

Seguridad en redes inalámbricas (Recopilado de Internet)

Primero vamos a explicar una serie de conceptos básicos:

SSID: Nombre de nuestra WLAN (red inalámbrica). Los puestos que deseen conectar por wireless al router, tienen que conocer este nombre y colocarlo en el apartado correspondiente de su configuración wireless.

ESSID Broadcast: Hace que nuestro SSID sea público, es decir, cualquiera que entre dentro del radio de acción de nuestro router, podrá ver nuestro **SSID** (Y conectarse a nuestra **WLAN** si no utilizamos **encriptación**).

Dirección MAC: Es un número que identifica a cada una de las tarjetas de red.



Filtrado de direcciones MAC: Permite especificar qué ordenadores pueden entrar en la red. Cuando se active esta característica, hay que introducir las direcciones MAC de cada cliente de la red (tarjeta inalámbrica) para permitirles el acceso a la red.

MEDIDAS DE SEGURIDAD RECOMENDADAS.

Si vamos a utilizar el router solamente mediante cable debemos desactivar la característica wireless del router. Esto lo haremos en el apartado **Wireless**, Esta es la medida más drástica que podemos tomar, pero normalmente tendremos este router para montar una red inalámbrica.

Las acciones que vamos a describir a continuación se pueden realizar independientemente unas de otras según nuestras necesidades de seguridad a la hora de configurar la red inalámbrica. También se pueden usar varias de ellas en combinación o incluso todas juntas

1.- Cambiar las claves de acceso por defecto al router.



Para evitar accesos indeseados al router es imprescindible cambiar las claves por defecto, así que cambiaremos el nombre de usuario y la contraseña. Para ello vamos al menú **Administration**. Debe quedar claro que esto evita que alguien acceda a la configuración de nuestro router.

En **Gateway Username (nombre de usuario)** pondremos otro que no sea **admin**.

También cambiaremos el campo **Gateway Password**. Para activar los cambios iremos a la parte inferior y pulsaremos **Save Settings (guardar configuración)**. La próxima vez que entremos a la configuración deberemos usar las nuevas claves.

2.- Desactivar SSID Broadcast (Difusión). Nombre de nuestra red.

Siendo uno de los datos que es necesario para poder conectar a nuestra red es importante no estar divulgándolo de manera tan evidente. Incluso sería necesario cambiarle el nombre, puesto que los programas habituales de búsqueda de redes son capaces de identificar la marca del router, y por tanto deducir el nombre por defecto.

Por tanto en **Wireless Network Name (SSID)**, pondremos otro diferente al definido por defecto.

En **Wireless SS ID Broadcast** marcaremos la opción **Disabled**.
Para guardar los cambios, pulsar **Save Settings (guardar configuración)**.

Ahora, para agregar un nuevo puesto (o sea un nuevo usuario) a nuestra red wireless tendremos que introducir a mano en cada una de las computadoras que quieran conectarse.

3.- Desactivar el servidor DHCP.

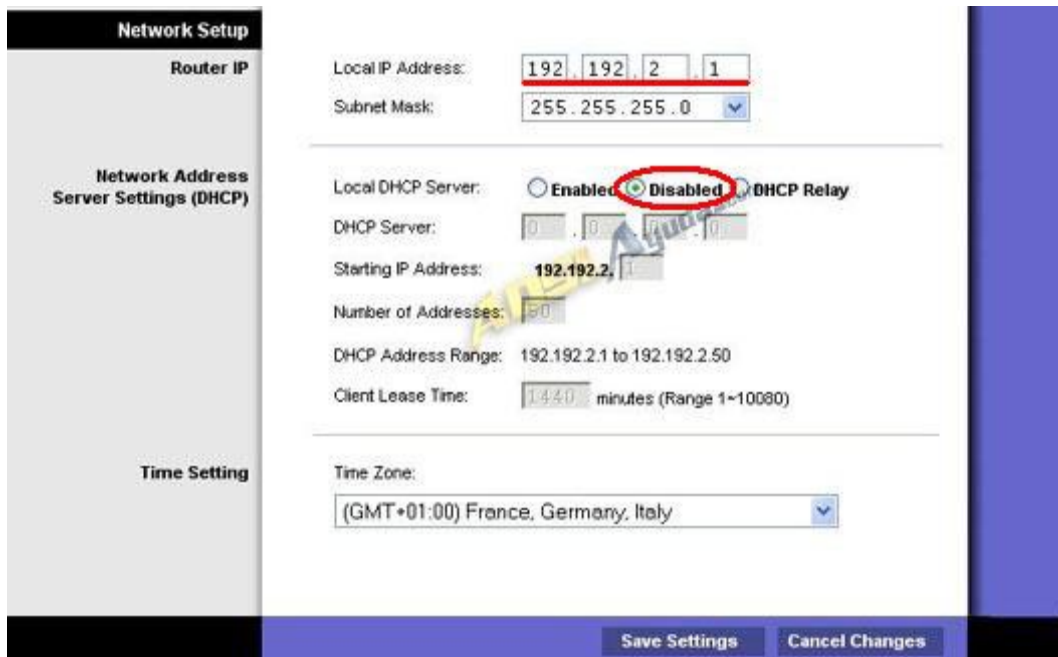
Si tenemos esta opción activada cualquier ordenador que tenga su tarjeta de red configurada en "**Obtener una ip automáticamente**" tendrá acceso a nuestra red. Sería conveniente no sólo desactivar esta opción sino, también, cambiar la **ip local que trae el router por defecto**, ya que siendo **192.168.1.1**, es demasiado evidente.

