GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

TRATAMIENTO DE LA INFORMACIÓN Y COMPETENCÍA DIGITAL
Redes Domésticas

Departament d'informàtica.
Autor: Francisco Aldarias Raya
Febrero-2024

Preparació Proves d'Accés

ÍNDEX

Nomenclatura

A lo largo de este tema se utilizarán distintos símbolos para distinguir elementos importantes dentro del contenido. Estos símbolos son:

[Importante]

[Atención]

[Interesante]

1 INTRODUCCIÓN

Una red doméstica es un tipo de red de área local (LAN) que se desarrolla a partir de la necesidad de facilitar la conexión entre los dispositivos digitales presentes en el interior o en las inmediaciones de una casa.
Con una red doméstica, todo el hogar puede compartir una conexión de Internet con varios dispositivos para que todas las personas puedan tener acceso a Internet al mismo tiempo. Puedes compartir el acceso a impresoras, archivos, carpetas y otros dispositivos hardware como los sistemas de juego.

Figura 1: Red doméstica

Hay dos grandes modos de conectar los dispositivos, mediante cables o por Wi-Fi. Se pueden tener dispositivos conectados con cables y/o dispositivos inalámbricos indistintamente en la misma red.

2 TÉRMINOS Y DEFINICIONES

• **Router** (módem o Enrutador): Es el dispositivo clave, el que crea la red doméstica al unir múltiples dispositivos mediante conexiones cableadas o inalámbricas.
• **Cable Ethernet:** Cable de red que se usa para conectar el dispositivo a la red. Se conectan a unos puertos llamados RJ-45 (parecido al del teléfono pero más grandes).
• **Red Wi-Fi**: Una red inalámbrica es usa una señal de frecuencia de radio en lugar de cables para poder conectar tus dispositivos. La señal Wi-Fi puede ser recogida por cualquier dispositivo compatible con tecnología inalámbrica, como una PC portátil o tablet, dentro de determinada distancia pero en todas las direcciones.
• **Señal de Wi-Fi** : Las señales electromagnéticas que se transmiten en el aire para que podamos transferir información, como audio, video, nuestras voces o datos.
• **Cobertura Wi-Fi** : El espacio o alcance al que llega o cubre tu señal de Wi-Fi.
• **Punto de acceso (PA)**: Dispositivo que permite conectarse a la red inalámbricamente. Se pueden usar para ampliar el alcance de una red Wi-Fi.
• **Dispositivo compatible con Wi-Fi** (cliente de Wi-Fi) : Dispositivos que se pueden conectar a la red a través de un router Wi-Fi o un PA (punto de acceso) inalámbrico.
• **Ancho de banda de Internet** : La velocidad máxima de transferencia de datos de una red o conexión a Internet. Se expresa en Megas o Megabits por segundo.
• **Servidor dhcp.** Software que configura los dispositivos de la red de forma automática. Suele estar en el router. El router suele tener activado el servidor dhcp.

3 CONFIGURACIÓN DE LA RED

El router es el componente central de cualquier red doméstica que dependa de los servicios de una operadora de telecomunicaciones que ofrezca comunicaciones de banda ancha es el módem. Este dispositivo se conecta, por un lado, al cable de nuestra compañía proveedora de internet (que puede ser un cable telefónico si es ADSL, coaxial o de fibra óptica), y por otro, ofrece conectividad a nuestra red doméstica.

Figura 2: Router wifi

En la actualidad, prácticamente la totalidad de los hogares con acceso a Internet cuentan con un router que cuenta con capacidades WiFi (con una o más antenas), y es un dispositivo al que no se le presta toda la atención que se debiera en cuanto a seguridad se refiere. Pues en la mayoría de los casos, una vez se ha procedido con la instalación del router wifi en nuestra casa, entendemos que por sí sola, cuenta con los suficientes mecanismos de protección que la convertirán en un muro infranqueable ante posibles intrusiones externas. ¿Pero realmente es así? Pues hemos de decir que no, ya que los routers traen algunas opciones de seguridad que por defecto no vienen activadas o configuradas de la manera más correcta. Si a esto le sumamos que los usuarios somos desconocedores de ello… el resultado es que nuestra conexión puede ser vulnerable.

