

UNIDAD 9

Despliegue de redes inalámbricas

1. Redes inalámbricas WLAN

1.1. ¿Qué son redes inalámbricas WLAN?

Una red de área local inalámbrica WLAN (*Wireless Local Area Network*) o red de área local sin hilos es una red de dispositivos que, como medio de transmisión, utiliza radiofrecuencia o rayos infrarrojos en lugar de par trenzado, cable coaxial o fibra óptica.

La radiofrecuencia ha desplazado a los rayos infrarrojos como medio de transporte, principalmente, debido a su mayor alcance y ancho de banda.

La no utilización de medios guiados (cables) permite extender la red local a puntos de difícil acceso y dar servicio a un mayor número de usuarios, como se necesita, por ejemplo, en un establecimiento público.

El IEEE (*Institute of Electrical and Electronic Engineers*) o Instituto de Ingenieros Eléctricos y Electrónicos establece en el grupo de documentos 802.11 las especificaciones y los estándares para las redes locales inalámbricas.

En el año 2000, el consorcio WECA (*Wireless Ethernet Compatibility Alliance*) o alianza de compatibilidad de redes de área local inalámbricas, formado por un grupo de fabricantes de dispositivos de telecomunicaciones, creó la certificación Wi-Fi, basada en el estándar IEEE 802.11, que indica que todos los dispositivos que poseen esta certificación pueden trabajar entre sí sin problemas de compatibilidad.

Actualmente, WECA se conoce como *Wi-Fi Alliance* a la que pertenecen más de 375 compañías y posee una certificación para cada estándar IEEE 802.11.

Vocabulario

Espectro electromagnético: es la distribución de energética del conjunto de las ondas electromagnéticas.

RF o radio frecuencia: es la zona del espectro electromagnético que se sitúa entre los 3 KHz y los 300 GHz.

Microondas: reciben este calificativo las ondas cuya frecuencia se encuentra entre 1 y 300 GHz.

1.2. Estándares WLAN

Los estándares 802.11 permiten la implementación de redes WLAN en las bandas de frecuencia de 2,4; 3,6 y 5 GHz y definen un conjunto de componentes físicos y lógicos, modos de operación y protocolos que abarcan la capa física y la de acceso al medio:

- En la primera capa se definen, entre otros conceptos, las frecuencias que se deben utilizar, la potencia de emisión, las velocidades de transmisión, etc.
- En la capa de acceso al medio se especifican la estructura de la trama, el establecimiento del enlace, etc.

Una característica importante es que este estándar permite la compatibilidad con las redes de área

local Ethernet (IEEE 802.3). De este modo se pueden tener redes locales mixtas.

A partir de su creación, en 1997, ha experimentado múltiples mejoras. La mayoría de las actualizaciones son compatibles con las versiones anteriores, siempre y cuando operen en la misma banda de frecuencias. El único inconveniente que presenta esta retrocompatibilidad es que, si dentro de un sistema existen diferentes estándares, la velocidad de transferencia máxima de la red fija siempre el dispositivo de menor velocidad.

Las características de los principales estándares se detallan a continuación:

Estándares WLAN más utilizados					
Estándar	Año	Frecuencia de trabajo	Velocidad máxima	Alcance en interior	Alcance en el exterior
802.11 legacy	1997	2,4 GHz	2 Mb/s	20 m	100 m
802.11a	1999	5,7 GHz	11 Mb/s	35 m	120 m
802.11b	1999	2,4 GHz	11 Mb/s	38 m	140 m
802.11g	2003	2,4 GHz	54 Mb/s	38 m	140 m
802.11n	2009	2,4 y 5 GHz	Superior a 300 Mb/s	70 m	250 m
802.11ac	2014	5 GHz	1300 Mb/s	50 m	130 m

El estándar 802.11n, al trabajar en las dos bandas de frecuencia, es compatible con todos los estándares anteriores. En la actualidad, el 802.11g puede operar a velocidades superiores gracias a nuevas técnicas de compresión, se le conoce como Pre-N y alcanza 108 Mb/s.

La especificación IEEE 802.11i se creó para mejorar la seguridad en los protocolos de autenticación y de codificación de los estándares anteriores. Incluye los protocolos TKIP (*Temporal Key Integrity Protocol*) o estándar de cifrado avanzado. Se implementa en WPA2 o *Wi-Fi Protected Access* (acceso Wi-Fi protegido).

MIMO

MIMO (*Multiple-Input Multiple-Output*) o multiple entrada multiple salida indica que el dispositivo permite el uso de más de una antena de transmisión o recepción para aumentar la tasa de transferencia de información.

El estándar IEEE 802.11n permite, utilizando esta tecnología, velocidades teóricas de hasta 600 Mb/s.

Itinerancia o roaming

Es la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

En una red inalámbrica, es la capacidad de un cliente para conectarse a diferentes AP. Para conseguirlo, las zonas de cobertura de los AP deben tener una pequeña superposición.

1.3. Componentes WLAN

Los dispositivos inalámbricos se pueden dividir en tres grupos:

- Distribución: puntos de acceso y equipos mixtos.
- Adaptadores de red inalámbrica o tarjetas de red: WNIC.
- Antenas.

