Trabajo Final de Carrera

Estudio sobre los riesgos y amenazas existentes en las redes sin hilos

Gerardo Cortés Suárez
Ingeniería Técnica de Telecomunicaciones:
Especialidad en Telemática
Universitat Oberta de Cataluña

RESUMEN

La popularización del uso de las redes inalámbricas se debe a diversos motivos: flexibilidad, ahorro de costes, escalabilidad, y una simple y fácil instalación. Desafortunadamente, esta tecnología cuenta con un gran inconveniente: la seguridad. Si una red inalámbrica no está debidamente protegida, podría ser insegura y, por lo tanto, vulnerable: cualquier usuario no autorizado con conocimientos básicos de informática podría acceder a ella.

Debido a los riesgos y amenazas a los cuales las redes inalámbricas están expuestos en la actualidad, este trabajo intentará demostrar que para la instalación de cualquier red inalámbrica, incluso para la más simple, diversas medidas de seguridad se deben tener en cuenta para su éxito.

Por ejemplo, si un usuario no autorizado realiza un ataque a la red inalámbrica, podría acceder a la red y será capaz de utilizar la información disponible en ella. El fracaso o éxito de estos ataques dependerán del nivel de seguridad configurado en la red. Mediante un caso práctico, se demostrará lo fácil que puede ser obtener la contraseña de una red WI-FI en el caso que no disponga de un nivel de seguridad adecuado. Para ello, se indicarán una serie de consejos y políticas de seguridad para minimizar los riesgos. Además, se expondrán diversas soluciones de seguridad existentes en el mercado.

A modo de conclusión, el objetivo principal del presente trabajo es mostrar que estas medidas mencionadas anteriormente deberían tenerse en cuenta por cualquier administrador al instalar una nueva red inalámbrica en una empresa para evitar posibles riesgos o amenazas.

****

ABSTRACT

The growing popularity of wireless networks is due to several reasons: flexibility, cost-saving, scalability and a simple and quick installation. Unfortunately, this technology also involves a big disadvantage: security. If a wireless network is not properly protected, it could be unsecure and therefore vulnerable: any non-authorised user with a basic IT knowledge could have access to it.

Given the risks and threats to which wireless networks are exposed nowadays, this work will try to demonstrate that for installation of any wireless network, even for a very simple one, several security measures have to be taken into account to succeed.

For example, if a non-authorised user carries out attacks to Wi-Fi networks, he could access the net and be able to use any information available in it. Failure or success from this attacks will depend on the security level set in the net. Using a practical case, it will be shown how easy it can be to decode a Wi-Fi password in case the network is not correctly protected. To do so, some advice and security policies will be exposed in order to minimize risks. Moreover, several existing security measures available in the market will be pointed out.

To conclude the main objective of the present paper is to show that these measures mentioned above should be taken into account by any administrator when installing a new wireless network in a company to avoid possible risks or threats.

Índice de contenidos

Índice de Ilustraciones

Índice de Tablas

1. Introducción al proyecto

1.1 Motivación

El crecimiento de las redes inalámbricas en diferentes ámbitos es hoy día una realidad que ofrece un gran abanico de posibilidades. En la actualidad, ha aumentado significativamente el número de empresas e instituciones que cuentan con la implantación de este tipo de tecnologías, viendo en ellas una gran ventaja para ofrecer algún tipo de servicio a sus usuarios. Aunque debido a su naturaleza, este tipo de tecnologías son más inseguras, con lo que hay que adoptar una serie de medidas de seguridad para evitar posibles riesgos y amenazas.

A nivel personal, la motivación principal por la realización de este Trabajo Final de Carrera (TFC) es la necesidad de profundizar y consolidar los conocimientos adquiridos durante los estudios de la Ingeniería Técnica en Telecomunicaciones, especialidad en Telemática de la Universidad Oberta de Catalunya.

Por otro lado, como profesional del mundo de las telecomunicaciones, considero que este proyecto me servirá para ampliar y profundizar en conceptos y aspectos relevantes en la seguridad de las redes inalámbricas.

1.2 Descripción

El presente Trabajo final de carrera se pretende analizar los riesgos y amenazas a las que están expuestas las redes inalámbricas, más concretamente las redes Wi-Fi.

El segundo capítulo pretende ser una introducción a las redes inalámbricas actuales: historia y tipos de redes inalámbricas, clasificándolas en consideración a diferentes aspectos.

El tercer capítulo estará centrado en las redes Wi-Fi. Para ello, se analizan los diferentes estándares, topologías, los canales y frecuencias que utilizan. Para finalizar este capítulo se mencionarán las ventajas y las desventajas del uso de esta tecnología.

En el cuarto capítulo, se realiza una descripción del proceso de asociación de un dispositivo a un Punto de Acceso en una red inalámbrica. Posteriormente, se analizan los tres protocolos de seguridad: WEP, WPA, WPA2. A continuación, se describe la tecnología WPS, indicando sus ventajas y vulnerabilidades. Finalizará el capítulo analizando el proceso de autenticación 802.1x y EAP.

En el quinto capítulo, se analizan los diferentes ataques más comunes que se pueden realizar a las redes inalámbricas, resumiendo cada uno de ellos. Finalizará resumiendo los aspectos que se deben tener en cuenta para poder evitarlos, o bien disminuir el impacto que tienen.

En el sexto capítulo se realizará un caso práctico donde se analizaran los diferentes ejemplos de ataques que pueden ser realizados en una red inalámbrica con los protocolos de seguridad WEP, WPA2/PSK y la tecnología WPS habilitados.

En el séptimo capítulo se resumirán las políticas de seguridad, que se deberán tener en cuenta a la hora de implementar una red Wi-Fi de forma segura.

Finalmente, en el octavo capítulo se citan diferentes soluciones de seguridad que pueden ser implementadas en redes inalámbricas empresariales, resumiendo cada una de ellas.

1.3 Objetivos

Para cumplir con el objetivo marcado en el inicio del TFC se pretende dar respuesta a los siguientes puntos:

1. Conocer las ventajas y desventajas de las redes Wi-Fi.
2. Analizar los mecanismos que ofrecen seguridad a redes WI-FI.
3. Identificar y analizar riesgos y amenazas de las redes inalámbricas.
4. Identificar las soluciones de seguridad existentes en el mercado para las redes inalámbricas.
5. Describir políticas y medidas de seguridad en redes inalámbricas.

1.4 Planificación

La elaboración de la planificación viene marcada por una serie de entregables que se deben realizar durante el transcurso del proyecto. A continuación, se exponen en una tabla las tareas junto con la fecha límite de entrega de cada una de ellas:

Tarea	Fecha límite
Decisión del proyecto y comunicación al consultor	23/09/2015
PEC 1: Entrega de la planificación del trabajo	30/09/2015
PEC 2: Primera entrega del proyecto	18/11/2015
PEC 3: Segunda entrega del proyecto	16/12/2015
Entrega de la memoria final	10/01/2016
Entrega de la presentación	17/01/2016
Inicio del tribunal	18/01/2016
Final del tribunal	22/01/2016

Tabla 1 Tareas y fechas límite

Seguidamente, mediante un diagrama de Gantt, realizado mediante Microsoft Project 2013, podemos observar el tiempo de dedicación aproximado de las diferentes tareas a lo largo del periodo total de duración del proyecto, indicándonos también las relaciones existentes entre tareas:

Nombre de tarea	Duración	Comienzo	Fin
TFC - Estudio sobre los riesgos y amenazas existentes en las redes sin hilos	**93 días**	**mié 16/09/15**	**vie 22/01/16**
Decision del proyecto y comunicación al consultor	4 días	mié 16/09/15	dom 20/09/15
PEC 1: Planificación del trabajo	**6 días**	**mié 23/09/15**	**mié 30/09/15**
Recopilación bibliografía	2 días?	mié 23/09/15	jue 24/09/15
Elaboración del plan de trabajo	3 días?	vie 25/09/15	mar 29/09/15
Entrega PEC 1	0 días	mié 30/09/15	mié 30/09/15
PEC 2: Primera entrega del trabajo	**35 días**	**jue 01/10/15**	**mié 18/11/15**
Recopilación información tencologia inalambrica	3 días?	jue 01/10/15	lun 05/10/15
Recopilación información sobre estandares IEEE 802.11	2 días?	mar 06/10/15	mié 07/10/15
Elaboración de la memoria	20 días?	jue 08/10/15	mié 04/11/15
Instalación/configuración laboratorio para casos prácticos	8 días?	jue 05/11/15	dom 15/11/15
Revisión documentación	2 días?	lun 16/11/15	mar 17/11/15
Entrega PEC 2	0 días	mié 18/11/15	mié 18/11/15
PEC 3: Segunda entrega del trabajo	**20 días**	**jue 19/11/15**	**mié 16/12/15**
Recopilación información sobre ataques Redes Wi-Fi	3 días?	jue 19/11/15	lun 23/11/15
Realización casos prácticos	6 días?	mar 24/11/15	mar 01/12/15
Elaboración de la memoria	7 días?	mié 02/12/15	jue 10/12/15
Revisión documentación	2 días?	lun 14/12/15	mar 15/12/15
Entrega PEC 3	0 días	mié 16/12/15	mié 16/12/15
Finalización TFC	**27 días**	**jue 17/12/15**	**vie 22/01/16**
Finalización de la memoria	18 días?	jue 17/12/15	sáb 09/01/16
Entrega de la memoria final	0 días	dom 10/01/16	dom 10/01/16
Elaboración de la presentaciónn	6 días?	lun 11/01/16	sáb 16/01/16
Entrega de la presentación	0 días	dom 17/01/16	dom 17/01/16
Tribunal	5 días	lun 18/01/16	vie 22/01/16

Ilustración 1 Descomposición de tareas

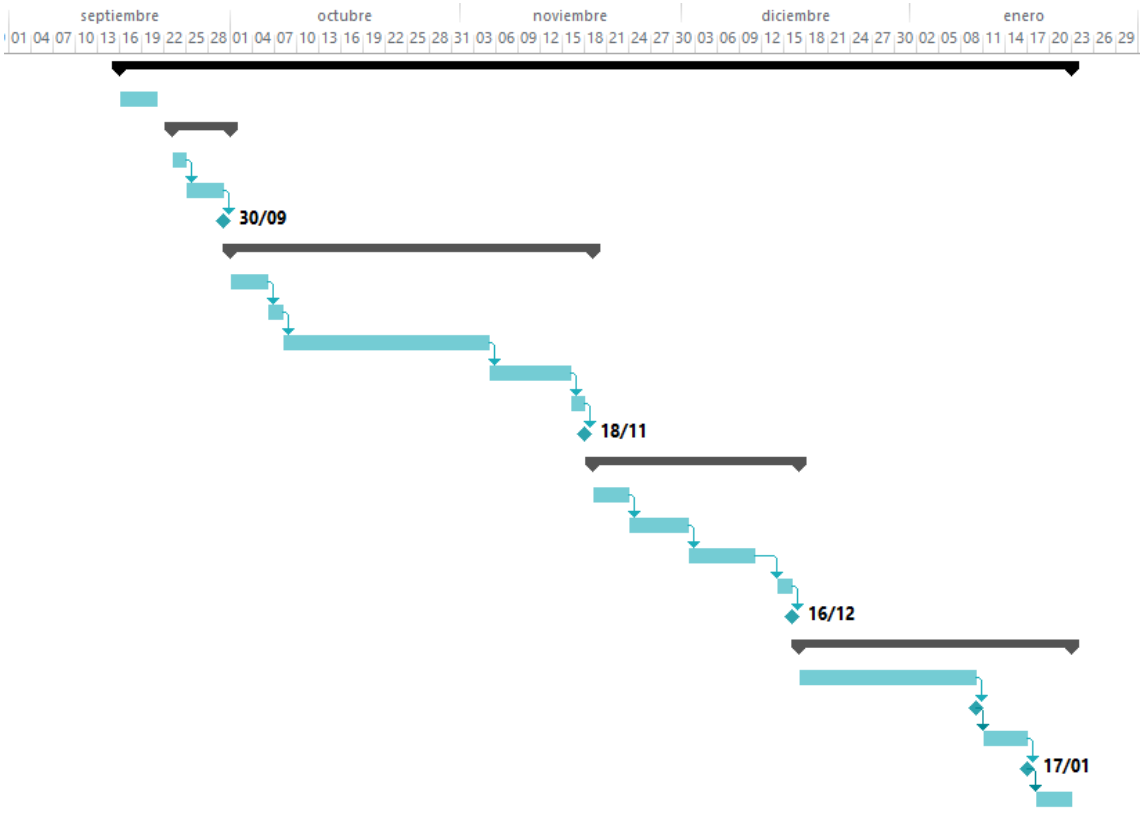


Ilustración 2 Diagrama de Gantt

2. Tecnología inalámbrica

2.1 Introducción

Una red inalámbrica es aquella en la que se permiten conectar distintos dispositivos sin la necesidad de utilizar una conexión física, sino que estableciendo las comunicaciones a través de ondas electromagnéticas en las cuales viaja la información. Proporcionando mayor movilidad a los usuarios y un ahorro notable de costes en su implantación debido a que no requiere instalación de cableado.

En los últimos años se ha verificado un elevado crecimiento de las redes inalámbricas. Esto ha sido debido a diversas razones: la necesidad de mantener conectividad a Internet de forma constante, la movilidad de los usuarios, mayor flexibilidad, etc. Con ello, han ido apareciendo en el mercado nuevas y diferentes tecnologías inalámbricas, como pueden ser: Wi-Fi, WIMAX, Bluetooth, GSM, GPRS, infrarrojos… que permiten conectar distintos dispositivos sin necesidad de utilizar cableado.

De todas las redes inalámbricas existentes, las que han tenido un mayor crecimiento a lo largo de su historia han sido las redes móviles, han pasado de ofrecer únicamente servicios de voz a ofrecer servicios de voz y datos conjuntamente. Uno de los factores que han posibilitado su crecimiento ha sido la aparición de teléfonos inteligentes o smartphone y la necesidad de los usuarios por tener una conexión permanente a Internet en cualquier lugar.

La primera tecnología en aparecer permitía el acceso a internet a los dispositivos fue la GSM, caracterizada por permitir transferencia de voz y datos, aunque esta última de forma muy reducida. Posteriormente, han ido apareciendo otras tecnologías: GPRS, UMTS, HSDPA/HSUPA y LTE. Todas ellas han incorporado mejoras significativas como puede ser la velocidad de transmisión y el acceso a internet. Actualmente, ha aparecido la tecnología LTE, también conocida como 4G, orientada totalmente al protocolo IP, con una tasa de transferencia de 100 Mbps en movimiento y 1 Gbps en reposo. Ya se están realizando estudios y pruebas para el desarrollo de la tecnología 5G, que tiene previsto su lanzamiento para el 2020.

La principal diferencia entre las redes móviles y el resto de redes inalámbricas existentes es su alcance. Mientras que las tecnologías Wi-Fi, WIMAX, Bluetooth, infrarrojos tiene un alcance limitado, las redes móviles pueden llegar a cubrir un 95% de la población.

Dada la diversidad de tecnologías existentes en la actualidad existe un gran problema: la interoperabilidad entre redes inalámbricas distintas. Es decir, permitir que diferentes tecnologías puedan intercambiar información, sin problemas de compatibilidad. Por ello, el IEEE creó un grupo de trabajo, encargado de estandarizar los traspasos entre redes inalámbricas de diferentes tecnologías.

2.2 Historia

Para hablar de la historia de la historia de las redes inalámbricas hay que remontarse al 1880, donde Graham Bell y Summer Tainter inventaron el primer aparato de comunicación sin cables, el fotófono, que permitía la transmisión del sonido por medio de una emisión de luz.

En 1888 el físico alemán Rudolf Hertz realizó la primera transmisión sin cables con odas electromagnéticas mediante un oscilador que utilizado como emisor y un resonador que hacía como receptor. Seis años después, las ondas de radio ya eran un medio de comunicación. En 1899 Guillermo Marconi consiguió establecer las comunicaciones inalámbricas a través del canal de la Mancha, entre Dover y Wilmereux. En 1907, se transmitían los primeros mensajes completos a través del atlántico. Durante la Segunda Guerra Mundial se produjeron importantes avances en este campo.

No fue hasta el 1971 cuando un grupo de investigadores bajo la dirección de Norman Abramson crearon la primera red de área local inalámbrica, mediante una red de comunicación por radio, dicha red se llamó ALOHA. Estaba formada por 7 computadoras situadas en distintas islas que se podían comunicar con un ordenador central al cual pedían realizar diferentes cálculos. Uno de los primeros problemas con lo que se encontraron fue el control de acceso al medio (MAC), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí. Este problema fue solucionado haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras mientras estuviera libre, de tal forma cuando una de las otras estaciones se disponía a transmitir antes “escuchaba” y aseguraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, este método es conocido como CSMA (Carrier Sense Multiple Access).

Un año después ALOHA se conectó mediante ARPANET al continente americano. ARPANET es una red de computadoras creada por el Departamento de Defensa de los Estados Unidos como medio de comunicación para los diferentes organismos del país.

A finales de 1980, el Grupo de Trabajo 802 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) comenzó a trabajar en la estandarización de las redes inalámbricas que utilizaran las bandas ISM de 2.4 GHz y 5.7 GHz. Mientras tanto, las compañías comenzaron el embarque propietario de tarjetas de radio para redes inalámbricas y los puntos de acceso con operación en el 902 MHz de la banda ISM.

El Grupo de Trabajo del IEEE 802.11 desarrolló la especificación para el Control de Acceso al Medio (MAC) y la capa Física (PHY) en las redes inalámbricas. El consejo de estándares del IEEE aprobó el estándar el 26 de Junio de 1997, el cual fue publicado por el IEEE el 18 de Noviembre de 1997.

En Diciembre de 1999, el IEEE liberó los suplementos (802.11a y 802.11b) para el estándar IEEE 802.11, en orden para incrementar la velocidad de la capa Física (hasta 11 Mbps en el 2.4 GHz de la banda ISM y hasta 54 Mbps en el 5.7 GHz de la banda ISM).

2.3 Tipos de redes inalámbricas

Las redes inalámbricas existentes pueden ser clasificadas en consideración a diferentes parámetros: su cobertura o ámbito y el tipo de onda electromagnética utilizada.

De acuerdo al tipo de cobertura, se pueden clasificar en:

- **WPAN (Wireless Personal Area Networks**): Redes personales caracterizadas por tener un área de cobertura limitada, abarcan un área de algunas decenas de metros como máximo. La tecnología principal de este tipo de redes es el Bluetooth, aunque también existen de otras como pueden ser el HomeRF, Zigbee y las conexiones infrarrojos.
- **WLAN (Wireless Local Area Network)**: Redes locales que aparecen como alternativa a las redes LAN cableadas. Tienen un alcance desde los 10 hasta los 300 metros, permitiendo que los dispositivos que se encuentran en el área de cobertura puedan conectarse entre sí. Las tecnologías relacionadas con este tipo de redes son las Wi-Fi, que serán tratadas con mayor detalle en los próximos capítulos.
- **WMAN (Wireless Metropolitan Area Network):** Redes de área metropolitana con un alcance de 4 a 10 kilómetros y ofrecen una velocidad total efectiva de 1 a 10 Mbps. Dentro de este tipo de redes podemos encontrar las tecnologías WiMAX, protocolo parecido a Wi-Fi, pero con mayor cobertura y ancho de banda. También es posible encontrar otros sistemas de comunicación como LMDS.
- **WWAN (Wireless Wide Area Network):** Redes que poseen el alcance más amplio de todas las redes inalámbricas indicadas anteriormente. Debido a este motivo, todos los teléfonos móviles están conectados a una red de este tipo. Por lo tanto, las tecnologías utilizadas en este tipo de redes son el GSM, GPRS y UMTS.