3.1 Riesgos de un router mal configurado

Cuando un router no cuenta con las medidas de seguridad y las configuraciones apropiadas podemos sufrir las siguientes consecuencias:

• **Robo de información confidencial.** Cuando un intruso se conecta a nuestra red privada podría llegar a acceder a nuestra información y si cuenta con los suficientes conocimientos podría acceder a los dispositivos personales, así como a los datos que estamos enviando y recibiendo de Internet o infectarnos con malware.
• **Utilizar la red para realizar acciones ilegales.** Si un delincuente logra acceder a nuestro router, podrá usar los dispositivos que hay en nuestra red para llevar a cabo acciones ilegales o maliciosas, como conectarse de manera repetitiva a una página web para sobrecargarla e impedir que funcione de manera correcta como el que hace poco sufrieron compañías como Twitter, Spotify o Ebay.
Esto nos afecta porque estamos **vinculados legalmente con lo que ocurra en tu red.** Cuando contratamos una conexión a Internet, nuestro proveedor vincula la dirección IP que tengamos en ese momento con el nombre del titular, de la misma manera que un número de teléfono está asociado a su suscriptor. Cualquier acción, ilegal o no, que se lleve a cabo desde nuestra red estará asociada directamente con el titular de la línea, es decir, con nosotros, y aunque se demuestre que hubo alguna intrusión en nuestro sistema, puede generar nos algún quebradero de cabeza.
• **Disminución del ancho de banda.** Las conexiones tienen una capacidad limitada, el ancho de banda, que se reparte entre los dispositivos que estén conectados, de forma que cuantos más equipos se conecten, más lento irán.

3.2 ¿Cómo acceder a la configuración del router?

Para llevar a la práctica esta acción será necesario, en primer lugar, conocer la dirección IP que nos da acceso al router. Se puede saber de varias formas, nosotros recomendamos seguir los siguientes pasos para el caso de ordenadores **Windows**:

Botón de **Inicio** >> (en el cuadro donde dice "Buscar programas y archivos") escribir **«cmd»** >>
Pinchar en el resultado >> Escribir **«ipconfig»** >> buscar la **«Puerta de enlace»**

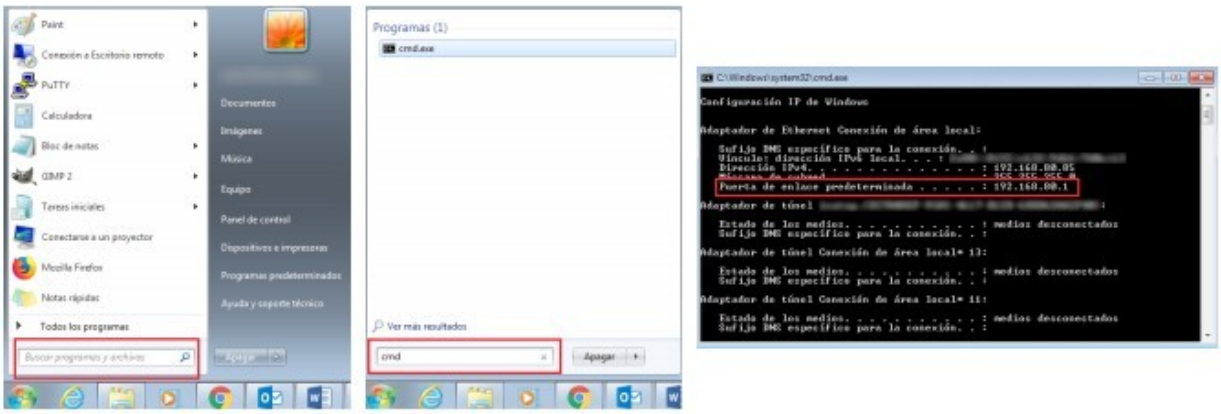
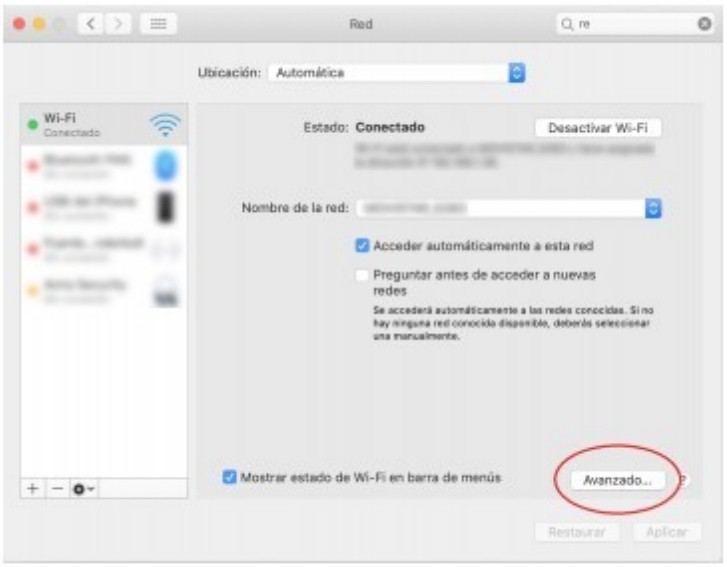