Punto de acceso (AP)

Un punto de acceso (AP) es un dispositivo que puede actuar como punto central de una red inalámbrica independiente. Tiene una dirección IP que permite configurarlo y su función principal es proveer a los clientes de acceso a la red inalámbrica. Las funciones de enrutamiento y

direccionalidad las suele delegar en servidores (routers).

También permite conectar redes sin hilos y cableadas, realizando la función de *bridge* o puente de red.

La capacidad de *roaming* o itinerancia que poseen los puntos de acceso permite interconectarlos entre sí y ampliar el área de cobertura de la WLAN. De esa manera, un usuario podrá moverse en la zona de cobertura sin notar pérdidas de calidad de la señal.

Una de sus principales limitaciones es que no puede administrar un número muy elevado de conexiones de manera simultánea. Un punto de acceso estándar puede soportar alrededor de 30 conexiones en un radio máximo de unos 100 metros.

Los puntos de acceso trabajan con las direcciones físicas o MAC de los dispositivos.

Equipos mixtos

Un equipo mixto es un dispositivo que centraliza las funciones del router, el switch y el punto de acceso.

Los equipos mixtos son adecuados para instalaciones domésticas o para empresa SoHo (*Small office-Home office*) o pequeña oficina-oficina en casa, ya que no se necesita una gran extensión geográfica ni un número elevado de clientes. Puesto que disponen de un equipo que realiza todas las funciones, se abaratan los costes de instalación y mantenimiento.

Adaptadores de red inalámbrica o tarjetas de red (WNIC)

Estos adaptadores, dependiendo de su punto de interconexión con el dispositivo, pueden dividirse en lo siguiente:

- **Adaptadores integrados:** van incluidos en la placa del dispositivo. Los adaptadores de portátiles, las tabletas, las consolas y los *smartphones* suelen ir equipados con un adaptador integrado.
- **Tarjetas PCI:** se conectan a un puerto PCI libre de un ordenador personal. Poseen una antena externa que puede ser sustituida por una de mayor potencia.
- **Adaptadores USB:** son dispositivos inalámbricos externos al ordenador que se conecta a un puerto USB libre. Su instalación es muy sencilla ya que el puerto USB es *Plug&Play* y, por lo tanto, el ordenador normalmente lo detecta de manera automática. También pueden cambiarse de equipo de forma rápida para adecuar las necesidades inalámbricas de la red.

Antenas

Una antena es un hilo de material conductor que permite emitir o recibir ondas electromagnéticas. Su funcionamiento se basa en el principio de inducción electromagnética, según el cual toda corriente eléctrica alterna que circule por un conductor inducirá un campo electromagnético asociado. A su vez, todo campo electromagnético que incide sobre un conductor inducirá una corriente eléctrica.

La dimensión de las antenas está directamente relacionada con la longitud de onda de las frecuencias para las que han sido diseñadas.

Estos son algunos de los parámetros que caracterizan a las antenas:

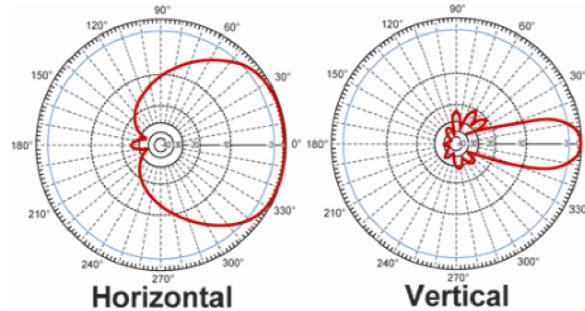
- **Diagrama de radiación:** es la representación gráfica de la potencia de radiación de la antena en función de su dirección. Dependiendo de su diagrama de radiación podremos clasificar

las antenas en diferentes tipos:

- **Isotrópica:** es una antena teórica que emite la misma potencia de radiación en todas las direcciones. Su diagrama de radiación es una esfera perfecta.
- **Omnidireccional:** es una antena que radia la misma cantidad de potencia en todas las direcciones de un plano de emisión. Su diagrama de radiación sería un toroide. Son las más utilizadas en las redes WLAN, ya que cubren de manera uniforme toda la superficie en la que se debe dar servicio inalámbrico.
- **Direccional:** es una antena que emite la máxima potencia en una dirección determinada. Suelen utilizarse para crear uniones punto a punto o conectar zonas muy alejadas. Se subdividen en:
 - Unidireccionales: emiten la potencia en un solo sentido.
 - Bidireccionales: reparten la potencia en los dos sentidos de la dirección.



- **Sectorial:** es una antena que emite su máxima potencia en un sector determinado. Suelen utilizarse en redes urbanas. Pueden cubrir sectores de 120°, 60°, etc.



Si realizamos una sección en el diagrama de radiación siguiendo el plano horizontal (XY), podremos comparar la potencia de radiación de diferentes antenas.

- **Ganancia:** es el incremento de potencia de una antena en la dirección de máxima radiación en relación con una antena modelo. Puede medirse en dBi (decibelios respecto a una antena isotrópica) o dBd (decibelios respecto a un dipolo), dependiendo de la antena usada como referencia. Un dipolo posee un diagrama de radiación omnidireccional. Si el resultado es positivo, indica mayor potencia de radiación que el modelo; si, por el contrario, el resultado es negativo, indica menor potencia de radiación.
- **Ancho de banda:** son las bandas de frecuencia en las cuales trabaja la antena de manera óptima.
- **Eficiencia:** es la relación entre la potencia emitida por la antena y la que le es suministrada

por el equipo transmisor. Cuanto mayor sea la eficiencia menor será la cantidad de potencia que se perderá en forma de calor.

