U10 - REDES INALÁMBRICAS

1. SEGURIDAD EN REDES INALÁMBRICAS

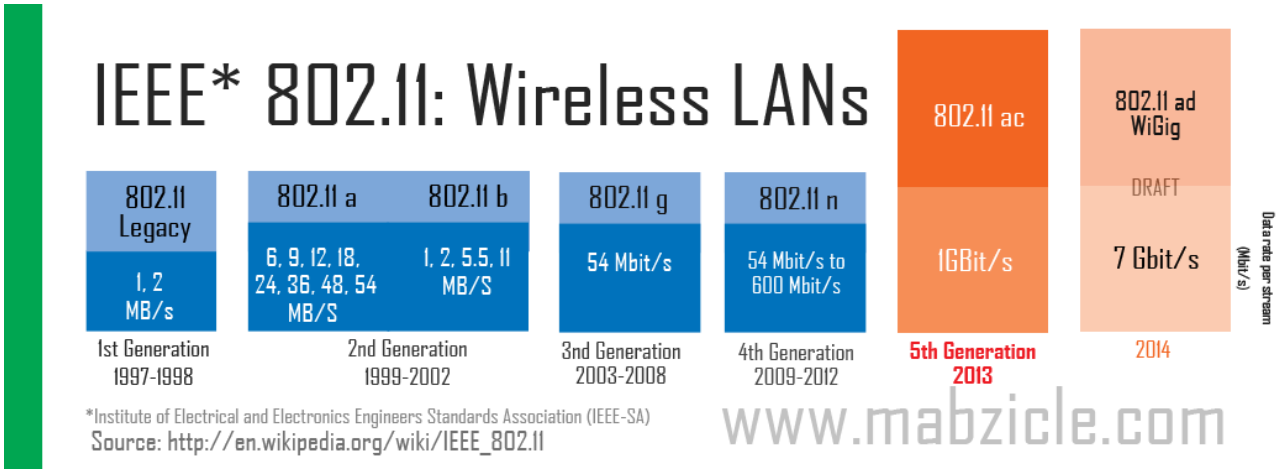
Actualmente las redes inalámbricas se utilizan cada vez más, superando ya en uso a las cableadas. Eso es debido a la reducción de costes que supone no necesitar una infraestructura de cable y por la movilidad que permite a los usuarios desplazarse por una organización con sus portátiles o dispositivos móviles como smartphones o tabletas.

Todos los ataques que se pueden realizar en una red cableada son igualmente válidos en redes wifi. Sin embargo, las redes inalámbricas presentan nuevos vectores de ataque que no existen en las redes cableadas y que aparecen por el mero hecho de que los datos circulan libremente por el aire, pudiendo ser escuchados por cualquiera.

Además de los problemas típicos de falta de cobertura, interferencia con puntos de acceso (AP) cercanos en el mismo canal o presencia de inhibidores de frecuencia, están los problemas de seguridad en el acceso y que se estudiarán en esta sección.

2. ESTÁNDARES WIFI

Existen distintos estándares que se han ido implementando con el paso del tiempo, con el objetivo de mejorar la conectividad y su rendimiento. Todos son mejoras y parten del inicial estándar **802.11**. Poseen características diferentes como la frecuencia que usan, el ancho de banda, la velocidad y el alcance o rango.



Los estándares más utilizados actualmente en las redes Wi-Fi son los siguientes:

802.11

- Velocidad (teórica)- 2 Mbit/s
- Velocidad (práctica) - 1 Mbit/s
- Frecuencia - 2,4 Ghz
- Ancho de banda - 22 MHz
- Alcance - 330 metros
- Año de implementación - 1997

802.11a

- Velocidad (teórica)- 54 Mbit/s
- Velocidad (práctica) - 22 Mbit/s
- Frecuencia - 5,4 Ghz
- Ancho de banda - 20 MHz
- Alcance - 390 metros
- Año de implementación - 1999

802.11b

- Velocidad (teórica)- 11 Mbit/s
- Velocidad (práctica) - 6 Mbit/s
- Frecuencia - 2,4 Ghz
- Ancho de banda - 22 MHz
- Alcance - 460 metros
- Año de implementación - 1999

802.11g

- Velocidad (teórica)- 54 Mbit/s
- Velocidad (práctica) - 22 Mbit/s
- Frecuencia - 2,4 Ghz
- Ancho de banda - 20 MHz
- Alcance - 460 metros
- Año de implementación - 2003

802.11n

- Velocidad (teórica)- 600 Mbit/s
- Velocidad (práctica) - 100 Mbit/s
- Frecuencia - 2,4 Ghz y 5,4 Ghz
- Ancho de banda - 20/40 MHz
- Alcance - 820 metros
- Año de implementación - 2009

802.11ac

- Velocidad (teórica)- 6.93 Gbps
- Velocidad (práctica) - 100 Mbit/s
- Frecuencia - 5,4 Ghz
- Ancho de banda - 80 o hasta 160 MHz
- Año de implementación - 2013

- Nuevo estándar sin interferencia pero con menos alcance, aunque hay tecnologías que lo amplían.

802.11ad

- Velocidad (teórica)- 7.13 Gbit/s
- Velocidad (práctica) - Hasta 6 Gbit/s
- Frecuencia - 60 Ghz
- Ancho de banda - 2 MHz
- Alcance - 300 metros
- Año de implementación - 2012

Otros estándares pendientes de aprobación.

Todas las mejoras recientes tratan de evitar la popular frecuencia de la banda de 2.4 GHz ya que está muy congestionada.

Podríamos decir que el estándar más utilizado es el 802.11ac, debido principalmente:

- Uso de la banda de 5GHz. Aunque en la práctica el radio de alcance es menor, en la práctica se puede alcanzar mayores distancias usando le tecnología "Beamforming", que localiza la señal de radio.
- La posibilidad de usar canales de radio más anchos. En vez de usar 40MHz de ancho de canal, AC puede funcionar con 80 o hasta 160MHz. Algunos tienen la posibilidad de usar la característica "*Channel Bonding",* es decir poder combinar dos canales independientes.
- Los routers actuales transfieren al mismo tiempo hasta seis flujos de datos (spatial streams) usando tres antenas. Con AC se pueden utilizar hasta cuatro antenas.

La introducción del 802.11n en 2009 fue el cambio más importante en la historia del estándar. Supuso un punto de inflexión introducir las redes **MIMO** (Multiple-input Multiple-output, Múltiple entrada múltiple salida).

Estas redes MIMO hacen uso de varias antenas en un mismo router para enviar y recibir datos de manera simultánea, agilizando así la velocidad de la conexión. Además, se consiguió mejorar la cobertura, llegando a 120 metros en interior y 300 metros en exteriores.