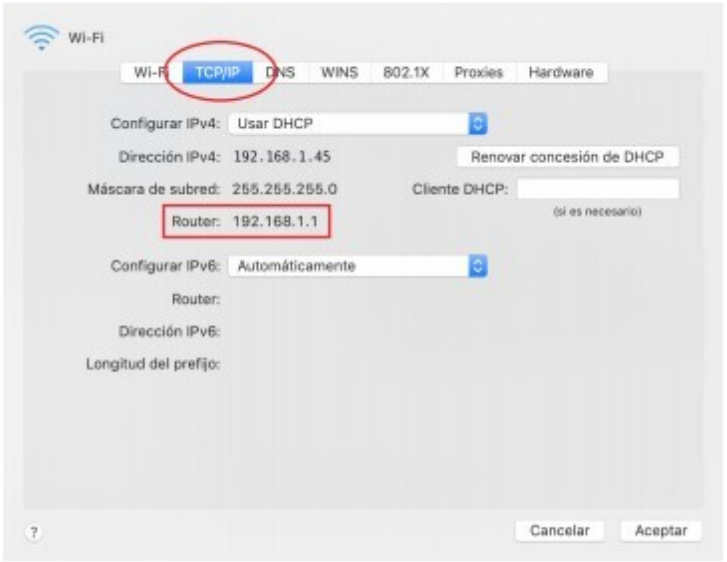
Figura 3: Conocer la IP del router

En el caso de ordenadores con sistema operativo **MAC OS,** los pasos que hay que seguir para saber la puerta de enlace, son los siguientes:

1 Acceder al icono de la manzana (parte superior izquierda de la pantalla), y ver las preferencias del sistema, acceder a Red, seleccionar en este caso wifi e ir a la configuración avanzada.



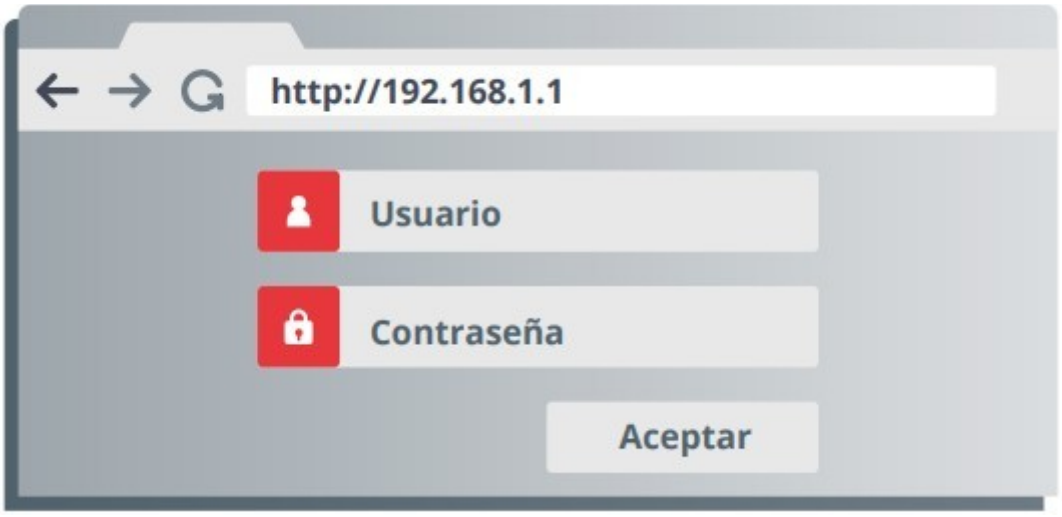
2 Por último habría que seleccionar la pestaña TCP/IP



