Capítulo 2

Familia IEEE 802.11

2.1. Introducción

En este capítulo estudiaremos con detalle la familia de estándares IEEE 802.11, perteneciente al grupo IEEE 802, el cual está dedicado por completo a la normalización de Redes de Área Local (LAN) centrándose en los dos niveles más bajos de la arquitectura OSI: capa física y capa de enlace. En la ilustración 2-1 vemos algunos de los estándares que propone el IEEE 802, así como su estructura de capas según el modelo OSI.

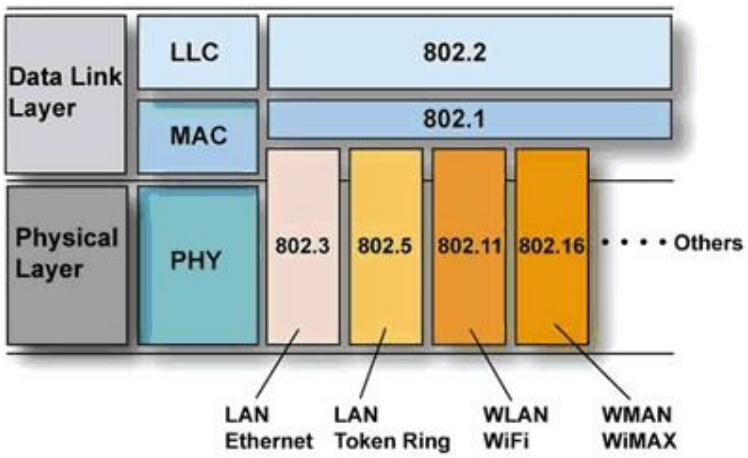


Ilustración 2-1: Estándares IEEE 802

El éxito de IEEE 802.11 o Wi-Fi radica en que al ser el primer estándar implementado en el mercado, se convirtió en el más utilizado para la creación de WLANs. Además ha demostrado su capacidad para ofrecer acceso de banda ancha en múltiples entornos públicos a precios asequibles.

Aclaremos el significado del término Wi-Fi. En multitud de ocasiones hemos oído expresiones como "…una red Wi-Fi" o "…acceso Wi-Fi", etc. ¿Pero qué significa realmente Wi-Fi (o WIFI, wifi, WiFi, Wi-fi)? Es la abreviatura de la expresión inglesa "Wireless Fidelity" (que significa Fidelidad Inalámbrica). Se utiliza como denominación genérica para los productos que incorporan cualquier variante de la tecnología inalámbrica 802.11, que permite la creación de redes inalámbricas WLAN. En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, que funciona en una banda de frecuencias de 2,4 GHz y permite la transmisión de datos a una velocidad de hasta 11Mbps. Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología de la familia IEEE 802.11: 802.11a, 802.11b, 802.11g.

En este capítulo presentaremos al detalle la arquitectura de la familia IEEE 802.11, a la vez que profundizaremos en su capa física y de enlace. Además, enumeraremos los principales protocolos que incluidos en esta familia resaltando sus características más notables.

2.2. Arquitectura de la familia IEEE 802.11

2.2.1. Arquitectura lógica-funcional. Componentes básicos

La arquitectura 802.11 está basada en una arquitectura celular.

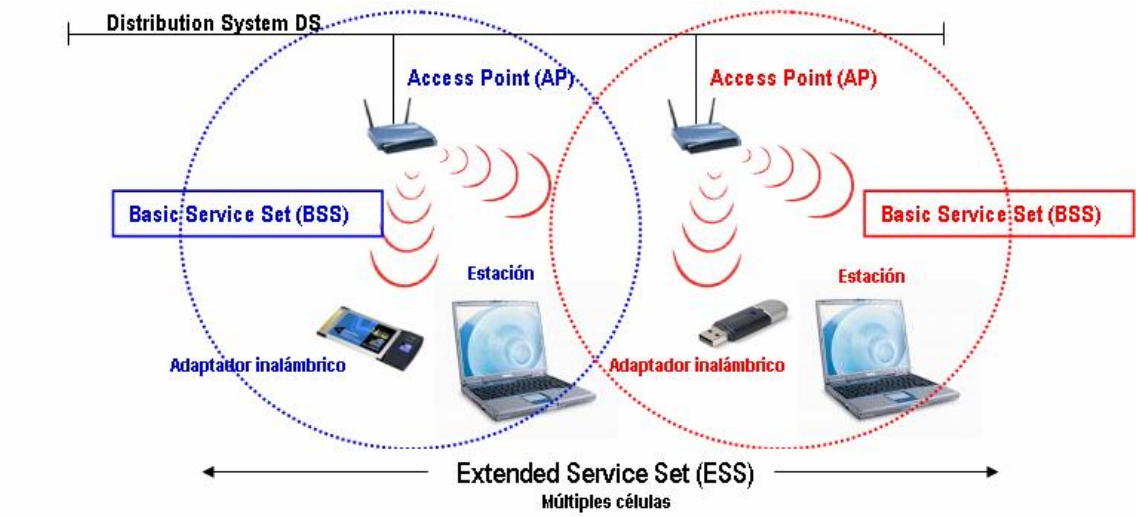


Ilustración 2-2: Arquitectura lógica-funcional de IEEE 802.11

El sistema se divide en celdas o células denominadas **BSS** ("Basic Service Set") o **Conjunto Básico de Servicios**. Un BSS está formado por nodos, fijos o móviles, llamados estaciones.

Cada BSS está gobernada por un **Punto de Acceso o AP** ("Access Point"). Según el apartado 5.2.1.1 del estándar 802.11 [2-1], un AP se define como una estación base provista de acceso al Sistema de Distribución (DS), capaz de proveer a las estaciones de los servicios de éste. Las funciones básicas que puede realizar son:

- Portal, para interconectar la WLAN y otra red LAN 802.x de otro tipo (Internet, intranet,…).
- Puente hacia otros puntos de acceso, para extender los servicios de acceso.
- Router, para encaminar los datos dentro de la zona de cobertura.

El AP es el elemento esencial de la red inalámbrica puesto que será el transmisor y el receptor de la señal que se transmita por el aire, y el que, por tanto, proporcione cobertura a las estaciones que forman parte de nuestra WLAN.

Las estaciones de un BSS obtienen acceso al **Sistema de Distribución o DS** ("Distribution System"), y por tanto a otros nodos fuera de su área de cobertura, a través del AP. El DS es el componente lógico de la 802.11 que se encarga de conducir las tramas hasta su destino [2-1]. En el estándar no se fija ninguna tecnología concreta pero en la mayoría de los casos está basado en tecnología Ethernet (aunque también puede ser radioeléctrico). Tiende a equipararse a la columna vertebral de la red (backbone network)

El conjunto de celdas y sus correspondientes puntos de acceso se presenta a los niveles superiores como una unidad lógica llamada **ESS** ("Extended Service Set") **o Conjunto de Servicio Extendido**, que es lo mismo que la unión de varias BSS.

El **medio inalámbrico** (el aire) es el medio de transmisión usado para comunicaciones de una estación a otra. La arquitectura de 802.11 define varias capas físicas para llevar a cabo esta transmisión.

Las **estaciones** (o clientes inalámbricos) suelen ser algún tipo de computadoras, provistas de interfaces de red inalámbricos, tanto portátiles como no. Estos interfaces suelen ser tarjetas. Normalmente los portátiles de última generación cuentan con adaptador inalámbrico incorporado. Todo aquel equipo que no tenga, necesitara uno para poder conectarse. Existen principalmente tres tipos: tarjeta PCI, tarjeta PCMCIA y adaptador USB.

Ilustración 2-3: Adaptadores inalámbricos

2.2.2. Modelo de referencia

La norma 802.11 sigue el mismo modelo o arquitectura que toda la familia 802, es decir, capa física y la capa de enlace.

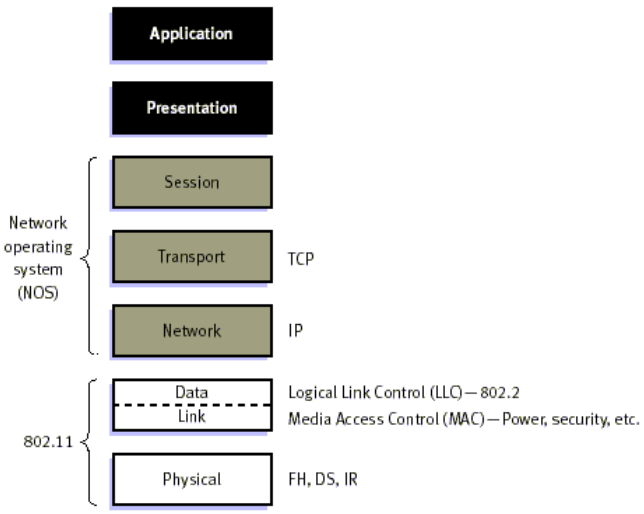


Ilustración 2-4: Modelo OSI y Familia IEEE 802.11

Viéndolo con un poco de más detalle, la **capa física** se divide en dos subcapas [2-2]:

- La subcapa inferior, **PMD** (Physical Media Dependent), que corresponde al conjunto de especificaciones de cada uno de los sistemas de transmisión a nivel físico. El estándar define cuatro: Infrarrojos, FHSS, DSSS o OFDM.
- La subcapa superior, **PLCP** (Physical Layer Convergence Procedure), se encarga de adptar las diversas especificaciones de la subcapa PMD a la subcapa MAC, inmediatamente superior.

La **capa de enlace** también se divide a su vez en dos subcapas [2-3]:

- La subcapa **MAC** (Media Access Control), donde se especifica el protocolo de acceso al medio propiamente dicho, así como una serie de peculiaridades propias de redes inalámbricas como son el envío de acuses de recibo (ACK), la posibilidad de realizar fragmentación de las tramas y los mecanismos de encriptación para dar confidencialidad a los datos transmitidos.

- La subcapa **LLC** (Logical Link Control), que ofrece un servicio de transporte único para todas las tecnologías. Tal y como vemos en la Ilustración 2-1 de este capítulo, esta subcapa es común a todo los estándares IEEE 802.

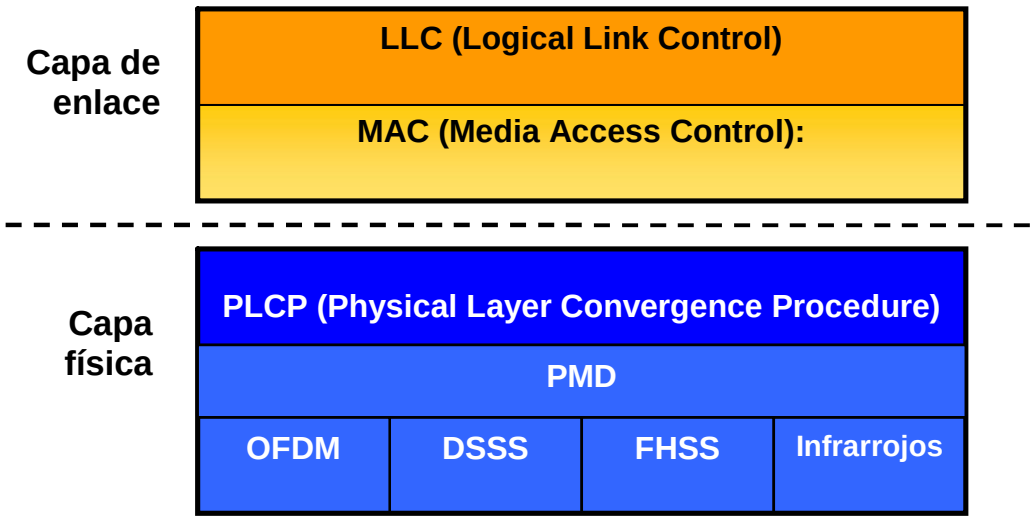


Ilustración 2-5: Modelo de referencia detallado de IEEE 802.11

2.2.3. Topologías de red

Tendremos distintas configuraciones de red dependiendo de las necesidades a y prestaciones a cubrir. Veamos las topologías básicas descritas por el estándar:

2.2.3.1. Modo Ad Hoc o IBSS (Independient Basic Service Set)

No existe punto de acceso. Las estaciones se comunican peer to peer (par a par, de igual a igual), es decir, no hay una base y nadie da permisos para comunicarse. El tráfico de información se lleva a cabo directamente entre los equipos implicados, sin tener que recurrir a un punto de acceso, obteniéndose un aprovechamiento máximo del canal de comunicaciones.

Ilustración 2-6: Modo Ad Hoc con 2 estaciones

Cada trama es recibida por todos los ordenadores que se encuentren dentro del rango de alcance del emisor. La cobertura se determina por la distancia máxima entre dos equipos, la cual suele ser apreciablemente inferior a las topologías con punto de acceso [2-4]. A nivel IP la numeración deberá corresponder a una red, es decir todos los ordenadores deberán configurarse con una dirección IP que tenga un prefijo común. Eventualmente uno de los ordenadores podría tener además una tarjeta de red, por ejemplo Ethernet, y actuar como router para el resto de forma que pudieran salir a la LAN cableada a través de el. En ese caso habría que definirle como router por defecto para el resto.

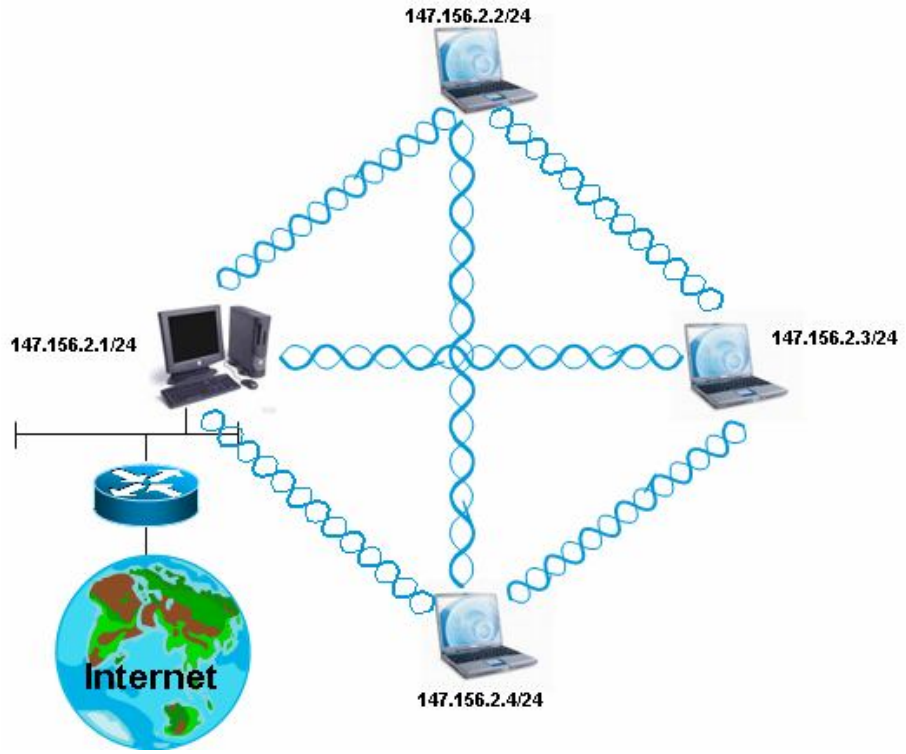


Ilustración 2-7: Modo Ad Hoc con 4 estaciones

2.2.3.2. Modo Infraestructura o BSS (Basic Service Set)

Existe un punto de acceso que realiza las funciones de coordinación. Las estaciones en cuanto descubren que se encuentran dentro del radio de cobertura de un AP se registran en el para que les tome en cuenta. La comunicación entre estaciones registradas en un AP nunca se realiza de forma directa sino que siempre se hace a través del AP (todo el tráfico pasa a través de él).