El estándar 802.11ac, caracteristicas y ventajas

El estándar 802.11ac se está implementando desde el comienzo del 2014; los componentes que lo emplean consumen menos energía, por lo que es ideal para dispositivos portables, además ahora es posible transmitir datos idénticos a usuarios diferentes.

Usando la banda de 5 GHz el radio de alcance es menor, pero en la práctica se pueden alcanzar distancias mayores usando la tecnología "Beamforming" que focaliza la señal de radio en determinadas zonas

La velocidad del 802.11ac se debe a dos factores:

1. La posibilidad de usar canales de radio más anchos: En lugar de usar 40 MHz de ancho de canal, AC puede funcionar con 80 o hasta 160 MHz. Otra posibilidad es la de usar la característica "Channel Bonding", es decir poder combinar dos canales independientes.
2. Antenas múltiples: Los routers actuales transfieren al mismo tiempo hasta seis flujos de datos (spatial streams) usando tres antenas. Con AC se pueden utilizar hasta cuatro antenas.

Podríamos decir que el estándar más utilizado actualmente es el 802.11ac.

El estándar 802.11ah o Wi-Fi HaLow, caracteristicas y ventajas

IEEE 802.11ah es un nuevo protocolo de redes inalámbricas que comienza a implementarse en el 2016. Surge a causa de los constantes requerimientos de la tecnología, la información y el mercado.

Se diferencia de los anteriores por:

- Usar frecuencias inferiores a 1 GHz
- Permitir aumentar el rango de alcance de estas redes, hasta alrededor de 1000 metros, con todas las posibilidades que ello conlleva.
- Tener un menor consumo de energía.

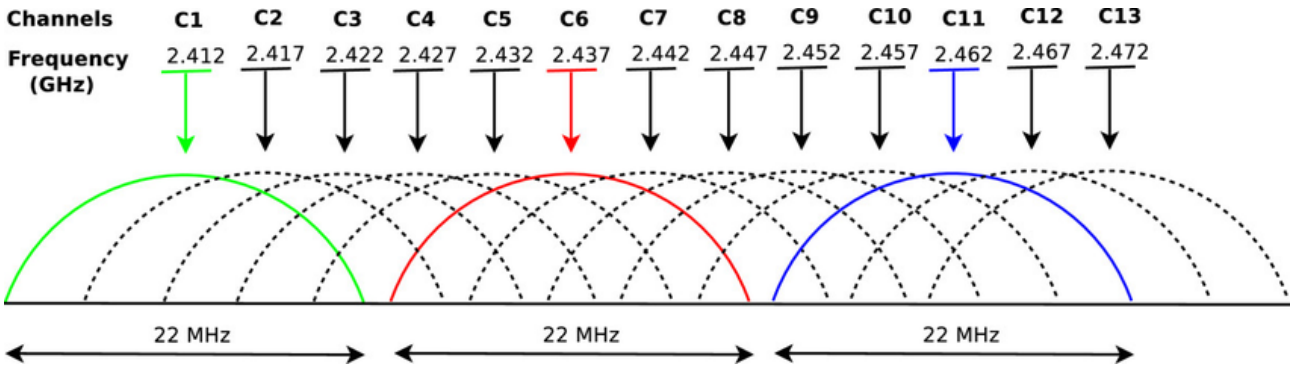
Wi-Fi alliance anunció que 802.11ah se conocería con el nombre Wi-Fi HaLow, y está desarrollado expresamente para el IoT (Internet of Things, o Internet de las cosas).

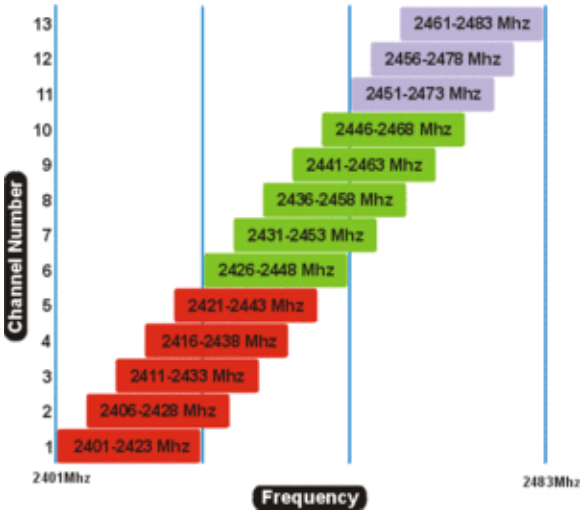
Será el gran competidor de Bluetooth en los próximos años, ya que está pensado para pulseras de monitorización, sensores domésticos, cámaras de seguridad, etc.; campos hasta ahora copados por el Bluetooth, respecto al que según la Wi-Fi Alliance ofrece un rendimiento energético similar.

3. CANALES Y ANCHO DE BANDA

La configuración WiFi de un router, si queremos que sea la idónea, no es del todo sencilla. La tecnología WIFI funciona sobre las bandas de 2,4 y 5 GHz, dentro del espacio radioeléctrico. Este espectro está regulado para garantizar la interoperabilidad entre equipos, de tal modo que radio, telefonía móvil y otras conexiones puedan funcionar también correctamente. Dentro del WiFi, hay varios canales de diferente amplitud.