Una vez que contamos con la dirección IP del router, necesitaremos de un navegador web para poder acceder al dispositivo, así como las credenciales de acceso que podrás encontrar bien en el manual del router o bien, en la pegatina que viene en su base o parte trasera. Una última opción sería consultar directamente al fabricante cuál es dicha contraseña.

3.3 Medidas de seguridad básicas

Una vez contamos con acceso al router, podremos fijar nuestra actividad en implementar una serie de medidas de seguridad básicas como las que se exponen a continuación:



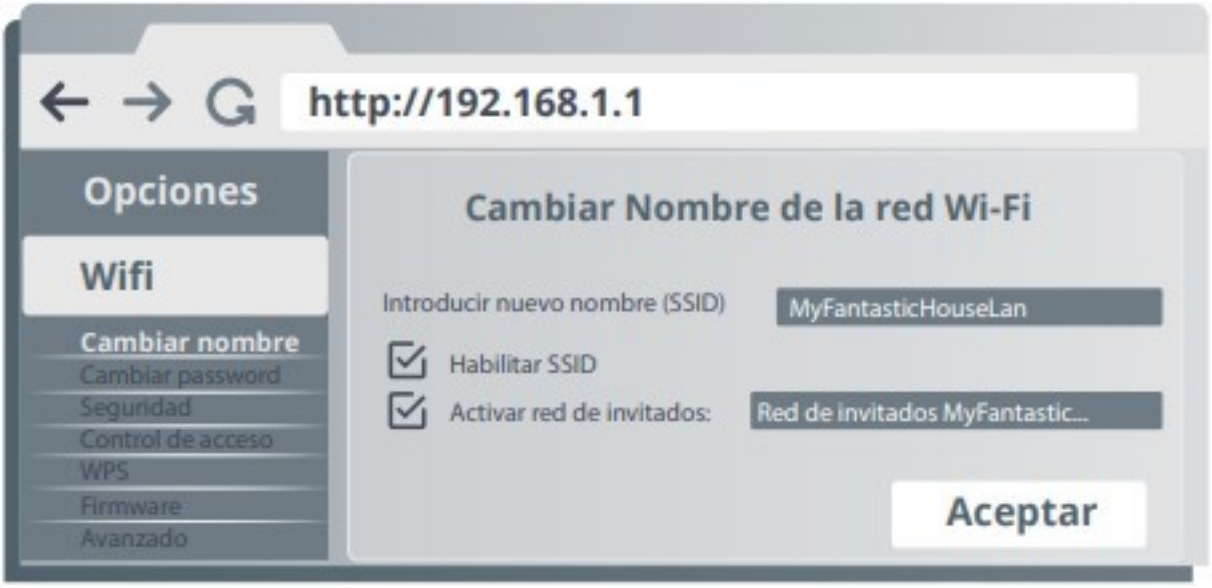
3.3.1 Cambiar la contraseña de acceso al router

Para poder cambiar la contraseña que permite el acceso a tu router, en primer lugar hay que buscar la opción de configuración que permite **cambiar la contraseña por defecto**.

Hay que tener en cuenta que cada dispositivo puede contener esta opción en un lugar distinto, por lo que habrá que realizar una búsqueda activa a través de los diferentes menús o disponer del manual del modelo concreto para llevar a cabo la tarea (normalmente disponible en formato digital en el paquete del dispositivo o descargable de la web del fabricante).

3.3.2 Modificar el nombre de la red wifi o (SSID)

Es muy recomendable cambiar el nombre de nuestra wifi por defecto porque da información de utilidad para un potencial atacante (proveedor de servicios, router, etc.).



Por lo tanto, lo mejor es quitar este tipo de información y cambiarlo por algo que no pueda ser asociado a nuestro SSID (Del inglés Service Set IDentifier o identificador de paquetes de servicio, se trata del nombre que identifica una red inalámbrica y es visible por toda la red).

