecteur de CD dans lequel se trouve le CD de l'Assistant Installation facile.

3. L'Assistant Installation facile devrait démarrer dans les secondes qui suivent. Si une fenêtre affichant le contenu du CD apparaît, double-cliquer sur **EasyInstall.exe**.

4. Si l'Assistant Installation facile ne démarre toujours pas, consulter la section « Configuration manuelle des paramètres réseau » à la page 109 pour une autre méthode de configuration.

Problème : L'Assistant Installation facile ne peut trouver le routeur.

Solution : Si l'Assistant Installation facile est incapable de trouver le routeur pendant le processus d'installation, vérifier les points suivants :

1. Si l'Assistant Installation facile est incapable de trouver le routeur pendant le processus d'installation, il est possible qu'un logiciel pare-feu d'un tiers soit installé sur l'ordinateur qui tente d'accéder à l'Internet. Ces logiciels pare-feu comprennent ZoneAlarm, BlackICE 5 PC Protection, McAfee Personal Firewall et Norton Personal Firewall.

Si un logiciel pare-feu se trouve sur l'ordinateur, veiller à ce qu'il soit correctement configuré. Il est possible de déterminer si le logiciel pare-feu empêche l'accès à l'Internet en le désactivant de façon temporaire. Si l'Internet fonctionne normalement alors que le pare-feu est désactivé, il faudra modifier les paramètres du pare-feu avant de l'activer de nouveau.

Consulter les instructions fournies par l'éditeur du logiciel pare-feu afin de configurer celui-ci pour permettre l'accès à l'Internet.

2. Débrancher l'adaptateur CA du routeur pendant 10 secondes, puis le rebrancher au routeur. Veiller à ce que le voyant d'alimentation du routeur soit allumé en vert et ne clignote pas. Si tel n'est pas le cas, vérifier que l'adaptateur CA est bien connecté au routeur et branché sur une prise murale.

3. Vérifier qu'un câble (utiliser le câble fourni avec le routeur) est branché entre (1) le port réseau (Ethernet) situé à l'arrière de l'ordinateur et (2) l'un des ports LAN, numérotés de 1 à 4 et situés à l'arrière du routeur.

***Remarque** : L'ordinateur ne doit PAS être branché sur le port « Internet/WAN » à l'arrière du routeur.*

4. Éteindre et redémarrer l'ordinateur, puis relancer l'Assistant Installation facile.

Si l'Assistant Installation facile est toujours incapable de trouver le routeur, consulter la section « Configuration manuelle des paramètres réseau » à la page 109 pour une autre méthode de configuration.

Problème : L'Assistant Installation facile ne peut connecter le routeur à l'Internet.

Solution : Si l'Assistant Installation facile est incapable de connecter le routeur à l'Internet, vérifier les points suivants :

1. Utiliser les suggestions de dépannage de l'Assistant Installation facile. Si l'écran de dépannage ne s'affiche pas automatiquement, cliquer sur la touche **Troubleshoot** (Dépannage) située dans le coin inférieur droit de la fenêtre de l'Assistant Installation facile.

2. Si le FSI utilise un nom d'utilisateur et un mot de passe, veiller à ce qu'ils soient correctement saisis. Certains noms d'utilisateurs exigent que le domaine du FSI figure à la fin du nom. Par exemple : **MonNom@MonFSI.com**. Il peut être nécessaire que la partie **@MonFSI.com** du nom d'utilisateur accompagne le nom d'utilisateur.

Si l'accès à l'Internet continue à poser problème, se reporter à « Configuration manuelle des paramètres réseau » à la page 109 pour une autre méthode de configuration.

Problème : L'Assistant Installation facile a terminé l'installation, mais le navigateur Web ne fonctionne pas.

- OU -

Pas de connexion à l'Internet. Le témoin WAN du routeur est éteint et le témoin Connected (Connecté) clignote.

Solution : S'il n'est pas possible d'établir une connexion Internet, si le témoin WAN est éteint et si le témoin Connected (Connecté) clignote, il se peut que le modem et le routeur ne soient pas correctement connectés.

1. Vérifier que le câble réseau entre le modem et le routeur est bien branché. À cette fin, Dynex recommande vivement l'utilisation du câble fourni avec le modem câble ou DSL. L'une des extrémités du câble doit être branchée sur le port Internet/WAN du routeur et l'autre extrémité sur le port réseau du modem.

2. Débrancher le modem câble ou DSL de son alimentation électrique pendant trois minutes. Après trois minutes, rebrancher le modem sur son alimentation électrique. Cette mesure peut aider le modem à reconnaître le routeur.

3. Débrancher l'alimentation du routeur, attendre 10 secondes, puis la rebrancher. Cette mesure permettra au routeur de tenter de nouveau d'entrer en communication avec le modem.

4. Essayer d'éteindre et de redémarrer l'ordinateur.

Problème : L'Assistant Installation facile a terminé l'installation, mais le navigateur Web ne fonctionne pas.

- OU -

Pas de connexion à l'Internet. Le témoin WAN du routeur est allumé et le témoin Connected (Connecté) clignote.

Solution : S'il n'est pas possible d'établir une connexion Internet, si le témoin WAN est allumé et si le témoin Connected (Connecté) clignote, il se peut que le type de connexion ne soit pas compatible avec le type de connexion offert par le FSI.

- S'il s'agit d'une connexion à *adresse IP statique*, le FSI doit attribuer à l'utilisateur l'adresse IP, le masque de sous-réseau ainsi que l'adresse de la passerelle. Voir « Autre méthode de configuration » à la page 77 pour de plus amples informations sur ce paramètre.
- Il faudra peut-être configurer le routeur selon des paramètres spécifiques au FSI. Pour effectuer une recherche dans notre base de connaissances traitant de problèmes liés aux FSI, consulter :
  http://www.dynexsupport.com et entrer « ISP ».

Si la connexion à l'Internet ne peut toujours pas ce faire après avoir vérifié ces paramètres, contacter l'assistance technique de Dynex.

Problème : L'Assistant Installation facile a terminé l'installation, mais le navigateur Web ne fonctionne pas.

- OU -

Pas de connexion à l'Internet. Le témoin WAN du routeur clignote et le témoin Connected (Connecté) est allumé en continu.

Solution : Si le témoin WAN clignote et que le témoin Connected (Connecté) est allumé en continu, mais qu'il n'est pas possible d'établir une connexion Internet, il est possible qu'un logiciel pare-feu d'un tiers soit installé sur l'ordinateur qui tente d'accéder à l'Internet. Ces logiciels pare-feu comprennent ZoneAlarm, BlackICE 5 PC Protection, McAfee Personal Firewall et Norton Personal Firewall.

Si un logiciel pare-feu se trouve sur l'ordinateur, veiller à ce qu'il soit correctement configuré. Il est possible de déterminer si le logiciel pare-feu empêche l'accès à l'Internet en le désactivant de façon temporaire. Si l'Internet fonctionne normalement alors que le pare-feu est désactivé, il faudra modifier les paramètres du pare-feu avant de l'activer de nouveau.

Consulter les instructions fournies par l'éditeur du logiciel pare-feu afin de configurer celui-ci pour permettre l'accès à l'Internet.

Problème : Impossible de se connecter sans fil à l'Internet.

Solution : S'il n'est pas possible d'établir une connexion Internet à partir d'un ordinateur sans fil, procéder comme suit :

1. Regarder les témoins sur le routeur. Ils devraient être comme suit :
   - Le témoin d'alimentation devrait être allumé.
   - Le témoin de connexion devrait être allumé et ne pas clignoter.
   - Le témoin WAN devrait être allumé ou clignoter.

2. Ouvrir le logiciel de l'utilitaire sans fil en cliquant sur l'icône dans la barre d'état, dans le coin inférieur droit de l'écran. Si une carte ou un adaptateur sans fil Dynex est également utilisé avec ce routeur, l'icône de la barre de tâches devrait ressembler à celle-ci

 (elle peut être rouge ou verte) :

3. La fenêtre qui s'ouvre dépend du modèle de carte réseau dont il s'agit. Toutefois, n'importe quel utilitaire doit posséder une liste des réseaux disponibles (**Available Networks**), présentant les réseaux sans fil auxquels il est possible de se connecter.

Est-ce que le nom du réseau sans fil apparaît dans la liste des résultats?

Oui, le nom du réseau apparaît – aller à la section intitulée « Impossible de se connecter sans fil à l'Internet, mais le nom du réseau figure dans la liste ».

Non, le nom du réseau n'apparaît pas – aller à la section intitulée « Impossible de se connecter sans fil à l'Internet, et le nom du réseau ne figure pas dans la liste ».

Problème : Impossible de se connecter sans fil à l'Internet, mais le nom du réseau figure dans la liste.

Solution : Si le nom du réseau figure dans la liste des réseaux disponibles (**Available Networks**), suivre les étapes suivantes pour se connecter sans fil :

1. Cliquer sur le nom de réseau correct dans la liste **Available Networks** (Réseaux disponibles).

2. Si des fonctions de sécurité (cryptage) sont activées pour le réseau, il faut entrer la clé du réseau. Pour plus d'informations en ce qui concerne la sécurité, voir « Sécurisation du réseau Wi-FiMD » à la page 89.

3. Au bout de quelques secondes, l'icône de la barre d'état, dans le coin inférieur gauche de l'écran, devrait devenir verte, indiquant une connexion réussie au réseau.

Problème : Impossible de se connecter sans fil à l'Internet, et le nom du réseau ne figure pas dans la liste.

Solution : Si le nom de réseau correct ne figure pas sous **Available Networks** (Réseaux disponibles) dans l'utilitaire de configuration sans fil, essayer de résoudre le problème de la manière suivante :

1. Déplacer temporairement l'ordinateur, si possible, à une distance de 2 à 3 mètres du routeur. Fermer l'utilitaire de configuration sans fil et le rouvrir. Si le nom de réseau correct s'affiche maintenant sous **Available Networks** (Réseaux disponibles), il peut s'agir d'un problème de portée ou d'interférence. Voir les suggestions proposées dans la section « Emplacement du routeur pour des performances optimales », à la page 114.

2. En utilisant un ordinateur qui est connecté au routeur au moyen d'un câble réseau (et non sans fil), vérifier que **Broadcast SSID** (Diffuser SSID) est activé. Ce paramètre se trouve sur la page de configuration *Channel and SSID* (Canal et SSID) du routeur sans fil.

Problème : Le réseau sans fil fonctionne de façon irrégulière.

Le transfert de données est parfois très lent.

Le signal est faible.

Il est difficile d'établir et/ou de maintenir une connexion de type VPN (Virtual Private Network).

Solution : La technologie sans fil est basée sur des ondes radio, ce qui signifie que les performances de connectivité et de débit entre les dispositifs diminuent à mesure que la distance entre les dispositifs augmente. D'autres facteurs qui provoquent une dégradation du signal (le métal est généralement le premier responsable) sont les obstructions telles que des murs et des appareils métalliques. Par conséquent, la portée normale des dispositifs sans fil, en intérieur, sera comprise entre 30 et 60 mètres. Noter également que la vitesse de connexion peut diminuer à mesure que l'on s'éloigne du routeur ou du point d'accès.

Afin de déterminer si des problèmes de connexion sans fil sont liés à la portée, Dynex suggère de déplacer temporairement l'ordinateur, si possible, à une distance de 2 à 3 mètres du routeur.

Modification du canal sans fil

Suivant le niveau local des communications sans fil et des interférences, il est possible qu'un changement de canal sans fil du réseau donne lieu à une amélioration des performances et de la fiabilité. Le canal sur lequel le routeur est réglé par défaut lorsqu'il est livré est le canal 11. Il est possible de choisir plusieurs autres canaux selon la région (voir « Modification du canal sans fil » à la page 88 pour les instructions concernant le choix d'un autre canal).

Limitation du débit de transmission sans fil

La limitation du débit de transmission sans fil peut améliorer la portée maximale sans fil et la stabilité des connexions. La plupart des cartes sans fil offrent la possibilité de limiter le débit de transmission. Pour modifier cette propriété, accéder au *Control Panel* (Panneau de configuration) de Windows, ouvrir **Network Connections** (Connexions réseau) et double-cliquer sur la connexion de la carte sans fil. Dans la boîte de dialogue *Properties* (Propriétés), sélectionner la touche **Configure** (Configurer) sous l'onglet **General** (Généralités) (les utilisateurs de Windows 98 devront sélectionner la carte sans fil dans la zone de liste, puis cliquer sur **Properties** [Propriétés]), puis choisir l'onglet **Advanced** (Avancé) et sélectionner la propriété de débit. Les cartes clients sans fil sont généralement configurées pour ajuster automatiquement le débit de transmission sans fil, mais cela peut provoquer des déconnexions périodiques lorsque le signal sans fil est trop faible ; en règle générale, les débits de transmission plus lents sont plus stables. Essayer différents débits de connexion jusqu'à trouver le meilleur pour l'environnement existant ; noter que tous les débits de transmission disponibles devraient être acceptables pour naviguer sur Internet. Pour plus d'informations, consulter le manuel de l'utilisateur de la carte sans fil.

Problème : Comment étendre la portée du réseau sans fil?

Solution : Dynex recommande l'utilisation d'un des produits suivants pour étendre la portée du réseau sans fil dans des maisons ou bureaux de surface importante :

- Point d'accès sans fil : Un point d'accès sans fil peut véritablement doubler la portée du réseau sans fil. Un point d'accès se positionne généralement dans une zone non couverte par le routeur sans fil G amélioré et est relié au routeur grâce soit à un câble Ethernet, soit au réseau de distribution électrique de la maison à l'aide de deux adaptateurs Ethernet pour câbles électriques.

Problème : Il est difficile de configurer la sécurité WEP (Wired Equivalent Privacy) sur un routeur sans fil Dynex ou un point d'accès Dynex.

Solution :

1. Se connecter au routeur ou au point d'accès sans fil.

Ouvrir le navigateur Web et entrer l'adresse IP du routeur ou du point d'accès sans fil. (L'adresse par défaut du routeur est 192.168.2.1 et celle du point d'accès est 192.168.2.254.) Se connecter au router en appuyant sur la touche **Login** (Connexion), située dans le coin supérieur droit de l'écran. Un message demande à l'utilisateur d'entrer son mot de passe. Si aucun mot de passe n'a été défini, laisser ce champ vide, puis cliquer sur **Submit** (Soumettre).

Cliquer sur l'onglet **Wireless** (Sans fil) sur la gauche de l'écran. Sélectionner l'onglet **Encryption** (Cryptage) ou **Security** (Sécurité) pour accéder à la page des paramètres de sécurité.

2. Sélectionner **128-bit WEP** (WEP 128 bits) dans la liste.

3. Après avoir sélectionné le mode de cryptage WEP, entrer manuellement la clé WEP hexadécimale ou taper un mot de passe dans le champ **Passphrase** (Mot de passe), puis cliquer sur**Generate** (Générer) pour créer une clé WEP à partir du mot de passe. Cliquer sur **Apply Changes** (Appliquer les modifications) pour terminer. Il faut maintenant configurer tous les clients pour qu'ils correspondent à ces paramètres. Une clé hexadécimale est une combinaison de chiffres et de lettres de A à F et de 0 à 9. Pour le mode WEP 128 bits, il faut entrer 26 caractères hexadécimaux.

Par exemple : C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = clé 128 bits

4. Cliquer sur **Apply Changes** (Appliquer les modifications) pour terminer. Le cryptage est maintenant configuré au niveau du routeur sans fil. Chacun des ordinateurs du réseau sans fil doit maintenant être configuré avec les mêmes paramètres de sécurité.

***Attention** : Si le routeur sans fil ou le point d'accès est configuré à partir d'un ordinateur doté d'un client sans fil, il faut s'assurer que la sécurité est activée pour ce client sans fil. Sinon, la connexion sans fil sera perdue.*

***Remarque pour les utilisateurs de Mac :** Les produits AirPort d'Apple de première génération ne prennent en charge que le cryptage sur 64 bits. Les produits Apple AirPort 2 prennent en charge le cryptage sur 64 bits ou 128 bits. Vérifier le produit Apple AirPort pour savoir quelle est la version utilisée. S'il n'est pas possible de configurer le réseau avec le cryptage sur 128 bits, essayer le cryptage sur 64 bits.*

Problème : Il est difficile de configurer la sécurité WEP (Wired Equivalent Privacy) sur une carte client Dynex (carte ou adaptateur de réseau sans fil).

Solution : La carte client doit utiliser la même clé que le routeur sans fil G amélioré ou le point d'accès. Par exemple, si le routeur sans fil ou point d'accès utilise la clé 00112233445566778899AABBCC, la carte client doit être paramétrée de façon à utiliser cette même clé.

1. Double-cliquer sur l'icône **Signal Indicator** (Indicateur de signal) pour afficher l'écran *Wireless Network Utility* (Utilitaire réseau sans fil). Cliquer sur **Advanced** (Avancé) pour afficher et configurer d'autres options de la carte client. L'utilitaire LAN sans fil s'affiche. Cet utilitaire permet de gérer toutes les fonctions avancées de la carte client.

2. Cliquer sur l'onglet **Wireless Network Properties** (Propriétés du réseau sans fil), puis sélectionner un nom de réseau dans la liste **Available networks** (Réseaux disponibles) et cliquer sur **Properties** (Propriétés).

3. Sélectionner **WEP** dans la liste **Data Encryption** (Cryptage de données).

4. Veiller à ce que la case **The key is provided for me automatically** (La clé est fournie automatiquement) qui se trouve en bas ne soit pas cochée. Si cet ordinateur est utilisé pour se connecter à un réseau d'entreprise, consulter l'administrateur réseau afin de savoir si cette case doit être cochée.

5. Entrer la clé WEP dans la boîte **Network Key** (Clé de réseau).

> ***Important** : Une clé WEP est une combinaison de chiffres et de lettres de A à F et de 0 à 7. Pour le mode WEP 128 bits, il faut entrer 26 clés. Cette clé de réseau doit être identique à la clé assignée au routeur sans fil G amélioré ou au point d'accès.*
>
> *Par exemple : C3030FAF4BB2C3D44BC3D4E7E4 = clé 128 bits*

6. Cliquer sur **OK**, puis sur **Apply** (Appliquer) pour enregistrer les paramètres.

Si la carte client sans fil utilisée n'est PAS une carte Dynex, consulter le manuel de l'utilisateur du fabricant de cette carte client sans fil.

Problème : Est-ce que les produits Dynex prennent en charge le WPA?

Solution :

> ***Remarque** : Pour utiliser la sécurité WPA, tous les clients doivent être mis à jour avec les logiciels et les pilotes qui la prennent en charge. À la date de publication de ce manuel, un correctif de sécurité est disponible pour téléchargement gratuit, auprès de Microsoft. Ce correctif ne fonctionne qu'avec Windows XP.*

Télécharger le correctif sur ce site :

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

Il faudra également télécharger sur le site d'assistance technique de Dynex le pilote le plus récent pour la carte réseau sans fil 802.11g de Dynex pour ordinateur de bureau ou portatif. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge. Le correctif de Microsoft ne prend en charge que les dispositifs avec pilotes compatibles WPA, tels que les produits 802.11g de Dynex.

Télécharger les pilotes les plus récents sur le site http://www.dynexproducts.com.

Problème : Il est difficile de configurer la sécurité WPA (Wi-Fi Protected Access) sur un routeur sans fil Dynex ou un point d'accès Dynex pour un réseau familial.

Solution :

1. Sélectionner **WPA-PSK (no server)** [WPA-PSK (pas de serveur)] dans la liste **Security Mode** (Mode de sécurité).

2. Sélectionner **TKIP** ou **AES** pour **Encryption Technique** (Technique de cryptage). Ce paramètre devra être identique sur les clients qui seront configurés.

3. Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres, des symboles ou des espaces. Cette même clé doit être utilisée sur tous les clients qui seront configurés. Par exemple, la clé pré-partagée peut ressembler à : « Clé réseau de la famille Dupont ».

4. Cliquer sur **Apply Changes** (Appliquer les modifications) pour terminer. Il faut maintenant configurer tous les clients pour qu'ils correspondent à ces paramètres.

Problème : Il est difficile de configurer la sécurité WPA (Wi-Fi Protected Access) sur une carte client Dynex (carte ou adaptateur réseau sans fil) pour un réseau familial.

Solution : Les clients doivent utiliser la même clé que le routeur sans fil G amélioré ou le point d'accès. Par exemple, si le routeur sans fil G amélioré ou le point d'accès est configuré avec la clé « Clé réseau de la famille Dupont », tous les clients doivent utiliser cette même clé.

1. Double-cliquer sur l'icône **Signal Indicator** (Indicateur de signal) pour afficher l'écran *Wireless Network Utility* (Utilitaire réseau sans fil).

2. Cliquer sur **Advanced** (Avancé). L'utilitaire LAN sans fil de Dynex s'affiche. Cet utilitaire permet de gérer toutes les fonctions avancées de la carte client de Dynex.

3. Cliquer sur l'onglet **Wireless Network Properties** (Propriétés du réseau sans fil), puis sélectionner un nom de réseau dans la liste **Available networks** (Réseaux disponibles) et cliquer sur **Properties** (Propriétés). La page *Properties* (Propriétés) s'affiche.

4. Sélectionner **WPA-PSK (no server)** [WPA-PSK (pas de serveur)] dans la liste **Network Authentication** (Authentification de réseau).

5. Entrer la clé WPA dans la boîte **Network Key** (Clé de réseau).

> ***Important** : Une clé WPA-PSK est une combinaison de chiffres et de lettres de A à Z et de 0 à 9. Pour le mode WPA-PSK, il est possible d'entrer de huit à 63 caractères. Cette clé de réseau doit être identique à la clé assignée au routeur sans fil G amélioré ou au point d'accès.*

6. Cliquer sur **OK**, puis sur **Apply** (Appliquer) pour enregistrer les paramètres.

Problème : Il est difficile de configurer la sécurité WPA (Wi-Fi Protected Access) sur une carte client Dynex (carte ou adaptateur réseau sans fil) pour une entreprise.

Solution :

1. Double-cliquer sur l'icône **Signal Indicator** (Indicateur de signal). L'écran *Wireless Network Utility* (Utilitaire réseau sans fil) s'affiche.

2. Cliquer sur **Advanced** (Avancé). L'utilitaire LAN sans fil de Dynex s'affiche. Cet utilitaire permet de gérer toutes les fonctions avancées de la carte client de Dynex.

3. Cliquer sur l'onglet **Wireless Network Properties** (Propriétés du réseau sans fil), puis sélectionner un nom de réseau dans la liste **Available networks** (Réseaux disponibles) et cliquer sur **Properties** (Propriétés). La page *Properties* (Propriétés) s'affiche.

4. Sélectionner **WPA** dans la liste **Network Authentication** (Authentification de réseau).

5. Cliquer sur l'onglet **Authentication** (Authentification), puis sélectionner les paramètres indiqués par l'administrateur réseau.

6. Cliquer sur **OK**, puis sur **Apply** (Appliquer) pour enregistrer les paramètres.

Problème : Il est difficile de configurer la sécurité WPA (Wi-Fi Protected Access) et la carte client utilisée n'est PAS une carte Dynex pour un réseau familial.

