INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

# Técnico en REDES &SEGURIDAD 8

# CONFIGURACIÓN DE REDES INALÁMBRICAS

**En este fascículo veremos la manera en que se debe configurar una red inalámbrica, desde los dispositivos de hardware utilizados hasta las opciones de seguridad.**


**Incluye e-book: Solución de problemas**

USERS

# Técnico en REDES &SEGURIDAD


**Coordinador editorial**
Paula Budris

**Asesores técnicos**
Federico Pacheco
Javier Richarte

**Nuestros expertos**
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez






Impreso en Sevagraf S.A. Impreso en Argentina.




Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

**ISBN 978-987-1857-78-4**

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

# En esta clase veremos...

La forma en que debemos llevar a cabo las tareas de configuración de una red Wi-Fi y las opciones de seguridad relacionadas.

En la clase anterior conocimos cómo realizar la implementación de una red inalámbrica. Vimos en detalle cómo funciona y cuáles son los estándares relacionados con esta tecnología. Configuramos de forma general un punto de acceso y verificamos las opciones de seguridad más importantes para mantener la red protegida. También aprendimos a instalar y configurar interfaces de red inalámbricas en sistemas Windows y Linux.

En esta entrega, nos dedicaremos a revisar en profundidad las tareas de configuración de una red inalámbrica. Analizaremos las topologías Wi-Fi y configuraremos un access point en forma avanzada. También conoceremos los alcances del wardriving, y los tipos de antenas y repetidores existentes.

Revisaremos algunos conceptos sobre autenticación con servidores AAA, TKIP y MIC, así como también aprenderemos a ocultar el SSID para aumentar el nivel de seguridad de una red.


**8**

**2**
**Topologías Wi-Fi**

**4**
**Configuración avanzada del AP**

**8**
**Protocolos WEP y TKIP**

**14**
**Tipos de antenas y repetidores de señal**

# Topologías Wi-Fi

## Desarrollaremos las diferentes topologías que podemos encontrar cuando nos enfrentamos con una red inalámbrica.

Así como las redes cableadas o Ethernet tienen diferentes topologías que se aprovechan en distintas situaciones, con las redes inalámbricas sucede lo mismo. A grandes rasgos, podemos identificar dos topologías diferentes, cada una de ellas con sus ventajas y desventajas. Por eso, a continuación veremos cuáles son esas topologías, sus usos, cómo implementarlas, y sus pros y contras.

En este diagrama, podemos apreciar cómo, en la topología infraestructura, los dispositivos se concentran en el router Wi-Fi.

### Modo ad hoc

La primera **topología** que veremos es, a su vez, la de más rápida implementación. Es el modo conocido como ad hoc, o descentralizado.

Se la denomina de esta manera porque no requiere de un punto de acceso para interconectar dos o más dispositivos inalámbricos, sino que todos ellos se enlazan entre sí. Más específicamente, cada nodo de la red está capacitado para reenviar los datos recibidos a los demás nodos (desde luego que aquellos que los reciban deben estar dentro del rango de cobertura de la placa de red del nodo transmisor).

Tal como sucede con las redes inalámbricas comunes, una red ad hoc también posee SSID (nombre de red con el que los demás nodos la reconocerán) y seguridad (que también puede ser WEP, WPA/WPA2, o cualquiera que soporte la placa de red sobre la cual se la está configurando).

Para configurar una red ad hoc desde **Windows 7**, bastará con hacer un clic en el botón **Inicio** y escribir en el cuadro de búsqueda la palabra **redes**. El sistema nos mostrará un listado de acciones posibles, del que vamos a seleccionar **Configurar una red ad hoc**; luego seguimos las indicaciones del asistente. Al finalizar, tendremos funcionando nuestra propia **red ad hoc**.

Analicemos las ventajas de este tipo de redes. En entornos militarizados, permiten establecer comunicación con los diversos centros de mando, vehículos o tropas terrestres, lo cual sería bastante dificultoso con una estructura fija. De la misma manera, ante desastres naturales o situaciones de emergencia, las redes ad hoc resultan más viables que las de infraestructura debido, justamente, a la descentralización. En el ámbito civil, podemos citar el ejemplo de un gran invernadero, donde una red ad hoc de sensores de riego es más efectiva que una red de infraestructura; en este última, en caso de fallar el access point, el sistema quedaría inhabilitado, mientras que de forma descentralizada, solo uno o unos pocos sensores dejarían de funcionar.

Si nuestra notebook es antigua, siempre podremos conectar un transreceptor Wi-Fi de la norma que necesitemos.

Y desde luego, para situaciones de presentaciones, clases, transferencia de archivos, etcétera, se vuelve fundamental una red ad hoc, ya que, principalmente, manejaremos dispositivos personales, como PDAs, smartphones, tablets y otros.
Como desventajas, podemos mencionar el desperdicio del ancho de banda en la definición de rutas para la información. Otro factor en contra es el consumo de potencia de los dispositivos conectados a este tipo de redes, ya que se multiplica el volumen de mensajes enviados. Por último, pero también fundamental, hay que mencionar el apartado de seguridad. Como los datos transmitidos pasan por nodos intermedios que no se conocen entre sí, la protección no es la más recomendada.

## LAS REDES WIMAX SON INALÁMBRICAS, PERO NO ESTÁN CONTEMPLADAS EN LAS ESPECIFICACIONES 802.11 DE LA IEEE, SINO EN LAS 802.16.

### Modo infraestructura

El equivalente a la topología Ethernet tipo estrella, pero Wi-Fi, se denomina **infraestructura**. En este tipo de redes wireless, existe un router central en el que convergen las peticiones de datos. Se llama access point y oficia como servidor de servicios de enrutamiento, control de tráfico, server DHCP, etc.
Configurar los dispositivos inalámbricos para funcionar en este tipo de redes es realmente sencillo. Solo debemos verificar que las propiedades del protocolo IPv4 del dispositivo inalámbrico estén en automático. Con un clic en el botón **Inicio**, escribimos **conexiones** y elegimos de la lista la opción **Ver conexiones de red**. Luego, elegimos la conexión de red inalámbrica y accedemos a sus propiedades mediante un clic con el botón derecho del mouse. De la lista de elementos que utiliza el dispositivo, escogemos IPv4 y, luego, presionamos el botón **Propiedades**. En la ventana emergente, debemos verificar que estén seleccionadas las opciones **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente** (si no lo están, procedemos a marcarlas). De esta manera, al encontrar un SSID, la notebook (la tomamos como mero ejemplo demostrativo) envía una solicitud de broadcast para identificar la puerta de enlace, y recibe el ofrecimiento de una IP que el access point tiene libre; luego de aceptarla, la placa de red wireless del equipo portátil se configura automáticamente con la dirección IP asignada, la máscara de subred y también la puerta de enlace predeterminada.
Ahora bien, las ventajas que podemos mencionar para esta topología comienzan con la velocidad de interconexión entre un punto y otro de la red, ya que entre la PC A y la Tablet B, solo tendremos el router. Esto permite que haya menos recorrido de la información, menor probabilidad de fallas en los paquetes por interferencias en la señal y, desde luego, el hecho de contar con un canal mucho más seguro que en una red ad hoc para transmitir datos sensibles. En cuanto a las desventajas de la topología, podemos decir que, como su piedra basal es el access point, si este llega a dañarse o desconfigurarse, la red caerá por completo; es que, sin él, no hay servidor DHCP que asigne direcciones IP a las terminales. Finalmente, diremos que, si quien realiza la configuración del router Wi-Fi no tiene los conocimientos necesarios sobre los protocolos y servicios involucrados, el resultado tal vez sea una red deficiente. ■

## Modelos y normas

**Con el avance de la tecnología en materia de conexiones inalámbricas, los dispositivos han diversificado sus capacidades y formatos. Esto no significa que tendremos problemas de compatibilidad, sino que, de acuerdo con la norma que necesitemos (802.11a, b, g, n), solo debemos centrarnos en el alcance de la señal y la estética del dispositivo. Por ejemplo, en la actualidad se pueden conseguir adaptadores del tipo nano, que en una notebook pasan prácticamente inadvertidos; incluso, se han comenzado a comercializar transreceptores que simulan una pequeña antena parabólica.**

Para conectar una PC de escritorio mediante Wi-Fi, bastará con instalarle una placa de red inalámbrica.

# Configuración avanzada del AP

Nos adentraremos en las opciones avanzadas de nuestro Access Point para conocer todas las configuraciones disponibles.

Para revisar las tareas de configuración avanzadas, vamos a utilizar un módem/router **Zyxel P-660HW-T1**, que, además de los clientes Wi-Fi, nos permitirá conectar hasta cuatro equipos de manera cableada. Sus opciones se encuentran en inglés, por lo que mantendremos la nomenclatura que utiliza el dispositivo tanto como su idioma, para evitar confusiones de cualquier tipo; a continuación conoceremos los detalles para configurarlo.

## Configuración NTP

La sigla **NTP** significa *Network Time Protocol* (protocolo de tiempo de red) y se utiliza para la sincronización de equipos conectados a una red mediante el puerto 123 del protocolo UDP, ruteando paquetes en redes con latencia variable.
Para configurarlo, ingresamos en el *Web Configurator* del router, mediante su IP. Luego de colocar la contraseña correspondiente, seremos transportados al menú inicial.
Ingresamos haciendo clic en la opción **Time and Date**, bajo el menú **Advanced Setup**, para obtener lo que pasamos a describir.
En **Time Server** desplegamos la opción **Use Protocol when Bootup** y seleccionamos la opción **NTP (RFC-1305)**. Debajo colocamos la IP del servidor, que debemos solicitar al ISP o al administrador de la red a la que estamos conectados.

El primer paso antes de configurar el router es el cambio de la contraseña predefinida, fundamental para que no nos modifiquen nada.


Luego elegimos la zona horaria, que para este ejemplo será **GTM-03:00**. De manera opcional, podemos marcar la casilla **Daylight Saving**, que nos permite indicar las fechas de inicio y fin del corrimiento del reloj para aprovechar la luz del día. Esto nos servirá en caso de configurar restricciones de acceso por horario.
La casilla **Synchronize system clock with Time Server now** se utiliza para comenzar la sincronización de manera inmediata.
En el apartado denominado **Date**, podemos configurar la fecha actual; mientras que **Time** es para asignar la hora.
Una vez que tengamos las opciones configuradas a nuestro gusto, simplemente hacemos un clic en el botón **Apply** para guardar la configuración que acabamos de definir.

SI UNA CONFIGURACIÓN MAL HECHA NO NOS PERMITE ACCEDER AL ROUTER, PODEMOS RECURRIR AL BOTÓN RESET, UBICADO EN LA PARTE TRASERA.

## Filtrado por MAC Address

Sabemos que la MAC Address de una interfaz de red o **NIC** (*Network Interface Card*) es una secuencia numérica expresada en hexadecimal que identifica al dispositivo de manera única a nivel mundial; esto quiere decir que, en teoría, no existen dos NIC con la misma MAC. La mayoría de los routers, sean Ethernet o Wi-Fi, tienen la capacidad de filtrar las conexiones y el tráfico mediante varios métodos. Uno de ellos es el filtrado por MAC Address. Veamos cómo configurarlo.
Desde el menú **Advanced Setup**, seleccionamos la opción **Wireless LAN** para acceder a las configuraciones del apartado inalámbrico. En la siguiente pantalla, hacemos clic en la opción **MAC Filter**. Ya en la pantalla de configuración, nos encontramos con dos desplegables. **Active** nos permite definir si el filtrado estará activo o no, en tanto que **Action** se usa para realizar el filtrado mediante dos criterios. Si seleccionamos **Allow Association**, se les permitirá vincularse al router a las MAC

Address que definamos en la tabla de configuración; mientras que, si elegimos **Deny Association**, se les denegará el acceso al router a las MAC definidas en la tabla. Luego, bastará con hacer un clic en el botón **Apply** para guardar los cambios.

