- 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.
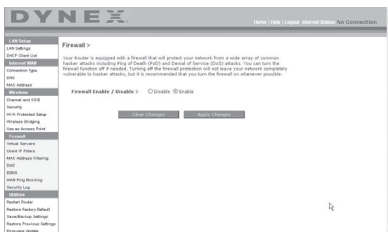
Configuring Internal Forwarding Settings

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.
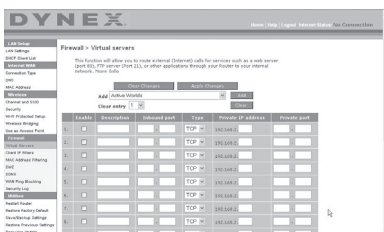

To enter settings into the virtual server:

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.
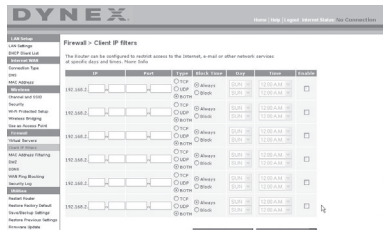

To restrict Internet access to a single computer:
  1 Open the *Firewall > Client IP filters* page, then enter the IP address of the computer you wish to restrict access to in the IP fields.
  2 Enter **80** in both the port fields, select **Both**, then select **Block**. You can also select **Always** 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.
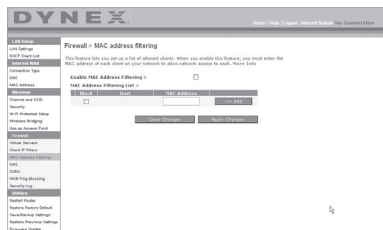
To set MAC Address Filtering:
1. Open the *Firewall > MAC Address filters* page, then click **Enable MAC Address Filtering**.
2. Enter the MAC address of each computer on your network by clicking in the space provided and entering the MAC address of the computer you want to add to the list.
3. Click **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.
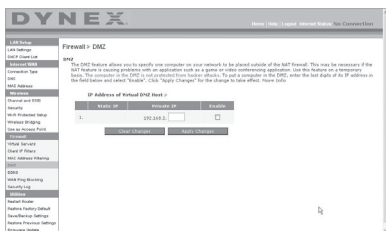
To set up a DMZ for a computer:
- Open the *Firewall > DMZ* page and enter the last digits of the computer's IP address in the **IP field**, click **Enable**, then click **Apply Changes** for the change to take effect.

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.
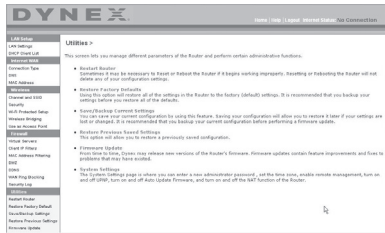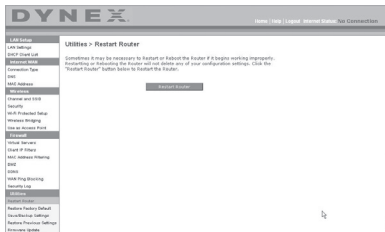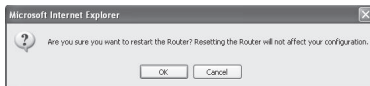

Restarting the router

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.
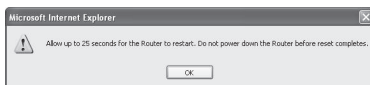
4 Click **OK**. Restarting the router can take up to 25 seconds. It is important not to turn off the power to the router during the restart.

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.
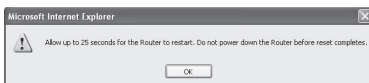
3 Click **OK**. Restoring the defaults includes restarting the router. Restarting the router can take up to 25 seconds. It is important not to turn off the power to the router during the restart.

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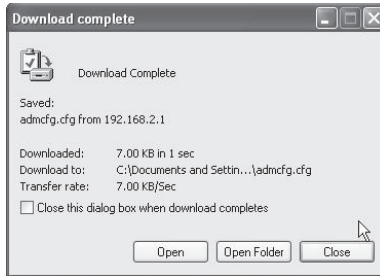
6 Click **Close**. The configuration is now saved.