Solution : Si la carte réseau sans fil WPA pour ordinateur de bureau ou portatif n'est PAS une carte Dynex et qu'elle n'est pas équipée d'un logiciel compatible WPA, un fichier de Microsoft, appelé « Windows XP Support Patch for Wireless Protected Access » peut être téléchargé gratuitement :

http://www.microsoft.com/downloads/search.aspx?displaylang=en

> ***Remarque** : Le fichier mis à disposition par Microsoft fonctionne uniquement avec Windows XP. À l'heure actuelle, les autres systèmes d'exploitation ne sont pas pris en charge. Il faudra également vérifier que le fabricant de la carte sans fil prend en charge le WPA et que le pilote le plus récent a été téléchargé à partir de son site Web et installé.*

Systèmes d'exploitation pris en charge :

- Windows XP Professionnel
- Windows XP Édition Familiale

Pour activer le WPA-PSK (pas de serveur) :

1. Sous Windows XP, cliquer sur **Start** (Démarrer), **Control Panel** (Panneau de configuration) et **Network Connections** (Connexions réseau).

2. Cliquer à l'aide du bouton droit de la souris sur l'onglet **Wireless Networks** (Réseaux sans fil). L'écran *Wireless Network Connection Properties* (Propriétés de la connexion au réseau sans fil) s'affiche. Vérifier que la case **Use Windows to configure my wireless network settings** (Utiliser Windows pour configurer mes paramètres réseau sans fil) est cochée.

3. Sous l'onglet **Wireless Networks** (Réseaux sans fil), cliquer sur **Configure** (Configurer). L'écran *Client Card Properties* (Propriétés de la carte client) s'affiche.

4. Pour un utilisateur de réseau familial ou de petite entreprise, sélectionner **WPA-PSK** sous **Network Administration** (Administration de réseau).

5. Sélectionner **TKIP** ou **AES** dans la liste **Data Encryption** (Cryptage de données). Ce paramètre devra être identique à celui configuré sur le routeur sans fil G amélioré ou le point d'accès.

6. Entrer la clé de cryptage dans la boîte **Network Key** (Clé de réseau).

Important : *Entrer la clé pré-partagée. Elle peut contenir de 8 à 63 caractères, qui peuvent être des lettres, des chiffres ou des symboles. Cette même clé doit être utilisée sur tous les clients qui seront configurés.*

7. Cliquer sur **OK** pour enregistrer les modifications.

Quelle est la différence entre les normes 802.11b, 802.11g, 802.11a et 802.11n ?

À l'heure actuelle, il existe quatre normes de réseaux sans fil, qui transmettent des données à des vitesses maximales très différentes. Chaque norme est basée sur la désignation utilisée pour la certification des normes réseaux. La norme de réseau sans fil la plus courante, 802.11b, transmet des informations à 11 Mbps; 802.11a et 802.11g fonctionnent à 54 Mbps; et Pre-N fonctionne à 108 Mbps. La version 802.11n offre des vitesses supérieures à 802.11g, ainsi qu'une zone de couverture sans fil jusqu'à deux fois plus étendue. Consulter le tableau suivant pour de plus amples informations.

Technologie sans fil	802.11b	802.11g	802.11a	802.11n
Vitesse	11 Mbps	54 Mbps	54 Mbps	600 % plus rapide que la norme 802.11g*
Fréquence	Les appareils domestiques courants tels que les téléphones sans fil et les fours à micro-ondes peuvent interférer avec la fréquence sans licence 2,4 GHz.	Les appareils domestiques courants tels que les téléphones sans fil et les fours à micro-ondes peuvent interférer avec la fréquence sans licence 2,4 GHz.	5 GHz – fréquence peut encombrée	Les appareils domestiques courants tels que les téléphones sans fil et les fours à micro-ondes peuvent interférer avec la fréquence sans licence 2,4 GHz.
Compatibilité	Compatible avec 802.11g	Compatible avec 802.11b	Incompatible avec 802.11b ou 802.11g	Compatible avec 802.11g ou 802.11b
Couverture*	Dépend des interférences - généralement de 30 à 60 mètres (100 à 200 pi) à l'intérieur	Dépend des interférences - généralement de 30 à 60 mètres (100 à 200 pi) à l'intérieur	La portée des interférences est en général de 15 à 30 mètres (50 à 100 pi)	Couverture supérieure de 800 % par rapport à la norme 802.11g*
Avantage	Technologie ancienne éprouvée	Largement répandue pour le partage d'une liaison Internet	Moins d'interférences – parfaite pour les applications multimédias	Technologie de pointe – la meilleure couverture et le meilleur débit

** La distance et la vitesse de connexion varient en fonction de l'environnement du réseau.*

Avis juridiques

Déclaration de la FCC

DÉCLARATION DE CONFORMITÉ AU RÈGLEMENT DE LA FCC CONCERNANT LA COMPATIBILITÉ ÉLECTROMAGNÉTIQUE

Nous, Dynex Corporation, 7601 Penn Avenue South, Richfield, Minnesota, États-Unis, déclarons sous notre seule responsabilité que le produit concerné par cette déclaration, DX-WEGRTR, est conforme à la section 15 du règlement de la FCC. Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas provoquer d'interférences préjudiciables, et (2) il doit accepter toute interférence reçue, y compris celles risquant d'engendrer un fonctionnement indésirable.

Attention : Exposition à des rayonnements radioélectriques.

L'émission de rayonnements de ce dispositif est très en dessous des limites d'exposition imposées par la FCC en la matière. Toutefois, le dispositif doit être utilisé de façon à minimiser le contact avec l'homme pendant son fonctionnement normal. En cas de connexion d'une antenne externe au dispositif, celle-ci devra être placée de façon à minimiser le contact avec l'homme pendant son fonctionnement normal. Afin d'éviter le risque de dépasser les limites d'exposition imposées par la FCC en matière de rayonnements radioélectriques, la distance entre un être humain et l'antenne ne devra pas être inférieure à 20 cm (8 pouces) pendant son fonctionnement normal.

Avertissement de la FCC

Tous changements ou toutes modifications qui ne seraient pas expressément approuvés par les responsables de l'application du règlement de la FCC pourraient rendre nul le droit de l'utilisateur d'utiliser cet équipement.

Certification relative à la sécurité du DHHS et de la FDA

Ce produit a été fabriqué et testé pour satisfaire aux normes de sécurité de la FCC, aux exigences et règles de conformité du Ministère de la santé des États-Unis (U.S. Department of Health and Human Services), ainsi qu'aux normes d'irradiation 21 CFR, section de chapitre J de la FDA.

Déclaration NMB-003 du Canada

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

FCC article 15

Cet appareil est conforme à l'article 15 du règlement de la FCC. Son utilisation est soumise aux deux conditions suivantes : (1) cet appareil ne doit pas provoquer d'interférences préjudiciables, et (2) il doit accepter toute interférence reçue, y compris celles risquant d'engendrer un fonctionnement indésirable.

Cet équipement a été mis à l'essai et déclaré conforme aux limites prévues pour un appareil numérique de classe B, définies dans la section 15 du règlement de la FCC. Ces limites ont été établies pour fournir une protection raisonnable contre les interférences préjudiciables lors d'une installation résidentielle. Cet équipement génère, utilise et diffuse des ondes radio et, s'il n'est pas installé et utilisé conformément aux instructions dont il fait l'objet, il peut provoquer des interférences préjudiciables aux communications radio. Cependant, il n'est pas possible de garantir qu'aucune interférence ne se produira pour une installation particulière. Si cet équipement produit des interférences préjudiciables lors de réceptions radio ou télévisées, qui peuvent être détectées en éteignant puis en rallumant l'appareil, essayer de corriger l'interférence au moyen de l'une ou de plusieurs des mesures suivantes :

- Réorienter ou déplacer l'antenne réceptrice.
- Augmenter la distance entre l'équipement et le récepteur.
- Brancher l'équipement sur la prise électrique d'un circuit différent de celui auquel le récepteur est relié.
- Contacter le revendeur ou un technicien qualifié pour toute assistance.

Déclaration RSS 310

Pour éviter que les interférences radio éventuelles affectent d'autres utilisateurs, le type d'antenne et son gain doivent être choisis afin que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure aux limites permises, permettant des communications parfaites.

Garantie limitée d'un an

Dynex Products (« Dynex ») garantit au premier acheteur de ce **DX-WEGRTR** neuf (« Produit »), qu'il est exempt de vices de fabrication et de main-d'œuvre à l'origine, pour une période d'un (1) an à partir de la date d'achat du Produit (« Période de garantie »). Ce Produit doit avoir été acheté chez un revendeur agréé des produits de la marque Dynex et emballé avec cette déclaration de garantie. Cette garantie ne couvre pas les Produits remis à neuf. Les conditions de la présente garantie s'appliquent à tout Produit pour lequel Dynex est notifié, pendant la Période de garantie, d'un vice couvert par cette garantie qui nécessite une réparation.

Quelle est la durée de la couverture?

La Période de garantie dure 1 an (365 jours) à compter de la date d'achat de ce Produit. La date d'achat est imprimée sur le reçu fourni avec le produit.

Que couvre cette garantie?

Pendant la Période de garantie, si un vice de matériau ou de main-d'œuvre d'origine est détecté sur le Produit par un service de réparation agréé par Dynex ou le personnel du magasin, Dynex (à sa seule discrétion) : (1) réparera le Produit en utilisant des pièces détachées neuves ou remises à neuf; ou (2) remplacera le Produit par un produit ou des pièces neuves ou remises à neuf de qualité comparable. Les produits et pièces remplacés au titre de cette garantie deviennent la propriété de Dynex et ne sont pas retournés à l'acheteur. Si les Produits ou pièces nécessitent une réparation après l'expiration de la Période de garantie, l'acheteur devra payer tous les frais de main-d'œuvre et les pièces. Cette garantie reste en vigueur tant que l'acheteur reste propriétaire du Produit Dynex pendant la Période de garantie. La garantie prend fin si le Produit est revendu ou transféré d'une quelconque façon que ce soit à tout autre propriétaire.

Comment obtenir une réparation sous garantie?

Si le Produit a été acheté chez un détaillant, le rapporter accompagné du reçu original chez ce détaillant. Prendre soin de remettre le Produit dans son emballage d'origine ou dans un emballage qui procure la même qualité de protection que celui d'origine. Si le Produit a été acheté en ligne, l'expédier accompagné du reçu original à l'adresse indiquée sur le site Web. Prendre soin de remettre le Produit dans son emballage d'origine ou dans un emballage qui procure la même qualité de protection que celui d'origine.

Pour obtenir le service de la garantie à domicile pour un téléviseur avec écran de 25 po ou plus, appeler le 1-888-BESTBUY. L'assistance technique établira un diagnostic et corrigera le problème au téléphone ou enverra un technicien agréé par Dynex pour la réparation à domicile.

Où cette garantie s'applique-t-elle?

Cette garantie ne s'applique qu'à l'acheteur original du Produit aux États-Unis et au Canada.

Ce qui n'est pas couvert par cette garantie limitée

La présente garantie ne couvre pas :

- la formation du client;
- Installation;
- les réglages de configuration;
- les dommages esthétiques;
- les dommages résultants de catastrophes naturelles telles que la foudre;
- les accidents;
- une utilisation inadaptée;
- une manipulation abusive;
- la négligence;
- une utilisation commerciale;
- la modification de tout ou partie du Produit;
- un écran plasma endommagé par les images fixes (sans mouvement) qui restent affichées pendant de longues périodes (rémanentes).

La présente garantie ne couvre pas non plus :

- les dommages ayant pour origine une utilisation ou une maintenance défectueuse;
- la connexion à une source électrique dont la tension est inadéquate;
- toute réparation effectuée par quiconque autre qu'un service de réparation agréé par Dynex pour la réparation du Produit;
- les produits vendus en l'état ou hors service;
- les consommables tels que les fusibles ou les piles;
- les produits dont le numéro de série usine a été altéré ou enlevé.

LA RÉPARATION OU LE REMPLACEMENT, TELS QU'OFFERTS PAR LA PRÉSENTE GARANTIE, CONSTITUENT LE SEUL RECOURS DE L'ACHETEUR. DYNEX NE SAURAIT ÊTRE TENU POUR RESPONSABLE DE DOMMAGES ACCESSOIRES OU CONSÉCUTIFS, RÉSULTANT DE L'INEXÉCUTION D'UNE GARANTIE EXPRESSE OU IMPLICITE SUR CE PRODUIT, Y COMPRIS , SANS S'Y LIMITER, LA PERTE DE DONNÉES, L'IMPOSSIBILITÉ D'UTILISER LE PRODUIT, L'INTERRUPTION D'ACTIVITÉ OU LA PERTE DE PROFITS. DYNEX PRODUCTS N'OCTROIE AUCUNE AUTRE GARANTIE EXPRESSE RELATIVE À CE PRODUIT; TOUTES LES GARANTIES EXPRESSES OU IMPLICITES POUR CE PRODUIT, Y COMPRIS MAIS SANS LIMITATION, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN BUT PARTICULIER, SONT LIMITÉES À LA PÉRIODE DE GARANTIE APPLICABLE TELLE QUE DÉCRITE CI-DESSUS ET AUCUNE GARANTIE EXPRESSE OU IMPLICITE, NE S'APPLIQUERA APRÈS LA PÉRIODE DE GARANTIE. CERTAINS ÉTATS ET PROVINCES NE RECONNAISSENT PAS LES LIMITATIONS DE LA DURÉE DE VALIDITÉ DES GARANTIES IMPLICITES. PAR CONSÉQUENT, LES LIMITATIONS SUSMENTIONNÉES PEUVENT NE PAS S'APPLIQUER À L'ACHETEUR ORIGINAL. LA PRÉSENTE GARANTIE DONNE À L'ACHETEUR DES GARANTIES JURIDIQUES SPÉCIFIQUES; IL PEUT AUSSI BÉNÉFICIER D'AUTRES GARANTIES QUI VARIENT D'UN ÉTAT OU D'UNE PROVINCE À L'AUTRE.

Pour contacter Dynex :

Pour le service à la clientèle, appeler le 1-800-305-2204
www.dynexproducts.com

Distribué par Best Buy Purchasing, LLC.
Dynex, 7601 Penn Avenue South, Richfield, Minnesota, U.S.A.

Enrutador inalámbrico G mejorado Dynex DX-WEGRTR

Contenido

Introducción

Gracias por comprar el enrutador inalámbrico G mejorado DX-WEGRTR de Dynex. Su fácil instalación y configuración le tendrán conectado a la red de forma inalámbrica en minutos. Asegúrese de leer esta Guía del Usuario en su totalidad, prestando especial atención a la sección titulada "Colocación de su enrutador para un rendimiento óptimo" en la página 182.

Los beneficios de una red de hogar

Su red de hogar le permitirá:

- Compartir una conexión a Internet de alta velocidad con todas las computadoras de su casa
- Compartir recursos, como archivos y discos duros, entre todas las computadoras conectadas en su hogar
- Compartir una única impresora con toda la familia
- Compartir documentos, música, videos e imágenes digitales
- Almacenar, recuperar y copiar archivos de una computadora a otra
- Participar en juegos en línea, consultar su correo electrónico y chatear de forma simultánea

Ventajas de una red inalámbrica

Estas son algunas de las ventajas de instalar una red inalámbrica Dynex:

- **Movilidad** – ya no necesitará dedicar una "sala de computadoras" – ahora podrá trabajar desde una computadora portátil o de escritorio conectada en red desde cualquier lugar que esté bajo su rango inalámbrico
- **Instalación sencilla** – El asistente de instalación sencilla de Dynex le permite realizar las configuraciones de manera cómoda
- **Flexibilidad** – instale y acceda a impresoras, computadoras y otros dispositivos de red desde cualquier punto de su hogar

- **Fácil ampliación** – la extensa gama de productos de interconexión en red de Dynex le permite ampliar su red para incluir dispositivos adicionales como impresoras y consolas de videojuegos
- **Sin necesidad de cableado** – podrá ahorrarse el gasto y las complicaciones de colocar cableado Ethernet por su hogar u oficina
- **Aceptación general en el sector** – elija entre una amplia gama de productos de interconexión en red compatibles

Características del producto

En pocos minutos podrá compartir su conexión a Internet y establecer una red entre sus computadoras. A continuación presentamos una lista de características que convierten su nuevo enrutador inalámbrico G mejorado de Dynex en la solución ideal para su red de oficina pequeña o del hogar.

Funciona con computadoras PC y Mac® – El enrutador soporta múltiples entornos de redes, incluyendo los sistemas operativos Mac OS®, X v10.x, Linux®, Windows® 2000, XP, Vista™ y otros. Todo lo que se necesita es un navegador de Internet y un adaptador de red que soporte TCP/IP (el idioma estándar de Internet).

Indicadores LED en el panel frontal – Los indicadores LED iluminados del panel frontal del enrutador indican qué funciones están activas. De un vistazo podrá saber si su enrutador se encuentra conectado a Internet. Esta característica elimina la necesidad de disponer de software avanzado y procedimientos de control de estado.

Interfaz avanzada de usuario a través de Web – Puede configurar las funciones avanzadas del enrutador fácilmente a través de su navegador de Web, sin necesidad de instalar software adicional en su computadora. No tiene que instalar discos y puede efectuar cambios y llevar a cabo funciones de configuración desde cualquier computadora de la red de forma rápida y sencilla.

Comparte dirección IP mediante NAT – Su enrutador utiliza el método de traducción de direcciones de red (NAT) para compartir la única dirección IP que le ha asignado su proveedor de servicios de Internet (ISP), evitando así el costo de agregar direcciones IP adicionales para su cuenta de servicios de Internet.

Firewall SPI – Su enrutador está equipado con un firewall que protege su red de una amplia gama de ataques habituales de piratas informáticos incluyendo IP Spoofing (simulación IP), Land Attack, Ping of Death (PoD), Denial of Service (DoS, denegación de servicio), IP con longitud cero, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect y fragment flooding.

Conmutador integrado de red de 4 puertos de 10/100 – El enrutador dispone de un conmutador de red integrado de 4 puertos que permite a las computadoras conectadas en red compartir impresoras, datos y archivos MP3, fotos digitales y mucho más. El conmutador cuenta con detección automática para ajustarse a la velocidad de los dispositivos conectados. El conmutador transferirá datos entre las computadoras e Internet simultáneamente sin interrumpir ni consumir recursos.

Compatibilidad con Plug-and-Play Universal (UPnP) – El UPnP (Universal Plug-and-Play) es una tecnología que ofrece un funcionamiento perfecto de las operaciones de mensajes de voz, mensajes de video, juegos y otras aplicaciones compatibles con UPnP.

Soporta paso a través de VPN – Si se conecta desde casa a su red de oficina utilizando una conexión VPN, su enrutador permitirá a su computadora equipada con VPN pasar por el enrutador y llegar a la red de la oficina.

Protocolo de configuración de host dinámico (DHCP) integrado – El protocolo de configuración de host dinámico (DHCP) integrado garantiza la conexión más sencilla posible a una red. El servidor DHCP asignará direcciones IP a cada computadora automáticamente de manera que no es necesario configurar una interconexión en red compleja.

Asistente de instalación sencilla – El asistente de instalación sencilla elimina las dudas del proceso de configuración de su enrutador. Este software automático establece por usted los ajustes de la red y configura el enrutador para la conexión con su proveedor de servicios de Internet (ISP). En cuestión de minutos, su enrutador inalámbrico estará listo y funcionando en Internet.

> ***Nota**: El software del asistente de instalación sencilla es compatible con Windows 2000, XP, Vista, y Mac OS Mac OSx 10.4.x. Si emplea otro sistema operativo, el enrutador inalámbrico podrá ser configurado utilizando el método alternativo descrito en la presente guía del usuario (véase Método alternativo de configuración en la página 145).*

Modo G mejorado* – Una mejora de rendimiento de 54g que provee la conectividad inalámbrica más rápida para redes 802.11g en entornos de uso real. Está diseñado para redes de casa que requieren mayor ancho de banda para aplicaciones tal como para compartir fotografías digitales. G mejorado hace que las redes inalámbricas 802.11g sean más eficientes sin afectar el rendimiento de redes vecinas y es compatible a alta velocidad con marcas líderes.

> ** Cuando funciona en el modo de G mejorado de 125, este dispositivo Wi-Fi puede obtener una tasa de transferencia de hasta 34.1 Mbps, la que es equivalente a la de un sistema con el protocolo 802.11g operando con una velocidad de señal de 125 Mbps. La tasa de transferencia actual variará dependiendo de factores ambientales, operacionales entre otros.*

Punto de acceso inalámbrico 802.11g integrado – 802.11g es una nueva y fascinante tecnología inalámbrica que alcanza velocidades de transmisión de datos de hasta 54 Mbps, casi cinco veces más rápida que 802.11b.

Filtrado de direcciones MAC – Para lograr una seguridad adicional, puede configurar una lista de direcciones MAC (identificadores exclusivos de los clientes) que dispongan de permiso para acceder a su red. Cada computadora cuenta con su propia dirección MAC. Simplemente deberá introducir dichas direcciones MAC en una lista usando la interfaz de usuario a través de Web y podrá controlar el acceso a su red.

Contenido del paquete

- Enrutador inalámbrico G mejorado de Dynex
- Guía de instalación rápida
- CD con software de instalación
- Cable Ethernet RJ-45
- Fuente de alimentación
- Guía del usuario

Requisitos de sistema

- Conexión a Internet de banda ancha, como un módem de cable o DSL con una conexión RJ45 (Ethernet)
- Por lo menos una computadora con un adaptador de interfaz de red instalado
- Protocolo de redes TCP/IP instalado en todas las computadoras
- Cable de red Ethernet RJ-45
- Navegador de Internet

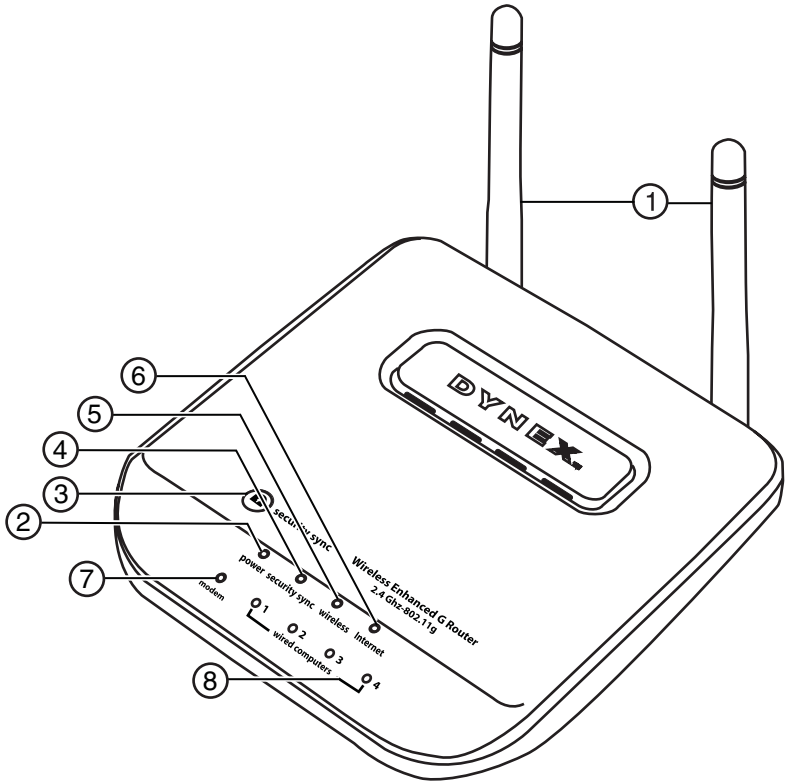
Requisitos del sistema para el software de instalación sencilla

- Una PC con sistema operativo Windows 2000, XP, o Vista, o una computadora Mac con Mac OSx 10.4x
- 64 MB de RAM mínimo
- Navegador Internet

Componentes

El enrutador ha sido diseñado para ser colocado sobre un escritorio. Todos los cables salen por la parte posterior del enrutador para lograr una mejor organización y utilidad. Los indicadores LED se encuentran fácilmente visibles en la parte frontal del enrutador para proporcionarle información sobre la actividad y el estado de la red.