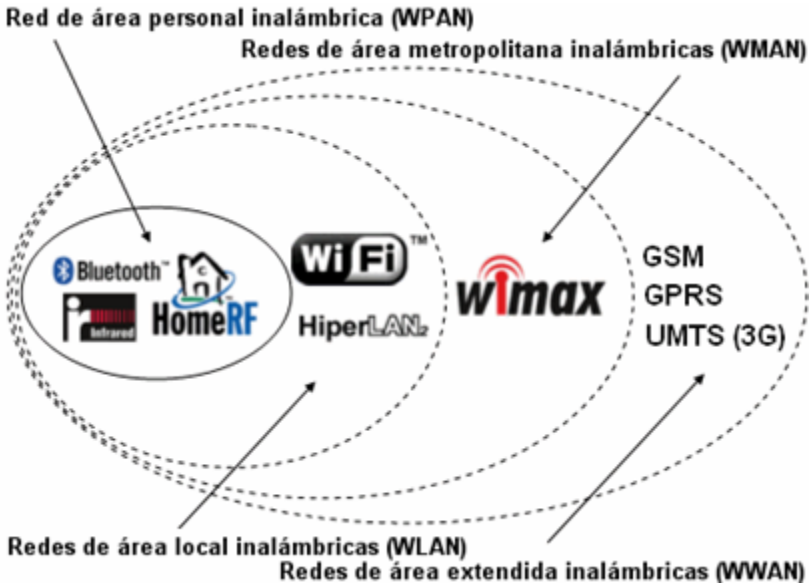


Ilustración 3 Clasificación de redes inalámbricas según su cobertura

De acuerdo al tipo de onda electromagnética utilizada, la clasificación es:

- **Ondas de radio:** Este tipo de ondas son omnidireccionales, se propagan en todas las direcciones o sentidos. En este rango se encuentran las bandas desde la ELF, comprendida entre los 3 y los 30 Hz, hasta la UHF, comprendida entre los 300 a los 3000 Hz. Al operar con frecuencias bajas, la transmisión no es sensible a las atenuaciones producidas por la lluvia.
- **Microondas terrestres:** Comprenden frecuencias en el rango de 1 GHz hasta los 300 GHz. Son utilizadas en antenas parabólicas en enlaces punto a punto. Tienen una cobertura de kilómetros, con el inconveniente de que el emisor y receptor deben estar perfectamente alineados. Al operar con frecuencias más elevadas, la atenuación producida por la lluvia si les puede llegar a afectar.
- **Microondas por satélite:** Consiste en realizar enlaces entre estaciones terrestres, también denominadas estaciones base. El satélite recibe la señal enviada por estas estaciones, la amplifica, la corrige y la retransmite a una o más antenas ubicadas en la tierra.
- **Infrarrojos:** Su rango de frecuencia va desde los 300 GHz hasta los 348 THz. Transmisor y receptor deben estar alineados correctamente. Tiene el inconveniente que no atraviesan obstáculos.

3. Tecnología Wi-Fi

En este capítulo, para entrar en contexto, se iniciará realizando una introducción a las redes Wi-Fi. A continuación, se hablará sobre la especificación IEEE 802.11, dirigidas a este tipo de redes inalámbricas. Para ello, se resumirán los principales protocolos más conocidos en la actualidad: 802.11, 802.11a, 802.11b, 802.11g, 802.11n y el 802.11ac.

También se analizarán los modos en los que pueden trabajar las redes Wi-fi, que son tres: modo infraestructura, modo Ad-Hoc y redes Mesh. Para finalizar, se hablará sobre los canales y frecuencias utilizados para que los dispositivos puedan operar.

3.1 Introducción a las redes Wi-Fi

Wi-Fi es una de las tecnologías de comunicación inalámbrica más utilizada en la actualidad, también conocida como WLAN (Wireless LAN). Es una marca de la Wi-Fi Alliance, organización comercial encargada de probar y certificar que los dispositivos cumplan las normas 802.11, relacionados a redes inalámbricas de área local.

Ilustración 4 Logotipo Wi-Fi

La norma IEEE 802.11 fue diseñada para sustituir el equivalente a las capas físicas y MAC de la norma 802.3 (Ethernet). Asimismo, en la forma en cómo se transmiten las tramas o paquetes de datos es en lo único que se diferencia con una red Ethernet. Por lo tanto, una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3.

Hoy en día podemos encontrarnos con diferentes tipos de comunicación WI-Fi, basados cada uno de ellos en el estándar llamado IEEE 802.11, entre ellas destacan: 802.11b, que emite a 11 Mb/seg, 802.11g que lo hace a 54 Mb/seg y 802.11n pudiendo llegar a los 600 Mb/seg, aunque también existen de otras.

Debido a los diferentes problemas de seguridad que existen en las redes Wi-Fi es recomendable la encriptación de la transmisión para emitir en un entorno seguro. Esto es posible gracias al protocolo de seguridad WPA2, se trata de una mejoría del WPA y es mucho más seguro que su predecesor WEP.

3.2 Familia de estándares IEEE 802.11

El Instituto de Ingeniería Eléctrica y Electrónica – abreviado como IEEE - es la mayor organización internacional sin fines de lucro, líder en el campo de la promoción de estándares internacionales, particularmente en el campo de las telecomunicaciones, la tecnología de

información y la generación de energía. Está formada por profesionales de las nuevas tecnologías y tiene un total de 425.000 miembros y voluntarios en 160 países.

Algunos de los productos del IEEE más conocidos son el grupo de estándares para las redes LAN/MAN IEEE 802, que incluye el de Ethernet (IEEE 802.3) y el de redes inalámbricas (IEEE 802.11), aunque existen de muchos otros.

La especificación IEEE 802.11 corresponde a un estándar internacional que define las características de una red WLAN. Concretamente define los estándares que se sitúan en los niveles inferiores de la pila OSI, más concretamente en la capa física y en el subnivel MAC de la capa de enlace de datos.

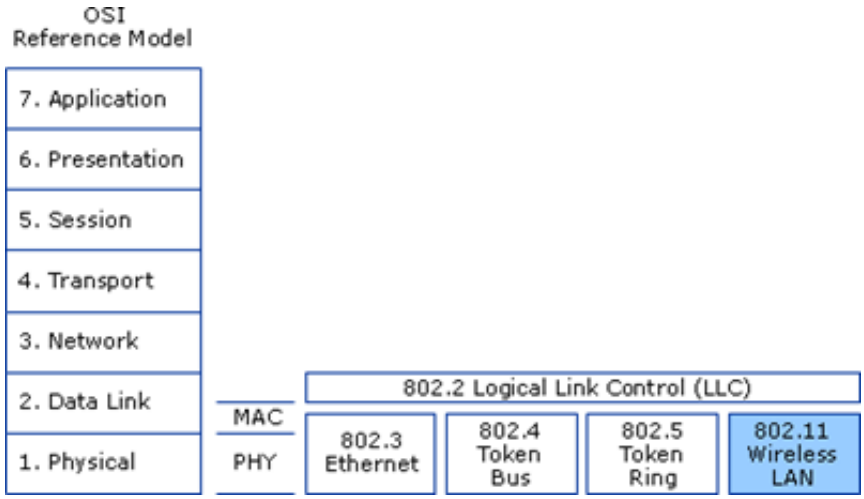


Ilustración 5 El Modelo OSI y el protocolo 802.11

Aunque existen una gran variedad de estándares que componen la familia 802.11 en este punto hablaremos sobre los que han tenido mayor relevancia a lo largo de la historia:

802.11 Legacy

Versión original del estándar IEEE 802.11 publicada en 1997. Especifica dos velocidades de transmisión de 1 y 2 Mbit/s que se transmiten mediante señales infrarrojas en la banda ISM a 2,4 GHz.

También define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, convirtiéndose en dificultades de interoperabilidad entre equipos de diferentes marcas.

En la actualidad este estándar está en desuso y fue sustituido rápidamente por el estándar 802.11b.

802.11a

La revisión 802.11a fue certificada en 1999. Utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de UNII a 5 GHz, utilizando la modulación OFDM (Multiplexación por división de frecuencias ortogonales) con 52 subportadoras, una técnica de modulación que permite una tasa de transmisión máxima de 54 Mbit/s. También utiliza la selección adaptativa de velocidad, es decir, la tasa de datos se reduce a 48, 36, 24, 18, 12, 9 y 6 Mbit/s a medida que se experimentan dificultades en la recepción.

Por último, la utilización de la banda de 5GHz cuenta con la ventaja de recibir menos interferencias. En cambio, también cuenta con la desventaja que introduce mayor atenuación en la transmisión, no pudiendo atravesar obstáculos, por lo que tiene un menor alcance a la de 2,4 GHz.

802.11b

La revisión 802.11b fue aprobada en 1999. Este estándar corrige las debilidades del estándar 802.11 legacy. Utiliza el mismo método de acceso y la misma técnica DDSS definida en el estándar 802.11.

Utiliza la banda de frecuencias de 2,4 GHz y una velocidad máxima de transmisión de 11 Mbit/s. También utiliza el mismo método de acceso definido en el estándar original CSMA/CA, reduciendo, en la práctica, la velocidad máxima de transmisión a 5,9 Mbit/s sobre TCP y 7,1 Mbit/s sobre UDP.

También soporta cambios dinámicos, para poder ajustarse automáticamente a ciertas condiciones. Por lo tanto, los dispositivos WLAN que utilizan este estándar ajustarán automáticamente sus velocidades de acuerdo a las condiciones de ruido.

Los productos que utilizan este estándar aparecieron rápidamente en el mercado debido a que es una extensión directa de la modulación DSSS, definida en el estándar original. Por tanto, los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b.

Finalmente, cabe destacar que los productos que utilizan el estándar 802.11b no son compatibles con los productos del estándar 802.11a por operar en distintas bandas de frecuencia.

802.11g

La revisión del estándar 802.11g fue aprobada en 2003. Utiliza la banda de 2,4 GHz y opera a una velocidad teórica máxima de 54 Mbit/s, cerca de 24,7 Mbit/s de velocidad real de transferencia, equivalente a la del estándar 802.11a. Es compatible con el estándar 802.11b y funciona en las mismas frecuencias.

Los equipos que trabajan bajo este estándar llegaron al mercado muy rápidamente, gracias a su interoperabilidad con el estándar 802.11b. En cambio, sufren de las mismas interferencias que el modelo 802.11b, la banda de 2.4 GHz está ya saturada, debido a la utilización de otros dispositivos que la utilizan.

802.11n

El estándar 802.11n fue certificado en 2009. Cuyo principal objetivo fue mejorar el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, incrementando la velocidad máxima de transferencia de 54 Mbit/s a un máximo de 600 Mbit/s. Hace uso simultáneo de las bandas 2,4 GHz y 5 GHz, pudiéndose comunicar con todos los anteriores estándares descritos sin problemas de incompatibilidad, tanto en la banda de 2,4 GHz como en la de 5 GHz.

La principal evolución que introdujo este estándar fue el empleo de la tecnología MIMO, que mejora la cobertura y velocidad de la señal inalámbrica, compaginando el envío y recepción de ésta debido al uso de varias antenas, permitiendo entre otras cosas trabajar con varios flujos de datos y aprovechando las reflexiones (rebotes que se producen cuando la señal llega a un obstáculo), fenómeno que en los estándares 80.2.11a/b/g serían percibidos como interferencias.

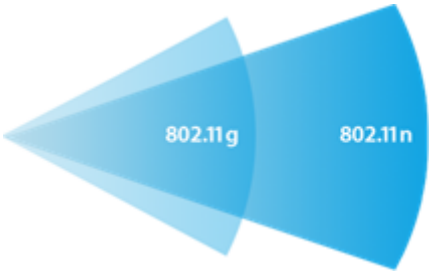


Ilustración 6 Cobertura y alcance de 802.11n respecto al estándar 802.11g

Aunque este estándar puede trabajar en la banda de los 2,4 GHz y de los 5 GHz se aconseja trabajar siempre que sea posible en la segunda, la de los 5 Ghz, ya que se consigue un mejor rendimiento al encontrarse mucho menos congestionada.

802.11ac

El estándar 802.11ac es una mejora del 802.11n y fue aprobado en 2014. Consiste en mejorar las tasas de transferencia hasta 1 Gbit/s dentro de la banda de 5GHz, utilizando hasta 8 flujos MIMO.

A continuación, se incluye una tabla resumen de los estándares más importantes:

Estándar	Año	Descripción
802.11	1997	Estándar WLAN original. Soporta 1 a 2 Mps
802.11a	1999	Estándar de alta velocidad de la banda de los 5 GHz. Soporta hasta 54 Mps
802.11b	1999	Estándar para la banda de los 2,4 GHz. Soporta 11 Mps
802.11e	2005	Estándar que añade requerimientos de QoS
802.11f	2000	Permite interoperabilidad entre operadores y fabricantes de redes WLAN
802.11g	2003	Establece una técnica de modulación adicional para la banda de los 2,4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.

Estándar	Año	Descripción
802.11h	2003	Tiene por objeto unir el estándar 802.11 con el estándar europeo
802.11i	2004	Destinado a mejorar la seguridad en la transferencia de datos
802.11j	2002	Es equivalente al 802.11h, en la regulación de Japón
802.11k	2003	Permite a los conmutadores y puntos de acceso inalámbricos calcular y valorar los recursos de radiofrecuencia de los clientes de una red WLAN
802.11n	2009	Estándar que utiliza la tecnología MIMO. Trabaja en la banda de 2,4 GHz y 5 GHz. Soporta hasta 600 Mps.
802.11ac	2014	Estándar para la banda de 5 GHz. Soporta hasta 1,93 Gbps

Tabla 2 Resumen estándares 802.11

3.3 Modos de funcionamiento

Los componentes básicos de una red inalámbrica WI-FI son:

- **Puntos de Acceso (AP):** Son dispositivos que actúan en la capa 2 del modelo OSI, enlace de datos. Funcionan como transmisores centrales y receptores de señales de radio en una red WI-FI, permitiendo el acceso a la red de las estaciones cercanas a ellos. Asimismo, actúan como enlace entre la red WI-FI y la cableada.
- **Adaptadores WLAN:** Son tarjetas de red que cumplen con el estándar 802.11 y permite a un equipo de usuario conectarse a una red WI-FI. Están disponibles en diferentes formatos, como tarjetas PCI, tarjetas PCMCIA, adaptadores USB y tarjetas Compact flash.
- **Estaciones o equipo terminal:** Cualquier dispositivo en el que se conecta un adaptador WLAN.

El estándar 802.11 define dos modos operativos:

- El **modo de infraestructura** en el que los clientes se conectan a un punto de acceso para comunicarse.
- El **modo Ad-Hoc** en el que los clientes se conectan entre sí sin ningún punto de acceso.

3.3.1 Modo de infraestructura

En el modo infraestructura existe un elemento central, el punto de acceso, conectado a la parte cableada de la red y permitiendo a los clientes conectarse a través de él. También es el encargado de controlar los accesos de los diferentes dispositivos en el área de cobertura y dirigir la información hacia y desde la red cableada. A la configuración formada por el punto de acceso y las estaciones ubicadas en el área de cobertura se le conoce como conjunto de servicio básico o BSS y forman una célula. Cada BSS es identificado a través de un identificador de 6 bytes, llamado BSSID, que corresponde con la dirección MAC del punto de acceso.

Cuando un punto de acceso es insuficiente para proporcionar cobertura total para que todos los dispositivos se conecten a él existe la posibilidad de unir dos o más puntos de acceso a través de un sistema de distribución (DS) común para formar un conjunto de servicio extendido o ESS. Un ESS se identifica mediante un ESSID, también abreviado como SSID, que es un identificador con un máximo de 32 caracteres en formato ASCII, que se corresponde con el nombre de la red y representa una medida de seguridad, aunque no la única, ya que un cliente debe conocer el SSID para poder conectarse a la red. Todos los dispositivos inalámbricos deben compartir el mismo SSID para poder comunicarse entre sí.

Cuando un usuario se mueve desde un BSS a otro, situado dentro del mismo ESS, el adaptador inalámbrico de su equipo puede cambiarse de punto de acceso, dependiendo de la calidad de la señal recibida. Los puntos de acceso se comunican entre sí para poderse intercambiar información.

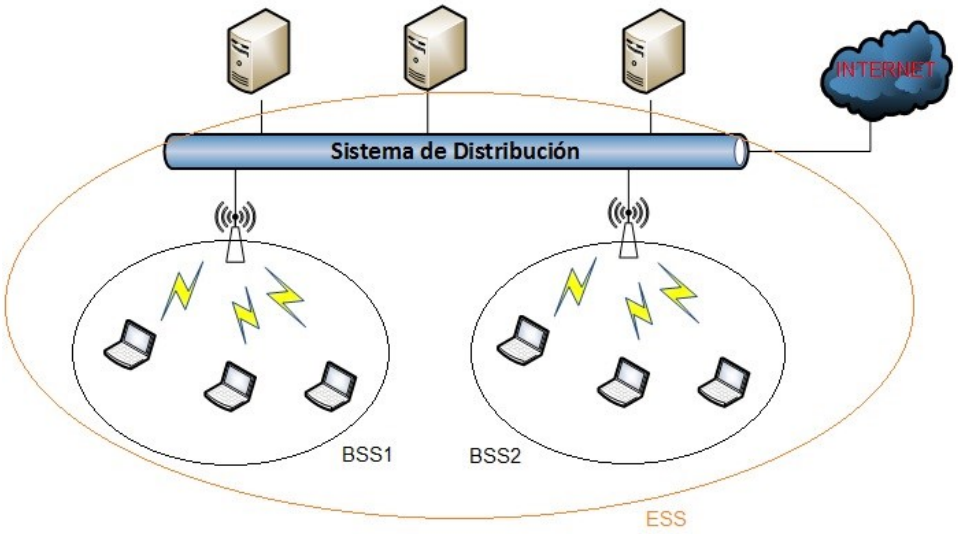


Ilustración 7 Modo Infraestructura

La desventaja principal del uso de un punto de acceso es que al ser un medio compartido, entre distintas estaciones, reduce la capacidad del canal en forma proporcional al número de clientes conectados. Su alcance puede ir desde 20 a 100 metros en interiores, y en exteriores puede variar entre 200 metros y algunos kilómetros, dependiendo de la antena utilizada.

Se recomienda no configurar el mismo canal en todos los puntos de acceso que se encuentren en la misma área física ya que se podrían producir interferencias entre ellos, provocando una inestabilidad en la conexión por parte de los usuarios.

3.3.2 Modo Ad-Hoc

En el modo Ad-Hoc las estaciones se conectan entre sí para formar una red punto a punto, en la que cada estación actúa como cliente y como punto de acceso simultáneamente.

La configuración formada por las diferentes estaciones recibe el nombre de conjunto de servicio básico independiente o IBSS. Un IBSS es una red inalámbrica que consta de al menos dos estaciones para poder funcionar y no necesita de ningún punto de acceso. Por lo tanto, IBSS crea una red temporal que permite a los usuarios que estén situados en la misma ubicación intercambiar información. Se identifica mediante un SSID, al igual que lo hace un ESS en el modo de infraestructura.

El rango del IBSS queda determinado por el rango de cada estación. Por lo que si dos estaciones de la red están fuera de rango de la otra, no podrán comunicarse. A diferencia del modo infraestructura, el modo Ad-Hoc no tiene un sistema de distribución capaz de enviar tramas de datos desde una estación a otra. Por lo que, por definición, un IBSS es una red inalámbrica restringida.

Además todas las estaciones que deseen conectarse a la red deben operar en el mismo rango de frecuencias; de lo contrario, aunque se puedan ver, no podrán interactuar entre ellas.

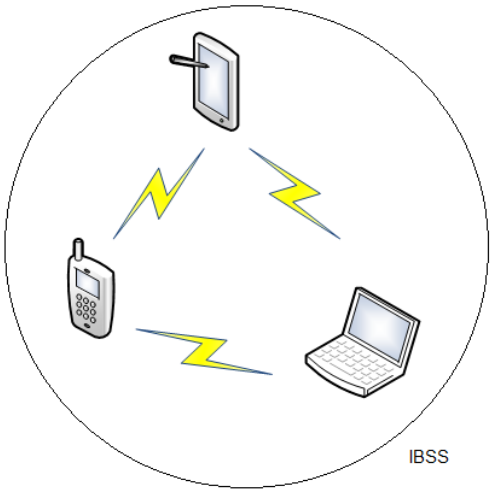


Ilustración 8 Modo Ad-Hoc

3.3.3 Otras topologías

La mezcla de las dos topologías anteriores es conocida como Red Mesh o Red Mallada. Son redes con topología de infraestructura que permite a estaciones que están fuera del rango de cobertura del AP poder unirse a algún dispositivo que se encuentre en su mismo rango de cobertura, siempre y cuando este se encuentre directa o indirectamente ligado al rango de cobertura del AP.

