Wireless LAN's

INTRODUCCIÓN

En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes de área local (Wireless LANs). La función principal de este tipo de redes es la proporcionar conectividad y acceso a las tradicionales redes cableadas (Ethernet, Token Ring...), como si se tratara de una extensión de éstas últimas, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 en mes de junio de 1997. En este estándar se encuentran las especificaciones tanto físicas como a nivel MAC que hay que tener en cuenta a la hora de implementar una red de área local inalámbrica.
Un estándar define, además de la topología de red, un conjunto de reglas de acceso y de transmisiones al interno de la misma. El estándar es el instrumento indispensable para garantizar la amplia difusión de una tecnología.
La norma 802.11 ha sufrido diferentes extensiones sobre la norma para obtener modificaciones y mejoras. De esta manera, tenemos las siguientes especificaciones:

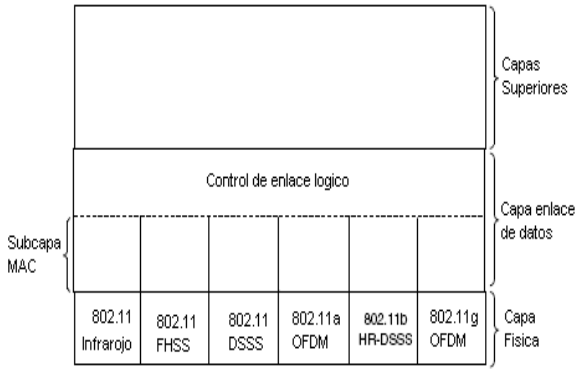


Figura 1: Partes del stack de protocolos de 802.11

- 802.11 Especificación para 1-2 Mbps en la banda de los 2.4 GHz, usando salto de frecuencias (FHSS) o secuencia directa (DSSS).
- 802.11b Extensión de 802.11 para proporcionar 11Mbps usando DSSS.
- Wi-Fi (Wireless Fidelity) Promulgado por el WECA para certificar productos 802.11b capaces de interoperar con los de otros fabricantes.
- 802.11a Extensión de 802.11 para proporcionar 54Mbps usando OFDM.
- 802.11g Extensión de 802.11 para proporcionar 20-54Mbps usando DSSS y OFDM. Es compatible hacia atrás con 802.11b. Tiene mayor alcance y menor consumo de potencia que 802.11a.
- 802.11g A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física

La idea que queremos resaltar es que, los sistemas WLAN no pretenden sustituir a las tradicionales redes cableadas, sino más bien complementarlas. En este sentido el objetivo fundamental de las redes WLAN es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red total donde coexistan los dos tipos de sistemas.

GENERALIDADES SOBRE REDES DE ÁREA LOCAL INALÁMBRICAS

Definición de Red de Área Local Inalámbrica

Una red de área local inalámbrica puede definirse como a una red de alcance local que tiene como medio de transmisión el aire. Por red de área local entendemos una red que cubre un entorno geográfico limitado, con una velocidad de transferencia de datos relativamente alta (mayor o igual a 1 Mbps tal y como especifica el IEEE), con baja tasa de errores y administrada de forma privada. Por red inalámbrica entendemos una red que utiliza ondas electromagnéticas como medio de transmisión de la información que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.
En las redes tradicionales cableadas esta información viaja a través de cables coaxiales, pares trenzados o fibra óptica. Una red de área local inalámbrica, también llamada wireless LAN (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada. Este tipo de redes utiliza tecnología de radiofrecuencia minimizando así la necesidad de conexiones cableadas. Este hecho proporciona al usuario una gran movilidad sin perder conectividad.
El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 54 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

Aplicaciones de los sistemas WLAN

Las aplicaciones más típicas de las redes de área local que podemos encontrar actualmente son las siguientes:

- Implementación de redes de área local en edificios históricos, de difícil acceso y en general en entornos donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales.

Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

- Redes locales para situaciones de emergencia o congestión de la red cableada.

- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes...
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.
- Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableadas situadas en dos edificios distintos.

Configuraciones WLAN

El grado de complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que queramos implementar podemos utilizar diversas configuraciones de red.

Peer to peer o redes ad-hoc

La configuración más básica es la llamada *de igual a igual* o *ad-hoc* y consiste en una red de dos terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. En la figura 2 mostramos un ejemplo. Para que la comunicación entre estas dos estaciones sea posible hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra. Las redes de tipo *ad-hoc* son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa.