Otra opción más drástica y segura es ocultar la emisión del SSID. Así no saldrá el nombre de la red al buscar redes para conectarse y sólo alguien que sepa el nombre podrá acceder.

3.3.3 Contraseña de acceso a la red wifi

Otro de los principales aspectos a tener en cuenta a la hora de evitar intrusiones, es hacer uso de contraseñas de acceso a la wifi que sean lo más robustas posibles.
No utilices las contraseñas por defecto que te haya proporcionado tu Proveedor de Servicios de Internet (ISP – del inglés Internet Service Provider, es la empresa que confiere conexión a Internet a sus clientes), por muy segura que parezca a simple vista. Recuerda que se considera una contraseña robusta es aquella que utiliza un mínimo de 8 caracteres que combinen minúsculas, mayúsculas, números y algunos caracteres especiales.

3.3.4 Actualización del Firmware

También deberás actualizar el firmware (Se trata del software que controla las funciones de un dispositivo físico o un hardware concreto) en tu router cada vez que haya una nueva versión disponible. Al usar la última versión del software te aseguras de tener todos los parches de seguridad disponibles.

Muchas personas no saben que sus routers también vienen con software, y esto es una parte muy importante para protegernos frente a posibles ataques que explotan vulnerabilidades en el software.

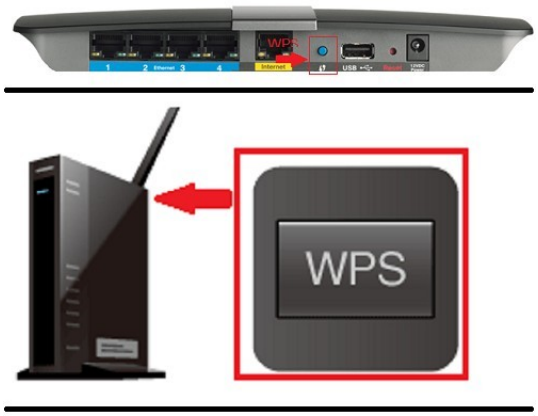
3.3.5 Configurar red wifi con cifrado WPA2 o WPA3

En las configuraciones de los routers, normalmente se ofrecían tres modalidades de cifrado: WEP, WPA y WPA2. Posteriormente, se incorporó una más robusta y la que más se recomendaba habilitar: WPA2-PSK(AES). Sin embargo, en octubre de 2017, se descubrió una vulnerabilidad denominada «ataque KRACK» que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica con el tipo de cifrado anteriormente mencionado. Ante este problema se ha desarrollado una nueva versión del protocolo WPA llamada WPA3. WPA viene de las siglas Wi-Fi Protected Access. Se trata de un estándar dirigido a la protección de los dispositivos, como los routers, de tal manera que nadie ajeno pueda acceder a los datos de manera inalámbrica. De esta forma WPA3 irá reemplazando progresivamente al WPA2. Las mejoras en autenticación, configuración o cifrado están orientadas a dificultar la acción de los atacantes, de tal forma que no puedan entrar en nuestra red.

Lo que no se debe tener configurado bajo ningún concepto es el cifrado WEP, ya que es muy inseguro y se puede robar la contraseña de la red en poco tiempo.

3.3.6 Desactivar WPS

Se trata de un mecanismo que facilita la conexión de dispositivos con nuestro router pulsando un botón y con un código PIN de 8 dígitos numéricos. El dispositivo que se quiere conectar a la wifi debe transmitir el código al router y éste a cambio le enviará los datos para acceder a la red.



Tener activada esta opción implica una nueva forma de conexión que podría ser utilizada por un atacante para acceder fácilmente a nuestra red wifi, ya que el tiempo que se necesita para averiguar este PIN es mucho menor que el de una contraseña WPA2-PSK(AES). Por lo tanto, deberemos renunciar a este tipo de utilidad, desactivando el WPS.

3.3.7 Red wifi para invitados

Existen modelos de routers que crean una red inalámbrica separada de nuestra red wifi y conocida como red de invitados. De esta manera, mediante la creación de esta red de invitados, evitaremos que quien se conecte a ella se tenga acceso a la red local, así como a los datos que aquí se albergan, evitando potenciales infecciones mediante la propagación de virus, malware o una fuga de información.