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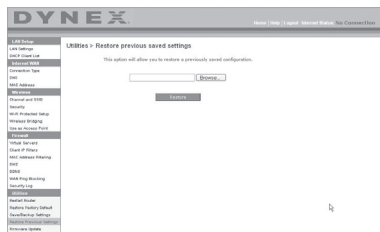
2 Click **Browse**. A window opens that lets you select the location of the configuration file. All configuration files end with a ".bin". Locate the configuration file you want to restore, then double-click on it. The following message opens.

3 Click **OK**. A reminder window appears.
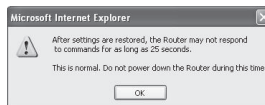
It will take up to 35 seconds for the configuration restoration to complete.

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.
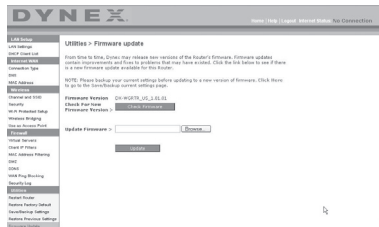
2 Click **Check Firmware**. The utility checks to see if there is an updated version of the firmware available.

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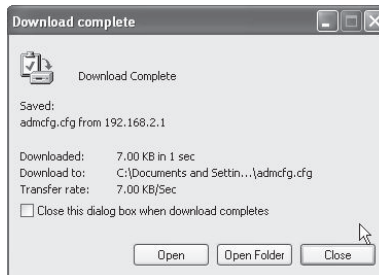
**5** Click **Close**. The download is complete. To update the firmware, follow the steps in **To updating the router's firmware**.

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.
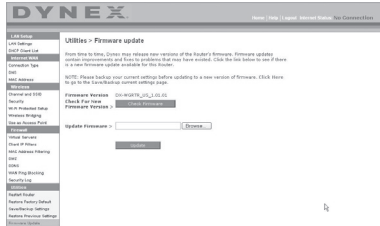
2 Browse to the firmware file you downloaded, then select the file by double-clicking on the file name.
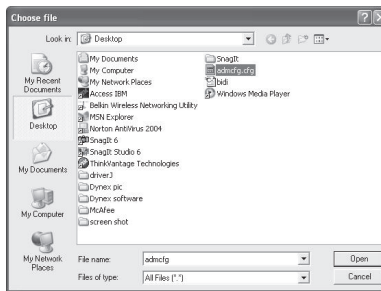
3 The **Update Firmware** box will now display the location and name of the firmware file you just selected. Click **Update**. You will be asked if you are sure you want to continue.
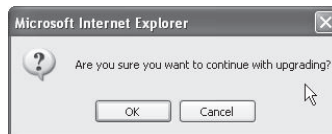
4 Click **OK**. You will see one more message. This message tells you that the router may not respond for as long as one minute as the firmware is loaded into the router and the router is rebooted.
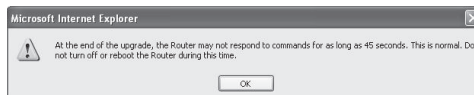
5 Click **OK**. A 60-second countdown will appear on the screen. When the countdown reaches zero, the router's firmware update will be complete. The router's home page should appear automatically. If not, type in the router's address (default = 192.168.2.1) into the navigation bar of your browser.

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

Utilities > System settings

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

- Type in current Password >

- Type in new Password >

- Confirm new Password >

- Login Timeout>   10   (1-99 minutes)

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

Time and Time Zone: July 25 2007   1:58:23 PM
Please set your time Zone. If you are in an area that observes daylight saving check this box. More Info

- Time Zone >   (GMT-08:00) Pacific Time(US, Canada); Tijuana

- Daylight Savings >   ☑ Automatically Adjust Daylight Saving

- Primary NTP Server >   192.43.244.18-NorthAmerica

- Backup NTP Server >   132.163.4.102-NorthAmerica

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

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

☐ Any IP address can remotely manage the router.