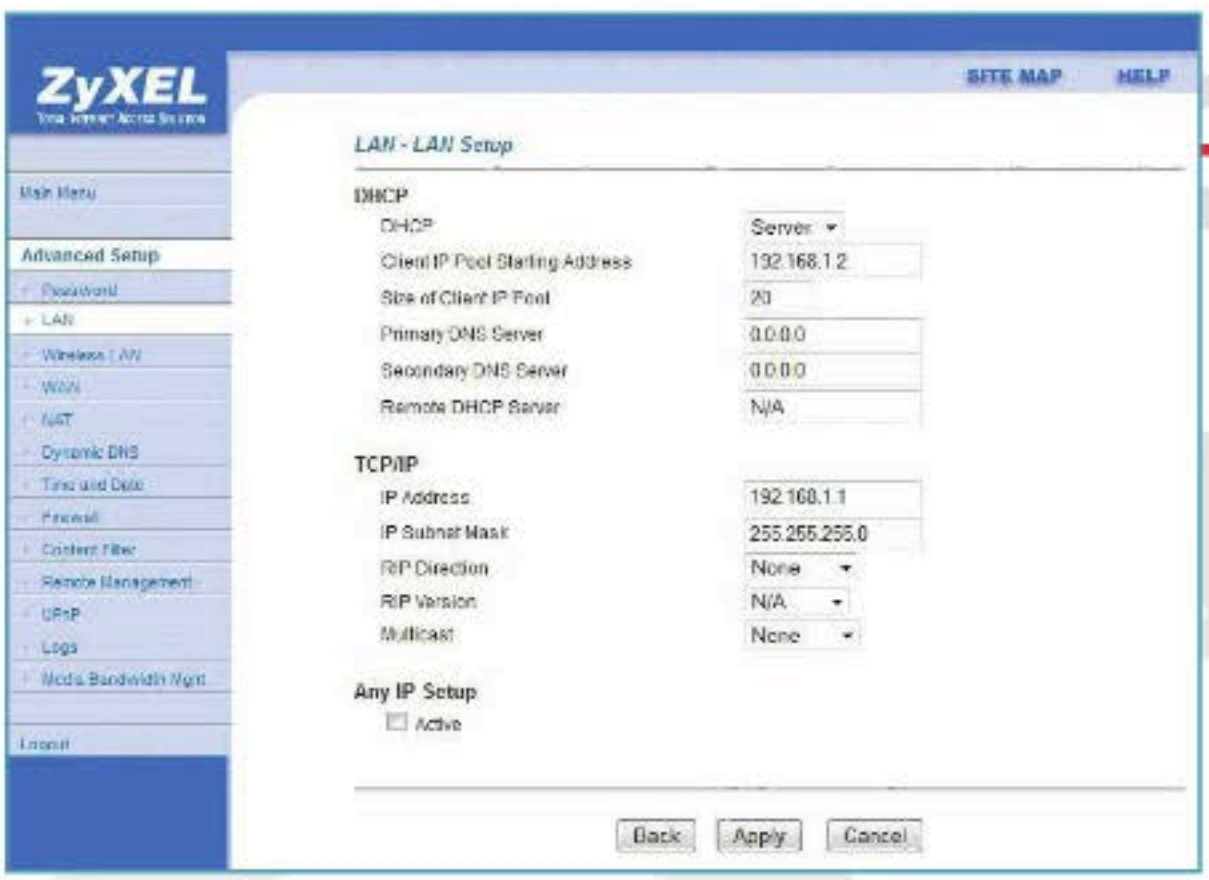
## Configuración DHCP

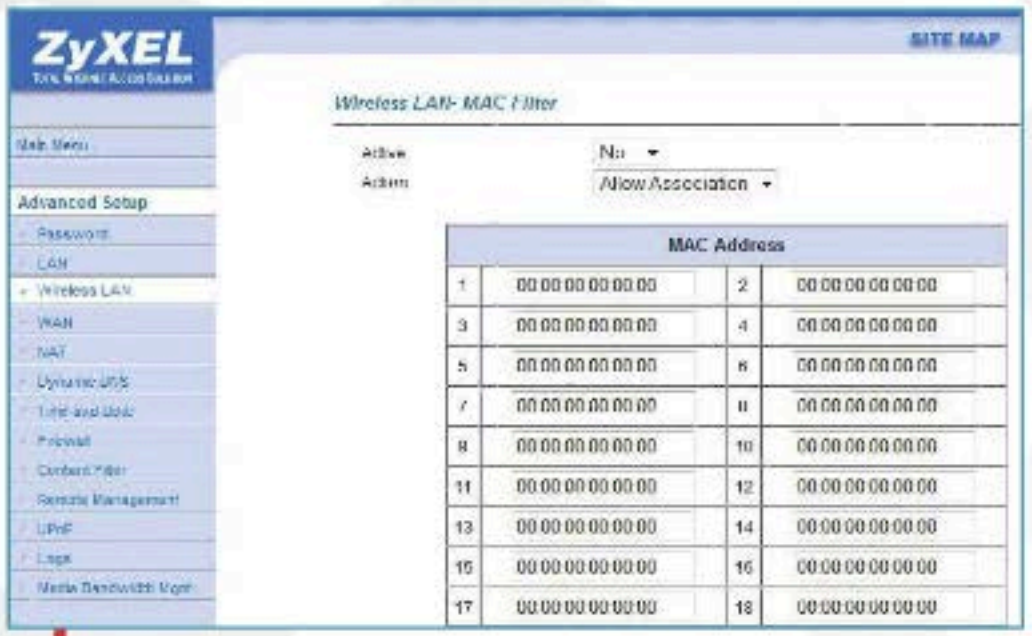
La función de **DHCP Server** se utiliza para configurar la IP que tendrá el router, y que será la **Puerta de Enlace Predeterminada** que utilizaremos para conectarnos a él; además, nos permite definir el rango y la cantidad de conexiones que habilitaremos. Nuevamente, en el menú seleccionamos la opción **LAN** y, en la pantalla siguiente, **LAN Setup**. Llegamos de esta manera a donde están las opciones que vamos a configurar. En el desplegable **DHCP** seleccionamos la opción **Server**, la cual nos habilitará la configuración. En **Client IP Pool StartingAddress** configuramos la dirección IP desde la cual comenzaremos a otorgar a los clientes que intenten conectarse a la red (por ejemplo: **192.168.1.2**). **Size of Client IP Pool** nos permite limitar la cantidad de clientes que se conectarán a nuestro router: si fijamos su valor en 10, el router permitirá conexiones desde la IP indicada anteriormente (192.168.1.2) hasta la décima IP consecutiva siguiente (192.168.1.12). Los servidores DNS primario y secundario no se configuran en nuestro ejemplo porque representan las IPs de los servidores que queremos utilizar en forma remota, como los de nuestro ISP. De igual manera, si en el desplegable DHCP seleccionamos **Relay**, debemos configurar el servidor DHCP remoto que utilizaremos ya que, mediante la opción **Relay**, el router solo oficiará de intermediario entre el servidor DHCP remoto y el cliente correspondiente.


**Desde la pantalla Wireless LAN, podemos configurar los filtros de acceso, por ejemplo, utilizando las direcciones MAC.**

Antes de continuar, vamos a hacer una salvedad. La configuración que estamos llevando adelante se basa en un servicio de asignación de direcciones IP dinámico. En caso de configurarlo de manera estática, deberíamos configurar también la IP fija en la placa de red inalámbrica en nuestra PC, notebook, tablet, etc. Esto haría que, cuando intentáramos acceder a otras redes wireless (cafeterías, aeropuertos, etc.), no pudiéramos hacerlo, ya que tendríamos una configuración incompatible con dichas redes. En tales casos, deberíamos reconfigurar la placa de red para que detectara la información de manera automática. Hecha esta aclaración, volvamos a lo nuestro. Llega el momento de configurar la sección TCP/IP: **IP Address**, es la dirección IP que tomará nuestro router y será la puerta de acceso predeterminada para todos los equipos que se conecten a él. **IP Subnet Mask** corresponde a la máscara de red que utilizaremos para la red a la que sirve nuestro router (si tenemos otro router, podemos crear otra red paralela, configurándole otra máscara de red diferente).

**Aquí, apreciamos todas las opciones de configuración disponibles para el servidor DHCP y el protocolo TCP/IP del router.**




**Este modelo de módem/router nos permite realizar el filtrado de hasta 32 MAC Address en total.**

No vamos a configurar las dos opciones de **RIP** (**Direction** y **Version**); es decir que quedarán en **None** y **N/A** respectivamente, porque se utilizan para aquellos casos en que trabajamos con más de una red (subnetting). La opción **Multicast** quedará en **None**, dado que la usaremos en el supuesto caso de que nuestro router genere transmisiones por suscripción (por ejemplo, una transmisión de video). Para finalizar, la casilla **Any IP Setup** quedará desactivada, lo que indicará al router que solo las IPs que estén dentro de la red del router (es decir, las que tengan su misma máscara de red) podrán salir a Internet.

## Configurar el firewall del router

El firewall, también conocido como cortafuegos, es un método de seguridad de red que permite la intercomunicación de terminales autorizadas y bloquea los accesos no autorizados. El sistema funciona sobre la base de reglas que pueden configurarse de acuerdo con las necesidades de la red. Una vez más, seleccionamos la opción **Firewall** y, en la siguiente pantalla, **Default Policy**, para llegar donde podremos activar tanto la funcionalidad del firewall en sí misma, como las reglas asimétricas. Para hacer una configuración básica del firewall, marcamos la casilla **Enable Firewall** y, en la tabla inferior, seleccionamos los tipos de conexión y las acciones por realizar: **Block** (bloquear) y **Forward** (redirigir).

Los tipos de conexiones son los siguientes:

- **LAN to LAN/Router**: indica las conexiones entre dos terminales de la red interna o entre una terminal y el router. Esta opción debería quedar en **Forward**.
- **LAN to WAN**: la configuramos también en Forward, ya que permitirá la salida de las terminales de la red hacia Internet.
- **WAN to LAN**: tengamos en cuenta que esta opción debe quedar bloqueada, pues salvo en casos excepcionales, no deseamos que desde Internet se pueda acceder a nuestra red.
- **WAN to WAN/Router**: esta opción debe correr la misma suerte que la opción anterior, ya que se refiere a las conexiones desde Internet hacia Internet (oficiando como intermediario) o desde Internet hacia el router.

En la tabla que mencionamos anteriormente también tenemos las casillas bajo el título **Log**, lo que nos permitirá llevar un registro de las acciones efectuadas por el firewall ante cada conexión.
En caso de ser necesario, podemos definir reglas en forma manual. Esta tarea se lleva a cabo desde la opción **Firewall/ Rule Summary**. Allí podremos seleccionar la dirección de los paquetes (por ejemplo, LAN to WAN) y agregar las reglas que necesitemos. Veamos un ejemplo. Primero activamos la regla, luego seleccionamos el tipo de acción (en nuestro caso, **Block**) y, por último, realizamos la configuración fina.
Desde **Source Address**, desplegamos **Address Type** y elegimos la opción **Range Address**; luego indicamos la IP de inicio del rango (192.168.1.2) y la IP de finalización (192.168.1.5). Terminamos con un clic en el botón **Add**. En la sección **Destination Address** dejamos seleccionado **Any**. En **Services** seleccionamos **FTP**, **IRC** y **TELNET**, haciendo clic en **Add** por cada uno; luego, pasamos a la lista de la izquierda y quitamos todo lo que no hayamos seleccionado nosotros. Desde **Schedule** marcamos las casillas **Everyday** y **Allday**. Finalmente, marcamos las casillas **Log** y **Alert** y pulsamos en el botón **Apply** para guardar los cambios.
¿Qué acabamos de hacer? Creamos una regla de conexión que bloquea las conexiones salientes de cualquier equipo que utilice una IP comprendida entre 192.168.1.2 y 192.168.1.5, mediante los servicios FTP (protocolo TCP en puertos 20 y 21), IRC (protocolos TCP y UDP en puerto 6667) y Telnet (protocolo TCP en puerto 23). También indicamos que el filtro se aplicará todos los días durante todo el día. Y finalmente, que guarde un

## ¿Router o módem/router?

Como sabemos, el tipo de dispositivo que vamos a adquirir dependerá de las necesidades en cuanto a la infraestructura de la red que estemos por armar y los servicios que necesitemos configurar. Tengamos presente que un módem/router tendrá diversas capacidades recortadas y será más apto para pequeñas redes hogareñas. En cambio, un router está más a la altura de una red corporativa, esté subneteada o no, con todos los servicios de seguridad y control de acceso disponibles para configurar hasta el más mínimo detalle necesario.

registro de cada vez que se utiliza la regla y envíe un alerta al administrador de la red cuando la regla intente ser violada.