Hay una clara pérdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí: los paquetes de información son enviados una vez al punto de acceso y otra vez al destino. Sin embargo, esto no es un problema si la mayoría del tráfico va dirigido a la LAN convencional. Además tenemos como ventaja que dos estaciones podrán establecer comunicación entre sí aunque la distancia entre ellas no les permita verse.

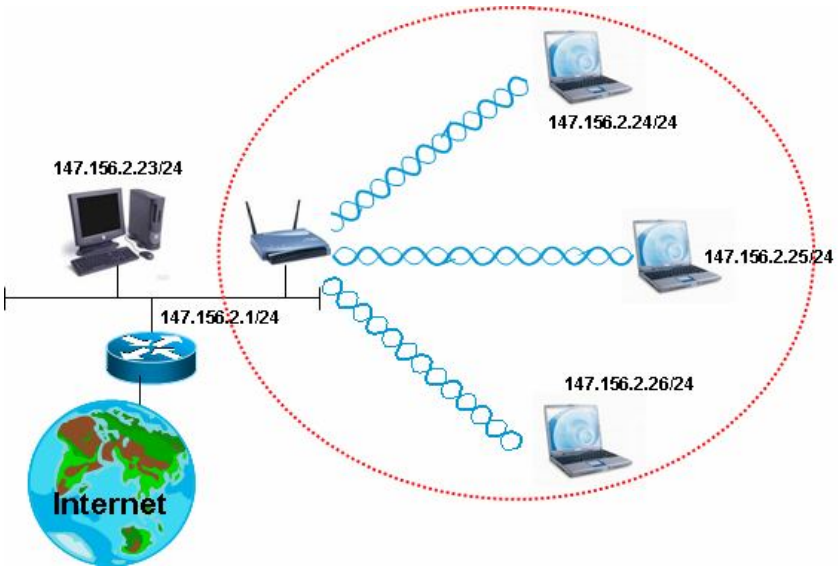


Ilustración 2-8: Modo Infraestructura o BSS

2.2.3.3. Modo BSS Extendido o ESS (Extended Service Set)

Es un caso específico del modo infraestructura. Consiste en tener dos o más APs interconectados (normalmente por una LAN convencional), de forma que cada AP abarca una zona o celda que corresponde a su radio de alcance. Los usuarios pueden moverse libremente de una celda a otra y su conexión se establecerá automáticamente con el AP del que reciban una señal más potente. A esto se le llama roaming o itinerancia entre celdas.

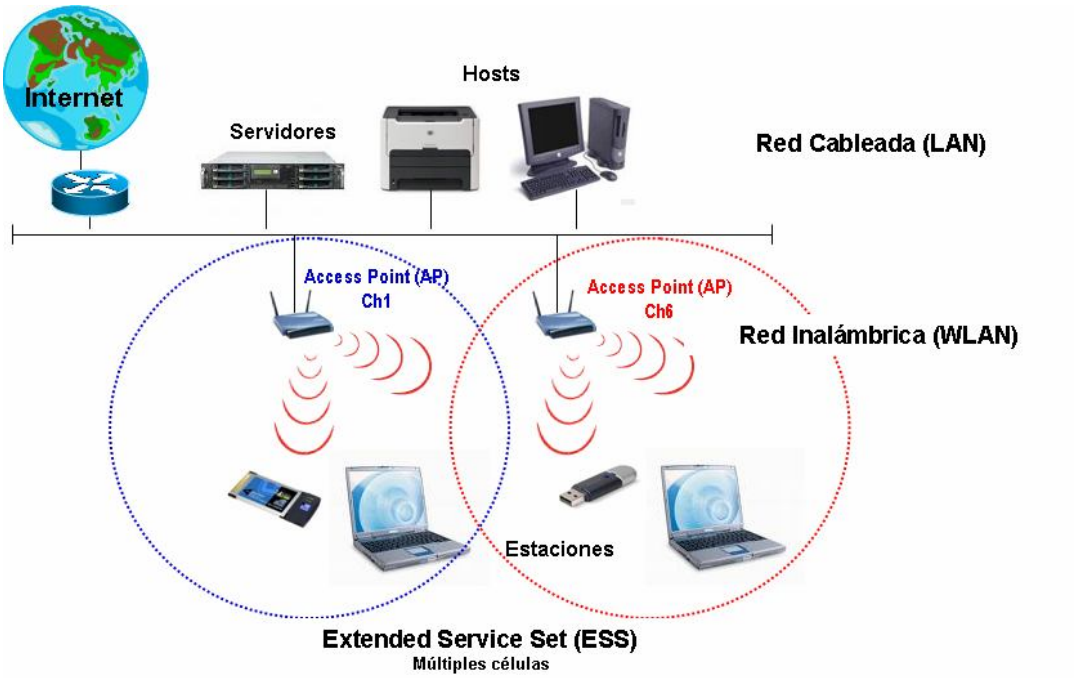


Ilustración 2-9: Modo ESS

2.3. La capa física

La capa física corresponde a la capa más baja del modelo de referencia OSI. Es la encargada de transmitir y recibir la información por el medio físico, que en este caso es el aire; y es donde se establecen las especificaciones eléctricas y mecánicas de las conexiones. Consiste en dos subniveles:

- Un **sistema físico dependiente del medio**, PMD, que define las distintas técnicas de transmisión de la información a través de un medio sin cables; y que establece los distintos tipos de modulaciones que los equipos deben usar para poder acceder al medio.

- Una **función de convergencia de capa física**, que adapta las capacidades del PMD. Esta función es implementada por el protocolo PLCP o Procedimiento de Convergencia de Capa Física, que define una forma de mapear unidades de datos MAC (MPDUs) en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones a través de la capa PMD.

El siguiente diagrama de bloques resume la capa física de 802.11 y sus extensiones. Seguiremos el esquema seguido por el diagrama en el desarrollo de este apartado: hablaremos sobre el espectro radioeléctrico de la familia IEEE 802.11; analizaremos también las distintas tecnologías de transmisión, haciendo hincapié en las técnicas de espectro ensanchado; por último repasaremos las modulaciones principales usadas por cada estándar.

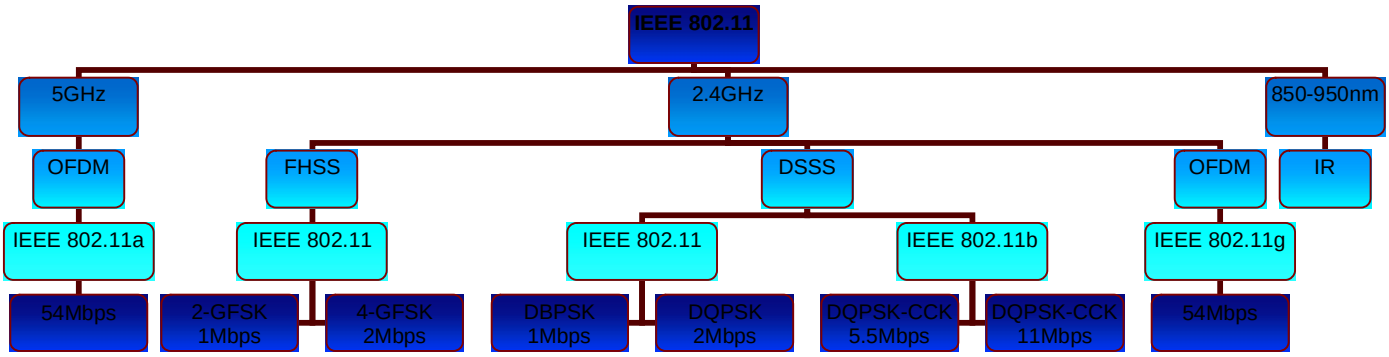


Ilustración 2-10: Diagrama descriptivo de la capa IEEE 802.11 y sus extensiones

Aclarar que el infrarrojo no ha recibido ninguna aceptación en el mercado de las WLANs y por eso quedará fuera de nuestro estudio.

2.3.1. Espectro radioeléctrico

Como toda tecnología radio, la familia IEEE 802.11 utiliza el espectro radioeléctrico, recurso escaso cuyo uso y asignación son globalmente regulados por organismos de ámbito internacional y nacional, como la ITU-R (International Telecommunication Union - Radio). Normalmente se requiere de licencia para ocupar una franja del espectro.

Los estándares 802.11 utilizan las bandas de 2.4Ghz y 5Ghz. Como no sería práctico pedir licencia para cada WLAN, el IEEE buscó una banda no regulada disponible en todo el mundo y consideró que la **banda de 2,4 GHz** (banda ISM, Industrial-Científica-Médica) era la más adecuada. Esta banda no requiere de licencia y los servicios de radiocomunicaciones que funcionan en ella deben aceptar la interferencia resultante de aplicaciones que también trabajan en esta banda. Asimismo no podrán causar interferencia alguna con otras emisiones del espectro.

Al estar disponible sin licencia para todo el que desee emitir en ella, es preciso adoptar algunas precauciones que eviten una excesiva interferencia entre emisiones. Por este motivo se establece que cualquier emisión debe ser con una potencia igual o inferior a 1mW y en espectro disperso o SS (Spread Spectrum). Las formas de hacer una emisión de espectro disperso las veremos con profundidad más adelante.

La ITU-R divide el mundo en tres regiones. Cada una tiene una regulación diferente de las frecuencias. Incluso dentro de las regiones, algunos países tienen normativas propias más restrictivas. En esta tabla se recogen los rangos que se especifican en el documento del estándar. Como puede verse España y Japón tienen rangos mucho más reducidos que el resto de países.

Región ITU-R	Rango	Potencia máxima
Europa	2,4000 – 2,4835GHz	100mW
España	2,4450 – 2,4750GHz	100mW
EEUU y Canadá	2,4000 – 2,4835GHz	1W
Japón	2,4710 – 2,4970GHz	10mW/MHz

Tabla 2-1: Banda 2.4GHz según la región ITU-R

En cuanto a la **banda de 5Ghz** ha sido recientemente habilitada para el estándar IEEE 802.11a, conocido como WIFI 5. La banda de 5 GHz permite canales de mayor ancho de banda y, además, no existen otras tecnologías que la estén utilizando (Bluetooth, microondas, etc.), por lo que hay muy pocas interferencias.

Sin embargo, la utilización de esta banda también tiene sus desventajas. Restringe el uso de los equipos 802.11a a únicamente puntos con visión directa, por lo que hace necesario la instalación de un mayor número de puntos de acceso. Adicionalmente los equipos que trabajan a 5GHz no pueden penetrar tan lejos como los estándares que trabajan a 2.4Ghz dado que sus ondas son más fácilmente absorbidas: a mayor frecuencia, menor longitud de onda y mayor facilidad para ser absorbida por un obstáculo.

2.3.2. Tecnologías de transmisión

A continuación vamos a ver las distintas técnicas de transmisión que se utilizan en la familia IEEE 802.11. Las técnicas a usar nos permitirán diferentes prestaciones, y el uso de unas u otras dependerá del entorno, las necesidades de la red y la variante del estándar que estemos usando.

Podemos dividirlas en dos grandes grupos: tecnologías de transmisión por infrarrojos y tecnologías de transmisión por ondas de radio. Como en 802.11 la transmisión por infrarrojos no es muy común y solo es posible en distancias muy cortas (10-20m) dentro de una misma habitación, vamos a centrarnos en las técnicas de propagación por ondas de radio. Son tres: FHSS, DSSS y OFDM.

2.3.2.1. Técnicas de Espectro Ensanchado

La técnica de espectro ensanchado, expandido, disperso o SS (Spread Spectrum) es una técnica de transmisión que consiste en la transformación reversible de una señal, de forma que su energía se disperse entre una banda de frecuencias mayor que la que ocupaba originalmente. Se caracteriza por:

- El ancho de banda utilizado en la transmisión es mucho mayor que el necesario para una transmisión convencional. Si R es la velocidad de transmisión (una modulación convencional tendría un ancho de banda de aproximadamente R Hz) y W es el ancho de banda empleado por la señal de espectro ensanchado, se cumple que $W/R >> 1$.

- El ensanchamiento de la banda se realiza a partir de una señal pseudoaleatoria [1], que se caracteriza por tener una apariencia de ruido (también se le llama pseudoruido).

- La señal transmitida sólo se podrá demodular si se el receptor es capaz de generar la misma señal de pseudoruido utilizada por el transmisor.

Pero ¿por qué utilizamos un ancho de banda mucho mayor del estrictamente necesario? Lo hacemos porque la señal ensanchada tiene una serie de características especiales muy interesantes para la transmisión. En primer lugar, la transmisión de señales con espectro ensanchado es mucho más resistente y robusta frente a las interferencias que otros tipos de transmisiones. Además, la señal es difícilmente detectable, ya que su nivel de potencia queda muy reducido por su dispersión espectral. Sólo después de la transformación de desensanchado, ésta recupera la relación señal a ruido suficiente para su demodulación. Incluso en el caso de que se detecte la señal, la transmisión es ininteligible para el receptor que no conozca la señal pseudoaleatoria utilizada para el ensanchado del espectro.

Esta señal ensanchada puede obtenerse de dos maneras:

- Codificar la señal original con una señal pseudoaleatoria **(DSSS o Espectro Ensanchado por Secuencia Directa).**

- Codificar la frecuencia de trabajo con una señal pseudoaleatoria **(FHSS o Espectro Ensanchado por Salto de Frecuencia)**.

FHSS (Frequency Hopping Spread Spectrum).

FHSS o Técnica de Espectro Ensanchado por Salto en Frecuencia se basa en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo. Pasado este tiempo se cambia la frecuencia de emisión (se cambia de canal) y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta (canal distinto) durante un intervalo muy corto de tiempo. La frecuencia de portadora va saltando de una frecuencia a otra siguiendo una secuencia pseudoaleatoria preestablecida, conocida por los dos extremos de la comunicación. El receptor sigue la secuencia de saltos.

[1] Una secuencia pseudoaleatoria es aquella que toma valores arbitrarios dentro de un determinado periodo de tiempo, a partir del cual la señal se repite.

Si un agente externo produce una interferencia y esta afecta a algún canal o canales en concreto, el receptor no podrá separar la señal del ruido y la trama no será recibida. En ese caso el emisor retransmitirá la trama, confiando que en el siguiente intento no coincida la interferencia con ninguno de los canales utilizados.

