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 173 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".*

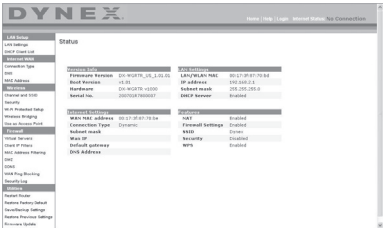
2. Para efectuar cambios en los ajustes del enrutador, deberá iniciar la sesión. Haga clic en **Login** (Iniciar sesión), o en cualquiera de los enlaces de la página principal para ir a la pantalla de inicio de sesión.
3. En la pantalla de iniciar sesión, deje la contraseña en blanco (el enrutador es 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 170.

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)

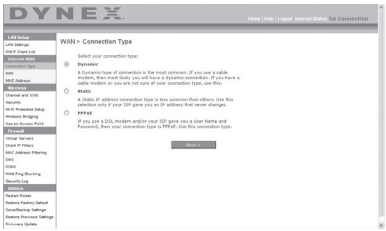
La ficha **Internet/WAN** es donde configurará su enrutador para conectar con su proveedor de servicios de Internet (ISP). El enrutador es capaz de conectarse prácticamente al sistema de cualquier ISP siempre que las configuración del enrutador haya sido configurada correctamente para el tipo de conexión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

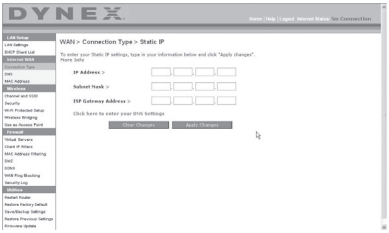
Cambiar la dirección MAC de WAN

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

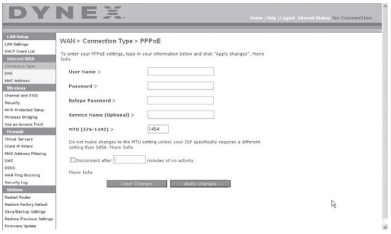
Una dirección IP estática es un tipo de conexión menos frecuente que los otros tipos de conexiones. Si su ISP emplea direccionamiento IP estático, necesitará su dirección IP, máscara de subred y dirección de puerta de enlace del ISP. Esta información puede obtenerla de su ISP o la puede encontrar en 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:

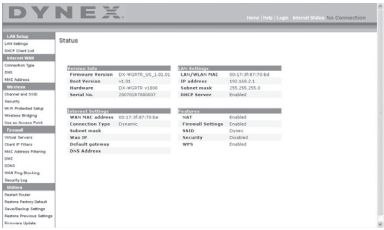
1. Asegúrese de que está utilizando la computadora que se encontraba ORIGINALMENTE CONECTADA a su módem antes de la instalación del enrutador. Haga clic en
2. Haga clic en **Clone** (Clonar) y luego en **Apply Changes** (Aplicar cambios). Su dirección MAC ha sido ahora clonada en el enrutador.

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.

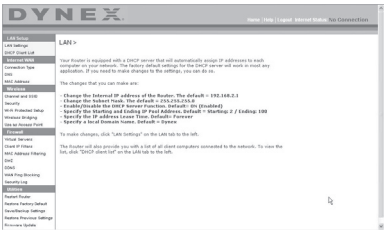
Usando la interfaz de usuario avanzada de Web

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.



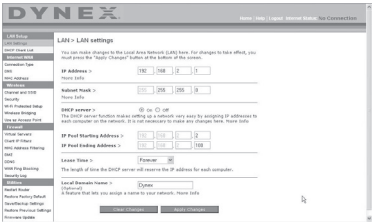
Viendo la configuración de LAN

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).