Banda 2’4GHz

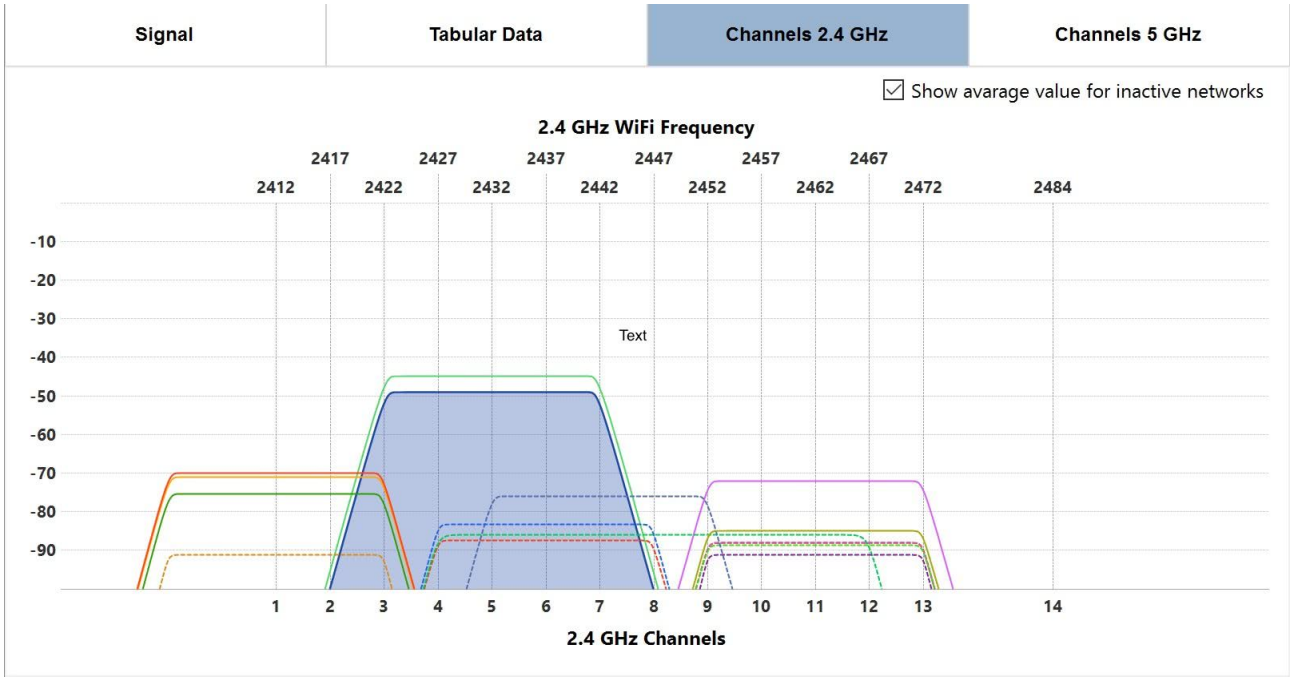




Todas las versiones Wi-Fi a través de **802.11n (a, b, g, n)** funcionan entre las frecuencias de canal de 2400 y 2500 MHz. Estos 100 MHz en el medio se dividen en 14 canales de 22 MHz cada uno. Como resultado, cada canal de 2,4 GHz se superpone con cuatro canales (véase el diagrama anterior). La superposición hace que el rendimiento de la red inalámbrica sea bastante bajo.

Si todos los dispositivos WiFi estuvieran configurados entre canales que no se solapenno habría problemas de interferencias. El problema está en que sí seguirían produciéndose interferencias dentro del canal. Si repartimos todas las redes WiFi entre solo tres canales, entonces tendremos una mayor densidad de dispositivos por canal, luego más competencia. El intercambio dentro de un canal es limitado,

y por tanto esta 'densidad' es la que produce interferencias, que del lado del usuario se traduce en problemas de conexión, lentitud, mala señal y un largo etcétera de contratiempos. Es por eso que, aunque en teoría los canales 1, 6 y 11 del WiFi son los mejores, en la práctica hay que atender a la configuración del resto de redes a nuestro alcance. Y según esto, configurar la que más nos convenga para evitar la saturación.

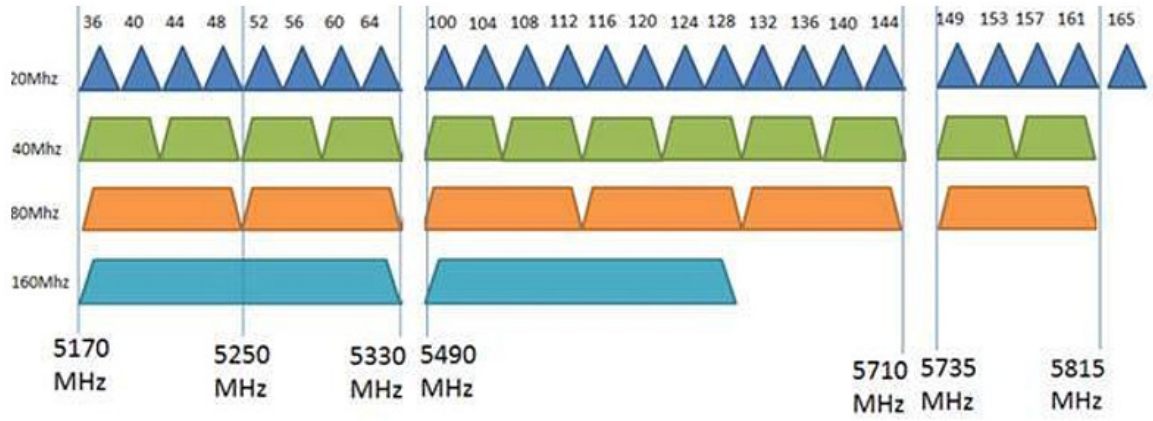


En España se pueden utilizar los canales 1-13; el canal 14 es el único prohibido, solamente se puede utilizar en Japón.

Este **estándar 802.11n** ofrece la posibilidad de operar con una amplitud de canal, o **ancho de banda de 40 MHz** uniendo dos canales de 20 MHz para ello. Cuanto mayor ancho de banda por canal mayor flujo de transferencia *–más velocidad-* entre el router y los dispositivos conectados. Sin embargo, la realidad es que la **saturación** del espacio radioeléctrico asignado sobre la banda de 2,4Ghz es tal, que utilizar un ancho de banda de 40 MHz puede provocar importantes problemas de **interferencias** entre los dispositivos.

Banda 5GHz

En España se permite el uso de los canales 36-64 y 100-140, al igual que en el resto de Europa.



Sobre el **estándar 802.11ac** la cosa es diferente, porque el **WiFi** opera sobre la **banda de 5 GHz** con mayor cantidad de canales y un **mayor ancho de banda** posible. Actualmente se puede aún aprovechar el **ancho de banda de 80 MHz, con opción de alcanzar los 160MHz** para para conseguir las máximas prestaciones de la conexión WiFi. Sin embargo, en el futuro es posible que, como ocurre ahora con los **2,4 GHz**, tengamos que *'migrar'* a **40 o incluso 20 MHz** para lidiar con la saturación de red.

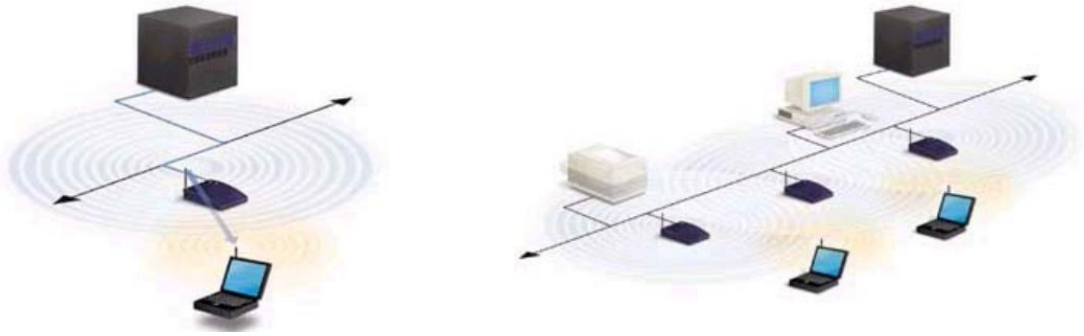
Por último para solucionar la congestión del espectro y las interferencias se han producido otras **mejoras técnicas.** Con la llegada de **Wave 2** se ha introducido **Multi User Mimo**. Es decir, que un router puede servir **varios flujo de tráfico** de forma simultánea a diferentes usuarios, de tal modo que la **tasa de transferencia** se optimiza para varios terminales en lugar de uno único.