Esta técnica utiliza la zona de los 2.4GHz, la cual organiza en 79 canales 1MHz de ancho de banda. El número de saltos de frecuencia por segundo es regulado por cada país. Esta técnica esta asociada a la modulación GFSK que explicaremos en la sección 2.3.3.

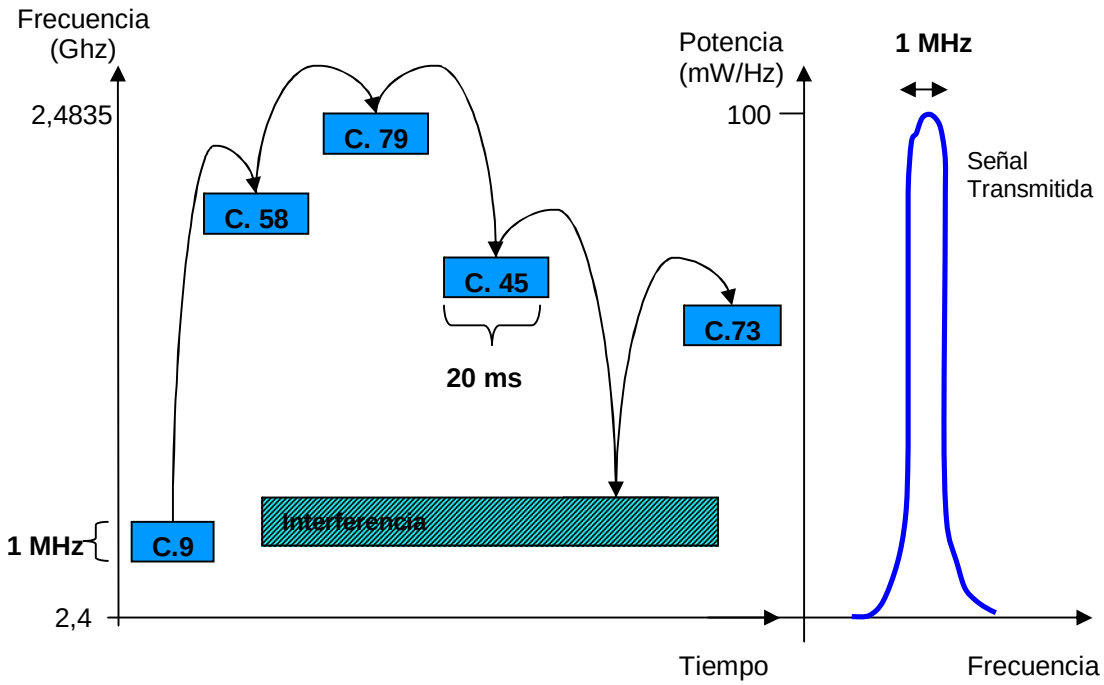


Ilustración 2-11: Funcionamiento FHSS

Tal y como muestra la ilustración de arriba, la potencia de emisión se concentra en una franja estrecha del espectro. Tenemos una señal transmitida de banda estrecha pero de gran intensidad (suficiente para cubrir el área de la WLAN), lo cual da una elevada relación señal / ruido (SNR o S / N). De acuerdo con el teorema de Shannon la elevada SNR permitirá una capacidad de canal alta (tasa de bits de información alta).

$$C = B \cdot \log_2(1 + SNR)$$

Ecuación 2-1: Teorema de Shannon

DSSS (Direct Sequence Spread Spectrum).

En DSSS o Técnica de Espectro Expandido por Secuencia Directa, los datos se codifican con un código de pseudorruido dando lugar a una secuencia de símbolos parecida al ruido y con mucha redundancia (el número de bits enviados realmente es muy superior a la tasa real de bits transmitidos). Esta redundancia se construye de tal manera que el receptor es capaz de regenerar los datos originales aún en el caso de que se presente una interferencia dentro del canal, siempre y cuando la interferencia sea de una anchura relativamente pequeña..

Veamos el procedimiento de ensanchado de la señal.

Ilustración 2-12: Procedimiento de ensanchado**.**

La señal original es una señal radio de banda estrecha que ha sido expandida aplicando una secuencia de chips [2] a cada uno de los bits que la componen. Estas secuencias de chips se llaman códigos de pseudorrruido, códigos pseudoaleatorios o códigos PN (Pseudorandom Noise). La duración de un chip es mucho menor que un periodo de bit de la secuencia original, por lo que la tasa del código PN será mucho mayor que el régimen binario de la secuencia original. Esto trae como consecuencia el ensanchado de la señal. De esta manera se aumenta el ancho de banda de la transmisión y se reduce la densidad de potencia espectral [2-5].

[2] Un chip es un dígito binario usado para el proceso de ensanchado, no contiene ningún tipo de información como la contenida en un bit

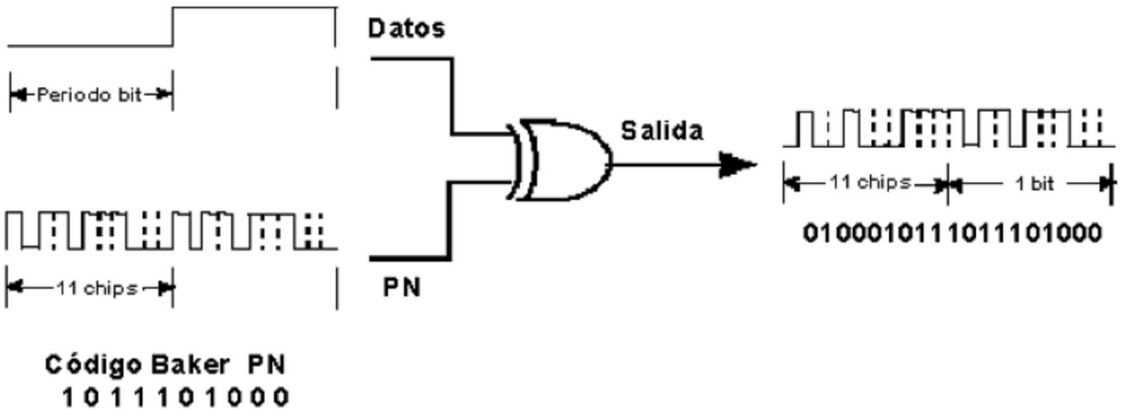


Ilustración 2-13: Proceso de codificación.

Como código PN en DSSS se usa una secuencia de Baker de 11 chips. Éstas tienen unas excelentes propiedades de autocorrelación y son muy tolerantes a los efectos del retardo producidos por multitrayecto. El proceso de codificación consiste en realizar una función XOR de la secuencia de Baker y la secuencia original de tal manera que cada bit a transmitir se codifica con toda la secuencia completa de 11 chips. El resultado de esta operación es una secuencia con una frecuencia once veces superior a la de la señal de datos original que se pretendía transmitir [2-6]. Todo esto se muestra en la ilustración anterior.

El proceso de transmisión en DSSS se resume con el siguiente diagrama

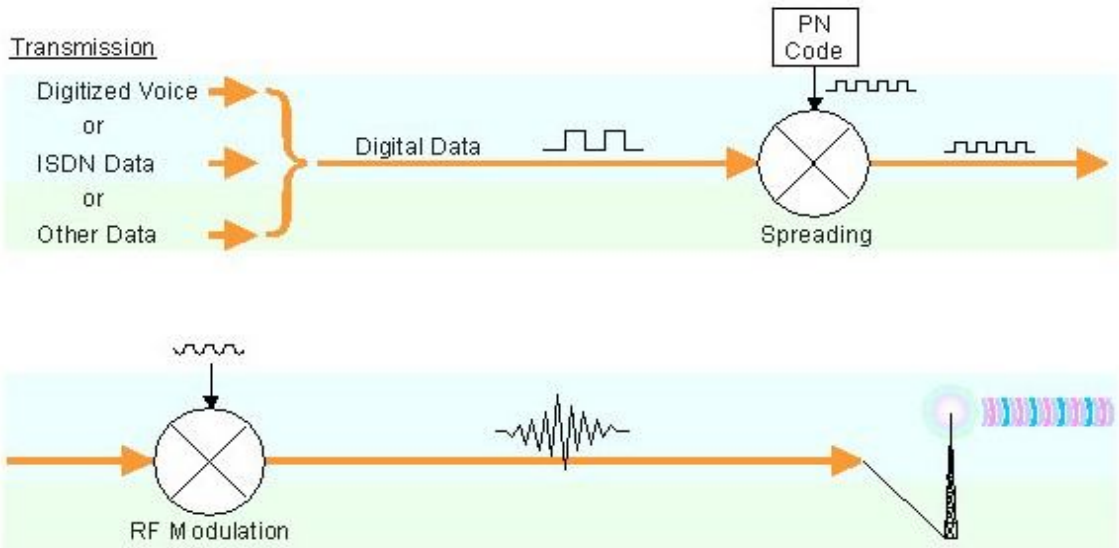


Ilustración 2-14: Esquema del transmisor DSSS

En el receptor, el correlador comparará la señal recibida con su secuencia PN. Transmisor y receptor deben usar la misma secuencia de ensanchado para determinar el bit que se codificó. Para un receptor de banda estrecha, la señal transmitida se puede confundir con ruido, en cambio, en un receptor adecuado en el que tengamos un correlador, se puede recuperar la señal consiguiendo además una gran protección frente al ruido tal y como se puede observar en la siguiente figura.

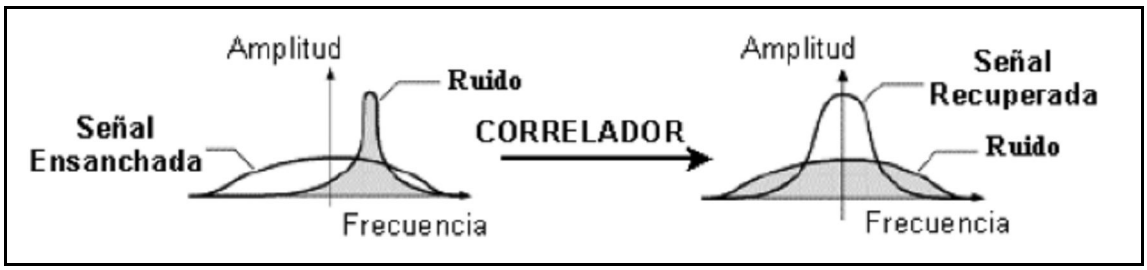


Ilustración 2-15: Efecto del ensanchado sobre el ruido**.**

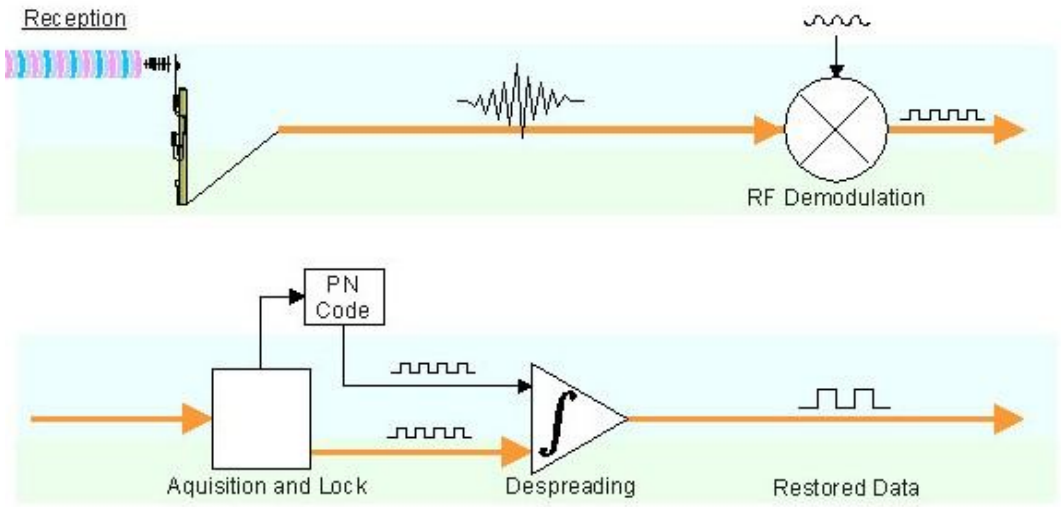


Ilustración 2-16: Esquema de un receptor DSSS

Ahora, la potencia de transmisión se reparte en un rango mucho más amplio que en FHSS, sin embargo son similares (en el ejemplo los 100mW máximos permitidos en Europa). Ahora tenemos una señal de banda ancha pero de baja intensidad, lo cual nos dará una SNR pequeña. La ley de Shannon nos dice que con una relación señal / ruido pequeña la capacidad del canal será menor.

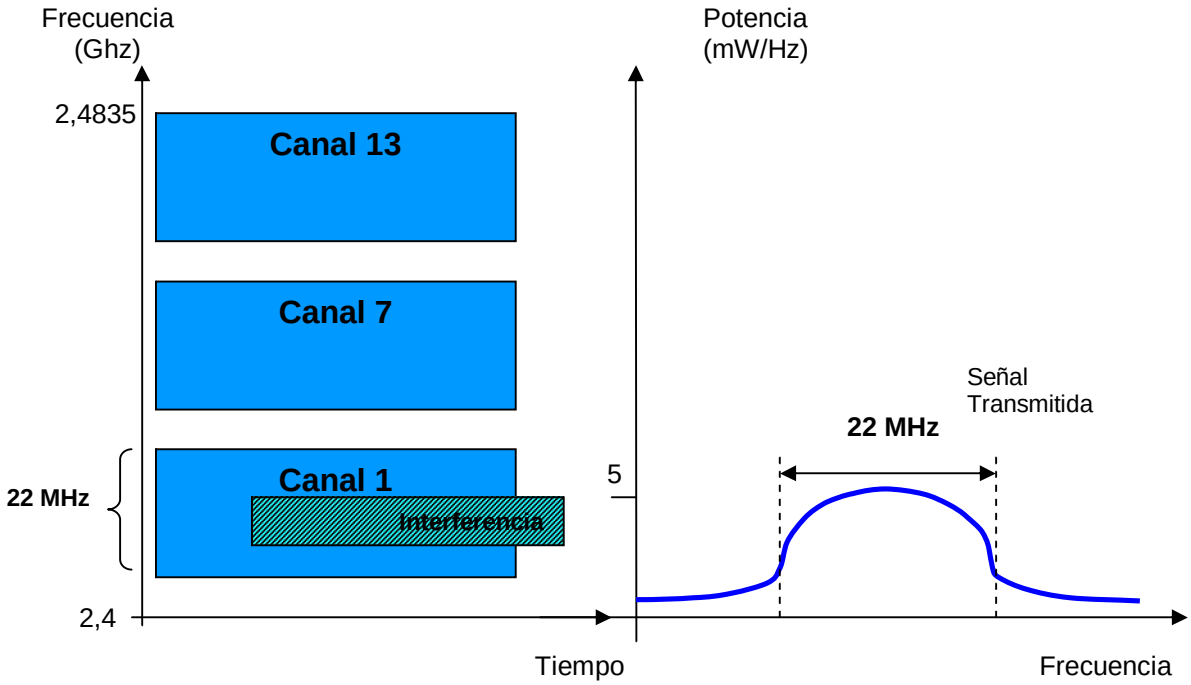


Ilustración 2-17: Funcionamiento DSSS

DSSS tiene definidos dos tipos de modulaciones a aplicar a la señal de información una vez se sobrepone la señal de chip tal y como especifica el estándar IEEE 802.11: la modulación DBPSK, Differential Binary Phase Shift Keying y la modulación DQPSK, Differential Quadrature Phase Shift Keying. Ambas las explicaremos en la sección 2.3.3.

