INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

7

Técnico en REDES &SEGURIDAD

INSTALACIÓN DE REDES INALÁMBRICAS

En este fascículo aprenderemos a realizar la instalación de redes inalámbricas y a configurar interfaces Wi-Fi. También revisaremos las opciones de seguridad.

Incluye e-book: Cloud Computing

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 instalación de redes inalámbricas, teniendo en cuenta su funcionamiento y los estándares relacionados con este proceso, además de algunos consejos sobre seguridad.

En la clase anterior analizamos todas las tareas de configuración relacionadas con las redes cableadas, revisamos cada una de las tecnologías y los protocolos relacionados, así como también las opciones de seguridad que necesitamos tener en cuenta. Aprendimos a realizar la asignación de permisos y a hacer un booteo remoto. Finalmente, vimos en detalle los aspectos de seguridad más importantes, como TCP Handshake.

En la presente entrega, nos dedicaremos a conocer la forma en que debemos realizar la implementación de redes inalámbricas. Veremos en detalle cómo funcionan y cuáles son los estándares relacionados con ellas, analizaremos las características de los tipos de redes inalámbricas existentes y revisaremos sus ventajas. Para continuar, configuraremos de manera general un punto de acceso inalámbrico y verificaremos las opciones de seguridad más importantes para mantener nuestra red protegida. También aprenderemos a instalar y configurar interfaces de red inalámbricas tanto en sistema Windows como en distribuciones Linux. Para terminar conoceremos los alcances del modo promiscuo en redes inalábricas.

7

2 Cómo funciona una red inalámbrica

4 Los estándares 802.11

8 Configuración básica del Access Point

24 Modo promiscuo en redes inalámbricas

Cómo funciona una red inalámbrica

Las redes inalámbricas han evolucionado y hoy son una alternativa fiable; a continuación, veremos su funcionamiento.

Una red inalámbrica es aquella en la que dos o más dispositivos pueden comunicarse sin necesidad de establecer una conexión por cable, a través de un enlace que utiliza ondas electromagnéticas, de radio, microondas o infrarrojo.
Existen diferentes tecnologías, diferenciadas por la frecuencia que utilizan, el alcance y la velocidad de la transmisión. Las redes inalámbricas facilitan la conectividad entre dispositivos remotos, que se encuentren a unos metros de distancia o a varios kilómetros.

Clasificación

Así como se clasifican las redes cableadas, también podemos clasificar las inalámbricas. En líneas generales, es posible encontrar los siguientes tipos de redes inalámbricas:

- **WPAN** (*Wireless Personal Area Network*): red de área personal inalámbrica, como las tecnologías Bluetooth.
- **WLAN** (*Wireless Local Area Network*): red de área local inalámbrica, similar a una LAN, pero sin cables.
- **WMAN** (*Wireless Metropolitan Area Network*): red de área metropolitana inalámbrica, basada en Wi-Max.
- **WWAN** (*Wireless Wide Area Network*): red de área extendida inalámbrica, como la tecnología para telefonía móvil, GPRS, GSM, 3G, etc.

Funcionamiento

Para llevar la información de un punto a otro se utilizan **ondas de radio**, sin necesidad de que exista un medio físico guiado, como en las redes cableadas. Cuando hacemos mención a ondas de radio, nos referimos, normalmente, a portadoras, sobre las cuales se transporta la información, que cumplen la función de llevar la energía a un receptor remoto. Los datos que se transmiten se superponen a la portadora de radio y, de este modo, se extraen en el receptor final. Este proceso se denomina **modulación de la portadora** por la información que está siendo transmitida. Si las ondas son transmitidas a distintas frecuencias de radio, es posible que existan varias portadoras en el mismo tiempo y espacio, sin interferir entre ellas.
El **receptor** debe situarse en la misma frecuencia que la portadora, e ignorar el resto. Este funcionamiento es similar al de una red cableada, en la cual el receptor debe conectarse a la red mediante

Red inalámbrica

Entre las ventajas de una red inalámbrica, encontramos la amplia libertad de movimientos y la reubicación de las estaciones de trabajo, una instalación mucho más rápida y menor costo de implementación, además, permite tener cobertura en puntos difíciles de conectar mediante el uso cables. Pero no todo es bueno, entre las desventajas podemos mencionar que pueden llegar a ser más inseguras (existen estándares que tienen gran robustez en cuanto a seguridad, pero su implementación implica un mayor costo), por otra parte, presentan un menor ancho de banda que las redes cableadas, en el caso de que las condiciones externas sean desfavorables.

el cableado normalizado. En las redes inalámbricas de área local (**WLAN**), las comunicaciones pueden realizarse de dos maneras: **ad hoc** e **infraestructura**.

Ad hoc (IBSS)

En una red de este tipo, los clientes se conectan entre sí, sin ningún punto de acceso; cada equipo que participa es cliente y punto de acceso. Los datos se envían directamente entre los equipos que participan, con un máximo de nueve clientes inalámbricos.

Infraestructura (BSS)

En el modo de infraestructura, la comunicación se realiza mediante puntos de acceso, más conocidos por su nombre en inglés, *access points* (**AP**); estos, además, permiten conectar la red inalámbrica a una red cableada. Estas redes funcionan sobre la base de ondas de radio específicas. El AP actúa como una puerta de entrada a la red inalámbrica en un lugar específico y una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios para hacerlo.

LAS TECNOLOGÍAS INALÁMBRICAS FACILITAN LA INTERCONEXIÓN ENTRE DISPOSITIVOS.

Peticiones

Cuando una estación hace una petición o envío de datos a otra, esta llega hasta el AP. La primera vez, este no sabe en qué lugar se encuentra la estación de destino, por lo que la envía por todos los terminales y espera la confirmación de cuál es el camino correcto. Una vez que la petición llega hasta la estación, esta devuelve la confirmación del camino, y el AP lo registra; entonces, almacena el recorrido de los paquetes, de manera que, la próxima vez, se dirigirán por el camino correcto. El enlace de datos inalámbrico posee condiciones de borde diferentes de la capa MAC Ethernet. Una de las más significativas es que utiliza cuatro campos de dirección, cuya interpretación depende del tipo de **Frame MAC** que se transmita. Los cuatro campos de dirección se etiquetan de la siguiente manera:

- **Address 1, Receptor**: indica qué estación inalámbrica debe procesar el frame. En caso de estar dirigido a una red Ethernet conectada a un AP, la dirección receptor es la interfaz inalámbrica en el AP, y el destino, el equipo conectado a la red.
- **Address 2, Transmisor**: se encarga de identificar la interfaz inalámbrica que transmite el frame correspondiente.
- **Address 3**: para filtrado por parte del receptor, permite conocer en qué interfaz está conectado.
- **Address 4**: solo se usa en modo ad hoc para generar un BSSID aleatorio.

SSID

SSID (*Service Set Identifier*) es el nombre de identificación de una red inalámbrica, que se incluye en todos los paquetes para identificarlos como parte de esa red. Puede contener hasta un máximo de 32 caracteres.
Es necesario tener en cuenta que los dispositivos inalámbricos deben compartir el mismo SSID para que la interconexión pueda llevarse a cabo. La identificación BSSID es utilizado por redes ad hoc, en tanto que para las redes de infraestructura se emplea el concepto ESSID, pero es posible llamarlos SSID en general. ■

Esquema de red ad hoc (IBSS): los dispositivos son portadores y clientes al mismo tiempo.

En la red de infraestructura (BSS), las interconexiones requieren de un Access Point.

Los estándares 802.11

El estándar 802.11 permitió la consolidación de las redes WLAN, al establecer un marco de referencia para el diseño de los dispositivos.

El estándar IEEE 802.11 define las normas de funcionamiento en redes locales inalámbricas, conocidas como **WLAN** (*Wireless Local Area Network*). El **IEEE** (**Instituto de Ingenieros Eléctricos y Electrónicos**) es una organización profesional sin fines de lucro dedicada a la estandarización, al avance de la innovación tecnológica y la excelencia en beneficio de la humanidad, según el concepto que se anuncia en el sitio web oficial.
En este estándar, se encuentran las especificaciones tanto físicas como a nivel de MAC que hay que seguir al implementar una red de área local inalámbrica, en cuanto a tecnologías de modulación y gestión de la transmisión y recepción de datos.

EL ESTÁNDAR 802.11 ESPECIFICA LA CAPA FÍSICA Y LA SUBCAPA MAC EN EL DISEÑO DE UNA RED DE ÁREA LOCAL INALÁMBRICA.

Métodos de transmisión

En el nivel físico, se definen los métodos de transmisión que mencionamos a continuación:

- **DSSS** (espectro ensanchado por secuencia directa): esta técnica consiste en la generación de un patrón de bits redundante para cada uno de los bits que componen la señal de información, y la posterior modulación de la señal resultante mediante una portadora de RF. El receptor debe realizar el proceso inverso para obtener la señal de información original.

Dispositivo USB de conexión inalámbrica (conocido como dispositivo de red USB) diseñado sobre la base del estándar 802.11n.

- **FHSS** (espectro ensanchado por salto en frecuencia): consiste en transmitir una parte de la información en una determinada frecuencia durante un corto intervalo de tiempo. Una vez que pasa ese tiempo, se cambia la frecuencia utilizada para realizar la emisión y, posteriormente, se sigue transmitiendo a otra frecuencia del espectro disponible.

- **OFDM** (multiplexación por división de frecuencias ortogonales): se trata de un método que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, cada una de las cuales se encarga de transportar información.

En el nivel de acceso al medio, subnivel MAC, se define el tipo de acceso al medio, y se controlan el sincronismo y los algoritmos del sistema de distribución, en caso del modo de infraestructura; se define como el conjunto de servicios que propone dicho modo. La arquitectura MAC definida por el estándar se compone de:

- La funcionalidad de coordinación distribuida (DFC).
- La funcionalidad de coordinación puntual (PCF).

Función de coordinación distribuida (DFC)

Dentro de un conjunto básico de servicios (BSS), esta función determina cuándo un dispositivo puede transmitir y/o recibir paquetes de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC, se encuentra la función de coordinación distribuida, y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.
Esta funcionalidad no es soportada por los servicios síncronos, debido a que esta técnica de contienda introduce algunos retardos aleatorios y, por lo tanto, no predecibles. Algunas de las características de DFC son las que mencionamos a continuación:

- Utiliza CSMA/CA con RTS/CTS, como protocolo de acceso al medio.
- Reconocimiento ACKs necesario, que provoca la generación de retransmisiones si no se reciben los datos.
- Usa campo Duration/ID que se encarga de contener el tiempo de reserva adecuado para transmisión y ACK.
- Implementa fragmentación de datos.
- Se encarga de conceder prioridad a tramas mediante la existencia de espaciado entre tramas (IFS).
- Presenta un soporte para realización de broadcast y también multicast sin necesidad de ACKs.

Acces point DLINK-DAP-1353 RB, 802.11n. Utiliza varios canales a la vez para enviar y recibir datos gracias a la incorporación de distintas antenas.