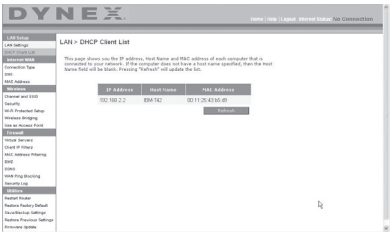
IP Pool (Conjunto de IP) – La gama de direcciones IP reservadas para la asignación dinámica a las computadoras de su red. El valor predefinido es 2 - 100 (99 computadoras) Si desea modificar este valor, puede hacerlo introduciendo una nueva dirección IP de inicio y final y haciendo clic en **Apply Changes** (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".

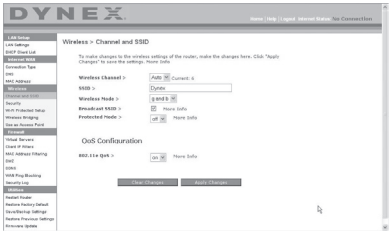
Viendo la página de la lista de clientes DHCP

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.

Cuándo utilizar 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.

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.

	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 WEP – 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)

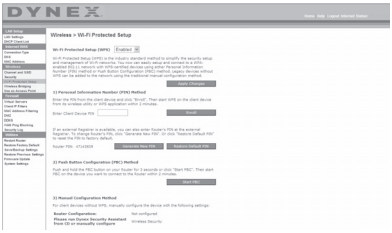
Su enrutador está equipado con el último estándar de seguridad, llamado *Wi-Fi Protected Access* (Acceso Wi-Fi protegido, WPA2) y con el común estándar de seguridad llamado *Wired Equivalent Privacy* (Privacidad equivalente por cable, WEP). Su enrutador también soporta la especificación *Wi-Fi Protected 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 las segunda generación de la norma 802.11 basada en la 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.

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 la A a la F y del 0 al 9. Para WEP de 64 bits deberá introducir 10 claves 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 o el punto de acceso desde una computadora con un cliente inalámbrico, necesitará asegurarse de que la seguridad esté ACTIVADA 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 (Inalámbrico) > Security (Seguridad)*
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 la A a la F y del 0 al 9. Para WEP de 128 bits deberá introducir 26 claves 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 o el punto de acceso desde una computadora con un cliente inalámbrico, necesitará asegurarse de que la seguridad esté ACTIVADA 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 para computadora de sobremesa o para PC 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:

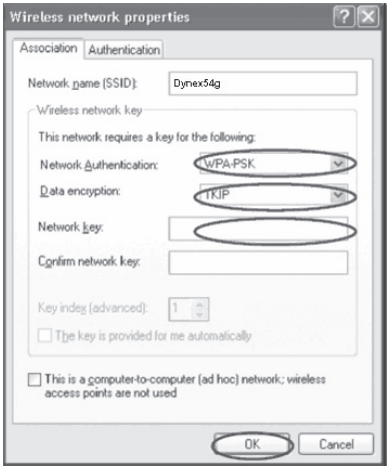
1 En Windows XP, haga clic en **Start** (Inicio), **Control Panel** (Panel de control), **Network Connections** (Conexiones de red).

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.

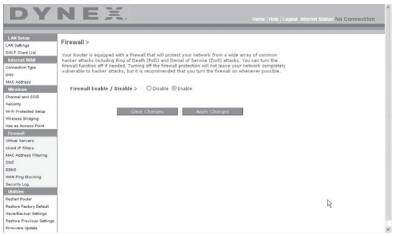
Configuración del firewall

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)

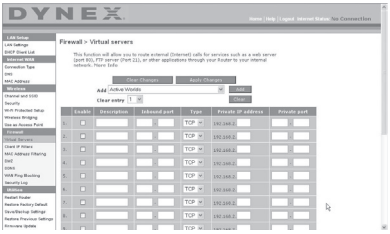
El firewall también protege puertos comunes que son empleados con frecuencia para atacar redes. Estos puertos aparecen como *Stealth* (Invisibles), lo que significa que, para cualquier intento y propósito, estos puertos no existen ante un posible pirata informático Si lo necesita,

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:

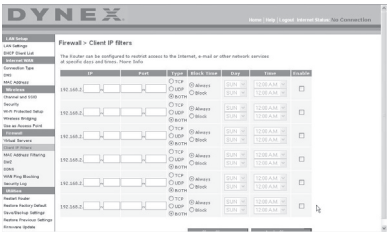
1. Abra la página *Virtual Servers* (Servidores virtuales) e introduzca la dirección IP en el espacio previsto para la máquina interna (servidor) y el(los) puerto(s) que se den pasar.
2. Seleccione el tipo de puerto (TCP o UDP), marque la casilla de verificación **Enable**(Activar) y haga clic en **Apply 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.