DSSS opera en la banda de 2.4 GHz con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en 14 canales con un ancho de banda por canal de 22 MHz. Cada canal está desplazado 5MHz con respecto al anterior, por lo que los canales contiguos se solapan.

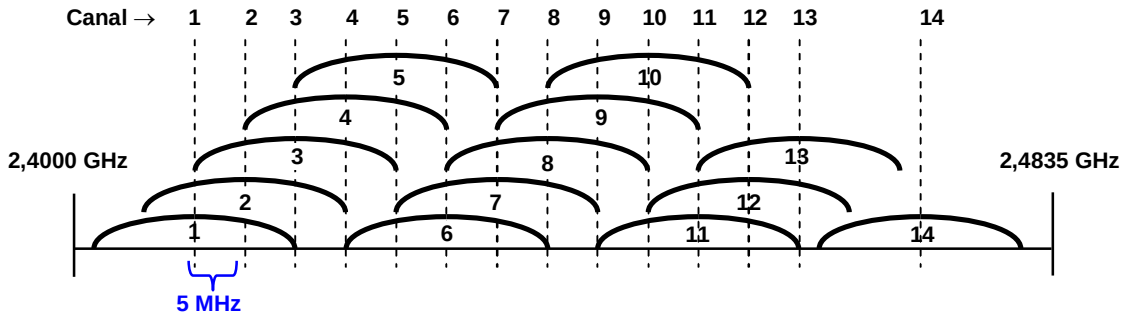


Ilustración 2-18: Distribuición de canales DSSS

En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30 MHz. Esto significa que de los 83.5 MHz de ancho de banda total disponible podemos obtener un total de 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica sin que aparezcan interferencias en un canal procedentes de los otros dos canales. En Estados Unidos la FCC sólo define 11 canales, de los cuales los no solapados son el 1, 6 y 11. En cambio, en Europa, la ETSI (European Telecommunications Standards Institute) define 13 canales de los cuales los no solapados son el 1, 7 y 13, como se observa en la ilustración 2-16.

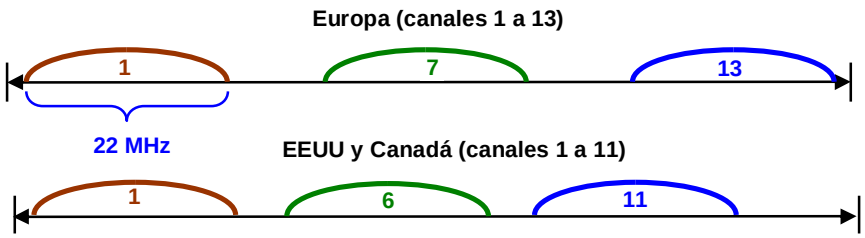


Ilustración 2-19: Canales no solapados

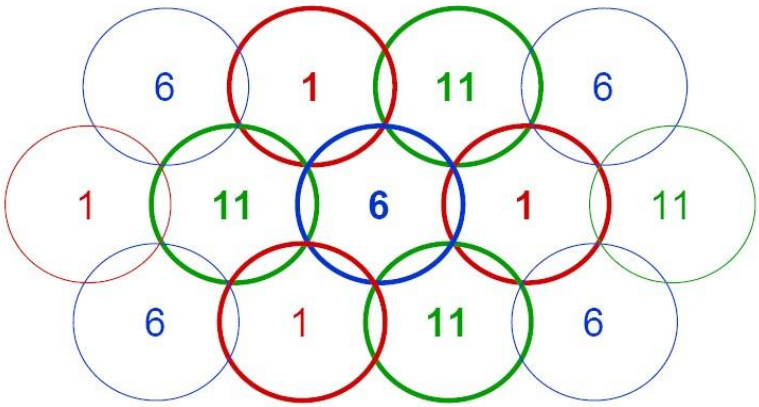


Ilustración 2-20: Distribución de celdas y canales

2.3.2.2. OFDM (Orthogonal Frequency Division Multiplexing).

OFDM o en español Multiplexación Ortogonal por División de Frecuencias, es una técnica que codifica una transmisión en múltiples subportadoras ortogonales. El procedimiento consiste en tomar un canal y dividirlo en otros más pequeños, llamados subcanales. Cada subcanal se usará para transportar información en paralelo y podrá ser modulado de forma diferente.

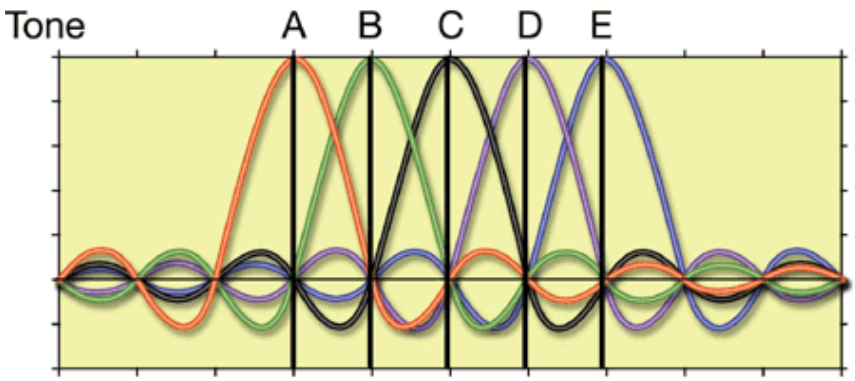


Ilustración 2-21: Subportadoras ortogonales de OFDM

OFDM es parecido a FDM (Multiplexión por División en Frecuencia), pero mientras que en FDM cada usuario dispone de un canal en exclusiva con bandas de guarda para evitar interferirse con otros canales adyacentes desperdiciando por consiguiente ancho de banda, OFDM selecciona canales que se superponen pero que no se interfieren gracias a la propiedad de la ortogonalidad. En concreto toma las señales de cada subcanal y las combina usando la transformada rápida inversa de Fourier (IFFT). Los receptores aplicarán la FFT a la forma de onda recibida para

extraer la amplitud de cada subportadora. De esta forma se consigue llegar a velocidades de transmisión de hasta 54Mbps.

Uno de los problemas de la transmisión de datos es la ISI (Interferencia Entre Simbólos) y la ICI (Interferencia Entre Canales). Para intentar resolverlas, OFDM se reserva la primera parte de cada símbolo como tiempo de guarda. La transformada de Fourier se realizará sólo sobre la parte del símbolo fuera del periodo de guarda. Seleccionar un tiempo de guarda adecuado es uno de los principales problemas de OFDM, si es demasiado corto no protegerá de interferencias y si lo alargamos reducimos la tasa de transmisión.

OFDM puede trasmitir datos a distintas velocidades (6, 9, 12, 18, 24, 36, 48 y 54Mbps) utilizando distintas técnicas de modulación (BPSK, QPSK o QAM).

2.3.2.3. Comparativa

A modo comparativo, introducimos la siguiente tabla que incluye las técnicas de propagación vistas anteriormente destacando sus principales características

Nivel físico	Infrarrojos	FHSS	DSSS	OFDM
Banda	850–950nm	2,4 GHz	2,4 GHz	2,4 y 5 GHz
Estándares	802.11	802.11	802.11 802.11b/g	802.11a/g
Velocidades (en Mbps)	**802.11:** 1 y 2	**802.11:** 1 y 2	**802.11**: 1 y 2 **802.11b**: 5'5 y 11. **802.11g:** 11, 5'5, 2, 1	**802.11a**: 6, 9, 12, 18, 24, 36, 48, 54. **802.11g:** 54, 48, 36, 24, 18, 11, 5.5, 2, 1.
Alcance (velocidad máx)	20 m	150 m	30 m	5 m
Utilización	Muy poca	Poca. En desuso	Mucha	Creciente
Antigüedad	-	Más antiguo	Media	Más moderno
Características	No atraviesa paredes	Interferencias con MW y Bluetooth. $SNR_{FHSS} > SNR_{DSSS}$ $Ptx_{FHSS} < Ptx_{DSSS}$	Buen rendimiento Buen alcance $SNR_{DSSS} < SNR_{FHSS}$ $Ptx_{DSSS} < Ptx_{FHSS}$	Máximo rendimiento

Tabla 2-2: Tabla comparativa de técnicas de propagación

2.3.3. Técnicas de Modulación

En este apartado tratamos el otro aspecto que nos queda por comentar de la capa física, las modulaciones. Destacaremos sobre todo sus principales características y su funcionamiento.

El principio de cualquier modulación es trasladar la información de una banda de frecuencias a otra, dotándola, además, de ciertas propiedades que contribuirán a adaptarla a las características del canal de comunicaciones. La modulación usada puede ser un aspecto crítico a la hora de decidirnos entre un estándar u otro, dado que el uso de una u otra puede ser la solución a un problema de interferencias excesivas, ambientes superpoblados o velocidades reducidas de transmisión. La modulación elegida marca la velocidad máxima a la que podemos aspirar dentro de un estándar y una vez elegida una, decidirnos por alguna de sus posibles variantes puede ser la clave para alcanzar tasas de transmisión elevadas.

Todas las modulaciones usadas por los estándares de la familia IEEE 802.11 son digitales. Las modulaciones digitales aportan una serie de ventajas sobre las modulaciones analógicas tradicionales, como pueden ser mayor inmunidad al ruido, multiplexación más fácil, mayor robustez a interferencias sobre el canal, posibilidad de dotar a la información de más seguridad y ahorro en el ancho de banda mediante la compresión de los datos.

2.3.3.1. GFSK (Gaussian Frequency Shift Keying).

GFSK o modulación por desplazamiento de frecuencia gaussiana corresponde a la modulación usada por FHSS. En ésta un 1 lógico es representado mediante un incremento de la frecuencia de la portadora, y un 0 mediante un decremento de la misma. GFSK es una versión mejorada de la modulación por desplazamiento de frecuencia (FSK). La G de gaussiano se refiere a la forma del pulso que se utiliza para su transmisión: la información es pasada por un filtro gaussiano antes de modular la señal. Esto se traduce en un espectro de energía más estrecho de la señal modulada, lo que permite que haya otros usuarios, reduciéndose así la probabilidad de interferirse entre ellos.

Entre las variedades de esta modulación usadas por FHSS encontramos dos, 2GFSK y 4GFSK. La implementación más básica de GFSK es 2GFSK (de dos niveles). Esta utiliza dos frecuencias diferentes para transmitir un uno o un cero. Para transmitir un 1 la frecuencia de la portadora se incrementará en un cierto valor; mientras que para la codificación de un 0 simplemente se transmitirá la portadora sin ningún incremento. La representación de esto lo podemos ver en la

siguiente figura, en la que se muestra como sería la señal para la representación de un símbolo uno y la señal para la representación de un símbolo cero. Con 2GFSK se consiguen tasas de hasta 1 Mbps.

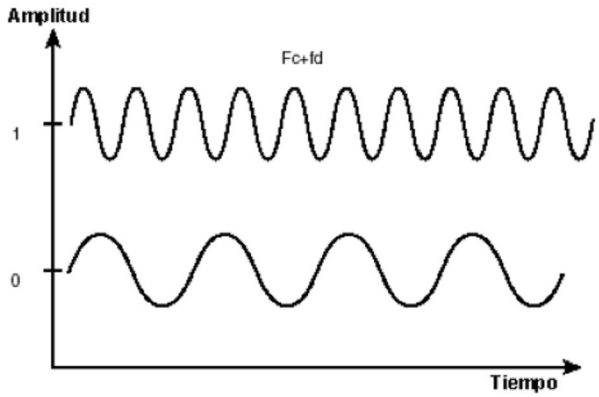


Ilustración 2-22: Señales 2-GFSK

Para poder enviar más datos tenemos dos posibilidades, usar una tasa de símbolos mayor o codificar más bits por símbolo. La modulación 4GFSK (GFSK de cuatro niveles) opta por usar cuatro símbolos en lugar de dos, así consigue codificar más bits por símbolo. Los cuatro símbolos son 00, 01, 10 y 11, ahora tenemos dos bits empaquetados por símbolo. Cada uno corresponde a una cierta frecuencia discreta. Se tiene así una tasa de datos de hasta 2 Mbps. La representación de los cuatro símbolos en frecuencia se muestra en la siguiente figura.

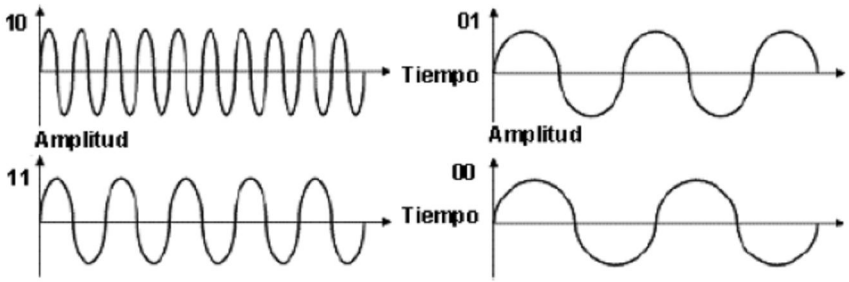


Ilustración 2-23: Señales 4-GFSK

2.3.3.2. PSK (Phase Shift Keying).

La modulación por desplazamiento de fase o PSK es una forma de modulación angular consistente en hacer variar la fase de la portadora entre un número finito de ángulos. Esta modulación es usada por OFDM. La diferencia con la modulación de fase convencional (PM) es que mientras en ésta la variación de

fase es continua, en la PSK la señal moduladora es una señal digital y, por tanto, tiene un número de estados limitado.

Dependiendo del número de posibles fases a tomar, recibe diferentes denominaciones. Así tendremos BPSK con 2 fases (equivalente a PAM), QPSK con 4 fases (equivalente a QAM), 8-PSK con 8 fases y así sucesivamente. A mayor número de posibles fases, mayor es la cantidad de información que se puede transmitir utilizando el mismo ancho de banda, pero mayor es también su sensibilidad frente a ruidos e interferencias.

La gran ventaja de las modulaciones PSK es que la potencia de todos los símbolos es la misma, por lo que se simplifica el diseño de los amplificadores y etapas receptoras (reduciendo costes) dado que la potencia de la fuente es constante. Las modulaciones BPSK y QPSK en particular, son óptimas desde el punto de vista de protección frente a errores.

2.3.3.3. DPSK (Differential phase shift keying).

Existen dos alternativas de modulación PSK: PSK convencional, donde se tienen en cuenta los desplazamientos de fase y PSK diferencial o DPSK, en la cual se consideran las transiciones.