Función de coordinación puntual (PCF)

En un nivel mayor que DCF se encuentra la función PCF, asociada a transmisiones libres de contiendas, porque utiliza técnicas de acceso deterministas. Fue pensada para servicios de tipo síncrono, que no toleran retardos aleatorios en el acceso al medio.

CSMA/CA

El **protocolo CSMA/CA** (múltiple acceso por detección de portadora para evitar colisiones) evita colisiones entre los paquetes de datos para transmitir y recibir simultáneamente. Primero examina si alguien está usando el canal, luego espera hasta que el canal está desocupado y, entonces, transmite un marco; si hay un choque, espera un período aleatorio e intenta otra vez. A continuación, listamos las acciones que corresponden al funcionamiento de CSMA/CA:

- Determina el estado que corresponde al canal: libre u ocupado.
- Si el medio no se encuentra ocupado, ejecuta IFS (espaciado entre tramas).
- Si durante el intervalo de consulta el medio se anuncia como ocupado, entonces el dispositivo debe esperar a que se libere antes de realizar otra acción.
- Cuando finaliza la espera (por medio ocupado), se ejecuta el algoritmo de Backoff, el que determinará una espera adicional y aleatoria en un intervalo llamado ventana de contienda (Contention Window, CW). El algoritmo devolverá un número aleatorio y entero de ranuras temporales. Su función es la de reducir las posibilidades de colisión, que son máximas si muchas estaciones esperan a que el medio quede libre para transmitir.
- Durante la espera determinada por el algoritmo de Backoff, se sigue escuchando al medio. Si este se anuncia como libre, avanza hasta que consume todas las ranuras asignadas. Si el medio no permanece libre, el algoritmo se suspende hasta que se cumpla dicha condición.

CSMA presenta una serie de problemas; los dos principales son los siguientes:

¿Qué estándar?

Uno de los razonamientos válidos para decidirnos por una tecnología es relevar nuestra necesidad y, sobre esa base, elegir. Sabemos que la IEEE rectifica constantemente el estándar con la intención de realizar mejoras en él. Por eso, hoy en día, el uso de 802.11a es un tanto obsoleto. Según nuestra necesidad, debemos seleccionar el equipamiento que formará nuestra red, considerando la velocidad máxima de transmisión, frecuencia y costo. En la actualidad, el estándar aceptable es el **G**, con sus variaciones propietarias **G+** o el uso de **n**.

Logo registrado por la Wi-Fi Alliance, que representa mundialmente las conexiones inalámbricas de área local.

▶ **Nodos ocultos**: una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no oye.
▶ **Nodos expuestos**: una estación cree que el canal está ocupado, pero en realidad está libre, pues el nodo al que oye no le interferiría para transmitir a otro destino.

En 802.11, esto se soluciona con CSMA/CA. Según este protocolo, antes de transmitir, el emisor envía una trama **RTS** (*Request to Send*) para indicar la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor manda sus datos.

LA WI-FI ALLIANCE BUSCÓ UN NOMBRE MÁS ACEPTABLE QUE IEEE 802.11B DS, Y LE DEJÓ ESTA TAREA A LA EMPRESA DE PUBLICIDAD INTERBRAND; DE ESTA COLABORACIÓN NACIÓ EL TÉRMINO WI-FI.

Bandas de frecuencia

El estándar 802.11 se encarga de definir el uso de las bandas de frecuencia, tengamos en cuenta que estas se encuentran en banda industrial, científica y médica (ISM).

Hagamos un poco de historia. En el año 1985, la **Comisión Federal de Comunicaciones** (**FCC**), intentando promover los productos inalámbricos, modificó la regulación del radioespectro, autorizando a los productos de redes inalámbricas a operar en las ISM mediante la modulación de esparcimiento de espectro, con una potencia de salida de hasta 1 Watt. Las bandas ISM son las siguientes:

▶ 902–928 MHz
▶ 2,4–2,4835 GHz
▶ 5,725–5,850 GHz

Los fabricantes de WLAN deben asegurar la certificación por la **Agencia Reguladora de Radiotransmisión** correspondiente, para vender sus productos. Los estándares IEEE 802.11 especifican dos modos de funcionamiento de una red: ad hoc e infraestructura:

▶ **Ad hoc** (IBSS, *Independent Basic Services Set*): red entre dispositivos sin punto de acceso, donde cada cliente es portadora.
▶ **Infraestructura** (BSS, *Basic Services Set*): presenta una serie de clientes con un punto de acceso central.

Extensiones del estándar

El estándar 802.11 es único, pero ha sufrido rectificaciones o extensiones para dar lugar a variedades con una letra al final, que veremos a continuación:

▶ **802.11 Legacy**: se publicó en 1997. Funciona en una frecuencia de 2,4 GHz, con una velocidad de transmisión máxima de 2 Megabits por segundo (en las mejores condiciones ambientales) y usando señales infrarrojas. Dispone de tres canales no superpuestos en banda de frecuencia de 2.4 GHz (ISM). Utiliza las tecnologías de transmisión **DSSS** o **FHSS**.

▶ **802.11a:** se lanzó al mercado en 1999. Funciona en 5 GHz, con una velocidad máxima de transmisión de datos de 54 Mbps. Dispone de 12 canales que no se solapan en ISM, puede alcanzar una distancia de 200 metros en condiciones favorables, pese a que la banda en 5 GHz tiene mayor dificultad con los objetos que estén en la ruta de la señal, haciendo que los intervalos sean,

Seguridad en redes inalámbricas

En la actualidad, se sabe que el cifrado WEP —que se incluía como medida de seguridad estándar— es fácilmente vulnerable a ataques de fuerza bruta, entre otros. Con la llegada del estándar 802.11i, se dio inicio a lo que se conoce como WPA2, que utiliza los protocolos TKIP y AES para la autenticación y encriptación. En este caso, se han detectado ataques de fuerza bruta con herramientas de hacking que permiten obtener la clave de identificación en la red cuando esta es sencilla, por lo que se recomienda utilizar claves complejas para garantizar la fiabilidad de nuestra red.

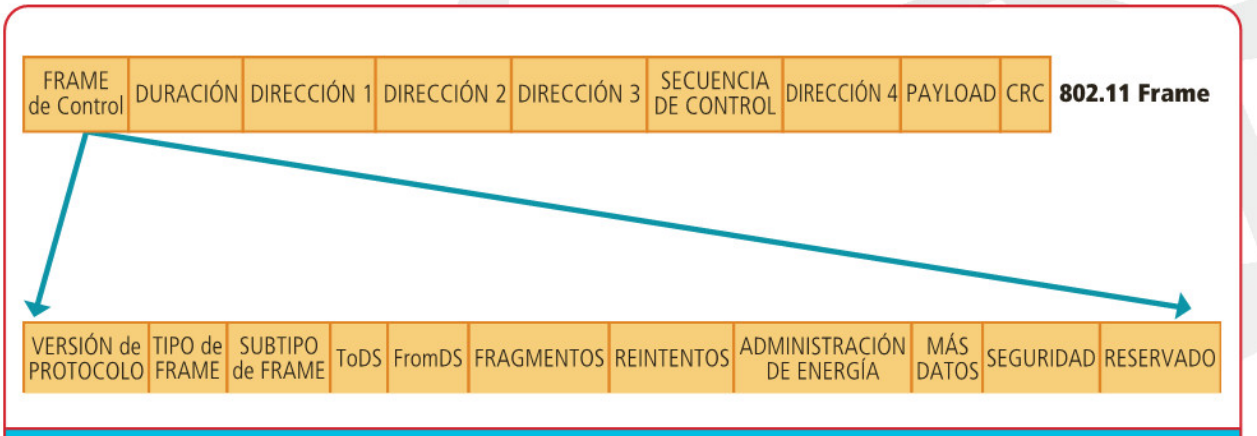
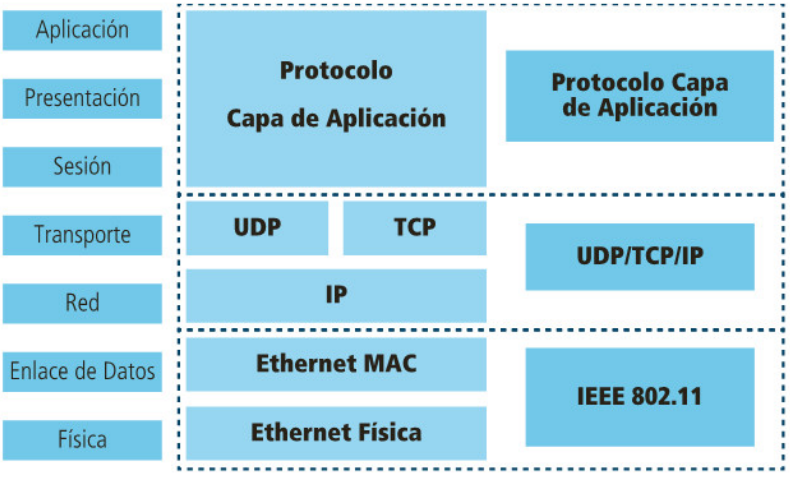


Diagrama que muestra la composición del frame o trama en el estándar 802.11.

a menudo, pobres. Utiliza el protocolo de transmisión OFDM.

▶ **802.11b:** publicado en 1999, este estándar fue desarrollado por la Wi-Fi Alliance (antes conocida como la *Wireless Ethernet Compatibility Alliance*). El organismo declara que su misión es proporcionar un foro de colaboración altamente eficaz y liderar el crecimiento de la industria con las especificaciones de las nuevas tecnologías y los programas.
En condiciones ideales de entorno y proximidad (por ejemplo, sin fuentes de atenuación que generen interferencias), funciona a 11 Mbps, una tasa mayor que Ethernet con cables (que es de 10 Mbps). Utiliza el mismo método de acceso definido en el estándar original CSMA/CA.

▶ **802.11g:** surgió en 2003, dispone de tres canales no superpuestos en banda 2,4 GHz de ISM. Durante el diseño de este estándar, se pensó en la compatibilidad con el estándar b, ya que utiliza las mismas frecuencias que este. Pero existe la salvedad de que, en redes bajo el estándar g, la existencia de nodos del estándar b reduce la performance, y pierde velocidad de transmisión.
En la actualidad, hay una variante llamada 802.11g+, capaz de alcanzar 108 Mbps máximos de transferencia. Suele funcionar en dispositivos de los mismos fabricantes porque utiliza protocolos propietarios.



Capas de injerencia del estándar 802.11 en el modelo OSI. Podemos ver claramente que se ubica en la capa física y la subcapa MAC.

▶ **802.11i**: utiliza los protocolos **TKIP** y **AES**, que da origen a WPA2.
Hasta la llegada de 802.11i, las redes WLAN eran inseguras. WPA utilizaba el algoritmo WEP (privacidad equivalente a cableado). A partir de 2001, se han encontrado ataques estadísticos que permiten recuperar la clave WEP.

▶ **802.11n**: utiliza el protocolo OFDM con MIMO y la asociación de canales (CB). Dispone de tres canales no superpuestos en ISM, banda de frecuencia de 2,4 GHz y 12 canales que no se solapan sin licencia nacional de información (UNII), en banda de frecuencia de 5 GHz con y sin CB.
El estándar 802.11n fue ratificado por la IEEE el 11 de septiembre de 2009 con una velocidad máxima de 600 Mbps. En la actualidad, existen productos con el estándar N con un máximo de 300 Mbps.