Un grupo de estaciones, en un área de cobertura llamada BSA (Basic Service Area), dentro de la cual viene garantizada la interconexión y viene utilizada una única función de coordinación, forman una BSS (Basis Services- Conjunto de Servicios Básicos). Por función de coordinación se entiende la función lógica que determina cuando una estación perteneciente a la BSS puede transmitir o recibir sobre el medio de comunicación compartido, el aire.
El estándar prevé dos funciones de coordinación:

DCF (Distributed Coordination Function), de tipo distribuida;

PCF (Point Coordination Function), que se basa sobre un único nodo de coordinación.

Figura 2 BSS

Modo Infraestructura - Distribution System (DS)

Para aumentar el alcance de una red, hace falta la instalación de un *access point (punto de acceso)*. Con este nuevo elemento doblamos el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso). En la figura 3 mostramos un ejemplo. Además, los *puntos de acceso* se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos. Para dar cobertura en una zona determinada habrá que instalar varios puntos de acceso de tal manera que podamos cubrir la superficie necesaria con las celdas de cobertura que proporciona cada punto de acceso y ligeramente solapadas para permitir el paso de una celda a otra sin perder la comunicación.

El estándar prevé que más BSS puedan ser conectadas con un backbone, llamada Distribution System (DS) dentro de una ESS (Extended Service Set), a través de un punto de acceso (AP: Access Point). Un AP es una estación particular que proporciona una interfaz hacia el DS para las estaciones pertenecientes a una BSS. Todas las STA (Estaciones) presentes en una BSS pueden comunicarse directamente entre ellas.
El estándar soporta las dos siguientes topologías de red:

Redes IBSS (Independent Basic Service Set)

Redes ESS (Extended Service Set)

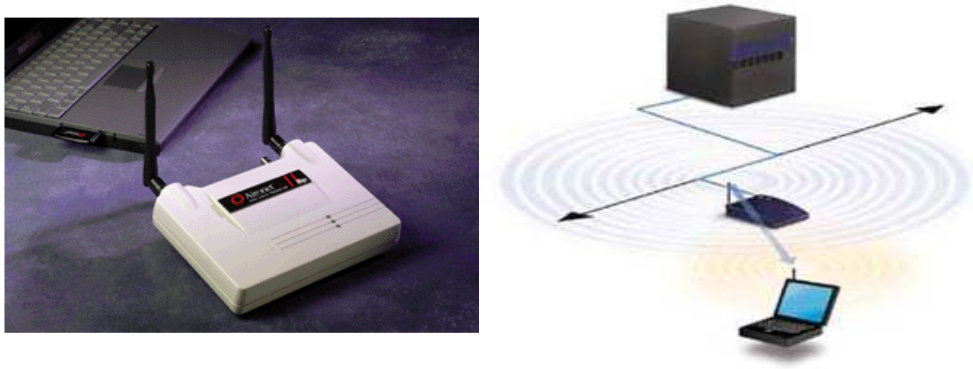


Figura 3 ESS

Enlace entre varias LAN o WMAN

Para finalizar, otra de las configuraciones de red posibles es la que incluye el uso de antenas direccionales. El objetivo de estas antenas direccionales es el de enlazar redes que se encuentran situadas geográficamente en sitios distintos tal y como se muestra en la figura 4. Un ejemplo de esta configuración lo tenemos en el caso en que tengamos una red local en un edificio y la queramos extender a otro edificio. Una posible solución a este problema consiste en instalar una antena direccional en cada edificio apuntándose mútuamente. A la vez, cada una de estas antenas está conectada a la red local de su edificio mediante un punto de acceso. De esta manera podemos interconectar las dos redes locales.