- Only this IP address can remotely manage the router>

- Remote Access Port > 8080

Before you enable this advanced feature of your router, MAKE SURE YOU HAVE SET THE ADMINISTRATOR PASSWORD. Remote management allows you to make changes to your router's settings from anywhere on the Internet. There are two methods of remotely managing 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 Enabling:
ADVANCED FEATURE! Allows you to turn the Network Address Translation feature off. In almost every case you would NOT want to turn this feature off. More Info
- NAT Enable / Disable > ◉ Enable ○ Disable

NAT is the method by which 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 Enabling:
ADVANCED FEATURE! Allows you to turn the UPNP feature of the Router on or off. If you use applications that support UPnP, enabling UPnP will allow these applications to automatically configure the router. More Info
- UPNP Enable / Disable > ◉ Enable ○ Disable

UPnP (Universal Plug-and-Play) is yet another advanced feature offered by your router. It is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant. Some applications require 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

Auto Update Firmware Enabling:
ADVANCED FEATURE! Allows you to automatically check the availability of firmware updates for your router. More Info
- Auto Update Firmware
Enable / Disable >   ○ Enable ⊙ Disable

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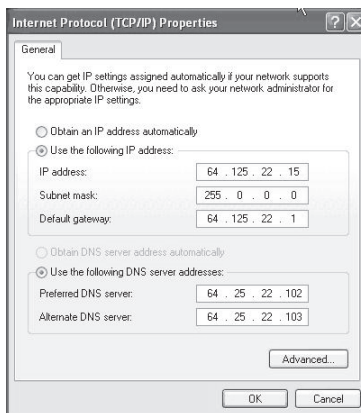
5 If **Use the following IP address** is selected, your router will need to be set up for a static IP connection type. Write the address information down. You will need to enter this information into the router.

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.
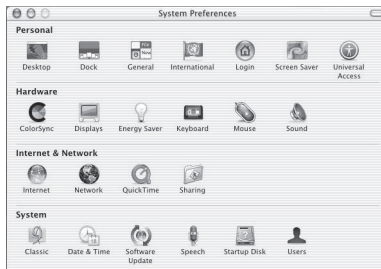
2 Click **Network**. The *Network* window opens.
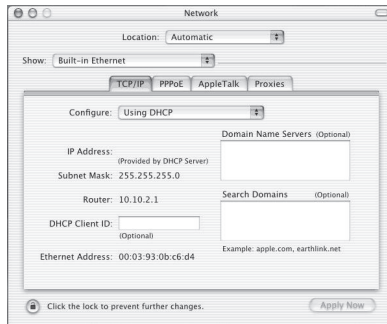
3 Select **Built-in Ethernet** from the **Show** list.
4 Click the **TCP/IP** tab. Next to **Configure:**, you should see **Manually** or **Using DHCP**. If you do not, check the **PPPoE tab** to make sure that **Connect using PPPoE** is NOT selected. If it is, you will need to configure your router 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.
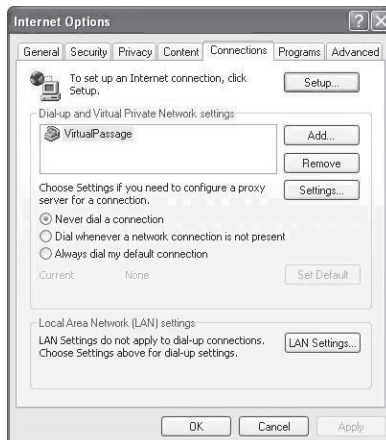
2 Click the **Connections** tab, then select **Never dial a connection**. If you cannot make a selection, go to the next step.

3 Click **LAN Settings…**. The *LAN Settings* page opens.
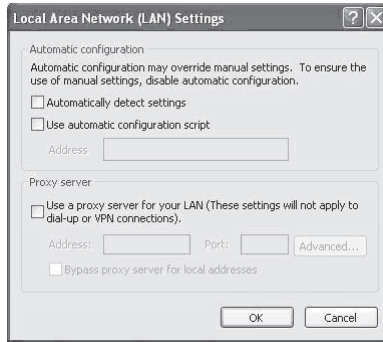
4 Make sure there are no check marks next to any of the displayed options. Click **OK** to close the page, then click **OK** again in the *Internet Options* page to exit.