▶ **802.11w** (en desarrollo): el TGw está orientado a generar un estándar con mayor robustez de seguridad en los protocolos de autenticación y codificación.

▶ **802.11ac** (en desarrollo): implica mejorar las tasas de transferencia hasta 3,2 Gbps dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz, usar hasta ocho flujos MIMO y tener modulación de alta densidad. ■

Configuración básica del Access Point

En estas páginas realizaremos el proceso de configuración de un Access Point desde cero, con el fin de dejarlo listo para usar.

Lo primero que debemos hacer al tener el **access point** en nuestras manos, después de desembalarlo, es tomar el manual que viene con él, ya sea en formato electrónico o en papel, y leerlo, porque esto nos ayudará en el proceso de configuración inicial. Tengamos en cuenta que cada dispositivo es diferente, por lo que el acceso a la administración tal vez sea distinto. En este ejemplo, vamos a configurar un access point de marca **Zyxel, P-660HW 600 series**, diseñado bajo el estándar 802.11g.

Conexión

Conectamos el AP a la alimentación eléctrica y, luego, desde los puertos LAN, conectamos el cable hasta nuestra PC en el conector llamado WAN. Verificamos que las luces se encuentren encendidas y comenzamos la configuración.

ES IMPORTANTE RESTRINGIR EL ACCESO A LA ADMINISTRACIÓN DEL ACCESS POINT SOLO A LA RED LAN.

Consola de administración

Accedemos a la consola de administración del AP desde un navegador web, escribiendo **http://192.168.1.1** en la barra de direcciones. Si debemos hacerlo en otro dispositivo, verificamos la IP de administración según las indicaciones del fabricante.

Al ingresar en la dirección mencionada, el dispositivo nos permite ver su estado y pasar a configurar sin una validación la conexión ADSL. Seleccionamos la opción **Configuración Avanzada**, ante lo cual nos pedirá una contraseña de acceso, presente en el manual del dispositivo. La mayoría de los access point utilizan un usuario **Admin**, y su contraseña puede variar, desde **admin**, **1234**, hasta estar en blanco. Para nuestro ejemplo, el AP tiene como contraseña **1234**; la ingresamos y hacemos clic en **login**. En este punto, ya estamos dentro del AP, donde podemos ver todas las opciones que incluye. La mayoría de los AP disponen de las siguientes:

- **Wizard Setup**: ofrece una herramienta paso a paso para realizar la configuración en forma sencilla.

- **Advanced Setup**: presenta cada ítem configurable en cuanto a conexión; por ejemplo, **WAN**, **LAN**, **WLAN**, **NAT**, **Firewall** y otras.

- **Maintenance**: trae opciones como **System Status**, **DHCP Table**, **Diagnostic** y **Firmware** (para su actualización), entre otras.

Disponemos de una conexión a Internet que nos brinda el módem, al cual conectamos el AP para distribuirla a través de la WLAN. De esta forma, buscamos utilizar Internet en todos los dispositivos que tiene conexión Wi-Fi. Vamos a configurar el AP para que cada dispositivo que se conecte (autorizado) se configure automáticamente, y tomaremos las medidas de seguridad pertinentes para que nuestra red no quede a merced de algún vecino con conocimientos informáticos avanzados que quiera utilizar nuestro acceso inalámbrico sin permiso o, peor aún, con malas intenciones.

Configuración WAN

Desde la consola de administración, nos dirigimos al menú **WAN Setup**; aquí encontramos diversos apartados que debemos configurar como mostramos a continuación:

- **Name**: aquí debemos seleccionar el nombre para la conexión; para este ejemplo, le pusimos **AccessW**.

Menú general del AP, en el que es posible visualizar todos los aspectos configurables.

▶ **Mode**: aquí podemos definir si el punto de acceso funcionará como bridge o routing; elegimos **Routing**.

▶ **Encapsulation**: se encarga de desplegar el listado de protocolos que admite. Seleccionamos **ENET ENCAP** para nuestra conexión que viene de un módem.

▶ **IP Adress**: aquí podemos elegir el método de asignación de IP, las opciones disponibles son automático o IP fija. En nuestro caso, como se obtiene la dirección IP que asigna el módem, seleccionamos **Obtain an IP Address Automatically**.

Para que los cambios queden establecidos, debemos hacer clic sobre el botón denominado **Apply**.

Configuración LAN

Ingresamos en el menú **LAN Setup**, desde donde podemos resetear la IP local del AP y habilitar el servidor DHCP (protocolo de configuración dinámica de host). Debemos asignar el rango de IP por el que deseamos comenzar y la cantidad de clientes que puede tener. Este servicio permite que cada dispositivo que se conecte a la red reciba una IP determinada; es decir, la red se configurará automáticamente en cada computadora o dispositivo que se conecte a ella, con la opción habilitada de **Obtener configuración automática**.

▶ **DHCP**: seleccionamos la opción **Server**, para habilitar el punto de acceso como servidor DCHP.

▶ **Client IP Pool Starting Address**: ingresaremos la IP privada por la cual queremos que comience a asignar el servidor; en nuestro caso es **192.168.1.10**.

▶ **Size of Client IP Pool**: se trata de la cantidad de clientes que queremos que se conecten por DHCP; por default, son 32 direcciones IP para conexión de clientes.

▶ **TCP/IP**: esta opción nos permite realizar la configuración de la IP del punto de acceso y la máscara de subred (cifra de 32 bits que especifica los bits que pertenecen a una dirección IP correspondiente a una red y a una subred).

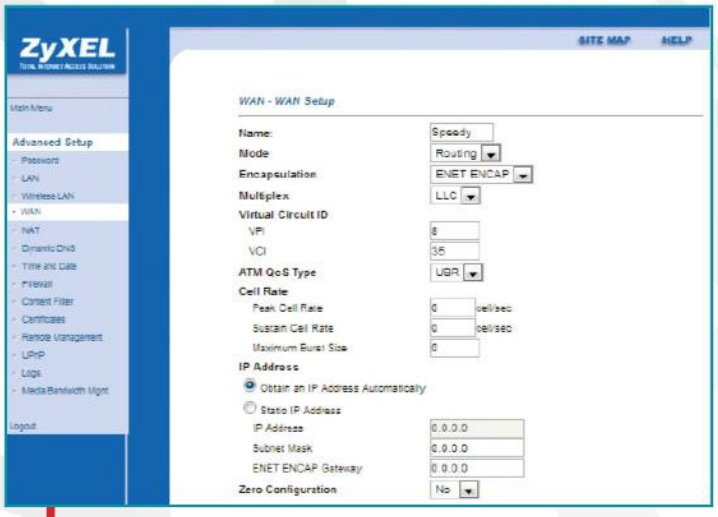
¿Es segura WPA2-PSK?

WPA2-PSK utiliza el cifrado AES, que es netamente superior a TKIP. Hasta la fecha, no se han encontrado vulnerabilidades a WPA2-PSK; sí se conocen formas de ataque que se realizan mediante la captura de paquetes de una sesión de autenticación de un cliente, y puede ejecutarse un proceso de cracking de la clave PSK, siempre que las claves sean sencillas, porque los ataques se realizan mediante diccionarios o tablas de rainbow **(tablas precalculadas).**

▶ **RIP (Routing Information Protocol)**: protocolo de información de enrutado, que permite a un router intercambiar información de enrutado con otros dispositivos de ese tipo. Los campos de dirección RIP controlan los paquetes RIP enviados. Poseen las siguientes opciones:

- **Both**: hace un broadcast de su tabla de enrutado periódicamente e incorpora la información RIP recibida.
- **Only**: no envía ningún paquete RIP, pero acepta paquetes que han sido enviados desde la red.
- **OutOnly**: manda paquetes RIP, pero no acepta ninguno de los paquetes marcados como RIP.
- **None**: no envía ningún paquete RIP e ignora cualquier paquete de este tipo que haya sido enviado.

El dispositivo **ZyxelP-660HW** sirve de ejemplo para conocer cómo debemos configurar un Access Point.



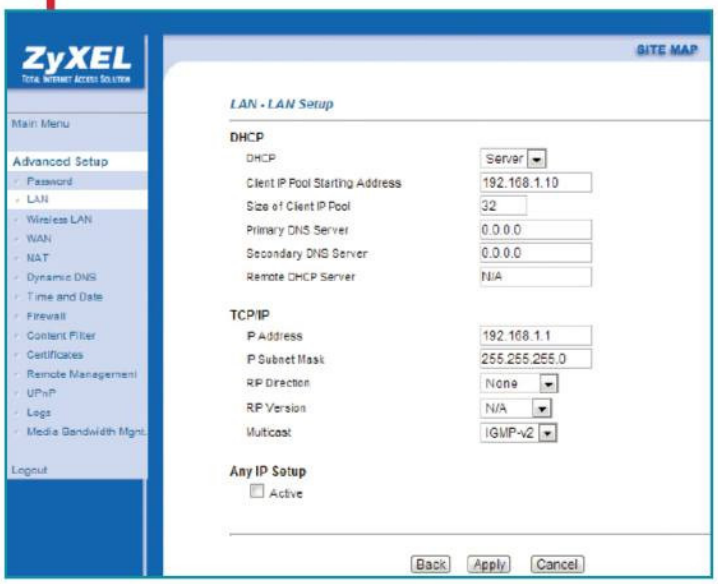
Menú de configuración WAN. Aquí seleccionamos el tipo de conexión y le asignamos un nombre para identificarla.

El campo **Versión** controla el formato y el método de broadcast de los paquetes RIP que envía (reconoce ambos formatos al recibir). **RIP-1** es universalmente soportado, y **RIP-2** aporta más información. Tanto **RIP-2B** como **RIP-2M** envían los datos de enrutado en formato **RIP-2**; la diferencia está en que **RIP-2B** usa broadcast de subred, mientras que **RIP-2M** usa multicast.

Configuración de WLAN

Para configurar las opciones de WLAN ingresamos en el menú **WLAN/Wireless**. Habilitamos la opción adecuada para activar

Configuración LAN y servidor DHCP. Definiremos la IP del AP, y si brindará el servicio DHCP, en qué rango de IP y hasta cuántos clientes aceptará.



wireless; generalmente la encontraremos como **Enable Wireless LAN**. A continuación, veremos algunas opciones.

▶ **Block traffic between WLAN and LAN**: permite limitar el tráfico entre las redes WLAN y LAN.

▶ **ESSID (Extended Service Set Identification)**: seleccionamos el nombre que identifica a nuestra red, con un máximo de 32 caracteres. Es recomendable no nombrarla con datos reales, como **FamiliaPerez**, ya que, al indicar el dueño de la conexión, se está exponiendo la red ante cualquiera que capte la señal.

▶ **Hide ESSID**: permite ocultar el nombre de la red; por lo tanto, cada dispositivo que desee conectarse necesitará conocer el SSID, identificar el dispositivo y, luego, validar con la clave de acceso.