Para poder transmitir la información hacia su destino con el número de saltos es necesario el uso de un protocolo de enrutamiento.

Este tipo de redes es tolerante a fallos, la caída de un nodo no implica que toda la red caiga, ya que hay diferentes caminos.

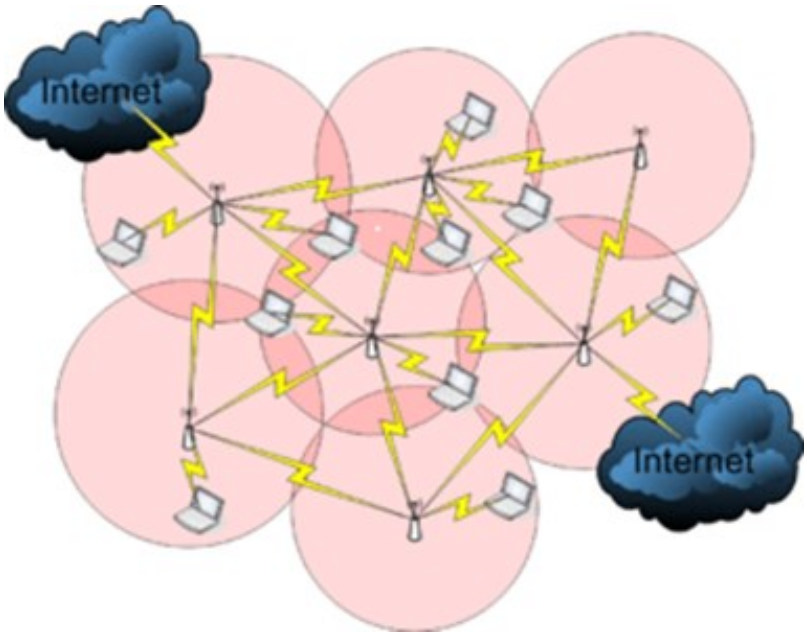


Ilustración 9 Topología de Red Mesh

3.4 Canales y frecuencias

En la definición del estándar IEEE 802.11 se especificó también los dos rangos de frecuencia disponibles para que los dispositivos pudieran emitir: 2,4 GHz y 5 GHz. Cada uno de ellos está subdividido, a su vez, en multitud de canales.

Para la banda de 2,4 GHz existen un total de 14 canales separados por 5 MHz cada uno de ellos. En Europa tan solo se utilizan 13 canales, el 14 está reservado para su uso en Japón. El problema de esta distribución reside en que cada canal necesita 22MHz de ancho de banda para poder operar y, por lo tanto, se produce el solapamiento de varios canales contiguos.

Por ejemplo, el canal 1 se superpone con los canales 2, 3, 4 y 5, por lo tanto los dispositivos que emitan en ese rango de frecuencias pueden generar interferencias. Lo mismo ocurre con el canal 6 y los canales 7, 8, 9 y 10. Por lo que en la práctica tan solo se pueden utilizar tres canales en forma simultánea, el canal 1, 6 y el 11.

La asignación de canales usualmente se hace únicamente en el AP, los clientes Wi-Fi automáticamente detectan el canal. En excepción de las redes Ad-hoc, que se podrá configurar el canal.

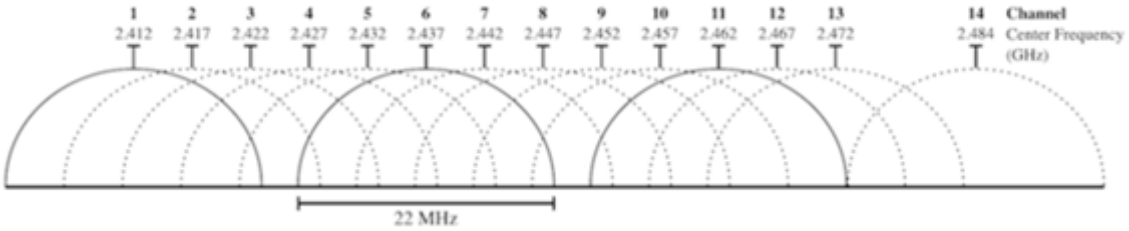


Ilustración 10 Canales y Frecuencias Wi-Fi

En cambio, la banda de 5 GHz tiene disponible un total de 23 canales utilizables para equipos inalámbricos. Tal como pasaba en la banda de los 2,4 GHz, los canales contiguos se superponen y se producen interferencias, por lo que es aconsejable usar tan sólo 12.

La principal diferencia entre la banda de 2,4 GHz y 5 GHz es el rango; a mayor frecuencia, menor alcance. Por lo tanto, la señal de la frecuencia de 2,4 GHz puede llegar más lejos. También, en la banda de 2,4 GHz la cobertura es mejor, debido a que las ondas se atenúan mucho más rápido a frecuencias más altas.

Por otro lado, la banda de 2,4 GHz está saturada, debido al gran número de dispositivos que trabajan en esta frecuencia, como pueden ser: microondas, teléfonos o ratones inalámbricos, dispositivos bluetooth, etc. Como resultado, la frecuencia de 2,4 GHz experimenta más interferencias que la de 5 GHz.

Por lo tanto, la principal causa de la variación de señal o baja velocidad en una conexión Wi-Fi es el uso de un canal de emisión saturado con interferencias, para evitarlo es aconsejable no configurar el mismo canal en todos los puntos de acceso ubicados en la misma área física. Para evitar esto, existen multitudes de utilidades en internet que informan sobre el canal en el cual transmiten los puntos de accesos cercanos, tales como.: inSSIDer, WiFi Analyzer, NetSumbler, etc.

3.5 Ventajas y desventajas de las Redes Wi-Fi

Las redes Wi-Fi presentan una gran cantidad de ventajas, entre ellas destacan:

- Al tratarse de redes inalámbricas, cualquier usuario que tenga acceso a la red puede conectarse a la red desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Permiten el acceso desde múltiples estaciones sin ningún problema ni gasto en infraestructura, a diferencia de las redes cableadas.
- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca Wi-Fi es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con compatibilidad total.

A pesar de todos los beneficios que presenta también tiene desventajas, común a cualquier tecnología inalámbrica. Algunas de ellas:

- La velocidad que alcanzan es baja, en comparación con las redes cableadas, debido a las interferencias y pérdidas de señal que el ambiente puede llevar.
- Uno de los problemas más graves es la seguridad. Existen diferentes herramientas que permiten calcular la contraseña de la red y acceder a ella. Este problema se agrava debido a que es difícil controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista.
- La potencia de la conexión puede verse afectada por obstáculos, tales como: árboles, paredes, montañas, etc.

4. Seguridad en redes Wi-Fi

Las redes Wi-Fi sufren una gran variedad de ataques, que van desde la introducción de virus hasta la alteración y robo de la información confidencial. Por lo tanto, uno de los problemas más graves a los cuales se enfrentan actualmente la tecnología Wi-Fi es la seguridad. Un elevado porcentaje de redes son instaladas sin tener en consideración la seguridad, convirtiéndolas en redes abiertas, sin proteger la información que por ellas circulan. Otra desventaja es debido a que no es posible controlar el alcance de transmisión de este tipo de redes, por lo tanto, cualquier usuario con conocimientos básicos de redes podría tener acceso a la red.

Existen diversas alternativas para garantizar la seguridad de estas redes, siendo las más comunes la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como pueden ser WEP, WPA y WPA 2, encargados de proteger su confidencialidad proporcionada por los propios dispositivos inalámbricos.

El estándar de la IEEE.802.11 propone tres servicios básicos de seguridad para el entorno de las WLAN: autenticación, confidencialidad e integridad.

Servicio de seguridad	Descripción
Autenticación	Provee servicios de seguridad para verificar la identidad entre los dispositivos clientes que se comunican. Esto provee control de acceso a la red denegando acceso a los dispositivos clientes que no pueden ser autenticados.
Confidencialidad	Provee privacidad conseguida por una red cableada. Pretende prevenir el compromiso de la información de un ataque pasivo.
Integridad	Asegura que los mensajes intercambiados no son modificados entre el tránsito entre los clientes y el AP en un ataque.

Tabla 3 Servicios de Seguridad en WLAN

4.1 Proceso de Asociación 802.11

Como parte de la seguridad en una red Wi-Fi es importante conocer cómo se realiza una conexión a una red inalámbrica por parte de un cliente. Siendo los componentes principales de este proceso los siguientes:

- **Beacon Frames**: Tramas que envía periódicamente el punto de acceso para comunicar su presencia de la red WLAN.
- **Sondas**: Tramas que envían los clientes de la WLAN para encontrar sus redes.
- **Autenticación**: Proceso por el cual se autoriza a un cliente WLAN acceder a la WLAN.

- **Asociación**: Proceso por el cual el punto de acceso sincroniza con el cliente WLAN.

Primera etapa

Por un lado, el punto de acceso envía tramas beacon Frames periódicamente en su zona de cobertura para comunicar su presencia y disponibilidad en la WLAN. Estas tramas contienen toda la información referente sobre la red WLAN inalámbrica (SSID, velocidad que admite, tipo de seguridad, etc.).

Por otro lado, si el cliente sólo quiere descubrir las redes WLAN disponibles, enviará un pedido de sondeo sin especificar el SSID. Todos los puntos de acceso configurados para responder este tipo de consultas, responderán. Por lo que, las redes WLAN con la opción de broadcast SSID deshabilitado no responderán.

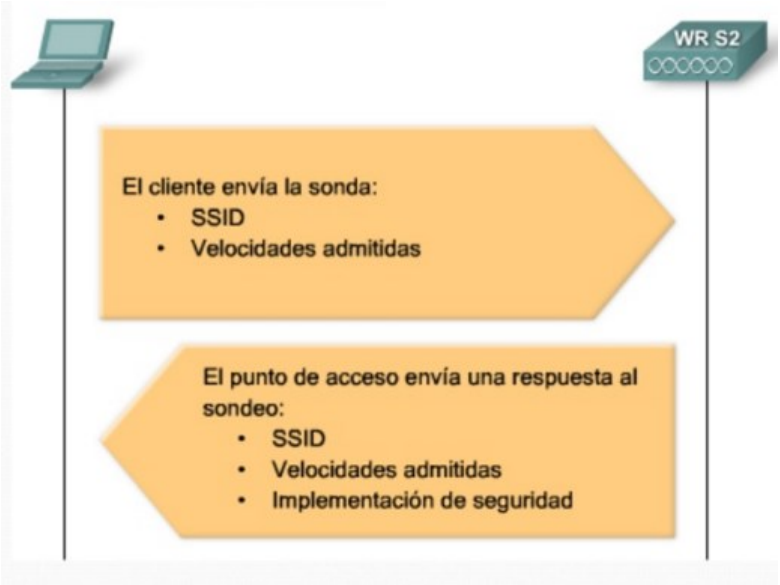


Ilustración 11 Sondeo de 802.11

Segunda etapa

Cuando el cliente detecta el punto de acceso deberá autenticarse. El estándar 802.11 propone dos mecanismos posibles de autenticación:

- **Sistema de autenticación abierto**: Autentica a cualquier cliente que lo solicite. Consta de una solicitud de autenticación por el cliente, conteniendo el ID del dispositivo (normalmente la dirección MAC). Esto es seguido de una respuesta de autenticación desde el punto de acceso que contiene un mensaje de resultado correcto o incorrecto.
- **Sistema de autenticación por clave compartida**: Se basa en el hecho de que ambos dispositivos que forman parte en el proceso de autenticación tengan la misma clave compartida.

Ilustración 12 Autenticación de 802.11

Tercera etapa

En esta etapa el cliente WLAN y punto de acceso intercambian las direcciones MAC y el identificador de asociación AID.

Una vez el cliente WLAN ya está asociado con un punto de acceso, el tráfico puede viajar de un dispositivo a otro.

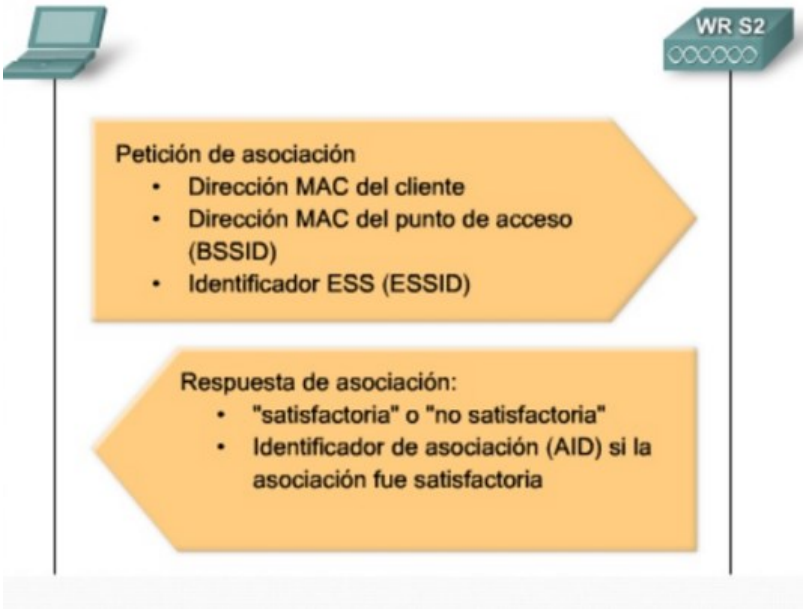


Ilustración 13 Asociación de 802.11

4.2 Protocolos de Seguridad

4.2.1 WEP

El protocolo WEP (Wired Equivalent Privacy) es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Su objetivo es proporcionar confidencialidad, autenticación y control de acceso en las redes inalámbrica. En referente a la autenticación, el protocolo WEP admite dos tipos de estándares 802.11: autenticación abierta o autenticación por clave compartida, ya comentados en el apartado anterior (asociación 802.11).

Las claves de cifrado utilizadas por WEP están basadas en algoritmo RC4, utilizado para cifrar las transmisiones realizadas a través del aire. El estándar define el uso de RC4 con claves (seeds) de 64 y/o 128 bits, de los cuales 24 bits corresponden al vector de inicialización (IV) y el resto, 40 o 104 bits, a la clave secreta compartida. El IV se genera dinámicamente y debe ser diferente en cada trama. La clave secreta es conocida tanto por emisor como por receptor. En cambio, el IV se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido.

El proceso de encriptación WEP es el siguiente

1. Se calcula el CRC de 32 bits, utilizado para garantizar la integridad de los mensajes (ICV, Integrity Check Value).
2. Se concatena el ICV al mensaje que se va a enviar.
3. Por otro lado, se concatena la clave secreta y el vector de inicialización, formado la semilla (seed).
4. El generador pseudoaleatorio de RC4 genera una secuencia de caracteres (Keystream), de la misma longitud que los bits obtenidos en el punto 2.
5. Se calcula al OR exclusiva (XOR) byte a byte de los caracteres del punto 2 con los del punto 4, obteniendo el mensaje cifrado.
6. Se añade el ICV al mensaje cifrado, obtenido en el punto anterior.
7. Para finalizar, se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama.

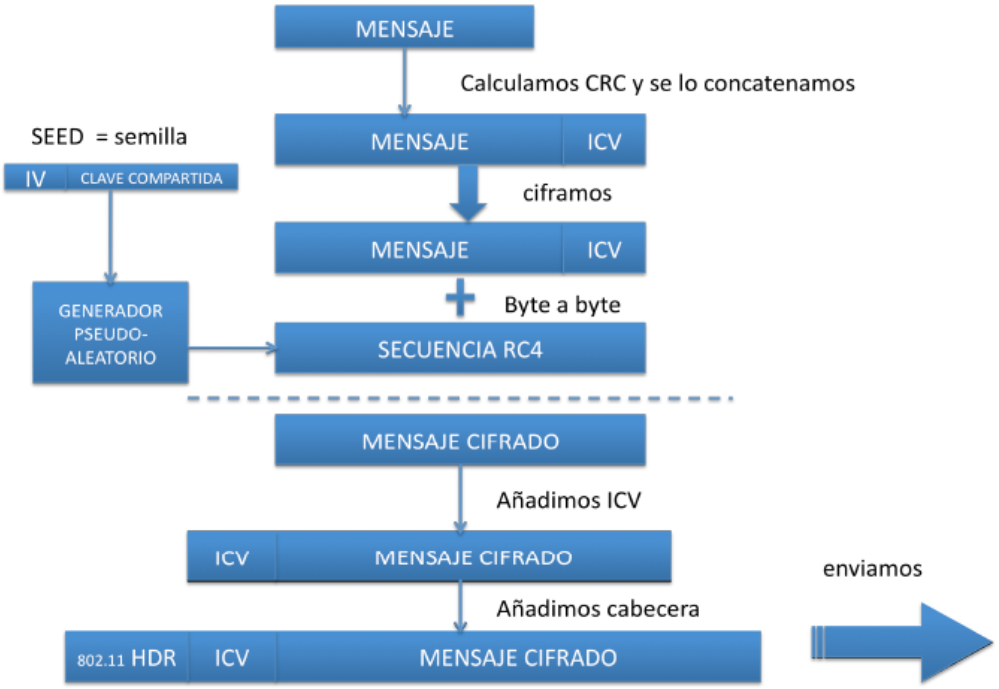


Ilustración 14 Cifrado WEP

La desencriptación se realiza calculando nuevamente la XOR de los datos recibidos y la clave secreta unida al IV.

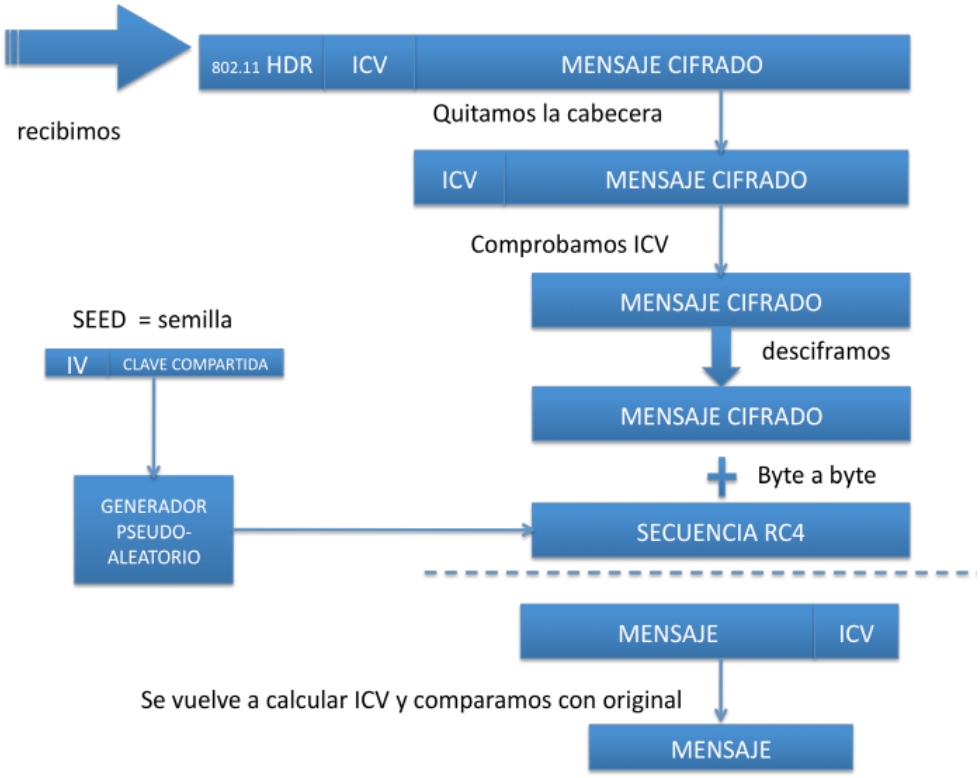


Ilustración 15 Descifrado WEP

Los principales problemas o defectos que encontrados en la implementación WEP son los siguientes:

- Es necesario ingresar manualmente la clave secreta en todos los dispositivos.
- En algún momento del envío y recepción de datos entre elementos del sistema, el vector de inicialización podría repetirse, lo cual no solamente crearía un conflicto, sino que también los hackers podrían analizar los paquetes enviados y descifrar la codificación.
- Al no contar con mecanismos de protección contra mensajes repetidos (replay) es posible capturar un mensaje e introducirlo en la red en un momento posterior.
- El sistema de cifrado RC4 tiene, principalmente, dos vulnerables: lo predecible que pueden llegar a ser los primeros bytes generados por RC4 y la concatenación de la clave compartida con un IV conocido, haciendo vulnerable le clave del algoritmo.