Panel frontal

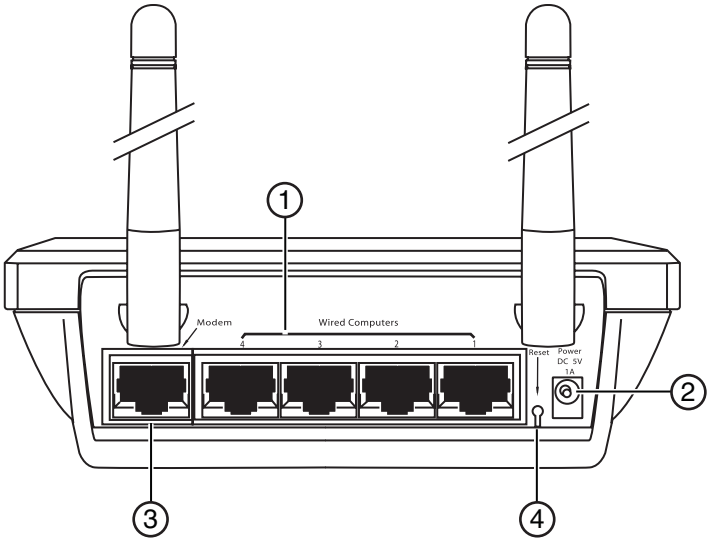


#	Componente	Descripción
1	Antenas	Permite que el enrutador se comunique con un cliente inalámbrico (tarjeta o adaptador USB).

#	Componente	Descripción
2	Indicador LED de Encendido/Listo	Cuando enciende el enrutador o cuando lo reinicia, transcurre un breve período de tiempo mientras el enrutador arranca. Durante ese tiempo, el indicador LED de Encendido/Listo parpadeará. Cuando el enrutador haya arrancado por completo, el indicador LED de Encendido/Listo se iluminará de forma PERMANENTE indicando que el enrutador está listo para ser utilizado. Apagado – El enrutador está apagado Verde parpadeante – El enrutador está arrancando Verde permanente – El enrutador está listo
3	Botón de sincronización de seguridad	Mantenga este botón presionado durante tres segundos, y en un lapso de dos minutos inicie el procedimiento de configuración de Wi-Fi protegida (WPS) en el dispositivo del cliente. Su cliente intercambiará de forma automática la información de seguridad y será añadido a su red inalámbrica. Al presionar el botón de sincronización de seguridad, WPS se habilitará automáticamente. Refiérase a "Usando la sincronización de seguridad (Configuración de Wi-Fi protegida, WPS)" en la página 159.
4	Indicador LED de sincronización de seguridad	Se ilumina para indicar que WPS está activado. Verde parpadeante – El enrutador está buscando un cliente WPS para conectarse. Verde permanente – Se ha establecido una conexión segura con el cliente.
4	Indicador LED de red inalámbrica	Apagado – La red inalámbrica está apagada Verde permanente – La red inalámbrica está lista Verde parpadeante – Actividad en la red
5	Indicador LED de Internet	Este indicador LED exclusivo le indica cuándo el enrutador está conectado a Internet. Cuando la luz está APAGADA, el enrutador no está conectado a Internet. Cuando la luz está parpadeando, el enrutador está intentado conectarse a Internet. Cuando la luz verde está encendida permanentemente, el enrutador está conectado a Internet. Si configuró la propiedad "Disconnect after x minutes" (Desconectar después de x minutos), este indicador LED es particularmente útil para controlar el estado de la conexión de su enrutador. Apagado – El enrutador no está conectado a Internet Verde parpadeante – El enrutador está intentando conectarse a Internet Verde permanente – El enrutador está conectado a Internet
6	Indicador LED de estado del módem	Este indicador LED se ilumina color VERDE para indicar que su módem ha sido conectado correctamente al enrutador. Parpadea rápidamente cuando se está enviando información a través del puerto entre en enrutador y el módem. Apagado – No hay enlace WAN Verde permanente – El enlace WAN es bueno Verde parpadeante – Actividad de WAN

#	Componente	Descripción
7	Indicadores LED de las computadoras conectadas	Estos indicadores LED están etiquetados del 1 al 4 y corresponden a los puertos numerados en la parte posterior del enrutador. Cuando una computadora se encuentra correctamente conectada a uno de los puertos LAN de la parte posterior del enrutador, el indicador LED se iluminará. Verde significa que se encuentra conectado un dispositivo 10Base-T y anaranjado significa que se encuentra conectado un dispositivo 100Base-T. Cuando envíe información mediante el puerto, el indicador LED parpadeará rápidamente. Apagado – La red inalámbrica está apagada Verde permanente – Dispositivo de 10base-T conectado Anaranjado permanente – Dispositivo de 100base-T conectado Parpadeante – Actividad en el puerto

Panel posterior



#	Componente	Descripción
1	Puertos para las computadoras conectadas por cable - Azul	Conecte sus computadoras por cable (no inalámbricas) a estos puertos. Estos son puertos RJ-45 de 10/100 con negociación automática y enlace automático para su uso con cable Ethernet estándar UTP categoría 5 ó 6. Los puertos están etiquetados del 1 al 4. Dichos puertos corresponden con los indicadores LED numerados de la parte frontal del enrutador.
2	Toma de alimentación	Conecte la fuente de alimentación de 5 V CC a esta toma.
3	Puerto de módem - Verde	Este puerto es para la conexión de su módem de cable o DSL. Utilice el cable suministrado con su módem para conectarlo a este puerto. La utilización de un cable distinto del suministrado con el módem por cable puede causar fallos en el funcionamiento.

#	Componente	Descripción
4	Botón de reinicio	El botón de **Reset** (Reinicio) se emplea en casos excepcionales cuando el enrutador puede estar funcionando mal. Al reiniciar el enrutador se restablecerá el funcionamiento normal del mismo manteniendo los ajustes programados. También puede restablecer los ajustes predefinidos de fábrica utilizando el botón de reinicio. Emplee la función restablecimiento en casos como cuando haya olvidado su contraseña personal. **Reinicio del enrutador** – Pulse y suelte el botón de **Reinicio**. Las luces del enrutador se iluminarán momentáneamente. La luz de Encendido/Listo comenzará a parpadear. Cuando la luz de Encendido/Listo se ilumine de color permanente, el reinicio habrá sido completado. Restablecimiento de la configuración predefinida de fábrica – Mantenga presionado el botón de **Reinicio** por lo menos durante diez segundos y luego suéltelo. Las luces del enrutador se iluminarán momentáneamente. La luz de Encendido/Listo comenzará a parpadear. Cuando la luz de Encendido/Listo se ilumine de color permanente, el restablecimiento habrá sido completado.

Preparación de su enrutador

Requisitos del módem

Su módem de cable o DSL deberá estar equipado con un puerto Ethernet RJ-45. Muchos módems cuentan tanto con un puerto Ethernet RJ-45 como con una conexión USB. Si dispone de un módem con Ethernet y USB, y está utilizando la conexión USB en estos momentos, se le solicitará utilizar el puerto Ethernet RJ45 durante el procedimiento de instalación. Si su módem sólo cuenta con un puerto USB, puede solicitar un tipo distinto de módem para su ISP o, en algunos casos, puede adquirir un módem que disponga de un puerto Ethernet RJ-45.

***Importante**: ¡Instale siempre primero su enrutador! Si está instalando diversos dispositivos de red por primera vez, es importante que su enrutador esté conectado y en funcionamiento antes de intentar instalar otros componentes de red, tales como tarjetas para computadoras portátiles y tarjetas para computadoras de escritorio.*

Asistente de instalación

Dynex le suministra el software de nuestro asistente de instalación sencilla para facilitarle la tarea de instalar su enrutador. Al utilizarlo, logrará que su enrutador esté listo y funcionando en pocos minutos. El Asistente de Instalación requiere que su computadora con Windows 2000 o XP esté conectada directamente a su módem de cable o DSL y que la conexión a Internet se encuentre activa y en funcionamiento en el momento de la instalación. En caso contrario, deberá utilizar la sección "Método alternativo de configuración" de esta Guía del Usuario para configurar su enrutador. Además, si está utilizando un sistema operativo diferente a Windows 2000 o XP, deberá configurar el enrutador utilizando la sección de "Método Alternativo de Configuración" de esta Guía del Usuario.

Conexiones de hardware

Para conectar el hardware:

1. Desconecte el cable de alimentación de su módem. Ponga el enrutador al lado del módem y extienda las antenas del enrutador.
2. Ubique el cable de red que conecta su módem y su computadora. Desconecte este cable del módem, y conéctelo en cualquier puerto azul en la parte posterior del enrutador.
3. Busque el cable de red nuevo (incluido en la caja con su enrutador) y conéctelo al puerto verde en la parte posterior del enrutador. Conecte el otro extremo del cable a s módem, en el puerto que ahora ha quedado disponible.
4. Conecte el cable de alimentación del módem. Espere 60 segundos para que el módem arranque. Conecte la fuente de alimentación del enrutador en el puerto negro en la parte posterior del enrutador. Conecte el otro extremo en un tomacorriente de pared.
5. Espere 20 segundos para que el enrutador arranque. Mire la parte frontal del enrutador y asegúrese de que los iconos de **Modem** y uno de los **Computadoras Cableadas** están iluminados color verde. Si no están iluminados, vuelva a comprobar sus conexiones.

Ejecución del software del asistente de instalación

Para ejecutar el software del asistente de instalación:

1. Apague todos los programas que se encuentren actualmente activos en su computadora.
2. Apague cualquier firewall o software para compartir la conexión a Internet existente en su computadora.
3. Inserte el CD de instalación en su computadora. El asistente de instalación aparecerá automáticamente en la pantalla de su computadora al cabo de 15 segundos. Haga doble clic en el asistente de instalación para ejecutarlo y siga las instrucciones en la pantalla.

***Importante**: Ejecute el software del asistente de instalación desde la computadora que esté directamente conectada al enrutador.*

***Nota**: Para usuarios de Windows: Si el asistente de instalación no arranca automáticamente, seleccione su unidad de CD/DVD desde **My Computer** (Mi PC) y haga doble clic en el archivo con el nombre **Setup Assistant** (Asistente de instalación) para iniciar el asistente de instalación.*

4 Cuando aparezca la pantalla de confirmación, asegúrese de que ha completado todos los pasos de la Guía de Instalación Rápida al marcar la casilla de verificación a la derecha de la flecha y haga clic en **Next** (Siguiente) para continuar.

El asistente de instalación indicará los pasos de la instalación que se han completado.

Al llegar el momento de nombrar su red, el asistente de instalación abrirá la pantalla *Naming your network* (Nombrar su red).

El nombre predefinido de la red inalámbrica o SSID. Este es el nombre de su red inalámbrica al que sus computadoras o dispositivos con adaptadores de red inalámbrica se conectarán.

5 Puede cambiar este nombre por el que desee o puede dejarlo sin modificar. Si desea cambiarlo, escríbalo en algún lugar para futuras referencias. Haga clic en **Next** (Siguiente) para continuar. La pantalla *Internet Account Info* (Información de la cuenta de Internet) aparecerá.

6 Si su cuenta de Internet requiere un nombre y una contraseña, se le pedirán mediante una pantalla parecida a la de la ilustración anterior. Escoja de la lista su país o su ISP.

El asistente de instalación configurará su enrutador enviando los datos al mismo y reiniciándolo. Espere recibir las instrucciones de la pantalla.

***Nota**: No desconecte ningún cable ni la alimentación del enrutador durante el reinicio. Hacerlo dejaría su enrutador inoperable.*

Una vez configurado el enrutador, el asistente de instalación verificará su conexión a Internet.

Esto finaliza la instalación del enrutador. Verá en la pantalla *Congratulations* (Felicidades) cuando su enrutador pueda conectarse a Internet. Abriendo su navegador ya puede navegar y visitar cualquier sitio Web.

7 El asistente de instalación se puede utilizar para configurar sus otras computadoras conectadas o inalámbricas para conectarlas a Internet haciendo clic en **Next** (Siguiente). Si decide añadir computadoras a su enrutador más tarde, seleccione **Exit the Assistant** (Salir del asistente), y haga clic en **Next** (Siguiente).

Para solucionar los problemas de configuración:

1 Si el asistente de instalación no le permite conectarse a Internet, verá la siguiente pantalla. Siga las instrucciones de la pantalla para completar los pasos necesarios para solucionar los problemas.

Para usar la asistencia opcional para conectar con otras computadoras:

1 Este paso opcional le ayudará a conectar computadoras cableadas o inalámbricas adicionales a su red. Siga las instrucciones de pantalla.

Ahora su enrutador está configurado y funcionando correctamente. Ahora es el momento de conectar sus otras computadoras.

Conexión inalámbrica de las computadoras

Las computadoras con adaptadores de red inalámbrica pueden usar esta red. Si todavía tiene que instalar los adaptadores, hágalo ahora. Luego siga las instrucciones sobre cómo conectarse. Cuando haga eso, busque su red: Wi-Fi de la casa de Juan.

Conexión de computadoras con cables

Las computadoras con adaptadores de red cableados pueden usar esta red. Si todavía tiene que instalar los adaptadores, hágalo ahora. Después, simplemente conecte un cable Ehernet entre el puerto de red de su computadora y uno de los puertos LAN disponible (etiquetado como **connections to computers** [Conexiones a computadoras] en la parte posterior de este enrutador).

Una vez que haya verificado que sus otras computadoras cableadas e inalámbricas están bien conectadas, su red está configurada y en marcha. Ahora puede navegar por Internet. Presione **Next** (Siguiente) para regresar al menú principal.

Configuración de seguridad inalámbrica

Asegúrese de completar la configuración básica de su enrutador antes de configurar la seguridad. Asegúrese de que todas sus computadoras (cableadas e inalámbricas) pueden conectarse con éxito a Internet mediante su enrutador.

Para configurar la seguridad:

1. En una computadora que tenga una conexión cableada (con cable) al enrutador, abra un navegador de Web. En el campo de dirección, teclee 192.168.2.1 (o su dirección IP personal), luego haga clic en **Enter** (Entrar).

2. En el menú de la izquierda, vaya a la sección inalámbrica y haga clic en **Security** (Seguridad).

   Si se le pide que inicie la sesión, ingrese su contraseña, o si todavía no tiene una contraseña personalizada, deje este espacio en blanco. Luego haga clic en **Submit** (Enviar).

3 Se le pedirá que escoja un tipo de seguridad. Nosotros le recomendamos WPA2-PSK como el modo de seguridad y WPA-PSK+WPA2-PSK como la autenticación, ya que es el más seguro y fácil de usar. Cuando ha hecho su elección, haga clic en **Apply Changes** (Aplicar cambios).

4 En el campo de “Pre-shared key” (clave previamente compartida), escriba una clave de seguridad que le sea fácil de recordar. Si utiliza signos de puntuación, la seguridad de su red aumentará (por ejemplo: "¡Mi equipo favorito es el de los Tigres!"). Haga clic en **Apply Changes** (Aplicar cambios).

5 Ahora vaya a cada una de sus computadoras inalámbricas. Utilice el software de la aplicación inalámbrica en cada una de ellas para hacer lo siguiente (refiérase a su adaptador inalámbrico en el manual del usuario para obtener instrucciones más detalladas):

a. Encuentre su red inalámbrica y conéctese.

b. Cuando se lo solicite, ingrese la frase que creó anteriormente.

***Nota**: Si una computadora no acepta la frase, es probable que todavía no admita WPA/WPA2. Vaya a la página Web del fabricante del adaptador inalámbrico y busque una actualización para el controlador.*

6 Si no desea actualizar el adaptador inalámbrico de su computadora para que funcione con WPA/WPA2, vuelva al paso 4 y escoja WEP. Refiérase a "Configuración de WEP" en la página 161 para obtener instrucciones sobre como configurar la codificación WEP.

Método alternativo de configuración

La interfaz de usuario avanzada es una herramienta basada en el navegador de Web que puede emplear para configurar el enrutador si no desea emplear el asistente de instalación sencilla. Asimismo, puede emplearla para gestionar funciones avanzadas del enrutador. Desde la interfaz de usuario avanzada de Web, podrá llevar a cabo las siguientes tareas:

- Visualizar los ajustes y el estado actual del enrutador
- Configurar el enrutador para que se conecte a su ISP con los ajustes que éste le ha proporcionado
- Modificar los ajustes actuales de red como la dirección IP interna, el conjunto de direcciones IP, los ajustes de DHCP, y más
- Configurar el firewall del enrutador para que funcione con aplicaciones determinadas (Reenvío de puertos)
- Configurar propiedades de seguridad, tales como restricciones de clientes, filtrado de direcciones MAC, WEP y WPA
- Activar la propiedad de DMZ para una única computadora de la red
- Modificar la contraseña interna del enrutador
- Activar/Desactivar el UPnP (Plug-and-Play Universal)
- Reiniciar el enrutador
- Efectuar copias de seguridad de sus ajustes de configuración

- Restablecer los ajustes de fábrica del enrutador
- Actualizar el firmware del enrutador

Para conectar su enrutador (paso 1):

1. Apague la alimentación de su módem desconectándolo de la fuente de alimentación.
2. Localice el cable de red conectado entre su módem y su computadora y desconéctelo de su computadora, dejando el otro extremo conectado al módem.
3. Inserte el extremo suelto que acaba de desenchufar en el puerto de la parte posterior del enrutador con la etiqueta **Modem** (Módem).
4. Conecte un cable de red (no incluido) desde la parte posterior de su computadora a uno de los puertos para computadora cableadas con las etiquetas **1-4**. Nota: No importa el número de puerto que seleccione.
5. Encienda su módem de cable o DSL volviendo a conectarlo a la fuente de alimentación.
6. Conecte el cable de alimentación en la pared y enchufe el cable en el conector de alimentación del enrutador.
7. Compruebe que su módem está conectado al enrutador verificando las luces en la parte frontal del enrutador. La luz verde con la etiqueta de **Modem** (Módem) debería estar encendida si el módem está bien conectado al enrutador. En caso contrario, vuelva a comprobar sus conexiones.
8. Asegúrese de que su computadora está conectada al enrutador correctamente verificando las luces con las etiquetas **1-4**. La luz que corresponde con el número de puerto conectado a su computadora deberá estar encendida si su computadora se encuentra correctamente conectada. En caso contrario, vuelva a comprobar sus conexiones.

Para configurar los ajustes de red de su computadora para trabajar con un servidor DHCP:

- Consulte la sección "Configuración manual de los ajustes de red" en la página 178 para obtener instrucciones.

Configuración del enrutador usando la interfaz de usuario avanzada de Web:

1. Mediante su navegador de Internet, podrá acceder a la interfaz de usuario avanzada del enrutador. En su navegador, teclee “192.168.2.1” en la línea de direcciones (no necesita ingresar nada más como “http://” ni “www”), y presione **Enter** (Entrar). Se abre la página principal del enrutador.

   ***Nota**: Si llegara a tener dificultades para acceder a la interfaz de usuario avanzada, consulte la sección “Configuración manual de los ajustes de red”.*

2. Para efectuar cambios en los ajustes del enrutador, deberá iniciar la sesión. Haga clic en **Login** (Iniciar sesión), o en cualquiera de los enlaces de la página principal para ir a la pantalla de inicio de sesión.
3. En la pantalla de iniciar sesión, deje la contraseña en blanco (el enrutador es enviado sin contraseña) y haga clic en **Submit** (Enviar) para iniciar sesión.

   Sólo una computadora a la vez puede acceder al enrutador con el fin de efectuar cambios en los ajustes del mismo.
4. Una vez que el usuario ha iniciado sesión para efectuar cambios, existen dos formas de cerrar la sesión. Hacer clic en **Logout** (Cerrar sesión) cerrará la sesión de la computadora.

- 0 -

5 El inicio de sesión tendrá un límite de tiempo y expirará después de un periodo de tiempo determinado. El tiempo de expiración predefinido es de 10 minutos. Este plazo puede ser modificado de 1 a 99 minutos. Para obtener más información, consulte la sección "Cambiando el ajuste de tiempo límite de sesión" en la página 176.

Usando la interfaz de usuario avanzada de Web

La página principal es la primera página que verá cuando acceda a la Interfaz de usuario avanzada de Web. La página principal le ofrece una imagen rápida del estado y los ajustes del enrutador. Desde esta página, es posible acceder a todas las páginas de configuración avanzada.

Vínculos de navegación rápida – Puede ir directamente a cualquiera de las páginas de la UI avanzada del enrutador haciendo clic directamente en estos vínculos. Los vínculos se encuentran divididos en categorías lógicas y agrupadas por fichas para facilitar la búsqueda de un ajuste concreto. Al hacer clic sobre el encabezamiento de color morado de cada ficha aparecerá una breve descripción de la función de la misma.

Botón "Home" – El botón **Home** (Inicio) se encuentra disponible en todas las páginas de la UI. Presionar este botón lo regresará a la página principal.

Indicador del estado de Internet – Este indicador está visible en todas las páginas de la UI, indicando el estado de la conexión del enrutador. Cuando el indicador muestra **conexión OK** (Conexión en buen estado) en verde, el enrutador se encuentra conectado a Internet. Cuando el enrutador no está conectado a Internet, el indicador mostrará el mensaje **no conexión** (sin conexión) en rojo. El indicador es actualizado automáticamente cuando efectúe cambios en las configuraciones del enrutador.

Botón de Login/Logout (Iniciar/Cerrar sesión) – Este botón le permite iniciar y cerrar la sesión del enrutador con sólo presionar un botón. Cuando ha iniciado sesión con el enrutador, este botón mostrará la palabra **Logout** (Cerrar sesión). Iniciar sesión con el enrutador le llevará a una página independiente de inicio de sesión en la que será preciso ingresar una contraseña. Cuando haya iniciado sesión con el enrutador podrá efectuar cambios en los ajustes. Cuando haya terminado de realizar los cambios, podrá cerrar la sesión haciendo clic en **Logout** (Cerrar sesión).

