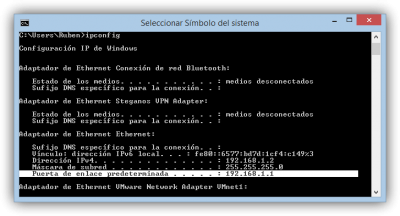
Cómo acceder a la configuración web del router

La forma más sencilla de configurar un router es hacerlo a través del servidor web que incluye. Esto ofrece una interfaz accesible desde cualquier navegador web de manera que desde allí podemos configurar la mayor parte de los aspectos básicos de este.

Para acceder a nuestro router simplemente debemos introducir en nuestro navegador la dirección IP del mismo que, generalmente, suele coincidir con la de la puerta de enlace. Para conocer esta dirección IP podemos abrir una ventana de MS-DOS en Windows y teclear:

* ipconfig

Aquí buscaremos la dirección IP de la puerta de enlace y la introduciremos para acceder a esta web de configuración.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-1.png)

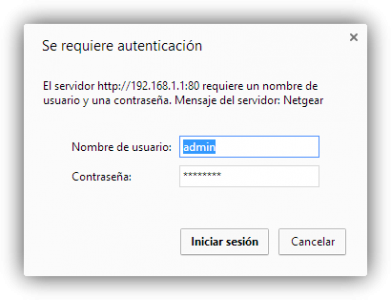
Contraseñas más utilizadas

Generalmente los routers vienen protegidos con contraseña para evitar que usuarios no autorizados puedan acceder a ellos. Si hemos cambiado la contraseña y no la sabemos debemos reiniciar obligatoriamente el router a los valores de fábrica para que se configuren, entre otras cosas, las contraseñas por defecto.

En cuanto a contraseñas por defecto, las más utilizadas por la mayoría de los routers son:

* admin/
* /admin
* admin/admin
* 1234/admin
* admin/1234
* 1234/234

Si ninguna de ellas funciona debemos consultar el manual o la pegatina de la parte inferior donde suelen venir escritas.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-2.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-3.png)

Configurar el Wi-Fi de nuestro router de forma segura y optimizada

Seguridad

Para evitar que los usuarios se conecten a nuestro punto de acceso y puedan navegar a través de Internet con nuestra conexión debemos configurar una serie de medidas de seguridad.

Lo primero que debemos hacer es elegir el tipo de cifrado que vamos a utilizar. No podemos dejar la red abierta porque cualquiera se conectaría a ella y nuestro tráfico no se cifraría ni tampoco utilizar un algoritmo sencillo de explotar que permita a usuarios con conocimientos obtener nuestra contraseña.

La mejor opción que debemos elegir en el apartado de cifrado es:

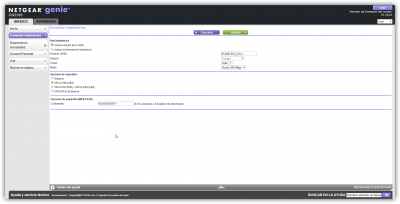
* WPA2-PSK [AES]

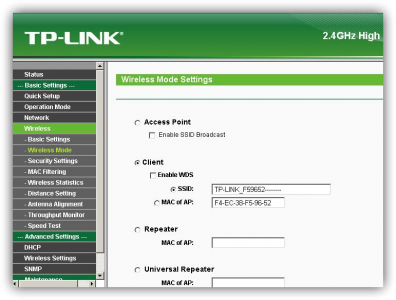
Una vez seleccionado este tipo de cifrado podemos configurar la clave de acceso. Al haber seleccionado una seguridad WPA2 la contraseña puede tener los caracteres que queramos, tanto mayúsculas como minúsculas o símbolos. Por ejemplo:

* ##ConTR4s3Na\_dMi\_RuT3r1990##

Cuanto más compleja sea la contraseña y sencilla de recordar para uno mismo, mejor.

Algunos puntos de acceso ofrecen la posibilidad de configurar WPA2 TKIP + AES. Esto implica que los dispositivos que sean compatibles con WPA2 utilizarán este tipo de cifrado para conectarse, pero los que no lo sean utilizarán el cifrado TKIP, correspondiente a WPA y menos seguro que el WPA 2. Si todos nuestros dispositivos son compatibles con WPA2 y AES debemos dejar esta opción seleccionada, sin TKIP.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-4.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-12.png)

¿2.4Ghz o 5Ghz?