▶ **Channel ID**: permite seleccionar el canal y la frecuencia dentro de los rangos admitidos por el AP.

Para continuar, ingresamos en el menú **Wireless LAN - 802.1x/WPA**. Buscamos y habilitamos la opción **Autentication Required**. Luego, tendremos la posibilidad de determinar el tiempo en segundos de reautenticación y de timeout; configuramos las siguientes opciones:

▶ **Key Management Protocol**: despliega las posibilidades WPA, WPA-PSK, WPA2 y WPA-PSK, de las cuales elegimos esta última.

▶ **Pre-Shared Key**: aquí debemos ingresar la clave de autenticación para que los dispositivos puedan conectarse a la red. Debe ser una clave robusta, que utilice letras mayúsculas, minúsculas, números y caracteres especiales. Admite hasta 63 caracteres, de modo que podemos agregar una larga frase (luego, hay que resguardar la clave para tenerla accesible cuando sea necesaria).

▶ **WPA Group Key UpdateTimer**: tiempo de actualización de la llave WPA, en segundos.

Una vez que todo está configurado, debemos probar con una estación de trabajo. Nos conectamos al ESSID con la clave de autenticación que ingresamos, esperamos a que nos asigne dirección IP y, así, ya terminamos la configuración básica del AP. Para verificar la conexión y ver quiénes están conectados al AP, desde la consola de administración ingresamos en el menú **DHCP Table**, donde veremos los dispositivos conectados y, recibiendo la configuración desde nuestro servicio de DHCP, los datos que obtendremos serán **MAC Address**, **IP asignada**, **nombre NetBios** y **tiempo de conexión**.

Consideraciones adicionales

En este punto ya tenemos nuestra red WLAN funcionando; para no pasar un mal momento, vamos a tomar algunas medidas de seguridad para la configuración del AP. Debemos tener en cuenta los puntos que mencionamos a continuación:

El panel de administración nos solicita la clave de autenticación, que puede conseguirse en el manual del dispositivo.

1) Cambiar la contraseña del usuario administrador por una clave robusta, en lo posible, con más de ocho caracteres. Ya que no es para uso cotidiano, conviene resguardarla en algún programa de administración de contraseñas u otro lugar seguro. En aquellos casos en que el dispositivo lo permita, deshabilitamos el usuario administrador y creamos usuarios personalizados.

2) Configurar el acceso a la consola de administración del punto de acceso mediante HTTPS. En el caso de que la red es corporativa o destinada al uso de clientes, podemos utilizar algunas herramientas desarrolladas para escuchar el tráfico en la red y extraer algunos datos de ella.

3) Debemos restringir el acceso a la administración del AP solo a la red LAN, y deshabilitarlo desde Internet.

4) Cambiar frecuentemente las claves, tanto las del usuario administrador como las de conexión al AP. Esta es una buena práctica, porque no sabemos qué cantidad de personas pueden disponer de la clave de conexión a la red ni su divulgación.

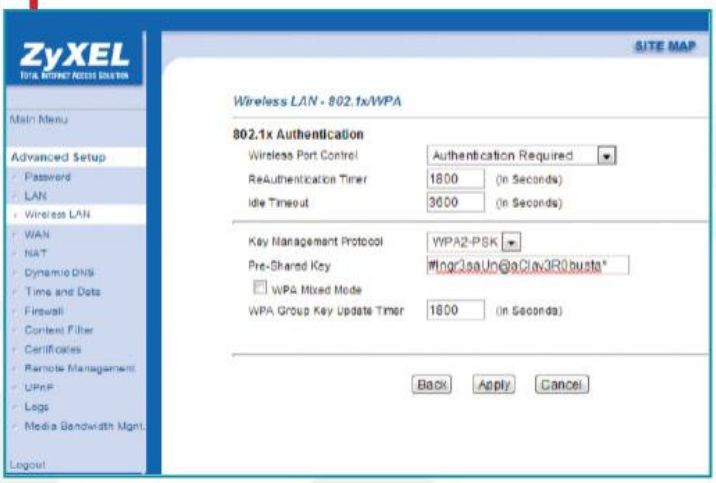
5) Utilizar el **filtrado MAC**, cuando sea posible, para habilitar solo a los dispositivos autorizados. Sabemos que esta medida de seguridad puede vulnerarse, pero, al menos, será una barrera que llevará más tiempo pasar.

LA RED WI-FI OFRECE LA COMODIDAD DE CONECTARNOS DESDE DISTINTOS PUNTOS DENTRO DE UN RANGO CONSIDERABLE DE ESPACIO.

6) Actualizar el **firmware** del dispositivo en forma periódica. Dicho de una manera simple, se trata del software que controla el hardware del access point. Los equipos de investigación suelen encontrar vulnerabilidades o graves agujeros de seguridad, y los fabricantes toman las medidas de parchear el firmware vulnerable con una nueva versión que corrige las fallas que hayan sido detectadas hasta el momento. Además, la realización de actualizaciones de firmware podría mejorar el rendimiento del dispositivo o solucionar algunos problemas de performance.

7) En caso de redes que deban tener un mayor nivel de protección, siempre se recomienda que las ondas inalámbricas no superen el radio en el cual el dispositivo debe funcionar, así se minimizan los accesos no deseados. ■

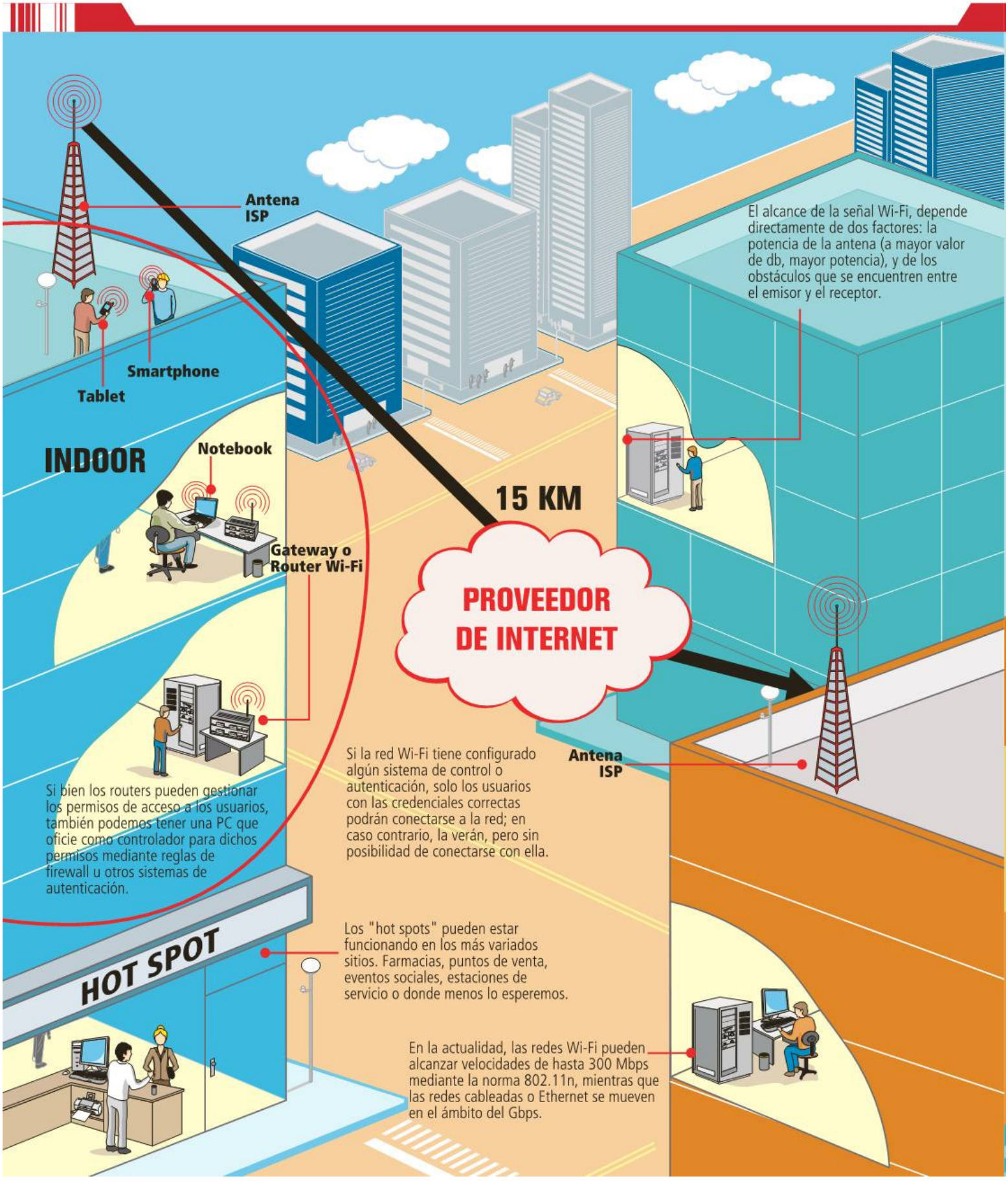
En esta imagen vemos la sección de configuración de la seguridad en el punto de acceso inalámbrico.



Alcance y cobertura

Debemos tener en cuenta que el **alcance de la señal** de la red depende de la potencia del access point, de la potencia del dispositivo Wi-Fi con el cual nos conectamos y de los obstáculos que la señal tenga que atravesar. Cuanto más lejos queramos llegar, a más altura tendremos que ubicar el dispositivo. Si la señal llega debilitada, debemos recurrir a un amplificador, utilizar un AP con mayor potencia o instalar antenas de mayor ganancia Dbi. No todos los dispositivos lo permiten, al igual que agregar una antena exterior.

Redes wireless



Hotel Wi-Fi

1 Para poder obtener un servicio de calidad, tanto el emisor como el receptor, deben tener una línea visual libre, sin interferencias que degraden la señal.

2 Para brindar conectividad continua, el área de cobertura de los access points debe superponerse por un margen del 20%. Evitamos así puntos ciegos en los que los usuarios pierden conectividad.