Para poder crearla, necesitaremos acceder a las opciones de conectividad Wireless, es decir, los ajustes de nuestra red wifi. Una vez dentro, y dependiendo del modelo de router, deberemos buscar el ajuste Guest Wifi / Virtual Acces Point, que nos permite crear un segundo punto de acceso a nuestra red local. Deberemos configurar un SSID

diferente con una contraseña alternativa a las que tenemos, tanto para el acceso al router como para el acceso a la red wifi local.

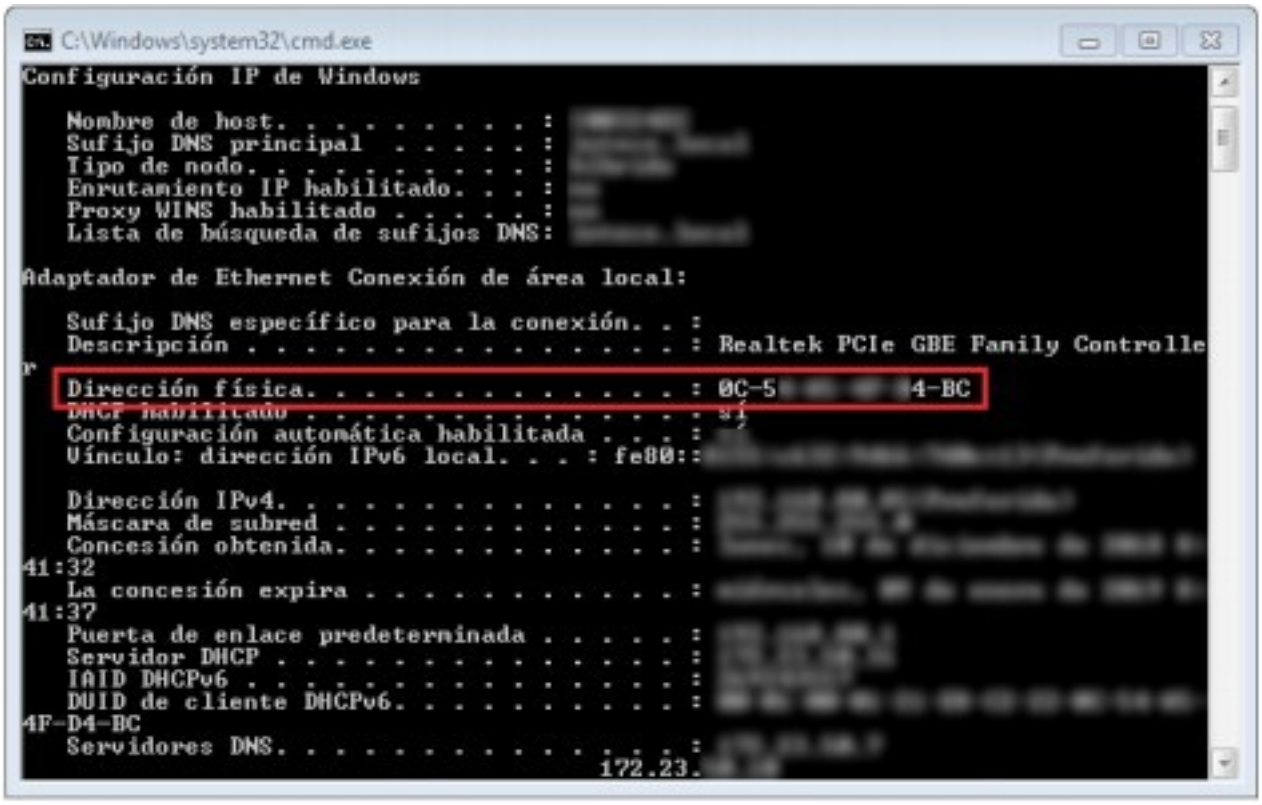
3.4 Medidas de seguridad complementarias