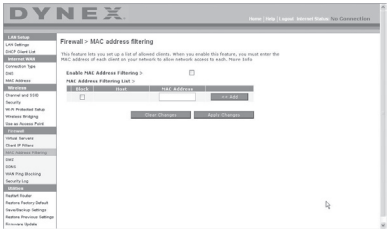


Para restringir el acceso Internet a una única computadora:

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)

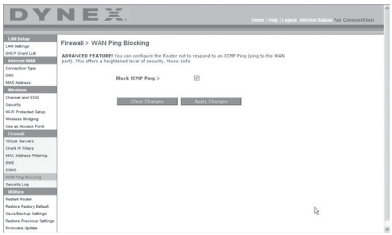
La característica DMZ le permite especificar una computadora de su red para ser colocada fuera del firewall. Esto puede ser necesario en el caso de que el firewall esté causando problemas con una aplicación como, por ejemplo, una aplicación de juegos o de videoconferencias. Utilice esta característica 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.

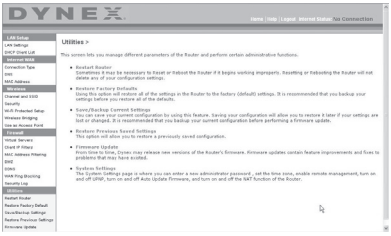


Para apagar la respuesta al ping

- 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.

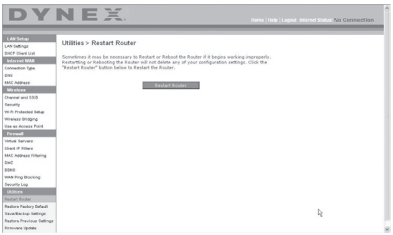


Reiniciando el enrutador

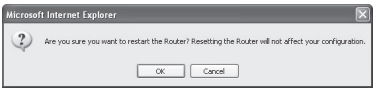
Algunas veces es posible que sea necesario reiniciar el enrutador en caso de que comience a funcionar mal. Al reiniciar el enrutador NO se borrará ninguno de sus ajustes de configuración.

Para reiniciar el enrutador para restablecer el funcionamiento:

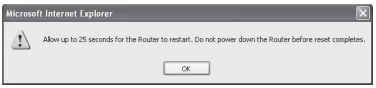
1. Haga clic en **Utilities** (Aplicaciones) situado en el menú de la izquierda y luego haga clic en **Restart Router** (Reiniciar enrutador). Se abrirá la página *Restart Router* (Reiniciar enrutador).



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.

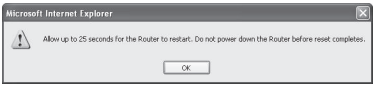
Restablecimiento de los ajustes predefinidos de fábrica

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.

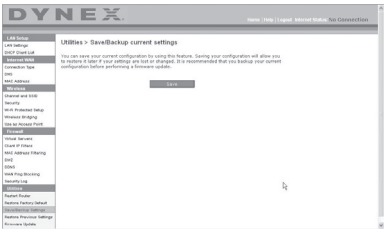
Aparecerá una cuenta regresiva de 25 segundos en la pantalla. Cuando la cuenta regresiva llegue a cero, el enrutador habrá sido reiniciado. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del enrutador (predefinido = 192.168.2.1) en la barra 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).