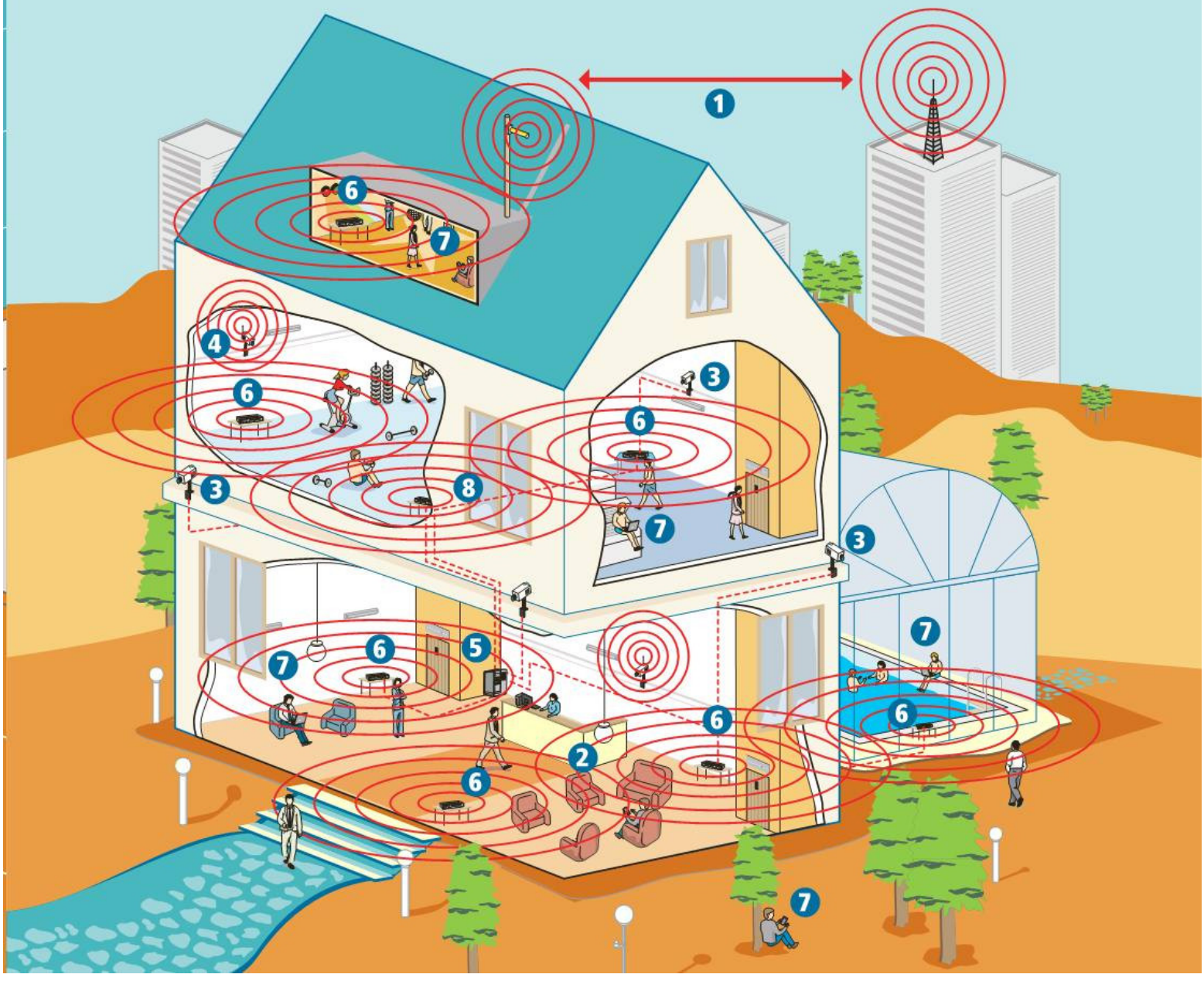
3 4 En materia de seguridad, podemos encontrar una amplia variedad de modelos de cámaras IP inalámbricas que aprovechan la ausencia de cables para ubicarse en lugares estratégicos.

5 Los racks nos permiten mantener asegurado el servidor que autenticará las credenciales de acceso de los usuarios, permitiéndoles hacer uso de los servicios de la red. Asimismo, no dará un control centralizado del funcionamiento de la red.

6 De acuerdo con las necesidades operativas específicas del entorno, pueden convivir dentro de la misma red soluciones inalámbricas y cableadas. Por ejemplo: puede resultar más costoso un sistema de impresión inalámbrico que uno que funcione conectado a un servidor mediante cable Ethernet.

7 Los usuarios podrán acceder al servicio mediante dispositivos como las notebooks/netbooks/ultrabooks, smartphones, tablets, e-book readers u otros que posean capacidades Wi-Fi (siempre y cuando sean compatibles con la norma con la que está configurado el servicio: una notebook de norma 802.11a no podrá conectarse a una red 802.11n, aunque sí sería posible a la inversa).

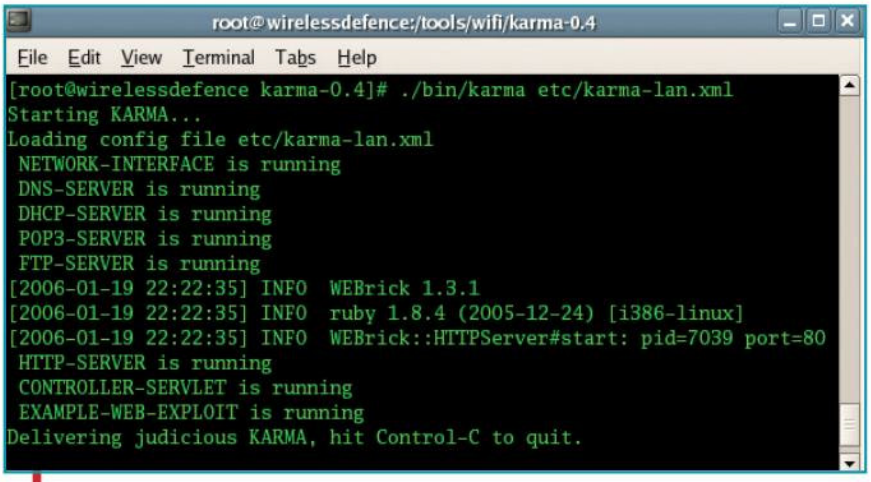
8 Para diseñar la red, debemos tener en cuenta que los access points se conectarán a uno o más switches mediante cables UTP (usualmente categoría 5E).



Ataques en redes inalámbricas

Los ataques a redes inalámbricas se basan en técnicas conceptuales. Aquí veremos algunos métodos aplicados en redes Wi-Fi y Bluetooth.

Los ataques a las redes wireless se basan en los métodos estándares, pero adaptados a esta tecnología. Como en cualquier caso, pueden dividirse en pasivos y activos. Los pasivos son aquellos en los que no se genera tráfico que interactúe con las redes, como el uso de analizadores de protocolos que permanecen a la escucha. En cambio, en los activos, el atacante realiza acciones; por ejemplo, inyecta paquetes manipulados de forma que puedan desasociar a un cliente válido. Los ataques pasivos tienen como objetivo recopilar información de la red y complementar otros ataques.



Inicio de la aplicación **karma**. Esta herramienta permite simular access points falsos para que los usuarios se conecten a ellos.

Técnicas clásicas

Dos técnicas clásicas íntimamente relacionados con estas redes son **Denial of Service** y **Man in the Middle**. En el DoS el objetivo es desasociar a un cliente válido para, luego, complementarlo con un **Man in the Middle** y capturar información de la sesión. A partir de esto, pueden implementarse ataques de fuerza bruta para obtener la clave compartida.

Algunas herramientas también permiten utilizar tablas precalculadas para acelerar el proceso. Otro típico ataque a redes inalámbricas es el uso de **Fake Access Points**, en el cual, mediante una aplicación, se simula un punto de acceso al que los clientes válidos se conectan. Cuando el cliente busca realizar la autenticación y asociación, realizará el proceso de envío de sus credenciales, que son almacenadas por esta aplicación. Luego de recopilar cada una de las credenciales, el atacante puede acceder a utilizarlas para autenticarse en la red como si fuese el usuario registrado en ella.

El uso de Bluetooth

Esta tecnología está marcadamente orientada a dispositivos móviles, como PDAs, teléfonos celulares, computadoras portátiles, impresoras y cámaras digitales. Está diseñada para dispositivos de bajo consumo y de corto alcance. Teniendo en cuenta la potencia de los dispositivos, estos pueden clasificarse en clase 1 (hasta 100 mW), clase 2 (hasta 2,5 mW) o clase 3 (hasta 1 mW), pero independientemente de eso, mantienen absoluta compatibilidad entre sí.

```
Session  Edit  View  Bookmarks  Settings  Help

                        Aircrack-ng 0.9.1

                [00:00:02] Tested 189 keys (got 210409 IVs)

  KB    depth   byte(vote)
   0    0/  1   48(  75) C5(  33) 72(  30) D3(  30) 2A(  27) 16(  15)
   1    0/  4   5B(  15) E4(  15) B0(  13) B9(  13) EF(   6) 12(   5)
   2    0/  1   FE(  44) 1E(  12) 5A(  12) D9(  12) 21(   5) 66(   5)
   3    0/  1   66(  72) 73(  15) 1A(  12) 2A(  12) 7F(  12) 4A(   5)
   4    0/  1   0D(  44) 07(  10) E9(   7) 3A(   6) 1E(   5) 31(   5)
   5    0/  1   5F(  24) 08(   8) 78(   5) 93(   5) E3(   5) FD(   5)
   6    0/  1   61( 465) 82(  46) 6C(  40) 8A(  38) CA(  35) 7B(  32)
   7    0/  1   00(  54) BF(  16) 3E(  10) 7F(   6) 83(   6) C5(   6)
   8    0/  1   3E(  91) 2E(  18) 10(  13) 72(  13) CA(  12) 2B(  11)
   9    0/  1   79(  83) A6(  25) 18(  17) 04(  15) 2C(  12) E0(  11)
  10    0/  1   CD(  74) 62(  15) A4(  12) 11(  10) 18(  10) 5B(   9)
  11    0/  1   7E( 104) 0F(  15) 12(  15) 64(  14) 4F(  13) 63(  12)

          KEY FOUND  [ 48:5B:FE:66:0D:5F:61:00:3E:79:CD:7E:BB ]
```

Búsqueda de claves WPA con la aplicación **aircrack-ng**, que permite realizar ataques a redes inalámbricas.

Wardriving

Una actividad relacionada con el ataque a redes inalámbricas es el llamado **wardriving** y sus derivados. No son ataques hacia una red en particular, sino una actividad cuyo objetivo es **encontrar redes inalámbricas** en distintas zonas geográficas. Para hacerlo, se recorre la ciudad en un vehículo (**wardriving**) o caminando (**warwalking**) portando notebooks que puedan ejecutar herramientas para tal fin. Los ataques más sofisticados, además, recurren a antenas externas para captar mayor cantidad de redes disponibles.

Ataques especiales

También existen ataques especiales, que fueron desarrollados para vulnerar el sistema WEP. El primero de ellos fue el **ataque inductivo de Arbaugh** (2001), que consistía en capturar tráfico WEP y analizar los vectores de inicialización. Dadas las debilidades de estos vectores, luego de haber capturado un cierto porcentaje, se utilizan métodos inductivos para hallar la clave. Aprovechando las debilidades que se presentaron en RC4, **Fluhrer**, **Mantin** y **Shamir** desarrollaron el ataque **FMS**. A diferencia del anterior, FMS se basó en las debilidades del algoritmo RC4 y su implementación en WEP.

En 2002, se optimizó el ataque FMS al reducir el tiempo de **crackeo**. Esta optimización recibió el nombre de ataque **H1kari**, por su desarrollador.
Nada nuevo surgió hasta 2004, cuando se publicó el ataque **Korek**, basado en capturar ciertos vectores débiles que proporcionaban información para obtener la clave mediante métodos estadísticos.