Leyes de la radiodinámica

Las limitaciones físicas de las redes inalámbricas están implícitas en las **leyes de la radio dinámica**:

- Un aumento de la velocidad equivale a una disminución del alcance de la transmisión.
- Un aumento de la potencia equivale a incrementar el alcance o cobertura, pero reduce la vida de la batería.
- Un aumento de la frecuencia de radio equivale a un aumento de la velocidad, pero una disminución del alcance.

Conversión dBi-dBd

Si los fabricantes expresan la ganancia (potencia) de sus antenas en dBi, para obtener el dBd hay que aplicar esta fórmula aproximada:

$$G_{dBd} = G_{dBi} - 2,15$$

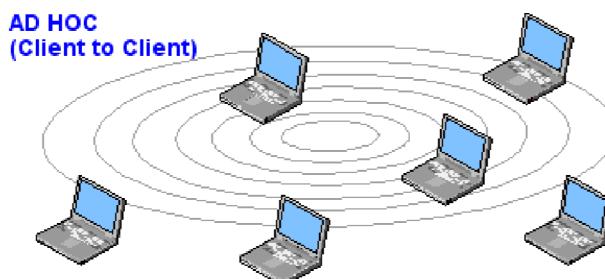
1.4. Modos de operación

El estándar IEEE 802.11 define dos modos de operación: *ad hoc* e infraestructura. Estos dos modos definen dos redes WLAN diferentes.

Redes *ad hoc*

Una red *ad hoc* es una red inalámbrica descentralizada. En ella todos los equipos están conectados sin necesidad de un nodo central que realice las funciones de router. Este tipo de redes no necesita ni puntos de acceso ni dispositivos mixtos; cada equipo actúa como punto de acceso y cliente inalámbrico.

Se crean cuando es necesario unir de forma ocasional dos o más equipos permitiéndoles compartir recursos. Debido a su sencillez y rápida configuración también son adecuadas para situaciones de emergencia en las cuales no podemos confiar en un nodo central, como desastres naturales, conflictos bélicos, etc.



Roles de funcionamiento de un AP

Recuerda, un AP puede trabajar dentro de una WLAN como:

- Nodo central de la red.
- Puente o *bridge* entre dos redes.
- Repetidor para permitir la ampliación de la zona de cobertura de la red.

Redes en infraestructura

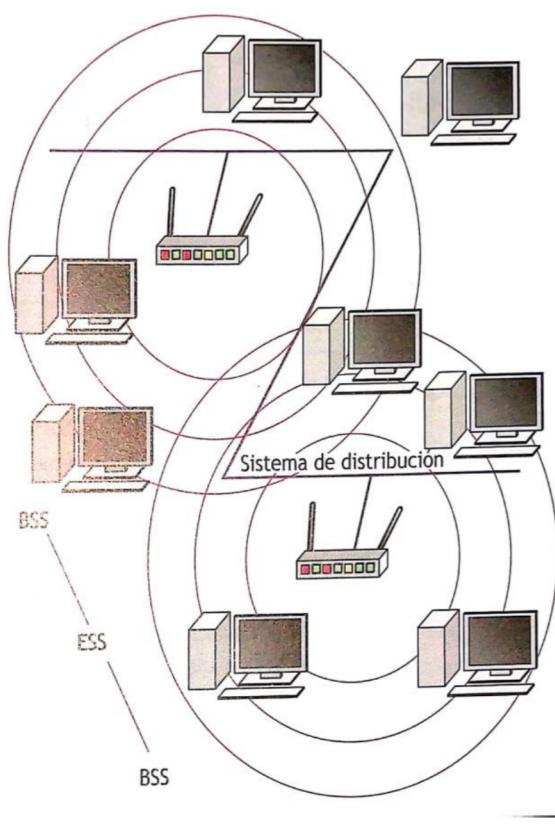
Estas redes son aquellas en las cuales los dispositivos se conectan a la red mediante puntos de acceso. Añadiendo AP adicionales se aumentará el alcance de la red y el número de usuarios.

Frente a las redes *ad hoc*, ofrecen una mejor escalabilidad, así como un sistema de seguridad centralizado.

1.5. Componentes lógicos

Algunos de los componentes lógicos que encontramos en una WLAN son:

- **BSS (*Basic Service Set*) o conjunto básico de servicios:** es el elemento básico de construcción de una red LAN inalámbrica IEEE 802.11. En el modo infraestructura, está compuesto por un único AP y las estaciones asociadas, el resto de dispositivos inalámbricos y los servicios que comparten. No se debe confundir con el término BSA (*Basic Service Area*) o área de servicio básico, que corresponde a la zona de cobertura del AP.
- **IBSS (*Independent Basic Service Set*) o conjunto básico de servicios independiente:** si la red está creada siguiendo una estructura *ad hoc*, el BSS recibe este nombre.