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.
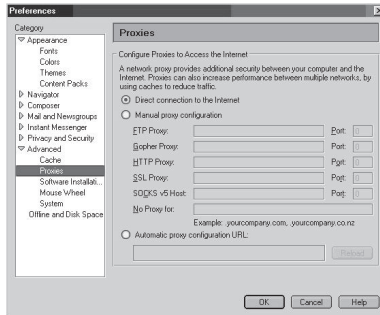
2 Click **Advanced**, then click **Proxies**.

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-typically 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

DYNEX® is a registered trademark of Best Buy Enterprise Services, Inc.
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
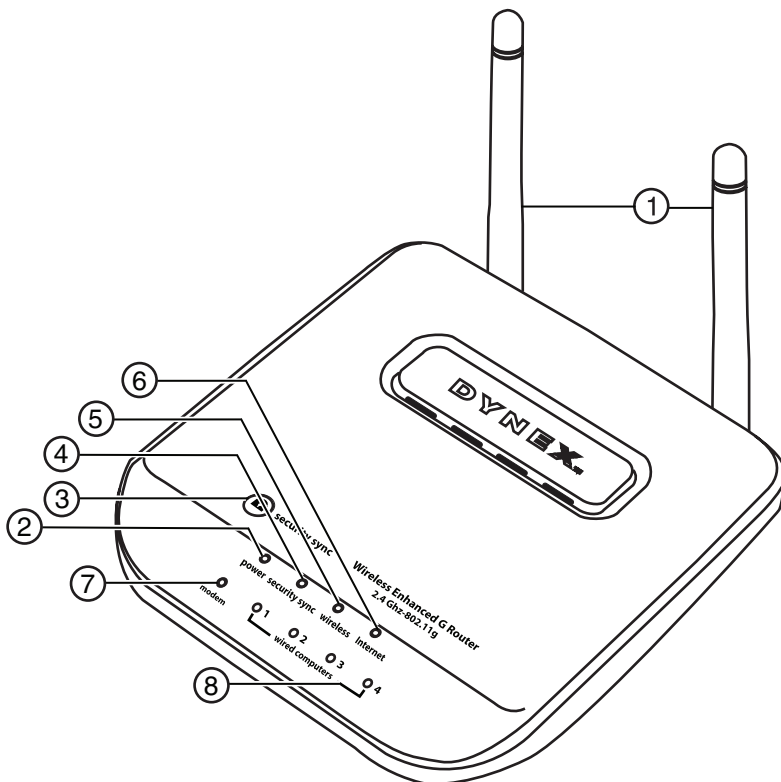- Navigateur Internet

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.
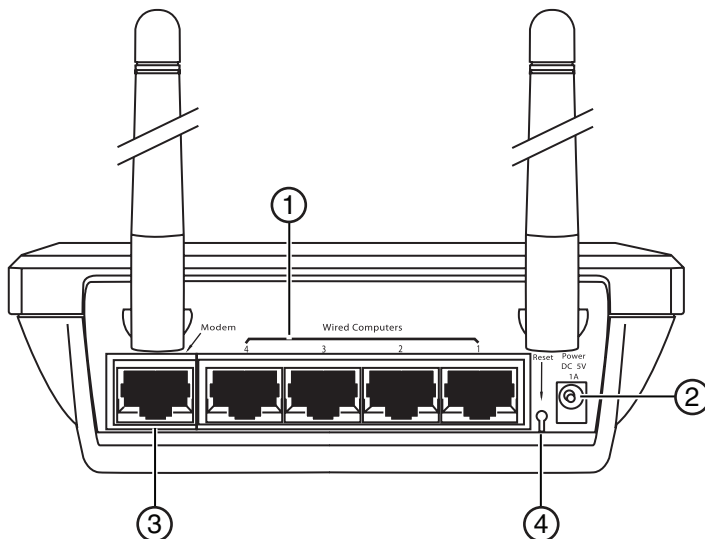
Panneau avant

#	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.