4. Conceptos sobre redes WIFI

Modos de conexión WI-FI

Existen dos tipos de conexiones Wi-Fi: el modo "infraestructura" y el modo "ad hoc".

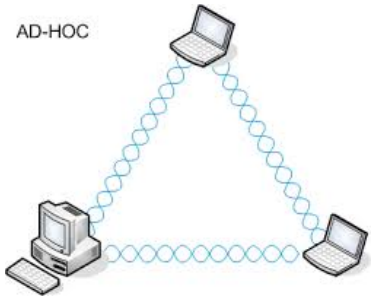
- El primero de ellos es la conexión que se efectúa entre un equipo o dispositivo y un punto de acceso inalámbrico (AP) ya sea un router o un punto público.



Las redes que emplean varios puntos de acceso permiten lo que se conoce como **roaming**, es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación.

Mediante el uso de puntos de acceso es posible conectar dos redes separadas por varios cientos de metros, como por ejemplo dos redes locales situadas en dos edificios distintos. De esta forma, una LAN no inalámbrica se beneficia de la tecnología inalámbrica para realizar interconexiones con otras redes, que de otra forma serian más costosas, o simplemente imposibles.

- El modo **ad-hoc** es la conexión que se establece entre dos equipos o dispositivos de forma independiente. Esta conexión solo permite algunos metros de alcance.



¿Qué es Wi-Fi Direct?

https://www.redeszone.net/2018/04/08/wi-fi-direct-configuracion-uso/

Wi-Fi Direct es la tecnología que permite crear una conexión entre dos dispositivos por Wi-Fi, de forma similar a una red ad hoc.

Los dispositivos que la admiten ya traen integrado un pequeño punto de acceso, por lo que no es necesario depender de una computadora para crear la red y todo se hace más sencillo y seguro.

Es importante conocer que solo es necesario que uno de los dispositivos admitan Wi-Fi Direct, además no importa que sean de fabricantes diferentes.

Con Wi-Fi Direct se puede conectar teléfonos, tabletas, impresoras, cámaras, protegidos mediante la autentificación WPA2.

Por ejemplo, de esa forma podemos compartir la conexión de internet en un teléfono celular con otro dispositivo ya sea un teléfono, tableta una computadora de escritorio o una Laptop.

Todo sin necesidad de instalar ninguna aplicación.

ESSID - SSID

Cada red wirelesss tiene un ESSID (Extended Service Set Identifier), que la identifica, viene a ser la identificación o nombre de la red WIFI. El ESSID consta de cómo máximo 32 caracteres y es case-*sensitive*. Es necesario conocer el ESSID del AP para poder formar parte de la red WIFI, es decir, el ESSID configurado en el dispositivo móvil tiene que coincidir con el ESSID del AP.

BBSID

Dirección MAC del punto de acceso, la emplean las tarjetas wireless para identificar y asociarse a redes inalámbricas.

Beacon Frames

Los puntos de acceso mandan constantemente anuncios de la red para que los clientes móviles puedan detectar su presencia y conectarse a la red inalámbrica. Estos “anuncios” son conocidos como BEACON FRAMES, si capturamos las tramas de una red inalámbrica podremos ver que

normalmente el AP manda el ESSID de la red en BEACON FRAMES, aunque esto se puede deshabitar por software en la mayoría de los AP que se comercializan actualmente.

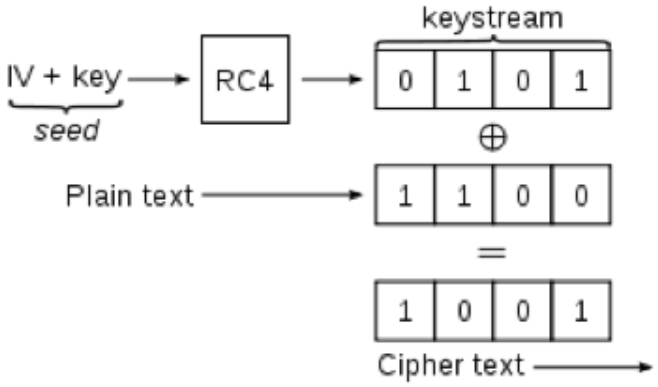
5. Mecanismos de cifrado

WEP

Wired Equivalent Privacy fue el primer mecanismo de protección wifi, que como todo el mundo ya sabe a estas alturas, es completamente inseguro y se desaconseja su utilización en cualquier entorno.

Algunas de sus características son:

- Utiliza una contraseña estática compartida de 40 o 104 bits que se combina con 24 bits del vector de inicialización IV.
- Algunos fabricantes amplían la clave, y en algunos casos el IV también, a una longitud de 128 o 232 bits (se llamó WEP2), pero no aporta una mejora real a la seguridad.
- Usa el algoritmo de cifrado de flujo (stream cipher) RC4.
- A través del la clave WEP más el IV, se genera un keystream que se combina con la trama usando una XOR bit a bit, produciendo la trama cifrada.
- No numera las tramas por tanto es vulnerable a ataques de replay (reinyectar la misma trama muchas veces en la red), así es que con inyección de paquetes se obtiene clave WEP en pocos minutos.



La principal debilidad de WEP es usar RC4 con claves estáticas que no cambian, a pesar de usar los IV. Mediante un ataque estadístico con criptoanálisis, herramientas como **aircrack-ng** pueden romper una clave WEP inyectando y capturando tráfico durante pocos minutos.

El mecanismo de **asociación en WEP** funciona en dos modos:

Modo “**open**”:

- No existe autenticación, configuración por defecto en los puntos de acceso
- Cualquier dispositivo wifi puede asociarse

- Para descifrar y generar tráfico válido, se necesita la clave

Modo "**shared**":

- Existe autenticación y se necesita la clave WEP para asociarse
- Paradójicamente es más inseguro que el método open
- El handshake (tramas que se usan para asociarse entre AP y dispositivo) se puede capturar y descifrar la clave fácilmente

WPA

WPA es el estándar de cifrado recomendado en las redes actuales y a ser posible en su versión WPA2. WPA y WPA2 surgen para mejorar la baja seguridad de WEP. WPA surgió primero como solución temporal. Algunas de sus características son:

- más económico que WPA2
- no necesita actualizar el hardware (router y tarjeta)
- vectores de inicialización mayores que WEP (48 bits)
- números de secuencia en cada trama
- integridad en tramas MIC (MICHAEL)
- utiliza claves dinámicas RC4 que van cambiando (TKIP)

WPA2 mejora sustancialmente a WPA en lo siguiente:

- soporta completamente la norma 802.11i
- utiliza el cifrado simétrico AES (CCMP) mucho más robusto que RC4 y que necesita más potencia de cálculo
- puede usar TKIP pero se recomienda AES
- necesita actualización hardware del equipamiento. Los routers o dispositivos más viejos sólo soportan WEP y WPA pero no WPA2 con AES
- tiene el modo personal (PSK o clave precompartida) y enterprise (EAP/802.1X con servidor RADIUS)

Sin embargo, WPA2 si se configura inadecuadamente, también es vulnerable a ataques:

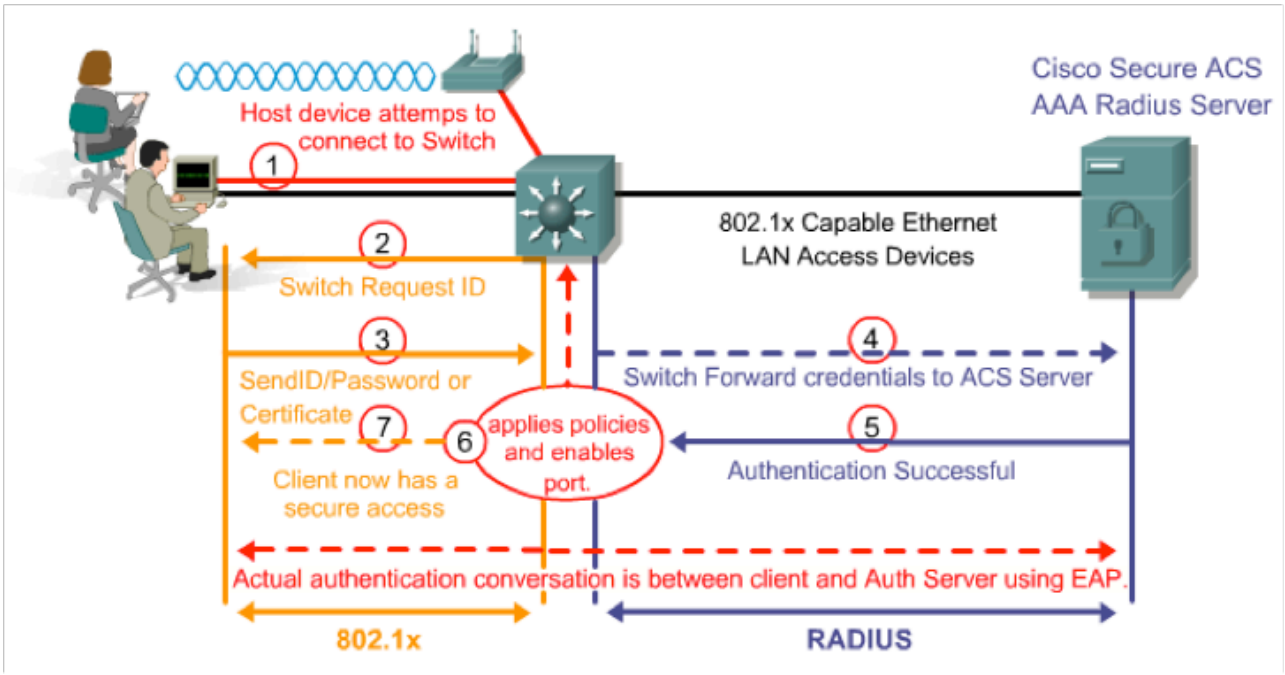
- **Contraseña maestra WPA/WPA2 débil**: si la contraseña elegida para WPA no es robusta, puede romperse con diccionarios o fuerza bruta. Tan sólo hay que capturar el handshake (protocolo de asociación de un cliente wifi a la red) e intentar averiguar la contraseña con alguno de estos métodos.
- **Configuraciones por defecto**: si no cambiamos la contraseña WPA y el nombre de la wifi que viene por defecto en el router de un proveedor de Internet, se puede obtener la clave WPA si el router del fabricante con muchas de las aplicaciones que hay disponibles por Internet, incluso para móviles. Esto es

debido a que algunos fabricantes implementan algoritmos de generación de la contraseña por defecto que son débiles y sencillos de adivinar mediante ingeniería inversa, a partir de los valores del BSSID (MAC del AP), nombre de la wifi y contraseña por defecto.

- **WPS** (Wi-Fi protected setup): este sistema permite configurar clientes wifi de forma sencilla para gente no iniciada, con tan solo estar cerca del punto de acceso mediante mecanismos como NFC, USB, pulsando un botón en el router o introduciendo un PIN. El uso del pin es bastante habitual, pero existen vulnerabilidades en muchos routers y puntos de acceso inalámbricos de fabricantes en los que si está habilitada esta característica y aunque la contraseña maestra WPA sea realmente compleja, es posible averiguar el PIN de WPS en unas pocas horas (son 8 dígitos separados en dos bloques de 4). Si se averigua el PIN, se puede transferir la configuración de la red al cliente a través de este protocolo.

WPA Enterprise

Utilizar WPA/WPA2 con claves precompartidas (PSK) es una buena solución para escenarios con pocos usuarios, como en un domicilio particular. Pero cuando estamos en una organización con cientos de usuarios potenciales, como un centro educativo, la solución más robusta es usar un sistema con WPA Enterprise con un servidor de autenticación RADIUS. De esta manera cada usuario del sistema accede con su usuario y contraseña único e intransferible, en vez de una contraseña compartida para todos que finalmente todo el mundo intercambia y es conocida por todos disminuyendo la seguridad de la red al poder conectarse cualquiera.