- **BSSID (*Basic Service Set Identifier*) o identificación del conjunto de servicios básicos:** cada BSS se identifica con un único BSSID. Para redes en modo infraestructura, el BSSID es la dirección MAC del AP; para redes en modo *ad hoc* es un número aleatorio.
- **ESS (*Extended Service Set*) o conjunto de servicios extendidos:** es un conjunto de dos o más BSS que permiten dar servicios comunes y comportarse como una única WLAN. Los puntos de acceso o BSS se conectan a través de un sistema de distribución o SD. Este sistema puede ser o bien un cable o bien una conexión inalámbrica.
- **SSID (*Service Set Identifier*) o identificador del conjunto de servicios:** es el nombre de la WLAN. Está compuesto por 32 dígitos alfanuméricos, como máximo, y lo utilizan los usuarios para identificarse y conectarse a la red. En WLAN con más de un AP (ESS) todos los puntos de acceso deberán tener el mismo SSID. Recibirá el nombre de ESSID (*Extended SSID*) o SSID extendido.

1.6. Seguridad

Uno de los principales problemas en las redes inalámbricas es la seguridad. Al utilizar el medio radioeléctrico, cualquier usuario con un dispositivo inalámbrico puede intentar escuchar las

transmisiones e incluso conectarse a la red. El estándar IEEE 802.11 y su actualización, el IEEE 802.11i, intentan mejorar la autenticación y el cifrado de la información.

EAP

Es el estándar que define la base a partir de la cual se pueden desarrollar sistemas de autenticación. En la actualidad existen unos 40 métodos de autenticación EAP, entre los cuales destacan:

- EAP-TLS.
- EAP-TTLS.
- PEAP.
- LEAP.

Autenticación

Es el proceso mediante el cual un cliente se identifica en la red a la que desea acceder para que esta decida si autorizarle o denegarle la entrada. La autenticación previene los accesos no deseados a la red, pero comporta un problema, ya que necesitamos como mínimo enviar una solicitud y, si esta no está cifrada, permite extraer información de red a un usuario no autorizado.

Los tipos de autenticación que fija el estándar IEEE 802.11 son:

- **Sistema abierto u Open System:** permite el acceso de todos los usuarios a la red inalámbrica, ya que no comprueba su identidad.
- **Clave compartida o PSK (Preshared Key):** en este sistema solo los usuarios que conozcan una clave previamente introducida en el punto de acceso podrán ser autorizados.
- **EAP (Extensible Authentication Protocol) o protocolo ampliable de autenticación:** permite la autenticación en los sistemas basados en el estándar IEEE 802.1X. Este último posibilita que todos los usuarios tengan claves de autenticación diferentes. IEEE 802.1X utiliza una estructura cliente-servidor y dispone de tres dispositivos básicos:
 - o Suplicantes: dispositivos que desean acceder a la red.
 - o Servidores de autenticación: dispositivos que guardarán las credenciales de los equipos que desean acceder a la red.
 - o Autenticadores: equipos a los que se conectan los clientes para autenticarse; normalmente se trata de un AP. Actúan como puente entre el servidor y el cliente.

Un ejemplo de este tipo de autenticación es el uso de un servidor RADIUS.

- **Filtros MAC:** los puntos de acceso permiten crear una lista de direcciones MAC para permitir o denegar el acceso a determinados dispositivos. Una vez que se ha realizado una primera autenticación, el AP busca la dirección MAC del dispositivo y confirma o deniega el acceso dependiendo del resultado.

RADIUS

Remote authentication dial-in user server o acceso telefónico de autenticación remota de usuarios en el servidor. Se utiliza la misma palabra para definir tanto el protocolo de autenticación como el servidor que realiza las funciones.

Cifrado

Como vimos en otra unidad, el cifrado consiste en aplicar un algoritmo sobre un texto en claro de forma que se obtenga otro compuesto por letras y símbolos que solo el receptor pueda leer.

El estándar IEEE 802.11 utiliza claves simétricas que pueden ser:

- Estáticas: las claves simétricas y estáticas son aquellas que no cambian de manera

- automática, lo que les hace más vulnerables a posibles ataques.
- Dinámicas: las claves simétricas y dinámicas son aquellas que van cambiando automáticamente. Así, el tiempo que la clave permanece activa es menor que el tiempo necesario para descifrarla:
 - o TKIP (*Temporal Key Integrity Protocol*) o protocolo de integridad temporal de clave: es un Sistema de claves dinámico. Utiliza una clave temporal de 128 bits, la dirección MAC del cliente y un vector de 16 octetos para generar la clave de autenticación.
 - o AES (*Advanced Encryption Standard*) o estándar avanzado de encriptación: es un sistema de claves dinámico basado en el cifrado por bloques. Adaptado por el gobierno de los Estados Unidos, presenta una mayor resistencia a los ataques.

Clonado de dirección MAC

Cuando se realiza un filtrado por dirección MAC, estas suelen enviarse sin

codificar para realizar la comprobación.

Esto puede provocar que sean escuchadas y replicadas por usuarios maliciosos.

WEP

WEP (*Wired Equivalent Privacy*) o privacidad equivalente a cableado fue el sistema de cifrado incluido en el estándar IEEE 802.11. Intentaba dotar a las WLAN de la misma seguridad que poseen las redes cableadas sin tener en cuenta la vulnerabilidad del medio de transmisión, ya que interceptar la información que circula a través de un cable es mucho más difícil que interceptar la que circula a través del medio radioeléctrico.

Utiliza una clave simétrica y estática que poseen todos los puntos de acceso y los clientes de la red. La clave es compartida, ya que utiliza la misma para autenticar y para cifrar la información.