Botón Help (Ayuda) – El botón de **Help** (Ayuda) le proporciona el acceso a las páginas de ayuda del enrutador. La opción de ayuda se encuentra disponible asimismo en muchas páginas haciendo clic en la opción **more info** (más información) situada junto a determinadas secciones de cada página.

LAN Settings (Configuraciones de LAN) – Le muestra la configuración de la red de área local (LAN) del enrutador. Es posible efectuar cambios en los ajustes haciendo clic en cualquiera de los vínculos ("IP Address" [dirección IP], "Subnet Mask" [Máscara de subred], "DHCP Server" [Servidor DHCP]) o haciendo clic en el vínculo de navegación rápida **LAN** (situado en la parte izquierda de la pantalla.

Features (Características) – Le muestra el estado del NAT, firewall y características inalámbricas del enrutador. Es posible efectuar cambios en los ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en los vínculos de **navegación rápida** en el lado izquierdo de la pantalla.

Internet Settings (Configuración de Internet) – Muestra la configuración de la parte de Internet/WAN del enrutador que conecta a Internet. Es posible efectuar cambios en cualquiera de estos ajustes haciendo clic en cualquiera de los vínculos o haciendo clic en el vínculo de **navegación rápida** - **Internet/WAN** en la parte izquierda de la pantalla.

Version Info (Información sobre la versión) – Muestra la versión del firmware, la versión del código de arranque, la versión del hardware y el número de serie del enrutador.

Page Name (Nombre de página) – La página en la que se encuentra puede identificarse con este nombre. La presente Guía del Usuario se referirá en ocasiones a las páginas por el nombre. Por ejemplo **LAN > LAN Settings** se refiere a la página "LAN Settings" (Ajustes de LAN).

Configuración de su enrutador para la conexión al proveedor de servicios de Internet (ISP)

La ficha **Internet/WAN** es donde configurará su enrutador para conectar con su proveedor de servicios de Internet (ISP). El enrutador es capaz de conectarse prácticamente al sistema de cualquier ISP siempre que las configuración del enrutador haya sido configurada correctamente para el tipo de conexión de su ISP. La configuración de la conexión a su ISP se suministra por su ISP.

Para configurar el enrutador con los ajustes que le ha proporcionado su ISP, deberá:

1. Hacer clic en **Connection Type** (Tipo de conexión) en el lado izquierdo de la pantalla y seleccionar el tipo de conexión que emplea.
2. Si su ISP le ha proporcionado la configuración de DNS, al hacer clic sobre **DNS** podrá ingresar las direcciones DNS para ISP que requieran ajustes específicos.
3. Al hacer clic en **MAC address** (Dirección MAC) podrá clonar la dirección MAC de su computadora o ingresar una dirección MAC de WAN específica en caso de ser requerida por su ISP.
4. Cuando haya finalizado de realizar los ajustes, el indicador de **Internet Status** (Estado de Internet) mostrará el mensaje **connection OK** (Conexión en buen estado) si su enrutador ha sido configurado correctamente.

Para configurar su tipo de conexión:

1. Haga clic en **Connection Type** (Tipo de conexión) desde el menú al lado izquierdo de la pantalla. Se abrirá la página *Connection Type* (Tipo de conexión). Desde esta página podrá seleccionar el tipo de conexión que utiliza haciendo clic en el botón situado junto a su tipo de conexión y seguidamente haciendo clic en **Next** (Siguiente).

Configurando el tipo de conexión de su proveedor de servicios de Internet (ISP) como IP dinámica

Un tipo de conexión dinámica es el tipo más común de conexión para módems de cable. Configure el tipo de conexión como **dynamic** (dinámica) es suficiente en muchos casos para completar la conexión con su ISP. Es posible que algunos tipos de conexión dinámica requieran un nombre de host. Si le ha sido asignado uno, puede ingresarlo en el espacio previsto para tal fin. Su ISP le asignará su nombre de host. Es posible que algunas conexiones dinámicas requieran la clonación de la dirección MAC de la PC que se encontraba originariamente conectada al módem.

Cambiar la dirección MAC de WAN

Si su ISP requiere una dirección MAC específica para conectarse al servicio, puede ingresar una dirección MAC específica o puede clonar la dirección MAC de la computadora actual mediante este vínculo.

Configurando el tipo de conexión de su proveedor de servicios de Internet (ISP) como IP estática

Una dirección IP estática es un tipo de conexión menos frecuente que los otros tipos de conexiones. Si su ISP emplea direccionamiento IP estático, necesitará su dirección IP, máscara de subred y dirección de puerta de enlace del ISP. Esta información puede obtenerla de su ISP o la puede encontrar en la documentación que su ISP le envió. Introduzca su información y haga clic en **Apply Changes** (Aplicar cambios). Una vez aplicados los cambios, el indicador de **Internet Status** (Estado de Internet) mostrará el mensaje**connection OK** (Conexión en buen estado) si su enrutador ha sido configurado correctamente.

Configurando el tipo de conexión de su ISP como PPPoE

La mayoría de proveedores de DSL emplean PPPoE como tipo de conexión. Si usted utiliza un módem de DSL para conectarse a Internet, es probable que su ISP emplee PPPoE para iniciar la sesión con el servicio. Si dispone de una conexión de Internet en su casa u oficina pequeña que no precisa módem, podrá utilizar asimismo PPPoE.

Su tipo de conexión es PPPoE si:

- Su ISP le proporcionó un nombre de usuario y una contraseña que son necesarios para conectarse a Internet;
- Su ISP le proporcionó software como WinPOET o Enternet300 que usted emplea para conectarse a Internet;
- Usted debe hacer doble clic en un icono del escritorio distinto al de su navegador para acceder a Internet.

Ingrese lo siguiente:

User Name (Nombre de usuario) – Este espacio ha sido previsto para ingresar el nombre de usuario asignado por su ISP.

Password (Contraseña) – Ingrese su contraseña y vuelva a introducirla en el campo *Retype Password* (Introducir contraseña de nuevo) para confirmarla.

Service Name (Nombre de servicio) – El nombre del servicio es requerido en raras ocasiones por un ISP. Si no está seguro si su ISP requiere un nombre de servicio, deje este espacio en blanco.

MTU – El ajuste MTU no debería ser modificado nunca a no ser que su ISP le proporcione un ajuste MTU específico. Si se efectúan cambios en el ajuste MTU, pueden surgir problemas con su conexión a Internet, incluyendo la desconexión, acceso lento a Internet y problemas para el correcto funcionamiento de las aplicaciones de Internet.

Disconnect after X minutes… (Desconectar después de X minutos) – Esta función se utiliza para desconectar automáticamente el enrutador de su ISP cuando no existe actividad durante un periodo determinado de tiempo. Por ejemplo, al colocar una marca junto a esta opción e ingresar **5** en el campo para los minutos, el enrutador se desconectará de Internet después de cinco minutos de inactividad en Internet. Esta opción deberá ser empleada en el caso de que usted pague por sus servicios de Internet por minutos.

Configurando los ajustes personalizados de Domain Name Server (DNS, Servidor de nombres de dominio)

Un *servidor de nombres de dominio* es un servidor situado en Internet que convierte los localizadores de recursos universales (URL) como "www.dynex.com" en direcciones IP. Muchos proveedores de servicios de Internet (ISPs) no precisan que usted introduzca esta información en el enrutador. La casilla de verificación **Automatic from ISP** (Automáticamente desde el ISP) deberá ser marcada si su ISP no ha proporcionado ninguna dirección DNS específica. Si utiliza un tipo de conexión de IP estática, es posible que deba introducir una dirección DNS específica y una dirección DNS secundaria para que su conexión funcione correctamente. Si su tipo de conexión es dinámica o PPPoE, es probable que no sea necesario introducir ninguna dirección DNS. Deje marcado la casilla de verificación **Automatic from ISP** (Automáticamente desde el ISP). Para introducir los ajustes de la dirección de DNS, desmarque la casilla de verificación **Automatic from ISP** (Automáticamente desde el ISP) e introduzca sus entradas DNS en los espacios previstos. Haga clic en **Apply Changes** (Aplicar cambios) para guardar los ajustes.

Configurando la dirección MAC (Controlador de acceso a los medios) de su WAN

Todos los componentes de la red incluyendo tarjetas, adaptadores y enrutadores, tienen un "número de serie" único llamado dirección MAC. Es posible que su proveedor de servicios de Internet registre la dirección MAC del adaptador de su computadora y que sólo permita a esa computadora en particular conectarse al servicio de Internet. Cuando instale el enrutador, su propia dirección MAC será "vista" por el ISP y esto puede provocar que la conexión no funcione. Dynex incorpora la posibilidad de clonar (copiar) la dirección MAC de la computadora al enrutador. Esta dirección MAC, será considerada por el sistema del ISP como la dirección MAC original y permitirá la conexión a la red. Si no está seguro si su ISP necesita que ver la dirección MAC original, simplemente clone la dirección MAC de la computadora que se encontraba originalmente conectada al módem. La clonación de la dirección no causará ningún tipo de problema en su red.

Para clonar su dirección MAC:

1. Asegúrese de que está utilizando la computadora que se encontraba ORIGINALMENTE CONECTADA a su módem antes de la instalación del enrutador. Haga clic en
2. Haga clic en **Clone** (Clonar) y luego en **Apply Changes** (Aplicar cambios). Su dirección MAC ha sido ahora clonada en el enrutador.

Para introducir una dirección MAC específica:

- Introduzca la dirección MAC en los espacios previstos para tal fin y haga clic sobre **Apply Changes** (Aplicar cambios) para guardar los cambios. La dirección MAC de WAN del enrutador será sustituida por la dirección MAC que haya especificado.

Usando la interfaz de usuario avanzada de Web

Mediante su navegador de Internet, podrá acceder a la interfaz de usuario avanzada del enrutador. En su navegador, teclee **192.168.2.1** (no teclee ningún nada más como "http://" o "www") y presione **Enter** (Entrar). Verá la pantalla principal del enrutador en la ventana de su navegador.

Viendo la configuración de LAN

Al hacer clic en el encabezado de la ficha **LAN Setup** (Configuración de LAN) accederá a la correspondiente página de encabezamiento. Aquí se puede encontrar una breve descripción de las funciones. Para ver la configuración o realizar cambios en alguno de los ajustes de LAN, haga clic en **LAN Settings** (Configuración de LAN), o para ver la lista de las computadoras conectadas, haga clic en **DHCP Client List** (Lista de clientes DHCP).

Modificando la configuración de LAN

Todos los ajustes de la configuración de la LAN interna del enrutador pueden verse y modificarse aquí.

IP Address (Dirección IP) – *IP address* es la dirección IP interna del enrutador. La dirección IP predefinida es **192.168.2.1**. Para acceder la interfaz de configuración avanzada de Web, introduzca esta dirección IP en la barra de direcciones de su navegador. Esta dirección se puede modificar en caso necesario. Para modificar la dirección IP, introduzca la nueva dirección IP y haga clic en **Apply Changes** (Aplicar cambios). La dirección IP seleccionada será una IP no enrutable.

Ejemplos de IP no enrutable son: 192.168.x.x (donde x es una cifra entre 0 y 255), y 10.x.x.x (donde x es una cifra entre 0 y 255).

Subnet Mask (Máscara de subred) – No es necesario modificar la máscara de subred. Esta es una característica exclusiva y avanzada de su enrutador Dynex. Es posible modificar la máscara de subred en caso necesario; sin embargo, NO realice cambios en la máscara de subred a no ser que una razón específica para hacerlo. El ajuste predefinido es **255.255.255.0**.

DHCP Server (Servidor de DHCP) – La función del servidor DHCP facilita en gran medida la tarea de configurar una red asignando direcciones IP a cada computadora de la red de forma automática. El ajuste predefinido es **On** (Activado). El servidor DHCP puede ser DESACTIVADO en caso necesario, sin embargo, para hacerlo deberá establecer manualmente una dirección IP estática para cada computadora de su red. Para desactivar el servidor DHCP, seleccione **Off,** (Desactivado) y luego haga clic en **Apply Changes** (Aplicar cambios).

IP Pool (Conjunto de IP) – La gama de direcciones IP reservadas para la asignación dinámica a las computadoras de su red. El valor predefinido es 2 - 100 (99 computadoras) Si desea modificar este valor, puede hacerlo introduciendo una nueva dirección IP de inicio y final y haciendo clic en **Apply Changes** (Aplicar cambios). El servidor DHCP puede asignar 100 direcciones IP automáticamente. Esto significa que usted no puede especificar un conjunto de direcciones IP superior a 100 computadoras. Por ejemplo, si comienza por el 50 deberá finalizar en el 150 o inferior, de forma que no se supere la cifra límite de 100 clientes. La dirección IP de inicio deberá ser inferior en su número a la dirección IP de final.

Lease Time (Tiempo límite de concesión) – La cantidad de tiempo que el servidor DHCP reservará la dirección IP para cada computadora. Le recomendamos dejar la configuración del tiempo de concesión en **Forever** (Para siempre). La configuración predefinida es **Forever**(Para siempre), lo que significa que cada vez que el servidor DHCP asigne una dirección IP a una computadora, la dirección IP para esa computadora en concreto no cambiará. Si configura el tiempo límite de concesión en intervalos menores como un día o una hora, las direcciones IP serán liberadas una vez transcurrido dicho periodo específico de tiempo. Esto significa además que la dirección IP de una computadora en particular puede cambiar a lo largo del tiempo. Si ha establecido cualquiera otra de las características avanzadas del enrutador, como DMZ o filtros IP de clientes, éstos dependerán de la dirección IP. Por esta razón, no es deseable para usted que cambie la dirección IP.

Local Domain Name (Nombre de dominio local) – El ajuste por defecto es **Dynex**. Puede establecer un nombre de dominio local (nombre de red) para su red. No es necesario modificar este ajuste a no ser que tenga una necesidad avanzada específica para hacerlo. Puede dar a la red el nombre que quiera como "MI RED".

Viendo la página de la lista de clientes DHCP

Puede visualizar una lista de las computadoras (conocidas como clientes) que se encuentran conectadas a su red. Puede ver la dirección IP de la computadora, el nombre de host (si se ha asignado uno a la computadora), y la dirección MAC de la tarjeta de interfaz de red (NIC) de la computadora. Presionar el botón **Refresh** (Actualizar) actualizará la lista. Si se han producido cambios, la lista se actualizará.

Configurando los ajustes de red inalámbrica

Hacer clic en el encabezado de la ficha **Wireless** (Inalámbrico) accederá a la página *Wireless* (Inalámbrico). En la ficha**Wireless** (Inalámbrico), encontrará vínculos que le permitirán cambiar los ajustes de red inalámbrica.

Modificación del nombre de red inalámbrica (SSID)

Para identificar su red inalámbrica, se emplea un nombre conocido como SSID (Service Set Identifier, Identificador del conjunto de servicios). El SSID predefinido del enrutador es "Dynex". Puede cambiar este nombre por el que desee o puede dejarlo sin modificar. Si existen otras redes inalámbricas operando en su área, deberá asegurarse de que su SSID sea único (que no coincida con el de otra red inalámbrica en la zona). Para modificar el SSID, introduzca el SSID que desee en el campo **SSID** y haga clic en **Apply Changes** (Aplicar cambios). La modificación es inmediata. Si modifica el SSID, es posible que sus computadoras con acceso inalámbrico deban ser configuradas de nuevo con su nuevo nombre de red. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

Utilización del conmutador del modo inalámbrico

Su enrutador puede funcionar en tres modos inalámbricos diferentes: "g y b", "sólo g", y "sólo b". Los diferentes modos son explicados a continuación.

g and b Mode (Modo g y b) – En este modo, el enrutador es compatible con clientes inalámbricos 802.11b y 802.11g de forma simultánea. Este es el modo predefinido de fábrica y garantiza el perfecto funcionamiento con todos los dispositivos compatibles con Wi-Fi. Si cuenta con una mezcla de clientes 802.11b y 802.11g en su red, recomendamos establecer el enrutador en modo g y b. Este ajuste sólo deberá ser modificado si tiene una razón determinada para hacerlo.

g only Mode (Modo sólo g) – El modo sólo g funciona solamente con clientes de tipo 802.11g. Se recomienda este modo si desea evitar que los clientes 802.11b accedan a su red. Para conmutar los modos, seleccione el modo deseado de la lista de **Wireless Mode** (Modo inalámbrico) y luego, haga clic en **Apply Changes** (Aplicar cambios).

b only Mode (Modo sólo b) – Recomendamos NO emplear este modo a menos que tenga una razón muy concreta para hacerlo. Este modo sólo existe para resolver problemas específicos que pueden producirse con algunos adaptadores de clientes 802.11b y NO es necesario para la interoperabilidad de los estándares 802.11g y 802.11b.

Cuando usar el modo "sólo b"

En algunos casos, es posible que clientes 802.11b más antiguos no sean compatibles con 802.11g inalámbrico. Estos adaptadores tienden a presentar un diseño inferior y es posible que empleen controladores o tecnología más antiguos. Conmutar a este modo puede resolver problemas que en ocasiones se producen con estos clientes. Si sospecha que está utilizando un adaptador de cliente que encaja en esta categoría de adaptadores, consulte primero con el vendedor del adaptador para comprobar si existe una actualización del controlador. Si no hay una actualización del controlador disponible, es posible que la conmutación al modo sólo b pueda resolver su problema. Tenga en cuenta que conmutar al modo "sólo b" puede reducir el rendimiento de 802.11g.

Enhanced G Mode* (Modo G mejorado) – El enrutador soporta dos modos de alta velocidad, modo G mejorado 125 y modo de ráfaga de trama (frame burst).

Seleccionar 125 Enhanced G mode (Modo G mejorado 125) resultará en que todos los dispositivos con el modo G mejorado 125 funcionarán en ese modo si todos son capaces de velocidades de 125 Mbps. Si cualquier dispositivo que no es G mejorado 125 se conecta o se asocia con la red, el enrutador cambiará automáticamente toda la red al modo de ráfaga de trama (frame burst).

Seleccionar **Frame Bursting** (Ráfaga de trama) resultará en que todos los dispositivos capaces de ráfaga de trama funcionarán en este modo y todos los clientes que no son capaces operarán en los modos de 802.11g normales. Ráfaga de trama soporta simultáneamente dispositivos capaces de ráfaga de trama y dispositivos que no son capaces. El modo de ráfaga de trama está basado en la especificación 802.11e que no ha sido formalizada.

Seleccionar **Off** (Desactivado) deshabilitará el modo de Turbo.

** Cuando funciona en el modo de G mejorado de 125, este dispositivo Wi-Fi puede obtener una tasa de transferencia de hasta 34.1 Mbps, la que es equivalente a la de un sistema con el protocolo 802.11g operando con una velocidad de señal de 125 Mbps. La tasa de transferencia actual variará dependiendo de factores ambientales, operacionales entre otros.*

QoS (Quality of Service) Configuration (Configuración de la Calidad de servicio, QoS) – QoS prioriza los datos importantes de su red tal y como el contenido multimedia y Voz sobre IP (VoIP) para que no interfiera con otros datos que se estén enviando a través de la red. Basado en 802.11e, usted puede activar o desactivar esta función seleccionándola en el menú desplegable (3) y seleccionando el modo de reconocimiento que desea utilizar. Si planea transferir documentos de multimedia o utilizar VoIP en su red, le recomendamos que active la función QoS.

Cambiando el canal inalámbrico

Existe una serie de canales de operación entre los que puede seleccionar. En los Estados Unidos, existen 11 canales. En Australia, Reino Unido y la mayor parte de Europa, existen 13 canales. Un pequeño número de países presentan otros requisitos respecto a los canales. Su enrutador está configurado para funcionar en los canales apropiados para el país en que reside. El canal por defecto es el 11 (a menos que se encuentre en un país que no permita el canal 11). Este canal puede ser modificado en caso necesario. Si existen otras redes inalámbricas operando en su área, su red deberá ser configurada para funcionar en un canal

diferente que el resto de redes inalámbricas. Para lograr el mejor rendimiento, utilice un canal que se encuentre al menos a cinco canales de distancia del de la otra red inalámbrica. Por ejemplo, si la otra red está funcionando en el canal 11, configure su red en el canal 6 o inferior. Para modificar el canal, selecciónelo de la lista desplegable y haga clic en **Apply Changes** (Aplicar cambios). La modificación es inmediata.

Usando la propiedad de transmitir SSID

Nota: *Esta característica avanzada deberá ser empleada exclusivamente por usuarios avanzados.*

Para garantizar la seguridad, puede optar por no transmitir el SSID de su red. Hacerlo así, mantendrá su nombre de red oculto a las computadoras que estén rastreando la presencia de redes inalámbricas. Para desactivar la transmisión del SSID, desmarque la casilla de verificación situada junto a **Broadcast SSID** (Transmitir SSID) y después haga clic en **Apply Changes** (Aplicar cambios). La modificación es inmediata. Ahora será preciso configurar cada computadora para conectarse con su SSID específico; ya no se aceptará la opción **ANY** (Cualquiera) para el SSID. Consulte la documentación de su adaptador de red inalámbrica para obtener información acerca de cómo realizar esta modificación.

Protected Mode Switch (Conmutador de modo protegido) Como parte de la especificación 802.11g, el modo protegido (Protected Mode) garantizará el funcionamiento correcto de los clientes 802.11g y de los puntos de acceso cuando exista un tráfico 802.11b intenso en el entorno de actividad. Cuando el modo protegido está **ACTIVADO**, el 802.11g busca otro tráfico de red inalámbrica antes de transmitir los datos. Por lo tanto, la utilización de este modo en entornos con tráfico 802.11b INTENSO o con interferencia produce los mejores resultados en cuanto a rendimiento. Si se encuentra en un entorno en el que existe un tráfico reducido o no existe tráfico de otra red inalámbrica, se logrará el mejor rendimiento si el modo Protegido se encuentra **DESACTIVADO**.

Protección de su red Wi-Fi®

Presentamos diferentes formas de maximizar la seguridad de su red inalámbrica y de proteger sus datos de intrusiones no deseadas. Esta sección está destinada al usuario de una pequeña oficina, oficina en el hogar y del hogar.

Al momento de la publicación de este manual, se encuentran disponibles tres métodos de codificación.

Nombre	Privacidad Equivalente por Cable (WEP) de 64 bits	Privacidad Equivalente por Cable (WEP) de 128 bits	Acceso protegido de Wi-Fi - TKIP	Acceso protegido de Wi-Fi 2
Sigla	WEP de 64 bits	WEP de 128 bits	WPA-TKIP/AES (o sólo WPA)	WPA2-AES (o sólo WPA2)
Seguridad	Buena	Mejor	Óptima	Óptima

Características	Claves estáticas	Claves estáticas	Codificación dinámica de claves y autentificación mutua	Codificación dinámica de claves y autentificación mutua
	Codificación de claves basada en el algoritmo RC4 (típicamente claves de 40 bits)	Más seguro que WEP de 64 bits usando una longitud de clave de 104 bits más 24 bits adicionales de información generada por el sistema	TKIP (Protocolo de Integridad de Clave Temporal) agregado para qué las claves se alternen y se fortalezca la codificación	AES (Estándar de codificación avanzada) no causa ninguna pérdida de tasa de transferencia

Privacidad Equivalente por Cable (WEP)

WEP es un protocolo común que agrega seguridad a todos los productos inalámbricos compatibles con Wi-Fi. WEP le provee a las redes inalámbricas el nivel equivalente de protección de privacidad que dan las redes cableadas.