Esto lo haremos en el menú de configuración básico, **Basic Wireless Settings**, en la parte inferior del mismo, en la sección **Network Setup**.

Para desactivar el servidor **DHCP**, pondremos el campo **Local DHCP Server en Disabled**.



Para cambiar la **IP local** del router, pondremos los campos de **Local IP Address** en los valores que deseemos para nuestra red local. Evidentemente, tendremos que cambiar también la configuración de red de los ordenadores. Si el router lo colocamos en (192.192.2.1), tendremos que cambiar las IPs locales en 192.192.2.2, 192.192.2.3, y sucesivas.



4.- Filtrado de direcciones MAC.

Cada tarjeta de red posee una dirección **MAC (Media Access Control)**, que en teoría es única para cada una de ellas.

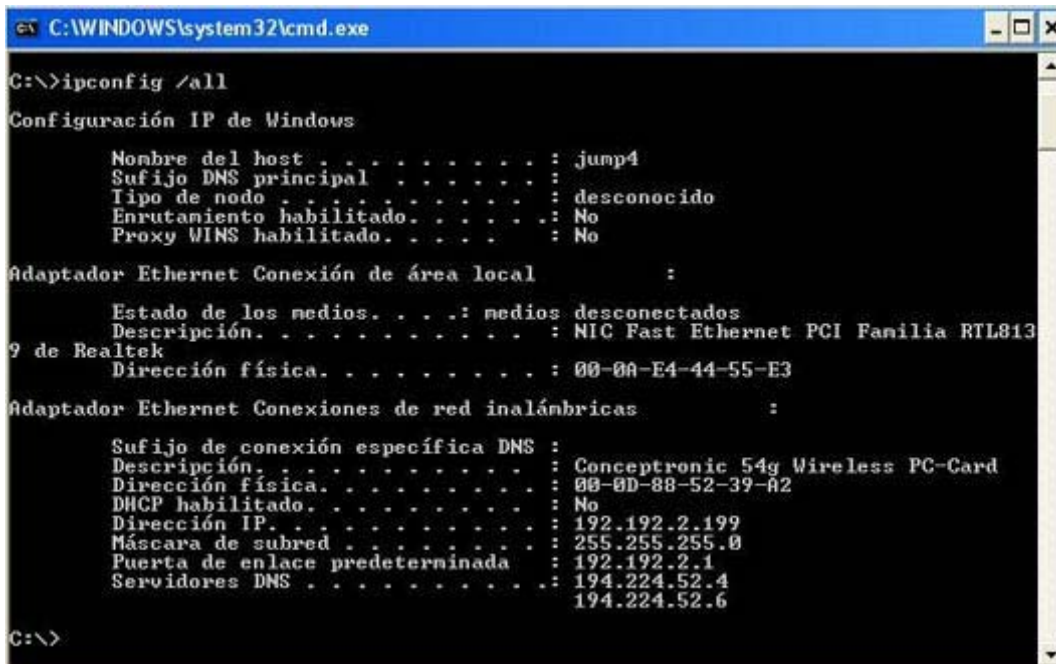
Está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (cada pareja se separa de otra mediante dos puntos ":" o mediante guiones "- "). Por ejemplo, una dirección MAC podría ser **E1:B1:CF:3D:4A:AA**.