3.4.1 Habilitar el filtrado por dirección MAC

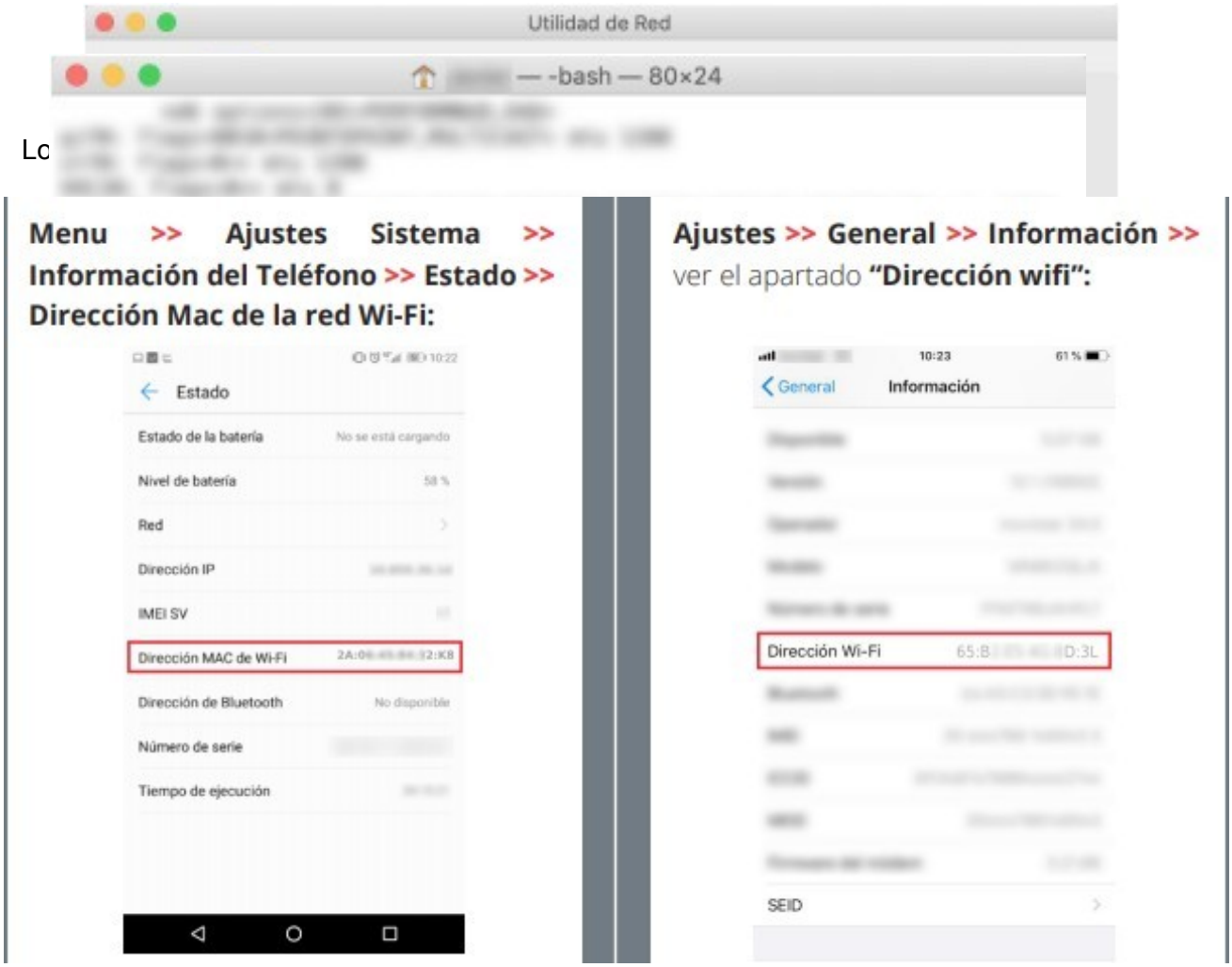
Mediante este mecanismo se pretende que únicamente las direcciones MAC que se encuentren guardadas en el router puedan conectarse a la red. Esta dirección es un identificador único asociado a un dispositivo concreto como un portátil o un smartphone. Por lo tanto, habrá que incluir las direcciones que entendamos como oportunas en nuestro router y para ello deberemos acceder a la configuración del dispositivo para establecerlo.