WEP de 64 bits – WEP de 64 bits se introdujo en un principio con codificación de 64 bits, que incluye una longitud de clave de 40 bits más 24 bits adicionales de datos generados por el sistema (64 bits en total). Algunos fabricantes de hardware se refieren a la codificación de 64 bits como codificación de 40 bits. Poco después de que se introdujese esta tecnología, los investigadores descubrieron que la codificación de 64 bits era demasiado fácil de decodificar.

Codificación de 128 bits – Como resultado de la potencial debilidad de la seguridad de la codificación WEP de 64 bits, se creó un método más seguro de codificación de 128 bits. La codificación de 128 bits incluye una longitud de clave de 104 bits, más 24 bits adicionales de datos generados por el sistema (128 bits en total). Algunos fabricantes de hardware se refieren a la codificación de 128 bits como codificación de 104 bits. La mayoría de equipos inalámbricos actualmente en el mercado es compatible con la codificación WEP tanto de 64 bits como de 128 bits, pero es posible que usted disponga de equipos más antiguos que sólo sean compatibles con la codificación WEP de 64 bits. Todos los productos inalámbricos de Dynex soportan WEP de 64 bits y de 128 bits.

Claves de codificación – Después de seleccionar ya sea el modo de codificación WEP de 64 bits o 128 bits, es sumamente importante que genere una clave de codificación. Si la clave de codificación no es consistente a través de toda la red inalámbrica, sus dispositivos de red inalámbrica no podrán comunicarse el uno con el otro. Puede introducir su clave hexadecimal de forma manual, o introducir una contraseña en el campo **Passphrase** (contraseña) y hacer clic en **Generate** (Generar) para crear una clave. Una clave hexadecimal es una combinación de números y letras de A–F y 0–9. En el caso de WEP de 64 bits necesitará ingresar 10 caracteres hexadecimales. En el caso de WEP de 128 bits necesitará ingresar 26 caracteres hexadecimales.

Por ejemplo:

AF 0F 4B C3 D4 = Clave WEP de 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = Clave WEP de 128 bits

La contraseña WEP NO es la misma que la clave WEP. Su tarjeta utiliza esta contraseña para generar sus llaves WEP pero diferentes fabricantes de hardware pueden tener distintos métodos para generar las claves. Si tiene equipos de diferentes vendedores en su red, lo más fácil sería usar la clave WEP hexadecimal generada en su enrutador inalámbrico e ingresarla manualmente en la tabla de clave de WEP hexadecimal en la pantalla de configuración de su tarjeta.

Sincronización de seguridad (WPS)

Su enrutador está equipado con el último estándar de seguridad, llamado *Wi-Fi Protected Access* (Acceso Wi-Fi protegido, WPA2) y con el común estándar de seguridad llamado *Wired Equivalent Privacy* (Privacidad equivalente por cable, WEP). Su enrutador también soporta la especificación *Wi-Fi Protected Setup* (Configuración Wi-Fi protegida, WPS), simplificando la configuración de la red inalámbrica. WPS utiliza metodologías familiares, como escribir un *Número Personal de Identificación* (PIN) o presionar un botón para permitrles a los usuarios la configuración automática de nombres de red y una fuerte codificación WPA/WPA 2 y autenticación de datos. De fábrica, la seguridad inalámbrica viene deshabilitada. Para activar la seguridad, debe determinar el estándar que desea utilizar. Para acceder a los ajustes de seguridad, haga clic en **Security** (Seguridad) en la ficha **Wireless** (Inalámbrico).

Usando la sincronización de seguridad (Configuración de Wi-Fi protegida, WPS)

La sincronización de seguridad (WPS) utiliza codificación WPA2. Sin embargo, no proporciona ningún tipo de seguridad adicional, pero estandariza el método de seguridad de su red inalámbrica. Es posible utilizar el método de configuración de botón (PBC) o el método PIN para permitir el acceso de un dispositivo a su red. Conceptualmente, los dos métodos funcionan de la siguiente manera:

PBC: Mantenga presionado el botón de sincronización de seguridad (WPS), situado en la parte superior de su enrutador durante tres segundos. A continuación, inicie el procedimiento de sincronización de seguridad (WPS) en el dispositivo del cliente en un lapso de dos minutos. Su cliente intercambiará de forma automática la información de seguridad y será añadido a su red inalámbrica. El cliente se ha añadido de forma segura a la red inalámbrica. Al presionar el botón de sincronización de seguridad, WPS se habilitará automáticamente. El método PBC también puede ser iniciado desde una computadora portátil.

PIN: El dispositivo cliente tiene un número PIN (de cuatro u ocho dígitos) asociado al WPS. Puede activar WPS mediante la interfaz gráfica mostrada a continuación. Introduzca el PIN del cliente en el registro interno del enrutador (accesible mediante esta interfaz gráfica). El cliente será automáticamente admitido a su red en menos de dos minutos.

1. Configuración de Wi-Fi protegida (WPS): Activado o desactivado.
2. Método del número de identificación personal (PIN): Mediante este método, el cliente inalámbrico que desee acceder a su red debe proveer al enrutador un PIN de 4 u 8 dígitos. Después de hacer clic sobre "Enroll" (Inscribir), deberá inicial el procedimiento de transferencia WPS desde el cliente en un lapso de dos minutos.
3. PIN del enrutador: Si hay un registro externo disponible, es posible introducir el PIN del enrutador en el registro. Haga clic en**Generate New PIN** (Generar un PIN nuevo) para modificar el PIN establecido por defecto o haga clic en**Restore Default PIN** (Restablecer el PIN predefinido) para restablecer el valor del PIN.
4. Método de configuración de botón (PBC): El método PBC es otro método que le permite conectarse a una red WPS. Presione el botón de sincronización de seguridad, situado en a parte posterior del enrutador, durante tres segundos y después inicie el PBC del dispositivo del cliente. También es posible presionar el botón "Start PBC" (Iniciar PBC) para iniciar este proceso.
5. Método de configuración manual: Esta sección indica los ajustes de seguridad por defecto si WPS no se utiliza.

El enrutador está equipado con WPA2, que es la segunda generación del estándar 802.11i basado en WPA. Esta ofrece un mayor nivel de seguridad mediante la combinación de los métodos avanzados de autenticación de red y los métodos de encriptación AES (Estándar de codificación avanzado) más eficaces.

Acceso de Wi-Fi Protegido (WPA)

WPA es un nuevo estándar de Wi-Fi que aporta mejoras a las funciones de seguridad WEP. Para utilizar la seguridad WPA, los controladores y el software de su equipo inalámbrico deberán haber sido actualizados para que sean compatibles con WPA. Dichas actualizaciones se encuentran disponibles en el sitio Web del vendedor de su equipo inalámbrico. Existen tres tipos de seguridad WPA: WPA-PSK (sin servidor), WPA (con servidor RADIUS) y WPA2.

WPA-PSK (sin servidor) utiliza lo que es conocido como una clave previamente compartida como la clave de la red. Una clave de red es una contraseña que es entre 6 y 8 caracteres de largo. Puede ser una combinación de letras, números o caracteres. Cada cliente utiliza la misma clave de red para acceder la red. Típicamente, este es el modo que se usará en un ambiente de casa.

WPA (con servidor RADIUS) es un sistema en el que un servidor RADIUS distribuye la clave de red a los clientes automáticamente. Esto se encuentra típicamente en un ambiente de negocios.

WPA2 requiere de el Advanced Encryption Standard [Estándar de Codificación Avanzado] (AES) para codificar la información, lo que ofrece mucho más seguridad que WPA. WPA utiliza Temporal Key Integrity Protocol [Protocolo de integridad de clave temporal] (TKIP) y AES para la codificación.

La mayoría de productos Wi-Fi se envían de fábrica con la seguridad desactivada. Así que una vez que su red está funcionando, necesitará activar WEP o WPA y asegurarse de que todos sus dispositivos inalámbricos comparten la misma clave de red.

***IMPORTANTE**: Ahora tiene que configurar todas las tarjetas/adaptadores de red inalámbrica para que sus configuraciones coincidan.*

Compartiendo las mismas claves de red

La mayoría de productos Wi-Fi se envían de fábrica con la seguridad desactivada. Así que una vez que su red está funcionando, necesitará activar WEP o WPA y asegurarse de que sus dispositivos inalámbricos comparten la misma clave de red.

La tarjeta de red inalámbrica G para computadora de sobremesa no puede acceder a la red porque emplea una clave de red diferente de la configurada en el enrutador inalámbrico G mejorado.

Usando una clave hexadecimal

Una clave hexadecimal es una mezcla de números y letras de la A a la F y del 0 al 9. Las claves de 64 bits son cinco cifras de dos dígitos. Las claves de 128 bits son 13 cifras de dos dígitos.

Por ejemplo:

AF 0F 4B C3 D4 = Clave de 64 bits

C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = Clave de 128 bits

***Nota para los usuarios de Mac**: Los productos originales Apple® AirPort® soportan exclusivamente una codificación de 64 bits. Los productos AirPort 2 pueden soportar la codificación de 64 bits o de 128 bits. Por favor, compruebe qué versión del producto está utilizando. Si no puede configurar su red con una codificación de 128 bits, inténtelo con una codificación de 64 bits.*

Configuración de WEP

Para configurar la codificación WEP de 64 bits:

1. Haga clic en **Security** (Seguridad) situado bajo el encabezado **Wireless** (Inalámbrico) en el menú de la izquierda. Se abrirá la página *Wireless (Inalámbrico) > Security (Seguridad)*
2. Seleccione **64-bit WEP** (WEP de 64 bits) de la lista de **Security Mode** (Modo de seguridad).
3. Introduzca su clave tecleando la clave hexadecimal manualmente, o puede poner marcar en el campo **Passphrase** (Contraseña) y luego escriba su contraseña.
4. Haga clic en **Generate** (Generar) para crear cuatro claves hexadecimales diferentes.

   Una clave hexadecimal es una combinación de números y letras de A-F y 0-9. En el caso de WEP de 64 bits necesitará ingresar 10 caracteres hexadecimales.

   Por ejemplo: AF 0F 4B C3 D4 = Clave WEP de 64 bits

5 Haga clic en **Apply Changes** (Aplicar cambios) para guardar los ajustes.

***Cuidado**: Si está configurando el enrutador inalámbrico G mejorado o el punto de acceso desde una computadora con un cliente inalámbrico, necesitará asegurarse de que la seguridad esté ACTIVADA (ON) para este cliente inalámbrico. De lo contrario, su cliente perderá su conexión inalámbrica.*

Para configurar la codificación WEP de 128 bits:

***Nota para los usuarios de Mac**: La opción de "Passphrase" (Contraseña) no funcionará con Apple AirPort. Para configurar la codificación para su computadora Mac, establezca la misma utilizando el método manual descrito en la siguiente sección.*

1 Haga clic en **Security** (Seguridad) situado bajo el encabezado **Wireless** (Inalámbrico) en el menú de la izquierda. Se abrirá la página *Wireless Security* (Seguridad inalámbrica).

2 Seleccione **128-bit WEP** (WEP de 64 bits) de la lista de **Security Mode** (Modo de seguridad).

3 Introduzca su clave tecleando la clave hexadecimal manualmente, o puede poner marcar en el campo **Passphrase** (Contraseña) y luego escriba su contraseña.

4 Haga clic en **Generate** (Generar) para crear cuatro claves hexadecimales diferentes.

Una clave hexadecimal es una combinación de números y letras de A-F y 0-9. En el caso de WEP de 128 bits necesitará ingresar 26 caracteres hexadecimales.

Por ejemplo: C3 03 0F AF 0F 4B B2 C3 D4 4B C3 D4 E7 = Clave WEP de 128 bits

5 Haga clic en **Apply Changes** (Aplicar cambios) para guardar los ajustes.

***Cuidado**: Si está configurando el enrutador inalámbrico G mejorado o el punto de acceso desde una computadora con un cliente inalámbrico, necesitará asegurarse de que la seguridad esté ACTIVADA (ON) para este cliente inalámbrico. De lo contrario, su cliente perderá su conexión inalámbrica.*

Cambiando la configuración de seguridad inalámbrica

Su enrutador está equipado con WPA (Acceso de Wi-Fi protegido), el más moderno estándar inalámbrico de seguridad. También es compatible con el estándar anterior de seguridad llamado WEP (Privacidad Equivalente por Cable). De fábrica, la seguridad inalámbrica viene deshabilitada. Para activar la seguridad, primero deberá determinar qué estándar desea utilizar. Para acceder a los ajustes de seguridad, haga clic en **Security** (Seguridad) en la ficha **Wireless** (Inalámbrico).

Configuración de WPA

***Nota**: Para utilizar la seguridad WPA, todos sus clientes deberán haber actualizado los controladores y el software que son compatibles con WPA. Al momento de la publicación de este manual, se puede descargar de Microsoft® una revisión de seguridad gratuita. Esta revisión sólo funciona con el sistema operativo Windows XP. Asimismo, deberá descargar el controlador más actualizado para su tarjeta de red inalámbrica G mejorado para PC de escritorio o portátil de Dynex desde la página de servicio de atención al cliente de Dynex. En la actualidad no existe soporte para otros sistemas operativos. La revisión de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Dynex.*

WPA emplea como clave de seguridad lo que se conoce como una "clave previamente compartida". Una clave previamente compartida es una contraseña de entre ocho y 63 caracteres de largo. Se compone de cualquier combinación de letras, números y otros caracteres. Todos los clientes emplean la misma clave para acceder a la red. Normalmente, este modo se utilizará en un entorno de hogar.

WPA2 es la segunda generación de WPA y ofrece una técnica de codificación más avanzada que WPA.

Para configurar WPA/WPA2:

1. Haga clic en **Security** (Seguridad) situado bajo el encabezado **Wireless** (Inalámbrico) en el menú de la izquierda. Se abrirá la página *Wireless (Inalámbrico) > Security (Seguridad)*
2. Seleccione **WPA/WPA2-Personal (PSK)** de la lista **Security Mode** (Modo de seguridad).
3. Seleccione **WPA-PSK** para utilizar sólo la autenticación WPA, o **WPA2-PSK** para utilizar sólo la autenticación WPA2, o puede seleccionar **WPA-PSK + WPA2-PSK** para utilizar WPA y WPA2 como tipo de autenticación.
4. Ingrese su clave previamente compartida. Ésta puede ser de 8 a 63 caracteres y pueden ser letras, números o símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale. Esta clave previamente compartida les permitirá a los usuarios total acceso a su red incluyendo los archivos y las impresoras compartidos.
5. Haga clic en **Apply Changes** (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes según el tipo de acceso que desea que tengan.

   Nota: *Si su tarjeta inalámbrica no está equipada con un software compatible con WPA, se puede descargar de forma gratuita un archivo de Microsoft llamado* ***Windows XP Support Patch for Wireless Protected Access*** *(Revisión de Windows XP para compatibilidad de acceso inalámbrico protegido).*

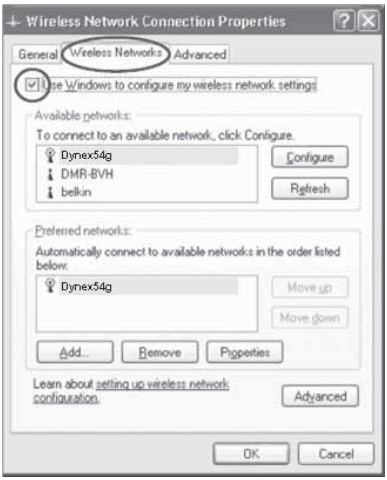
   El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos.

   Importante*: Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA y de haber descargado e instalado el controlador más actualizado de su página de soporte.*

Para configurar la utilidad de red inalámbrica de Windows XP para emplear WPA-PSK:

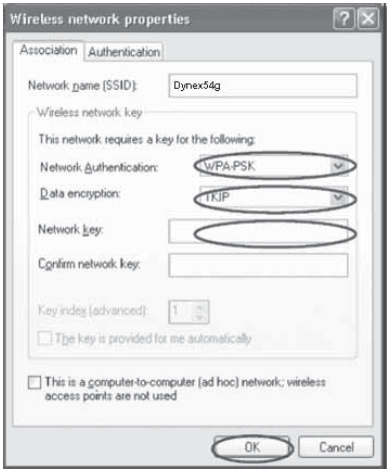
1. En Windows XP, haga clic en **Start** (Inicio), **Control Panel** (Panel de control), **Network Connections** (Conexiones de red).
2. Haga clic con el botón secundario en **Wireless Network Connection Properties** (Propiedades de onexiones de redes inalámbricas) y haga clic en **Properties** (Propiedades).

3 Haga clic en la ficha **Wireless Networks** (Redes inalámbricas). Se abrirá la siguiente pantalla.



4 Compruebe que esté marcada la casilla de verificación **Use Windows to configure my wireless network settings** (Utilizar Windows para configurar mis configuraciones de red inalámbrica).

5 Haga clic en la ficha **Wireless Networks** (Redes inalámbricas), luego haga clic en **Configure** (Configurar). Se abrirá la siguiente pantalla.



6 Para usuarios de hogar u oficina pequeña, seleccione **WPA-PSK** en **Network Authentication** (Autenticación de red).

***Nota**: Seleccione **WPA** si está utilizando esta computadora para conectarse a una red corporativa que soporte un servidor de autenticación como el servidor RADIUS. Consulte con su administrador de red para obtener más información.*

7 Seleccione **TKIP** o **AES** en **Data Encryption** (Codificación de datos). Este ajuste deberá ser idéntico al del enrutador que configure.

8 Introduzca su clave de codificación en el campo **Network key** (Clave de red).

***Importante**: Ingrese su clave previamente compartida. Ésta puede ser de 8 a 63 caracteres y pueden ser letras, números o símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.*

9 Haga clic en **OK** (Aceptar) para aplicar los ajustes.

Usando el modo de punto de acceso

***Nota**: Esta característica avanzada deberá ser empleada exclusivamente por usuarios avanzados. El enrutador puede ser configurado para funcionar como un punto de acceso a la red inalámbrica. El empleo de este modo anulará la característica de compartir IP de NAT y el servidor DHCP En el modo de punto de acceso (AP), el enrutador deberá ser configurado con una dirección IP que se encuentra en la misma subred que el resto de la red con la que desea establecer comunicación. La dirección IP predefinida es 192.168.2.254 y la máscara de subred es 255.255.255.0. Estas pueden ser personalizadas para adaptarse a sus necesidades.*

Para usar el modo de punto de acceso:

1 Haga clic en **Use as access point** (Utilizar como punto de acceso) situado bajo el encabezado **Wireless** (Inalámbrico) en el menú de la izquierda. Se abrirá la página *Gíreles (Inalámbrico) > Use as Access Point* (Usar como punto de acceso).

2 Seleccione **Enable** (Activar). Cuando seleccione esta opción, estará capacitado para modificar la configuración de IP.

3 Configure sus ajustes de IP para coincidir con los de su red, y haga clic en **Apply Changes** (Aplicar cambios).

4 Conecte un cable desde el puerto del módem del enrutador a la red existente.

Ahora el enrutador está funcionando como un punto de acceso. Para acceder de nuevo a la interfaz de usuario avanzada del enrutador, escriba la dirección IP que ha especificado en la barra de direcciones de su navegador. Podrá establecer las configuraciones de codificación, el filtrado de direcciones MAC, el SSID y el canal de forma normal.

Configuración del firewall

Su enrutador se encuentra equipado con un firewall que protegerá su red de una amplia gama de ataques habituales de piratas informáticos, incluyendo:

- IP Spoofing (Suplantación de IP)
- SYN flood (Inundación SYN)

- Land Attack (Ataque Land)
- UDP flooding (Inundación UDP)
- Ping of Death [Ping de la muerte] (PoD)
- Tear Drop Attack (Ataque Tear Drop)
- Denial of Service [Denegación de servicio] (DoS)
- ICMP defect (Defecto de ICMP)
- IP con longitud de cero
- RIP defect (Defecto de RIP)
- Smurf Attack (Ataque Smurf)
- Fragment flooding (Inundación de fragmentos)
- TCP Null Scan (Escán de TCP Null)

El firewall también protege puertos comunes que son empleados con frecuencia para atacar redes. Estos puertos aparecen como *Stealth* (Invisibles), lo que significa que, para cualquier intento y propósito, estos puertos no existen ante un posible pirata informático Si lo necesita, puede apagar la función de firewall; sin embargo, se recomienda dejar el firewall activado. Si desactiva la protección por firewall, no dejará su red completamente vulnerable a los ataques de los piratas, pero es recomendable dejar activado el firewall.

Configurando los ajustes de reenvío interno

La función de *Virtual Servers* (Servidores virtuales) le permitirá enrutar llamadas externas (Internet) para servicios como servidor web (puerto 80), servidor FTP (puerto 21) y otras aplicaciones a través de su enrutador hasta su red interna. Debido a que sus computadoras internas están protegidas por un firewall, las computadoras externas a su red (a través de Internet) no pueden acceder a ellas, ya que no pueden ser *vistas*. Será preciso que se ponga en contacto con el vendedor de la aplicación para descubrir los ajustes de los puertos precisos.

Para introducir los ajustes en el servidor virtual:

1. Abra la página *Virtual Servers* (Servidores virtuales) e introduzca la dirección IP en el espacio previsto para la máquina interna (servidor) y el(los) puerto(s) que se den pasar.
2. Seleccione el tipo de puerto (TCP o UDP), marque la casilla de verificación **Enable**(Activar) y haga clic en **Apply Changes** (Aplicar cambios).

   Cada celda de puerto de entrada tiene dos campos con cinco caracteres máximo por campo que permite determinar un alcance entre un puerto mínimo y un puerto máximo, por ejemplo; [xxxxx]-[xxxxx]. En cada celda, puede introducir un valor de puerto único completando los dos campos con el mismo valor (por ejemplo; [7500]-[7500]) o un alcance amplio de puertos (por ejemplo; [7500]-[9000]). Si necesita múltiples valores de puerto único o una combinación de alcances y un valor único, debe utilizar entradas múltiples hasta un máximo de 20 entradas (por ejemplo; 1. [7500]-[7500], 2. [8023]-[8023], 3. [9000]-[9000]). Únicamente podrá pasar un puerto por cada dirección IP interna. Abrir los puertos de su firewall puede representar un riesgo para la seguridad. Puede activar y desactivar los ajustes de forma rápida. Se recomienda que desactive los ajustes cuando no esté utilizando una aplicación específica.

Configurando los filtros IP de clientes

El enrutador puede ser configurado para restringir el acceso a Internet, a e-mail o a otros servicios de red en determinados días y horas. La restricción puede ser configurada para una sola computadora, para una gama de computadoras o para múltiples computadoras.