Normalmente la MAC viene impresa en la tarjeta de red, aunque también se puede consultar mediante el comando `ipconfig /all` en ms-dos. Para consultar la dirección MAC de los equipos, por tanto, habrá que hacer lo siguiente:

En **Windows 98** pulsamos en **Inicio -> Ejecutar -> command**. Se abrirá la ventana del intérprete MS-DOS. Introducimos el comando **winipcfg**. En el desplegable del cuadro que aparece debemos seleccionar nuestro adaptador de red.



En **Windows 2000 o XP** pulsamos en **Inicio -> Ejecutar -> cmd**.
Se abrirá la ventana del intérprete MS-DOS, en la que introducimos el comando **ipconfig /all**.



```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : jump4
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexión de área local :

Estado de los medios. . . . . : medios desconectados
Descripción. . . . . : NIC Fast Ethernet PCI Familia RTL813
9 de Realtek
Dirección física. . . . . : 00-0A-E4-44-55-E3

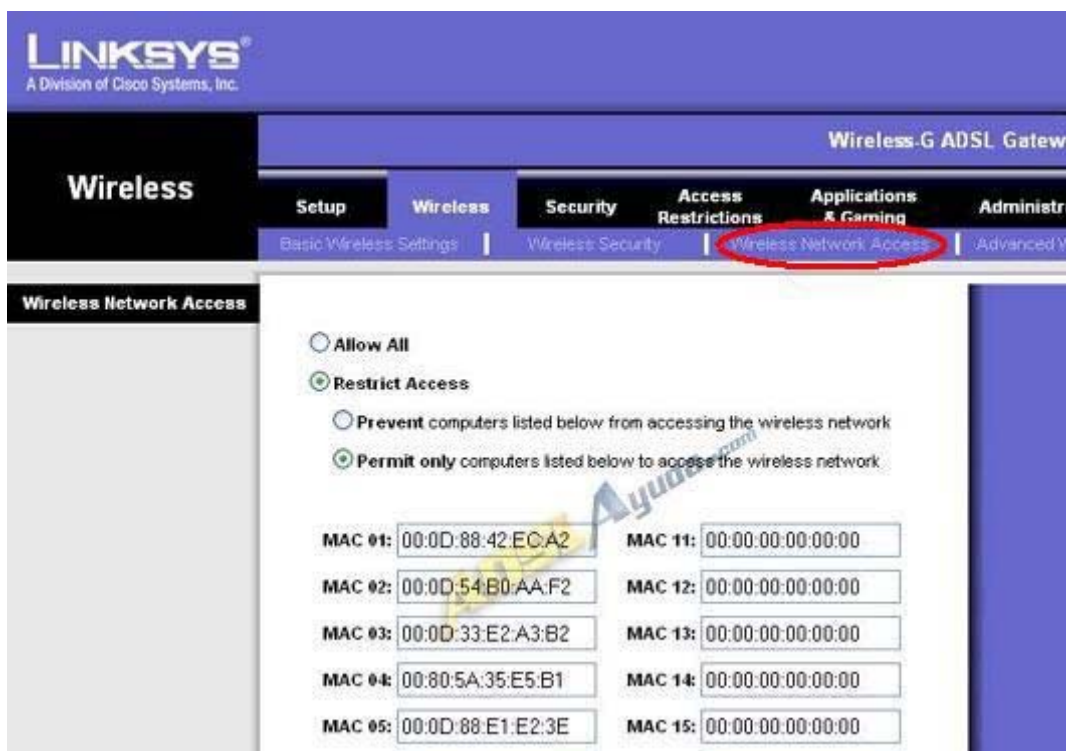
Adaptador Ethernet Conexiones de red inalámbricas :

Sufijo de conexión específica DNS :
Descripción. . . . . : Conceptronic 54g Wireless PC-Card
Dirección física. . . . . : 00-0D-88-52-39-A2
DHCP habilitado. . . . . : No
Dirección IP. . . . . : 192.192.2.199
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.192.2.1
Servidores DNS . . . . . : 194.224.52.4
                            194.224.52.6

C:\>
```

Al activar el **filtrado de direcciones MAC** del router estamos autorizando el acceso al mismo únicamente a las tarjetas de red que introduzcamos en la lista.

Iremos al **menú Wireless** y dentro de él, al apartado **Wireless NetWork Access**.