DPSK es la técnica usada por DSSS y significa (en español) modulación diferencial por desplazamiento en la fase. En una modulación diferencial lo importante no es la forma de la onda, si no los cambios que se producen en ella respecto a la anterior. La codificación diferencial no permite una detección del todo óptima, pero tampoco se necesita un control excesivo sobre la fase de la portadora. Este tipo de modulaciones, como la información va en la fase y no en la amplitud, son relativamente inmunes al ruido, que suele afectar a la amplitud. Además utiliza una electrónica más simple y barata.

El problema de DPSK es que si cometemos un error en la recepción, como para la siguiente decodificación nos basaremos en la actual, el error tiende a propagarse a intervalos adyacentes. Este problema no se presenta en su versión no diferencial, PSK.

Las dos modulaciones diferenciales usadas son DBPSK y DQPSK. El formato más simple es DBPSK, en este sólo se detectará un cambio en la fase de la portadora. Si en lugar de un bit por símbolo queremos usar más carga de datos por símbolo, a fin de aumentar la tasa de transmisión, usaremos DQPSK. Con DBPSK se conseguirán tasas de transmisión en DSSS de 1 Mbps, llegando a los 2 Mbps si la

elección es DQPSK. Si las condiciones del medio son muy adversas se deberá trabajar con DBPSK, por ser una modulación más robusta.

2.3.3.4. Otras Modulaciones

CCK (Complementary Code Keying) es la modulación usada por el estándar 802.11b para conseguir velocidades de 5'5 y 11Mbps. Esta técnica sirve para modular los datos a la vez que para ensanchar la señal y fue adoptada para reemplazar al código de Baker.

El flujo de datos a enviar se divide en grupos de 8 bits. Cada grupo de 8 bits se empleará para codificar los parámetros de fase, que más tarde darán lugar a la palabra de código. La equivalencia entre los bits de un grupo y la fase a la que representan está basada en la modulación DQPSK. La palabra de código en CCK (generada a partir de los grupos de 8 bits) poseerá una longitud de 8 chips y será utilizada a su vez para ensanchar esos 8 bits de información.

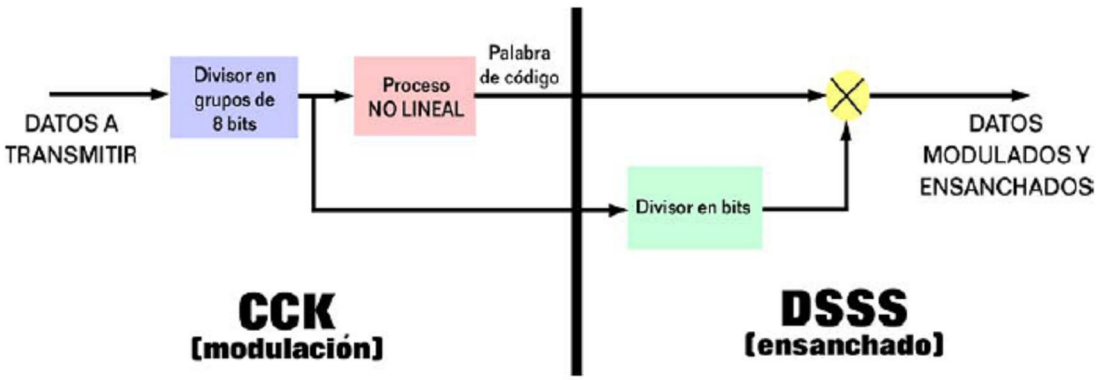


Ilustración 2-24: Modulador DQPSK-CCK

PBCC (Packet Binary Convolutional Coding) es una modulación que fue adoptada por el comité IEEE 802.11b como complemento opcional a la obligatoria CCK debido a que se pensó que podría ofrecer mayor robustez para aplicaciones futuras. Utiliza una estructura de código diferente a la de CCK y su constelación de señal es más compleja. PBCC usa una 8-PSK frente a la DQPSK empleada por CCK. Usando 8-PSK, PBCC es capaz de alcanzar 22 Mbps de tasa de transmisión, aunque no se aprovecha la totalidad de la tasa potencial que ofrece este método. Esta modulación posee una buena respuesta a la interferencia, y al efecto multitrayecto sólo si se emplean complejos ecualizadores. Además, el proceso de decodificación es muy complejo y no está aprobada por los organismos reguladores.

2.4. La capa MAC

Como vimos anteriormente, el nivel de enlace de la familia 802.11 se divide a su vez en dos subniveles: MAC y LLC. Este apartado se dedica al estudio del subnivel MAC o de Control de Acceso al Medio, situado entre cualquiera de los diferentes niveles físicos estudiados antes y el subnivel LLC (Logical Link Control).

Tenemos un medio, en nuestro caso el aire, compartido por una serie de estaciones, todas ellas queriendo transmitir. Sin embargo sólo una de ellas puede acceder al canal en cada momento. Los métodos de acceso al medio permiten regular el uso del canal de la mejor manera posible, atendiendo a cuatro criterios principalmente: retardo de acceso, caudal efectivo, equidad y simplicidad. La capa MAC proporciona el mecanismo de control de acceso al medio compartido y cada estación y punto de acceso debe implementar una capa MAC.

La arquitectura MAC se compone de dos funcionalidades: la función de coordinación puntual (PCF) y la función de coordinación distribuida (DCF). Cada una de estas funciones define un modo de acceso para las estaciones que conforman la red. La DCF se usa para servicios que acceden al medio mediante contienda con otros usuarios (acceso aleatorio) y la PCF para servicios libres de contienda (acceso determinista).

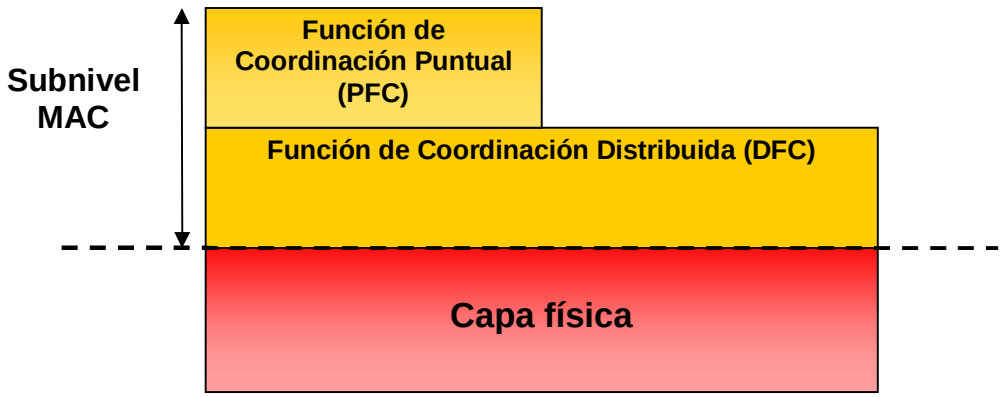


Ilustración 2-25: Modelo de referencia de la capa MAC

Además la capa MAC proporcionará otros servicios básicos específicos de la tecnología inalámbrica como son la gestión de movilidad, la gestión de potencia, la

sincronización y funciones de seguridad. Todo esto lo veremos con detalle a continuación.

2.4.1. Función de Coordinación Distribuida

Definimos función de coordinación como la funcionalidad que determina cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo de nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida (DFC) y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.

El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios no predecibles por lo que no son tolerados por los servicios síncronos.

Sus características las podemos resumir en estos puntos:

- Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio.
- Utiliza los reconocimientos (ACKs), provocando retransmisiones si no se reciben.
- Usa NAV (Network Allocation Vector) para que todos los nodos que estén escuchando conozcan cuándo volverá a quedar libre el canal.
- Implementa fragmentación y reensamblado de datos
- Concede prioridad a tramas mediante el espaciado entre tramas (IFS)

2.4.1.1. Protocolo de Acceso al Medio

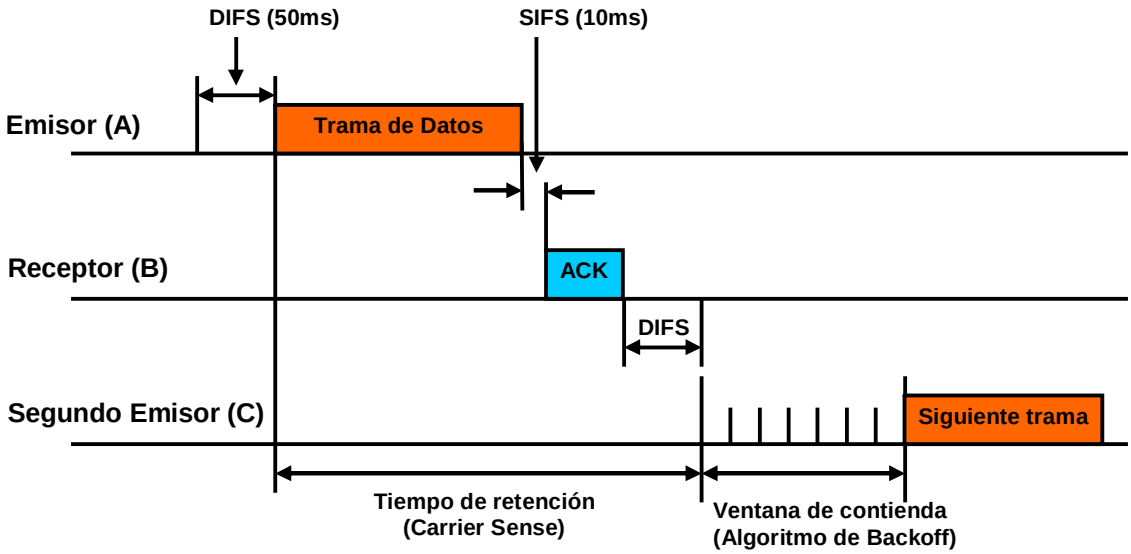
CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

El protocolo básico de acceso de Ethernet (estándar IEEE 802.3) es el CSMA/CD (Carrier Sense Multiple Access / Collision Detection). Esta técnica consiste en lo siguiente: las estaciones antes de transmitir miran primero si hay otra haciéndolo. Si no es así intentan transmitir ellas, manteniéndose a la escucha del canal. Si aprecian diferencia entre la señal del canal y su señal suponen que ha ocurrido una colisión (detección de colisión). En ese momento dejan de transmitir el paquete y difunden una señal especial (señal de jamming) para avisar al resto de

estaciones que deben descartar el paquete. Después esperan un tiempo aleatorio antes de volver a intentar transmitir.

Dado que es muy costoso implementar radiorreceptores que transmitan y reciban al mismo tiempo, la técnica empleada en 802.11 es CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) o Acceso Múltiple por Detección de Portadora con Evasión de Colisiones. La diferencia principal radica en la detección de colisiones, ya que en el aire es difícil detectar una colisión, lo que hace que CSMA/CA intente evitar las colisiones (Collision Avoidance).

Para entender claramente el funcionamiento de CSMA/CA utilizaremos un ejemplo:



DIFS: DCF (Distributed Coordination Function) Inter Frame Space
SIFS: Short InterFrame Space

Ilustración 2-26: Funcionamiento de CSMA/CA

Supongamos que una estación "A" desea transmitir una trama hacia "B" y detecta que el canal está libre. "A" espera el tiempo DIFS (50ms) y a continuación empieza a transmitir. De esta forma se asegura que cualquier trama emitida en la red irá separada de la anterior al menos por este espacio de tiempo.

Una vez ha terminado de emitir su trama, "A" espera una confirmación (ACK) de "B". Dicha confirmación es un mensaje de alta prioridad, por lo que no ha de esperar el tiempo habitual DIFS después de que termine la trama de "A", sino que sólo ha de esperar el tiempo SIFS (10ms).

En algún momento durante la emisión de la trama de "A", un segundo emisor "C" desea enviar una trama a una estación "D" (no mostrado en la figura). "C" escucha el canal y comprueba que está ocupado, por lo que espera hasta que termine la transacción actual.

Cuando la transmisión de la trama de "A" a "B" termina, "C", que seguía a la escucha, detecta el canal libre y comienza un tiempo de espera DIFS. Como el canal vuelve a estar ocupado a los SIFS segundos (10ms) por el ACK de "B" y no se ha llegado a producir una pausa lo bastante grande (el tiempo esperado ha sido menor que DIFS, 50ms), "C" seguirá esperando hasta el fin del ACK.

Cuando por fin termina el ACK de "B", "C" comienza de nuevo el tiempo de espera que ahora sí es lo suficientemente grande (esta vez el tiempo de espera ha sido mayor o igual que DIFS, 50ms). Pero ahora no transmite de inmediato sino que la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina otra espera adicional y aleatoria escogida uniformemente entre un intervalo [CWmín, CWmáx] llamado ventana de contienda (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) y su función es la de reducir la probabilidad de colisión con otras estaciones que pudieran también estar observando el proceso de "A" y "B" y esperando para transmitir a continuación.

Mientras se ejecuta la espera marcada por el algoritmo de Backoff, "C" continúa escuchando el medio. Si durante la ventana de congestión asignada "C" detecta que alguna estación transmite, congelará su contador de tiempo aleatorio para volver a activarlo un tiempo DIFS (50ms) después de que haya cesado toda actividad. Si por el contrario no detecta actividad alguna, la espera proseguirá hasta consumir todas las ranuras temporales asignadas.

Colisiones

Las colisiones pueden producirse porque dos estaciones a la espera elijan el mismo número de intervalos (mismo tiempo aleatorio) para transmitir después de la emisión en curso. En este caso la estación repite el proceso antes descrito, pero al tratarse de un segundo intento esta vez se amplía el rango de intervalos para la elección del tiempo aleatorio. El número de intervalos crece de forma exponencial hasta un valor máximo a partir del cual el contador se reinicia y el proceso se repite desde el principio. El proceso es similar a Ethernet salvo que las estaciones no detectan la colisión sino que infieren que se ha producido cuando no reciben el ACK esperado.

También se produce una colisión cuando dos estaciones deciden transmitir a la vez, o casi a la vez. Pero este riesgo es mínimo.