En la actualidad, el protocolo WEP está definitivamente en desuso, y no debería ser utilizado, ni siquiera con rotación de claves.

4.2.2 WPA

WPA (Wi-Fi Protected Access) es un estándar para proteger las redes Wi-Fi, creado para corregir los fallos de seguridad del protocolo WEP.

WPA soluciona la debilidad el vector de inicialización (IV) de WEP, mediante la introducción de vectores del doble de longitud (48 bits), permitiendo un total 2^{48} combinaciones de claves posibles, un número muy por encima de los (2^{24}) 16 millones que permitía WEP. Aunque sigue utilizando el algoritmo RC4 como sistema de cifrado.

Utiliza el protocolo de gestión de claves dinámicas (TKP – Temporal Key Integrity Protocolo) que permite utilizar una clave diferente para cada trama transmitida. La clave es generada a partir de la clave base, la dirección MAC del dispositivo emisor y del número de serie del paquete como IV. Cada paquete que se transmite incluye un número de serie único de 48 bits que se incrementa en cada trama, para asegurar claves distintas. Con esto se consigue evitar los ataques de colisión o de replay, ya que si se inyecta un paquete con la misma clave, el paquete estaría fuera de secuencia y sería descartado.

También se ha eliminado el CRC-32 y se ha incluido un nuevo código denominado MIC (Message Integrity Code) o Michael, código que verifica la integridad de las tramas.

Para la autenticación, se sustituye el mecanismo de autenticación de secreto compartido de WEP y se incluyen dos tipos de autenticación:

- **Con clave previamente compartida** (PSK – Pre-Shared Key): Este tipo de autenticación es normalmente utilizado por usuarios domésticos o por pequeñas redes. Requiere introducir la misma clave compartida en todos los dispositivos de la WLAN.

- **Con servidor RADIUS**: Este es el modo de utilización de las empresas, debido a que requiere de un Servidor para realizar las funciones de autenticación, autorización y contabilidad.

4.2.3 WPA2

WPA2 (Wi-Fi Protected Access 2) es un sistema para proteger redes Wi-Fi y fue creado para corregir las vulnerabilidades detectadas en su antecesor, WPA. Este sistema cumple con todas las características del estándar IEEE 802.11i. Siendo este sistema la versión certificada del estándar 802.11i, que fue ratificada en junio de 2004.

La principal ventaja de WPA2 respecto a WPA es que este primero utiliza el sistema de cifrado por bloques conocido como AES (Advanced Encryption Standard), mientras que WPA sigue utilizando el sistema de cifrado por flujo, RC4, heredado de WEP.

Otra ventaja de este sistema es que incluye el protocolo de encriptación CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), sustituyendo al TKIP, utilizado en WPA. El uso del protocolo CCMP es obligatorio en el estándar WPA2, pero opcional en WPA.

CCMP emplea el algoritmo de seguridad AES. A diferencia de TKIP, la integridad de la clave de administración y mensaje es manejada por un único componente creado alrededor de AES utilizando una clave de 128 bits.

	ESTÁNDARES		
	WEP	WPA	WPA2
Algoritmo cifrado	RC4	RC4	AES
Tipo cifrado	Flujo	Flujo	Bloque
Protocolo de seguridad	-	TKIP	CCMP
Distribución de claves	Manual	EAP	EAP
Comprobación integridad	CRC-32	TKIP	CCMP
Año aparición	1999	2002	2004

Tabla 4 Resumen y comparativa de los diferentes estándares de seguridad

4.3 Wi-Fi Protected Setup

WI-FI Protected Setup es un estándar que es promovido por la Wi-Fi Alliance, que permite la creación de redes WLAN seguras. WPS no es un sistema de seguridad, sino que un conjunto de mecanismos cuyo objetivo es facilitar la configuración de las redes inalámbricas con seguridad

WPA o WPA2, de usuarios domésticos y pequeñas oficinas. Lo que hace WPS es establecer mecanismos que permiten a diversos dispositivos obtener las credenciales necesarias para poder autenticarse en la red.

Ilustración 16 Logotipo WPS

La arquitectura de WPS tiene tres elementos, cada uno de ellos con roles diferentes que permiten a este sistema funcionar:

- **Registrar**: Dispositivo que tiene la facultad de generar o quitar credenciales. Puede ser un AP u otra estación.
- **Enrollee**: Dispositivo que intenta asociarse a la red WLAN.
- **Authenticator**: AP que funciona como puente entre Registrar y Enrollee.

Existen diversas formas en que WPS permite la configuración y el intercambio de credenciales:

- **PIN** (Personal Identification Number): es un número de 4 ó 8 dígitos de longitud. Este debe ser de conocimiento de Registrar así como la contraparte que desea conectarse Enrollee.

Ilustración 17 WPS: Intercambio de claves mediante PIN

- **PBC** (Push Botton Configuration): la configuración y el intercambio se hace de manera física, a través de un botón en el AP o en cualquier elemento Registrar; durante el lapso en que es presionado el botón, cualquier otro dispositivo próximo puede ganar acceso a la red.

Ilustración 18 WPS: Intercambio de claves mediante PBC

- **USB**: a través de este método las configuraciones se transmiten de un dispositivo Registrar a uno Enrollee por medio de un dispositivo de almacenamiento.

- **NFC**: a través de comunicación NFC, que permite la comunicación sin hilos entre dispositivos próximo (menos de 20 cm). En este caso, el dispositivo Enrollee se debe situar próximo del Registrar para poder realizar la autenticación.

4.3.1 Ventajas de sistema WPS

- La configuración mediante botón PBC es útil cuando por ejemplo no disponemos de un PC para configurar el punto de acceso.
- Con esta funcionalidad y tan solo pulsando el botón WPS en ambos dispositivos, estos quedarían asociados y configurados en apenas un minuto con cifrado incluido.
- No se necesita conocer el nombre de la red ni la contraseña, ya que por defecto esta se genera aleatoriamente al usar el botón WPS por primera vez en caso de que no hubiera una escrita anteriormente.

4.3.2 Vulnerabilidades WPS

La mayor vulnerabilidad de este sistema es que al ser un estándar impulsado por la misma Wi-Fi Alliance, para que un dispositivo tenga la certificación Wi-Fi debe poseer esta característica activada por defecto, por lo que hoy en día son más los dispositivos que presentan esta vulnerabilidad que hasta el día de hoy no tiene solución.

Cuando un cliente desea asociarse al punto de acceso, envía un número PIN formado por 8 dígitos. Cuando el cliente envía el PIN incorrecto, el punto de acceso responde con un mensaje EAP-NACK. Al no existir ningún mecanismo para limitar los intentos, este sistema es susceptible de ser atacado por fuerza bruta. El problema se agrava porque, según ha descubierto Stefan Viehböck, el punto de acceso responde con EAP-NACK tan solo con enviar los cuatro primeros dígitos, por lo que no hay necesidad de introducir los 4 restantes y, por lo tanto, las combinaciones posibles se reducen de 100 millones (10^8) a tan solo 20.000 (10^4+10^4). Como el último dígito del PIN pertenece al checksum, los intentos se reducen a 11.000 (10^4+10^3).

Por lo tanto, con 11.000 combinaciones posibles y sin mecanismos de protección para ataques de fuerza bruta, es posible averiguar el PIN en menos de dos horas.

4.4 Autenticación 802.1x

La norma 802.1x surgió como una respuesta a la necesidad de proporcionar seguridad a nivel de usuario. Para autentificación y encriptación utiliza el protocolo EAP. En una arquitectura 802.1x existen siempre tres elementos:

- **Suplicant** (Peticionario): Se designa por este término al cliente que desea acceder a una red e intenta autentificarse. En una red Wi-Fi es el cliente que desea conectar con el punto de acceso para entrar en la red.

- **Authenticator** (Autentificador): Es el equipo que recibe la petición de conexión del cliente y que por tanto ha de tramitar la autentificación de este. En el caso de las redes Wi-Fi este rol lo lleva a cabo el punto de acceso.
- **Authenticator Server** (Servidor de Autentificación): Es el equipo que mantiene y gestiona de forma centralizada las credenciales de los usuarios. Dicho servicio se implementa mediante un servidor RADIUS.

El funcionamiento base del estándar 802,1x se centra en la denegación de cualquier tráfico que no sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ello, el autenticador crea un puerto que define dos caminos, uno autorizado y otro no: manteniendo el primero cerrado hasta que el servidor de autenticación le comunique al cliente que dispone de acceso.

En la siguiente ilustración se puede observar la comunicación y relación existente entre los diferentes elementos:

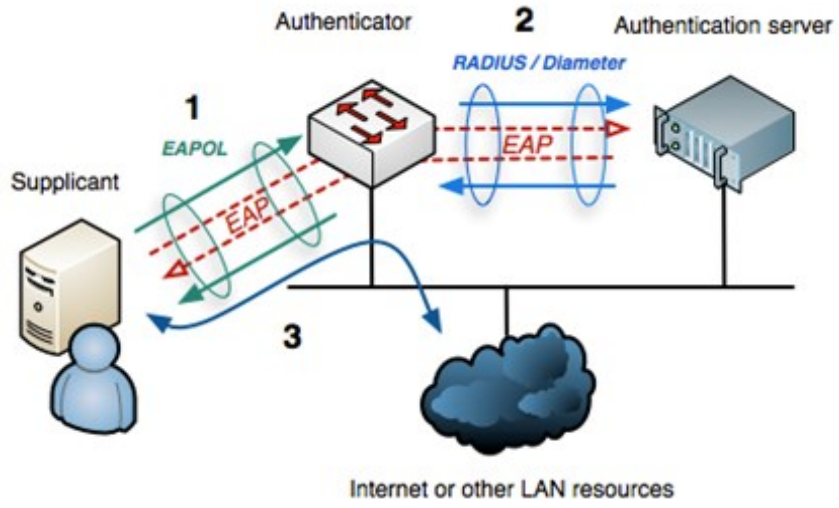


Ilustración 19 Arquitectura 802.1x

Este tipo de autentificación proporciona grandes ventajas deseables en redes con un número elevado de usuarios o que requieran un control sobre el uso de estos de la red.

La principal característica es que existe un solo punto donde almacenar todas las credenciales y usuarios y que este sistema será el responsable último de asignar el tipo de acceso de cada uno. Así pues, el servidor RADIUS podrá llevar a cabo labores AAA (Authentication, Authorization and Accounting) de forma centralizada.

Al disponer de un servidor RADIUS ya no se dispone de una sola clave para garantizar el acceso a cualquier usuario de la red, si no que las credenciales dependerán de cada usuario, lo cual permitirá entre otras cosas llevar un registro de los accesos a la red y la asignación de diferentes privilegios y niveles acceso dependiendo del usuario.

Así mismo se incrementa la seguridad del sistema, pues las claves ya no residen el punto de acceso, que es el extremo de la red, si no en un servidor dedicado cuyo nivel de seguridad es mayor. También se solventa el problema de robos de claves o credenciales, puesto que, al ser únicas por cada usuario, la sustracción de una solo será significativa para el usuario afectado, y no para el resto de usuarios de la red. Bastará con cambiar las credenciales de ese usuario o bloquearlo para restablecer la seguridad en la red, sin afectar en el proceso al resto de clientes como ocurre en las arquitecturas de clave única.

4.5 Autenticación EAP

802.1x utiliza un protocolo de autenticación llamado EAP que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, kerberos, ldap, etc. EAP actúa como intermediario entre solicitante y el motor de validación, permitiendo la comunicación entre ambos.

Existen múltiples tipos de EAP, algunos son estándares y otras soluciones propietarias. Entre los tipos de EAP se encuentran:

- **EAP-TLS**: Sistema de autenticación fuerte basado en certificados digitales, tanto en el cliente como en el servidor, por lo que requiere una configuración PKI entre ambos extremos.
- **EAP-TTLS**: Sistema de autenticación basado en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, creando un túnel para transmitir el usuario y contraseña. Este tipo de autenticación, a diferencia de EAP-TLS sólo requiere certificado de servidor.
- **PEAP:** Utiliza seguridad de capa de transporte para crear un canal cifrado entre un cliente y un servidor de autenticación (RADIUS o NPS). No especifica un método de autenticación, pero proporciona seguridad adicional para otros protocolos de autenticación EAP que pueden opera a través del canal cifrado TLS que proporciona PEAP. Es utilizado como método de autenticación para los clientes inalámbricos que usen el protocolo 802.11, pero no se puede utilizar en clientes de redes virtuales (VPN). Para redes WLAN se pueden utilizar dos tipos de EAP para usar PEAP:
    - **EAP-MS-CHAPV2:** Utiliza nombre de usuario y contraseña para la autenticación de usuarios y un certificado del almacén de certificados del equipo servidor para la autenticación del servidor.
    - **EAP-TLS:** Sistema de autenticación fuerte basado en certificados digitales.

Una vez han sido mencionadas las medidas de seguridad que pueden ser utilizadas para proteger una red inalámbrica se adjunta una tabla resumen de las mismas, en las que se describen las principales características de cada una de ellas:

Medidas de seguridad	Principales características
WEP	Primer sistema de cifrado asociado al protocolo 802.11. Utiliza una misma clave simétrica y estática en las estaciones de trabajo y el punto de acceso. El estándar no contempla ningún mecanismo de distribución de claves automáticas, lo que obliga a escribir la clave manualmente en cada uno de los dispositivos de la red. El algoritmo de encriptación utilizado es RC4 con claves (seed). Es considerado como el menos seguro de todos por su seguridad para romperlo.
WPA	Las principales características de WPA son la distribución dinámica de claves, utilización robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autenticación. WPA incluye IEEE 802.1x, EAP, TKIP, MIC. Tiene dos métodos de funcionamiento, con servidor RADIUS y con clave previamente compartida.
WPA2	Versión certificada del estándar 802.11i. Está basado en el WPA. WPA2 incluye nuevo algoritmo de cifrado AES.
WPS	Mecanismo creado para facilitar la conexión de dispositivos a la WI-FI. Permite a diversos dispositivos obtener las credenciales necesarias para poder autenticarse en la red sin necesidad de conocerlas
Autenticación 802.11x	Proporciona un sistema de control de acceso y autenticación basado en la arquitectura cliente/servidor. Restringe la conexión de dispositivos no autorizados a la red. Para autentificación y encriptación utiliza el protocolo EAP
Tipo de autenticación EAP-TLS	La autenticación se realiza mediante certificados digitales. Se requiere una infraestructura PKI.
Tipo de autenticación EAP-TTLS	La autenticación se realiza mediante la identificación de usuario y contraseña que se transmiten cifrados. Sólo requiere certificado de servidor.
Tipo de autenticación PEAP	Proporciona protección a clientes y autenticadores que utilizan EAP. La seguridad se realiza a nivel de transporte para crear la comunicación entre el cliente y el autenticador. Requiere un certificado para la autenticación de servidores y credencial (nombre de usuarios y contraseña) para la autenticación de usuarios.

Tabla 5 Resumen de las medidas de seguridad WI-FI

También se incluye otra tabla resumen con las ventajas e inconvenientes de cada una de las medidas propuestas

Medidas de seguridad	Ventajas	Inconvenientes
WEP	Soportado por casi todos los dispositivos	Fácil vulnerabilidad. Existen herramientas que permiten romper la clave secreta.
WPA	Gran simplicidad de aplicación en relación a los buenos resultados de protección que ofrece	Fácil vulnerabilidad mediante ataques de fuerza bruta en caso de utilizar Pre-Share Key débiles.
WPA2	Ofrece el mayor grado de seguridad respecto a WEP y WPA. También cumple con el estándar 802.11i	Existen incompatibilidades con ciertos dispositivos. De igual modo, fácil vulnerabilidad mediante ataques de fuerza bruta en caso de utilizar Pre-Share Key débiles

Medidas de seguridad	Ventajas	Inconvenientes
WPS	Permite asociar un dispositivo a la red sin necesidad de introducir la clave ni conocer el nombre de la red	Vulnerable mediante ataques de fuerza bruta.
Autenticación 802.11x	Se basa en un servidor de autenticación, con lo que se incluye mayor seguridad.	Normalmente utilizado en el ámbito empresarial debido a su compleja instalación y configuración. Requiere un servidor para la autenticación.

Tabla 6 Ventajas e inconvenientes de las medidas de seguridad WI-FI

En este capítulo se han tratado básicamente tres medidas de seguridad (WEP, WPA, WPA2) y un mecanismo utilizado para facilitar la conexión de dispositivos a nuestra W-Fi (WPS).

Tras el análisis realizado en este capítulo de los métodos de seguridad para este tipo de redes se pueden concluir las siguientes recomendaciones:

- En entornos empresariales se recomienda utilizar el mecanismo WPA2-Enterprise. Debido a que el modo WPA/WPA2 con clave precompartida (PSK) ha sido vulnerado, considerándose poco seguro para estos entornos.
- En entornos particulares es recomendable la utilización de WPA2-PSK mediante una contraseña robusta, debido a que es más seguro que los mecanismos WPA y WEP. El tipo de cifrado seleccionado debería ser AES, TKIP es un protocolo de encriptación provisional para remplazar el cifrado WEP, el cual sigue siendo poco seguro.
- En cualquiera de los entornos, residencial o empresarial, se recomienda evitar emplear WEP como mecanismo de seguridad debido al gran número de vulnerabilidades que presenta. En el caso de que no sea posible utilizar WPA2 ni WPA, siempre es recomendable utilizar WEP antes que transmitir la información sin cifrar.
- En cualquiera de los entornos se recomienda deshabilitar la tecnología WPS debido a que puede ser vulnerable mediante un ataque de fuerza bruta y con ello obtener las claves. En caso de no poder ser deshabilitada se debería actualizar el firmware del mismo. Existe un firmware OpenSource, cuyo nombre es DD-WRT, el cual no está demostrado que no es susceptible a este tipo de ataques.

5. Ataques sobre redes Wi-Fi

Dado que el aire es el medio utilizado para la transmisión inalámbrica, hace que este tipo de redes sean más susceptibles a recibir ataques por parte de cualquier atacante equipado con el material adecuado

Los ataques realizados sobre una red inalámbrica pueden ser clasificados en dos categorías, en base a la forma de proceder de los atacantes:

- **Ataques pasivos**: Se produce cuando un usuario no autorizado accede a la red para espiar la información y, aunque no la modifica, la guarda para analizarla y posteriormente utilizarla para realizar un ataque activo. Este tipo de ataque es muy difícil de detectar debido a que no altera los datos, sin embargo, es posible evitarlos mediante el cifrado de la información.
- **Ataques activos**: Se produce cuando un usuario no autorizado accede a la red y realiza una alteración o modificación en el contenido de los datos o simplemente impide su utilización.