## Filtrado de accesos por tiempo

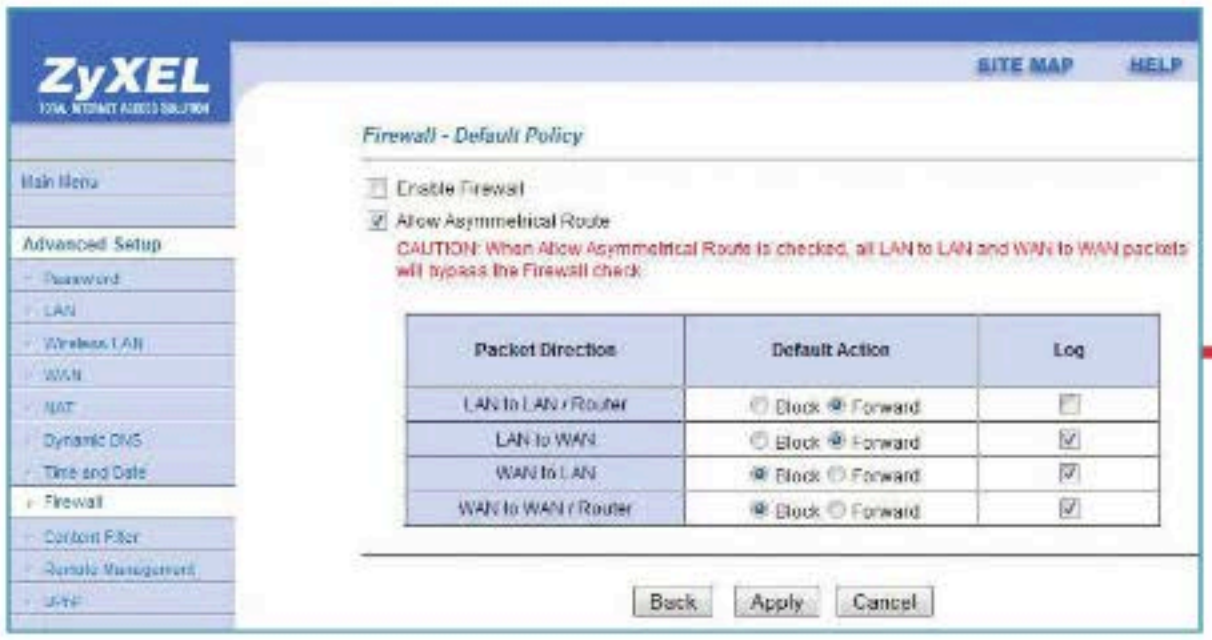
Otra forma de administrar los bloqueos de acceso es por tiempo. ¿En qué consiste esta técnica? Simple: se especifican horarios y días de la semana en los que el bloqueo se hace efectivo. Fuera de esas especificaciones, el acceso a la conexión no tiene restricciones más allá de las que indiquemos en otros apartados.
Para activar el filtrado de acceso por tiempo, hacemos clic en **Content Filter**; en la siguiente pantalla, presionamos en la opción **Schedule** para acceder a la configuración. En la pantalla que se presenta a continuación, veremos dos secciones claramente diferenciadas: **Days to Block** y **Time of Day to Block**.

### LOS DATOS PARA ACCEDER AL PANEL WEB SE ENCUENTRAN EN EL MANUAL DEL ROUTER.

En la primera sección, podemos seleccionar individualmente los días en que queremos que el bloqueo sea efectivo, marcando las respectivas casillas de verificación; o, simplemente, podemos marcar **Everyday** para que el bloqueo se active todos los días.
En lo que respecta a las horas del bloqueo, el router que tomamos como ejemplo utiliza el formato de 24 horas. Una vez más, podemos activar la casilla **All day** para bloquear el acceso durante las 24 horas, o indicar la hora y los minutos en que comenzará la acción, seguido de la hora y los minutos en que terminará. Solo resta presionar **Apply** para guardar los cambios.

## Bloqueo de acceso por host

El bloqueo de acceso por host es conocido también con el nombre de **Access List**.




**Para habilitar el firewall, debemos ingresar en la pantalla que vemos en la imagen y activar el servicio. Las reglas se configuran en otro apartado.**

Suele encontrarse bajo ese nombre en los routers que ofician exclusivamente como tales. En el dispositivo que estamos utilizando como ejemplo, no veremos las listas de acceso por dos motivos: porque es un dispositivo tecnológicamente antiguo (tiene más de un lustro en actividad y aún cumple su función a la perfección), pero, además, no es simplemente un router, sino que incorpora la capacidad de obtener acceso a nuestro servicio ADSL. De todos modos, veremos de qué manera implementar un sistema, aunque no igual pero bastante similar, con las limitaciones del caso.
Como vimos anteriormente, accedemos a **Content Filter** y seleccionamos la opción **Trusted**. Dentro de su configuración, encontraremos dos cuadros de texto en los que ingresamos las IP de inicio y final del rango de IPs a las que queremos que no se les aplique ninguno de los bloqueos o restricciones configuradas. Por sí mismo, este método no bloquea absolutamente nada, sino que brinda una especie de salvoconducto para las IPs comprendidas en el rango configurado. Si configuramos el bloqueo de acceso por tiempo para que se active todos los días, estaremos bloqueando el acceso al router, aunque si configuramos el rango permitido en **Trusted**, generaremos una lista de acceso.
Además, podemos configurar el servidor DHCP en forma estática y asignar una IP fija a una MAC Address en particular, para lograr que la configuración realizada en **Trusted** sea más robusta todavía. ■

**Desde el apartado Content Filter, podemos activar bloqueos por tiempo y permisos por rangos de IPs de confianza.**

# Protocolos WEP y TKIP

El protocolo TKIP cumplió un importante papel en el reemplazo temporal de WEP y, aunque pronto quedó obsoleto, fue un gran avance en su momento. Aquí conoceremos sus detalles.

Cuando surgió el protocolo **WEP**, todo parecía estar bajo control, pero los hackers e investigadores de seguridad informática no tardaron en encontrarle una serie de vulnerabilidades que, como ya hemos visto, hicieron que quedara obsoleto en pocos años. Al principio, no se pensaba que su vida iba a ser tan corta, pero una vez más, los cálculos de los ingenieros que desarrollaron WEP no fueron precisos. Entonces se creó **TKIP**, sigla de **Temporal Key Integrity Protocol**, también denominada hashing de clave WEP.

## Seguridad

Con el ocaso de WEP, que ya no proveía suficiente seguridad en la capa de enlace, uno de los problemas que se encontraron fue que no se podía desperdiciar todo el hardware que se había creado y comercializado para los sistemas Wi-Fi, y fue preciso encontrar una solución que incluyera retrocompatibilidad y que solo requiriera una actualización en el firmware de los dispositivos inalámbricos. TKIP utiliza como base el mismo algoritmo que WEP, pero con una construcción de llaves de cifrado más robusta que este. Hacia fines del año 2002, la **Wi-Fi Alliance** y el grupo de trabajo de **IEEE802.11i** definieron el estándar TKIP bajo el nombre de **Wi-Fi Protected Access** (**WPA**); más tarde se incluyeron sistemas ya conocidos y bien probados, como el protocolo 802.1X y el algoritmo criptográfico AES (el estándar internacional de la criptografía simétrica). Posteriormente pasaron dos años más hasta que se publicó el protocolo que se conoció como **WPA2**, con la especificación completa y la incorporación de **AES** como estándar de cifrado.


La idea principal de TKIP había sido oficiar como solución temporal para resolver el problema natural de WEP acerca de la reutilización de los **vectores de inicialización** (**IV**). En este punto, es necesario recordar que, para encriptar los datos, WEP se encarga de usar el mismo vector de inicialización de manera periódica; esto constituye la base de prácticamente todos los ataques que fueron concebidos contra él.

## Funcionamiento

El proceso de funcionamiento de TKIP se inicia con la existencia de una clave temporal de 128 bits que se comparte entre los distintos clientes que se encuentran conectados a los puntos de acceso en la red inalámbrica. Luego TKIP combina esta clave temporal con la dirección MAC del cliente remoto y adiciona un vector de inicialización de 16 octetos, para generar la clave que cifrará los datos. De esta manera, se consigue que cada equipo utilice diferentes flujos cifrantes, ya que dependen de su propia dirección MAC, además de la clave común a todos los equipos. También aplica un hash para proteger los vectores de inicialización débiles por cada paquete, de modo que estos no queden expuestos.

Con respecto a lo que mencionamos sobre la retrocompatibilidad, TKIP continúa utilizando el algoritmo **RC4** para encriptar los datos; pero, a diferencia de WEP, las claves de cifrado se cambian cada 10.000 paquetes, lo que proporciona un método que garantiza una mayor seguridad. Por ejemplo, si un atacante quisiera romper una clave basada en TKIP, y el conjunto de 10.000 paquetes atravesaran la red

inalámbrica en un período de cinco minutos, entonces tendría solo cinco minutos para romper el cifrado; y no solo eso, sino que, en caso de romperlo en cuatro minutos, solo le quedaría uno para utilizar la red con la clave descubierta, porque a los cinco minutos la clave volvería a cambiarse automáticamente. En redes con mayor cantidad de tráfico, los 10.000 paquetes se alcanzarán más rápidamente, por lo que el tráfico en exceso no debilitará al propio protocolo, como sí ocurría con WEP, en el que, al haber más paquetes viajando por la red, aumentaba sustancialmente la probabilidad de romper la clave o también descifrar los datos que se encuentran en tránsito.

Sobre la base de estas variaciones que no incluyeron nuevos algoritmos complejos que hubiera que resolver con otro hardware, las empresas y los particulares encontraron una gran ventaja en el uso de TKIP, porque pudieron aumentar su nivel de seguridad sin cambiar los dispositivos, que por aquel entonces tenían un costo bastante más elevado que en la actualidad. No obstante, los especialistas no tardaron en aclarar que la solución de TKIP era tan temporal como la T de su sigla, y que pronto debía incluirse un nuevo estándar.


El portal especializado Security By Default se hizo eco de las entonces nuevas vulnerabilidades de TKIP en el año 2009.

## Mejoras

Otra de las mejoras que TKIP introdujo en la seguridad de las redes inalámbricas fue un nuevo sistema de verificación de integridad. Estos sistemas se llaman de forma genérica **MIC**, por **Message Integrity Codes** (códigos de integridad de mensajes), para diferenciarlos de otra de las acepciones de **MAC** (**Message Authentication Code**) que se confundía usualmente con otros usos de esta sigla, como **Medium Access Control** o **Mandatory Access Control**. MIC evitó los ataques llamados de **bit-flip** en paquetes cifrados, que implicaban que el receptor aceptara un mensaje al que se había realizado una modificación, sin poder comprobarlo. Tengamos en cuenta que los ataques de bit-flip se basan conceptualmente en el cambio de un bit en el texto cifrado, de tal modo que este pueda ser reflejado de forma predecible en el texto plano, aunque el atacante no esté directamente habilitado para leer el texto plano en sí mismo.

Este tipo de ataques no está directamente dirigido al cifrado, como lo haría el criptoanálisis, sino sobre un mensaje en particular o una serie de mensajes. Dependiendo la forma en que se aplique, esto podría derivar también en una denegación de servicios contra todos los mensajes de un canal en especial que utilice un determinado mecanismo de cifrado. El ataque es especialmente peligroso cuando el intruso conoce el formato del mensaje, por lo que puede modificarlo para obtener un mensaje similar, pero con alguna diferencia importante.

Aunque el protocolo TKIP no es el más utilizado, los routers mantienen la compatibilidad con él.

**SI BIEN EL PROTOCOLO TKIP FUE UNA BUENA TRANSICIÓN DESDE WEP HASTA WPA2, SU VIDA ÚTIL RESULTÓ CORTA.**

Por ejemplo, un cambio en la dirección de destino podría alterar la ruta del mensaje, por lo que se podría forzar el recifrado de modo más débil; entonces, las posibilidades de descifrarlo crecerían. Los cifrados de flujo como RC4 son vulnerables a este tipo de ataques, y dado que WEP se basa en RC4, esto constituyó un problema que, incluso, se conocía antes de implementar masivamente TKIP, que lo seguia utilizando.

La solución debió incluir la posibilidad de autenticar los mensajes con alguna especie de clave extra o firma digital, para conseguir que, si algún bit se cambiara en el camino entre el cliente y el punto de acceso, pudiera ser detectado al instante; en pocas palabras, para evitar ataques de **man-in-the-middle**. Esta funcionalidad de MIC en TKIP puede ser específicamente habilitada en los puntos de acceso y routers inalámbricos que la posean.

En TKIP, si dos mensajes no logran ser verificados por su MIC en un periodo de 60 segundos, el dispositivo regenera la clave temporal y cambia de esa forma el cifrado de los siguientes paquetes. El algoritmo de MIC implementado en TKIP utiliza 64 bits y se conoce con el nombre de **Michael**.

A COMIENZOS DEL AÑO 2009, EL PROTOCOLO TKIP FUE DADO DE BAJA POR LA IEEE Y SE DEJÓ DE UTILIZAR EN FORMA OFICIAL.