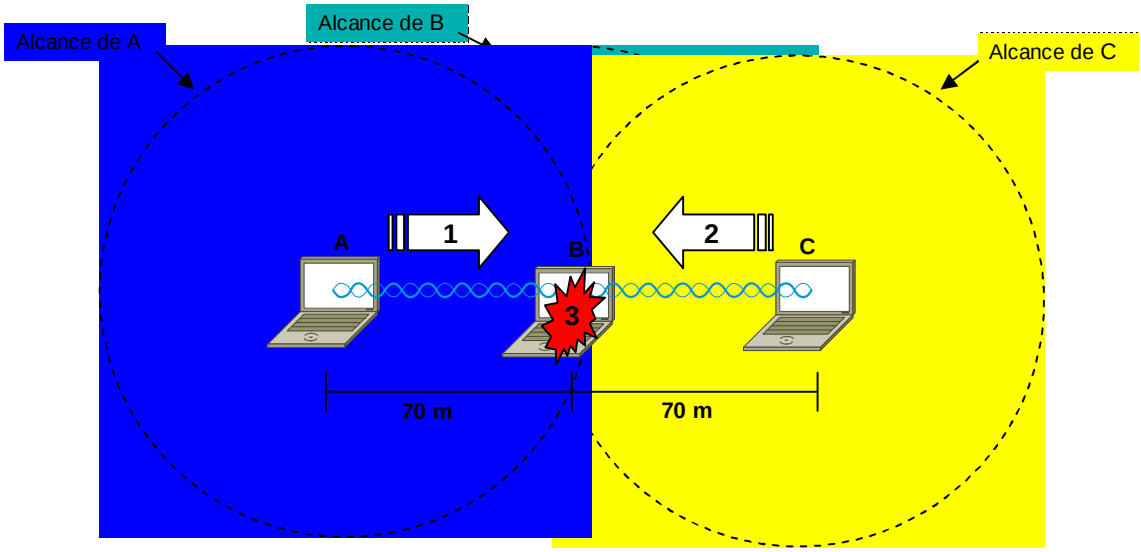
El problema de CSMA/CA en entornos inalámbricos

CSMA/CA en un entorno inalámbrico y celular presenta dos problemas principalmente:

- **Estación oculta.** Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no oye.
- **Estación expuesta.** Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

Esto provoca conflictos como el que describimos en la ilustración 2-27.

Supongamos que "A" quiere enviar una trama a "B". "A" detecta que el canal está libre y empieza a transmitir. Instantes más tarde, cuando "A" está aún transmitiendo, "C" quiere también enviar una trama a "B"; "C" detecta que el canal está libre, ya que el no está recibiendo la emisión de "A" pues se encuentra fuera de su radio de cobertura. Por tanto "C" empieza a transmitir y en "B" se produce una colisión. Como consecuencia "B" no recibe correctamente ni la trama de "A" ni la trama de "C".



1: A quiere transmitir una trama a B. Detecta el medio libre y transmite

2: Mientras A está transmitiendo C quiere enviar una trama a B. Detecta el medio libre (pues no capta la emisión de A) y transmite

3: Se produce una colisión en la intersección por lo que B no recibe ninguna de las dos tramas

Ilustración 2-27: Problema de la estación oculta

MACA (MultiAccess Collision Avoidance)

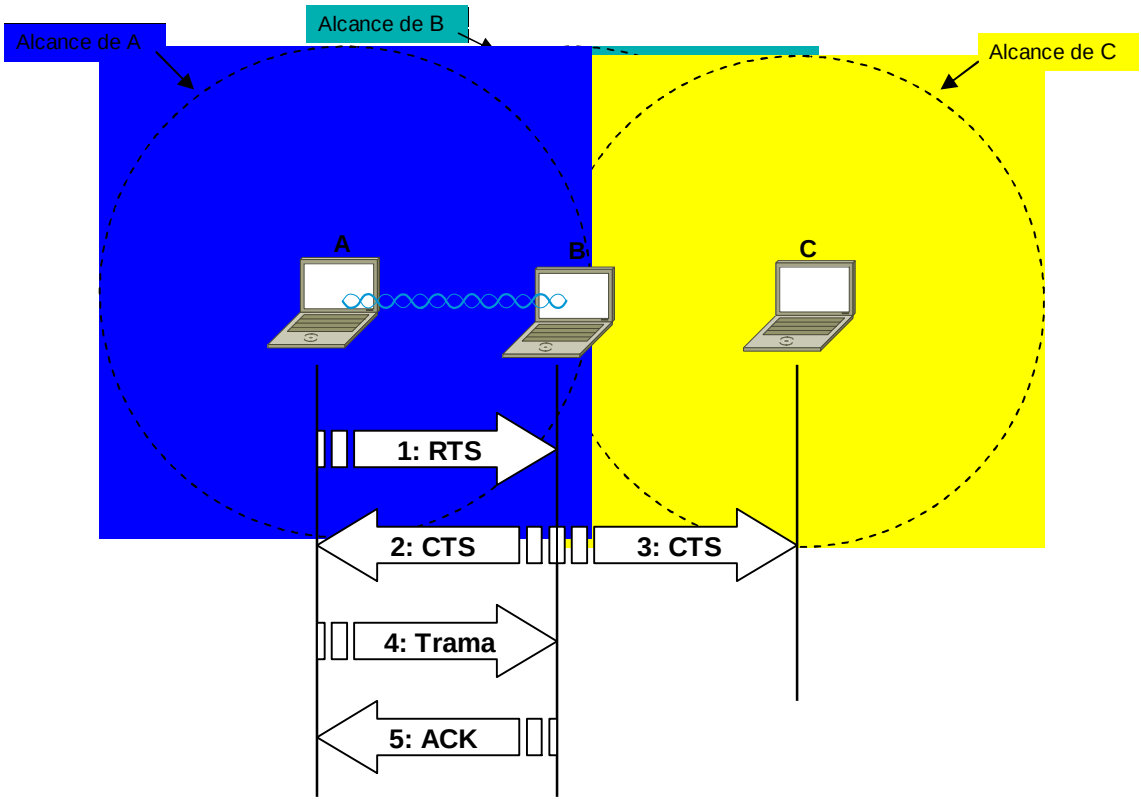
La solución que propone 802.11 al problema de la estación oculta/expuesta es complementar el protocolo CSMA/CA con el intercambio de mensajes RTS y CTS. Antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

El uso de mensajes RTS/CTS se denomina a veces Virtual Carrier Sense. Y el uso conjunto de CSMA/CA y RTS/CTS conforma el llamado protocolo MACA (MultiAccess Colision Avoidance). Veamos cómo se soluciona el problema planteado en la ilustración anterior con el uso de este protocolo.

El emisor "A" envía un mensaje RTS a "B" en el que le advierte de su deseo de enviarle una trama; además en dicho mensaje "A" le informa de la longitud de la misma. Este mensaje no es recibido por "C".

Como respuesta al mensaje de "A", "B" envía un CTS en le que le confirma su disposición a recibir la trama que "A" le anuncia. Dicho mensaje CTS lleva

también indicada la longitud de la trama que "B" espera recibir de "A". "C" no recibe el mensaje RTS enviado por "A", pero sí recibe el CTS enviado por "B". Del contenido del mensaje CTS, "C" puede deducir por cuanto tiempo estará ocupado el canal que comparte con "B", pues el mensaje incluye indicación de la longitud de la trama a transmitir y "C" conoce la velocidad con que se realiza la transmisión.



1. Antes de transmitir la trama, A envía un RTS a B: "quiero transmitir a B una trama de 500bytes"

2. B responde con un CTS: "OK, envíame esa trama de 500 bytes"

3. C no capta el RTS pero sí el CTS: "No puedo transmitir en un periodo equivalente de 500 bytes

4 y 5. A envía la trama y recibe la confirmación de B

Ilustración 2-28: Intercambio de mensajes RTS/CTS

2.4.1.2. NAV (Network Allocation Vector)

Las estaciones tienen un conocimiento específico de cuándo va a finalizar el periodo de reserva del canal de la estación que está transmitiendo/recibiendo en ese momento. Esto se hace a través de una variable llamada NAV (Network Allocation Vector) que mantendrá una predicción de cuando el medio quedará liberado. Tanto al enviar un RTS como al recibir un CTS, se envía el campo Duration/ID con el valor reservado para la transmisión y el subsiguiente

reconocimiento Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo Duration/ID. En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.

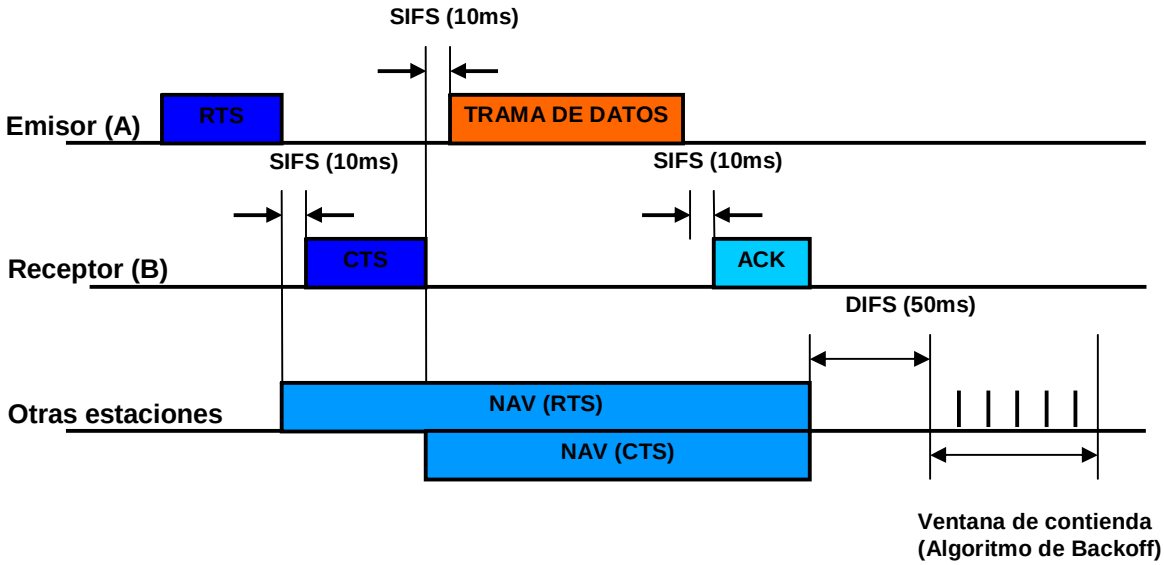


Ilustración 2-29: NAV

2.4.1.3. Fragmentación Y Reensamblado

Muchas de las interferencias que se producen en las transmisiones por radio afectan la emisión en intervalos muy cortos de tiempo. En estos casos la transmisión de tramas grandes resulta especialmente comprometida, pues el riesgo de que una interferencia estropee toda la emisión es muy grande. En situaciones de elevada tasa de error del medio físico es preferible manejar tramas de pequeño tamaño. Sin embargo el nivel de red, que no tiene un conocimiento de la situación de la red inalámbrica, suministra el paquete al nivel de enlace para que lo envíe en una única trama. Por este motivo el nivel MAC de 802.11 prevé un mecanismo por el cual el emisor puede, si lo considera conveniente, fragmentar la trama a enviar en otras más pequeñas. El receptor a su vez reensamblará la trama original para que sea entregada a los niveles superiores, con lo que la fragmentación actuará de forma transparente a ellos.

En el caso de producirse fragmentación cada fragmento se enviará siguiendo el mecanismo de CSMA/CA antes descrito, y recibirá el correspondiente ACK del receptor. Por cada fragmento se devuelve un ACK por lo que, en caso necesario, es retransmitido por separado. El overhead (o sobrecabecera) que puede

introducir el uso de la fragmentación es considerable, pero puede ser rentable cuando la red tiene mucho ruido. Si el emisor ve que las tramas no están llegando bien puede decidir fragmentar las tramas grandes para que tengan más probabilidad de llegar al receptor. Todas las estaciones están obligadas a soportar la fragmentación en recepción, pero no en transmisión.

2.4.2. Función de Coordinación Puntual

La otra forma de acceso al medio se basa en la función de coordinación puntual (PFC). Con esta función se pueden transmitir tramas sin tener que pasar por una contienda para ganar el medio, lo que puede ser útil para tramas en las que el tiempo de procesado es crítico como la transmisión de voz o vídeo. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio.

Existe un nodo organizador o director, llamado punto de coordinación o PC. El punto de coordinación se encuentra ubicado en el punto de acceso y controla las transmisiones de tramas por parte de las estaciones. Al principio de un periodo libre de contienda, PC gana el control del medio dado que sólo espera un intervalo PIFS, intervalo menor que el del resto de las estaciones que operan bajo DFC. Entonces enviará una trama de configuración CF-Poll (trama Beacon) a cada estación que pueda transmitir en PFC, concediéndole el poder de transmisión. Esta trama incluye el campo CF (Contention Free) con los parámetros establecidos para el periodo libre de contienda, y cuando las estaciones la reciban, actualizarán su NAV al valor que se indique. El PC mantendrá una lista con todos los datos de las estaciones que se han asociado al modo PFC. La concesión de transmisiones será por riguroso listado y no permitirá que una estación envíe dos tramas hasta que la lista se haya completado.

DCF y PFC pueden operar conjuntamente en una misma celda dentro de una estructura llamada supertrama. Una parte de esta supertrama se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finaliza este periodo, el punto de acceso toma el medio y se inicia un periodo libre de contienda en el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.

2.4.3. Formato de trama MAC

Hay tres tipos de tramas MAC:

- **Tramas de datos**: usadas para la transmisión de datos
- **Tramas de control**: usadas para el control de acceso al medio (p.e. RTS/CTS)
- **Tramas de gestión**: se transmiten de la misma forma que las tramas de datos pero contienen información de gestión y no pasan a las capas superiores.

Cada uno de estos tipos está dividido a su vez en subtipos que dependerán de la función específica de la trama.

Todas las tramas IEEE 802.11 están formadas por los siguientes campos:

Preámbulo	Cabecera PLCP	Datos MAC

Ilustración 2-30: Formato de una trama IEEE 802.11 genérica

2.4.3.1. Preámbulo

Es dependiente del medio físico e incluye dos campos:

- **Synch:** secuencia de 80 bits para seleccionar la antena adecuada (si trabajamos en diversidad) y para sincronización
- **SFD (Starter Frame Delimiter):** consiste en un patrón de 16 bits (0000 1100 1011 1101) para la delimitación y temporización de la trama.

2.4.3.2. Cabecera PLCP

Contiene información lógica que usará la capa física para decodificar la trama.

2.4.3.3. Datos MAC

La trama MAC genérica tiene los siguientes campos:

Octetos:

2	2	6	6	6	2	6	0-2312	4
Control Trama	**Duration/ID**	**Add1**	**Add2**	**Add3**	**Control Secuencia**	**Add4**	**Cuerpo de trama**	**CRC**

Cabecera MAC

Ilustración 2-31: Formato de una trama MAC genérica

- **Control de Trama**. Lo examinaremos aparte más abajo.
- **Duration/ID.** Tiene dos significados dependiendo del tipo de trama. En tramas del tipo Power-Save para dispositivos con limitaciones de potencia, contiene el identificador de estación. En el resto de tramas, es el valor reservado para la transmisión, usado para el cálculo de NAV.
- **Campos Address1-4.** Contiene las direcciones de 48 bits (direcciones MAC) de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.
- **Control de secuencia.** Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- **Cuerpo de la trama**. Varía según el tipo de trama que se quiere enviar.
- **FCS.** Contiene el checksum.

Control de Trama

Los campos de control de trama tienen el formato siguiente:

Octetos:

2	2	4	1	1	1	1	1	1	1	1
Protocol Versión	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mng	More Data	WEP	Order

Ilustración 2-32: Contenido del campo Control de Trama

- **Protocol Version:** para expansiones futuras.
- **Type/Subtype:** Type identifica si la trama es del tipo de datos, control o gestión; Subtype identifica el subtipo dentro de cada uno de estos tipos.
- **ToDS/FromDS:** Indica si la trama se envía/recibe al/del sistema de distribución.
- **More Fragments:** Se activa si se usa fragmentación.
- **Retry:** Se activa si la trama es una retransmisión.
- **Power Management:** Se activa si se utiliza el modo ahorro de energía.