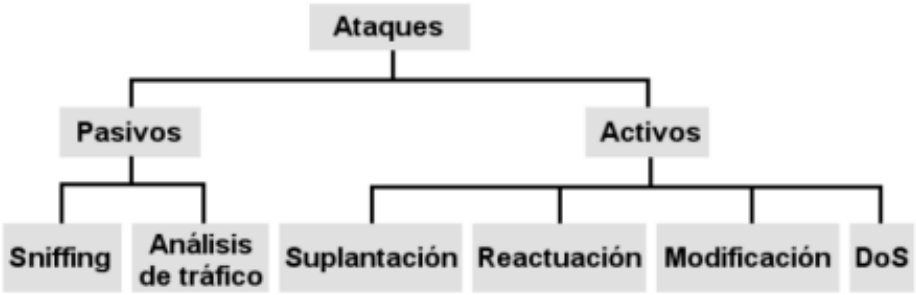


Ilustración 20 Clasificación ataques Wi-Fi

5.1 Ataques activos

5.1.1 Suplantación

Ataque que consiste en la obtención de la identidad de un usuario autorizado por parte del atacante. Este ataque normalmente se ejecuta con otros tipos de ataques activos.

Dentro de este ataque se incluyen los siguientes:

- **Man in the Middle**: El atacante se ubica entre el AP y el dispositivo inalámbrico del cliente, consiguiendo controlar toda la comunicación realizada entre ambos, y pudiendo: modificar, alterar o bloquear la información.
- **MAC Spoofing:** Ataque utilizado normalmente cuando la red a la cual se quiere atacar está protegida mediante el mecanismo de filtrado de direcciones MAC. Consiste en detectar una MAC autorizada y utilizarla en un dispositivo no autorizado, esto se consigue mediante un sniffer y un software para alterar la MAC, con esto el AP creerá que el dispositivo con la MAC falsa es un usuario legítimo.

- **ARP Poisoning:** Ataque que tiene como objetivo enviar mensajes ARP falsos a la red. Normalmente, la finalidad es modificar las tablas ARP que tienen los equipos de la red, asociando la dirección MAC del atacante con la dirección ip de otro equipo de la red. Por lo que, cualquier tráfico dirigido a ese equipo será erróneamente enviado al atacante, en lugar de a su destino final.
- **Session Hijacking**: Ataque cuyo principal objetivo es desautenticar a un cliente legítimo conectado a la red, mediante un ataque de Denegación de Servicio, para posteriormente suplantarlo.
- **Honeypot**: Este ataque consiste en utilizar un AP con el mismo ESSID de la red a la que se desea atacar y en el mismo rango de cobertura. De esta forma, cuando algún usuario se asocie mediante su login y contraseña poderlos capturar.

5.1.2 Reactuación

Consiste en capturar mensajes legítimos y repetirlos con el fin de producir un efecto no deseado, como podría ser envío de masivos de emails masivos, etc…

5.1.3 Modificación

Consiste en capturar mensajes enviados por un usuario autorizado y modificarlos, borrarlos o reordenarlos, para producir un efecto no autorizado.

5.1.4 Denegación de Servicio

Consiste en evitar que los clientes legítimos consigan acceder a la red o a un servicio que ofrezcan. Existen diferentes formas de realizar este tipo de ataque, como ejemplo:

- **Saturación del ambiente con ruido RF**: Este ataque se produce cuando algún atacante produce deliberadamente ruido, causando interferencias cerca de la red y con esto degrada la calidad de la señal, provocando que los usuarios pierdan la conectividad a la red.
- **Torrente de autenticaciones**: Cuando se está trabajando con estándar 802.1x y el servidor RADIUS, es necesario que todos los usuarios se autentiquen, lo que consume recursos hasta que el usuario sea registrado. Si el atacante envía falsas peticiones de autenticación en grandes cantidades, repetitivas y simultáneas tendría el sistema ocupado todo el tiempo logrando que los usuarios legítimos no puedan hacer uso de la red.

- **Desautenticación de clientes**: Disponiendo de las direcciones MAC necesarias, la del AP y la de los clientes asociados, el atacante podrá falsificar y crear paquetes de desautenticación como los que envía el AP para desautenticar las estaciones.

5.2 Ataques pasivos

5.2.1 Sniffing

Consiste en capturar tráfico de la red para posteriormente poder obtener datos como pueden ser direcciones IP, direcciones MAC, direcciones de correo electrónico, passwords, usuarios etc.

5.2.2 Análisis del tráfico

Consiste en obtener información de la red mediante el análisis del tráfico y sus patrones, como por ejemplo a qué horas se encienden ciertos dispositivos, el tráfico que se envía, a qué hora hay más tráfico, etc.

5.3 Ataques protocolo WEP

Debido al gran número de debilidades que este protocolo de seguridad WEP presenta en el intercambio de claves han ido apareciendo diferentes tipos de ataques contra él. Todos ellos se caracterizan porque requieren la captura de un gran número de paquetes para poder obtener la clave.

5.3.1 Ataque Caffe Latte

A diferencia de la mayoría de ataques existentes, el ataque Caffe Latte se distingue del resto por realizarse al cliente y no al AP.

Este ataque se basa en la idea que en el cifrado WEP el usuario tiene que autenticarse, mientras que el AP no. Debido a esta falta de autenticación mutua provoca que un atacante pueda suplantar un AP mediante la copia del ESSID y llegue a emparejarse con el cliente.

5.3.2 Ataque de fragmentación

El ataque de fragmentación está basado en el protocolo de fragmentación de paquetes y en la predicción de su nuevo valor de cifrado. Tras el proceso de predicción de cifrado de los fragmentos se obtienen una cantidad de keystream utilizados para crear el nuevo paquete que será válido para el AP. Estos paquetes serán utilizados para realizar ataques de inyección que serán utilizados para obtener la clave WEP del AP.

5.3.3 Ataque de fuerza bruta

Los ataques por fuerza bruta son aquellos que intenta obtener la clave mediante la prueba de todas las combinaciones posibles. Para poder realizar este ataque es obligatorio conocer el texto en claro y el texto cifrado del mensaje Una vez obtenidos estos dos mensajes se aplicará el cifrado sobre el texto claro hasta obtener la clave WEP.

Este método, por definición, siempre consigue su objetivo, por lo que el inconveniente que tienen es de recursos y tiempo. En el caso que la clave sea suficientemente larga, el número de combinaciones posibles se dispara exponencialmente, por lo tanto, el proceso puede llegar a ser extremadamente lento.

5.3.4 Ataque mediante criptoanálisis estadístico FMS y Korek

El ataque FMS (Fluher, Martin y Shamir) es el primer ataque WEP implementado a partir de las debilidades conocidas en 2001. Este ataque consiste en recoger del orden de 5 millones de IVs para descifrar una clave de 128 bits.

Para realizar el ataque es necesario la existencia de tráfico en la red, por lo que es necesario que haya clientes conectados a ella. Además los paquetes capturados tienen que contener IVs válidos. Por lo que, las técnicas de reinyección de tráfico pueden ayudar a generar IVs mediante paquetes falsos.

Aunque este ataque fue mejorado por Korek en 2004, descubriéndose una serie de ataques que permiten descartar algunas claves según patrones.

5.3.5 Ataque mediante criptoanálisis estadístico PTW

En 2005 apareció otro ataque sobre RC4. Este ataque aprovecha las correlaciones entre la clave que usa RC4 y el KeyStrem que genera. Por ello, fue utilizada esta debilidad para realizar el ataque PTW, permitiendo recuperar la clave con tan solo 85.000 paquetes que contengan IVs. La condición necesaria para el éxito de este ataque es que los paquetes sean del tipo ARP.

5.4 Ataques protocolo WPA/WPA2 PSK

Los ataques al protocolo WPA/WPA2 PSK consisten en capturar el handshake, o secuencia de autenticación WPA. Por lo que, para capturar el handshake es necesario esperar a que un cliente se conecte a la red o, de lo contrario, provocar la desconexión para que una vez se vuelva a conectar sea posible capturarlo.

Una vez capturado todo lo necesario, será preciso conocer la PSK y, para ello, se utilizará la fuerza bruta o un diccionario para poder obtener la clave utilizada en el cifrado.

5.4.1 Ataques de diccionario

Una vez capturados los paquetes de una sesión de autenticación de un cliente se debe utilizar un ataque por fuerza bruta mediante el uso de un diccionario, para descifrar la clave.

El diccionario no es más que un archivo de texto donde se incluyen una lista de posibles claves. Por lo que, al realizar el ataque por fuerza bruta comprobará consecutivamente las palabras del diccionario para validar la clave. Por lo que, el éxito del ataque depende de la seguridad que la clave presente y si se encuentra en el diccionario, ya que de contrario no podría ser descifrada.

5.4.2 Ataque Hole 196

En la página 196 del estándar dice que los mensajes enviados con claves de grupo (GTK), es decir, las claves pensadas para comunicaciones broadcast no tienen protección contra Spoofing. Por lo que un atacante puede enviar un mensaje con una clave GTK con la ip que quiera, es decir, enviando un mensaje con una clave GTK pero a una MAC dirigida en lugar de a una dirección MAC de broadcasting. Haciendo esto, sólo la víctima procesará ese paquete broadcast y, por tanto, salvo que la tabla de ARPs tenga la resolución de la MAC del Gateway estática, se producirá un envenenamiento de la IP que permitirá suplantar al router.

A partir de ese momento, cuando la víctima se comunique con el Gateway se utilizarán las claves PTK asociadas a esa IP, que el atacante entregará para hacer el MITM.

Una vez han sido examinados algunos de los ataques que pueden ser realizados sobre las redes WI-FI se resumirán en la siguiente tabla:

ATAQUES PASIVOS	
Tipo de ataque	**Principales características**
Suplantación	Obtención de la identidad de un usuario autorizado por parte del atacante
Reactuación	Inyectar en la red paquetes interceptados para repetir operaciones realizadas por un usuario legítimo
Modificación	El atacante borra, manipula, añade o reordena los mensajes transmitidos
Denegación de Servicio	Evitar que los clientes legítimos consigan acceder a la red

ATAQUE ACTIVOS	
Tipo de ataque	**Principales características**
Análisis del tráfico	Consiste en analizar el tráfico en la red
Sniffing	Capturar tráfico de la red

ATAQUES DE SUPLANTACIÓN	
Tipo de ataque	**Principales características**
Man in the Middle	El atacante se sitúa entre el AP y cliente para poder modificar, alterar o bloquear la información
MAC Spoofing	Consiste en detectar una MAC autorizada y utilizarla en un dispositivo no autorizado
ARP Poisoning	Consiste en enviar mensajes ARP falsos a la red, modificando las tablas ARP de los dispositivos de la red
Session Hijacking	Consiste en desautenticar a un cliente legítimo de la red para poder suplantarlo
Honeypot	Consiste en utilizar un AP con el mismo ESSID de la red a la que desea atacar y en el mismo rango cobertura

ATAQUES DE DENEGACIÓN DE SERVICIO	
Tipo de ataque	**Principales características**
Saturación del ambiente con ruido RF	El atacante produce ruido para causar interferencias y degradar la señal, evitando que los usuarios puedan conectarse a ella
Torrente de autenticaciones	Se realizan muchos intentos de autenticación falsas contra el servidor RADIUS evitando que los usuarios legítimos puedan conectarse a ella
Desautenticación de clientes	Falsificar direcciones MAC para crear paquetes de desautenticación para desautenticar a los dispositivos

ATAQUES AL PROTOCOLO WEP	
Tipo de ataque	**Principales características**
Caffe Late	Debido a que el AP no debe autenticarse un atacante puede suplantar el AP.
Fragmentación	Permite al atacante generar e inyectar paquetes cifrados en una red WEP.
Fuerza bruta	El atacante intenta obtener la clave mediante la prueba de todas las combinaciones posibles.
FMS y Korek	Consiste recoger muchos Ivs para poder descifrar la clave
PTW	Ataque que aprovecha la correlación entre la clave usada por RC4 y el Keystream que genera para recuperar la clave

ATAQUES AL PROTCOLO WPA/WPA2 PSK	
Tipo de ataque	**Principales características**
Diccionario	El atacante intenta obtener la clave mediante un archivo de texto donde se incluye una lista de posibles claves
Hole 196	El atacante envía mensajes GTK con una ip falsificada con lo que el atacante con lo que se puede producir un envenenamiento de la IP, permitiendo suplantar el router

Tabla 7 Resumen de ataques sobre las redes WI-FI

Para finalizar este capítulo, se indicarán una serie de precauciones que se deberían tener en cuenta para evitar o minimizar el impacto de los ataques anteriormente descritos:

- **Evitar la conexión a redes WI-FI sin protección** (hoteles, aeropuertos, cafeterías, bibliotecas, etc.). La mayoría de estas redes no transmiten datos codificados o de forma

segura. En caso que se debe conectar a ellas sería recomendado **utilizar conexiones VPN**. De esta manera la conexión se cifra entre un cliente VPN y un servidor VPN, estableciéndose a través de un túnel de comunicación seguro

- **Utilizar**, siempre que sea posible, **el protocolo HTTPS** para acceder a las diferentes URLs. A diferencia de HTTP, https cifra la información. De este modo si la conexión es interceptada por un tercero no podrá descifrarla.
- **Utilizar certificados**, para cifrar las comunicaciones y autenticar los servidores.
- **Disponer** de **software antivirus** en los dispositivos clientes.
- **Limitar el alcance de la señal WI-FI** tan solo a la zona deseada. De esta forma se puede evitar que un atacante, desde el exterior, pueda conectarse al AP.

6. Caso Práctico

6.1 Introducción

En este caso práctico se analizarán algunos de los ataques que pueden ser realizados sobre las redes Wi-Fi. En el primer caso, se realizará un ataque sobre un AP configurado con el protocolo de seguridad WEP. En el segundo, configurando el AP con el protocolo de seguridad WPA2/PSK. Finalmente, el último ataque se realizará al AP con la tecnología WPS habilitada y con el protocolo de seguridad WPA2/PSK. De esta forma se pretende demostrar, debido a las diferentes vulnerabilidades que presentan cada una de estas tres tecnologías, la facilidad con la que se pueden obtener las respectivas claves de acceso en los diferentes casos que se presentan, en el caso de no presentarse las suficientes medidas de seguridad.

Para llevar a cabo los diferentes tipos de ataques se utilizará un entorno de laboratorio. Por lo tanto, en alguna ocasión puede ser necesario crear tráfico en la red. Para ello, se utilizará las conexiones inalámbricas de diferentes dispositivos, tales como: iPad, Smartphone y portátil. De este modo será posible simular que hay clientes conectados a la red inalámbrica.

El esquema de los diferentes ataques realizados será el siguiente:

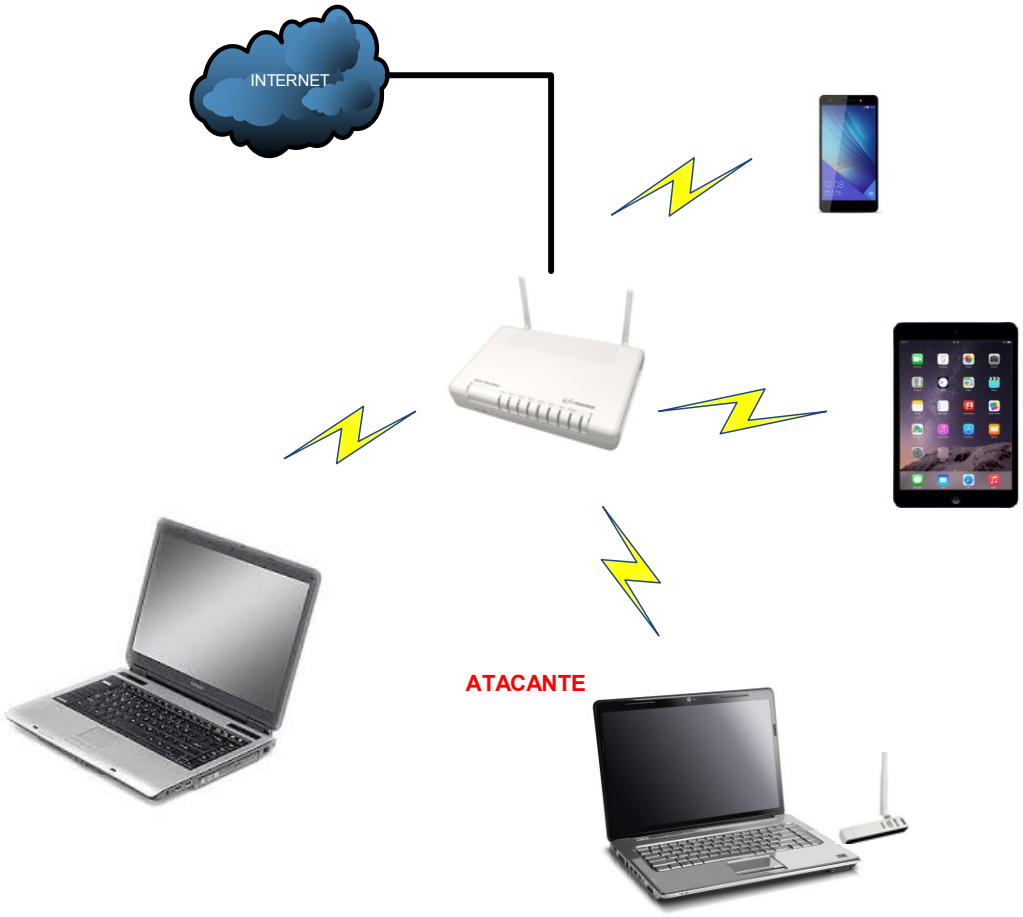


Ilustración 21 Esquema ataques WEP, WPA2/PSK y WPS

6.2 Requisitos

Para realizar los diferentes ataques se ha utilizado el siguiente material:

- Un AP que ofrezca la posibilidad de configurar los protocolos de seguridad WEP, WPA/WPA2 y la tecnología WPS.
- Software para realizar los diferentes ataques.
- Tarjeta de red inalámbrica que soporte el modo monitor.
- Diccionario que contenga un listado de palabras para realizar ciertos ataques.

El AP utilizado para poder configurar los métodos de seguridad WEP, WPA2 y WPS ha sido el que proporciona movistar a sus clientes, COMTREND C5813.

Para realizar los diferentes ataques se ha utilizado la distribución de Linux llamada KALI. Es una distribución Debian GNU/Linux que cuenta con una multitud de herramientas utilizadas para la auditoría y seguridad inalámbricas en general. Cuenta con alrededor de 600 programas preinstalados, incluyendo entre ellos: Scáners y Sniffers de Red, crackeadores de contraseñas, programas para ataques Wireless, entre otros muchos otros.

Para efectuar los dos primeros ataques, a los protocolos de seguridad WEP y WPA2, se ha utilizado aircrack-ng, que es una colección de herramientas que permiten auditar y atacar redes inalámbricas. Las herramientas que incluye aircrack son las siguientes:

- **airmon-ng**. Permite poner la tarjeta inalámbrica en modo monitor (sniffer).
- **airodump-ng.** Guarda los paquetes de la interfaz WLAN para ser procesador posteriormente con aircrack-ng.
- **aircrack-ng.** Permite romper el protocolo WEP y WPA para conseguir la clave de encriptación.
- **aireplay-ng.** Permite inyectar paquetes ARP-request en una red inalámbrica para generar tráfico y, de esta forma, que sea más fácil romper la clave con aircrack-ng.

En cambio, para el ataque a la tecnología WPS se ha utilizado la herramienta Reaver, integrada también en la distribución de Linux KALI. Reaver es una herramienta utilizada para explotar la debilidad de APs con WPS activado por medio de un ataque de fuerza bruta probando todas las posibilidades hasta encontrar el PIIN del AP. Por lo tanto, Reaver sirve para conseguir la clave WPA o WPA2 de un AP sin la necesidad de diccionarios.

6.3 Ataque WEP

Como se ha visto en el capítulo 4, el protocolo WEP está basado en el algoritmo de RC4 con una clave secreta de 40 ó 104 bits, combinado con un vector de inicialización de 24 bits. WEP no fue creado por expertos criptográficos y desde su aparición han ido apareciendo numerosas

vulnerabilidades ante los problemas del algoritmo RC4 que utiliza: debilidades de no validación y ataques IV conocidos.