## Ataques

Pese a su constante mecanismo de autenticación por regeneración de claves temporales, TKIP no necesita un servidor **RADIUS** para funcionar, aunque dicho sistema de autenticación y autorización podía incorporarse en caso de querer reforzar el sistema de control de acceso a la red.
Dos ataques conocidos que se dieron sobre TKIP fueron el de Beck-Tews y el de Ohigashi-Morii. El primero se basó en la vulnerabilidad del protocolo al ataque de recuperación de secuencia, que si se logra implementar, permite al atacante transmitir una serie de entre siete y quince paquetes a discreción dentro de la red. Este ataque fue detallado en un documento de investigación de Martin Beck y Erik Tews a finales del año 2008. Un año más tarde, otro investigador realizó modificaciones sobre este ataque, y consiguió la inyección de hasta 596 bytes maliciosos en un período de menos de veinte minutos.
El otro ataque conocido, también basado en el anterior, fue desarrollado por dos investigadores japoneses, Toshihiro Ohigashi y Masakatu Morii. Ellos descubrieron una manera más simple y rápida de realizar lo mismo, pero utilizando la técnica de man-in-the-middle y sin requerir la habilitación del sistema de **QoS** (**Quality of Service**) en el Access Point remoto, que era un requisito para los ataques anteriores.
A comienzos del año 2009, TKIP fue dado de baja por la IEEE y se dejó de utilizar oficialmente, con lo cual, a partir de ese entonces, no se esperaría que se siguiera usando en contextos comerciales, aunque esto no haya sido así de inmediato. ■

## Ataques a distintos niveles

A medida que los algoritmos criptográficos se estandarizaron y los protocolos de red mejoraron, los atacantes enfocaron sus esfuerzos en las implementaciones de hardware o de software. Se encontraron fallas en firmware que llevaron los problemas de seguridad a niveles que trascendían las teorías puras de los protocolos y los métodos de seguridad.

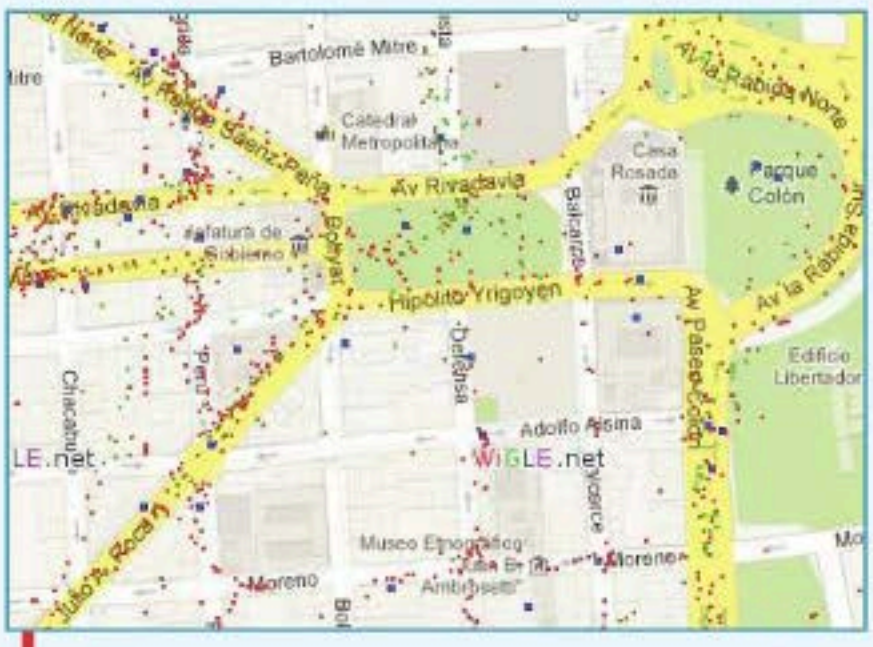
# Qué es el wardriving

## Buscar redes inalámbricas Wi-Fi empleando un vehículo en movimiento parece un argumento sacado de una película; veamos cómo funciona.

Se llama **wardriving** a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Su nombre deriva del **wardialing** (basado en la película *Juegos de Guerra*, de los años 80), pero no se limita solo a la búsqueda de redes Wi-Fi libres, sino que también implica localizar sistemas informáticos, como en la mencionada película, donde un joven hacker intenta infiltrarse en sistemas ajenos por simple curiosidad.
Originalmente, implicaba el escaneo de redes desde una notebook en un automóvil, pero hoy en día, se popularizó el uso del smartphone para el mismo propósito, con la ventaja de la **geolocalización** por GPS. Tengamos en cuenta que el objetivo del wardriving es localizar una red vulnerable para, luego, hacer un posterior análisis de ella en el lugar.
El sitio más popular para esta práctica, en donde se registran todos los hallazgos, es **WiGLE** (*Wireless Geographic Logging Engine*, **http://wigle.net**). Allí se registran no solo las redes Wi-Fi, sino también las posiciones de las torres de telefonía celular.
Para Windows, el software más usado es **NetStumbler** (**http://stumbler.net**), pero existen equivalentes para todas las plataformas, con hincapié en los sistemas operativos de los smartphones. Tan solo debemos buscar wardriving en nuestro market. Una variante muy interesante es el **Bus Wardriving**, que aprovecha los aburridos trayectos en colectivo y evita los riesgos de conducir por la ciudad con un ojo puesto en la notebook.


Hasta el gigante de Mountain View fue acusado de realizar wardriving desde el Street View Car, por la recolección de datos y redes Wi-Fi.

No debemos confundir esta práctica con una comunidad inalámbrica en la que los usuarios deciden construir una red para garantizar el acceso universal a la sociedad. Para quienes practican wardriving, el objetivo es saber qué hay dentro de una red vulnerable, al igual que sucedía con la antigua técnica de wardialing, que consistía en hacer llamadas automáticamente con el fin de encontrar módems conectados.

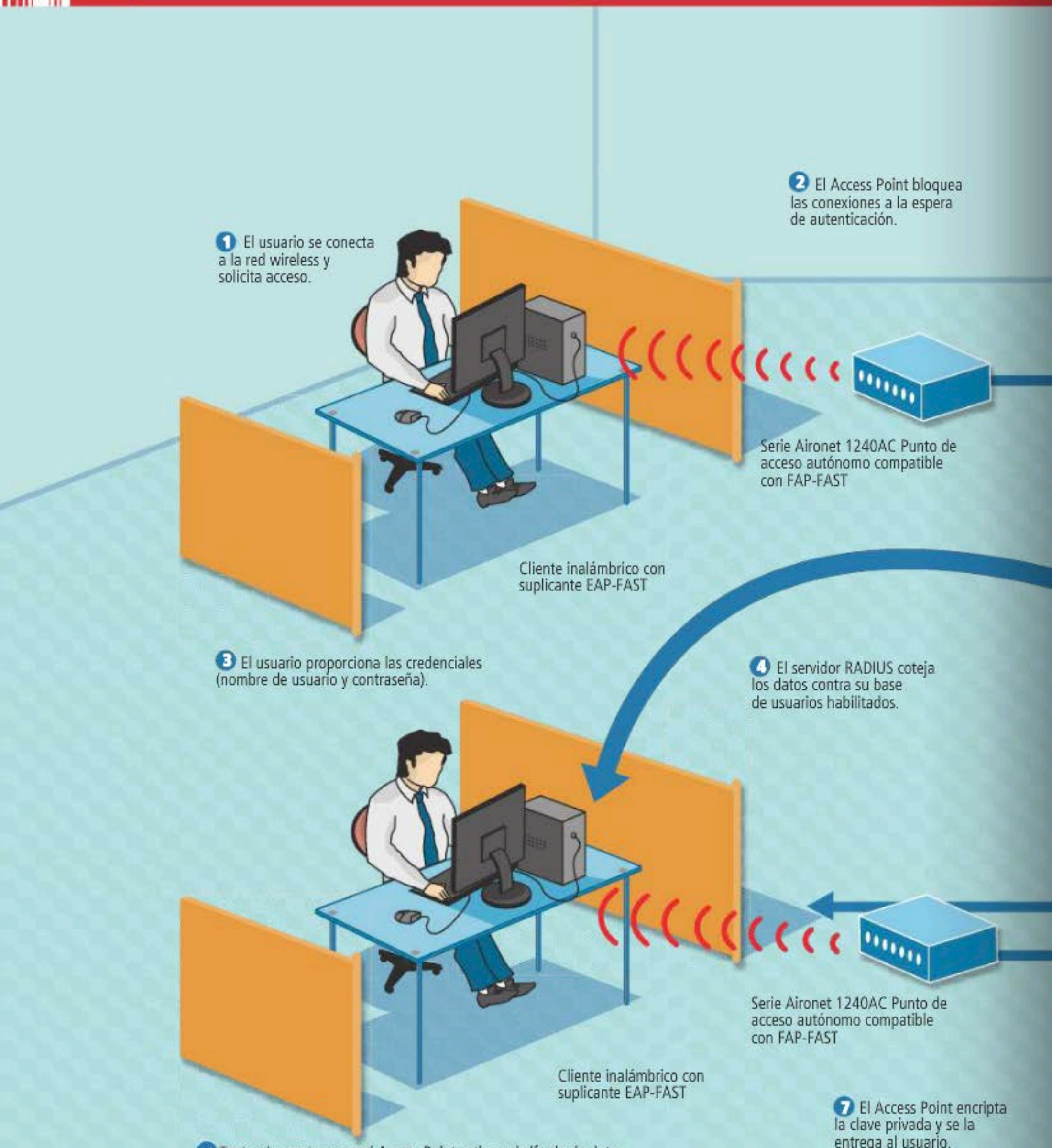



La ciudad de Buenos Aires es escaneada permanentemente sin que nos demos cuenta.

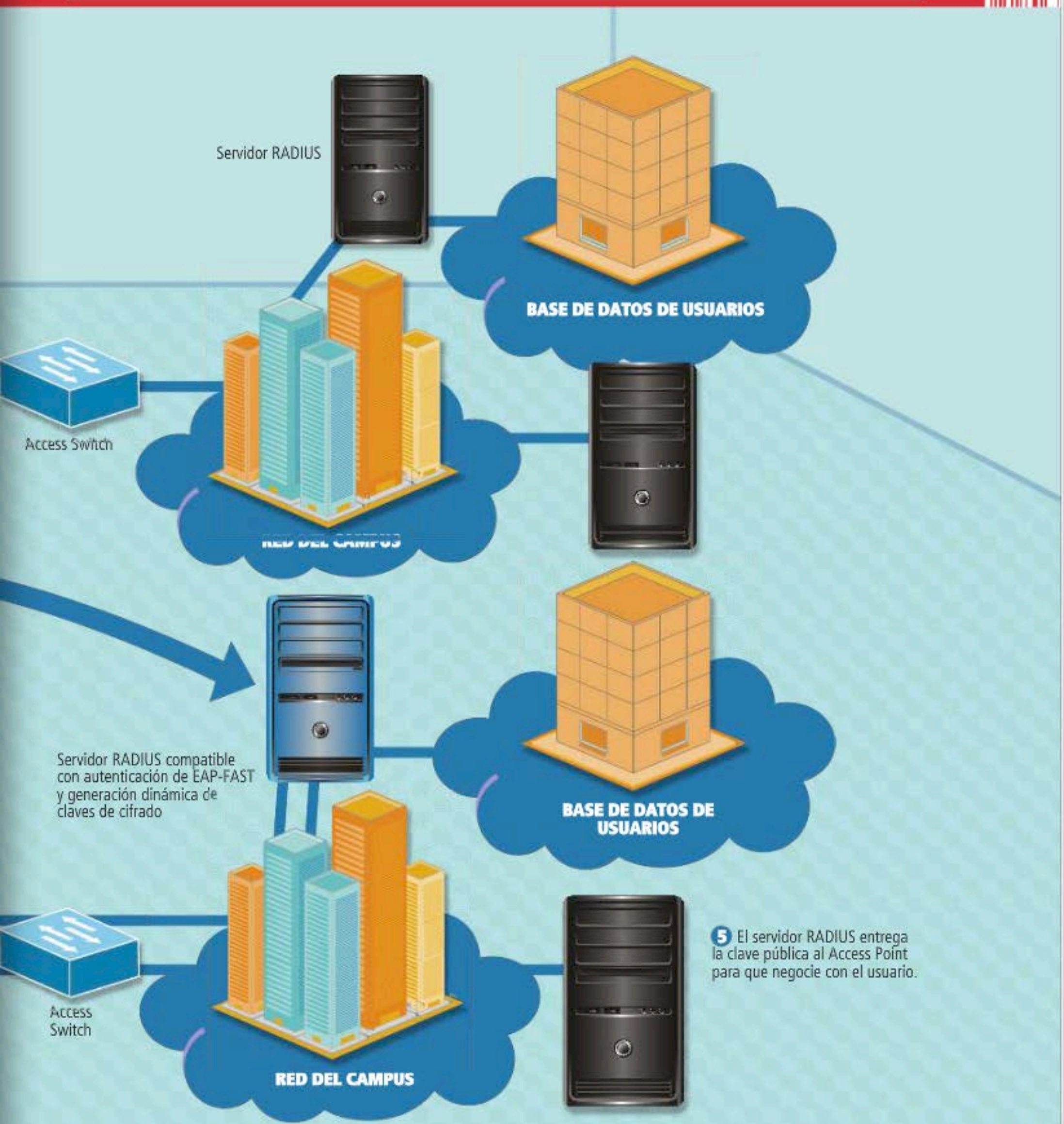
### EL WARDRIVING LOCALIZA UNA RED VULNERABLE PARA, LUEGO, HACER UN POSTERIOR ANÁLISIS EN EL LUGAR.