- **More Data:** Se activa si la estación tiene tramas pendientes en un punto de acceso.
- **WEP:** Se activa si se usa el mecanismo de autenticación y encriptado.
- **Order:** Se utiliza con el servicio de ordenamiento estricto.

2.4.4. Servicios básicos y gestión de movilidad

Cuando una estación quiere acceder a una BSS existente, primero necesita obtener información de sincronización, bien del punto de acceso si estamos trabajando en modo infraestructura, o bien de otra estación si estamos trabajando en el modo Ad Hoc. La estación puede obtener esta información mediante dos métodos:

- **Escaneado pasivo**: en este caso la estación espera a recibir una trama Beacon del AP. La trama Beacon, como explicamos posteriormente, es una trama de guía enviada periódicamente (10 veces por segundo) por el AP y que contiene información de sincronización.
- **Escaneado activo**: en este caso la estación intenta encontrar un punto de acceso transmitiendo una trama Probe Request, y esperando la respuesta por parte del AP, Probe Response.

Una vez que la estación ha encontrado un punto de acceso y decide unirse a su célula, deberá autenticarse. El proceso de **autenticación** es el paso previo a la asociación, absolutamente necesario, en el que la estación se identifica al AP, y éste verifica su identidad. Si responde positivamente, la estación quedará registrada en su tabla de direcciones MAC. Si por el contrario le deniega el permiso, la estación no podrá asociarse a la célula. **Desautenticación** es el proceso inverso por el cual una estación solicita darse de baja en la lista de equipos permitidos.

Terminado el proceso de autenticación, comenzará el proceso de **asociación** que consiste en el intercambio de información entre AP y estación sobre sus capacidades. Este proceso permite conocer al AP la posición actual de la estación, y sólo después de finalizarlo la estación sería capaz de transmitir y recibir tramas.

Los equipos gestionan el **envío de datos** hacia y desde la célula. La información se transmite con **privacidad.**

El AP se comportará como un puente inalámbrico y/o como un portal entre las estaciones de su celda y el sistema de distribución. Se encargará de la **distribución** de un paquete desde el punto de acceso origen hasta el punto de acceso destino, si es que el destino es otra estación de la WLAN; o se encargará de la función de **integración** o pasarela si el destino son otras redes o sistemas IEEE 802.x (se encargará de aspectos necesarios como el redireccionamiento).

Si una estación se mueve y cambia de celda detectará otro AP con señal más potente y cambiará su registro. Esto permite la **itinerancia o roaming** que no es más que el movimiento de una estación de una célula a otra sin que las conexiones se corten. Esta función es similar al handover de la telefonía móvil con dos diferencias principalmente:

- En una WLAN (red de conmutación de paquetes) la transición de célula a célula debe ser llevada a cabo entre transmisiones de paquetes, justo al contrario de lo que ocurre en GSM (red de conmutación de circuitos) donde la transición debe ocurrir durante una conversación telefónica. Esto hace que para las WLANs sea un poco más "sencillo".

- Una desconexión temporal puede no afectar a la conversación en su sistema de voz, pero en una WLAN, donde las retransmisiones sí son procedentes, reduciría el rendimiento significativamente.

El estándar 802.11 no define cómo debería de llevarse a cabo el roaming pero sí define las herramientas básicas para ello. Éstas son el escaneado pasivo/activo, explicado anteriormente; y el proceso de **reasociación**, que consiste en el cambio de punto de acceso asociado por parte de una estación. Este cambio se produce cuando el AP al que se encuentra asociado en esos momentos no le proporciona la calidad suficiente, y es la propia estación quien decide cuándo ocurre esto. Entonces realiza una búsqueda para encontrar otro AP. El terminal envía una petición de reasociación al nuevo AP. Si la petición no es aceptada el terminal busca otro AP. Si la petición de reasociación es aceptada, el AP notifica el proceso al sistema de distribución, siendo informado el antiguo AP.

2.4.5. Gestión de potencia

Las Wireless LANs están relacionadas con aplicaciones móviles, y en este tipo de aplicaciones la energía es un recurso escaso. De hecho mucho de los dispositivos de las WLANs trabajan con baterías. Por este motivo el estándar 802.11 dedica un apartado del estándar a la gestión de potencia. En concreto define un modo de

operación de bajo consumo o de potencia limitada que permite a las estaciones "hibernar" durante periodos largos de tiempo sin que conlleve pérdidas de información. A este mecanismo de ahorro de energía se le denomina **Power Saving** y a las estaciones bajo este modo de funcionamiento, PS-STAs (Power Save Stations).

El control de este tipo de estaciones lo llevará el punto de acceso, que tendrá conocimiento de qué estación se ha asociado en este modo. La idea es que los APs mantengan un registro actualizado de todas las PS-STAs y almacenen los paquetes direccionados a éstas, bien hasta que las estaciones los requieran, bien hasta que decidan cambiar de modo de operación. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.

Antes de "echarse a dormir" las estaciones deben avisar a su AP, para que retenga las tramas que se les envíen durante ese tiempo. Periódicamente las estaciones dormidas han de "despertarse" y escuchar si el AP tiene algo para ellos. Si es así el punto de acceso le enviará una trama TIM o Traffic Indication Map para que la estación despierte en el próximo intervalo de portadora. Si las estaciones no solicitan las tramas retenidas pasado un tiempo, el AP las descartará.

2.4.6. Sincronización

La sincronización entre estaciones se consigue mediante una función de sincronización (TSF). Según el modo de funcionamiento ésta será de una manera u otra, aunque nosotros nos centraremos sólo en la TSF para el modo infraestructura.

En el modo infraestructura todas las estaciones sincronizan su reloj de acuerdo con el reloj del punto de acceso, de tal manera que éste enviará el valor de su reloj en el momento de la transmisión en una trama portadora o Beacon. Las estaciones receptoras comprueban su reloj en el momento de recepción, y lo corrigen para mantenerlo sincronizado con el reloj del AP.

2.5. Seguridad

Uno de los problemas más graves a los que se enfrenta WiFi es la seguridad ya que de por sí, el aire es un medio de propagación de libre acceso, y por tanto una red inalámbrica puede verse sometida a escuchas ilegales, acceso no autorizado, usurpación y suplantación de identidad, interferencias aleatorias, denegación de servicio, etc. Para evitar todo esto es imprescindible dotar a las redes inalámbricas de unos determinados mecanismos que garanticen la seguridad de la comunicación.

La siguiente imagen muestra los niveles principales en los que se centra la seguridad de una WLAN y en los que nosotros haremos hincapié a continuación

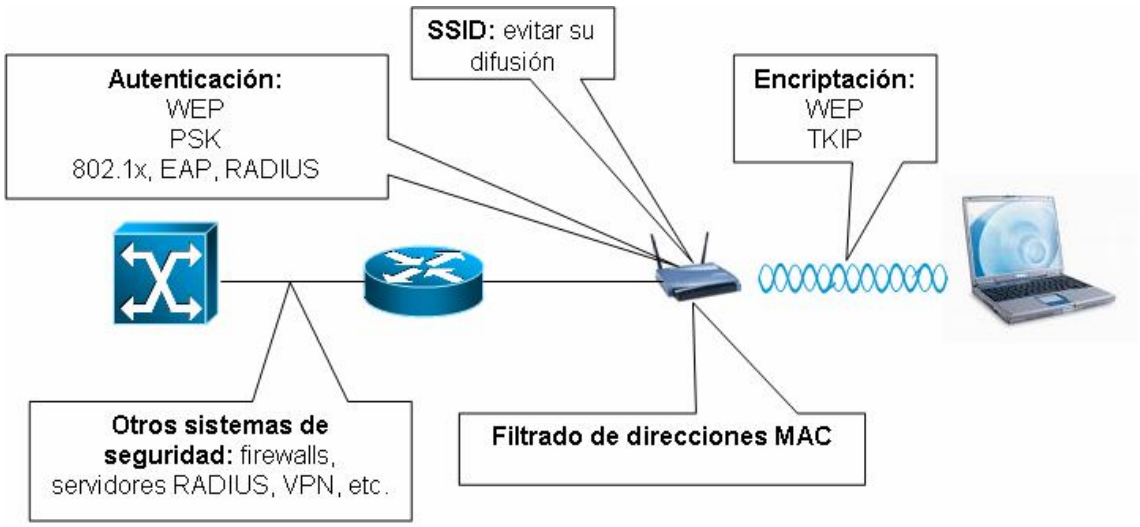


Ilustración 2-33: Niveles de seguridad en una WLAN

2.5.1. SSID

El "Service Set ID" (SSID) es una cadena de generalmente 32 caracteres alfanuméricos que identifican a nuestra Wireless Local Area Network. Algunos fabricantes se refieren al SSID como el nombre de nuestra WLAN, aunque en realidad es algo más que el simple nombre. Para que los dispositivos de nuestra WLAN se comuniquen los unos con los otros deben de ser todos configurados con el mismo SSID. Diferentes SSIDs permitirán la superposición de redes inalámbricas.

Existen dos tipos de identificadores para una red inalámbrica. En una red Ad Hoc (sin puntos de acceso) el identificador es llamado Basic Service Set Identification o BSSID. En una red en modo infraestructura (incluye puntos de acceso) el identificador es el Extended Service Set Identification o ESSID, al cual nos referimos, sin pérdida de generalidad, como SSID.

Existen dos estrategias de seguridad con respecto al SSID.

La primera es cambiar el SSID que tiene asignado nuestro punto de acceso por defecto (los fabricantes asignan a sus dispositivos SSID genéricos que son conocidos o fácilmente obtenibles). De esta forma no se ofrece protección extra a los clientes de la red, pero será más difícil para los intrusos buscar una red concreta, saber exactamente a dónde van a acceder o conocer el fabricante de nuestro punto de acceso. El cambio hay que hacerlo como si se tratara de una contraseña, es decir, no revelar información de nuestra WLAN como su localización, su contenido o cosas así. La elección del SSID, como cualquier otra contraseña, debe seguir las reglas básicas de éstas, o sea, un conjunto de caracteres (letras, números o símbolos) que no tengan ningún significado.

La segunda es ocultar el SSID de nuestra WLAN. Sería como tener una "contraseña" sin la cual el cliente no podrá conectarse a la red (si no sabemos el nombre de la red a la que queremos conectarnos no podemos conectarnos). Pero este nivel de seguridad es fácilmente sobrepasado porque existen métodos alternativos para averiguar el SSID oculto como la captura y posterior análisis de las tramas de asociación.

2.5.2. Filtrado de direcciones MAC

Este método consiste en definir listas de control de acceso (ACL, "Access Control List") en los puntos de acceso. Cada uno de estos puntos puede contar con una relación de las direcciones MAC (direcciones físicas de 48 bits que nos suministra el fabricante y que identifican unívocamente a cada dispositivo físico) de cada uno de los clientes que queremos que se conecten a nuestra red inalámbrica. Cada tarjeta de red o adaptador inalámbrico cuenta con una dirección MAC que lo identifica de forma inequívoca, y si el punto de acceso no la tiene dada de alta, simplemente no recibirá contestación por su parte.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes pequeñas. Sin embargo, posee varias desventajas que no lo hacen práctico para uso en redes grandes, tales como:

- Cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se vuelve inmanejable.

- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack o WellenReiter. De este modo, el atacante puede hacerse pasar por un cliente válido.

- En caso de robo del adaptador inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido.

- Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado, por lo tanto debería usarse conjuntamente con uno.

2.5.3. WEP (Wired Equivalent Privacy)

WEP es el método de seguridad original del protocolo 802.11 que permite la autenticación de los usuarios y el encriptado de los datos. En la actualidad está obsoleto ya que presenta numerosas debilidades que lo hacen inseguro.

2.5.3.1. Autenticación WEP

Un punto de acceso debe de autenticar a una estación antes de que ésta se asocie al AP. Es importante recalcar que lo que se autentica con WEP son las estaciones, y no los usuarios. El estándar IEEE 802.11 define dos tipos de autenticación:

Open System Authentication

El Sistema de Autenticación Abierta es el protocolo de autenticación por defecto para 802.11 por el cual el sistema autentica a cualquiera que lo requiera incluso sin aportar la clave WEP correcta. Es como considerar que no hay autenticación, es decir, la estación puede asociarse a cualquier punto de acceso. Esto se usa normalmente cuando se tiene un interés especial en la facilidad de uso, y el administrador de red no tiene preocupación por la seguridad.

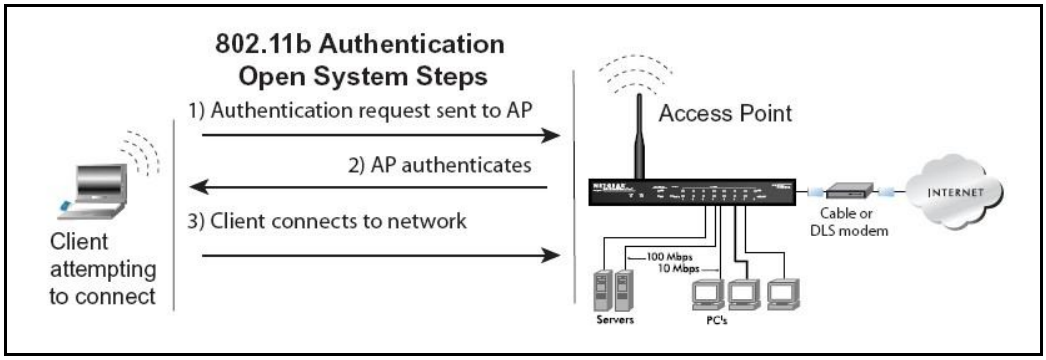


Ilustración 2-34: Open System Authentication

Shared Key Authentication

El Sistema de Autenticación de Clave Compartida usa un mecanismo de desafío/respuesta con una clave secreta (de 64 o 128 bits) compartida por la estación y el punto de acceso, de manera que se niega el acceso a todo aquel que no tenga la clave asignada.

La estación envía una solicitud de autenticación al AP, y éste le responde con un texto desafío de 128 octetos generado con un generador de números pseudo-aleatorios (PRGN), la clave secreta y el vector de inicialización (IV). La estación debe encriptar el texto de desafio con ayuda de su clave WEP y el IV, y enviarlo al punto de acceso. El AP lo desencriptará y lo comparará con el texto de desafío original. Si coinciden autenticará a la estación. En caso contrario fallará la autenticación (ocurrirá si el cliente tiene la clave errónea o no tiene clave). El proceso se muestra en la siguiente ilustración.