En cuanto a la frecuencia, si nuestro router y todos los dispositivos conectados a él soportan la tecnología de 5Ghz debemos utilizar esta ya que tiene muchos menos dispositivos que la utilizan (la red de 2,4Ghz está en muchos lugares saturada de dispositivos que se conectan en un área cercana por Wi-Fi a otros puntos de acceso), ofrece una mayor cobertura, una mayor velocidad y una mejor estabilidad, sin embargo, si alguno de nuestros dispositivos no soporta esta frecuencia no podrá conectarse a Internet, por lo que entonces debemos configurar la red a 2.4Ghz y elegir el canal menos saturado.

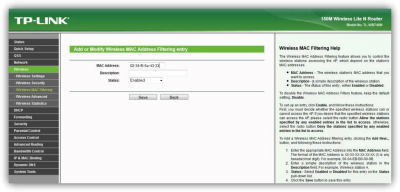
La mayoría de los routers actuales cuentan con un análisis automático de canal de manera que ellos mismos elegirán el menos saturado para trabajar.

Filtrado MAC

Algunos modelos permiten configurar un «Filtrado MAC» que analiza todas las direcciones MAC que se conectan al punto de acceso y permite o bloquea el acceso según la configuración.

Si nuestro AP dispone de esta función podemos añadir a la «lista blanca» las direcciones MAC de nuestros dispositivos configurando este filtrado de manera que sólo puedan conectarse a Internet aquellas direcciones MAC incluidas en la lista blanca, quedando todas las demás (por ejemplo usuarios no autorizados) con el acceso bloqueado.

[](http://www.adslzone.net/app/uploads/2014/01/wifi-11.png)

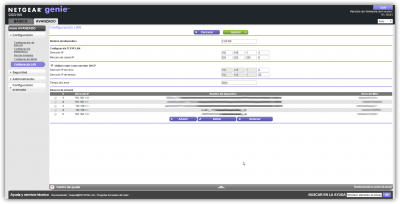
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-13.png)

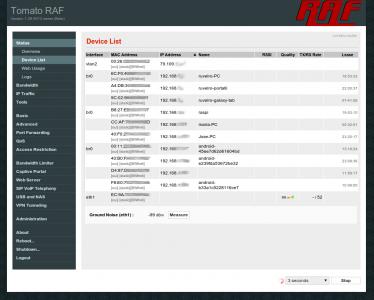
Configurar el servidor DHCP

Todos los routers y puntos de acceso disponen de un servidor DHCP. Este servidor se encarga automáticamente de dar una dirección IP de un rango especificado a cada dispositivo que se conecta junto a la máscara de subred, puerta de enlace y [servidores DNS.](https://www.adslzone.net/dns.html)

Por defecto tanto los puntos de acceso como los sistemas operativos estarán configurados para obtener una IP a través de este servidor siendo cada vez una diferente dentro del rango, sin embargo, podemos configurarlo de manera que asociemos una dirección MAC a una IP fija, quien siempre obtendrá dicha IP automáticamente desde este servidor.

Si queremos poder abrir los puertos de nuestro router y no tener problemas con las direcciones IP debemos configurar correctamente este servidor DHCP o configurar nuestro ordenador o dispositivo con una IP fija.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-5.png)

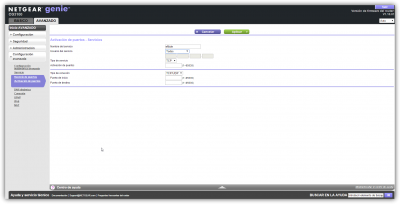
[[](http://www.adslzone.net/app/uploads/2013/10/DHCP.jpg)](http://www.adslzone.net/app/uploads/2013/10/DHCP.jpg)

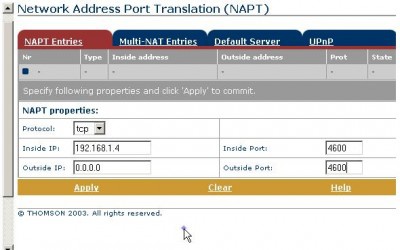
Abrir puertos

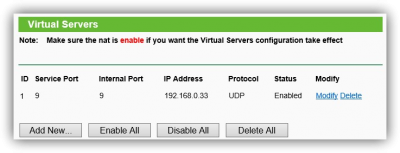
Abrir los puertos es una de las acciones más solicitadas por los usuarios. Los puertos generalmente se utilizan para establecer conexiones de diferentes aplicaciones con los correspondientes servidores remotos para poder funcionar, por ejemplo, un cliente torrent para poder descargar o un juego online para poder conectarse con el servidor de dicho juego.