Un dato curioso es que, hace algunos años, Google fue acusado en Europa de practicar wardriving desde su famoso auto para Street View, por medio de la captación de datos de localización de Wi-Fi con identificación de sus titulares y de datos de las comunicaciones. Aunque el buscador en principio respondió que nunca había ocultado esta práctica y que se utilizaba para ofrecer servicios de geolocalización a los usuarios, más tarde reconoció en su blog oficial que sí lo practicaban, y entonces todos los datos recopilados fueron eliminados. ■

# Autenticación de la red

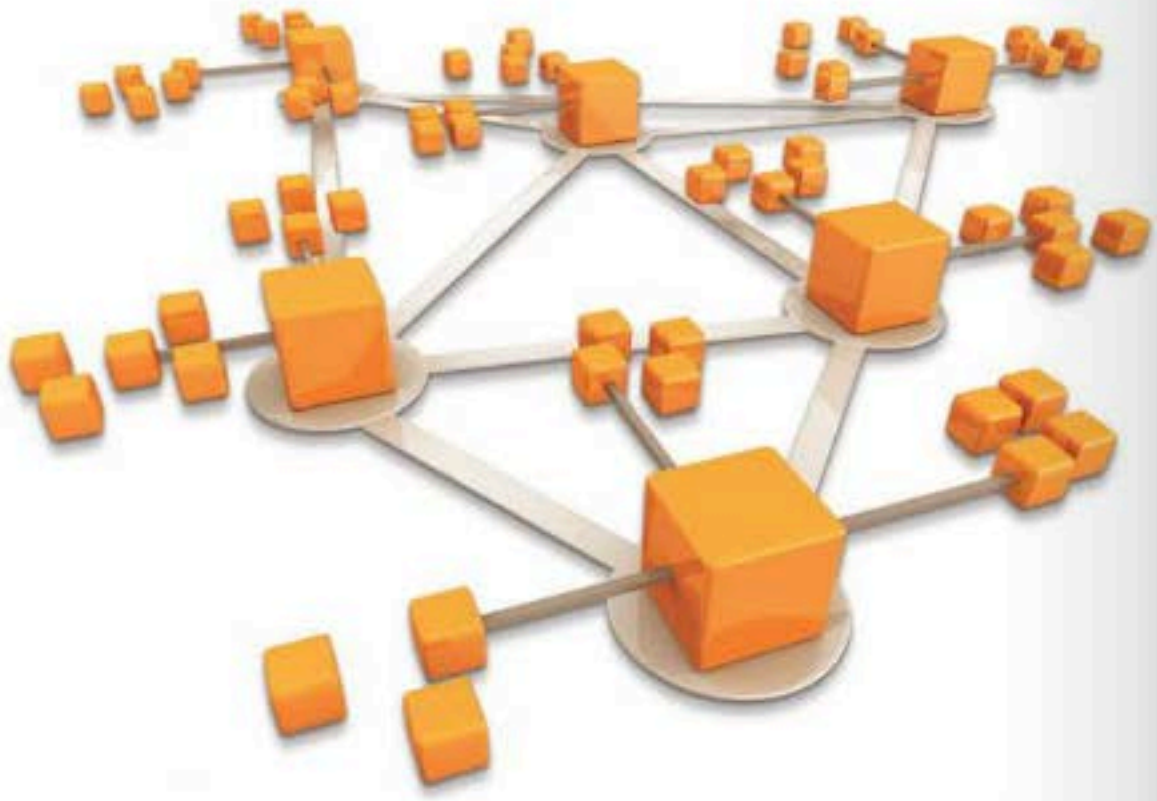


EN ESTAS PÁGINAS VEREMOS INFORMACIÓN BÁSICA
SOBRE LOS PROCESOS DE AUTENTICACIÓN DE LA RED.



# Tipos de antenas y repetidores de señal

La movilidad que nos brinda una conexión Wi-Fi es indiscutible. Aquí optimizaremos un router y crearemos enlaces punto a punto.



Cuando pensamos en Wi-Fi, lo primero que se nos viene a la mente es nuestra notebook con una conexión hogareña; y un router que, a veces, es provisto por el ISP, con un alcance promedio no mayor a los veinte metros, porque es fabricado para uso domiciliario y no siempre es suficiente para cubrir la distancia o la intensidad que queremos. En su diseño original, el router o Access Point incluye una antena isótropa, es decir, que irradia energía en todas las direcciones en forma uniforme para darle una mayor cobertura a la vivienda u oficina donde se instale.

**UNA ANTENA ES UN ELEMENTO PASIVO QUE NO APORTA ENERGÍA A LA SEÑAL DEL ROUTER.**

## Antenas

Para no tener que apuntar con nuestra PC al router (lo que nos obligaría a mantener el equipo en una posición fija), se utilizan antenas omnidireccionales, que son independientes de la posición en cuanto a la recepción de la señal. Estas antenas emiten señal hacia todos lados, a costa de desperdiciar potencia. Una antena es un elemento pasivo, es decir, no aporta energía a la señal que viene desde el router o Access Point. Pero aunque no aporte energía, sí tiene ganancia, que se expresa en relación a la potencia en dBi (*i* de isótropa).

Cuando decimos que una antena tiene una ganancia de 7 dBi, significa que ha ganado 7 decibeles respecto a una antena isótropa. Entonces, la antena tendrá una ganancia de X cantidad de veces en referencia a la antena que viene originalmente con el Access Point. Las antenas direccionales tienen una ganancia de esa cantidad en una sola dirección, por lo que tendrán una pérdida igual o mayor en otra.

## Frecuencias

Una red Wi-Fi utiliza un radio de frecuencias para comunicarse entre dispositivos que trabajan con el estándar **IEEE 802.11**, que define el uso de los niveles inferiores de la arquitectura OSI: la capa física y la de enlace de datos. La revisión 802.11a opera en la banda de 5 GHz, y el estándar 802.11b y 802.11g funciona en la banda de 2.4 GHz.

## Antenas de interior

Una antena de interior es la primera solución en caso de que necesitemos tener una mayor cobertura. Por lo general, es de 7 u 8 dBi, y mejora significativamente el alcance de una red inalámbrica y la potencia de la señal en todas direcciones. Evita el gasto de agregar Access Points adicionales o repetidores inalámbricos, porque podemos instalar con rapidez una simple antena. La mayoría de las antenas del mercado cuentan con un conector SMA. Debemos verificar que nuestro equipo cuente con dicho conector, ya que los routers más económicos no disponen de ningún tipo de ficha, y la antena no siempre es desmontable. La antena cuenta con una extensión de cable promedio de 1,5 metros, que le da una mayor flexibilidad en el montaje. Suele venir con un kit para base de montaje (a veces, imantada), lo que

permite una transmisión óptima de la señal para todos los ambientes, condiciones y orientación en distintos ángulos. Sus ventajas son las siguientes:

- Económico.
- Instalación Plug & Play.

Su desventaja es la dependencia de la estructura edilicia.

## Antenas de exterior

Hay mucha variedad en el mercado, y eso puede generar confusión porque implica tener en cuenta el rango de frecuencia, ganancia, potencia y el patrón o ángulo de radiación, tal como mencionamos:

- La **frecuencia** está dada por la norma: 802.11b y 802.11g funcionan en 2,4 GHz, y la 802.11a en 5 GHz.

- El cálculo de ganancia es el mismo que empleamos en las antenas para interior.

- El nuevo factor es la potencia: un sucinto examen de las especificaciones técnicas del equipo que instalemos (router o AP) revelará que tiene una potencia de transmisión de X dBm. Como ya vimos, dB significa 'decibeles' (la unidad utilizada en estos cálculos); y dBm significa 'decibeles relativos al nivel de referencia de 1 milivatio' (mW). Como referencia, sabemos que 20 dBm, 100 mW es la potencia típica de un router inalámbrico Wi-Fi.

- Patrón de radiación (**pattern**): las antenas de altas ganancias tienden a ser direccionales, es decir, se apuntan hacia la fuente y tienen un ángulo de acción angosto. El pattern dibuja el espectro para determinar dónde hay mayor ganancia en la antena.

Para la instalación de antenas de exterior, entran en juego otros factores, como la pérdida del cable. La distancia del cable, el grosor y los conectores o adaptadores pigtail influyen en la performance. Por cada uno de los factores anteriores, hay fórmulas de cálculo que podremos encontrar en la Web fácilmente; incluso, los mismos fabricantes proporcionan herramientas para simplificar el trabajo de instalación.

## MIMO

Hoy es común encontrar equipos con tecnología **MIMO** de entrada múltiple, salida múltiple (*Multiple-Input & Multiple-Output*), que utilizan varios transmisores y receptores para transferir más datos al mismo tiempo y, consecuentemente, varias antenas (dos o tres). La tecnología MIMO aprovecha las ventajas de un fenómeno de ondas de radio denominado multiruta, en el que la información transmitida rebota en las paredes, techos y otros objetos. MIMO aprovecha las ventajas de múltiples rutas para combinar la información de varias señales y, así, mejorar tanto la velocidad como la integridad de los datos.
La principal razón para que un usuario final quiera aplicar una tecnología MIMO es lograr velocidades de hasta 600 Mbit/s; esto es diez veces más que el estándar 802.11g (el protocolo de red inalámbrico más popular).

**Con similares prestaciones a la antena parabólica, la principal ventaja que tiene la antena de tipo parrilla es el menor peso.**

Sus ventajas son:

- Mayor velocidad.
- Mínima tasa de error.

La principal desventaja es que, en caso de necesitar una mayor cobertura, el reemplazo de tres antenas al mismo tiempo, tal vez, no sea económico.

## Access Point

El Access Point es, hoy en día, la mejor opción para tener una conexión Wi-Fi que nos permita alcanzar una mayor cobertura, roaming transparente y funciones de bridging.
Para una pyme, el punto débil de la conexión a Internet es el router hogareño con Wi-Fi. Un router robusto

## Smartphone

**Nuestro teléfono celular puede ser una poderosa herramienta a la hora de planificar la cobertura de una planta. Sin importar el SO que utilicemos, el mercado está plagado de muy buenas aplicaciones que nos ayudarán con nuestra red Wi-Fi. Con un analizador, podremos determinar qué canales están libres, cuál es la intensidad en dBi de la señal, y encontrar puntos ciegos. Incluso, podemos encontrar apps para cargar el plano de la planta que queremos cubrir.**

Aquí vemos una clásica antena parabólica (conocida como dish antenna) para enlaces de tipo punto a punto.

(corporativo) no cuenta con Wi-Fi, y la forma de armar una red inalámbrica es con la instalación de, al menos, un AP. Para esta función, la conexión del AP es muy sencilla, casi plug & play: solo debemos conectar el equipo a la red por medio de un conector RJ-45 y configurar los niveles de seguridad que creamos convenientes.
La aplicación más común de un AP es la de sumar rangos de cobertura. Por ejemplo, en un edificio con dos pisos, podríamos instalar uno por cada piso y, así, lograríamos cobertura en todo el lugar. Sin importar dónde se ubique el usuario, siempre se garantizará conexión. Pero aunque esta parezca ser la mejor solución, hay que tener en cuenta cuál será la mejor experiencia para el cliente.

## PARA COMPENSAR LA FALTA DE VELOCIDAD, SUELE TRABAJARSE CON TECNOLOGÍAS MIMO.

El SSID (*Service Set IDentifier*) es el identificador de red inalámbrica, y es provisto por el AP. Cuando configuramos el Access Point, lo primero que debemos hacer es asignarle un SSID.

En nuestro ejemplo, a los distintos Access Points de cada planta les daremos nombres como:

- Empresa_AP_PB
- Empresa_AP_Primer_Piso
- Empresa_AP_Segundo_Piso

En primera instancia, esto se presta a confusión para el usuario y nos obliga a registrarnos tres veces (una vez por cada equipo). Sería algo así como si quisiéramos usar la red Wi-Fi del vecino dependiendo de si estamos en nuestra casa o en la puerta de calle.