Ataques en Bluetooth

La seguridad en Bluetooth se basa en sus mecanismos de autenticación y cifrado, implementados en la **pila Bluetooth**, una aplicación que administra sus servicios y fue desarrollada por distintos fabricantes. Para su implementación existen tres modos primarios. El **modo 1** no contempla seguridad; los mecanismos de autenticación y cifrado están deshabilitados. En el **modo 2**, la seguridad actúa en la capa **L2CAP** de la pila del protocolo (nivel de servicios), es decir, se aplica una vez que el canal ya fue establecido. En el **modo 3**, el dispositivo inicia el procedimiento de seguridad antes de que el canal se establezca, en las capas bajas de la pila, y realiza autenticación vía PIN. A diferencia del modo 2, toda la comunicación es cifrada.
Como es opcional, al cifrar el canal, puede ocurrir que diferentes dispositivos no se pongan de acuerdo con el cifrado.

Los ataques también son conceptuales con adaptaciones. Algunos de ellos son:

- **Blue Printing**: es una técnica de **fingerprinting** de dispositivos, que permite detectar datos del fabricante y modelo del dispositivo a través de su dirección MAC.
- **Blue Smack**: ataque de DoS que aprovecha debilidades en la capa **L2CAP**. Consiste en armar paquetes que realicen un requerimiento y hagan que el dispositivo no responda o se reinicie.
- **Blue Jacking**: este ataque consiste en conectarse a un dispositivo y colocarle imágenes, mensajes o contactos..
- **Blue Spam**: ataque que está basado en la búsqueda de dispositivos a los que se les envían mensajes arbitrarios.
- **Cracking Bluetooth PIN**: se encarga de aprovechar debilidades en la gestión de claves y el algoritmo de cifrado.
- **Blue Bug**: se trata de una vulnerabilidad que consiste en realizar el envío de algunos comandos al celular a través de un canal encubierto. ■

Aquí observamos la simbología que identifica nodos Wi-Fi.

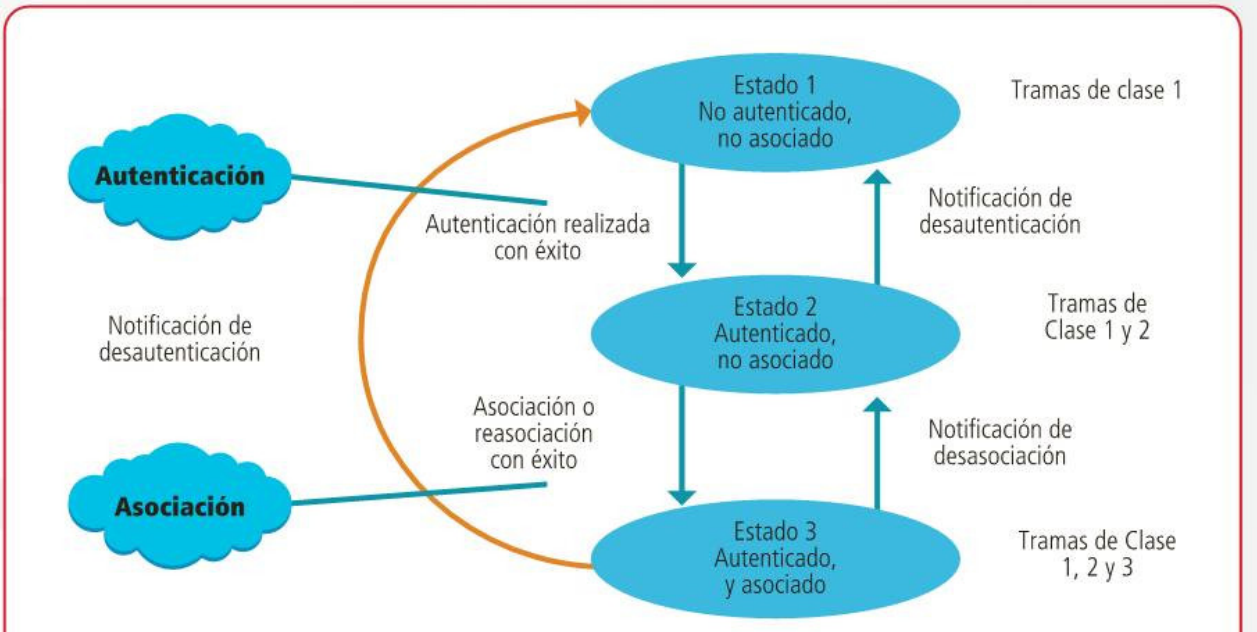
Seguridad en redes Wi-Fi

La seguridad en redes inalámbricas se basa, principalmente, en el protocolo de cifrado utilizado y el mecanismo de autenticación elegido, aquí veremos algunos consejos.

Para encarar el tema de la seguridad en redes inalámbricas, debemos comenzar con los conceptos relacionados a la asociación y autenticación, pero antes, recordaremos el concepto de identificador de red, el **SSID**. Sabemos que el **SSID** (*Service Set IDentifier*) es el **identificador** de cada red inalámbrica, lo cual representa, de alguna manera, el nombre de esta. Debemos tener en cuenta que, cuando un cliente conoce el SSID de una determinada red y quiere conectarse, empieza el proceso de asociación. En caso de no conocer el nombre, de todos modos puede utilizar técnicas para descubrir redes existentes; esto implica que esconder el SSID no sea considerado como un método válido de seguridad. A partir de allí, el estándar 802.11, originalmente, definía dos métodos básicos: autenticación abierta y autenticación de clave compartida (*Pre Shared Key*, o **PSK**).

Autenticación

En la actualidad, el estándar soporta tres métodos: la autenticación abierta, por clave compartida y frente a un servidor externo. De forma complementaria, los distintos equipos también permiten realizar autenticación por direcciones **MAC**.
En la autenticación abierta, el proceso se realiza en texto plano. No se verifica ni al usuario ni al host, sino que es abierta a cualquiera que quiera conectarse. Viene de la mano del uso del sistema WEP, donde un cliente puede asociarse al punto de acceso con una clave WEP incorrecta o, incluso, sin ella, pero no



Representación del proceso de autenticación y asociación para el sistema de cifrado WEP.

Los access point se encargan de enviar el paquete final con el resultado del pedido de autenticación.

podrá enviar o recibir datos, porque la carga de paquetes estará cifrada. Un aspecto importante es que el encabezado no está cifrado por el WEP, solo la transmisión de los datos lo está.
La autenticación por clave compartida es similar a la anterior, aunque agrega una etapa más. En este caso, es necesario que todos los participantes en el proceso de autenticación conozcan la clave WEP. El equipo que quiere autenticarse (cliente) envía una trama AUTHENTICATION REQUEST para indicar que se desea utilizar una clave compartida.
El AP responde enviando al cliente una trama que contiene 128 octetos de texto (**desafío**). El desafío se genera con la clave compartida y un **IV** (**vector de inicialización**) aleatorio, utilizando un **PRNG** (generador de números pseudoaleatorios). Cuando el cliente recibe la trama, copia el contenido del texto de desafío en el **payload** de una nueva trama que encripta con WEP a partir de la **passphrase** y añade un nuevo IV (elegido por el equipo cliente). Ya construida esta nueva trama cifrada, el cliente la manda al AP. El Access point desencripta la trama recibida y comprueba que el **ICV** (*Integrity Check Value*) sea válido.
En segundo lugar, también comprueba que el texto del desafío concuerde con el enviado en el primer mensaje. Si la comprobación es correcta, se produce la autenticación entre el equipo cliente y el punto de acceso. Luego, se vuelve a repetir el proceso pero, esta vez, el primero que manda la trama con el AUTHENTICATION REQUEST es el AP, ya que, de esta manera, se asegura una autenticación mutua. En la próxima sección veremos las implicancias de seguridad de los métodos de autenticación basados en los diferentes protocolos.
Otro tipo de autenticación es la que se realiza contra un servidor externo. Este método no es parte del sistema WEP, sino que fue implementado recién a partir de WPA. La autenticación se realiza frente a un servidor externo, normalmente **RADIUS** (*Remote Authentication Dial-In Use Server*) y utilizando el protocolo de autenticación **IEEE 802.1x**. Analizaremos más en detalle este método cuando veamos el sistema WPA.

Protocolos de seguridad

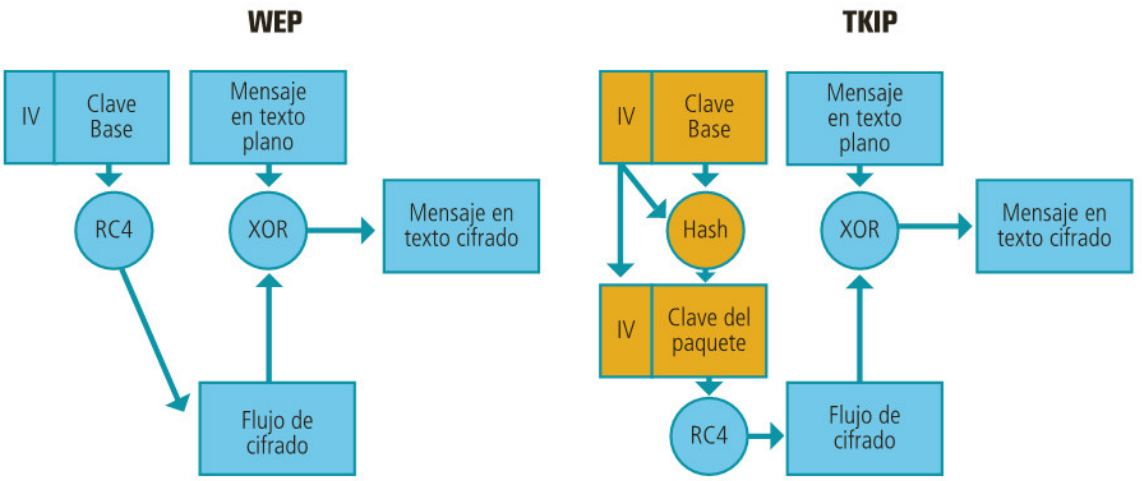
El primer sistema de cifrado para redes inalámbricas fue WEP (**Wired Equivalent Privacy**), desarrollado en 1999. Para comprender su funcionamiento, tengamos en mente los conceptos de autenticación por clave compartida. Como algoritmo de cifrado, utilizaba RC4, en un principio, con una clave de 40 bits (llevada a 64 por la presencia de un IV de 24 bits) y, más tarde, con una implementación de 104 bits de clave (incrementada a 128 por la acción del mismo vector). Otra característica propia de WEP es el chequeo de integridad realizado a los paquetes, que se implementa con un **CRC** (*Cyclic Redundance Check*) de 32 bits. La forma de implementar este sistema es sencilla: tanto el cliente como el AP deben conocer la clave compartida. Dadas las debilidades que iremos viendo a continuación, en la actualidad WEP no proporciona ningún tipo de seguridad, ya que, con las

LAS HERRAMIENTAS DE SEGURIDAD PARA LINUX PUEDEN TENER VENTAJAS RESPECTO A SUS PARES EN WINDOWS.

herramientas adecuadas, es posible echar por tierra en minutos la seguridad de una red bajo este sistema.
Su funcionamiento es bastante sencillo comparado con los nuevos métodos de cifrado. A partir de la clave compartida, se genera una **semilla** que se utilizará para generar las claves de sesión de RC4 con la que se cifrará el tráfico. A continuación, se divide la clave compartida en cuatro bloques de 8 bits cada uno y, luego, se les aplica la **función XOR**, para así generar la semilla. Luego, esa ingresará al **PRNG** para generar 40 cadenas de 32 bits. De ellas se tomará un bit para construir la clave, es decir que se obtendrán

WiFiSlax

En Linux, podemos encontrar distribuciones para una infinidad de usos. Algunas de ellas, están orientadas a la seguridad; en este caso, nos centraremos en WiFiSlax, una distribución orientada específicamente a redes inalámbricas. WiFiSlax posee una amplia variedad de aplicaciones y drivers de la mayoría de las placas wireless. Podemos descargar la distribución, de manera gratuita, desde el sitio web www.wifislax.com.