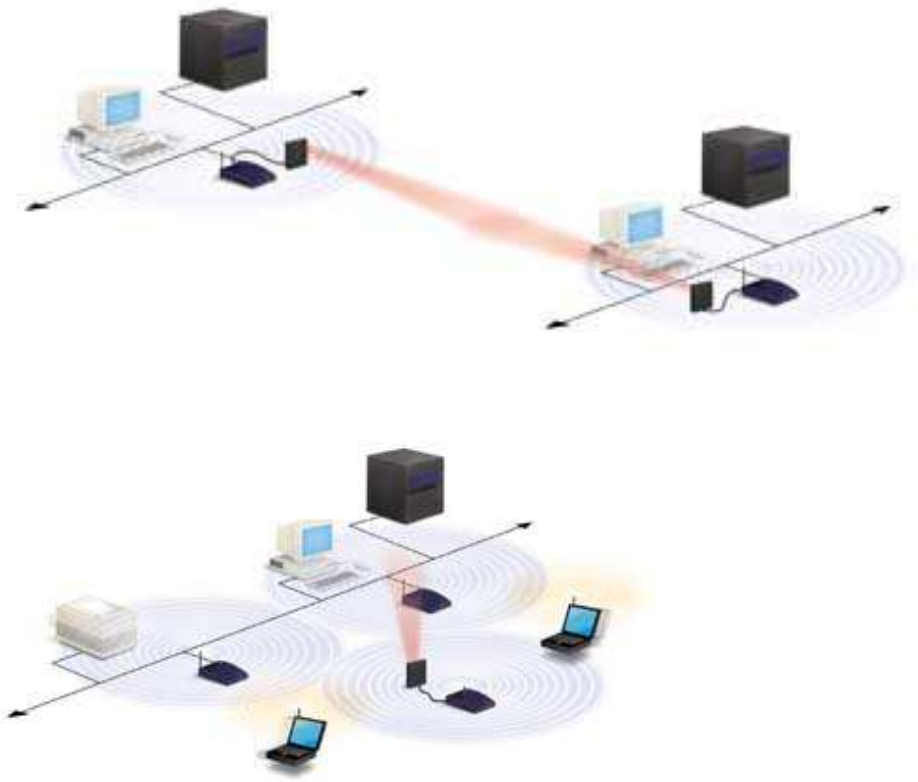


Figura 4 ESS

Las redes ESS están formadas por muchas BSS interconectadas a través de un DS, el cual puede ser realizado tanto con tecnología cableada como con tecnología sin cables (figura 4). Este se ocupa de transferir la denominada MSDU (MAC Service Data Units) entre AP pertenecientes a diversas BSS. Esta tipología de red es necesaria con el fin de permitir la interacción entre terminales que no se encuentran al interno de la cobertura radio de un único Basic Service Set.

Arquitecturas básicas de despliegues

Una vez entendidos los modos y servicios internos que proporciona la recomendación 802.11, se pueden describir los principales modelos de arquitecturas que se pueden emplear en los despliegues de redes inalámbricas.
_ Modo punto de acceso básico. Es el modo de infraestructura más elemental en el cual un punto de acceso (puede ser un bridge o un router), está conectado a una red local y en su parte inalámbrica puede tener asociados un conjunto de estaciones. Es el modo habitual en la mayor parte de las más pequeñas instalaciones. En algunos casos se denomina modo root.

_ Modo con roaming. Si se disponen de varios puntos de acceso y se configuran como una ESS con la misma SSID en todas las celdas, entonces es posible realizar el roaming de las estaciones entre ellas. Es la disposición más acertada para instalaciones de envergadura y que necesitan movilidad.

_ Modo de balanceo de carga. En zonas con elevado consumo que puede llegar a degradar e incluso saturar la capacidad de un punto de acceso, pueden desplegarse uno o más puntos de acceso en la misma ubicación y en canales de frecuencia no interferentes de tal forma que

se consiga repartir el número de estaciones y su carga entre ellos de forma dinámica. El SSID será igual en todos. El ancho de banda será teóricamente el de un punto de acceso multiplicado por el número de ellos. Además del aumento del ancho de banda, proporciona cierto nivel de redundancia que reduce el impacto de una falta de operatividad de un punto de acceso, aunque a costa del consumo de varios canales de frecuencia.

_ Modo hot stand-by. Se configuran dos puntos de acceso en la misma ubicación con idénticos parámetros y conectados a la misma red fija. Uno de ellos se pone en modo activo y el otro en stand-by en escucha permanente. En cuanto detecta que el primer punto de acceso no está operativo, cambia al modo activo y toma el control de la celda.
Aunque no pueden proporcionar el doble de ancho de banda como en el caso del modo de balanceo de carga, sólo consumen un canal de frecuencia.

_ Modo repeater. Un punto de acceso se conecta a otro mediante WDS (Sistema de distribución inalámbrico) y ambos empleando el mismo canal y SSID. De esta forma el segundo punto de acceso extiende la cobertura del primero y permite que estaciones alejadas accedan a la red local cableada. Como inconveniente, se ha de indicar que se reduce muy por debajo del 50% la eficiencia del medio, ya que necesita enviar cada paquete de información dos veces a través del mismo canal.