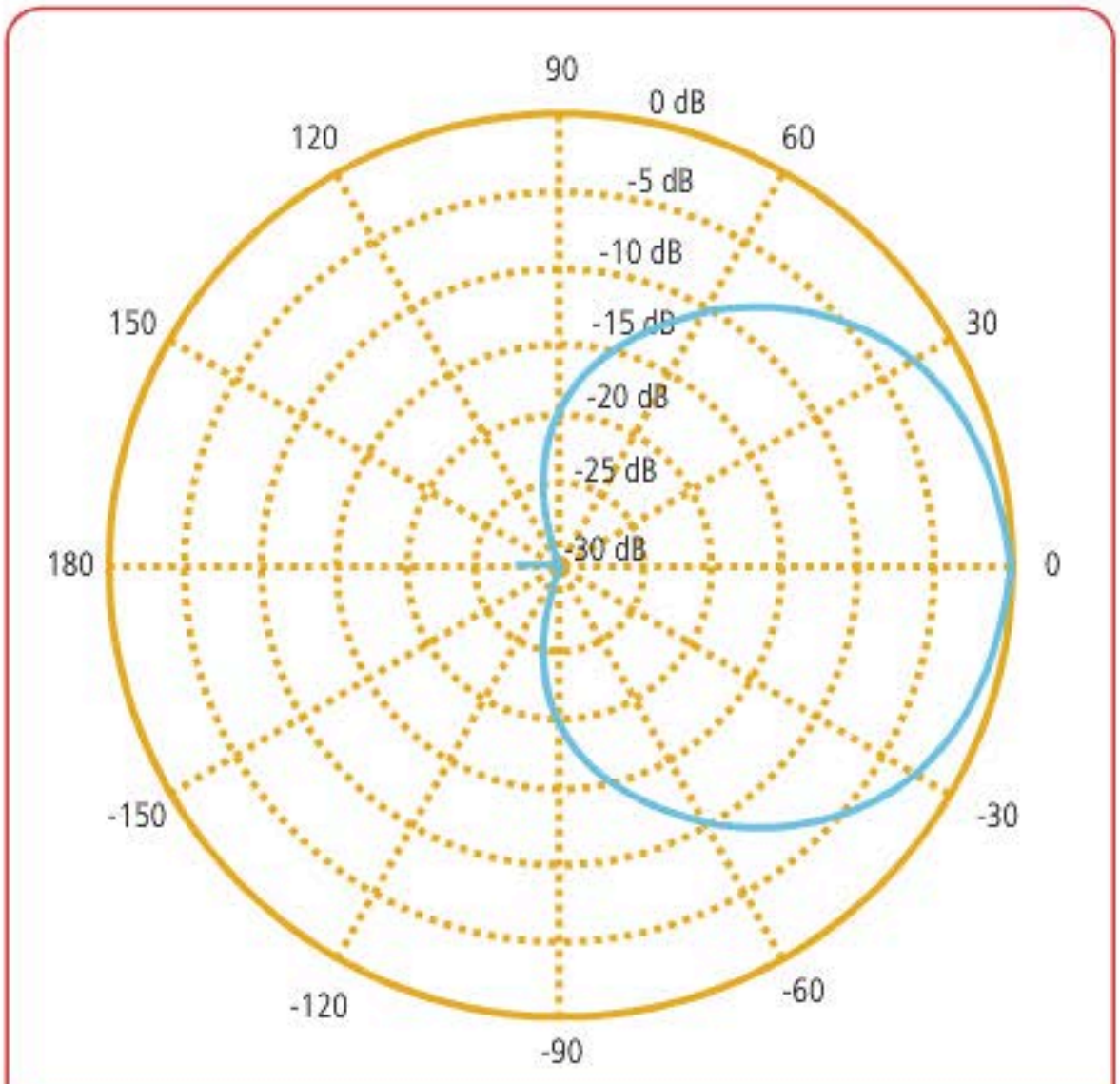
## WDS

Cuando se diseñó el estándar 802.11, se pensó en la WDS (*Wireless Distribution System*), una función que nos permite establecer la interconexión inalámbrica entre los Access Points.
De esta manera, podremos usar el AP del primer piso como repetidor de la señal de planta baja, o como repetidor de la señal del segundo piso.
Con WDS, un AP puede funcionar solo como AP, como puente con otro AP (brigde) o ambas cosas. De esta manera, podemos incrementar una red inalámbrica, dado que cada Access Point se conecta a cualquier otro Access Point disponible de forma cableada o inalámbrica.
Para configurar un WDS, se requiere que todos los equipos usen el mismo espectro de radiofrecuencia (2,4 GHz o 5 GHz), y es altamente recomendable que sean de la misma marca y modelo. Por supuesto, todos deben soportar la función WDS y utilizar el mismo canal.
En cada AP hay que introducir la dirección MAC del otro AP. Para establecer la seguridad inalámbrica, podemos utilizar cifrado WEP (no suele funcionar con WPA), compartir las claves y filtrar direcciones MAC.
Otra aplicación es la de modo repetidor para expansión de la red inalámbrica. Imaginemos una instalación de uso industrial, en donde queremos atravesar el edificio y el cableado, que se dificulta por las maquinarias intermedias. Con un AP (sin cablear) en el centro, podríamos repetir la señal recibida al AP más lejano.

Algunos equipos montan el AP sobre el foco, lo que anula el factor de pérdida por cable.

## Parabólica

Cuando necesitamos un enlace a larga distancia, se nos viene en mente la clásica antena satelital del tipo microondas. La aplicación más frecuente es en un enlace punto a punto (point to point, o PtP).
Estas antenas se caracterizan por llevar un reflector parabólico, cuya superficie refleja las ondas electromagnéticas generadas por un pequeño dispositivo radiante desde el foco del paraboloide. El reflector parabólico se encarga de concentrar en su foco la señal de las ondas que recibe.
Las antenas parabólicas (Dish Antenna) pueden ser transmisoras, receptoras o full duplex, y son utilizadas generalmente en frecuencias altas, en la banda de 5 GHz (aunque también las hay en 2,4 GHz). Para compensar la falta de velocidad, suelen trabajar con tecnologías tipo MIMO (equivalente a dos antenas). Utilizando un solo reflector parabólico, en el foco de la antena, en realidad, hay dos receptores.
Para evitar la pérdida por cable, el montaje del Access Point se realiza en la parte trasera del plato, de manera que la distancia del cable es de apenas 20 cm hasta el foco del reflector.




La superposición y el montaje aseguran una cobertura total.

Las ventajas de esta tecnología son:

- Mayor velocidad.
- Mínima tasa de error.

Como desventaja, podemos mencionar un reducido ángulo de cobertura.

## Parrilla

El reflector parabólico se encarga de concentrar en su foco la señal de las ondas que recibe. Se distingue porque, en vez de un plato, la estructura es en forma de parrilla, más liviana (en el peor de los casos, menos de 2 kilos), lo que facilita su instalación en altura, y también, menos vulnerable a los vientos. Para ciertas condiciones climáticas, montar un plato de 60 centímetros a 15 metros de altura es muy recomendable.

## Sector

Una antena de sector es un tipo de antena de microondas direccional cuyo concepto es formar parte de una circunferencia y lograr una cobertura de 360 grados.

Los diseños típicos son de 90° y 120°, de modo que con tres o cuatro antenas completamos la cobertura total. A menudo, tiene unos grados extras para asegurar la superposición y el montaje. Existen modelos de antenas que ajustan su grado de cobertura, lo cual nos da el beneficio de la escalabilidad. Podemos empezar con tres antenas ajustadas a 120° y, con el tiempo, sumar otras hasta duplicarlas. Sus ventajas son:

- 360° de cobertura.
- Mayor alcance que una antena omnidireccional.

Su desventaja es el costo más elevado.

## Omnidireccional

Con seeguridad, es la antena más simple de instalar, porque no requiere orientación ni ajuste de ningún tipo. Sus ventajas son las siguientes:

- 360° de cobertura.
- Bajo costo.

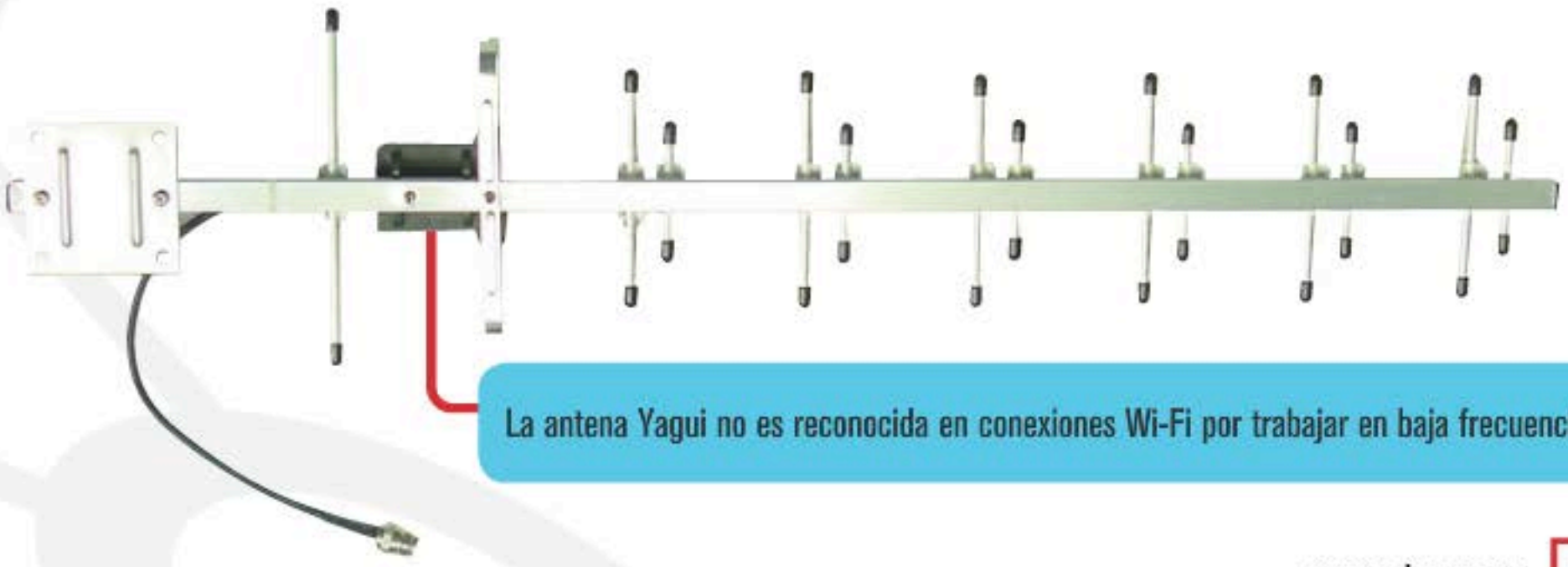
Su principal desventaja es el alcance limitado.

## Yagui

Por trabajar en 900 MHz, estas antenas no suelen asociarse con una red inalámbrica Wi-Fi, pero se comercializan en conjunto con APs de la misma frecuencia y con tecnología MIMO, lo que nos dará una velocidad aceptable y un muy buen alcance.

## Seguridad

Una instalación del tipo punto a punto, de alta frecuencia y con un ángulo reducido es la menos vulnerable, ya que, para poder hacer una intromisión, el atacante debe interponerse en el campo visual de las dos antenas con un equipamiento específico. Por otro lado, cuando instalamos un servicio de Hot Spot, debemos ser conscientes de que cualquier extraño tendrá acceso a la red, por lo que tendremos que implementar seguridad adicional en nuestro servidor. ■



La antena Yagui no es reconocida en conexiones Wi-Fi por trabajar en baja frecuencia.

# Consejos para mejorar la señal wireless

Veremos varias formas de mejorar el alcance e intensidad de una red Wi-Fi, solucionando los errores comunes y optimizando la configuración.

Durante la instalación de un router hogareño, este dispositivo siempre termina al lado del televisor o junto al teléfono inalámbrico, ya que nuestro proveedor de Internet suele ser por TV cable o línea telefónica; casualmente, esas son las peores ubicaciones. La primera recomendación es que el router esté alejado de equipos electrónicos que puedan generar interferencia en la señal, como la TV, el teléfono inalámbrico y hasta un celular.

**SI AUMENTAMOS LA GANANCIA DEL ROUTER, TAMBIÉN DEBEMOS AUMENTAR LA GANANCIA EN LA PC, YA QUE LA COMUNICACIÓN ES FULL DUPLEX.**

Pero también debemos prestar atención a lo que hay del otro lado de la pared: un microondas en la cocina a escasos centímetros no solo perjudicará la señal, sino que también puede dañar físicamente nuestro router. Por otra parte, una heladera con una parrilla trasera metálica de casi 2 metros de altura seguramente nos dejará sin señal.


Otro error muy común de los proveedores de Internet es instalar equipos en la periferia de la vivienda (al lado de la ventana). Lo ideal es que la instalación sea en el centro de esta, para logar una mejor cobertura con una antena isótropa. Esta ubicación también fortalece la seguridad, al evitar que la señal se escape por las ventanas y que un extraño intente ingresar en nuestra red. La calefacción, el aire acondicionado, y los lugares pequeños y cerrados donde guardamos los equipos (como un placard) son factores externos que atentan contra la performance de la señal.

## Canal

Casi todos los routers y access points vienen preconfigurados en CH6, y un vecino podría perjudicarnos al competir por el mismo canal. El canal es la frecuencia a la cual trabaja el equipo. Lo ideal sería que, antes de configurar el router, verifiquemos qué canales están libres en el espectro que nos rodea. Algunos routers incluyen la herramienta necesaria para ver el tráfico de señales, aunque la opción más simple es instalar un analizador de Wi-Fi en nuestro smartphone.