Codifica la información que transmite utilizando el protocolo RC4, un sistema muy simple de encriptación. La fuerza de la clave ante los ataques se basa en su longitud. Puede ser de 40, 104 o 232 bits. Todas las claves incluyen 24 bits adicionales aleatorios para dotar de una mayor rigidez a la contraseña. A estos bits se les conoce como vector de inicialización.

WEP soporta los métodos de autenticación de sistema abierto y clave compartida.

El sistema WEP presenta una baja resistencia a los ataques informáticos, que son sencillos de realizar mediante el uso de determinado software que permanece a la escucha para conseguir la clave de acceso. Esto se debe a que los vectores de inicialización se envían sin cifrar en las conexiones iniciales y el sistema WEP genera mucho tráfico, dando más oportunidades de descifrar la clave. Además, existen métodos de ataque que permiten incrementar el tráfico.

Para solucionar estos problemas se creó el sistema WPA y posteriormente el estándar IEEE802.11i, que fijaría el sistema WPA2.

Ataques al sistema WEP

El método de autenticación del sistema abierto es más seguro que el de clave compartida.

Esto se debe a que cuando accedemos con clave compartida es posible descifrar la contraseña mediante la intercepción de los primeros cuatro paquetes de cada una de las fases de autenticación.

Es mejor utilizar el cifrado WEP una vez hayamos establecido la conexión.

WPA

WPA (*Wi-Fi Protected Access*) o acceso Wi-Fi protegido es un sistema creado para solucionar los problemas del sistema WEP. Fue diseñado por la *Wi-Fi Alliance* como paso intermedio para la creación del estándar IEEE 802.11i. En un principio, la idea era que fuera

compatible con todos los dispositivos inalámbricos que soportaban WEP mediante una actualización de su *firmware*, pero algunos dispositivos no pueden implementarlo.

El sistema WPA fue creado para utilizarse con un servidor de autenticación que cumpla el estándar IEEE 802.1X/EAP, normalmente RADIUS, y para funcionar mediante claves diferentes para cada usuario.

Admite también la validación mediante clave compartida, PSK. Este modo de autenticación es adecuado para entornos domésticos y pequeñas redes. Además, mejora la seguridad respecto al sistema WEP, ya que incorpora el cifrado dinámico TKI, además de un sistema de verificación de mensajes.

MIC

Message Integrity Code o código de integración del mensaje es el sistema que utiliza WPA para verificar sus mensajes.

Se conoce también como Michael.

WPA2

WPA2 (*Wi-Fi Protected Access Two*) o *acceso Wi-Fi protegido dos* fue creado para corregir los problemas de seguridad del WPA. Está fijado en el estándar IEEE 802.11i. Mejora los sistemas de protección del WPA incorporando el cifrado AES al modo de acceso de clave compartida.

Wi-Fi Alliance divide los sistemas WPA de la siguiente forma:

- Modo personal: los que utilizan la clave compartida.
- Modo empresarial: los que utilizan servidores de autenticación.

Se puede ver un resumen de los dos sistemas en la siguiente tabla:

Sistema WPA		WPA	WPA2
Modo personal	Autenticación	PSK	PSK
	Cifrado	TKIP	AES
Modo empresarial	Autenticación	802.1X/EAP	802.1X/EAP
	Cifrado	TKIP	AES

Ataques sobre los sistemas inalámbricos

Entre otros, existen dos tipos básicos de ataques contra contraseñas:

- **Ataque de diccionario:** consiste en intentar averiguar una contraseña probando todas las palabras de una lista, como puede ser un diccionario. Conociendo alguno de los parámetros que intervienen en la generación de la clave se reduce el tiempo de proceso. Por ejemplo, en el sistema de cifrado AES sobre redes inalámbricas, se incorpora la SSID para generar la contraseña. Si se hace visible el nombre del punto de acceso se estarán facilitando los ataques por diccionario. Si se oculta el nombre del AP, solo podrán acceder a la red aquellos usuarios que lo conozcan por adelantado, aunque existen programas que permiten averiguarlo.
- **Ataque de fuerza bruta:** consiste en probar todas las combinaciones posibles hasta encontrar la que permite el acceso. Es menos eficiente que el ataque por diccionario. Para provocar que sea tan costoso en tiempo que no merezca la pena intentarlo, se deberá aumentar la fortaleza de la contraseña. Utilizaremos para ello el máximo número de caracteres permitidos por el sistema de acceso para la contraseña, así como los diferentes

tipos de caracteres posibles: mayúsculas, minúsculas, números y símbolos. También es recomendable que los caracteres se dispongan aleatoriamente sin formar palabras reales. En un ataque normalmente se combinan los dos tipos.

Para realizar ataques a WLAN basadas en cifrado WEP, normalmente se utilizan *packets sniffers* o analizadores de paquetes. Con ellos se capturan paquetes y se envían a un software matemático especialista en descifrar contraseñas. Cuanto más larga sea la contraseña, más paquetes se necesitarán.

Para atacar redes basadas en cifrado WPA se intenta desconectar al cliente, capturar el *handshake* o saludo y descifrarlo mediante un ataque de tipo diccionario.

Handshake

Cada vez que un cliente se conecta a una red que utiliza un cifrado WPA,

envía un paquete-saludo o *handshake* al AP.