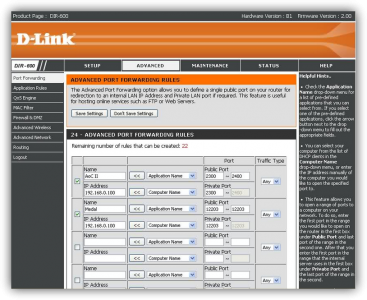
Cada aplicación suele utilizar un puerto único comprendido entre 0 y 65535, aunque los primeros 1024 están reservados para aplicaciones elementales y no deben utilizarse (por ejemplo el puert0 80 es el HTTP, el 443 HTTPS, 21 FTP, 22 SSH, etc).

Si queremos que nuestra conexión funcione bien debemos abrir en nuestro router los puertos que utilice la aplicación que vamos a utilizar vinculando cada puerto a la dirección IP de nuestro ordenador.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-6.png)

[](http://www.adslzone.net/app/uploads/2013/10/puertos21.jpg)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-14.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-15.png)

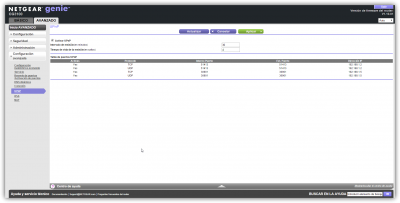
Podemos conocer la IP de nuestro ordenador fácilmente tecleando en una ventana de MS-DOS:

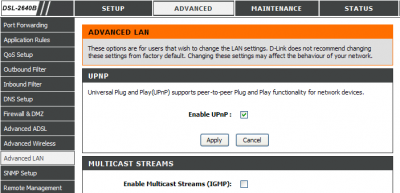
* ipconfig

Debemos asociar el puerto (o rango de puertos) a la IP de nuestro ordenador, aunque debemos tener en cuenta que si utilizamos un servidor DHCP esta puede variar.

UPnP

Algunos modelos de routers vienen por defecto con un servidor UPnP. Este servidor es el encargado de que las comunicaciones se llevan a cabo correctamente sin tener que preocuparse de los puertos (ya que él se encarga de redirigir el tráfico) abriendo las conexiones cuando sea necesario y cerrándolas cuando ya no se necesiten.

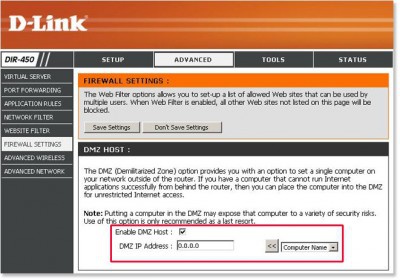
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-7.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-16.png)

Para que las conexiones UPnP funcionen correctamente el programa que intenta acceder a la red también debe ser compatible con esta tecnología.

DMZ

DMZ, o Zona Desmilitarizada es una opción que incluyen algunos modelos de routers que es capaz de situar un dispositivo en una zona diferente con acceso directo a Internet. Con esto el efecto es similar a «tener todos los puertos abiertos» y «no tener ninguna restricción por parte del firewall», siendo eficaz tanto para descargar sin restricciones ni bloqueos, así como para jugar con total libertad.

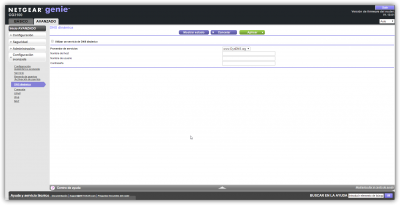
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-17.jpg)

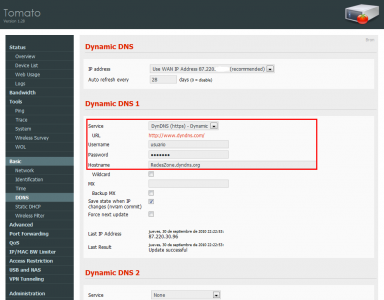
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-18.jpg)

Esta configuración es recomendable, por ejemplo, para videoconsolas ya que estas generalmente no corren riesgo de ser víctimas de un malware ni de ataques informáticos, pero no debemos configurar la IP de un ordenador en la DMZ ya que estaría completamente expuesto a las amenazas de Internet.