## Cambio de antena

Si pensamos cambiar una antena de interior para lograr mayor alcance en nuestra vivienda, tengamos presente que la comunicación es en ambos sentidos (full duplex). En el caso de una notebook, un adaptador Wi-Fi por USB sería lo más práctico y cómodo, pero estos dispositivos no suelen tener más ganancia de la que originalmente viene en la notebook. Entonces, deberíamos pensar en instalar un AP como cliente. No obstante, el uso de una antena direccional en vez de una multidireccional nos permite orientarla mejor para aprovechar la conexión. Si aumentamos la ganancia en el router, también debemos aumentar la ganancia en la PC, porque la comunicación es full duplex.

## Access Point

Sin dudas, el AP siempre es la mejor opción a la hora de mejorar la cobertura de la señal Wi-Fi. WDS (*Wireless Distribution System*) es la función que nos permite la interconexión inalámbrica entre el access point y el router, y repetirá la señal sin agregado de cables; solo se requiere una conexión eléctrica.

## Nada por defecto

Sin caer en la paranoia de apagar el router cuando no lo usamos, los pasos más básicos que debemos seguir son no dejar ninguna configuración de fábrica y cambiar las contraseñas. Existe una gran cantidad de programas que, mediante el SSID por defecto, son capaces de proporcionarnos la contraseña que viene de fábrica. Lo mejor es cambiar el SSID que ya tiene cargado el router, y hasta podríamos mantenerlo oculto para evitar intromisiones.

## Antena parabólica

Una opción es instalar un access point con antena parabólica, pero sin el plato reflector; de esta forma lograremos mayor cobertura en una vivienda, sin equipos o antenas a la vista.

## Modernizarnos

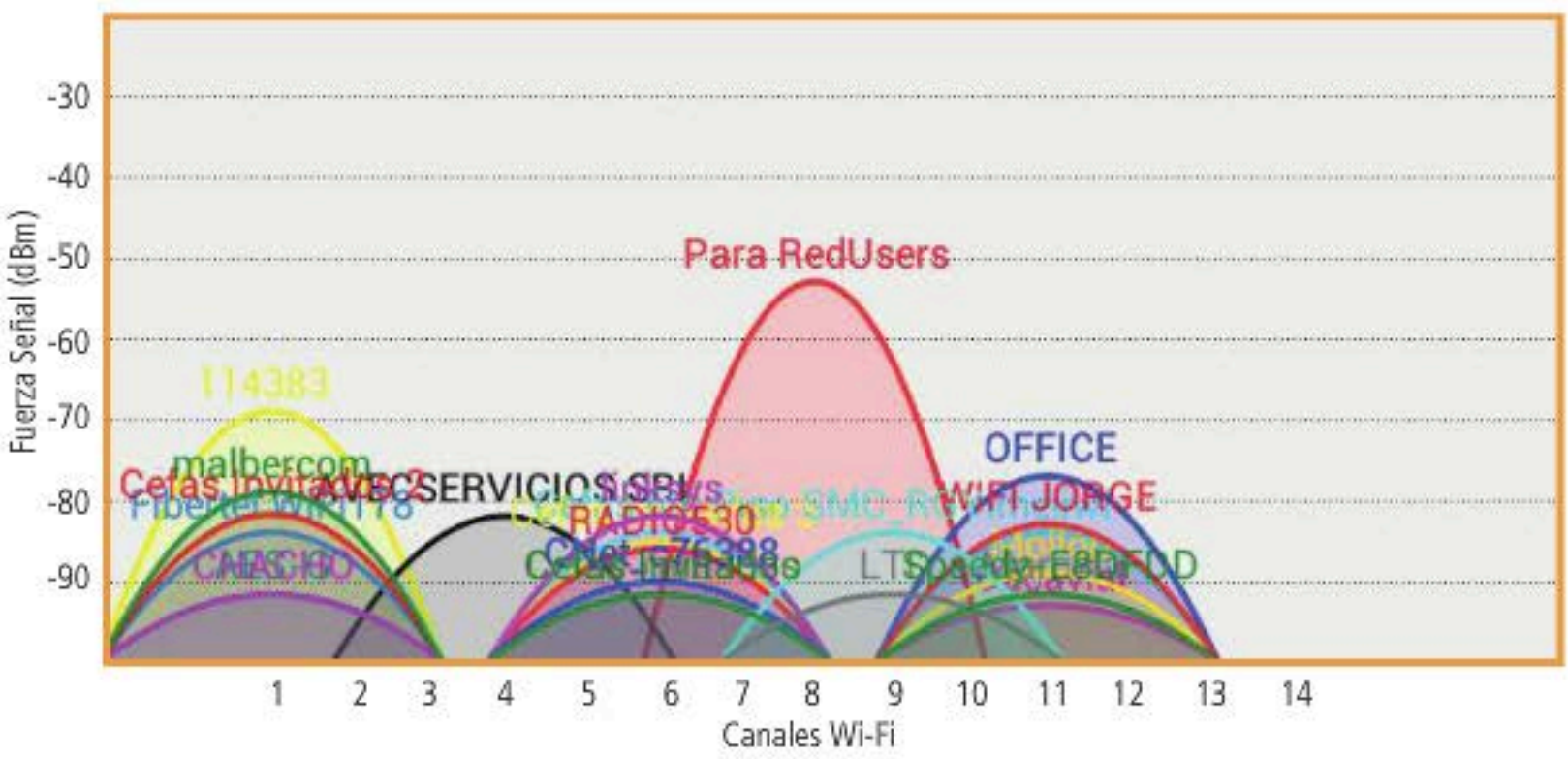
Un **router viejo** debería de cubrir nuestras necesidades de ancho de banda si solo queremos compartir Internet, pero, con uno más moderno, podemos optimizar nuestra red con funciones adicionales como la tecnología MIMO, que mejora notablemente la velocidad y la integridad de los datos. Otras funciones que nos beneficiarán mucho son:

- **QoS (Quality of Service):** como su nombre lo indica, calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones, como la transmisión de voz o video.
- **WMM (Wi-Fi MultiMedia):** al igual que QoS, proporciona calidad de servicio a las aplicaciones multimedia en la red Wi-Fi.

Una buena costumbre es actualizar el firmware de nuestro router; es una tarea muy sencilla en los últimos equipos fabricados.

## Unificar tecnologías

Instalar un **router MIMO**, con el estándar 802.11n y una velocidad de hasta 450 Mbps, no nos servirá de mucho si nuestra notebook trabaja con 802.11b a una velocidad de 54 Mbps. Por supuesto que la solución no es cambiar de notebook, pero si deberíamos pensar en adquirir un adaptador USB con la misma tecnología que nuestro router. ■




Con un analizador de Wi-Fi en nuestro celular, sabremos cuál es el canal libre, para así optimizar la señal.

# Limitación del alcance de la señal inalámbrica

Pese a que siempre solemos buscar el mayor alcance de nuestra señal para la red, debemos tener en cuenta que, en materia de seguridad, a veces menos es más. Revisemos algunos consejos importantes.

Cuando planificamos la zona de cobertura de nuestra red inalámbrica, siempre esperamos que la señal logre extenderse hasta todos los recovecos que necesitamos. En el caso de una instalación hogareña, querríamos que todas las habitaciones tuvieran la posibilidad de conectarse a la red, además de otras zonas como el balcón o la terraza y, por qué no, también el baño.

## Entornos corporativos

En lo que respecta a los entornos corporativos, la situación no es muy diferente, ya que se espera que todas las oficinas y pasillos tengan cobertura, de modo tal que los usuarios puedan conectarse desde sus puestos de trabajo sin pérdida de calidad o de paquetes. En algunos casos, también necesitaremos que la señal se propague no solo de manera horizontal, sino también vertical, como en una casa de dos pisos.

El problema en estos casos es que la propagación de las ondas electromagnéticas quizá se vea limitada por los materiales de construcción de la propia edificación, que filtrarán la señal que queremos hacer llegar hasta el otro piso. Recordemos que, entre los pisos de un edificio, suele haber grandes cantidades de hierro, concreto y caños, todos ellos con altos índices de absorción y rechazo de **señales electromagnéticas** de la frecuencia a la que estamos trabajando. Cualquiera sea el caso, previamente habremos diseñado y calculado los dispositivos y las antenas para que su área de cobertura alcance a todas las zonas, extendiendo alguna en caso de ser necesario, o agregando nuevos dispositivos repetidores o antenas con mayor ganancia.

Un bloqueador de señal aplica una denegación de servicio en el espectro electromagnético con sus propias antenas.

**EN EL DISEÑO DE LA RED INALÁMBRICA ES ESENCIAL NO EXCEDERSE DE LA ZONA DE COBERTURA ESPERADA.**

## Zona de cobertura

Ahora bien, pensemos qué sucedería si la zona de cobertura excede un poco la que esperamos; la respuesta parece ser: nada. Lo cierto es que esto es correcto en principio, pero no es así si lo analizamos desde el punto de vista de la seguridad de la información. Pensemos en un departamento cuyas paredes se comparten con otras paredes de departamentos de otras personas. Si nuestra señal excede la cobertura de la propia zona, estaremos haciendo llegar señal al otro lado, en caso de que esta logre atravesar la barrera atenuadora de la pared. Esto es especialmente cierto en las edificaciones más modernas, cuyos materiales de construcción no son tan robustos como hace algunas décadas.

Lo peor que puede pasar en estos casos es que nuestro vecino capte la señal inalámbrica de nuestra red, lo cual tampoco es tan grave si tenemos suficiente confianza con él; además, se supone que la señal llegará atenuada a tal punto que no debería ser posible navegar o conectarse a la misma velocidad que en las zonas próximas a las antenas, dentro del área de cobertura de mayor potencia. Si bien esto es cierto, un potencial atacante buscará especialmente este tipo de excedentes en el alcance de las señales para conectarse

Las oficinas modernas, con paredes delgadas o cristales, permiten que la señal se extienda, pero hay que tener cuidado con los intrusos.

y realizar ataques, pero no a nuestra red, sino desde nuestra red; este sería realmente el peor de los casos. Si un intruso se conecta a nuestra red, ya sea porque esta no tiene ningún tipo de cifrado o porque él ha podido obtener las credenciales de acceso, podría lanzar ataques y realizar acciones ilegales desde nuestra conexión, en caso de estar conectados a Internet. Entonces, legalmente hablando, los responsables seríamos nosotros.
Con todo esto, queremos decir que es necesario calcular bien las zonas de cobertura de la señal, e incluso, si alguna zona requiere una ampliación de la potencia, tener en cuenta hasta dónde puede alcanzar la señal una vez amplificada. Para este fin, podemos utilizar un smartphone, por ejemplo, aprovechando que son dispositivos elementales desde el punto de vista de las antenas, y ver si con él logramos captar la señal a medida que nos vamos alejando de la zona en la cual se supone que tenemos conectividad. Esta manera de medir la zona nos indicará cuál es la cobertura real. Esto se aplica también para las zonas de cobertura vertical.

## Denegación de servicio

Otro problema concerniente a la cobertura son los ataques de denegación de servicio aplicados a la propia señal del espectro electromagnético, mediante el uso de dispositivos bloqueadores de señal, llamados **jammers**. Estos inhiben la señal real mediante la generación de ruido de alta potencia en la misma frecuencia de trabajo en que se encuentra nuestra señal inalámbrica.

Encontramos inhibidores de señal fijos o portátiles, así podemos llevarlos a cualquier parte.