Como paso previo, hemos de conocer la dirección MAC de los diferentes dispositivos que queramos añadir, bien sean ordenadores, teléfonos móviles, tablets, etc.

En el caso de dispositivos con sistema operativo Windows obtendremos la dirección MAC a través de la consola de MSDOS haciendo uso del comando especial «ipconfig /all». En este caso, deberemos buscar el campo «dirección física».



En el caso de dispositivos con sistema operativo Mac OS, se puede hacer de dos formas:
Bien accediendo a las «Utilidades de Red» o a través de un terminal haciendo uso del comando «ifconfig». El «interfaz en0» suele ser el que se utiliza para conectarse a la wifi.



3.4.2 Reducir los rangos de direcciones IP permitidas

Si siempre vamos a tener los mismos equipos conectados a la red, podemos utilizar la opción de deshabilitar el funcionamiento automático del servicio DHCP en el router que se encarga de asignar direcciones IP a cada equipo conectado a la red. Esto nos obligará a tener que configurar los valores de forma manual en todos los dispositivos que tengamos en casa, pero puede aportar un grado más de seguridad.
También podemos jugar con el rango de direcciones IP permitidas y restringirlo hasta los valores que queramos evitando que queden multitud de direcciones libres. Es muy sencillo de hacer. Solo hay que buscar la opción dentro de la configuración de la LAN en la que ponga algo similar a «Start IP Address/End IP Address» y ahí especificar los valores deseados (por ejemplo de la IP 192.168.1.33 a la 192.168.1.35, que permitiría conectar 3 equipos a la red).

3.4.3 Limita la potencia de emisión de las antenas

Puede parecer obvio, pero si no llega la señal, difícilmente alguien podrá localizar tu red y mucho menos conectarse a ella.
La mayoría de los routers permiten gestionar de algún modo la potencia emitida por las antenas y así manejar el radio de cobertura de la red de forma aproximada. Lo habitual es que nos encontremos con alguna opción en la que se nos permita variar el porcentaje de nivel de señal o la potencia transmitida.

Aquí debemos procurar bajar la intensidad para que sigamos pudiendo conectarnos a la red dentro de casa, pero para que la potencia decaiga mucho fuera de ella. Podemos ir comprobándolo simplemente moviéndonos con el móvil por la casa y sus alrededores y viendo qué cobertura wifi tenemos.

3.4.4 Deshabilitar la administración remota

La administración remota sirve para que podamos configurar nuestro router fuera de nuestra red privada como por ejemplo desde la red wifi del domicilio de un familiar. Esta opción es conveniente tenerla deshabilitada, ya que de esta forma evitamos que alguien pueda conectarse a nuestro router desde Internet.

3.4.5 Control de equipos en la red

Los router cuentan con una opción en la que muestran los dispositivos conectados a la red. Accediendo a esta sección de la página de configuración podemos conocer un listado de los dispositivos conectados en tiempo real y comprobar si hay alguien que no debería estar.

3.4.6 Deshabilita UPnP

También habrá un ajuste en tu panel de administración para UPnP siglas en inglés de Universal Plug and Play. Esto le permite a los dispositivos en la red como computadoras, impresoras, y otros dispositivos a descubrirse entre ellos mismos dentro de la red. Esto puede introducir riesgos de seguridad, y debe deshabilitarse si la opción está presente.

3.4.7 Apagar el router

En los horarios en que no vayas a utilizar tu conexión a Internet o en periodos de tiempo en los que no te encuentres en casa, se recomienda apagar el router. Es la mejor garantía de que nadie se conectará.

4 BIBLIOGRAFÍA

•https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridaden-redes-wifi.pdf
•https://www.kaspersky.es/blog/siete-consejos-para-hacer-el-wi-fi-de-tu-casa-masseguro/5053/
•https://www.soporteparapc.com/2014/07/guia-como-configurar-router-yacceder.html
•https://www.osi.es/es/actualidad/blog/2017/10/16/te-refrescamos-como-protegerla-red-wifi-de-casa
• https://www.tp-link.com/es/support/emulator/
• https://www.malagana.net/emuladores-de-routers-dlink/
• https://www.snbforums.com/threads/router-ui-emulators.30552/