Ambos ataques se basan en el hecho de que para ciertos valores de la clave es posible que los bytes iniciales del flujo de la clave dependan de tan sólo pocos bits de la clave de encriptación. Como la clave de encriptación está compuesta por la clave secreta y los IV, ciertos valores de IV muestran claves débiles. Por lo tanto, consiguiendo suficientes IV débiles se podrá obtener la clave WEP.

Como el tráfico de red habitual no genera de forma rápida suficientes vectores deberán ser usadas técnicas de inyección de paquetes para aumentar la velocidad del proceso de captura. Este proceso implica que se envíen al AP paquetes de forma continua y muy rápida para poder capturar así un gran número de IVs en un periodo corto de tiempo.

Una vez que se han capturado un gran número de IVs, podrán ser utilizados para obtener la clave WEP. El número de IVs necesarios para la obtención de una clave WEP no es ciencia exacta y dependerá de muchos factores, entre ellos la longitud de la clave WEP. Normalmente, una clave WEP de 64 bits puede ser recuperada con 300.000 IVs, en cambio, una clave de 124 bits con 1.000.000 de IVs

Para realizar este tipo ataque es necesario que haya clientes conectados al AP. De lo contrario no será posible capturar tráfico.

La configuración del Router es la siguiente:

Paso 1 – Colocar la tarjeta Wireless en modo monitor

En este paso se colocará la tarjeta Wireless en el modo denominado “modo monitor”. En este modo la tarjeta puede escuchar y capturar cualquier paquete Wireless que se encuentre en el aire. Normalmente la tarjeta únicamente solo escuchará y capturará los paquetes que le indiquemos.

Primero, se comprueba en que interfaz está la tarjeta Wireless, escribiendo en una consola:

 # iwconfig

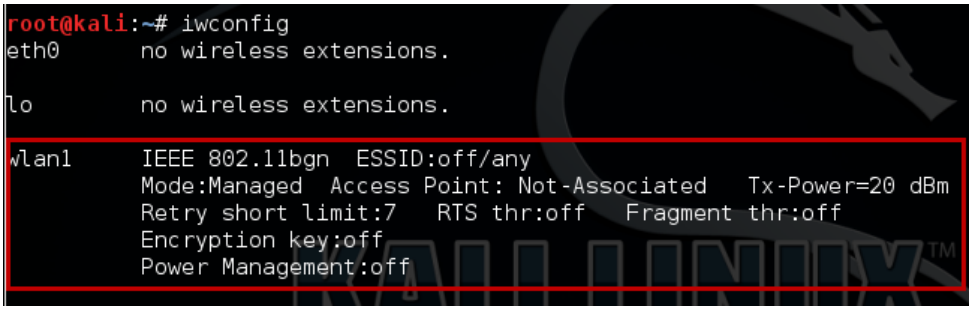


Ilustración 22 Identificación de la Interfaz inalámbrica

A continuación, se procede a poner la tarjeta en modo monitor, escribiendo en un terminal:

 # airmon-ng start wlan1

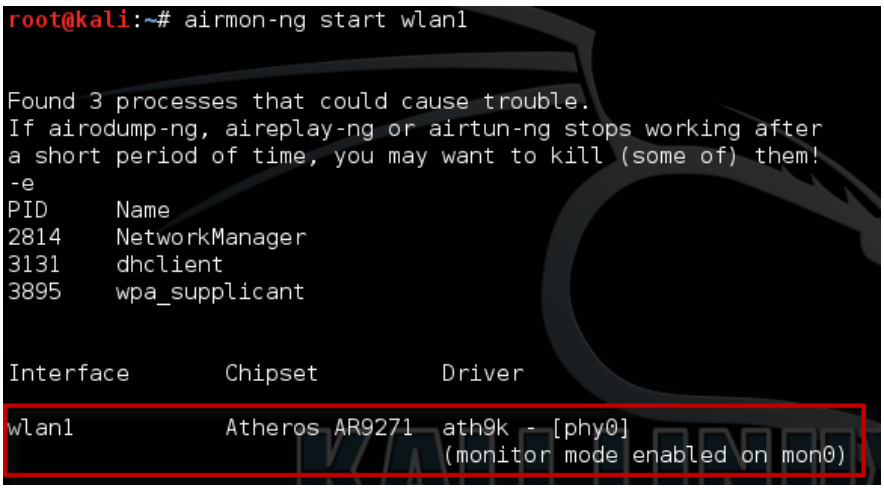


Ilustración 23 Tarjeta en modo monitor

Paso 2 - Iniciar airodump-ng para capturar los IVs

La finalidad de este paso es capturar IVs. Se iniciará airodump-ng para capturar los IVs del AP especificados.

Para ello, se abre una consola y se escribe

#airodump-ng –c 3 –bssid 00:1A:2B:3E:6F:A8 –w GCORTES mon0

Donde:

- -c 3 es el número del canal de la red Wireless
- --bssid 00:1A:2B:3E:6F:A8 es la dirección MAC del AP.
- -w GCORTES es el nombre del archivo en el que se guardarán los IVs.
- mon0 es el nombre de la interfaz colocada en modo monitor.

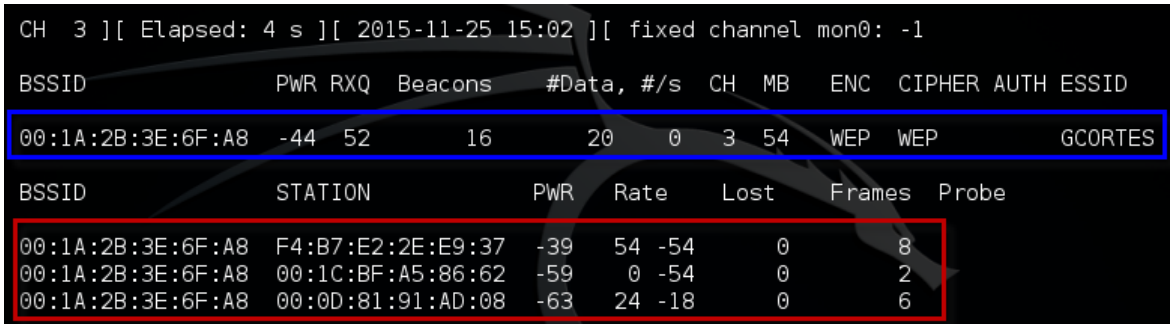


Ilustración 24 Identificación de la red.

Paso 3 - Usar aireplay-ng para hacer una falsa autenticación con el punto de acceso.

Para que el AP acepte cualquier paquete, la dirección MAC de origen del mismo debe estar previamente asociada con el AP o, de lo contrario, el AP ignorará los paquetes, enviando paquetes de "DeAuthenitcation". Por lo tanto, no se crearán nuevos IVs porque el AP está ignorando todos los paquetes inyectados.

Una de las razones principales por la que la inyección podría fallar es debido a la falta de asociación con el punto de acceso.

Para asociarse al punto de acceso, se utilizará la falsa autenticación. Por lo tanto, se abre otra consola y se escribe:

 # aireplay-ng -1 0 -e GCORTES –a 00:1A:2B:3E:6F:A8 –h C4:E9:84:DB:1E:C7 mon0

Donde:

- -1 significa falsa autenticación.
- 0 tiempo de reasociación, en segundos.
- -e GCORTES es el nombre de la red Wireless (BSSID).
- -a 00:1A:2B:3E:6F:A8 es la dirección MAC del AP.
- -h C4:E9:84:DB:1E:C7 es la dirección MAC de la tarjeta Wireless con la que estamos realizando la falsa autenticación.
- mon0 es el nombre de la interfaz que se encuentra en modo monitor.

Se obtendrá un mensaje indicando que la asociación se ha realizado correctamente.

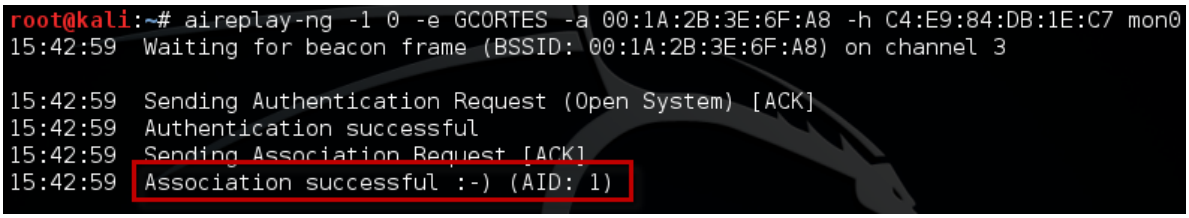


Ilustración 25 Falsa autenticación

También se puede ver que el equipo ya está asociado al AP:

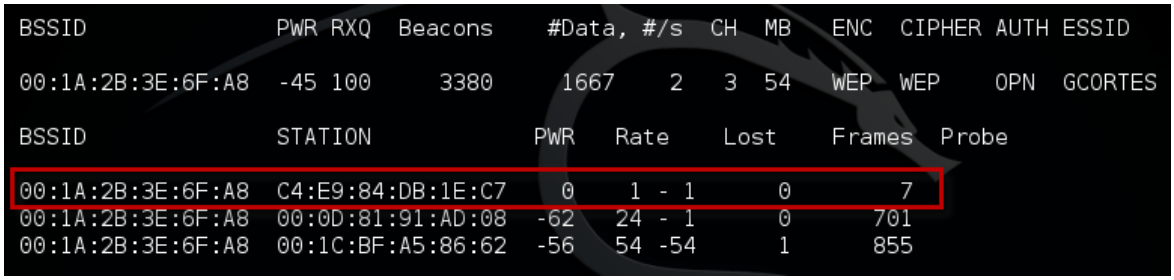


Ilustración 26 Dispositivo asociado al AP

Paso 4 - Iniciar aireplay-ng para inyectar paquetes de peticiones ARP

La finalidad de este paso es utilizar aireplay-ng para capturar peticiones ARP y, posteriormente, inyectarlas a la red. La razón por la que se escogen los paquetes ARP es porque el AP reenvía estos paquetes y con esto se consigue que se generen nuevos IVs. De esta forma se conseguirá un gran número de IVs en poco tiempo.

Se abre otra consola y se escribe:

#aireplay-ng -3 –b 00:1A:2B:3E:6F:A8 –h C4:E9:84:DB:1E:C7 mon0

Donde:

- -3 significa ataque de renvío de paquetes ARP.
- -b 00:1A:2B:3E:6F:A8 es la dirección MAC del AP.
- -h C4:E9:84:DB:1E:C7 es la dirección MAC de la tarjeta Wireless con la que se está realizando la falsa autenticación.

Empezará a escuchar las posibles peticiones ARP y cuando capture una, será inyectada mediante aireplay-ng.

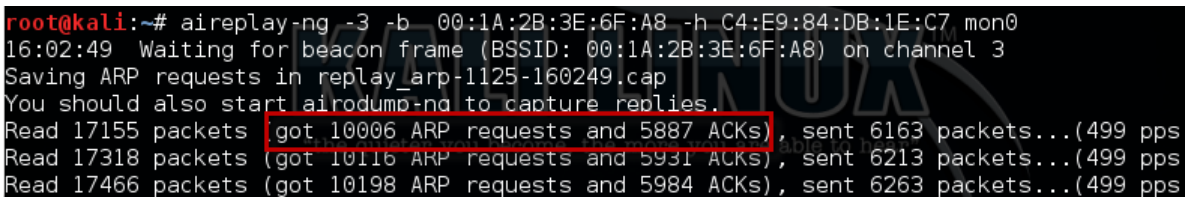


Ilustración 27 Inyección de paquetes

Se puede comprobar que se está inyectando revisando la pantalla de airodump-ng. Se observa que los paquetes de datos (data) incrementan de forma muy rápida. También se verá que el valor de la columna “#/s”, que indica el número de paquetes de datos por segundo, es elevado.

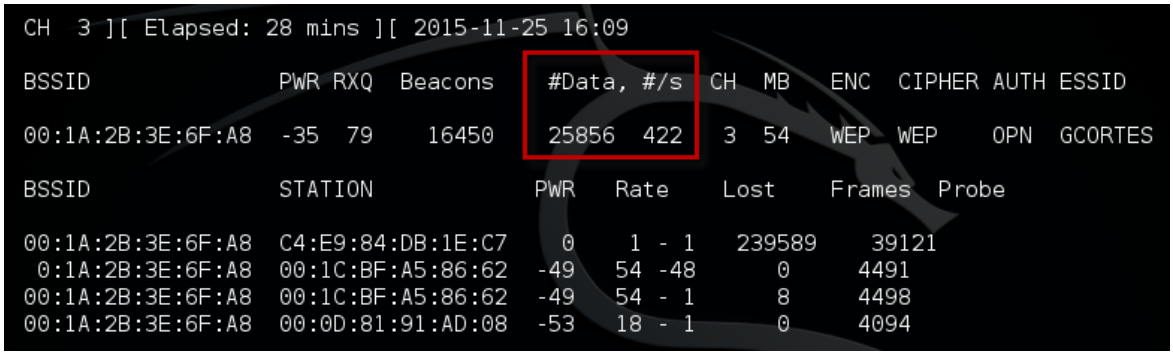


Ilustración 28 Captura de paquetes de datos

Paso 5 - Ejecutar aircrack-ng para obtener la clave WEP

El propósito de este paso es obtener la clave WEP a partir de los IVs guardados del paso anterior.

Se inicia otra consola y se escribe:

#aircrack-ng –b 00:1A:2B:3E:6F:A8 GCORTES-01.cap

Donde:

- -b 00:1A:2B:3E:6F:A8 es la dirección MAC del AP. Esto es opcional ya que al inicio del ataque ya se la he aplicado un filtro para tan solo capturar paquetes de este AP.
- GCORTES-01.cap es el archivo que analizará para obtener la clave WEP

En este proceso se irán analizando los paquetes IV obtenidos en el paso 1 y almacenados en el fichero GECOSU-01.cap.

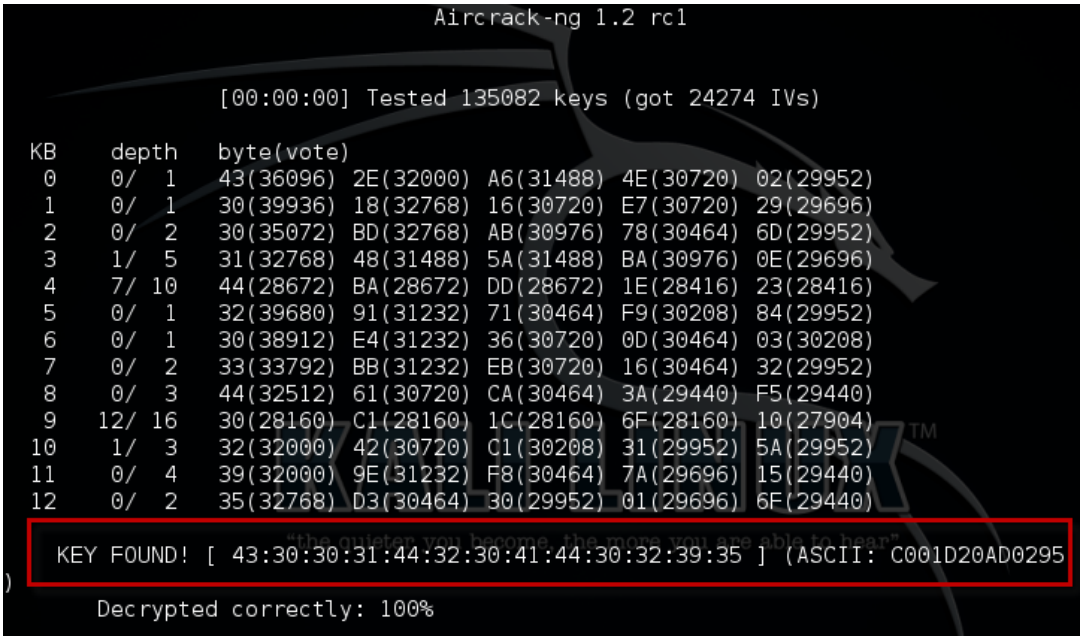


Ilustración 29 Obtención de la clave WEP

Por lo tanto, mediante este tipo de ataque, queda demostrado que el protocolo de seguridad WEP es totalmente vulnerable, siendo posible obtener la clave en pocos minutos.

6.4 Ataque WPA2 PSK

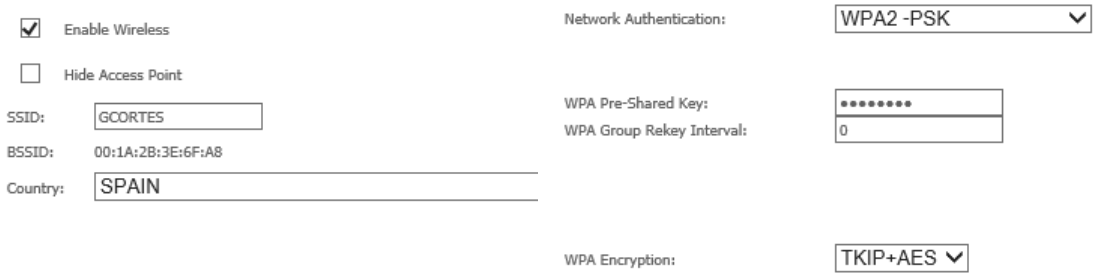
En este punto se obtendrá la clave WPA2 utilizando un sistema de clave compartida (WPA2-PSK).

Para obtener las claves de las redes inalámbricas con el protocolo de seguridad WEP se pueden utilizar métodos “estáticos” de inyección para acelerar el proceso. En cambio, WPA2 únicamente se pueden utilizar técnicas de fuerza bruta. Esto es debido a que la clave no es estática, por lo que capturando IVs como pasaba en la encriptación WEP, no se conseguirá obtener más rápidamente la clave. Lo único necesario para poder iniciar el ataque es el handshake entre el cliente y el AP. El handshake se genera en el momento que el cliente se conecta a la red a través del punto de acceso.

Por lo que, la única forma de obtener la clave es utilizando un diccionario. El hecho de tener que usar fuerza bruta es un inconveniente porque se hace un uso intenso del procesador del PC, limitando el número de claves por segundo a probar, dependiendo de la capacidad de la CPU. El proceso puede durar horas o días utilizando un diccionario adecuado.

El objetivo de este ataque es capturar el handshake WPA2 y, posteriormente, utilizarlo junto a “aircrack-ng” para obtener la clave pre-compartida. Para acelerar el proceso se desautenticará a un cliente Wireless. De lo contrario, nos deberíamos esperar a que un cliente se autentique en la red.

La configuración del router será la siguiente:



Paso 1 – Colocar la tarjeta Wireless en modo monitor

Colocar la tarjeta en modo monitor, para que pueda capturar cualquier paquete en el aire. De esta forma, en los próximos pasos será posible capturar los 4 paquetes que forman el handshake WPA/WPA2. Para ello escribimos en un terminal:

 # airmon-ng start wlan1

Paso 2 – Iniciar airodump-ng para capturar el handshake.

El objetivo de este paso es capturar los 4 paquetes que forman el handshake, en el momento que un cliente se autentica con el AP en el cual estamos realizando el ataque.

Para ello, se escribe en otro terminal:

 # airodump –c 3 --bssid 00:1A:2B:3E:6F:A8 -w WPA2 mon0

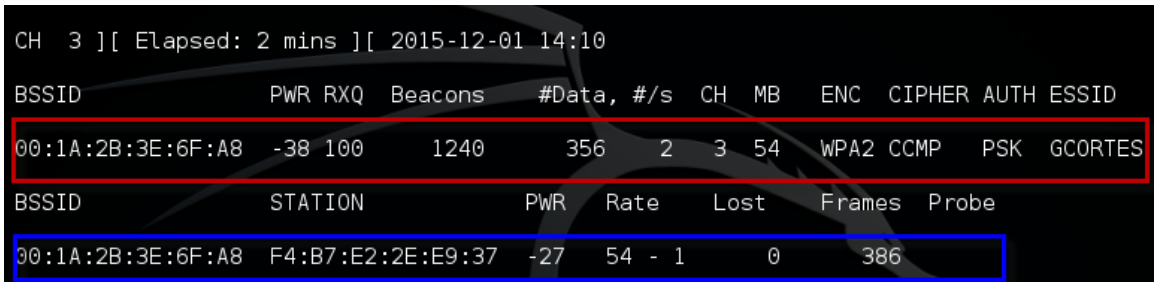


Ilustración 30 Identificación de la red

En la imagen, se puede observar con un recuadro rojo la información referente al punto de acceso. Con un recuadro azul se observa que hay un cliente conectado al AP.