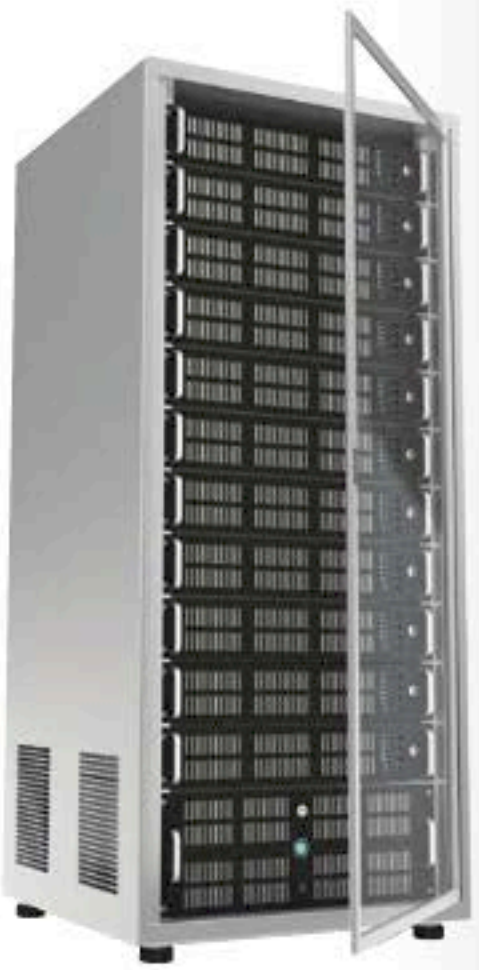
Por supuesto que existen distintos tipos de bloqueadores de señal en función de las diferentes tecnologías de conexión. Por ejemplo, encontramos jammers diseñados para tecnologías Bluetooth, para Wi-Fi, para **GPS**, para **GSM**, entre otras.
Los bloqueadores no son dispositivos de grandes dimensiones físicas, sino que pueden caber en un bolsillo y funcionar con baterías recargables. Por lo tanto, una persona podría estar siendo víctima del bloqueo de señal sin sospechar siquiera que otra en la misma habitación está realizando el ataque.
Si bien esta técnica es invasiva, se usa para autoprotección en contextos que requieren absoluta privacidad. En estos casos, no se admitiría de ninguna manera que algún miembro estuviera siendo espiado con micrófonos inalámbricos (que trabajan en el rango de la **radiofrecuencia**) o que la ubicación de los celulares pudiera ser identificada mediante el GPS interno. ■

## Bloqueadores

**Si bien los bloqueadores de señal pueden ser utilizados como medida de seguridad, en general su uso está centrado en los ataques de denegación de servicio a señales ajenas. Esta práctica y el uso de estos dispositivos están legalmente prohibidos en varios países del mundo, aunque en algunos se admiten en ciertos contextos, como en las cárceles, para evitar el contacto de los presidiarios con ubicaciones distantes; o en escuelas, para impedir que los alumnos reciban información por vía inalámbrica durante los exámenes.**

# Autenticación con servidores AAA

## Una forma de obtener autenticación en redes, ya sean cableadas o no, es mediante el uso de protocolos especiales denominados AAA.



La sigla **AAA** puede traducirse en español como Autenticación, Autorización y Auditoría (originalmente, **Authentication**, **Authorization** y **Accounting**). Cuando hablamos de AAA (**triple A**), no nos estamos basando en un solo protocolo o en alguno en especial, sino en una familia de protocolos que proveen los servicios anteriormente mencionados. Si le adicionamos el concepto de **Auditoría**, tendríamos lo que a veces se conoce como AAAA, o cuádruple A. Para comprender mejor estos sistemas de autenticación, debemos recordar primero los conceptos que representan.

### Autenticación

Autenticación es el proceso por el que una entidad demuestra que es quien dice ser, probando así su identidad frente a un sistema u otra entidad. En general, una entidad es un cliente, y la otra es un servidor ante el cual se requiere autenticación. Al presentar alguno de los factores de autenticación ya conocidos —algo que uno tiene (por ejemplo, un **token**), algo que uno sabe (por ejemplo, un **password**) y algo que uno es (por ejemplo, una huella dactilar)—, se logra que el sistema valide al usuario en cuestión. En algunos casos, también puede darse el requisito de la presentación de dos de los tres tipos de factores, para obtener lo que se denomina autenticación **Two Factors**. Vale la pena destacar que, en muchos casos, no es indispensable enviar por la red las credenciales de autenticación (usuario y contraseña, por ejemplo), sino que se cuenta con mecanismos que ofrecen mayor seguridad, como los sistemas de **Challenge-Response** (desafío-respuesta), utilizados ampliamente en redes inalámbricas. Estos se basan en el envío de información por parte del servidor, que el cliente procesa para, luego, devolver una respuesta única posible, cuya verificación reflejará el hecho de que el cliente conocía la forma de resolver el desafío. Así se valida que es quien decía ser.

El segundo elemento de los sistemas de triple A es la autorización, que se refiere a que, una vez que el usuario fue autenticado, se le permita acceder a determinados recursos, basándose en los privilegios específicos que el sistema de seguridad le permite.

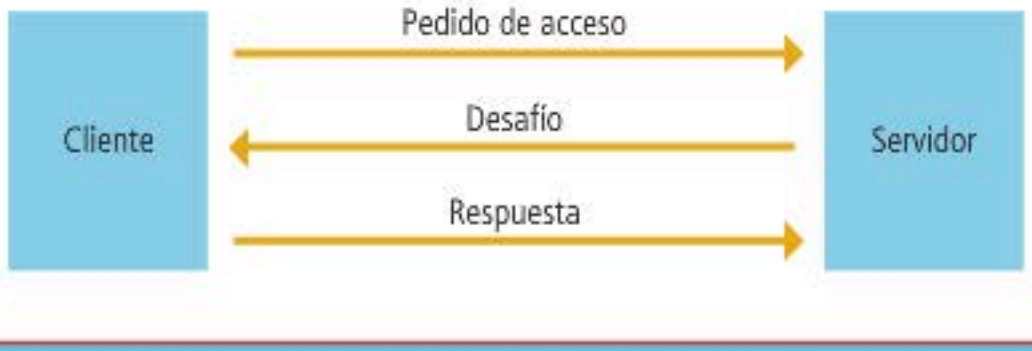
Existen diversos métodos para garantizar los privilegios correspondientes a las diferentes entidades, desde sistemas mandatorios, hasta sistemas discrecionales o basados en roles, reglas y contextos. En esta instancia, un usuario de un sistema o red pasará a tener acceso a los diferentes recursos, como ancho de banda, carpetas y archivos, servicios y aplicaciones, y más.

### Accounting

Finalmente, tenemos el concepto de **accounting**, que como bien decíamos, no se refiere a contabilidad en el sentido de lo que uno podría imaginarse (contadores realizando tareas de liquidación de

### Más sobre RADIUS

Livingston Enterprises desarrolló el protocolo **RADIUS** para sus productos de la serie PortMaster de servidores NAS. Dada su popularidad, se publicó como RFC 2138 y RFC 2139 al poco tiempo. Hoy en día, existen muchas implementaciones de servidores RADIUS, incluyendo algunas de código abierto. También se implementan servidores proxy RADIUS para administración centralizada, que permiten reescribir paquetes al vuelo.




En este diagrama, se presenta el proceso de desafío respuesta entre un servidor de autenticación y el cliente conectado.

sueldos o temas impositivos), ni a auditoría en el sentido de listas de verificación de cumplimiento de tareas realizada por un auditor. En este caso, se refiere a la capacidad de un sistema de registrar eventos, normalmente soportada por los sistemas de logs, que no son más que registros secuenciales que permiten determinar las acciones realizadas por una entidad activa en una red (usuario, servicio, proceso, etcétera). Por lo general, esta información se utiliza luego para la correcta administración de los recursos, la planificación de la capacidad y, también, para la recopilación de información en caso de incidentes que la requieran. Existen diversos protocolos bien conocidos que implementan estos conceptos, entre los cuales mencionaremos los más utilizados: **RADIUS**, **DIAMETER**, **TACACS** y su sucesor, **TACACS+**.

## RADIUS

RADIUS es el acrónimo en inglés de **Remote Authentication Dial-In User Server**, y es quizás el más conocido. Utiliza el puerto UDP 1812 UDP y funciona como cliente-servidor. Su éxito residió, probablemente, en su implementación en proveedores de acceso a Internet (**ISP**), que fueron los que primero debieron incluir una instancia de autenticación remota a través de la red para validar las conexiones de sus clientes. Estas conexiones pueden ser tanto inalámbricas como por medio de **cablemódems**, líneas **ADSL** o accesos **dial-up**. RADIUS recibe la información de credenciales de acceso por medio del protocolo **PPP** a través de un servidor conocido como **Network Access Server**, que redirige el pedido a un servidor RADIUS con el propio protocolo RADIUS. Este comprueba que la información sea correcta mediante otros mecanismos de autenticación (**PAP**, **CHAP** o **EAP**) y, en caso de ser aceptada, autoriza al cliente a acceder al sistema y le provee los recursos necesarios, como una dirección IP. RADIUS permite manejar sesiones, lo cual es útil para la medición de tiempo para facturación, como en hoteles o ISPs.

## DIAMETER

Más adelante se creó **DIAMETER**, basado en el mismo concepto que RADIUS y tomando muchas de sus funcionalidades e ideas. De hecho, así como RADIUS equivale a la palabra *radio* en inglés (en referencia a la mitad del diámetro de un círculo), el nombre DIAMETER hace evidente referencia a "el doble del radio", es decir, "el doble de RADIUS".
Está pensado para trabajar tanto de modo local como en el llamado estado de alerta, sondeo y captura (AAA roaming), con lo cual puede ofrecer servicios dinámicos y flexibles. DIAMETER no es retrocompatible, pero ofrece un método de actualización para quienes parten de RADIUS. Algunas de sus diferencias son: usa TCP en vez de UDP, puede usar **IPSEC** o **TLS**, es **peer-to-peer** en vez de cliente-servidor, permite negociar capacidades, y tiene notificación de errores.
El último es **TACACS**, acrónimo de **Terminal Access Controller Access Control System**, creado por **Cisco** y usado, normalmente, en sistemas **UNIX** y descrito en el RFC 1492. Posteriormente surgió **TACACS+**, que pese a su nombre similar, es muy diferente y no es compatible con el anterior. ■

# Ocultar el SSID para aumentar la seguridad

El ocultamiento del SSID, o nombre de red, es solo una leyenda urbana en lo que respecta a la seguridad de una red Wi-Fi. Veamos los detalles.

En cuestiones de seguridad de redes inalámbricas, existen muchos mitos o leyendas urbanas. Uno de ellos es la del ocultamiento del SSID (*Service Set IDentifier*), también llamado nombre de red. Este procedimiento consiste en no transmitir la señalización del SSID por la red, con lo cual, supuestamente, quien no conoce el nombre de la red no podría acceder ni conectarse a ella.

## Métodos

Esta afirmación no es para nada exacta, ya que el señalamiento (**beaconing** en inglés) es solo uno de los cinco métodos de transmisión del SSID en una red Wi-Fi; este también se transmite mediante **probe request** (petición de sondeo), **probe response** (respuesta de sondeo), **association request** (petición de asociación) y **re-association request** (petición de reasociación), por lo que quien realmente quiere averiguar el SSID de una red wireless no tiene más que aplicar las herramientas correctas y capturar tal información.

**CON SOFTWARE ESPECÍFICO, AVERIGUAR EL SSID DE UNA RED INALÁMBRICA ES UNA TEREA MUY SENCILLA.**

## Ocultamiento

La ventaja del ocultamiento del SSID en una red inalámbrica se aplica a usuarios con pocos o nulos conocimientos de redes, ya que fuera de esta situación, no presenta ninguna ventaja. En cambio, sí tiene una desventaja importante en cuanto al enrutamiento mediante access points, dado que, cuando el AP está en modo idle, si no recibe el **SSID beaconing**, puede interpretarlo como un corte en la conexión y provocar la interrupción del servicio. Además, el ocultamiento del SSID vuelve a las interfaces inalámbricas menos amigables para el usuario final. Otros mitos de seguridad en redes wireless, son los siguientes:

- **Desactivación de servidor DHCP**: para usuarios experimentados, la adquisición del rango de IPs que admite el router es una tarea sencilla.
- **El filtrado por MAC Address**: hoy en día, el clonado de MACs es muy sencillo.
- **Autenticación LEAP**: se trata de un método desarrollado por la empresa Cisco, pero vulnerado hace tiempo.
- **Posicionamiento de la antena y potencia**: ubicar la antena en el centro de la red y reducir la potencia de la señal solo consigue que las terminales más alejadas de la antena tengan fluctuaciones de señal.
- **Utilizar 802.11a o Bluetooth**: tengamos en cuenta que no resulta útil emplear otras frecuencias en la señal wireless, ya que las NICs actuales son compatibles con todas las normas; y la norma Bluetooth ha presentado diversos problemas de seguridad y algunas limitaciones de rendimiento. ■

```
                    Menu 3.5- Wireless LAN Setup

                ESSID= Nexus
                Hide ESSID= No
                Channel ID= CH01 2412MHz
                RTS Threshold= 2432
                Frag. Threshold= 2432
                WEP= Disable
                  Default Key= N/A
                  Key1= N/A
                  Key2= N/A
                  Key3= N/A
                  Key4= N/A
                Edit MAC Address Filter= No



                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

La opción de ocultamiento de SSID, vista en el modo consola, al cual se accede mediante el comando Telnet seguido de la IP del router.

# PRÓXIMA ENTREGA

## 9

## SEGURIDAD EN REDES CABLEADAS E INALÁMBRICAS

En este número veremos la seguridad tanto en redes cableadas como inalámbricas, revisaremos el funcionamiento del firewall y entregaremos consejos útiles.

Técnico en
# REDES &SEGURIDAD


**PROFESORES EN LÍNEA**
profesor@redusers.com

**SERVICIOS PARA LECTORES**
usershop@redusers.com


## SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.


REDES &SEGURIDAD 00008
9 789871 857784


## CONTENIDO DE LA OBRA