Configurar un servidor DDNS

Los usuarios que necesitan conectarse desde fuera de casa a sus ordenadores o recursos pueden optar por configurar un servidor DDNS o Dynamic Domain Name Server. Esto permite que nuestra dirección IP, aunque sea dinámica, esté siempre actualizada y vinculada a un dominio del estilo: mi\_nombre.no-ip.org.

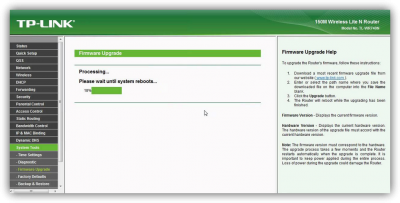
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-8.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-19.png)

Algunos modelos de routers vienen por defecto con esta función, por lo que si tenemos un DDNS podemos habilitarlo en nuestro router de manera que se actualice automáticamente siempre que nuestra dirección IP cambie.

Actualizar el Firmware

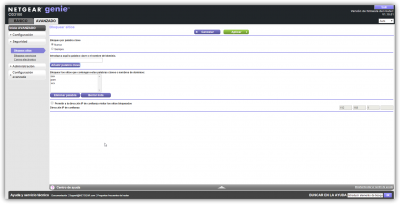
El firmware de un router es lo que generalmente conocemos como sistema operativo. Este suele recibir actualizaciones periódicamente en las que se incluyen nuevas funciones y características a la vez que corrige importantes fallos de seguridad que pueden aparecer con el tiempo, por lo que es de vital importancia mantener siempre las versiones más actualizadas de cara a poder navegar seguros por la red.

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-20.png)

Algunos modelos de router se actualizan automáticamente según están conectados a Internet, sin embargo, otros deben actualizarse manualmente descargando previamente el firmware al ordenador y desde allí enviarlo al router para que se apliquen los cambios.

Configurar un control parental

El control parental permite bloquear ciertas páginas web no apropiadas para menores e incluso filtrar ciertas palabras para que en caso de encontrar una web con dichos contenidos, esta no llegue a establecerse.

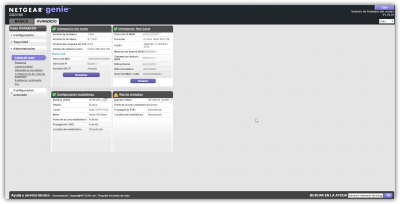
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-11.png)

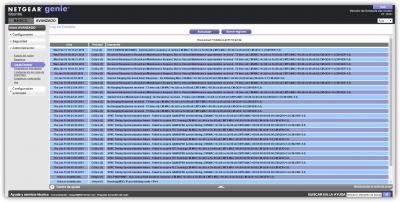
[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-23.jpg)

Para aquellos padres que tienen menores bajo su responsabilidad esta opción podrá ayudar (aunque no es 100% eficaz) a que el menor no acceda a páginas web no recomendadas para él quedando bloqueadas en el router y registradas en el registro del propio router.

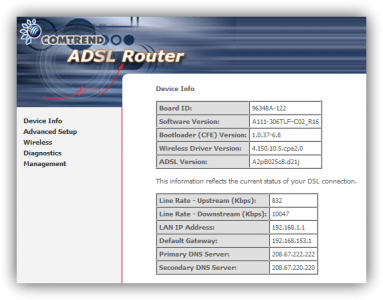
Comprobar los eventos del router  y el estado del mismo

Generalmente estos dispositivos suelen contar con un completo registro de eventos donde podremos consultar todo lo que ocurre en él, por ejemplo, intentos de acceso no autorizados, acceso a páginas web bloqueadas, asignaciones de direcciones DHCP a los dispositivos conectados, problemas de conexión, etc.



[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-10.png)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-21.gif)

[](http://www.adslzone.net/app/uploads/2015/02/C%C3%B3mo-configurar-un-router-de-forma-correcta-foto-22.png)