Paso 3 - Usar aireplay-ng para deautentificar a un cliente conectado

Este paso es opcional, ya que se podría esperar a que un cliente se autentique al AP, para así conseguir su handshake. Pero para acelerar el proceso se ha optado por desautenticar a un cliente ya conectado al AP. Para ello, se enviará al cliente un mensaje con el fin de desasociarlo con el AP. De esta manera, el cliente se tendrá que reautenticar con el AP. Durante la reuntenticación se generarán los 4 paquetes de autenticación (handshake). Una vez, capturados estos paquetes serán utilizados para obtener, mediante un diccionario, la clave precompartida WPA

En otra terminal se escribe:

#aireplay-ng -0 1 –a 00:1A:2B:3E:6F:A8 –c F4:B7:E2:2E:E9:37 mon0

Donde:

- -0 significa desautenticación.
- 1 es el número de deautenticaciones enviadas. .
- -a 00:1A:2B:3E:6F:A8 es la dirección MAC del punto de acceso.
- -c F4:B7:E2:2E:E9:37 es la dirección MAC del cliente que vamos a desautenticar.
- mon0 es el nombre de la interfaz colocada en modo monitorización.

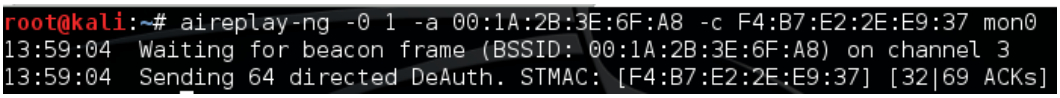


Ilustración 31 Desautenticación del cliente

En la imagen se puede observar que al volverse a autenticar el cliente se ha capturado el handshake.

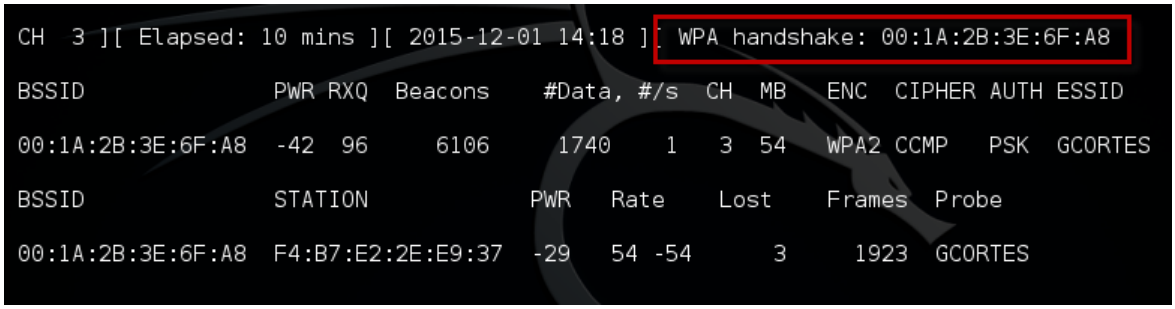


Ilustración 32 Captura del handshake

Paso 4 - Ejecutar aircrack-ng para obtener la clave pre-compartida

El objetivo de este paso es conseguir la clave WPA2-PSK. Para ello, ha sido necesario el uso de un diccionario. La utilidad de la herramienta aircrack-ng es comprobar cada una de las palabras contenidas en el diccionario para probar si coincide con la clave.

En otra consola se escribe:

#aircrack-ng –w wordlist.lst –b 00:1A:2B:3E:6F:A8 WPA2-01.cap

Donde:

- -w wordlist.lst es el nombre del archivo de diccionario.
- WPA2-01.cap es el nombre del archivo que contiene los paquetes capturados
- –b 00:1A:2B:3E:6F:A8 es la dirección MAC del AP.

Por último, la clave se incluya en el diccionario utilizado y, por lo tanto, el ataque ha tenido éxito.

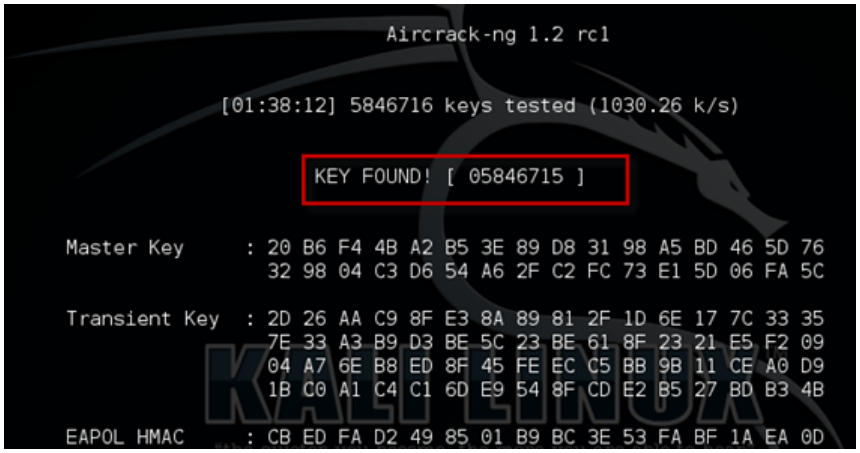


Ilustración 33 Obtención de la clave WPA

A diferencia del método utilizado para obtener la clave WEP, en este último, después de capturar el handshake, no hace falta que ningún cliente esté conectado al AP para aplicar la fuerza bruta, mediante diccionario.

Con este tipo de ataque queda demostrado que el protocolo de seguridad WPA2-PSK también puede ser vulnerado, sobre todo si se dispone de una contraseña poco segura. A diferencia del

ataque al protocolo WEP, en este tipo de ataque el éxito o fracaso del mismo dependerá de la complejidad de la contraseña y del tipo de diccionario utilizado.

6.5 Ataque al WPS

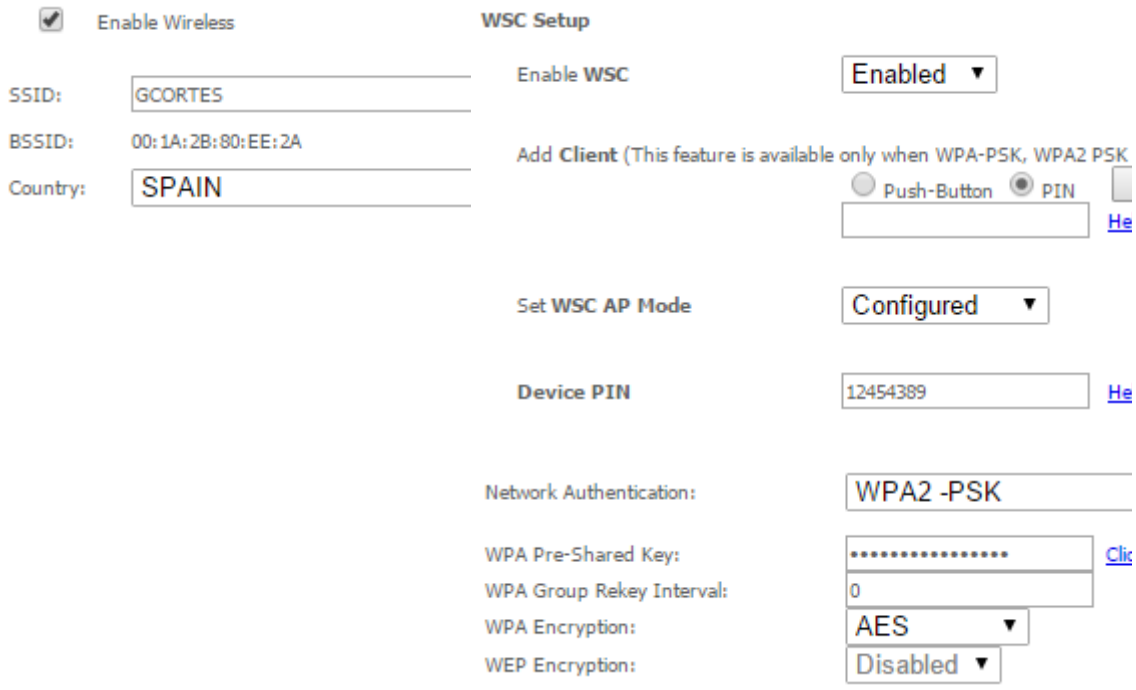
La idea de WPS no es la de añadir más seguridad a las redes WPA o WPA2, sino facilitar a los usuarios la configuración de la red, sin necesidad de utilizar complicadas claves o tediosos procesos.

El sistema de PIN de la tecnología WPS puede ser vulnerado en poco tiempo, debido a un error en el diseño del sistema WPS, por el que el AP "avisa" de que se está introduciendo el PIN incorrecto, tras solo comprobar los cuatro primeros dígitos de ese número de identificación personal de ocho bits.

Mediante un ataque por fuerza bruta, llevaría entre dos y diez horas descifrar los 8 números del PIN del WPS del AP, pues con ese error la seguridad pasa de 100.000.000 de posibilidades a solo 11.000, debido a que solo hay que "acertar" con dos grupos de números por separado: uno de cuatro y otro de tres, pues el último es solo un checksum.

Es importante remarcar que indistintamente del protocolo de seguridad utilizado; WEP, WPA/WPA2, la red inalámbrica seguirá siendo igual de vulnerable. También destacar que el PIN es generado automáticamente por el AP y no puede ser modificado por el usuario.

La configuración del router será la siguiente:



Paso 1 – Colocar la tarjeta Wireless en modo monitor

Colocar la tarjeta en modo monitor, para que pueda capturar cualquier paquete en el aire. Para ello se debe escribir en un terminal:

 # airmon-ng start wlan1

Paso 2 – Listar las redes que tienen WPS habilitado

Este paso tiene el objetivo de localizar las redes inalámbricas con la característica WPS habilitada, con lo que quiere decir que serán totalmente vulnerables al ataque.

Se ejecutará el siguiente comando en un terminal:

 # wash –i mon0

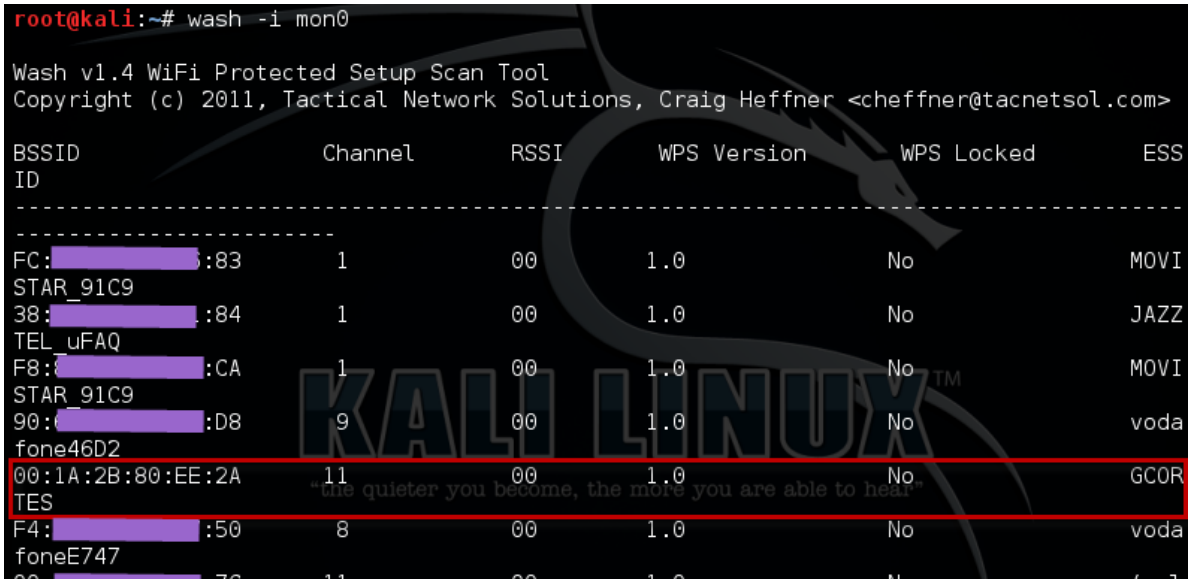


Ilustración 34 Detección de redes con WPS activado

Existen algunos modelos de AP que incorporan un mecanismo de seguridad que hacen se bloqueen cada cierto intento fallido de obtener el PIN, lo que haría mucho más difícil obtener la clave. Por ello, la columna" WPS Locked" nos advierte si el AP tiene el WPS bloqueado.

Paso 3 – Ejecutar reaver para obtener el PIN y la clave pre-compartida

Este último paso tiene como objetivo final iniciar el ataque, el cual no es por paquetes como en los casos anteriores (WEP y WPA). El sistema testeará todas las combinaciones posibles de un grupo de 8 dígitos.

Por lo tanto, en otro terminal se ejecutará:

 # reaver –i mon0 –b 00:1A:2B:80:EE:2A –c 11 –vv

Donde:

- -i mon0 es el nombre de la interfaz colocada en modo monitorización.
- -b 00:1A:2B:80:EE:2A es la dirección MAC del AP.

- - c 11 es el canal donde se encuentra el AP.
- -vv utilizado para mostrar más información durante el ataque.

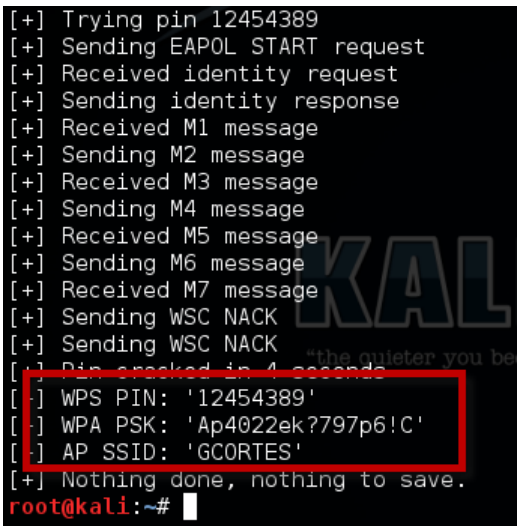


Ilustración 35 Obtención del PIN y la clave WPA

Finalmente, una vez obtenido el PIN, ejecutando el siguiente comando nos informará inmediatamente de la clave utilizada por el AP:

 # reaver –i mon0 –b 00:1A:2B:80:EE:2A –c 11 –vv –p 12454389

Donde:

- –p 12454389 es el PIN

En resumen, en este punto se ha podido demostrar que aunque se disponga de un buen protocolo de seguridad (WPA2-PSK con una contraseña compleja) configurado en la red inalámbrica si está en ella la tecnología WPS habilitada existirá un gran agujero de seguridad en la red, debido a la vulnerabilidad que presenta. Por lo tanto, la seguridad no depende de la complejidad de la contraseña sino en la propia tecnología WPS.

6.6 Valoración económica

A continuación, se mostrará una tabla indicando el coste que ha tenido la realización del caso práctico:

Nombre	Descripción	URL	Importe
KALI LINUX	Kali Linux 64 bits	https://www.kali.org	0 €
USB INALÁMBRICO	TP-LINK TL-WN722N USB	www.tp-link.com	15,95 €
DICCIONARIO	-	http://diccionariowpa.com/	0 €
PUNTO DE ACCESO	Comtrend C5813	http://www.comtrend.com	0 €
PORTATIL	HP ProBook 4540s	http://www.hp.es	625 €
SOFTWARE VIRUTALIZACIÓN	VirtualBox	https://www.virtualbox.org	0 €
		TOTAL	**640,90 €**

Tabla 8 Valoración económica

7. Políticas de seguridad

Para reducir los riesgos de seguridad a la hora de instalar una red inalámbrica se deben tomar ciertas medidas de seguridad. A continuación, se mencionan las más importantes:

- **No dejar la red inalámbrica abierta**, sin protección alguna. De esta forma, cualquiera que tenga la señal al alcance se podrá conectar, acceder a la información privada, además de reducir ancho de banda disponible en la conexión.
- **Apagar el AP en caso de que no se vaya a utilizar.** Esto reducirá las probabilidades de éxito de un ataque contra la red inalámbrica.
- **Cambiar la configuración por defecto del AP**. Cambiar los valores de fábrica de ESSID, usuarios y contraseñas que tiene el AP. Aunque también es fácilmente descifrable en unos pocos minutos, buscando por internet hay cientos de páginas que te proporcionan esta información.
- De las opciones de **encriptación**, elegir la **WPA2-PSK**, que es sin duda la más difícil y tediosa de atacar. En caso que sea posible, ya que algunos dispositivos no lo soportan, elegir el sistema de **cifrado AES**. Conviene también elegir una contraseña que no sea obvia.
- **Ocultar la red**, haciendo que el SSID no sea visible y tampoco "transmita beacon frames" para anunciarse. No es una medida de seguridad muy fuerte, pues existen programas que fácilmente las revelan, pero ayuda a complicar las cosas un poco más a quien tenga intención de acceder a nuestra red. El inconveniente es que para configurar nuevos dispositivos, deberá hacerse de forma manual.
- **Crear una lista de direcciones MAC permitidas**. Cada dispositivo con tarjeta de red inalámbrica, ya sea móvil, tablet u ordenador, tiene una dirección única que lo identifica .Con esa información, podemos crear una lista de dispositivos autorizados en nuestra red, para que ningún otro dispositivo se pueda conectar sin ser dado de alta esa dirección en la lista. Sin embargo, hay que tener en cuenta que un usuario avanzado con malas intenciones puede cambiar la MAC de su ordenador por una autorizada.
- **Habilitar Firewall en el router**. Algunos routers incorporan un firewall que evitarán intrusiones vía inalámbrica.
- **Limitar el número de conexiones del AP**, para que no haya más de las necesarias, así no admitirá nuevas conexiones.
- También es una buena opción **desactivar el DHCP**. De esta forma, cuando un dispositivo trate de conectarse a la red deberá tener una dirección IP, una máscara de subred y una dirección Gateway, que se deberán de asignar manualmente, con lo que las posibilidades de acertar con la IP son bajas.

- **No permitir la consola de administración en la WAN**: ni la consola de comandos vía Telnet o SSH. Dejar que solo alguien conectado a la LAN pueda configurar las características del dispositivo.
- Si es posible, **controlar la intensidad de la señal Wi-Fi** que emite el AP, de forma que se limitará su alcance tan sólo a la zona de cobertura deseada.

Aunque estas medidas de seguridad resultan insuficientes para el ámbito empresarial. En este caso, sería interesante aplicar también las siguientes medidas:

- Realizar una **segmentación de la red** en distintas VLANs (Virtual Local Area Network). De esta forma, se pueden tener los sistemas en una VLAN y el acceso a los clientes en otra VLAN distinta, de tal modo que no sean visibles entre sí. De esta forma, el tráfico de cada red inalámbrica viaja en forma aislada a través de la LAN corporativa y los usuarios de cada red solo tendrán acceso a los recursos
- Aunque la encriptación WPS2-PSK es bastante fuerte, en este caso es preferible utilizar **WPA2-EMPRESARIAL** debido a que funciona mediante el uso de usuario y contraseña o sistemas de certificados.
- **Disponer de un sistema de detección de intrusos inalámbricos** (WIDS, Intrusion Detection System), para saber qué está ocurriendo en la red inalámbrica y poder reaccionar ante posibles ataques.
- **Implementar herramientas de monitorización de red.** Ellas pueden alertar al administrador de la red en el caso de un tráfico de datos excesivos.

Tampoco se deberán olvidar las medidas de seguridad aplicadas sobre los dispositivos que utilizan los usuarios, debido a que estos también pueden ser un punto de ataque:

- **Limpiar la lista de puntos de acceso memorizados**. Conviene revisar la lista de puntos de acceso memorizados para eliminar aquellos esporádicos y dejar únicamente los realmente confiables.