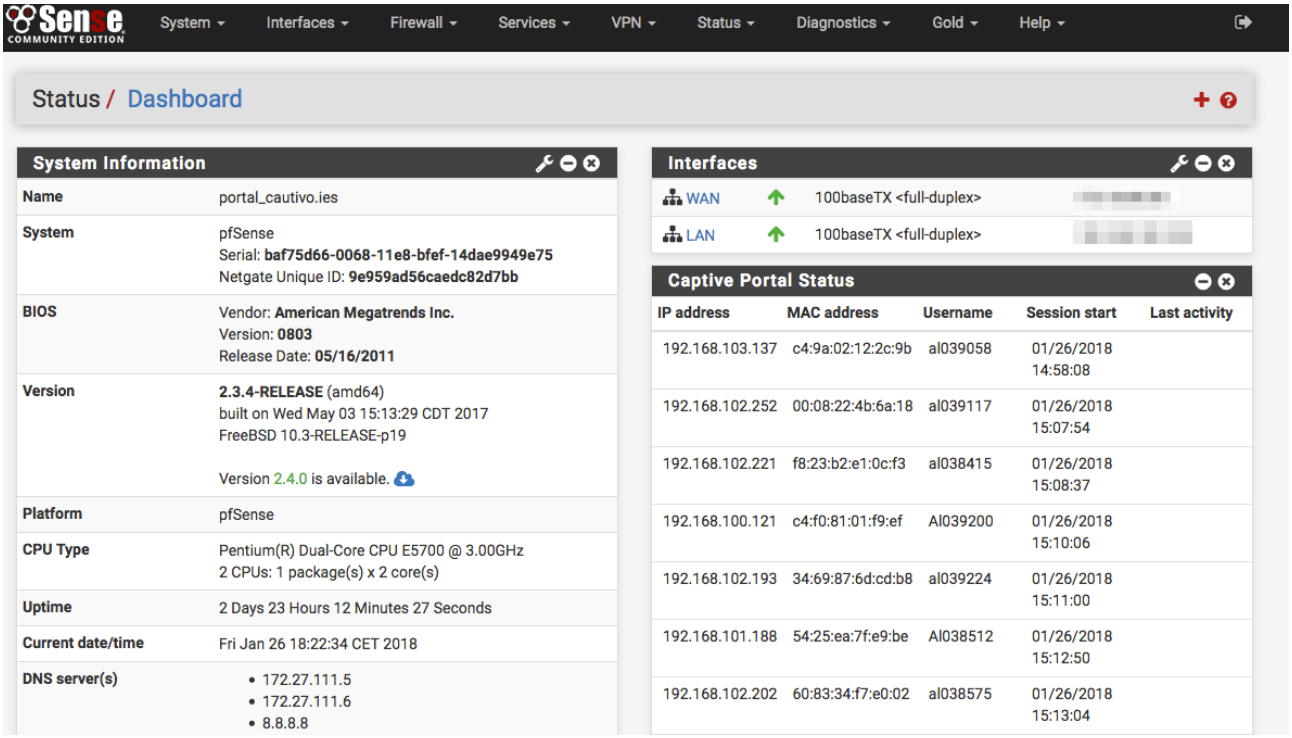


Existen muchos tutoriales en Internet que explican como montar un servidor RADIUS con **freeradius** y una base de datos de usuarios LDAP o Active Directory, donde se almacenan todos los usuarios del sistema.

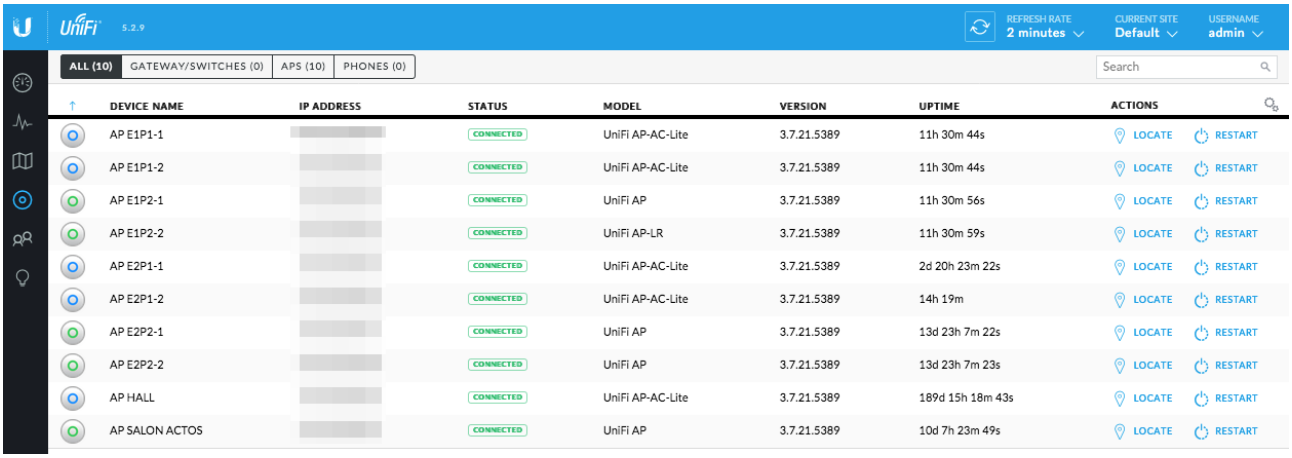
En el IES Severo Ochoa usamos una red wifi con WPA/WPA2 Enterprise con un servidor freeradius y una base de datos de usuarios LDAP.

Los usuarios (profesores, alumnos y PAS) acceden a la red wifi con su usuario y contraseña, que es el mismo con el que acceden al Moodle del centro (no el de formación semipresencial que lo gestiona la Consellería), así como los otros servicios que disponemos en la red del centro. De esta forma, con las mismas credenciales acceden a todos los servicios a los que les autoriza el servidor RADIUS.

El acceso a la red wifi se realiza por medio de un portal cautivo montado sobre SO libre pfSense, desde donde podemos controlar y gestionar todos los usuarios y accesos que hay en la red.



Además, utilizamos una wifi unificada con puntos de acceso de la marca **Ubiquity**, que utiliza un software controlador de los puntos de acceso que se puede instalar en Windows o en GNU/Linux. Este software centraliza la gestión de los AP y genera estadísticas de uso, rendimiento y cobertura e incluso detección de puntos de acceso falsos. Los puntos de acceso se alimentan a través del cable de datos mediante Power Over Ethernet (PoE).



6. Ataques a redes wifi

Podemos hacer una clasificación como la siguiente:

Ataques usados en redes cableadas

Funcionan en la redes inalámbricas, exactamente igual que en redes cableadas:

- MITM (con ARP, con ICMP Redirection, con DHCP o DNS Spoofing, etc)
- DHCP Starvation, Rogue DHCP
- DNS Spoofing, etc

Ataques de acceso

Serían los que atacan al sistema de acceso o asociación al AP, como por ejemplo:

- Asociación falsa
- Inyección de paquetes
- Fuerza bruta
- Ingeniería inversa
- Ataque WPS

Ataques de denegación de servicio

Serían los que atentan contra el funcionamiento y la disponibilidad de la red wifi:

- Interferencias electromagnéticas (vecinos, microondas, bluetooth, teléfonos DECT, etc)
- Inhibidores
- Desasociación de cliente

Ataques a los propios clientes

Serían los que atacan a los dispositivos wifi:

- Interferencias electromagnéticas (vecinos, microondas, bluetooth, teléfonos DECT, etc)
- Desasociación de clientes
- Puntos de acceso falsos (Rogue/Fake AP, Evil Twin)

Ataques de acceso

Como se ha citado previamente, serían los que intentan romper al sistema de acceso o asociación al AP, intentado descubrir las credenciales de acceso. A continuación se cita brevemente las características más destacables de ellos:

Ataque arpreplay

- Ataque de acceso contra WEP

- Necesita asociación con el AP
- Se utiliza en combinación con airodump-ng y aircrack-ng
- Captura un paquete ARP, y lo reinyecta miles de veces para provocar que el AP genere más vectores de inicialización (IV)