Este paquete-saludo contiene la contraseña encriptada.

2. Términos de redes

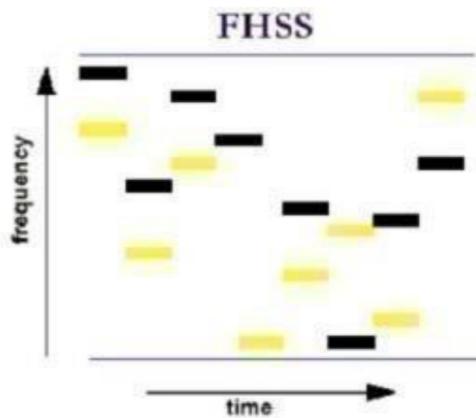
FHSS

Según Wikipedia

El espectro ensanchado por salto de frecuencia (del inglés Frequency Hopping Spread Spectrum o FHSS) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.

Según otras fuentes

En FHSS consiste en transmitir una parte de los datos en una determinada frecuencia durante un intervalo de tiempo, llamado *dwell time*, los datos se transmiten saltando de una frecuencia a otra, en un orden determinado según una secuencia seudocaleatoria almacenada en unas tablas, que han de conocer el



emisor y el receptor. Estos saltos están programados en un determinado tiempo que conoce y sigue el receptor por lo que sólo ve, o entiende, ese canal de transmisión.

Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia.

Resumiendo

FHSS consiste en una comunicación entre dos puntos por radiofrecuencias, las cuales modifican su frecuencia de forma aleatoria entre unas frecuencias acordadas de antemano, las cuales van cambiando cada cierto tiempo. Las primeras investigaciones sobre esta técnica son de Nicola Tesla aunque se considera a Hedy Lamarr la inventora pues creo la patente más conocida.



DSSS

Según Wikipedia

El espectro ensanchado por secuencia directa (*Direct Sequence Spread Spectrum*), es uno de los métodos de codificación de canal en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.

Según otras fuentes

En DSSS los datos son mezclados ordenadamente con ruido, van transmitiéndose primero en una frecuencia A, luego en otra B y en una tercera C. La cantidad de frecuencias utilizadas y el orden de la mezcla son determinadas por un algoritmo específico.

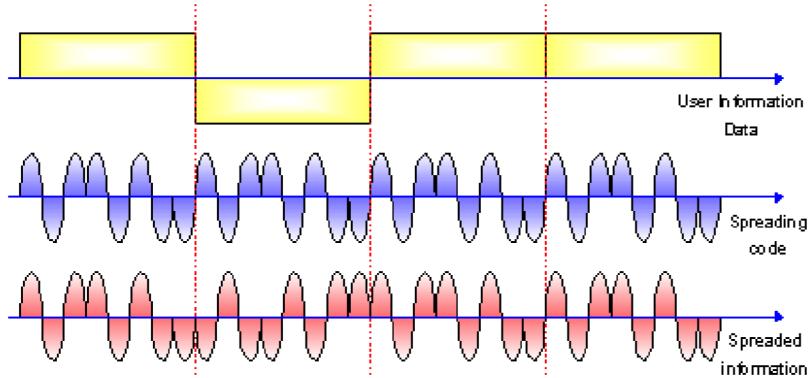
Solo los receptores que han recibido antes el código de mezcla con ruido o de expansión de datos pueden deshacer la mezcla y entender los datos.

Resumiendo

DSSS consiste en la transmisión de información de un punto a otro con radiofrecuencias que van cambiando de frecuencia en un orden, es decir, primero se trasmisaría en una frecuencia A, luego C

y luego B, siempre siguiendo un orden y, además, añadiendo ruido para ofuscar la señal.

DSSS Example

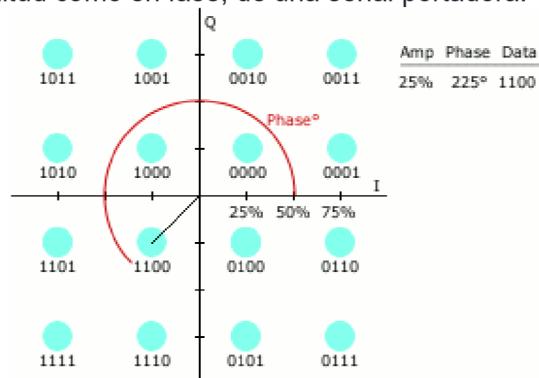


OFDM

Según Wikipedia

La Multiplexación por División de Frecuencias Ortogonales, en inglés *Orthogonal Frequency Division Multiplexing* (OFDM), es una técnica de transmisión que consiste en la multiplexación de un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK.

La modulación de amplitud en cuadratura o **QAM** (acrónimo de *Quadrature Amplitude Modulation*, por sus siglas en inglés) es una técnica que transporta dos señales independientes, mediante la modulación, tanto en amplitud como en fase, de una señal portadora.



La modulación por desplazamiento de fase o PSK es una forma de modulación angular que consiste en hacer variar la fase de la portadora entre un número determinado de valores discretos.

Según otras fuentes

La modulación por división ortogonal de frecuencia, es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferente frecuencia.

Resumiendo

OFDM consiste en la modulación de ondas en QAM o PSK, las cuales llevan la información "por dentro", es decir, va camuflada en ondas y codificando valores mayores a los 0 y 1 binarios.