Debemos activar la casilla **Restrict Access** y después **Permit Only computers**... A continuación iremos introduciendo las direcciones MAC de los ordenadores de nuestra red.

Para dar de alta una nueva dirección MAC de algún ordenador que queramos añadir a la red, deberemos acceder al router a través de alguno de los ordenadores que ya tenga conexión.

Ninguna de estas medidas por sí sola es segura, todas se pueden saltar. Pero todas ellas combinadas dificultará en extremo que nuestra red sea accesible.

NOTA: *Es muy posible que durante la aplicación de alguna de los pasos anteriores, sobre todo si tenemos poca experiencia, perdamos el acceso al router. En algunas de estas ocasiones (por ejemplo: nos hemos equivocado al escribir la dirección MAC del único pc) no nos quedará más remedio que resetear el router para devolverlo a sus valores de fábrica y así poder empezar de nuevo. Para ello pulsaremos el botón Reset de la parte posterior durante 10 segundos. El router recuperará de esta manera la configuración inicial.*

CONFIGURACIÓN POR DEFECTO DEL ROUTER

Vamos a analizar la configuración del router tal y como viene de fábrica.

- Dirección IP del router: 192.168.1.1
- Servidor DHCP Activado. (El servidor DHCP asigna automáticamente una dirección IP dentro de su propio rango a todo aquel ordenador que lo solicite).
- Wireless activado.
- Difusión ESSID activada.
- SSID: Linksys
- Claves de acceso al router: Usuario: admin. Contraseña: admin
- Sin filtrado de direcciones MAC
- Sin encriptación.

Es decir, la configuración perfecta para que se tenga completo acceso a nuestro router, nuestra adsl e incluso los pcs de nuestra red.

3.- Encriptación. (Asignar una clave se acceso a nuestra red)

La encriptación es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros.. Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.

Encriptación: Hay varios tipos de encriptación en lo que respecta a seguridad de una red inalámbrica.

WEP (Wired Equivalent Privacy) o Privacidad Equivalente a Cableado. Nos ofrece dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave del ordenador debe coincidir con la clave del router.

WPA (Wireless Protected Access) Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). Es una opción más segura, pero no todos los dispositivos wireless lo soportan.

Diferencia entre WEP y WPA

WEP (Protocolo de equivalencia con red cableada)

La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una "clave" de cifrado antes de enviarlo al aire.

Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 13 dígitos alfanuméricos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo. Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

WPA (Wi-Fi Protected Access)

WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de

autenticación:

* **Para el uso personal doméstico:** El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

* **Para el uso en empresarial/de negocios:** El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor **RADIUS**.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP (ver arriba). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

La tecnología SecureEasySetup™ (SES) de Linksys o AirStation OneTouch Secure System™ (AOSS) de Buffalo permite al usuario configurar una red y activar la seguridad de Acceso protegido Wi-Fi (WPA) simplemente pulsando un botón. Una vez activado, SES o AOSS crea una conexión segura entre sus dispositivos inalámbricos, configura automáticamente su red con un Identificador de red inalámbrica (SSID) personalizado y habilita los ajustes de cifrado de la clave dinámico de WPA. No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña ni clave asociada con una configuración de seguridad tradicional inalámbrica.

Resumiendo:

Con **WPA-PSK** hay una autenticación por password del usuario, la encriptación es dinámica . No todos los dispositivos inalámbricos soportan el modo WPA-PSK . La utilidad de windows de configuración de redes inalámbricas suele dar problemas, es recomendable instalar la que traen los dispositivos inalámbricos en el cd de drivers .

Si queremos aumentar la seguridad de nuestra red wifi podemos usar **WPA2 PSK**, que es un protocolo de encriptación más robusto que **WEP**. Basicamente, la diferencia entre un protocolo y otro es que WPA2-PSK soporta una clave de hasta 63 caracteres alfanuméricos, y además, a partir de la **pre-shared key** que le introducimos, el sistema va generando nuevas claves que transmite al resto de equipos, lo cual dificulta la acción de descifrado. Hay programas capaces de esnifar el tráfico generado en una red encriptada con WEP y a partir de un volumen de datos (sobre los 4 Gb) son capaces de descifrar nuestra clave.

Si sustituimos WEP por WPA2-PSK lo que hacemos es cambiar de clave automáticamente cada pocos minutos, lo que supone un plus de seguridad importante.