Para restringir el acceso Internet a una única computadora:

1. Abra la página de *Firewall* > *Client IP filters* (Filtros IP de clientes), y a continuación introduzca la dirección IP de la computadora a la que desea restringir el acceso en los campos de IP.
2. Introduzca **80** en ambos campos de puerto y seleccione **Both** (Ambos) y después seleccione **Block** (Bloquear). También puede seleccionar **Always** (Siempre) para bloquear el acceso de forma permanente.
3. Seleccione el día de comienzo en la parte superior, el tiempo de comienzo en la parte superior, el día de finalización en la parte inferior y la hora de finalización en la parte inferior.

4 Haga clic en **Enable** (Activar) y luego en **Apply Changes** (Aplicar cambios). La computadora de la dirección IP especificada tendrá bloqueado el acceso a Internet en los momentos establecidos. Asegúrese de haber seleccionado la zona horaria correcta en **Utilities**> **System Setting**> **Time Zone** (Utilidades > Ajustes del sistema > Zona horaria).

Configuración del filtrado de direcciones MAC

El filtro de direcciones MAC es una potente característica de seguridad que le permite especificar qué computadoras están permitidas en la red. Cualquier computadora que trate de acceder a la red y no esté especificada en la lista de filtros no obtendrá permiso para acceder. Cuando active esta propiedad, deberá introducir la dirección MAC de cada cliente (computadora) de su red para permitir el acceso a la misma de cada uno de ellos.

Para configurar el filtrado de direcciones MAC:

1 Abra la página *Firewall > MAC Address filters*, y haga clic en **Enable MAC Address Filtering** (Activar filtrado de direcciones MAC).

2 A continuación, introduzca la dirección MAC de cada computadora de su red haciendo clic en el espacio previsto para tal fin e introduciendo la dirección MAC de la computadora que desee añadir a la lista.

3 Haga clic en **Add** (Agregar) y luego en **Apply Changes** (Aplicar cambios) para guardar los ajustes. Puede disponer de una lista de filtrados de direcciones MAC de hasta 32 computadoras.

***Nota**: No podrá borrar la dirección MAC de la computadora que está utilizando para acceder a las funciones administrativas del enrutador (la computadora que está utilizando ahora mismo).*

Activación de la zona desmilitarizada (DMZ)

La característica DMZ le permite especificar una computadora de su red para ser colocada fuera del firewall. Esto puede ser necesario en el caso de que el firewall esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencias. Utilice esta característica de forma temporal. La computadora que se encuentra en la DMZ NO está protegida contra los ataques de piratas informáticos. Si la suscripción a su ISP le proporciona direcciones IP (WAN) públicas adicionales, es posible situar computadoras adicionales fuera del firewall dado por hecho que cada computadora utiliza un IP (WAN) público diferente.

Para configurar la DMZ en una computadora:

- Abra la página *Firewall* > *DMZ* e introduzca los dígitos finales de su dirección IP en el **campo IP**, haga clic en **Enable** (Activar) y en **Apply Changes** (Aplicar cambios) para que los cambios tengan efecto.

Bloqueo de un Ping de WAN

Los piratas informáticos utilizan lo que se conoce como *pinging* (verificar actividad) para encontrar víctimas potenciales en Internet. Al verificar la actividad de una dirección IP específica y recibir una respuesta de la dirección IP, el pirata informático puede determinar si hay allí algo de interés. El enrutador puede ser configurado de forma que no responda a un ping de ICMP proveniente del exterior. Esto eleva el nivel de seguridad de su enrutador.

Para apagar la respuesta al ping

- Abra la página *Firewall* > *WAN Ping Blocking* (Bloqueo de Ping de WAN) y seleccione Block ICMP Ping (Bloquear Ping de ICMP) luego haga clic en **Apply Changes** (Aplicar cambios). El enrutador no responderá a ningún ping de ICMP.

Ficha de aplicaciones

Esta pantalla le permite gestionar diferentes parámetros del enrutador y llevar a cabo determinadas funciones administrativas.

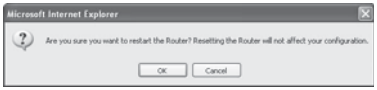
Reiniciando el enrutador

Algunas veces es posible que sea necesario reiniciar el enrutador en caso de que comience a funcionar mal. Al reiniciar el enrutador NO se borrará ninguno de sus ajustes de configuración.

Para reiniciar el enrutador para restablecer el funcionamiento:

1. Haga clic en **Utilities** (Aplicaciones) situado en el menú de la izquierda y luego haga clic en **Restart Router** (Reiniciar enrutador). Se abrirá la página *Restart Router* (Reiniciar enrutador).

2. Haga clic en el botón **Restart Router** (Reiniciar enrutador). Aparecerá el siguiente mensaje.



3. Haga clic en **OK** (Aceptar). Aparecerá el siguiente mensaje.

4. Haga clic en **OK** (Aceptar). El reinicio del enrutador puede llevar hasta 25 segundos. Es importante no apagar la alimentación del enrutador durante el reinicio.

   Aparecerá una cuenta regresiva de 25 segundos en la pantalla. Cuando la cuenta regresiva llegue a cero, el enrutador habrá sido reiniciado. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del enrutador (predefinido = 192.168.2.1) en la barra de direcciones de su navegador.

Restablecimiento de los ajustes predefinidos de fábrica

El empleo de esta opción restablecerá todos los ajustes predefinidos de fábrica del enrutador. Se recomienda que realice una copia de seguridad de sus ajustes antes de restablecer todos los ajustes de fábrica.

Para restaurar los ajustes predefinidos de fábrica:

1. Haga clic en **Utilities** (Aplicaciones) situado en el menú de la izquierda y luego haga clic en **Restore Defaults** (Restablecer ajustes predefinidos). Aparecerá el siguiente mensaje de advertencia.

2. Haga clic en **OK** (Aceptar). Aparecerá el siguiente mensaje.

3. Haga clic en **OK** (Aceptar). El restablecimiento de los ajustes por defecto implica asimismo el reinicio del enrutador. El reinicio del enrutador puede llevar hasta 25 segundos. Es importante no apagar la alimentación del enrutador durante el reinicio.

   Aparecerá una cuenta regresiva de 25 segundos en la pantalla. Cuando la cuenta regresiva llegue a cero, el enrutador habrá sido reiniciado. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del enrutador (predefinido = 192.168.2.1) en la barra de direcciones de su navegador.

Guardando la configuración actual

Puede guardar su configuración actual utilizando esta propiedad. Guardar su configuración le permitirá restablecerla posteriormente en caso de que sus ajustes se pierdan o se modifiquen. Se recomienda realizar una copia de seguridad de su configuración actual antes de llevar a cabo una actualización del firmware.

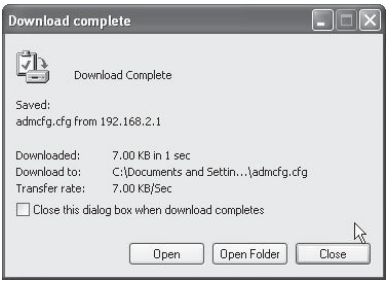
Para guardar la configuración actual:

1. Bajo el encabezado de **Utilities** (Aplicaciones) situado en el menú de la izquierda haga clic en **Save/Backup Settings** (Guardar/Respaldar los ajustes). Se abrirá la página *Save/Backup Settings* (Guardar/Respaldar los ajustes).

2. Haga clic en **Save** (Guardar). Se abrirá la ventana de descarga de archivos.
3. Haga clic en **Save** (Guardar). Se abrirá una ventana que le permitirá seleccionar la ubicación en la que desea guardar el archivo de configuración.

4 Seleccione una ubicación. Puede dar al archivo el nombre que quiera o utilizar el nombre predefinido "Config". Asegúrese de dar un nombre al archivo que le permita encontrarlo más tarde. Cuando haya seleccionado la ubicación y el nombre del archivo, haga clic en **Save** (Guardar).

5 Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana.



6 Haga clic en **Close** (Cerrar). La configuración ha sido guardada.

Restablecimiento de una configuración anterior

Esta opción le permitirá restablecer una configuración guardada anteriormente.

Para restablecer una configuración guardada anteriormente:

1 Bajo el encabezamiento de**Utilities** (Aplicaciones) situado en el menú de la izquierda, haga clic en **Restore Previous Settings** (Restablecer configuración anterior). Se abrirá la página *Restore Previous Settings* (Restablecer configuración anterior).

2 Haga clic en **Browse** (Examinar). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de configuración. Todos los archivos de configuración presentan la extensión ".bin". Localice el archivo de configuración que desea restablecer y haga doble clic en él. Se muestra el siguiente mensaje.

3 Haga clic en **OK** (Aceptar). Una ventana de aviso se abre.

Completar el restablecimiento de la configuración puede llevar hasta 35 segundos.

4 Haga clic en **OK** (Aceptar). Aparecerá una cuenta regresiva de 35 segundos en la pantalla. Cuando la cuenta regresiva llegue a cero, la configuración del enrutador habrá sido restablecida. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del enrutador (predefinido = 192.168.2.1) en la barra de direcciones de su navegador.

Actualización del firmware

De vez en cuando, es posible que Dynex publique nuevas versiones del firmware del enrutador. Las actualizaciones del firmware contienen mejoras de las propiedades y soluciones para los problemas que puedan existir. Cuando Dynex publique un nuevo firmware, usted podrá descargarlo de la página Web de actualizaciones de Dynex con el fin de instalar la versión más actualizada del firmware de su enrutador.

Para buscar y descargar una nueva versión del firmware:

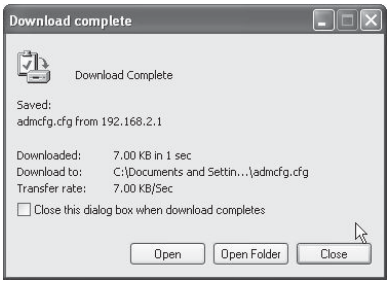
1 Bajo el encabezamiento de **Utilities** (Aplicaciones) situado en el menú de la izquierda, haga clic en **Firmware Update** (Actualización del Firmware). **La página** The *Utilities (Aplicaciones) > Firmware updates (Actualización de firmware)* se abre.

2 Haga clic en **Check Firmware** (Verificar firmware). La aplicación verificará si existe una versión actualizada del firmware disponible.

3 Si encuentra una nueva versión del firmware disponible, se abrirá una ventana que le permitirá seleccionar la ubicación en la que desea guardar el archivo de firmware. Seleccione una ubicación. Puede dar al archivo el nombre que quiera o utilizar el nombre predefinido. Asegúrese de guardar el archivo en un lugar que le permita encontrarlo más tarde. Cuando haya seleccionado la ubicación, haga clic en **Save** (Guardar).

***Nota**: Le recomendamos guardarlo en su escritorio para localizar el archivo fácilmente.*

4 Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana.

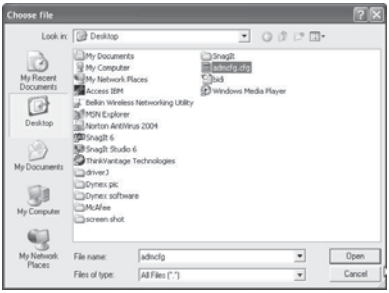


5 Haga clic en **Close** (Cerrar). La descarga se ha completado. Para actualizar el firmware, siga los pasos en la sección **Para actualizar el firmware del enrutador**.

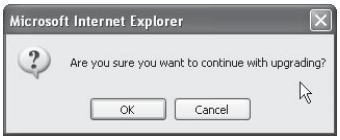
Para actualizar el firmware del enrutador:

1 En la página *Firmware Update* (Actualización del firmware), haga clic en **Browse** (Examinar). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de actualización del firmware.

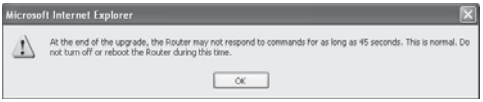
2 Navegue hasta llegar al archivo de firmware descargado y seleccione el archivo haciendo doble clic en el nombre del mismo.



3 El cuadro **Update Firmware** (Actualización del firmware) mostrará la ubicación y el nombre del archivo del firmware que acaba de seleccionar. Haga clic en **Update** (Actualizar). Se le preguntará si está seguro que desea continuar.



4 Haga clic en **OK** (Aceptar). Verá un mensaje más. Este mensaje le indica que es posible que el enrutador no responda durante un minuto, ya que el firmware se carga en el enrutador y éste se reinicia.



5 Haga clic en **OK** (Aceptar). Aparecerá una cuenta regresiva de 60 segundos en la pantalla. Cuando la cuenta atrás llegue a cero, la actualización del firmware del enrutador habrá sido completada. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del enrutador (predefinido = 192.168.2.1) en la barra de direcciones de su navegador.

La actualización del firmware ha sido completada.

Cambiando la configuración del sistema

La página *System Settings* (Configuración del sistema) es en donde podrá introducir una nueva contraseña de administrador, establecer la zona horaria, activar la gestión remota y activar y desactivar la función NAT del enrutador.

Configurando o cambiando la contraseña del administrador

El enrutador se distribuye con la contraseña en blanco. Si desea añadir una contraseña para disfrutar de una mayor seguridad, puede establecerla aquí. Escriba su contraseña y guárdela en un lugar seguro, ya que la necesitará si precisa acceder al enrutador en el futuro. Se recomienda asimismo que establezca una contraseña si piensa utilizar la opción de gestión remota de su enrutador.

Cambiando el ajuste de tiempo límite de sesión

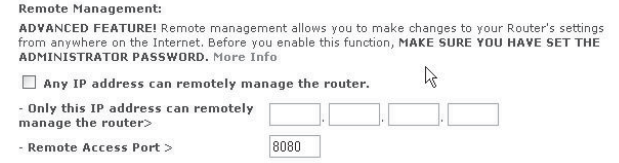
La opción de tiempo límite de sesión le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del enrutador. El temporizador arranca cuando no existe actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después deja su computadora sola sin hacer clic en "Logout" (Cerrar sesión). Si suponemos que el tiempo límite es de 10 minutos, entonces 10 minutos después de que abandone la computadora, la sesión se cerrará. Deberá iniciar una sesión de nuevo para realizar más cambios. La opción del tiempo límite de acceso responde a razones de seguridad y el ajuste predefinido es de 10 minutos.

***Nota**: Solamente una computadora podrá iniciar sesión a la vez en la interfaz de configuración avanzada del enrutador.*

Configurando la hora y la zona horaria

El enrutador mantiene la hora conectándose a un servidor SNTP (Simple Network Time Protocol, protocolo horario de red simple). Esto permite al enrutador sincronizar el reloj del sistema con la hora global de Internet. El reloj sincronizado en el enrutador se emplea para grabar el registro de seguridad y para controlar el filtrado de clientes. Seleccione la zona horaria en la que reside. Si reside en una zona que se realiza el cambio de hora de verano, coloque una marca en la casilla de verificación junto a **Automatically Adjust Daylight Saving**" (Ajustar la hora automáticamente según el horario de verano). Es posible que el reloj del sistema no se actualice inmediatamente. Espere al menos 15 minutos para que el enrutador contacte los servidores de hora de Internet y obtenga una respuesta. Usted no podrá configurar el reloj por sí mismo.

Activando la gestión remota



Antes de activar esta característica avanzada de su enrutador, ASEGÚRESE DE QUE HA ESTABLECIDO LA CONTRASEÑA DE ADMINISTRADOR. La gestión remota le permite efectuar cambios en los ajustes de su enrutador desde cualquier parte en Internet. Existen dos métodos de gestionar el enrutador remotamente. El primero consiste en permitir el acceso al enrutador desde cualquier parte en Internet seleccionando la opción **Any IP address can remotely manage the Router** (Cualquier dirección IP puede gestionar el enrutador

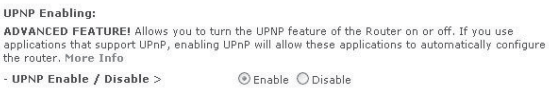
remotamente). Al introducir su dirección IP de WAN desde cualquier computadora en Internet, aparecerá una ventana de iniciar sesión en la que deberá introducir la contraseña de su enrutador. El segundo método consiste en permitir la gestión remota únicamente a una dirección IP específica. Este método es más seguro pero menos conveniente. Para utilizar este método, introduzca la dirección IP desde la que vaya a acceder al enrutador en el espacio previsto y seleccione **Only this IP address can remotely manage the Router** (Únicamente esta dirección IP puede gestionar el enrutador remotamente). Antes de activar esta función, se RECOMIENDA ENFÁTICAMENTE que establezca su contraseña de administrador. Si deja la contraseña vacía, expondrá potencialmente su enrutador a la intrusión externa.

Activando/Desactivando la traducción de direcciones de red (NAT)

***Nota**: Esta característica deberá ser modificada exclusivamente por usuarios avanzados.*

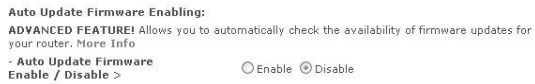
La traducción de direcciones de red (NAT) es el método en el que el enrutador comparte la única dirección IP asignada por su ISP con el resto de computadoras de la red Esta función deberá ser desactivada únicamente si su ISP le asigna múltiples direcciones IP o si necesita desactivar NAT para una configuración avanzada del sistema. Si dispone de una sola dirección IP y desactiva la NAT, las computadoras de su red no podrán acceder a Internet. Es posible asimismo que sucedan otros problemas. Al desactivar la NAT se desactivarán las funciones de su firewall.

Activando/Desactivando UPnP



El UPnP (Plug-and-Play Universal) es otra propiedad avanzada ofrecida por su enrutador. Es una tecnología que ofrece un funcionamiento perfecto de las opciones de mensajes de voz, mensajes de vídeo, juegos y otras aplicaciones compatibles con UPnP. Algunas aplicaciones requieren que el firewall del enrutador sea configurado de una forma específica para funcionar correctamente. Ésto normalmente requiere la apertura de puertos TCP y UDP. Una aplicación compatible con UPnP tiene la capacidad de comunicarse con el enrutador, básicamente "diciendo" al enrutador la forma en que necesita que sea configurado el firewall. El enrutador se envía de fábrica con la función de UPnP desactivada. Si está utilizando cualquier aplicación compatible con UPnP y desea sacar partido de las características UPnP, puede activar la característica UPnP. Seleccione **Enable** (Activar) en la sección **UPnP Enabling** (Activación de UPnP) de la página de *Utilities* (Aplicaciones) y haga clic en **Apply Changes** (Aplicar cambios) para guardad el cambio.

Activando/Desactivando la actualización automática del firmware



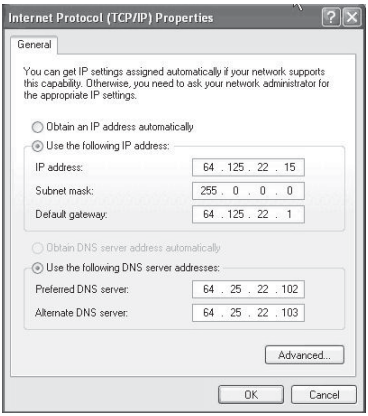
Esta innovación proporciona al enrutador la capacidad integrada de buscar automáticamente una nueva versión del firmware y de informarle de que está disponible una nueva versión. Cuando acceda a la interfaz avanzada del enrutador, éste efectuará una búsqueda para comprobar si está disponible una nueva versión del firmware. En caso afirmativo, aparecerá una notificación. Puede optar por descargar la nueva versión o ignorar el mensaje. El enrutador se envía de fábrica con esta característica activada. Si desea desactivarla, seleccione **Disable** (Desactivar) y haga clic en **Apply Changes** (Aplicar cambios).

Configuración manual de los ajustes de red

Para que su computadora se comunique adecuadamente con su enrutador, necesitará cambiar la configuración de TCP/IP de su PC a DHCP.

Para configurar manualmente los adaptadores de red en Windows 2000, NT, XP o Vista:

1. Haga clic en **Start** (Inicio), **Settings (Configuración)** y después **Control Panel** (Panel de control).
2. Haga doble clic en el icono **Network and dial-up connections** (Conexiones telefónicas y de red) (Windows 2000) o en el icono **Network** [Redes] (Windows XP o Vista).
3. Haga clic con el botón secundario en la **Local Area Connection** (Conexión de área local) asociada a su adaptador de red y seleccione **Properties** (Propiedades) del menú desplegable.
4. Haga clic en **Internet Protocol (TCP/IP)** [Protocolo de Internet (TCP/IP)] y haga clic en **Properties** (Propiedades). Se abrirá la siguiente pantalla.



5. Si se encuentra seleccionada la opción **Use the following IP address** (Utilizar la siguiente dirección IP), su enrutador deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección. Deberá introducir esta información en el enrutador.
6. Si no se encuentran seleccionadas, seleccione **Obtain an IP address automatically** (Obtener una dirección IP automáticamente) y **Obtain DNS server address automatically** (Obtener una dirección de servidor DNS automáticamente), luego haga clic en **OK** (Aceptar).

   Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el enrutador.

Para configurar manualmente los adaptadores de red en Windows 98SE o Me:

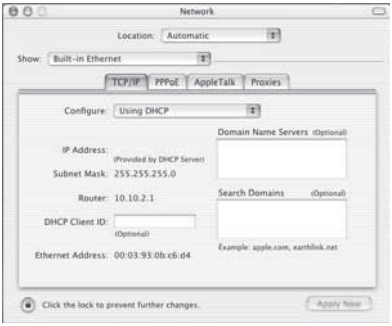
1. Haga clic con el botón secundario en **My Network Neighborhood** (Mi entorno de red) y seleccione **Properties** (Propiedades) de la lista.
2. Seleccione **TCP/IP** y **Settings** (Configuración) para su adaptador de red instalado. Aparecerá la siguiente ventana.
3. Si se encuentra seleccionada la opción **Specify an IP address** (Especificar una dirección IP), su enrutador deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección. Deberá introducir esta información en el enrutador.
   - Escriba la dirección IP y la máscara de subred en la ficha **IP Address** (Dirección IP).
   - Haga clic en la ficha **Gateway** (Puerta de enlace). Escriba la dirección de la gateway (puerta de enlace) en el cuadro.
   - Haga clic en la ficha **DNS Configuration** (Configuración de DNS). Escriba la(s) dirección (direcciones) de DNS en el cuadro.
4. Si no se encuentran seleccionadas, haga clic en **Obtain an IP address automatically** (Obtener una dirección IP automáticamente) en la ficha **IP Address** (Dirección IP) y haga clic en **OK** (Aceptar).
5. Reinicie la computadora. Una vez reiniciada la computadora, el adaptador o los adaptadores de su red estarán configurados para su uso con el enrutador.

Configure la computadora que está conectada al módem de cable o DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir computadoras a su enrutador una vez que éste haya sido configurado para conectarse a Internet.

Para configurar manualmente los ajustes de red en Mac OS X:

1. Haga clic en el icono **System Preferences** (Preferencias del sistema). Se abre el menú *System Preferences* (Preferencias del sistema).

2 Haga clic en **Network** (Red). La ventana *Network* (red) se abrirá.



3 Haga clic en **Built-in Ethernet** (Ethernet integrada), de la lista **Show** (Mostrar).

4 Haga clic en la ficha**TCP/IP**. Junto a **Configure:** (Configurar:) verá la opción **Manually** (Manualmente) o **Using DHCP** (Usando DHCP). Si no es el caso, revise la **ficha PPPoE** para asegurarse de que la opción **Connect using PPPoE** (Conectarse usando PPPoE) NO está seleccionada. Si está seleccionada, deberá configurar su enrutador para un tipo de conexión de PPPoE utilizando su nombre de usuario y su contraseña.