DBPSK

Según Wikipedia

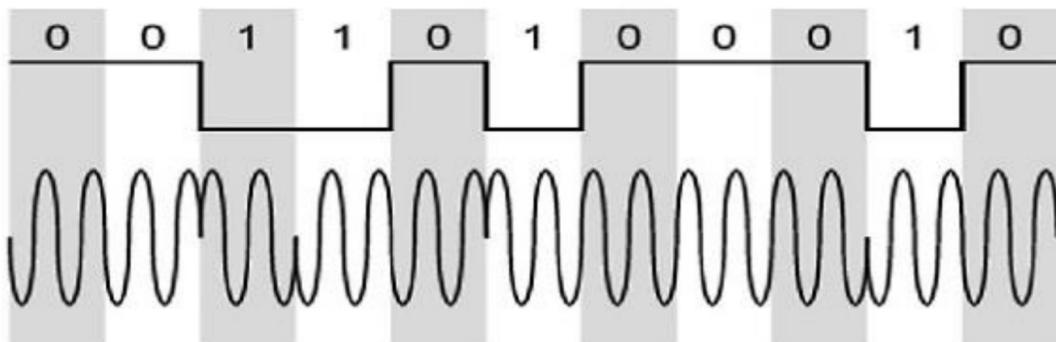
La Multiplexación por La modulación por desplazamiento diferencial de fase (conocida como DPSK, por las siglas en inglés de *Differential Phase Shift Keying*), es una forma de modulación digital, donde la información binaria de la entrada está compuesta en la diferencia entre las fases de dos elementos sucesivos de señalización, y no en la fase absoluta.

Según otras fuentes

DBPSK (*Differential Binary Phase Shifter Keying*) es una técnica de modulación digital que no maneja estados absolutos, sino que tiene en cuenta la diferencia que tenga la señal de salida.

Resumiendo

DBPSK es el cambio continuo de la frecuencia de la onda, cambiando radicalmente de "0" a "1", es decir cambiando de 0° a 180° .



DQPSK

Según Wikipedia

Este esquema de modulación es conocido también como Quaternary PSK (PSK Cuaternaria). Esta modulación digital es representada en el diagrama de constelación por cuatro puntos equidistantes

del origen de coordenadas. Con cuatro fases, QPSK puede codificar dos bits por cada símbolo. La asignación de bits a cada símbolo suele hacerse mediante el código Gray, que consiste en que, entre

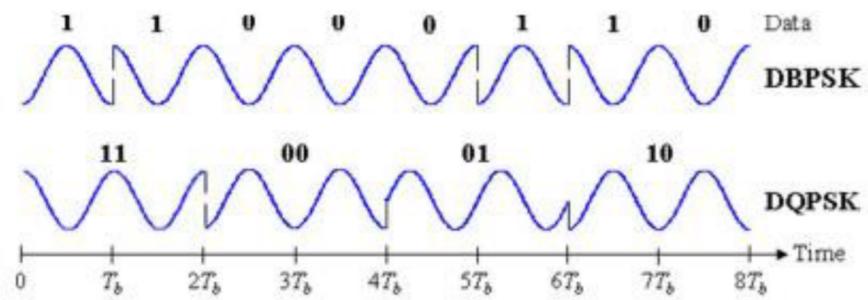
dos símbolos adyacentes, los símbolos solo se diferencian en 1 bit, con lo que se logra minimizar la tasa de bits erróneos.

Según otras fuentes

DQPSK (Differential Quadrature Phase Shift Keying o cuadratura diferencial de cambio de fase seguro) es una técnica de modulación en la que el operador puede asumir una de cuatro fases, cada cambio de fase, o símbolo, que representa 2 bits. Las combinaciones de bits son 00, 01, 11 y 10. En consecuencia, la secuencia de datos puede transportar 2 bits a la vez. Usando esta técnica, se evita la transición de fase a través del origen.

Resumiendo

DQPSK es una técnica que consiste en el cambio de frecuencia de onda en pares, es decir, cambia radicalmente de "00" a "11" en pares, cada dos ondas.



3. Órdenes Linux utilizadas en redes Wi-Fi

ifconfig

La orden *ifconfig* permite configurar o desplegar numerosos parámetros de las interfaces de redes, como la dirección IP (tanto dinámica, como estática), o la máscara de red. Si se llama sin ningún parámetro, suele mostrar la configuración actual de las interfaces de red activas en ese mismo momento, con detalles como pueden ser la dirección MAC o el tráfico que ha circulado por las mismas hasta el momento.