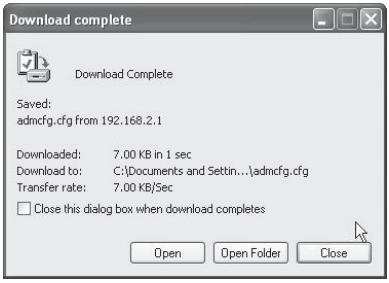


2 Haga clic en **Save** (Guardar). Se abrirá la ventana de descarga de archivos.

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.



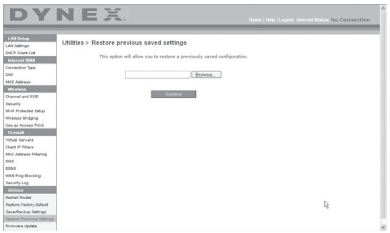
6 Haga clic en **Close** (Cerrar). La configuración ha sido guardada.

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.

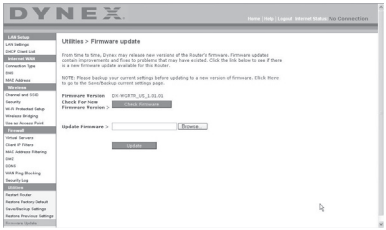
4 Haga clic en **OK** (Aceptar). Aparecerá una cuenta regresiva de 35 segundos en la pantalla. Cuando la cuenta regresiva llegue a cero, la configuración del enrutador habrá sido restablecida. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección del 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.

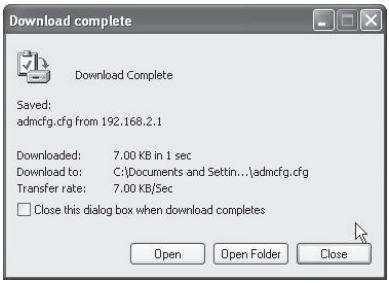


2 Haga clic en **Check Firmware** (Verificar firmware). La aplicación verificará si existe una versión actualizada del firmware disponible.

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.*

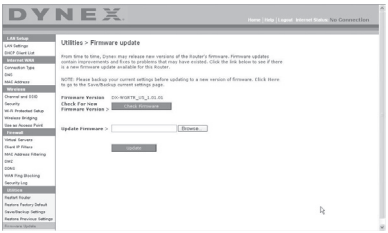
4 Cuando el proceso de almacenamiento se haya completado, verá la siguiente ventana.



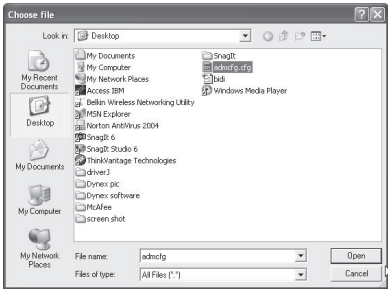
5 Haga clic en **Close** (Cerrar). La descarga se ha completado. Para actualizar el firmware, siga los pasos en la sección **Para actualizar el firmware del enrutador**.

Para actualizar el firmware del enrutador:

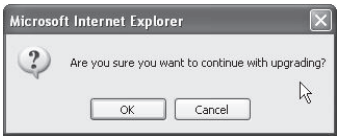
1 En la página *Firmware Update* (Actualización del firmware), haga clic en **Browse** (Examinar). Se abrirá una ventana que le permitirá seleccionar la ubicación del archivo de actualización del firmware.



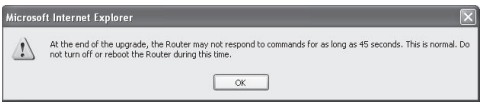
2 Navegue hasta llegar al archivo de firmware descargado y seleccione el archivo haciendo doble clic en el nombre del mismo.



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.