***Nota**: Si se encuentra seleccionada la opción **Manually** (Manualmente) en la lista de **Configure** (Configurar) su enrutador deberá ser configurado para un tipo de conexión de IP estática. Escriba la información de la dirección. Deberá introducir esta información en el enrutador.*

5 Seleccione **Using DHCP** (Usar DHCP) en la lista **Configure:** (Configurar:) y haga clic en **Apply Now** (Aplicar ahora).

Su(s) adaptador(es) de red está(n) configurado(s) ahora para su uso con el enrutador.

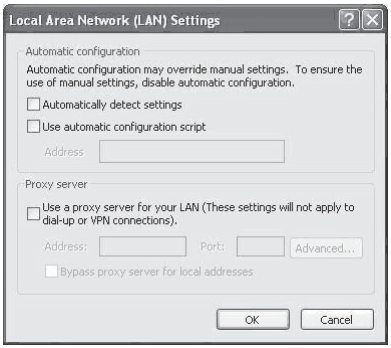
Ajustes recomendados del navegador de Web

En la mayoría de los casos, no necesitará efectuar ningún cambio en los ajustes de su navegador de Web. Si tiene problemas para acceder a Internet o a la interfaz de usuario avanzada de Web, modifique los ajustes de su navegador e introduzca los ajustes recomendados en la presente sección.

Para modificar los ajustes en Internet Explorer 4.0 o más reciente:

1. Inicie su navegador de Web. Seleccione *Tools* (Herramientas) y después **Internet Options** (Opciones de Internet). Se abrirá la página *Internet Options* (Opciones de Internet).

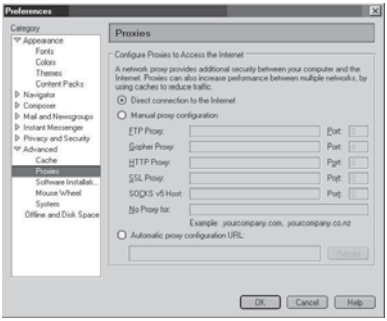
2. Haga clic en la ficha **Connections** (Conexiones) y seleccione **Never dial a connection** (Nunca marcar una conexión). Si no puede efectuar una selección, vaya al siguiente paso.
3. Haga clic en **LAN Settings…** (Configuración de LAN…). Se abre la pantalla *LAN Settings* (Configuración de LAN).



4. Asegúrese de que no existan marcas de verificación junto a ninguna de las opciones mostradas. Haga clic en **OK** (Aceptar) para cerrar la página y haga clic de nuevo en **OK** (Aceptar) en la página de *Internet Options* (Opciones de Internet) para salir.

Para modificar los ajustes en Netscape® Navigator® 4.0 o más reciente:

1 Inicie Netscape y abra el menú **Edit** (Editar) y haga clic sobre **Preferences** (Preferencias). Se abrirá la página *Preferences* (Preferencias).



2 Haga clic en **Advanced** (Avanzado) y en **Proxies** (Proxy).

3 Seleccione **Direct connection to the Internet** (Conexión directa con Internet) y haga clic en **OK** (Aceptar) para salir.

Localización y corrección de fallas

Colocación de su enrutador para un rendimiento óptimo

Su conexión inalámbrica será más potente cuanto más cerca se encuentre la computadora de su enrutador. El alcance típico de funcionamiento de sus dispositivos inalámbricos en interiores se sitúa entre los 100 y los 200 pies. De la misma forma, su conexión y rendimiento inalámbricos se verán algo mermados a medida que aumente la distancia entre los dispositivos conectados a su enrutador inalámbrico y los dispositivos conectados. Es posible que usted lo aprecie o no. Si se aleja aún más de su enrutador, es posible que descienda su velocidad de conexión.

Los factores que pueden debilitar las señales al interferir en el recorrido de las ondas de radio de su red, son los aparatos u obstáculos de metal y las paredes.

Si tiene dudas sobre el rendimiento de su red que pueden estar relacionadas a los factores de alcance hubo obstrucción, intente mover la computadora una posición entre 5 y 10 pies del enrutador inalámbrico para darse cuenta si la distancia es el problema.

***Nota**: Mientras que unos elementos que se listan a continuación pueden afectar el rendimiento de la red, éstos no evitarán que su red inalámbrica funcione. Si tiene dudas de que su red no esté operando a su efectividad máxima, está lista de verificación podría ayudar.*

1. Colocación del enrutador inalámbrico

Coloque su enrutador, el punto central de conexión de su red, lo más cerca posible del centro de sus dispositivos de red inalámbrica.

Para lograr la mejor cobertura de red inalámbrica para sus "clientes inalámbricos" (es decir, computadoras equipadas con tarjetas de red inalámbrica para PC portátiles o de escritorio y adaptadores inalámbricos para USB):

- Asegúrese de que las antenas de su enrutador estén situadas de forma paralela entre sí y orientadas verticalmente (apuntando hacia el techo). Si su enrutador está colocado en posición vertical, oriente las antenas hacia el techo en la máxima medida posible.
- En las casas con varias plantas, coloque el enrutador en el piso más cercano posible al centro de la casa. Esto puede implicar la colocación del enrutador inalámbrico en uno de los pisos superiores.
- Intente no colocar el enrutador cerca de un teléfono inalámbrico de 2.4 GHz.

2. Evite obstáculos e interferencias

Evite colocar su enrutador cerca de dispositivos que puedan emitir "ruido" de radioemisión, tales como hornos microondas. Otros objetos que pueden impedir la comunicación inalámbrica incluyen:

- Refrigeradores
- Lavadoras o secadoras
- Armarios de metal
- Acuarios de gran tamaño
- Ventanas con protección contra rayos ultravioleta de base metálica.

Si su señal inalámbrica parece debilitarse en algunos puntos, asegúrese de que este tipo de objetos no esté bloqueando la ruta de la señal entre sus computadoras y el enrutador.

3. Ubicación del teléfono inalámbrico

Si el rendimiento de su red inalámbrica sigue afectado después de tener en cuenta los aspectos mencionados anteriormente, y usted tiene un teléfono inalámbrico:

- Pruebe a alejar los teléfonos inalámbricos de su enrutador y de sus computadoras conectadas de forma inalámbrica.
- Desenchufe y saque la batería de todos los teléfonos inalámbricos que operen dentro de la banda de 2.4 GHz. Si esto soluciona el problema, su teléfono probablemente esté causando interferencias.
- Si su teléfono permite la selección de canales, modifique el canal del teléfono para situarlo en el canal más alejado de su red inalámbrica. Por ejemplo, sitúe el teléfono en el canal 1 y su enrutador inalámbrico en el canal 11 (la selección del canal dependerá de la región donde vive). Consulte el manual del usuario de su teléfono para obtener instrucciones detalladas.
- En caso necesario, considere la posibilidad de cambiar su teléfono inalámbrico por uno de 900MHz o de 5 GHz.

4. Elija el canal "más tranquilo" para su red inalámbrica

En los lugares donde las casas y las oficinas están muy juntas, tales como edificios de apartamentos o complejos de oficinas, puede ser que haya redes inalámbricas en los alrededores que estén en conflicto con su red. Utilice la capacidad de inspección de sitio de su aplicación inalámbrica para localizar otras redes inalámbricas disponibles, y coloque su enrutador y computadoras en un canal lo más alejado posible del resto de las redes.

Pruebe con más de uno de los canales disponibles con el fin de descubrir la conexión más nítida y de evitar las interferencias de teléfonos inalámbricos cercanos o de otros dispositivos inalámbricos.

Estas guías deberán permitirle abarcar el área de cobertura más extensa posible con su enrutador. En caso de que necesite abarcar un área más amplia, le recomendamos el módulo de extensión/punto de acceso inalámbrico G mejorado de Dynex.

5. Conexiones seguras, VPN y AOL

Las conexiones seguras requieren generalmente un nombre de usuario y una contraseña y se emplean cuando la seguridad es importante. Las conexiones seguras incluyen:

- Conexiones de red privada virtual (VPN) utilizadas con frecuencia para conectarse remotamente a una red de oficina.
- El programa "Bring Your Own Access" (Trae tu propio acceso) de America Online (AOL), que le permite emplear AOL a través de la banda ancha proporcionada por otro servicio por cable o DSL
- La mayoría de las páginas Web de servicios bancarios en línea
- Muchas páginas Web comerciales requieren un nombre de usuario y una contraseña para acceder a su cuenta. Las conexiones seguras pueden verse interrumpidas por una configuración de administración de energía de la computadora que le haga pasar "al modo de suspensión". La solución más sencilla para evitarlo es conectarse de nuevo ejecutando otra vez el software de VPN o AOL, o accediendo de nuevo a la página Web segura.

Una segunda alternativa consiste en modificar la configuración de administración de energía de su computadora, de forma que no pase al modo de suspensión; sin embargo puede ser que esto no se apropiado para PC portátiles. Para modificar su configuración de gestión de la energía en Windows, consulte **Power Options** (Opciones de energía) en el **Control Panel** (Panel de Control).

Si continúa teniendo dificultades con conexiones seguras, VPN y AOL, revise los pasos anteriores para asegurarse de haber tratado estos temas.

Problema: El CD de instalación no arranca automáticamente.

Solución: Si el CD no inicia el asistente de instalación sencilla de forma automática, podría suceder que la computadora esté ejecutando otras aplicaciones que estén interfiriendo con la unidad de CD.

1. Si la pantalla del asistente de instalación sencilla no aparece en un plazo de 15 -20 segundos, haga doble clic en el icono **My Computer** (Mi PC) situado en su escritorio para abrir su unidad de CD.

2. A continuación, haga doble clic sobre la unidad de CD en la que se haya colocado el CD del software de instalación.

3. El asistente de instalación sencilla debería iniciarse al cabo de unos segundos. Si por el contrario, aparece una ventana mostrando los archivos contenidos en el CD, haga doble clic en **EasyInstall.exe**.

4. Si el asistente de instalación sencilla aún no se inicia, consulte la sección "Configuración manual de los ajustes de red" en la página 178 para informarse sobre el método alternativo de configuración.

Problema: El software de instalación sencilla no puede encontrar mi enrutador.

Solución: Si el asistente de instalación sencilla no es capaz de encontrar el enrutador durante el proceso de instalación, compruebe los siguientes puntos:

1. Si el asistente de instalación sencilla no puede encontrar el enrutador durante el proceso de instalación, puede que la computadora que está tratando de acceder a Internet tenga un firewall de un tercero instalado. Estos son algunos ejemplos de firewall de un tercero: ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, y Norton Personal Firewall.

Si tiene instalado un firewall en su computadora, asegúrese de configurarla adecuadamente. Puede determinar si el software de firewall está impidiendo el acceso a Internet apagándolo temporalmente. Si el firewall está desactivado y el acceso a Internet funciona adecuadamente, necesitará modificar las configuraciones de firewall para que funcione correctamente cuando está activado.

Consulte las instrucciones suministradas por el editor del software de su firewall sobre la forma de configurar el firewall para permitir el acceso a Internet.

2. Desconecte la alimentación eléctrica del enrutador por unos 10 segundos y luego vuelva conectarla. Asegúrese de que la luz indicadora de corriente del enrutador esté encendida; debe ser verde permanente. Caso contrario, asegúrese de que el adaptador de CA esté conectado al enrutador y al tomacorriente de pared.

3. Asegúrese de que el cable (utilice el cable que viene con el enrutador) esté conectado entre (1) el puerto de red (Ethernet) en la parte posterior de la computadora y (2) uno de los puertos LAN marcados del "1" al "4" en la parte posterior del enrutador.

> ***Nota**: La computadora NO deberá estar conectada al puerto llamado "Internet/WAN" de la parte posterior del enrutador.*

4. Trate de apagar y reiniciar su computadora y luego de volver a ejecutar el asistente de instalación sencilla.

Si el asistente de instalación sencilla aún no puede encontrar el enrutador, consulte la sección "Configuración manual de los ajustes de red" en la página 178 para informarse sobre el método alternativo de configuración.

Problema: El asistente de instalación sencilla no puede conectar mi enrutador a Internet.

Solución: Si el asistente de instalación sencilla no puede conectar el enrutador a Internet, revise los siguientes puntos:

1. Emplee las sugerencias de la resolución de problemas del asistente de instalación sencilla. Si la pantalla de resolución de problemas no se abre de forma automática, haga clic en el botón **Troubleshoot** (Resolver Problema) en la esquina inferior derecha de la ventana del asistente de instalación sencilla.

2. Si su ISP requiere un nombre de usuario y contraseña, asegúrese de haber introducido su nombre de usuario y contraseña correctamente. Algunos nombres de usuario requieren que el dominio del ISP aparezca al final de los mismos. Por ejemplo: **minombre@miisp.com**. Es posible que sea necesario introducir la parte **@miisp.com** del nombre de usuario junto a su nombre de usuario.

Si continúa sin obtener conexión a Internet, consulte la sección "Configuración manual de los ajustes de red" en la página 178 para informarse sobre el método alternativo de configuración.

Problema: El asistente de instalación sencilla completó la instalación pero mi navegador de Internet no funciona.

- 0 -

No puedo conectarme a Internet. La luz WAN del enrutador está apagada y la luz "Connected" (Conectado) está parpadeando.

Solución: Si no puede conectarse a Internet y la luz "WAN" está apagada y la luz "Connected" (Conectado) está parpadeando, el problema podría radicar en que su módem y enrutador no están conectados adecuadamente.

1. Asegúrese de que el cable de red entre el módem y el enrutador esté conectado. Le recomendamos emplear con este fin el cable suministrado con su módem de cable o DSL. El cable debe estar conectado a un extremo en el puerto Internet/WAN del enrutador, y al otro extremo en el puerto de red de su módem.

2. Desconecte el módem de cable o DSL de su fuente de alimentación durante 3 minutos. Después de 3 minutos vuelva a conectar el módem a su fuente de alimentación. Esto puede obligar al módem a reconocer correctamente el enrutador.

3. Desconecte la alimentación eléctrica del enrutador, espere 10 segundos y luego vuelva conectarla. Esto provocará que el enrutador vuelva a intentar la comunicación con el módem.

4. Pruebe a apagar y a reiniciar de nuevo su computadora.

Problema: El asistente de instalación sencilla completó la instalación pero mi navegador de Internet no funciona.

- 0 -

No puedo conectarme a Internet. La luz WAN del enrutador está apagada y la luz "Connected" (Conectado) está parpadeando.

Solución: Si no puede conectarse a Internet y la luz WAN está encendida y la luz "Connected" (Conectado) está parpadeando, el problema podría radicar en que su tipo de conexión no coincide con la conexión del ISP.

- Si tiene una conexión con *dirección IP estática*, su ISP deberá asignarle la dirección IP, la máscara de subred y la dirección de gateway (puerta de enlace). Refiérase a "Método alternativo de configuración" en la página 145 para obtener detalles sobre la modificación de este ajuste.
- Es posible que deba configurar su enrutador para cumplir los requisitos específicos de su ISP. Para consultar nuestra base de conocimiento ("Knowledge Base") sobre temas específicos del ISP, vaya a: http://web.dynexsupport.com e ingrese "ISP".

Si todavía no puede acceder a Internet después de verificar estos ajustes, póngase en contacto con el soporte técnico de Dynex.

Problema: El asistente de instalación sencilla completó la instalación pero mi navegador de Web no funciona.

- 0 -

No puedo conectarme a Internet. La luz WAN de mi enrutador está parpadeando y la luz "Connected" (Conectado) es permanente.

Solución: Si la luz WAN está parpadeando y la luz "Connected" (Conectado) es permanente pero no puede acceder a Internet, puede que la computadora que está tratando de acceder a Internet tenga un firewall de un tercero instalado. Estos son algunos ejemplos de firewall de un tercero: ZoneAlarm, BlackICE PC Protection, McAfee Personal Firewall, y Norton Personal Firewall.

Si tiene instalado un firewall en su computadora, asegúrese de configurarla adecuadamente. Puede determinar si el software de firewall está impidiendo el acceso a Internet apagándolo temporalmente. Si el firewall está desactivado y el acceso a Internet funciona adecuadamente, necesitará modificar las configuraciones de firewall para que funcione correctamente cuando está activado.

Consulte las instrucciones suministradas por el editor del software de su firewall sobre la forma de configurar el firewall para permitir el acceso a Internet.

Problema: No puedo conectarme a Internet de forma inalámbrica.

Solución: Si no puede conectarse a Internet desde una computadora inalámbrica, compruebe lo siguiente:

1. Contemple las luces de su enrutador. Las luces de su enrutador deberán aparecer de la siguiente manera:

- La luz de alimentación (Power) deberá estar encendida.
- La luz de conectado (Connected) deberá estar encendida pero no intermitente.
- La luz WAN deberá estar encendida o intermitente.

2. Abra el software de su aplicación inalámbrica haciendo clic en el icono de la bandeja del sistema en la esquina inferior derecha de la pantalla. Si está utilizando una tarjeta inalámbrica o adaptador de Dynex, el icono de la bandeja tendrá el siguiente aspecto

 (el icono puede ser rojo o verde):

3. La ventana exacta que aparece variará dependiendo del modelo de tarjeta inalámbrica del que disponga; sin embargo, todas las utilidades deberán presentar una lista de **Redes Disponibles** - aquellas redes inalámbricas a las que se puede conectar.

¿Aparece en los resultados el nombre de su red inalámbrica?

Sí, el nombre de mi red aparece en la lista - Entonces, consulte la solución de problemas "No puedo conectarme a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista".

No, el nombre de mi red no aparece en la lista. Entonces, consulte la solución de problemas "No puedo conectarme a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista".

Problema: No puedo conectarme a Internet de forma inalámbrica pero el nombre de mi red aparece en la lista.

Solución: Si el nombre de su red aparece en la lista **Available Networks** (Redes Disponibles), siga los siguientes pasos para realizar la conexión inalámbrica:

1. Haga clic en el nombre correcto de la red en la lista de **Available Networks** (redes disponibles).

2. Si la red tiene activada la seguridad (codificación), deberá introducir la clave de red. Para obtener más información acerca de la seguridad, consulte la sección "Protección de su red Wi-Fi®" en la página 157.

3. En pocos segundos, el icono de la bandeja del sistema, en la esquina inferior izquierda de su pantalla, deberá ponerse de color verde indicando la correcta conexión con la red.

Problema: No puedo conectarme a Internet de forma inalámbrica y el nombre de mi red no aparece en la lista.

Solución: Si el nombre correcto de la red no está incluido en la lista **Available Networks** (Redes Disponibles), pruebe a realizar los siguientes pasos para la resolución del problema:

1. Mueva temporalmente la computadora, si es posible, a una distancia de 5 a 10 pies del enrutador. Cierre la utilidad inalámbrica y vuelva a abrirla. Si ahora aparece el nombre correcto de la red en la lista **Available Networks** (Redes Disponibles), es posible que tenga un problema de alcance o de interferencia. Consulte las sugerencias enumeradas en "Colocación de su enrutador para un rendimiento óptimo" en la página 182.

2. Empleando una computadora que esté conectada al enrutador a través de un cable de red (al contrario que de forma inalámbrica), asegúrese de que **Broadcast SSID** (emitir SSID) esté activado. Esta configuración se encuentra en la página de configuración inalámbrica titulada *Channel and SSID* (Canal y SSID).

Problema: El rendimiento de mi red inalámbrica es irregular.

La transferencia de datos es lenta en ocasiones.

La potencia de la señal es débil.

Tengo dificultad para establecer y/o mantener una conexión de red privada virtual (VPN).

Solución: La tecnología inalámbrica está basada en la radioemisión, lo que significa que la conectividad y el rendimiento entre dispositivos descenderán a medida que aumente la distancia entre los mismos. Otros factores que causan una degradación en la señal (los metales son generalmente los peores culpables) son las obstrucciones tal como paredes y aparatos electrodomésticos metálicos. Como resultado, el rango de alcance típico de interiores de sus dispositivos inalámbricos se encontrará entre 100 y 200 pies. Tenga en cuenta, además, que la velocidad de conexión puede reducirse cuando más se aleje del enrutador o punto de acceso.

Con el fin de determinar si los problemas de conexión inalámbrica están relacionados con el alcance, le sugerimos mover temporalmente la computadora, a ser posible, entre 5 y 10 pies de distancia del enrutador.

Cambiando el canal inalámbrico

Según la interferencia y el tráfico inalámbrico en el área, cambiar el canal inalámbrico de su red puede mejorar el rendimiento y la fiabilidad. El canal 11 es el canal predefinido con el que se envía de fábrica el enrutador. Puede elegir entre varios canales dependiendo de su región (refiérase a "Cambiando el canal inalámbrico" en la página 156 para obtener instrucciones sobre cómo elegir otros canales).

Limitando la velocidad de transmisión inalámbrica

Limitar la velocidad de transmisión inalámbrica puede ayudar a mejorar la estabilidad de la conexión y el alcance inalámbrico máximo. La mayoría de tarjetas inalámbricas tienen la habilidad de limitar la tasa de transmisión. Para cambiar esta propiedad, vaya a *Windows Control Panel* (Panel de control de Windows), abra la ventana **Network Connections** (Conexiones de red) y haga doble clic sobre la conexión de su tarjeta inalámbrica. En el cuadro de diálogo de *Properties* (Propiedades) seleccione el botón **Configure** (Configurar) en la ficha **General** (los usuarios de Windows 98 deberán seleccionar la tarjeta inalámbrica en el cuadro de lista y luego hacer clic en **Properties** [Propiedades]), y luego elija la ficha **Advanced** (Avanzado) y seleccione la propiedad de velocidad. Las tarjetas inalámbricas cliente normalmente se configuran para ajustar automáticamente la tasa de transmisión

inalámbrica por usted, pero hacer esto puede causar desconexiones periódicas cuando la señal inalámbrica es demasiado débil. Como regla general, las tasas de transmisión más lentas son más estables. Experimente con diferentes tasas de conexión diferentes hasta que encuentre la mejor para su ambiente; note que todas las tasas de transmisión disponibles serán aceptables para navegar el Internet. Para obtener mayor asesoría, consulte el manual del usuario de su tarjeta inalámbrica.

Problema: ¿Cómo se amplía el alcance de la red inalámbrica?

Solución: Dynex recomienda el empleo de los siguientes productos para ampliar la cobertura de la red inalámbrica en hogares u oficinas de gran tamaño.

- Punto de acceso inalámbrico: Un punto de acceso inalámbrico puede duplicar de forma efectiva el área de cobertura de su red inalámbrica. Por lo general, se coloca el punto de acceso en un área que su enrutador inalámbrico G mejorado no cubre actualmente y se conecta al enrutador utilizando ya sea un cable Ethernet o a través de las líneas eléctricas de su hogar utilizando dos adaptadores Ethernet Powerline.

Problema: Tengo dificultades para configurar la WEP (Privacidad Equivalente por Cable) en un enrutador inalámbrico de Dynex o punto de acceso de Dynex.