Ataque de fragmentación

- Ataque de acceso contra WEP
- Obtiene el PRGA xor (hasta 1500 bytes)
- El PRGA o keystream es el XOR del texto plano y cifrado que se usa para cifrar en RC4
- Ejemplo: 0011(texto plano)+0110(texto cifrado)=0101(PRGA)
- Con el xor, se genera un paquete ARP con packetforge-ng y se reinyecta
- Requiere al menos un paquete de datos del AP
- Si funciona, es uno de los más rápidos

Ataque chopchop

- Se usa cuando no hay clientes asociados
- Su objetivo es obtener el PRGA xor, como el ataque anterior
- Se genera un paquete ARP con packetforge-ng y se reinyecta
- Algunos AP's no son vulnerables
- Mas lento que el ataque de fragmentación

Ataque WEP por diccionario

- Se descifra la clave mediante fuerza bruta
- La clave es la combinación del BSSID y de XX
- Hace falta capturar un IV al menos
- Se utiliza la herramienta wlandecrypter
- Una vez capturado el IV, el ataque se hace con :

aireplay-ng --w <diccionario> <fichero.cap>

Ataque WPA por diccionario

- Se descifra la clave mediante fuerza bruta
- Hace falta al menos un cliente conectado
- Es necesario capturar el handshake entre cliente y AP
- Muchas veces no es inmediato capturarlo, hay que estar cerca del cliente y el AP

- En Internet existen enormes ficheros de diccionario (de varias decenas o centenas de gigas) con las combinaciones de los SSID más habituales y permutaciones de contraseñas
- Una vez capturado, el ataque se hace con :

aireplay-ng -a 2 -w <diccionario> <fichero.cap>

Ingeniería inversa contra WPA

- Es un ataque contra punto de acceso vulnerables de distintos operadores
- Se descubre mediante ingeniería inversa el algoritmo de generación de claves por defecto de sus routers, que normalmente involucra la MAC (BSSID) y el nombre (SSID)
- Afecta a muchos tipos de SSID como WLAN_XXXX, JAZZTEL_XXXX, ONOXXXX, etc.

Ataque WPS

Como ya se indicó, este sistema permite configurar clientes wifi de forma sencilla para gente no iniciada, con tan solo estar cerca del punto de acceso mediante mecanismos como NFC, USB, pulsando un botón en el router o introduciendo un PIN. El uso del pin es bastante habitual, pero existen vulnerabilidades en muchos routers y puntos de acceso inalámbricos de fabricantes en los que si está habilitada esta característica y aunque la contraseña maestra WPA sea realmente compleja, es posible averiguar el PIN de WPS en unas pocas horas (son 8 dígitos separados en dos bloques de 4). Si se averigua el PIN, se puede transferir la configuración de la red al cliente a través de este protocolo. Un ejemplo es la aplicación **Reaver-WPS** o **WPS Pin Generator** (disponible para móviles)

Ataques DoS

Algunos ejemplo de ataques de denegación de servicio (DoS), ya sean intencionados o no, serían:

Interferencias electromagnéticas

Pueden ocasionar interferencia a nuestra wifi:

- bluetooth
- hornos microondas
- inhibidores de frecuencia
- AP de vecinos en nuestro mismo canal

Pueden ser intencionadas con un emisor de Wifi en el mismo canal o accidentales por AP adyacentes en nuestro canal, por ello se recomienda usar la banda 5 GHz en 802.11n o 802.11ac si lo permite nuestro AP y tarjetas (que no sean 802.11n lite, pues trabajan en 2,4 Ghz)

Desasociación de clientes

En estos ataques se fuerza continuamente a que un cliente se desasocie del AP inutilizando su conexión. El atacante se hace pasar por el AP, enviando paquetes de desasociación, por ejemplo

usando la herramienta arpreplay-ng:

```
aireplay-ng --deauth
```

Ataques a clientes

Desasociación de clientes

Además de ser un ataque DoS, la desasociación de clientes tiene más usos. Uno de ellos es forzar a que el cliente se vuelva a asociar enviando en claro el nombre del red (SSID, ESSID) en la trama de asociación que puede ser capturada por el atacante revelando el nombre de una wifi oculta.

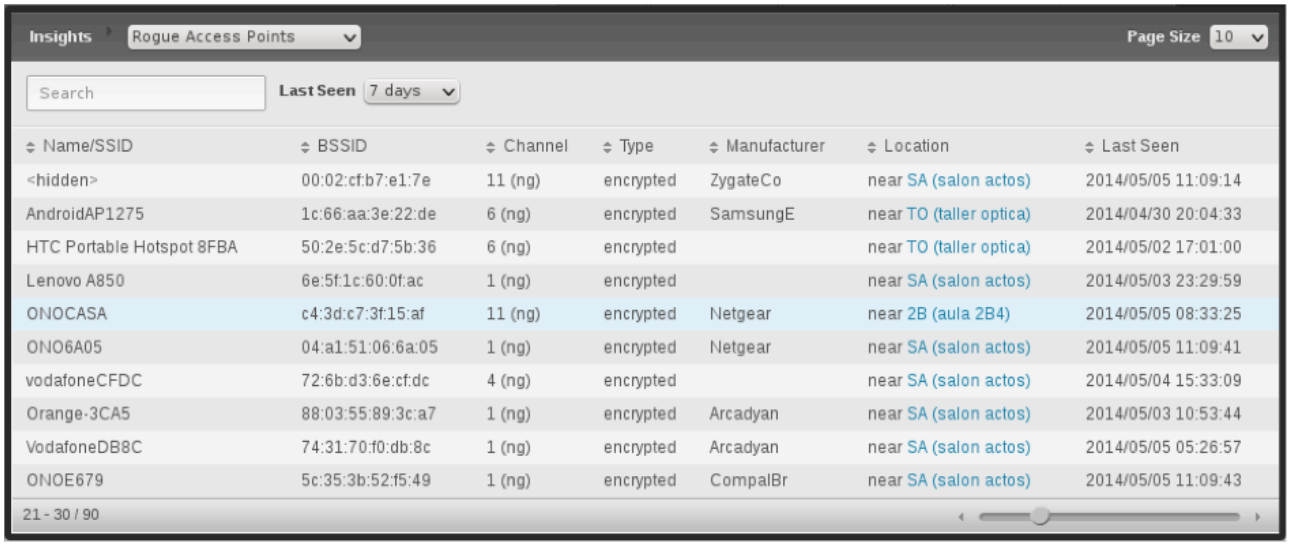
La otra funcionalidad es obligar a que el cliente realice de nuevo el handshake WPA para asociarse al AP, para de esta manera una vez capturado y guardado, realizar un ataque de diccionario o fuerza bruta. Como ya se ha citado, en Internet existen enormes ficheros a modo de tablas rainbow (no son exactamente tablas rainbow, pero les llaman así en muchos sitios) con las combinaciones de contraseñas o SSID ya con su hash precalculado para de esta forma atacar más rápido. Si además se combina con el lenguaje CUDA de las potentes GPU, el tiempo se reduce considerablemente.