En este diagrama, podemos apreciar que WEP usa un IV y una clave base que genera IVs débiles. TKIP usa IV y clave base para producir un hash que será la nueva clave, distinta por paquete.

cuatro claves de 40 bits. De estas cuatro, WEP utilizará solo una. Hasta aquí vimos de qué forma se genera la clave; ahora veamos cómo se cifra una trama de datos. En primer lugar, se calcula el CRC de 32 bits de la trama (solo el payload) que se quiere enviar. Al final de esa trama, se añade el resultado del CRC como ICV. Luego, se selecciona una llave de 40 bits de las cuatro posibles y, junto a ella, se añade al comienzo un IV de 24 bits. Esta secuencia de 64 bits (clave + IV) se utilizará para cifrar la trama WEP.
Es importante aclarar que el protocolo WEP no fue creado por expertos en seguridad. Esto se puso de manifiesto cuando se hallaron serias vulnerabilidades que ponían en riesgo las redes que implementaban este sistema. En primer lugar, encontramos las debilidades asociadas al algoritmo **RC4**. Al momento de la salida del protocolo WEP, RC4 ya había sido criptoanalizado, y se pudo reducir el espacio efectivo de claves, permitiendo aplicar fuerza bruta y obtener resultados en tiempos relativamente cortos.

EL TEMA DE LA SEGURIDAD EN REDES INALÁMBRICAS SE HA ESTANCADO DESDE WPA2, DADO QUE SE LLEGÓ A UN PUNTO EN QUE EL RIESGO YA NO SE CENTRA EN EL CIFRADO.

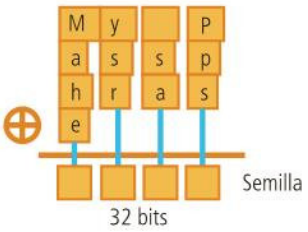
Por otro lado, los **vectores de inicialización** eran demasiado cortos. Con una longitud del vector de 24 bits, se obtiene un espacio de vectores pequeño, de alrededor de 16 millones; si bien este parece un número muy grande, computacionalmente, puede procesarse en un tiempo bastante corto. Las primeras herramientas que atacaban el sistema WEP recorrían el espacio efectivo de vectores en poco menos de seis horas.

Además, el **chequeo de integridad** es débil, ya que CRC es un proceso lineal fácilmente alterable; es un chequeo válido solo a nivel funcional. Los sistemas posteriores descartaron este método como comprobación de integridad. Finalmente, WEP no incluye un método integrado de actualización de claves. El hecho de usar una misma clave compartida por todos los clientes, de la que finalmente se obtienen cuatro claves, le quita entropía al sistema. A partir de estas debilidades, se han desarrollado varios métodos de ataque a este sistema, algunos basados en ataques estadísticos, otros inductivos.

WPA

Con la escasa protección que brindaba WEP, se hizo necesario desarrollar un nuevo sistema de seguridad para redes wireless. Debido a que un nuevo sistema hecho desde cero iba a demandar mucho tiempo y a que era necesario mantener retrocompatibilidad con los equipos que soportaban WEP, la Wi-Fi Alliance desarrolló WPA (*Wi-Fi Protected Access*), que se basaba en WEP, pero fortalecía sus aspectos débiles. Mientras tanto, el IEEE empezaba a desarrollar un nuevo sistema desde cero, que tendría en cuenta los últimos avances en materia de criptografía y seguridad: **IEEE 802.11i**.
WPA ofrece mayor nivel de seguridad que WEP y comparte bastantes características con el estándar IEEE 802.11i, porque fue creado como sistema de transición entre WEP y este último mientras se finalizaba su desarrollo. La mejora más importante respecto de WEP quizá sea la posibilidad de utilizar un servidor de autenticación externo, el cual permite distribuir claves diferentes a cada usuario por medio del protocolo **802.1x**. También puede emplearse, de un modo menos seguro pero más simple, a través de claves compartidas manualmente. Este último modo es muy utilizado en entornos hogareños y de pequeñas empresas; por lo

general, se lo denomina **WPA personal**. Aunque se siguió utilizando RC4, se introdujeron varias mejoras con relación a este proceso. Por un lado, se pasó de utilizar claves de 64 bits a usar las de 128 bits. Además, se duplicó el tamaño de los vectores de inicialización (de 24 a 48 bits). Esto trajo aparejado el aumento del espacio de claves, y redujo la problemática de reutilización de IVs que existía en WEP. En última instancia, se reemplaza el CRC como chequeo de integridad por un nuevo algoritmo, denominado **Michael**. Este no se basa solo en el payload, sino que, además, utiliza otros parámetros, como la dirección MAC de origen, la de destino y un valor generado en forma pseudoaleatoria; de este modo, se elimina el problema de linealidad asociado a CRC. Desde el punto de vista del atacante, el único ataque posible contra este método es la **fuerza bruta**. Sin embargo, durante octubre de 2008, la compañía de seguridad rusa **ElcomSoft** descubrió una vulnerabilidad en TKIP. El método descubierto no permite recuperar la contraseña, pero encuentra un problema en el cifrado, y está limitado a descifrar paquetes concretos o inyectar nuevos y en pequeñas cantidades. Un ataque posible sería generar una denegación de servicio o redirigir el tráfico. Es importante destacar que un ataque de fuerza bruta no es una debilidad de WPA.



Se hace una XOR con la cadena ASCII para obtener una semilla de 32 bits

M	y		P	a	s	s	p	h	r	a	s	e
4D	79	20	50	61	73	73	70	68	72	61	73	65

4D XOR 61 XOR 68 XOR 65 = **21**
79 XOR 73 XOR 72 XOR 0 = **78**
20 XOR 73 XOR 61 XOR 0 = **32**
50 XOR 70 XOR 73 XOR 0 = **53**

} **SEMILLA**

Esquema general de la generación de la semilla correspondiente a WEP.

WPA2

En paralelo al desarrollo e implementación de WPA, el IEEE formó un grupo de trabajo para hallar una solución definitiva al problema de seguridad de las redes inalámbricas. En 2004, fue aprobada la edición final de este estándar, denominado **802.11i**. La Wi-Fi Alliance se basó por completo en este estándar para desarrollar WPA2. De manera análoga a WPA, llama **WPA2-Personal** a la versión de clave compartida, mientras que la versión con autenticación 802.1x se conoce como **WPA2-Enterprise**.

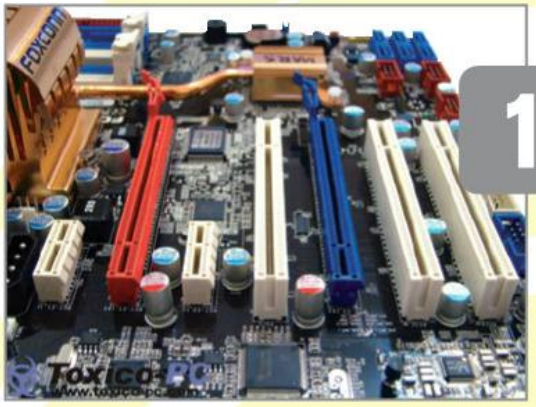
En este caso, la autenticación está íntegramente basada en el estándar 802.1x mediante **EAP** y **RADIUS**. Además, en el proceso de autenticación deja de utilizar TKIP en forma predeterminada para pasar a usar **CCMP** (*CCM Protocol*), aunque sigue permitiendo el uso de TKIP para mantener compatibilidad con los dispositivos diseñados para WEP.

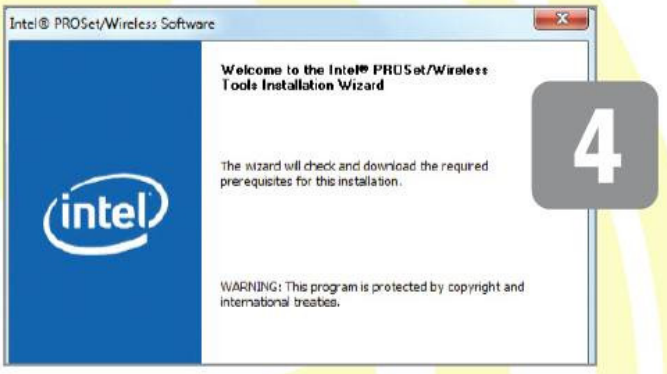
El **CCMP** está basado en AES en su modo de operación **CCM** (*Counterwith* **CBC-MAC**, *Cipher Block Chaining and Message Authentication Code*) con una longitud de clave y tamaño de bloque de 128 bits. Es el análogo a TKIP en WPA y utiliza claves de 128 bits con un vector de inicialización de 48 bits.

La existencia de WPA2 hace que, al encontrarse este cifrado en una red, el atacante no considere un ataque al protocolo, sino que se enfoque en el robo de claves del usuario en otra instancia. ■

Interfaces Wi-Fi en Windows

Una red inalámbrica es más económica que una cableada. En estas páginas aprenderemos en detalle a realizar su implementación.



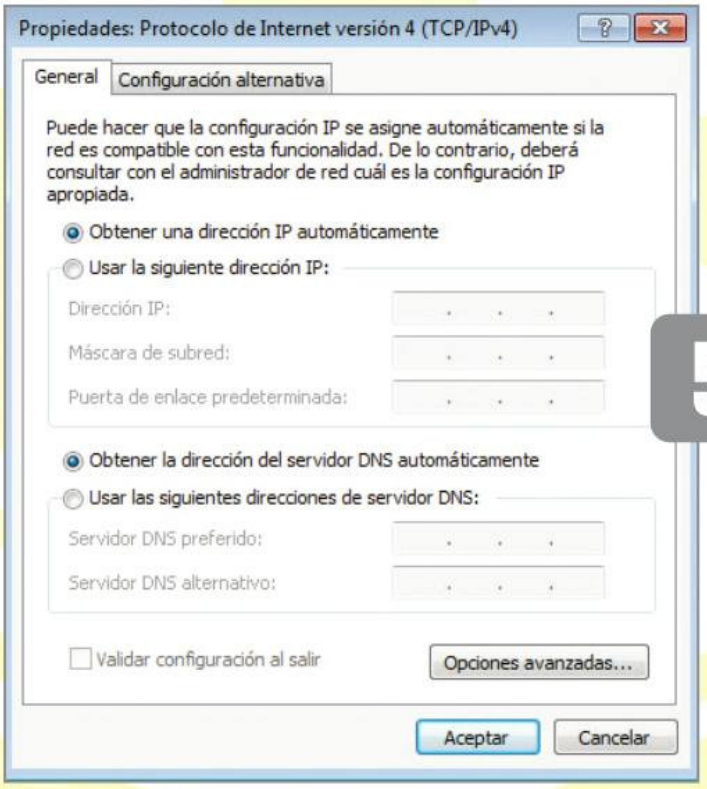


1 Abrimos el gabinete de la computadora e individualizamos el tipo de puerto de conexión (slot) de la placa madre que vamos a utilizar para conectar la placa de red Wi-Fi. Este puede ser PCI o PCI-E (1x) (PCI Express). La diferencia entre ellos radica en el tamaño.