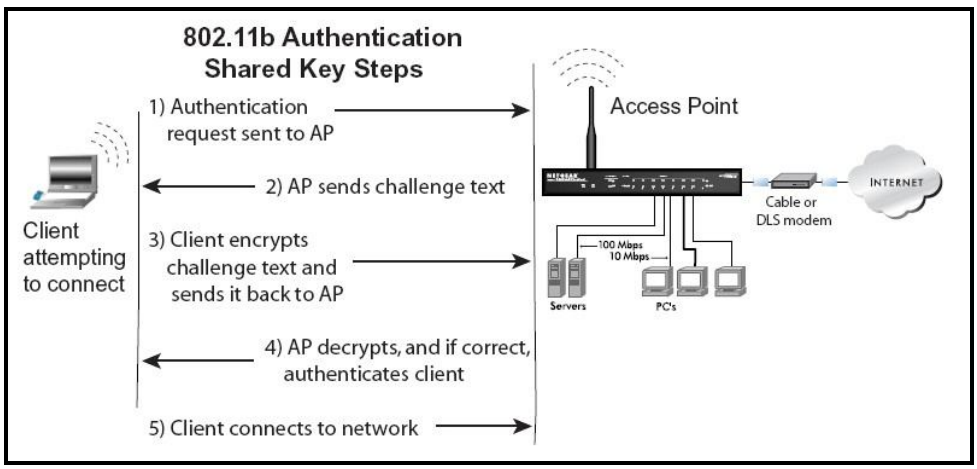


Ilustración 2-35: Shared Key Authentication

2.5.3.2. Encriptación WEP

La clave compartida que se usará para encriptar o desencriptar las tramas de datos, es la misma que se usa para la autenticación, lo que puede ser considerado un riesgo de seguridad. WEP utiliza el algoritmo RC4 para ello, con claves de 64 o 128 bits. Veremos que en realidad son 40 ó 104 bits respectivamente, ya que los otros 24 van en el paquete como Vector de Inicialización (IV). No veremos el proceso de encriptado/desencriptado. Tan sólo destacar que usando claves de 104 bits un cracker tardaría mucho más tiempo en descifrarla que usando una de 40 bits.

2.5.3.3. Debilidades de WEP

En principio WEP fue diseñado para evitar simples fisgoneos. A continuación enumeramos las debilidades más importantes que hacen de WEP un método inseguro y fácilmente atacable:

1. **Encriptación y autenticación comparten clave**. La clave compartida que se usa para encriptar y desencriptar las tramas de datos es la misma que la que se usa para la autenticación. Es un riesgo de seguridad alto, porque el que consigue sobrepasar el nivel de seguridad de autenticación sobrepasará automáticamente el de encriptación.

2. **Los mensajes de autenticación pueden ser fácilmente falsificables.** WEP es un método de encriptación de datos y no un mecanismo de autenticación en sí, lo que provoca debilidades. Un atacante que utilice técnicas de monitorización para observar una autenticación exitosa, puede más tarde falsificar el proceso.

3. **Actualizaciones y cambios de clave.** Las redes inalámbricas que utilizan esta tecnología tienen una única clave WEP compartida por todos los nodos de la red. Dado que la sincronización del cambio de claves resulta una tarea tediosa y difícil, éstas son modificadas con muy poca frecuencia, lo que reduce la seguridad.

4. **Tamaño y reutilización de la clave y el IV.** Es un inconveniente ya que son consideradas de tamaño insuficiente. Además existe un 50% de probabilidad de que se reutilicen claves, por lo que las hacen fácilmente detectables.

5. **Algoritmo de encriptación.** Inadecuado por dos motivos. El primero es que genera claves frágiles. Se considera que una clave es frágil cuando existe mayor correlación entre la clave y la salida de la que debería existir. El otro motivo es que está basado en CRC-32 que es un algoritmo excelente para la detección de ruido y errores comunes en la transmisión pero no como solución de criptografía.

2.5.4. WPA / WPA2

WPA (Wi-Fi Protected Access) es un estándar propuesto por los miembros de la Wi-Fi Alliance (asociación que reúne a los grandes fabricantes para WLANs), en colaboración con la IEEE, para la seguridad de WLANs. Está basado en las especificaciones de 802.11i y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance. Esta norma data del año 2003.

WPA intenta resolver las deficiencias de seguridad de WEP mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

2.5.4.1. Autenticación

Utilizará un método u otro según el modo de operación que configuremos en el punto de acceso. De acuerdo con la complejidad de la red, habrá dos modalidades:

a) **Modalidad de red empresarial.** Para grandes empresas. El punto de acceso emplea el protocolo EAP sobre 802.1x y RADIUS para la autenticación. Bajo esta modalidad se requiere de la existencia de un servidor de autenticación en la red.

b) **Modalidad de red doméstica**. . En el entorno del hogar o en pequeñas empresas, en donde no se precisa llevar a cabo una compleja gestión de usuarios, el mecanismo de autenticación usado es PSK. Esta modalidad no requiere de servidor de autenticación.

PSK (Pre-Shared Key)

Es un método de autenticación se basa en el uso de claves o contraseñas introducidas manualmente. No necesita un servidor de autenticación por lo que resulta muy sencillo de implementar. Todo lo que necesitamos hacer es introducir una clave maestra o PSK en cada uno de los puntos de acceso y de las estaciones

que conforman nuestra WLAN. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Esta PSK nunca se transmite por el aire ni se utiliza para encriptar el flujo de datos, sino, simplemente para iniciar el proceso de claves dinámicas TKIP, por lo que es mucho más seguro que WEP. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

802.1x, EAP y RADIUS

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor que restringe la conexión de equipos no autorizados a una red. Fue inicialmente creado por la IEEE para uso en redes de área local cableadas, pero se ha extendido también a las redes inalámbricas. Prácticamente la totalidad de los puntos de acceso que se fabrican en la actualidad son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes (Ilustración 2-35):

- **El suplicante.** Es aquella entidad que pretende tener acceso a los recursos de la red. Por ejemplo, un usuario con un PC con adaptador inalámbrico que intenta conectarse a la WLAN.
- **El servidor de autenticación**. Es la entidad que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. Aporta la inteligencia al proceso ya que es el que realiza la negociación. Por ejemplo, un servidor RADIUS.
- **El autenticador.** Es el equipo de red que recibe la conexión del suplicante. Actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza. En nuestro caso sería el punto de acceso.

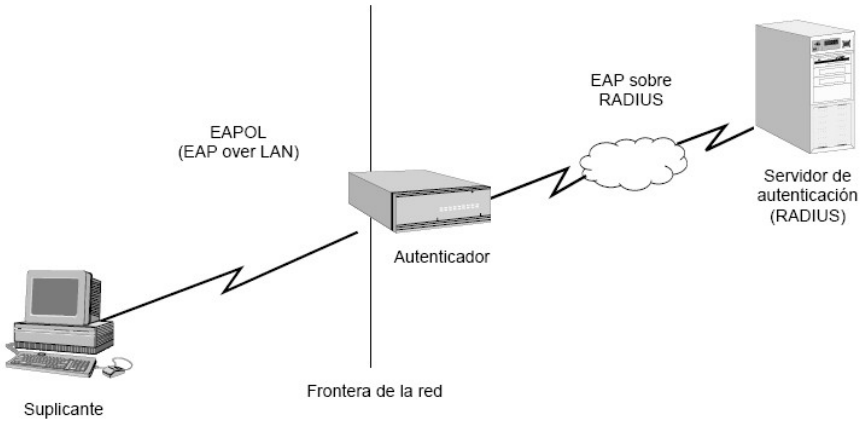


Ilustración 2-36: Arquitectura funcional del protocolo 802.1x

La autenticación se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servidor RADIUS (Remote Authentication Dial-In User Service), que actúan tal y como muestra el siguiente diagrama:

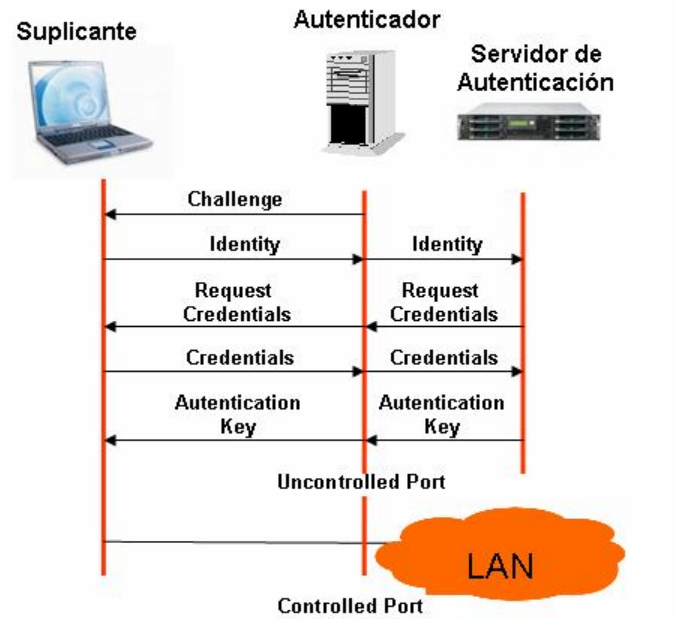


Ilustración 2-37: Diálogo EAPOL – RADIUS

Por último comentar que existen dos variantes del protocolo EAP según la modalidad de autenticación que se emplee: las que emplean certificados de seguridad, y las que utilizan contraseñas. Las variantes de EAP que emplean certificados de seguridad son las siguientes: EAP-TLS, EAP-TTLS y PEAP; y las que utilizan contraseñas: EAP-MD5, LEAP y EAP-SPEKE.

2.5.4.2. Encriptación WPA

Para el cifrado WPA emplea el protocolo TKIP (Temporal Key Encryption Protocol) que es más sofisticado criptológicamente hablando, y que resuelve notablemente las debilidades de WEP. Aporta importantes mejoras como son:

- Proceso de encriptación independiente del proceso de autenticación.
- Actualización de claves en cada envío de trama para evitar ataques que puedan revelarla. El cambio de clave es sincronizado entre las estaciones y el punto de acceso.
- MIC (Message Integrity Check) o Función de Chequeo de Integridad del Mensaje también llamada Michael. Es una función que añade una comprobación de integridad de los datos más robusta que el habitual CRC y que incluye las direcciones físicas (MAC) del origen y del destino y los datos en texto plano de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- Mejoras de los algoritmos de cifrado de trama, de gestión y de generación de claves e IVs. Ahora son más robustos e incluyen privacidad e integridad de datos.
- Utilización de un vector de inicialización IV extendido. De 24 pasa a 48 bits y se llama TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden
- Mantiene la compatibilidad con WEP, y con el hardware utilizado anteriormente tan sólo mediante una actualización del firmware.

2.5.4.3. WPA2

Wi-Fi Protected Access 2 es un estándar de seguridad que surge como evolución de WPA. La estructura es básicamente la misma pero presenta algunos elementos diferenciadores:

- Método seguro IBSS para redes en modo Ad Hoc
- Utilidades para VoIP en 802.11
- Protocolo de encriptación mejorado: AES (Advanced Encrpytion Standard)

WPA2 requiere de actualizaciones de hardware, por lo que se encuentra en fase de despliegue todavía.

2.5.4.4. ¿Es WPA/WPA2 perfecto?

Evidentemente no. No existe un mecanismo de seguridad completamente invulnerable, por lo que WPA / WPA2 también tiene sus puntos débiles y podrá ser mejorable. El principal de ellos es que es susceptible a ataques de denegación de servicio o DoS (Denial of Service) mediante el envío de paquetes basura (encriptados erróneamente) hacia la red. Si el punto de acceso recibe dos paquetes que no superan el código de integridad de mensaje (MIC) en un intervalo de 60 segundos, significará que la red está bajo un ataque activo, y como resultado el punto de acceso tomará medidas drásticas como la disociación de cada estación. Esto previene de ataques de DoS pero provocará la pérdida de conexión durante 60 segundos. A pesar de este inconveniente, WPA / WPA2 da un paso más adelante que WEP en la seguridad de las WLANs por lo que recomendamos su uso.

2.6. Principales protocolos de la familia IEEE 802.11

Una vez vistos todos los pormenores de la familia IEEE 802.11, veamos de una manera esquemática sus principales protocolos y características. Lo hacemos en forma de tabla, en la siguiente página.

Además, dentro del IEEE 802.11 hay definidos una serie de grupos de trabajo que se encargan de investigar y desarrollar diferentes protocolos que complementan a los estándares anteriores. Estos grupos son:

- **IEEE 802.11c.** Define las características de los puntos de acceso para ser utilizados como puentes.
- **IEEE 802.11d**. Establece definiciones y requisitos para permitir que el estándar 802.11 opere en países en los que actualmente no se puede implantar el estándar.
- **IEEE 802.11e**. Se podría definir como la implementación de características de QoS ("Quality of Service") y multimedia para las redes 802.11a/b.
- **IEEE 802.11f.** Básicamente, es una especificación que funciona bajo el estándar 802.11g y que se aplica a la intercomunicación entre puntos de acceso de distintos fabricantes, permitiendo el roaming o itinerancia de clientes.
- **IEEE 802.11h**. Una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos de posibles interferencias.
- **IEEE 802.11i.** Este estándar permite incorporar mecanismos de seguridad para redes inalámbricas y ofrece una solución interoperable y un patrón robusto para asegurar datos.
- **IEEE 802.11x**. Pretende mejorar los mecanismos de seguridad de la 802.11, con los protocolos de seguridad extendida (EAP).
- **IEEE 802.11 Super G.** Estándar propietario que utiliza tecnología "pseudo MIMO" y que alcanza una velocidad máxima de transferencia de 108 Mbps. Es proporcionado por el chipset Atheros.

Tabla 2-3: Principales estándares de la familia IEEE 802.11

	802.11 legacy	802.11b	802.11a	802.11g	802.11n
Banda	2.4Ghz / 850-950nm	2.4GHz	5Ghz	2.4GHz	2.4GHz / 5GHz
Capa física	FHSS / DSSS / IR	DSSS	OFDM	DSSS / OFDM	MIMO / OFDM
	GFSK / DPSK	DPSK sin/con CCK o PBCC	PSK / QAM	DPSK / PSK / QAM	
Tasa máxima	2 Mbps	11Mbps	54 Mbps	54 Mbps	600 Mbps
Throughput (*)	0.9 Mbps	4.5 Mbps	23 Mbps	20 Mbps	135 Mbps
Alcance interior (*)	20m	40m	35m	40m	70m
Alcance exterior (*)	100m	150m	120m	150m	300m
Año	1997	1999	1999	2003	2008
Uso	En desuso	Muy extendido	Poco extendido	Extendido y creciente	En desarrollo
Rendimiento	Buen rendimiento	Rendimiento medio	Mejor rendimiento	Rendimiento medio	Máximo rendimiento
Consumo	Bajo consumo	Bajo consumo	Mayor consumo	Bajo consumo	
Canales sin solapamiento	No	3 canales simultáneos	12 canales simultáneos		
Compatibilidad		Incompatible con 802.11a	Incompatible con 802.11b	Compatible con 802.11b	Compatible con todos
Interferencias	Bluetooth, microondas, DECT, ...			Bluetooth, microondas, ...	
Otras			Necesita licencia en algunos países		

(*) Valores aproximados

CAPÍTULO 2: FAMILIA IEEE 802.11 26