Por ello es importante no solo cambiar la contraseña por defecto WPA por una con al menos 20 caracteres alfanuméricos, sino también cambiar el nombre de la red (SSID).

Puntos de acceso falsos

Tambień conocido como **Rogue AP**, **Fake AP** o **Evil Twin**, consiste en instalar un punto de acceso falso cerca del cliente al que queremos atacando, simulando una de sus redes preferidas abiertas que aparece en su PNL (Preferred Network List). De esta manera el cliente podría conectarse de forma automática y el atacante situarse en medio de sus comunicaciones pudiendo interceptar sus comunicaciones.

Muchos puntos de acceso profesionales llevan **detección de Rogue AP** funcionando como detectores de intrusos inalámbricos (WDS).



Aunque este tipo de ataque es fácil realizarlo con un AP y un portátil con las herramientas necesarias, existen a la venta dispositivos para realizar este tipo de ataques de forma muy sencilla, como por ejemplo el *Pineapple*:

7. Mecanismos de protección

Falsas medidas de seguridad

Cuando se habla de seguridad en redes inalámbricas, muchas veces se dan algunas recomendaciones que en absoluto mejoran la seguridad y producen al usuario una falsa sensación de protección ante acceso no autorizados. Conviene pues, conocerlas para que no perdamos el tiempo en aplicarlas. Estas falsas medidas son:

- **Utilizar WEP** como sistema de cifrado: WEP es el primer sistema que se implantó para dotar de protección a las redes wifi y actualmente es posible romper cualquier red wifi protegida con WEP en cuestión de pocos minutos, con técnicas como la inyección de paquetes, el modo monitor para capturar tramas y una herramienta de criptoanálisis como **aircrack-ng** o **wepcrack**. Todas estas herramientas se encuentran disponibles en Internet e incluso hay asistentes en algunas distribuciones de auditoría que permiten hacer el proceso sin ser experto. WEP utiliza un algoritmo de cifrado llamado RC4 cuya implementación para redes wifi está rota desde hace muchos años. Por tanto, no se recomienda su uso.
- **Usar filtrado de MAC** en el AP: muchos puntos de acceso y routers inalámbricos tienen la opción de sólo permitir el acceso a la red wifi a determinados dispositivos usando la dirección física MAC de su tarjeta de red. Es muy fácil ver las direcciones MAC asociadas a un punto de acceso con software de monitorización como **airodump-ng** y cambiar la MAC de la tarjeta wifi del atacante desde cualquier sistema operativo. Por tanto, no se recomienda usar esta técnica porque es muy fácil saltársela con pocos conocimientos de redes.
- **Deshabilitar el anuncio de la red**, también como conocido como difusión o broadcast del **SSID** (Service Set Identifier): todos los puntos de acceso por defecto envían tramas "beacon" con el nombre de la wifi cada 100 milisegundos. De esta forma podemos ver las redes a nuestro alrededor. Si deshabilitamos esta función en el router, nadie puede ver el nombre de nuestra red y conectarse. Pero de nuevo, con herramientas como **airodump-ng** pueden verse

las MAC asociadas a un AP dado (aparece su BSSID, que es la MAC del AP) y el nombre de la red aparece como **<hidden>** (oculto). Después, es fácil lanzar un ataque de **desautenticación** contra el cliente asociado haciéndose pasar por el AP, con lo que se fuerza a que el cliente vuelva a asociarse automáticamente y en este momento, el cliente envía el nombre de la wifi (SSID) en la trama de conexión, que es capturada por el atacante. Este proceso se hace en cuestión de pocos segundos.

Recomendaciones para Wi-Fi

A continuación, se citan las recomendaciones más destacables en materia de redes inalámbricas:

- **WPA PSK**: En caso de no querer aventurarse en montar un RADIUS en el centro con gestión centralizada de usuarios en LDAP, Samba, Active Directory, etc. se recomienda usar WPA2 con AES en la medida de lo posible y una clave compleja. Los expertos en seguridad han revelado que una clave PSK de 20 caracteres alfanuméricos se podría romper por fuerza bruta usando toda la capacidad de cómputo del planeta en una media de unos 100 años. Las vulnerabilidades de WPA vienen por usar contraseñas débiles, por no cambiar la contraseña ni el nombre de la wifi por defecto o por tener activo WPS. En cualquier caso, no recomiendo WPA PSK en un centro con cientos de usuarios porque al final, esa contraseña es conocida por todos, incluso por gente ajena al centro, por tanto es como no tener contraseña. Si hay algún ataque, no es posible identificar al usuario porque es la misma contraseña para todos.
- **WPA Enterprise**: Ya se han comentado las ventajas de este sistema. El problema es la curva de aprendizaje necesaria para gente no experimentada y que es más complejo de administrar un RADIUS o un LDAP/Active Directory.
- **No conectarse a redes abiertas** bajo ningún concepto ni montar soluciones como portales cautivos abiertos. En las redes wifi abiertas puede conectarse cualquiera que disponga de las herramientas necesarias para hacer ataques MITM (las hay incluso apps para móviles como dSploit, zAnti, Wifikill, etc). Los portales cautivos como los de los hoteles, aeropuertos, cafeterías, etc. que muestran una página web de identificación una vez nos conectamos (portal cautivo) son extremadamente fáciles de saltar con los conocimientos adecuados, a no ser que protejan con algún sistema como claves WPA. Por tanto, no se recomienda la instalación de un portal cautivo abierto con autenticación web pues es fácil atacar el sistema y a los usuarios, así como evitar la autenticación.
- **Eliminar las redes abiertas de la lista de redes preferidas**, de esta forma, al borrarlas de la lista de nuestro dispositivo, un atacante cerca de nosotros no puede averiguar las redes abiertas a las que nos hemos conectado y crear una red que se llame igual. A esta técnica se le conoce como Rogue AP o Evil Twin. De esta forma nuestro dispositivo se conectaría automáticamente y el atacante podría espiar nuestras comunicaciones.
- **Deshabilitar WPS**, por las razones expuestas anteriormente. Existen herramientas como **reaver**, que permite atacar este protocolo.
- **Cambiar contraseñas** WPA y nombre de la red **por defecto.**

Mecanismos de protección adicionales (modo paranoico)

A continuación se citan algunas medidas que pueden ser recomendables, si bien se pierde algo de funcionalidad en muchas ocasiones al activarlas:

- Deshabilitar DHCP en el router o punto de acceso wifi
- Limitar número de clientes asociados
- Modificar la potencia y direccionalidad de la señal (cambiar antena o usar antena windsurfer)
- Aislar comunicación entre clientes
- Instalar un firewall en el perímetro entre red cableada e inalámbrica
- Utilizar entradas ARP estáticas