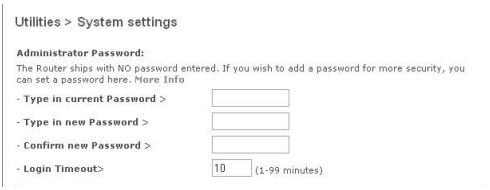
5 Haga clic en **OK** (Aceptar). Aparecerá una cuenta regresiva de 60 segundos en la pantalla. Cuando la cuenta atrás llegue a cero, la actualización del firmware del enrutador habrá sido completada. La página principal del enrutador deberá aparecer automáticamente. En caso contrario, ingrese la dirección 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

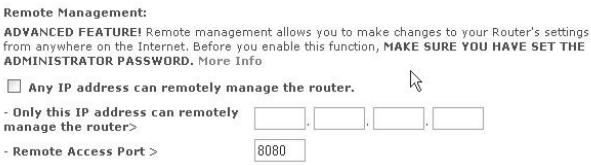
La opción de tiempo límite de sesión le permite establecer el periodo de tiempo que podrá permanecer en la interfaz de configuración avanzada del enrutador. El temporizador arranca cuando no existe actividad. Por ejemplo, usted ha efectuado algunos cambios en la interfaz de configuración avanzada y después 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.

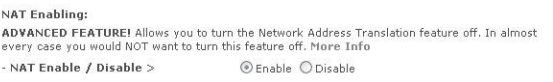
Activando la gestión remota



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.

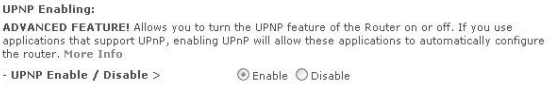
Activando/Desactivando la traducción de direcciones de red (NAT)

***Nota**: Esta característica deberá ser modificada exclusivamente por usuarios avanzados.*



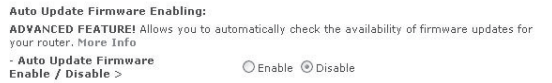
La traducción de direcciones de red (NAT) es el método en el que el enrutador comparte la única dirección IP asignada por su ISP con el resto de computadoras de la red Esta función deberá ser desactivada únicamente si su ISP le asigna múltiples direcciones IP o si necesita desactivar NAT para una configuración 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



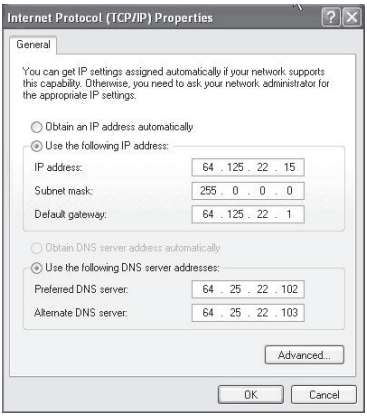
Esta innovación proporciona al enrutador la capacidad integrada de buscar automáticamente una nueva versión del firmware y de informarle de que está disponible una nueva versión. Cuando acceda a la interfaz avanzada del enrutador, éste efectuará una búsqueda para comprobar si está disponible una nueva 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.

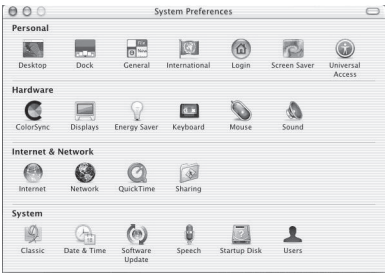
4 Si no se encuentran seleccionadas, haga clic en **Obtain an IP address automatically** (Obtener una dirección IP automáticamente) en la ficha **IP Address** (Dirección IP) y haga clic en **OK** (Aceptar).

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.

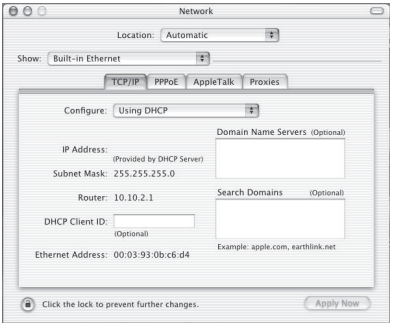
Configure la computadora que está conectada al módem de cable o DSL utilizando PRIMERO los siguientes pasos. Asimismo, puede emplear estos pasos para añadir computadoras a su enrutador una vez que éste haya sido configurado para conectarse a Internet.

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 Haga clic en **Using DHCP** (Usando 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.