Opciones principales

- *up*: marca la interfaz como disponible para que sea usada por la capa IP. También permite reactivar una interfaz que se ha desactivado temporalmente la opción *down*.
- *down*: marca la interfaz como inaccesible a la capa IP. Esto inhabilita cualquier tráfico IP a través de la interfaz.
- *netmask*: asigna una máscara de subred a una interfaz. Se puede dar como un valor de 32 bits en hexadecimal precedido del prefijo 0x, o en notación de cuaterna usando números decimales separados por puntos.
- *pointopoint*: se usa para enlaces IP punto-a-punto en los que intervienen únicamente dos máquinas.
- *broadcast*: la dirección de difusión se obtiene, usando la parte de red de la dirección y activando todos los bits de la manera correspondiente a la máquina.
- *irq*: permite establecer la línea de irq usando por ciertos dispositivos, puede ser de utilidad para algunas tarjetas Ethernet.
- *metric*: esta opción puede ser usada para asignar un valor de métrica a la tabla de encaminamiento creada para la interfaz. Esta métrica es usada por el protocolo de información de encaminamiento, para construir las tablas de encaminamiento para la red.
- *mtu*: esto fija la unidad máxima de transferencia, o lo que es lo mismo, el máximo número de octetos que la interfaz es capaz de manejar en una única transacción.
- *arp*: esta opción es específica de redes de difusión como las Ethernet o las de radio-paquetes. Permite el uso de ARP, para detectar la dirección física de las máquinas conectadas a la red. (-arp inhabilita el uso de ARP para esta interfaz)
- *promisc*: Pone la interfaz en modo promiscuo. Esto hace que la interfaz reciba todos los paquetes, independientemente de si eran para ella o no. Esto permite el análisis de tráfico de red utilizando utilidades como filtros de paquetes, también llamado fisgoneo de Ethernet. (-promisc apaga el modo promiscuo)
- *allmulti*: las direcciones de envío múltiple (multicast) son como las direcciones de difusión de Ethernet, excepto que, en el lugar de incluir automáticamente a todo el mundo, los únicos que reciben paquetes enviados a una dirección de envío múltiple son aquellos programados para escucharla. Es útil para videoconferencia basada en Ethernet o audio para red, en los que solo los interesados pueden escuchar. (-allmulti deshabilita el modo allmulti).

Recordar que actualmente todas las acciones que se pueden realizar con la orden *ipconfig* se pueden realizar con la orden *ip*.

iwconfig

La orden iwconfig es similar a ifconfig, pero está dedicada a las interfaces inalámbricas. Se utiliza para establecer los parámetros de la interfaz de red que son específicas para operar con la red inalámbrica. También puede ser utilizada para mostrar los parámetros y estadísticas de los servicios inalámbricos. Todos estos parámetros y estadísticas son dependientes del dispositivo.

Opciones principales

- *freq*: establece la frecuencia de funcionamiento o canal en el dispositivo.
- *sens*: ajusta el umbral de sensibilidad. Este es el más bajo nivel de señal para que el intento de paquetes de hardware de recepción, las señales más débiles se ignoren. Esto se utiliza para evitar la recepción de ruido de fondo.
- *mode*: se establece el modo de funcionamiento del dispositivo, que depende de la red.
 - *mode monitor*: se utiliza para esnifar el tráfico de redes externas.
 - *mode managed*: se usa como modo infraestructura, mediante puntos de acceso y/o router.
 - *mode ad-hoc*: para conectar varios ordenadores sin punto de acceso.
- *channel*: se fija el canal elegido para nuestra tarjeta inalámbrica. También se puede utilizar la frecuencia.
- *freq*: Se fija el valor de frecuencia para nuestra tarjeta inalámbrica. También podemos utilizar el canal.
- *rate*: Fijamos la velocidad en las comunicaciones para 802.11b. También se puede utilizar 54M. O ponerlo en modo automático.
- *power period*: Tiempo de actividad de la tarjeta, cuando no se utiliza la conexión a red. Por lo tanto, en modo monitor la captura de datos no funcionaría correctamente.
- *frag*: La fragmentación permite dividir un paquete IP en varios más pequeños.

iwlist

La orden iwlist se utiliza para mostrar información adicional de una interfaz de red inalámbrica que no se muestra con iwconfig. Sirve para seleccionar una categoría de información, que es mostrada de forma detallada.

Opciones principales

- *scan*: devuelve la lista de puntos de acceso y celdas Ad-Hoc dentro de rango, y opcionalmente un montón de información sobre ellos (ESSID, calidad, frecuencia, modo ...). El tipo de información devuelta depende de lo que admite la tarjeta.
- *freq*: devuelve la lista de frecuencias disponibles y el número de canales definidos.
- *rate*: lista de las tasas de transferencia soportadas por el dispositivo.
- *key*: lista los tamaños de claves de cifrado soportadas y muestra todas las claves de cifrado disponibles en el *dispositivo.power*: lista de los diversos atributos de administración de energía y los modos del dispositivo.
- *txpower*: lista las potencias de transmisión disponible en el dispositivo
- *retry*: Lista la cantidad de reintentos de transmitir y reintentos de vuelta en el dispositivo.
- *events*: Lista de eventos soportados por el dispositivo inalámbrico.
- *--version*: Muestra la versión de las herramientas, así como las versiones recomendadas y actuales de las extensiones inalámbricas de la herramienta y las distintas interfaces inalámbricas.

iwevent

iwevent se encarga de visualizar los eventos o log generados al conectarse a una red.

Hay dos tipos de eventos por este comando:

- a) La primera clase de evento está relacionada con un cambio de configuración inalámbrica en la interfaz. Solo los ajustes que podrían dar lugar a un fallo en la conexión serán mostrados en el evento. Los sucesos notificados son los siguientes:
 1. Network ID
 2. ESSID
 3. Frecuencia
 4. Modo
 5. Cifrado
- b) La segunda clase de eventos son generados por el hardware, cuando algo ocurre o una tarea se ha terminado.

Esta orden se queda funcionando, a la espera de eventos, hasta que la paremos.