Solución:

1. Acceda a su enrutador inalámbrico o punto de acceso.

Abra su navegador de Web e introduzca la dirección IP del enrutador inalámbrico o punto de acceso (la dirección IP predefinida del enrutador es 192.168.2.1 y la dirección IP predefinida del punto de acceso es 192.168.2.254). Acceda a su enrutador haciendo clic en el botón **Login** (Iniciar sesión) de la parte superior derecha de la pantalla. Se le solicitará que ingrese su contraseña. Si nunca antes ha establecido una contraseña, deje en blanco el campo de contraseña y haga clic sobre **Submit** (Enviar).

Haga clic en la ficha **Wireless** (Inalámbrico) situada en la parte izquierda de su pantalla. Seleccione la ficha **Encryption** (Codificación) o **Security** (Seguridad) para acceder a la pantalla de ajustes de seguridad.

2. Seleccione **128-bit WEP** (WEP de 128 bits) de la lista.

3. Después de seleccionar su modo de codificación WEP, podrá introducir su clave WEP hexadecimal manualmente, o introducir una contraseña en el campo **Passphrase** y hacer clic en **Generate** (Generar) para crear una clave WEP a partir de la contraseña. Haga clic en **Apply Changes** (Aplicar cambios) para finalizar. Ahora deberá hacer que todos sus clientes coincidan con estos ajustes. Una clave hexadecimal es una combinación de números y letras de A-F y 0-9. En el caso de WEP de 128 bits necesitará ingresar 26 caracteres hexadecimales.

Por ejemplo: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = Clave de 128 bits

4. Haga clic en **Apply Changes** (Aplicar cambios) para finalizar. Ahora está establecida la codificación en el enrutador inalámbrico. Cada computadora de su red inalámbrica deberá ser configurada ahora con los mismos ajustes de seguridad.

***Cuidado**: Si está configurando el enrutador inalámbrico o punto de acceso desde una computadora con un cliente inalámbrico, necesitará asegurarse de que el modo de seguridad esté activado para este cliente inalámbrico. De lo contrario, perderá su conexión inalámbrica.*

***Nota para los usuarios de Mac**: Los productos originales Apple AirPort soportan exclusivamente la codificación de 64 bits. Los productos AirPort 2 pueden soportar la codificación de 64 bits o de 128 bits. Compruebe qué versión del producto Apple AirPort está utilizando. Si no puede configurar su red con una codificación de 128 bits, inténtelo con una codificación de 64 bits.*

Problema: Tengo dificultades para configurar la WEP (Privacidad Equivalente por Cable) en una tarjeta de cliente de Dynex (Tarjeta de red inalámbrica o adaptador de red inalámbrico).

Solución: La tarjeta de cliente deberá emplear la misma clave que el enrutador inalámbrico G mejorado o punto de acceso. Por ejemplo, si su enrutador inalámbrico o punto de acceso utilizan la clave 00112233445566778899AABBCC, la tarjeta de cliente debe ser configurada con la misma clave.

1. Haga doble clic en el icono de **Signal Indicator** (Indicador de señal) para abrir la pantalla de *Wireless Network Utility* (Aplicación de red inalámbrica). El botón **Advanced** (Avanzado) le permitirá ver y configurar más opciones de su tarjeta de cliente. Aparecerá la aplicación de LAN inalámbrica. Esta utilidad le permitirá gestionar todas las propiedades avanzadas de la tarjeta cliente.

2. Haga clic en la ficha **Wireless Network Properties** (Propiedades de la red inalámbrica) seleccione un nombre de red de la lista **Available Networks** (Redes disponibles) y haga clic en el botón **Properties** (Propiedades).

3. Seleccione **WEP** de la lista de **Data Encryption** (Codificación de datos).

4. Asegúrese de que la casilla de verificación **The key is provided for me automatically** (La clave se me proporciona automáticamente) que se encuentra en la parte inferior no esté marcada. Si está utilizando esta computadora para conectarse a una red corporativa, consulte con su administrador de red si es necesario marcar esta casilla.

5. Introduzca su clave WEP en el cuadro **Network key** (Clave de red).

***Importante**: Una clave WEP es una mezcla de números y letras de la A a la F y del 0 al 9. Para la WEP de 128 bits deberá introducir 26 claves. Esta clave de red deberá coincidir con la clave asignada a su enrutador inalámbrico G mejorado o punto de acceso.*

Por ejemplo: C3 03 0F AF 4B B2 C3 D4 4B C3 D4 E7 E4 = Clave de 128 bits

6. Haga clic en **OK** (Aceptar) y después en **Apply** (Aplicar) para guardar el ajuste.

Si NO está utilizando una tarjeta de cliente inalámbrica de Dynex, consulte el manual del usuario del fabricante de la tarjeta cliente inalámbrica que esté utilizando.

Problema: ¿Soportan los productos Dynex la seguridad WPA?

Solución:

***Nota**: Para utilizar la seguridad WPA, todos sus clientes deberán haber actualizado los controladores y el software que son compatibles con WPA. Al momento de la publicación, se puede descargar de Microsoft una revisión de seguridad gratuita. Esta revisión sólo funciona con el sistema operativo Windows XP.*

Descargue la revisión en la siguiente dirección:

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

Asimismo, deberá descargar el controlador más actualizado para su tarjeta de red inalámbrica G para PC de escritorio o portátil de Dynex desde la página de servicio de atención al cliente de Dynex. En la actualidad no existe soporte para otros sistemas operativos. La revisión de Microsoft sólo es compatible con dispositivos con controladores preparados para WPA, como los productos 802.11g de Dynex.

Descargue el último controlador en http://www.dynexproducts.com.

Problema: Tengo dificultades para configurar la seguridad WPA (Acceso protegido Wi-Fi) en un enrutador de Dynex o punto de acceso de Dynex para una red de hogar.

Solución:

1. Seleccione **WPA-PSK (no server)** [WPA-PSK (sin servidor)] de la lista de **Security Mode** (Modo de seguridad).

2. Seleccione **TKIP** o **AES** en **Encryption Technique** (Técnica de codificación). Este ajuste deberá ser idéntico al de los clientes que instale.

3. Ingrese su clave previamente compartida. Ésta puede estar compuesta por entre ocho y 63 caracteres entre letras, números, símbolos o espacios. Esta misma clave deberá ser utilizada en todos los clientes que instale. Por ejemplo, su PSK será algo así como esto: "Clave de red familia Smith".

4. Haga clic en **Apply Changes** (Aplicar cambios) para finalizar. Ahora deberá hacer que todos los clientes coincidan con estos ajustes.

Problema: Tengo dificultades para configurar la seguridad WPA (Acceso protegido de Wi-Fi) en una tarjeta cliente de Dynex (tarjeta de red o adaptador inalámbrico).

Solución: Los clientes deberán emplear la misma clave que el enrutador inalámbrico G mejorado o punto de acceso. Por ejemplo, si la clave es "Clave de red familia Smith" en el enrutador inalámbrico G mejorado o punto de acceso, los clientes deberán emplear también la misma clave.

1. Haga doble clic en el icono de **Signal Indicator** (Indicador de señal) para abrir la pantalla de *Wireless Network Utility* (Aplicación de red inalámbrica).

2. Cuando haga clic en el botón **Advanced** (Avanzado) aparecerá la aplicación de LAN inalámbrica de Dynex. Esta aplicación le permitirá gestionar todas las propiedades avanzadas de la tarjeta cliente de Dynex.

3. Haga clic en la ficha **Wireless Network Properties** (Propiedades de la red inalámbrica) seleccione un nombre de red de la lista **Available Networks** (Redes disponibles) y haga clic en el botón **Properties** (Propiedades). Se abrirá la página *Properties* (Propiedades).

4. Seleccione **WPA-PSK (no server)** [WPA-PSK (sin servidor)] de la lista de **Network Authentication** (Autenticación de red).

5. Introduzca su clave de WPA en el campo **Network key** (Clave de red).

***Importante**: WPA-PSK es una combinación de números y letras de la A a la Z y del 0 al 9. Para WPA-PSK, puede ingresar de ocho a 63 caracteres. Esta clave de red deberá coincidir con la clave asignada a su enrutador inalámbrico G mejorado o punto de acceso.*

6. Haga clic en **OK** (Aceptar) y después en **Apply** (Aplicar) para guardar los ajustes.

Problema: Tengo dificultades para configurar la seguridad WPA (Acceso protegido de Wi-Fi) en una tarjeta cliente de Dynex (tarjeta de red o adaptador inalámbrico) en una oficina.

Solución:

1. Haga doble clic en el icono **Signal Indicator** (Indicador de señal). Se abre la pantalla *Wireless Network Utility* (Aplicación de red inalámbrica).

2. Cuando haga clic en el botón **Advanced** (Avanzado) aparecerá la aplicación de LAN inalámbrica de Dynex. Esta aplicación le permitirá gestionar todas las propiedades avanzadas de la tarjeta cliente de Dynex.

3. Haga clic en la ficha **Wireless Network Properties** (Propiedades de la red inalámbrica) seleccione un nombre de red de la lista **Available Networks** (Redes disponibles) y haga clic en el botón **Properties** (Propiedades). Se abrirá la página *Properties* (Propiedades).

4. Seleccione **WPA** de la lista de **Network Authentication** (Autenticación de red).

5. En la ficha **Authentication** (Autenticación), seleccione los ajustes indicadas por su administrador de red.

6. Haga clic en **OK** (Aceptar) y después en **Apply** (Aplicar) para guardar los ajustes.

Problema: Tengo dificultades para configurar la seguridad WPA (Acceso protegido de Wi-Fi) en una tarjeta de cliente que NO es de Dynex para una red de hogar.

Solución: Si está utilizando una tarjeta inalámbrica para PC de escritorio o portátil que NO es de Dynex y esta tarjeta no está equipada con un software compatible con WPA, se puede descargar de forma gratuita un archivo de Microsoft llamado "Windows XP Support Patch for Wireless Protected Access" (Revisión de Windows XP para compatibilidad de acceso inalámbrico protegido):

http://www.microsoft.com/downloads/search.aspx?displaylang=en

***Nota**: El archivo que Microsoft pone a su disposición sólo funciona con Windows XP. En la actualidad no existe soporte para otros sistemas operativos. Asimismo, deberá asegurarse de que el fabricante de la tarjeta inalámbrica soporte WPA y de haber descargado e instalado el controlador más actualizado de su página de soporte.*

Sistemas operativos soportados:

- Windows XP Professional
- Windows XP Home Edition

Para activar WPA-PSK (sin servidor):

1. Con sistemas que tienen Windows XP, haga clic en **Start** (Inicio), **Control Panel** (Panel de control), **Network Connections** (Conexiones de red).

2. Haga clic con el botón secundario en la ficha **Wireless Networks** (Redes inalámbricas). Se abre la pantalla *Wireless Network Connection Properties* (Propiedades de Conexión de red inalámbrica). Compruebe que esté marcada la casilla de verificación **Use Windows to configure my wireless network settings** (Utilizar Windows para configurar mis configuraciones de red inalámbrica).

3. En la ficha **Wireless Networks** (Redes inalámbricas), haga clic sobre el botón **Configure** (Configurar). Se abre la pantalla *Client Card Properties*.

4. Para usuarios de hogar u oficina pequeña, seleccione **WPA-PSK** en **Network Administration** (Administración de red).

5. Seleccione **TKIP** o **AES** en **Data Encryption** (Codificación de datos). Este ajuste deberá ser idéntico al del enrutador inalámbrico G mejorado o punto de acceso que haya configurado.

6. Introduzca su clave de codificación en el campo **Network key** (Clave de red).

Importante: *Ingrese su clave previamente compartida. Ésta puede ser de 8 a 63 caracteres y pueden ser letras, números o símbolos. Esta misma clave deberá ser utilizada en todos los clientes que instale.*

7. Haga clic en **OK** (Aceptar) para aplicar los ajustes.

¿Cual es la diferencia entre 802.11b, 802.11g, 802.11a y 802.11n?

Actualmente hay cuatro niveles de estándares de redes inalámbricas, que transmiten datos a muy diferentes velocidades máximas. Cada uno está basado en la designación para certificar estándares de redes. El estándar de redes inalámbricas más común, 802.11b, transmite información a 11 Mbps; 802.11a y 802.11g trabaja a 54 Mbps; y Pre-N trabaja a 108 Mbps. 802.11n transmite a velocidades que superan las del 802.11g y tiene un área de cobertura dos veces más amplia. Refiérase a la siguiente tabla para obtener más información detallada.

Tecnología inalámbrica	802.11b	802.11g	802.11a	802.11n
Velocidad	11 Mbps	54 Mbps	54 Mbps	Un 600% más rápida que el estándar 802.11g*

Frecuencia	Equipos caseros comunes tal como teléfonos inalámbricos y hornos de microondas pueden interferir con la banda sin licencia de 2.4 GHz	Equipos caseros comunes tal como teléfonos inalámbricos y hornos de microondas pueden interferir con la banda sin licencia de 2.4 GHz	5 GHz - banda con muy pocos dispositivos	Equipos caseros comunes tal como teléfonos inalámbricos y hornos de microondas pueden interferir con la banda sin licencia de 2.4 GHz
Compatibilidad	Compatible con 802.11g	Compatible con 802.11b	Incompatible con 802.11b o 802.11g	Compatible con 802.11g o 802.11b
Cobertura*	Depende de la interferencia – típicamente 100 - 200 pies en interiores	Depende de la interferencia – típicamente 100 - 200 pies en interiores	El rango de interferencia es típicamente de 50-100 pies	Cobertura hasta un 800 % mayor que el estándar 802.11g*
Ventajas	Madurez - Tecnología heredada	Común – Ampliamente usado para compartir Internet	Menos interferencia – Bueno para aplicaciones de multimedia	Tecnología de vanguardia – El mejor alcance y la mejor tasa de transferencia

** La distancia y la velocidad de conexión variarán según su entorno de red.*

Avisos legales

Declaración de la FCC

DECLARACIÓN DE CONFORMIDAD CON EL REGLAMENTO DE FCC PARA COMPATIBILIDAD ELECTROMAGNÉTICA

Nosotros, Dynex Corporation, con sede en 7601 Penn Avenue South, Richfield, Minnesota, U.S.A., declaramos bajo nuestra sola responsabilidad que el producto DX-WEGRTR, al que hace referencia la presente declaración cumple con la sección 15 de las normativas de la FCC. Su utilización está sujeta a las siguientes dos condiciones: (1) Este dispositivo no puede causar interferencia dañina, y (2) este dispositivo debe aceptar cualquier interferencia recibida incluyendo interferencias que puedan causar una operación no deseada.

Cuidado: Exposición a las radiaciones de radiofrecuencia.

La energía de salida emitida por este dispositivo se encuentra muy por debajo de los límites de exposición a radiofrecuencias. No obstante, el dispositivo será empleado de tal forma que se minimice la posibilidad de contacto humano durante el funcionamiento normal. Cuando se conecta una antena externa al dispositivo, dicha antena deberá ser colocada de tal manera que se minimice la posibilidad de contacto humano durante el funcionamiento normal. Con el fin de evitar la posibilidad de superar los límites de exposición a radiofrecuencias establecidos por la FCC, la proximidad del ser humano a la antena no deberá ser inferior a los 20 cm (8 pulgadas) durante el funcionamiento normal.

Advertencia de la FCC

Cualquier cambio o modificación que no esté aprobado expresamente por la parte responsable por el cumplimiento con el reglamento de FCC puede anular la autoridad del usuario para operar este equipo.

Certificación de seguridad de DHHS y FDA

Este producto está hecho y probado para cumplir con los estándares de seguridad de los requisitos del FCC y con el rendimiento de seguridad del Departamento Estadounidense de Salud y Servicios Humanos, y también con los estándares de rendimiento de radiación del FDA 21 CFR, subcapítulo J.

Declaración del ICES-003 de Canadá

Este aparato digital de Clase B cumple con el ICES-003 canadiense.

FCC Parte 15

Este dispositivo satisface la parte 15 del reglamento FCC. La operación de este producto está sujeta a las dos condiciones siguientes: (1) Este dispositivo no puede causar interferencia dañina, y (2) este dispositivo debe aceptar cualquier interferencia recibida incluyendo interferencias que puedan causar una operación no deseada.

Este equipo ha sido sometido a prueba y se ha determinado que satisface los límites establecidos para ser clasificado cómo dispositivo digital de la Clase B de acuerdo con la Parte 15 del reglamento FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias dañinas en un ambiente residencial. Este equipo genera, usa y puede emitir energía de radiofrecuencia, y si no se instala y usa de acuerdo con las instrucciones, puede causar interferencias perjudiciales a las comunicaciones de radio. Sin embargo, no se garantiza que no ocurrirá interferencia en una instalación particular. Si este equipo causa interferencias perjudiciales en la recepción de la señal de radio o televisión, lo cual puede comprobarse encendiendo y apagando el reproductor alternativamente, se recomienda al usuario corregir la interferencia mediante uno de los siguientes procedimientos:

- Cambie la orientación o la ubicación de la antena receptora.
- Aumente la distancia entre el equipo y el receptor.
- Conecte el equipo a un tomacorriente de un circuito distinto de aquel al que está conectado el receptor.
- Solicite consejo al distribuidor o a un técnico calificado para obtener ayuda.

Declaración de RSS 310

Para reducir el potencial de interferencia de radio a otros usuarios, el tipo de antena y su ganancia deben ser elegidos de tal forma que la potencia radiada equivalente (EIRP) no sea más que la permitida para una comunicación exitosa.

Garantía limitada de un año

Dynex Products ("Dynex") le garantiza a usted, el comprador original de este nuevo **DX-WEGRTR** ("Producto"), que éste se encontrará libre de defectos de material o de mano de obra en su fabricación original por un periodo de un (1) año a partir de la fecha de compra del Producto ("Período de Garantía"). Este Producto debe ser comprado en un distribuidor autorizado de productos Dynex y empacado con esta declaración de garantía. Esta garantía no cubre Productos reacondicionados. Si notifica a Dynex durante el Período de Garantía sobre un defecto cubierto por esta garantía que requiere reparación, los términos de esta garantía se aplican.

¿Cuánto dura la garantía?

El Período de Garantía dura por un año (365 días) a partir de la fecha en que compró el Producto. La fecha de compra se encuentra impresa en el recibo que recibió con el producto.

¿Qué es lo que cubre esta garantía?

Durante el Período de Garantía, si un centro de reparación autorizado de Dynex concluye que la fabricación original del material o la mano de obra del Producto se encuentran defectuosos Dynex (cómo su opción exclusiva): (1) reparará el Producto con repuestos nuevos o reacondicionados; o (2) reemplazará el Producto con uno nuevo o con uno reacondicionado con repuestos equivalentes. Los Productos y repuestos reemplazados bajo esta garantía se volverán propiedad de Dynex y no se le regresarán a usted. Si se requiere la reparación de Productos y partes después de que se vence el Período de Garantía, usted deberá pagar todos los costos de mano de obra y de repuestos. Esta estará vigente con tal que usted sea el dueño de su producto Dynex durante el Periodo de Garantía. El alcance de la garantía se termina si usted vende o transfiere el producto.

¿Cómo se obtiene la reparación de garantía?

Si ha comprado el Producto en una tienda de ventas, lleve su recibo original y el Producto a la tienda en donde lo compró. Asegúrese de que vuelva a colocar el Producto en su empaque original o en un empaque que provea la misma protección que el original. Si compró el Producto en un sitio Web, envíe por correo su recibo original y el Producto a la dirección postal listada en el sitio Web. Asegúrese de colocar el Producto en su empaque original o en un empaque que provea la misma protección que el original.

Para obtener servicio de garantía a domicilio para un televisor con una pantalla de 25 pulgadas o más, llame al 1-888-BESTBUY. El soporte técnico diagnosticará y corregirá el problema por teléfono o enviará un técnico certificado por Dynex a su casa.

¿En dónde es válida la garantía?

Esta garantía sólo es válida al comprador original del Producto en los Estados Unidos y en Canadá.

¿Qué es lo que no cubre la garantía?

Esta garantía no cubre:

- Capacitación del cliente
- Instalación
- Ajuste de configuración
- Daños cosméticos
- Daños debido a actos de la naturaleza, tal cómo rayos
- Accidentes
- Mal uso
- Abuso
- Negligencia
- Uso comercial
- Modificación de alguna parte del Producto
- Un panel de pantalla de plasma dañado por la persistencia de imágenes estáticas (sin movimiento), mostradas por periodos de tiempo extendido (efecto "burn-in").

Esta garantía tampoco cubre:

- Daño debido al uso o mantenimiento incorrecto
- La conexión a una fuente de voltaje incorrecta
- El intento de reparación por alguien que no sea una compañía autorizada por Dynex para reparar el Producto
- Productos vendidos tal cual (en el estado en que se encuentran) o con todas sus fallas
- Productos consumibles, tal cómo fusibles o baterías
- Productos en los cuales el número de serie asignado en la fábrica ha sido alterado o removido

EL REEMPLAZO DE REPARACIÓN SEGÚN PROVISTO BAJO ESTA GARANTÍA ES SU ÚNICO RECURSO. DYNEX NO SERÁ RESPONSABLE POR DAÑOS INCIDENTALES O CONSECUENTES DEBIDO AL INCUMPLIMIENTO DE CUALQUIER GARANTÍA EXPRESA O IMPLÍCITA RELACIONADA CON ESTE PRODUCTO, INCLUYENDO PERO SIN LIMITARSE A LA PÉRDIDA DE INFORMACIÓN, LA PÉRDIDA DE NEGOCIOS O DE GANANCIAS. DYNEX PRODUCTS NO HACE NINGUNA OTRA GARANTÍA EXPRESA E IMPLÍCITA RELACIONADA A ESTE PRODUCTO, INCLUYENDO PERO SIN LIMITARSE A, CUALQUIER GARANTÍA IMPLICITA DE O CONDICIONES DE COMERCIALIZACIÓN O IDONEIDAD PARA UN USO PARTICULAR, ESTÁN LIMITADAS EN DURACIÓN AL PERÍODO DE GARANTÍA DECLARADO ANTERIORMENTE Y NINGUNA GARANTÍA YA SEA EXPRESA O IMPLÍCITA SE APLICARÁ DESPUÉS DEL PERÍODO DE GARANTÍA. ALGUNOS ESTADOS, PROVINCIAS Y JURISDICCIONES NO PERMITEN RESTRICCIONES EN CUANTO A LA DURACIÓN DE UNA GARANTÍA IMPLÍCITA, ASÍ QUE LA RESTRICCIÓN ANTERIOR PUEDE NO APLICARSE EN SU CASO. ESTA GARANTÍA LE DA DERECHOS LEGALES ESPECÍFICOS, Y USTED PUEDE POSEER OTROS DERECHOS QUE VARÍAN DE ESTADO A ESTADO, O DE PROVINCIA A PROVINCIA.

Póngase en contacto con Dynex:

Para servicio al cliente favor llamar al 1-800-305-2204
www.dynexproducts.com

Distribuido por Best Buy Purchasing, LLC
Dynex, 7601 Penn Avenue South, Richfield, Minnesota, U.S.A.

DYNEX®

www.dynexproducts.com (800) 305-2204

07-366
P75505