  La mayoría de los dispositivos almacenan un listado de las redes a las cuales nos hemos conectado previamente, almacenando incluso las credenciales de acceso. Cada cierto intervalo de tiempo nuestra WiFi intenta conectarse de forma automática a cada una de las redes almacenadas, y es posible que nos encontremos formando parte de una red inalámbrica involuntariamente. Esto es debido a que para realizar su asociación con el punto de acceso tan solo se comprueba el nombre de la red (SSID) y el sistema de seguridad.
- **Disponer de Sistema antivirus**. Pueden ayudar a detectar y bloquear intentos de ataque a nuestro terminal.
- **Disponer de los últimos parches de seguridad**. Las aplicaciones y los servicios de los dispositivos pueden contener fallos de seguridad que un atacante podría utilizar para ganar acceso a nuestro equipo. Por lo tanto, las actualizaciones facilitadas periódicamente por los

fabricantes de software deben ser instaladas en cuanto estén disponibles, preferiblemente de manera automática.

- **Instalar Firewall en los dispositivos**. De esta forma se evitarán conexiones no deseadas, tanto hacia el dispositivo como desde el dispositivo.
- **Utilizar conexión VPN** (Virtual Private Networks) basadas en SSL o IPSec, siempre que sea posible. De este modo el tráfico que se genera viaja cifrado, dificultando que un tercero puede tener acceso a la información confidencial. El único inconveniente que este tipo de tecnologías protegen el tráfico en capas de comunicación superiores (nivel 3 en caso de IPSec y nivel 5 en el SSL), por lo que un atacante podría realizar ataques sobre capas inferiores (nivel 2).

8. Soluciones de seguridad Wi-Fi

A lo largo del apartado anterior se ha hablado de algunas soluciones que pueden ayudar a mantener las redes Wi-Fi seguras, como pueden ser los estándares de seguridad: WEP, WPA, WPA2 y autenticación 802.1x. En cambio, en este capítulo se hablarán sobre otras soluciones de seguridad que deberían tenerse en cuenta a la hora de desplegar una red inalámbrica en el ámbito empresarial,

8.1 Controlador de puntos de acceso

El uso de un controlador de puntos de acceso, no solo facilita la gestión y mantenimiento de una red Wi-Fi, si no que puede servir así mismo para aumentar su seguridad. Las posibilidades que proporciona un controlador dependerán del fabricante y modelo, pues no hay un estándar, siendo algunas de las más interesantes:

- **Firewall**: Es habitual que los controladores implementen funcionalidades de firewall, que permitan controlar el tráfico que pasa de la red cableada a la red Wi-Fi, en base a direcciones de origen o destino, aplicaciones, servicios, etc. El firewall es también un elemento importante en la defensa ante ataques DoS

- **Comunicación por túnel**: Dentro de ese túnel se transmitirá el tráfico de los clientes desde el punto de acceso al controlador. Esto permite que los clientes Wi-Fi inseguros no tengan acceso a la red directamente, si no que todo el tráfico deberá pasar por el controlador, el cual, según las políticas asignadas a cada tráfico por la funcionalidad de firewall en éste incluida, denegará o permitirá el acceso a partes o toda la red. La tunelización del tráfico también proporciona la posibilidad de que los puntos de acceso estén conectados a segmentos de red diferentes, ya que de este modo el tráfico de los clientes siempre accederá a la red por el mismo punto de ésta, aquel al que esté conectado el controlador. Además, si el túnel se realiza con un protocolo seguro como SSL, la comunicación entre los puntos de acceso y el consolador podrá hacerse a través de redes de terceros o incluso Internet, lo que permite la extensión de la red inalámbrica a zonas remotas atravesando redes inseguras sin exponer el trafico propio.

- **Gestión por usuario:** En conjunción con un servidor de autentificación será posible asignar diferentes accesos a los usuarios en función de sus credenciales, de una manera más detallada y compleja que si el proceso lo llevara a cabo el punto de acceso. Así pues podrán asignarse a diversas redes, concederles accesos a diferentes servicios, etc.

- **Gestión del ancho de banda**: El controlador podrá ofrecer una funcionalidad por la cual regulará el ancho de banda disponible en función de la aplicación o usuario que desee hacer uso de ella.

- **Localización espacial**: Un controlador puede ofrecer un servicio de localización. Puesto que tiene control de los diferentes puntos de acceso, puede monitorizar los clientes y la potencia de recepción de estos por cada uno de los puntos de acceso. Si el Controlador tiene conocimiento

de la situación espacial de los puntos de acceso, triangulando la posición con respecto a los distintos puntos de acceso en base a la potencia recibida por estos, podrá obtener la posición del cliente.

- **Limitación física del alcance de la red:** Un controlador podrá denegar el acceso a la red a aquellos equipos cuya red se encuentre fuera de los límites de aquello que se le indique como zona de cobertura. Es de indicar que con este método los clientes fuera de la zona de cobertura de la red seguirán recibiendo la señal, con lo que podrían intentar otros medios de ataque a esta si la encriptación no es adecuada, pero no podrán conectarse a la red.

8.2 WIPS (Wireless Intrusion Prevention System)

Un WIPS es un conjunto de equipos de red que tienen como objetivo prevenir y detectar intrusiones en la red Wi-Fi.

Un sistema WIPS se compone de tres parte lógicas: los sensores que recogerán los datos de la red, el servidor que recolectará los datos de los distintos sensores, los analizara y relacionará, y la consola que utilizará el personal encargado de la seguridad de la red para acceder a los datos y visualizar las alarmas. Estos tres bloques lógicos no siempre están separados físicamente, pues es habitual que el servidor implemente un servidor WEB que sea el utilizado para acceder a sus datos y configuraciones a través de un navegador. En algunos sistemas WIPS está incluida en el controlador de puntos de acceso, que hará la función de servidor, que en conjunción con los puntos de acceso, que harán las funciones de sensores, pueden llevar a cabo parte de las funciones que realizaría un WIPS dedicado.

Ilustración 36 Solución WIPS

Un WIPS monitoriza el espectro radioeléctrico de la red Wi-Fi con el objeto de detectar ataques de diversa índole, como pueden ser:

- **Puntos de acceso infiltrados**: El WIPS puede detectar puntos de acceso infiltrados, usando técnicas simples como un conteo de los puntos de acceso que detecta, hasta algunas más

complejas que implican relacionar la dirección MAC de cada punto con la potencia que de ellos recibe. En caso de que se reciba información de la misma MAC con una potencia diferente, significaría que o bien se ha cambiado de localización el punto de acceso, lo cual no suele ser habitual, o que un nuevo punto de acceso, en una localización diferente, ha intentado suplantar al equipo legal. Una vez detectado el equipo infiltrado el WIPS lo notificará al administrador de la red, y en algunos sistemas permitirá habilitar contramedidas que bloqueen al punto de acceso infiltrado.

- **Puntos de acceso mal configurados**: Puede detectar conversaciones entre puntos de acceso y los clientes, detectando parámetros y configuraciones erróneas. También, mediante la información emitida en los paquetes de beacon puede avisar de fallos en la configuración de puntos de acceso.

- **Clientes mal configurados**: Un cliente cuyos intentos de conexión a la red sean denegados de forma repetitiva, será detectado como un fallo de configuración de dicho cliente o como el intento de conexión de un atacante que provocara muchos intentos de conexión denegados por la red.

- **Conexiones no autorizadas**: WIPS tiene una lista de los clientes autorizados, podrá detectar la conexión de los clientes no autorizado.

- **Redes ad-hoc**: una red ad-hoc puede ser un punto de vulnerabilidad importante. Una red ad-hoc, puede ser creada involuntariamente, por un error de configuración, un troyano, etc. lo que crea un agujero de seguridad. El WIPS, mediante la monitorización de los canales Wi-Fi, podrá detectar este tipo de redes y asociaciones, pudiendo indicar así mismo el equipo que crea dicha red y que está creando la vulnerabilidad.

Un WIPS también podrá detectar ataques como pueden ser: MAC spoofing, honeypot, Man-in-the-Middle

Algunos fabricantes de este tipo de soluciones pueden ser: AirTight Networks, Aruba Networks, Cisco, Fluke Networks, Meraki, Motorola.

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki			x		
Motorola				x	

Ilustración 37 Calificación soluciones WIPS

8.3 Portal cautivo

Un portal cautivo es una aplicación utilizada generalmente en redes inalámbricas abiertas para controlar el acceso a la misma, aunque también puede utilizarse en redes cableadas. Por un lado, se utiliza para presentar al usuario alguna información de interés (información corporativa, políticas de uso, etc.) y por otro le permite al usuario facilitar al sistema sus credenciales de acceso.

Cuando un usuario, una vez seleccionada la red WIFI y establecida la conexión inalámbrica, intenta acceder a una página web utilizando cualquier navegador, el portal cautivo captura esta solicitud y en lugar de la página solicitada le presenta al usuario la página de registro al sistema, bloqueando cualquier otro tipo de tráfico. Una vez que el usuario introduce sus datos y estos son comprobados se le permite el acceso a la red facilitándole la página web inicialmente solicitada.

Normalmente un portal cautivo consta de dos partes: una puerta de enlace (gateway) y un servidor de autenticación. El gateway gestiona las reglas de cortafuegos, denegando el acceso a la red a los usuarios no identificados y estableciendo qué puertos y protocolos están permitidos a los usuarios autorizados. El gateway se conecta con el servidor de autenticación que realiza la comprobación de los datos de usuario, bien utilizando una base de datos local o consultando a un servidor RADIUS, para permitir o denegar el acceso a la red, así como asignar algunas restricciones como un límite de tiempo o un ancho de banda determinado.

Un portal cautivo puede instalarse en un ordenador que actúe como router o bien, si no necesita demasiado espacio de almacenamiento y capacidad de procesamiento, en un router hardware con firmware basado en Linux (como por ejemplo alguno de los modelos WRT54G de Linksys).

Entre los distintos sistemas de portal cautivo con software libre podemos señalar NoCat, Wifidog, Chillispot, ZeroShell, etc.

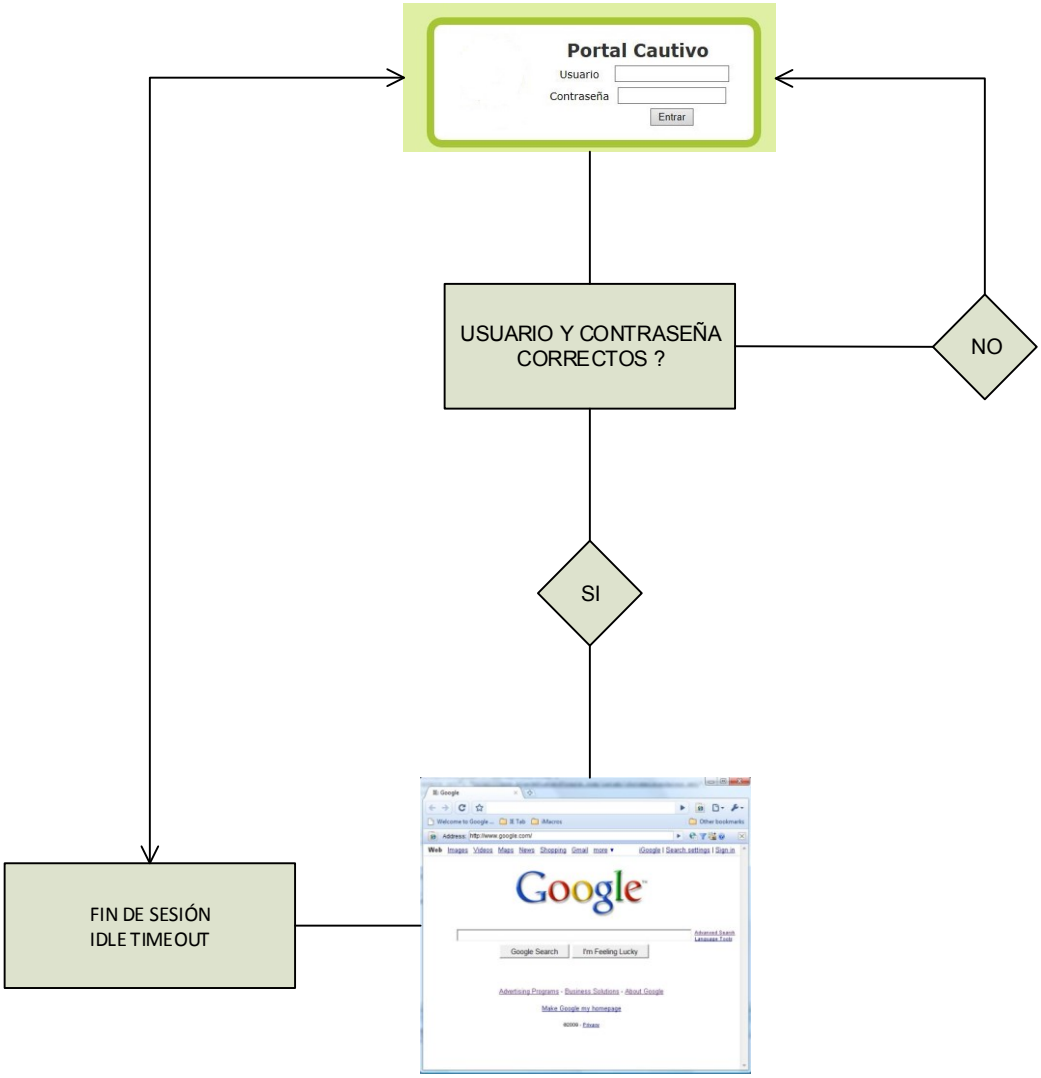


Ilustración 38 Proceso conexión al portal cautivo

8.4 Servidores RADIUS

RADIUS es un servidor de punto final responsable de recibir solicitudes de conexiones y de la autenticación de los usuarios. Este servidor desempeña la autenticación utilizando EAP. Una de las principales características es la capacidad de manejar sesiones, notificando el inicio y el final de una conexión, pudiendo utilizar estos valores para generar estadísticas.

Actualmente, existen muchos tipos de servidores RADIUS, tanto comerciales como de código abierto. Algunos de ellos pueden ser: freeradius, tekradius, zeroshell, pfsense. routerOS

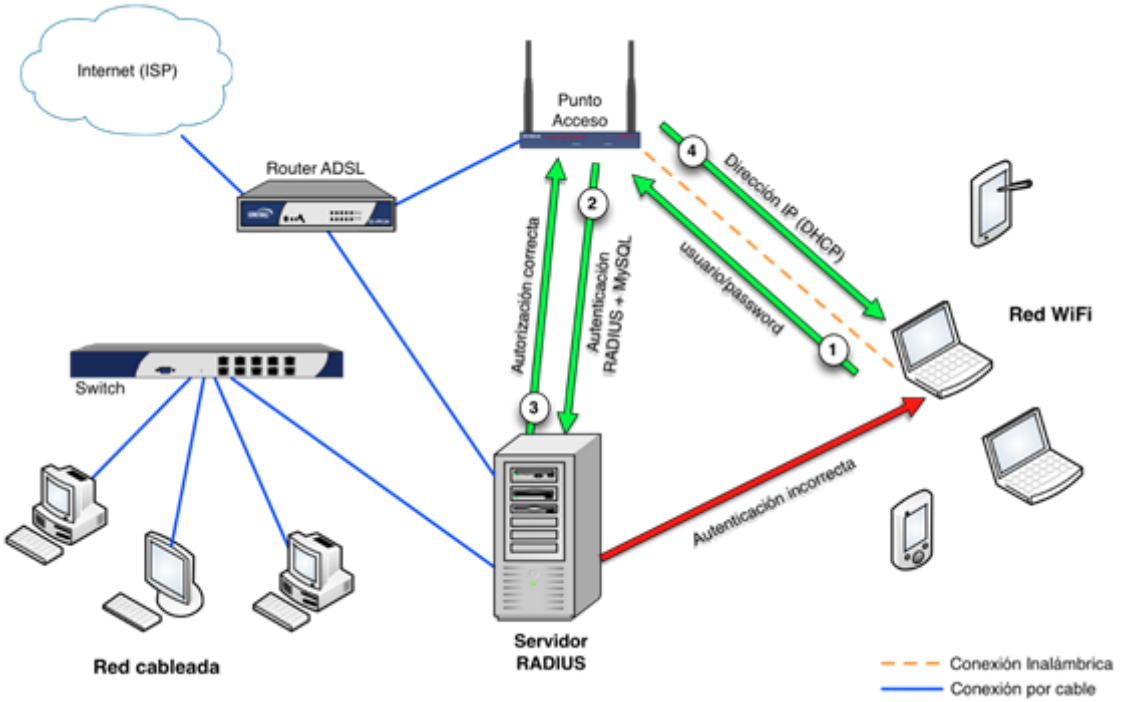


Ilustración 39 Ejemplo esquema RADIUS

9. Glosario de términos y abreviaturas

AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution protocol
ARPANET	Advanced Research Projects Agency Network
BSS	Basic Service Set
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DHCP	Dynamic Host Configuration Protocol
DS	Distribution System
DSSS	Direct-sequence spread spectrum
EAP	Extensible Authentication Protocol
ELF	Extremely Low Frequency
ESS	Extended Service Set
ESSID	Extended Service Set ID
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTK	Group Temporal Key
PTK	Pairwise Transient Key
HSDPA	High Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
IBSS	Independent Basic service Set
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol security
ISM	Industrial Scientific and Medical
IV	Initialization Vector
LMDS	Local Multipoint Distribution Service
LTE	Long Term Evolution
MAC	Media Access Control
MIC	Message Integrity Code
MIMO	Multiple-input Multiple-output
MITM	man-in-the-middle

NACK	Negative-Acknowledgement
NFC	Near field communication
OSI	Open System Interconnection
PBC	Push Bottom Configuration
PEAP	Protected Extensible Authentication Protocol
PHY	Physical Layer
PIN	Personal Identification Number
PSK	pre-shared key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
SSH	Secure SHell
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIMAX	Worldwide Interoperability for Microwave Access
WIPS	wireless intrusion prevention system
WLAN	wireless local area network
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WPS	Wi-Fi Protected Setup
WWAN	Wireless Wide Area Network
XOR	OR Exclusive

10. Bibliografía

10.1 Libros

Roldan Martínez, D; Huidobro Moya, J. M. (2006). **Comunicaciones en redes WLAN.** Ed Creaciones Copyright.

Neil, R; Ron, S. (2003). **Manual de redes inalámbricas**. Ed McGraw-Hill.

Gómez López, J. (2008). **Guía de campo Wi-Fi**. Ed RA-MA

Carballar. J. A. (2007). Wi-Fi: **Instalación, Seguridad y Aplicaciones**. Ed RA-MA

Carballar, J.A. (2010). Wi-Fi: **Lo que necesita conocer**. Ed Grupo RC

10.2 Artículos

Guillaume Lehembre, Seguridad Wi-Fi – WEP, WPA y WPA2. Hakin9. (1/2006). http://www.hakin9.org

10.3 Páginas Web

https://es.wikipedia.org/wiki/Wifi

https://ieeesbc.wordpress.com/¿que-es-la-ieee/

https://es.wikipedia.org/wiki/IEEE_802.11

http://www.aircrack-ng.org/

https://www.kali.org/

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

http://www.criptored.upm.es/intypedia/video.php?id=introduccion-seguridad-wifi

http://lasinformaticas2012.blogspot.com.es

http://fundamentofficial.blogspot.com.es/2014/07/redes-inalambricas-wifi.html

http://seguridad-en-redes-wifi.weebly.com

http://highsec.es/2013/09/atacando-wep-sin-ap-o-ataque-caffe-latte/

https://code.google.com/p/reaver-wps/wiki/README

http://www.seguridadparatodos.es/2012/01/vulnerabilidad-en-el-protocolo-wifi.html

http://jose-linares.com/acceder-al-wifi-ajeno-gracias-a-una-vulnerabilidad-en-wps/

http://www.wi-fi.org/

http://www.dd-wrt.com