2 A continuación, debemos adquirir una placa de red Wi-Fi compatible con el puerto individualizado. Dentro de lo posible, deberíamos elegir una compatible con puertos PCI-E (1x), ya que es la más nueva de ambas tecnologías.

3 Quitamos los restos de polvo que pueda haber en la ranura del slot con un aerosol de aire comprimido o con un pincel seco. Después insertamos la placa de red en el puerto (existe una única orientación posible) y la fijamos al gabinete.

4 Acto seguido, encendemos la computadora y procedemos a instalar los drivers o controladores del nuevo dispositivo. Por lo general, encontraremos los drivers en el CD que viene junto con la placa. Iniciamos el instalador y seguimos las instrucciones.



5

6

7

8

5 Seleccionamos **Centro de redes y recursos compartidos/Cambiar la configuración del adaptador**. Hacemos clic derecho sobre el adaptador inalámbrico y seleccionamos **Propiedades/Protocolo de Internet versión 4 (TCP/IPv4)**. Por último, nos queda indicar si la IP es dinámica o estática. Si es estática, debemos indicar la IP fija, la máscara de subred y la puerta de enlace.

6 Hacemos un clic izquierdo sobre el icono de la placa de red inalámbrica, ubicado en la esquina inferior derecha, junto a la hora y fecha. Cuando el menú se despliega, seleccionamos la red a la cual queremos conectarnos y presionamos el botón **Conectar**.

7 Si la red posee seguridad configurada, solicitará una contraseña para poder conectarnos. Ingresamos la clave válida, que es definida al crear la red inalámbrica durante la configuración del router Wi-Fi, y presionamos la opción **Aceptar**.

8 Tengamos presente que, antes de quitar la tapa del gabinete y conectar la placa de red inalámbrica al puerto del motherboard, es necesario desconectar la PC de la red eléctrica, para no dañar los componentes.

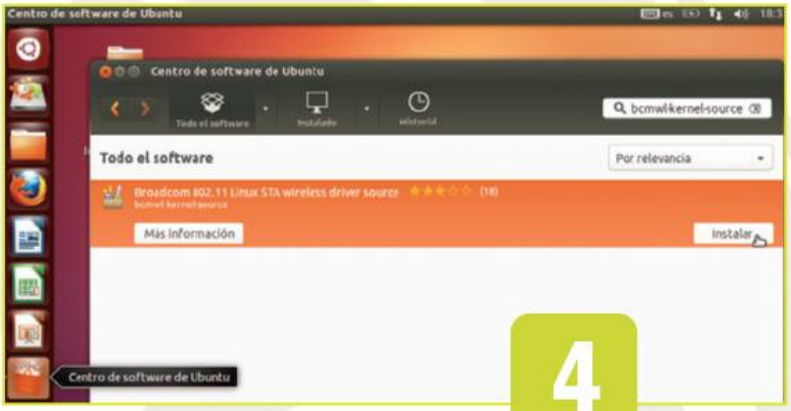
Interfaces Wi-Fi en Linux

Ubuntu es una distribución Linux que posee una interfaz de usuario para la instalación de drivers, muy ágil para principiantes.

1

2

3



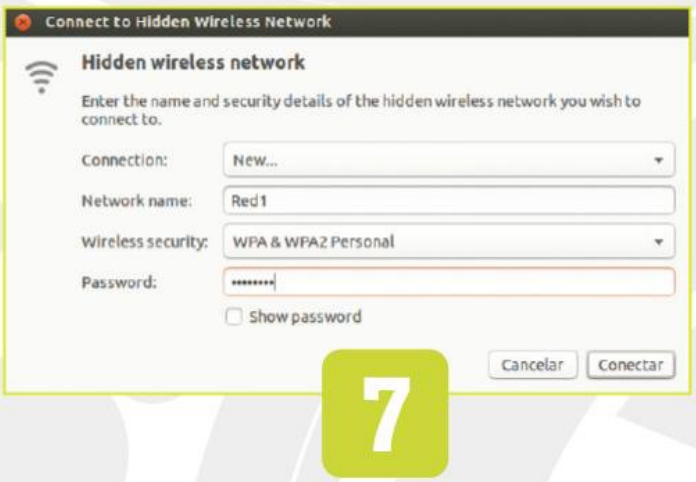
4

1 Al igual que en el procedimiento de instalación sobre Windows, abrimos el gabinete de la computadora e identificamos el puerto de conexión que utilizaremos para conectar la placa inalámbrica. Como en la sección anterior, podemos utilizar PCI o PCI Express.

2 Para continuar, es necesario adquirir una placa de red Wi-Fi que sea compatible con el puerto que utilizaremos. Tengamos en cuenta que conviene elegir una placa compatible con puertos PCI-E (1x), ya que es la más nueva de ambas tecnologías, aunque también podemos elegir PCI, como en este ejemplo.

3 Retiramos los restos de polvo que pueda haber en la ranura del slot usando un aerosol de aire comprimido o un pincel seco. Insertamos la placa de red en el puerto (existe una única orientación posible), en forma perpendicular a la placa madre, y la fijamos al gabinete.

4 Abrimos el gestor de paquetes Synaptic o el Centro de software de Ubuntu. Elegimos el paquete que contiene el driver para el modelo y marca de nuestra placa Wi-Fi, por ejemplo, `bcmwl-kernel-source` y lo instalamos.



5 El Centro de software de Ubuntu permite acceder a la información relevante sobre el driver que estamos instalando. Entre otras cosas, obtendremos un listado del contenido del paquete de software instalado. Los drivers de las placas Wi-Fi más populares, generalmente, suelen ser privativos.

6 Para poder configurar una red en Ubuntu, debemos acceder a **Configuración del sistema/Red**. Una vez posicionados sobre este punto, seleccionamos Inalámbrica y la activamos, así veremos el listado de redes inalámbricas detectadas.

7 En este punto del proceso, solo nos resta seleccionar la red a la cual deseamos conectarnos o ingresar el nombre de la red inalámbrica, el tipo de clave de seguridad para acceder a ella, la clave, entre otros datos. Al finalizar, presionamos el botón **Conectar**.

8 En caso de que no exista la versión para Ubuntu del driver para la placa de red, podemos utilizar el driver **archivo *.inf** del dispositivo para Windows. Para hacerlo, debemos instalar previamente la aplicación **ndiswrapper** a través del Centro de software de Ubuntu.

Modo promiscuo en redes inalámbricas

Las interfaces utilizadas en redes inalámbricas pueden utilizarse en modo promiscuo, tal como sus pares de redes cableadas.

El **modo promiscuo** es un estado en el que un equipo de una red cableada o inalámbrica captura todo el tráfico que circula por él, y no solo el que está dirigido a sí mismo, que es lo que normalmente haría. En redes inalámbricas esto se llama **modo monitor**.

En el ámbito de la seguridad, esto resulta útil para determinar rangos de direcciones IP de equipos de red habilitados para navegar o para realizar ataques contra WEP, que se basan en capturar paquetes y aplicar técnicas estadísticas. No todas las placas inalámbricas pueden trabajar en modo promiscuo, y es importante verificarlo al elegir una placa o notebook. El modo monitor también permite la inyección de paquetes y los ataques que simulan **access points** reales.

Técnicas

Es posible detectar la existencia de equipos con placas en modo promiscuo mediante herramientas basadas en el envío de paquetes que nadie debería responder, excepto, los sistemas en modo promiscuo.

Un aspecto importante a la hora de comprar una placa inalámbrica es su chipset.

Una de las técnicas implica la detección de latencia en paquetes **ICMP**. En este caso, se lanzan peticiones **TCP** erróneas para que ningún sistema las tenga en cuenta. Inmediatamente después, se envía un ping con destino a toda la red. Quien esté en modo promiscuo, debería tardar un poco más en responder, ya que estará ocupado procesando los ICMP. Tengamos en cuenta que, si el atacante bloquea los ICMP en el **firewall** local, evitaría ser descubierto.

Existe otra técnica que implementa la detección mediante paquetes **ARP**, enviando un paquete a la dirección IP de un sistema y a otra que no existe. En caso de que se encuentre en modo promiscuo, procesará esos paquetes y los responderá. Esto se reitera para todas las IP locales válidas, para verificar los equipos. Un atacante avanzado podría evitar ser descubierto no respondiendo a los paquetes.

Resoluciones DNS

El último método es la detección por resoluciones **DNS**. Suele ocurrir que el software de captura de paquetes tiene activada por defecto la opción de resolver las IP de los sistemas que encuentra y los destinatarios de paquetes que captura.

Si se lograra enviar paquetes desde una dirección inexistente hasta otra para verificar si se solicitan las resoluciones de DNS, se estaría encontrando un equipo en modo promiscuo. Si el atacante deshabilita la opción en el **sniffer**, evitará la posibilidad de ser detectado. ■

Software relacionado

En cuanto al software para la detección de placas en modo promiscuo, podemos mencionar, por ejemplo, PromqryUI para entornos Windows, y SniffDET para Linux. Como software de captura de paquetes, podemos considerar las clásicas herramientas Wireshark (ex Ethereal), ettercap y tcpdump, y de manera más avanzada, Cain y Abel, que solo funciona bajo Windows y, además de realizar capturas, permite otros tipos de ataques a contraseñas y de **ARP poisoning**.

PRÓXIMA ENTREGA

8

CONFIGURACIÓN DE REDES INALÁMBRICAS

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

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 00007
9 789871 857784

CONTENIDO DE LA OBRA

1 Introducción a las redes informáticas
2 Tipos de redes y topologías
3 Dispositivos de red
4 Instalación de redes cableadas
5 Puesta en marcha de una red cableada
6 Configuración de redes cableadas
7 INSTALACIÓN DE REDES INALÁMBRICAS
8 Configuración de redes inalámbricas
9 Seguridad en redes cableadas e inalámbricas
10 Configuración avanzada de routers
11 Recursos compartidos y dispositivos multimedia
12 Seguridad física de la red
13 Impresoras de red
14 Hardware de servidores
15 Administración de Windows Server
16 Administración de sistemas Linux
17 Administración y asistencia remota
18 Servidores web y FTP
19 Servidores de mail
20 Servidores de archivos e impresión
21 Servidores adicionales
22 VLAN, VPN y trabajo remoto
23 Telefonía IP
24 Cámaras IP