_ Modo bridge. Permite conectar dos o más redes cableadas mediante un segmento inalámbrico. Uno de los bridges actúa en modo root, centralizando el tráfico, mientras que los otros adaptadores actúan como estaciones. La solución con sólo dos bridges es la apropiada para enlaces punto a punto, por ejemplo para interconectar las redes de dos edificios distantes.

_ Modos híbridos. Se configuran por la combinación de alguno de los anteriores, como por ejemplo un modo de punto de acceso básico con estaciones y a la vez con un bridge conectado con equipos fijos en su red cableada.

Actualmente la mayoría de los equipos inalámbricos pueden operar en múltiples modos.

NIVEL FÍSICO. ARQUITECTURA Y TECNOLOGÍAS DE MODULACIÓN

La arquitectura de la capa de nivel físico, es donde nos centraremos en describir ligeramente el funcionamiento de la capa de convergencia, fundamentalmente resaltando el proceso de transmisión-recepción y las técnicas de modulación utilizadas por 802.11.

Estándar	Data Rate [Mbps]	Frecuencia	Modulación
802.11	1, 2	2.4 GHz	FHSS, DSSS, IR
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5 GHz	OFDM
802.11b	1, 2, 5.5, 11	2.4 GHz	HR-DSSS
802.11g	6, 12, 24, 36, 48, 54	2.4 GHz	OFDM
802.11n	Aprox. 100 Mbps	------	------

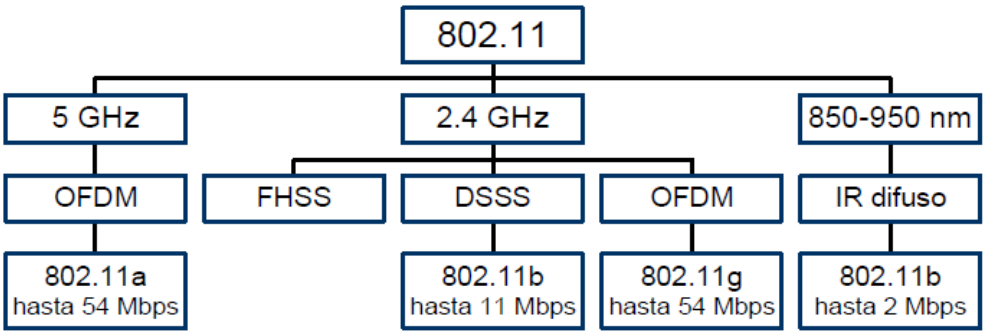
Arquitectura de capas 802.11

La capa física proporciona una serie de servicios a la capa MAC o capa de acceso al medio. Diferentes tecnologías de capa física se definen para transmitir por el medio inalámbrico.

La capa física de servicios consiste en dos protocolos:

- ✓ Una función de convergencia de capa física, que adapta las capacidades del sistema físico dependiente del medio (PMD). Esta función es implementada por el protocolo PLCP o procedimiento de convergencia de capa física, que define una forma de mapear MPDUs o unidades de datos MAC en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones o STASs a través de la capa PMD.
- ✓ Un sistema PMD, cuya función define las características y un medio de transmitir y recibir a través de un medio sin cables entre dos o más STAs.

La comunicación entre MACs de diferentes estaciones se realizará a través de la capa física mediante de una serie de puntos de acceso al servicio, donde la capa MAC invocará las primitivas de servicio.
Además de estas capas, podemos distinguir la capa física de gestión. En esta capa podemos distinguir la estructura MIB (Management Information Base) que contienen por definición las variables de gestión, los atributos, las acciones y las notificaciones requeridas para gestionar una estación. Consiste en un conjunto de variables donde podemos especificar o contener el estado y la configuración de las comunicaciones de una estación.



Tecnologías utilizadas en las Redes Inalámbricas

Podemos distinguir tres tecnologías, dos de espectro ensanchado y una de infrarrojos.

A. Tecnologías de espectro ensanchado

La tecnología de espectro ensanchado consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez de concentrar la energía de las señales alrededor de una portadora concreta lo que se hace es repartirla por toda la banda disponible. Este ancho de banda total se comparte con el resto de usuarios que trabajan en la misma banda frecuencial. Existen dos tipos de tecnologías de espectro ensanchado:

- Espectro Ensanchado por Secuencia Directa (DSSS)
- Espectro Ensanchado por Salto en Frecuencia (FHSS)

Tecnología de espectro ensanchado por secuencia directa (DSSS)

Esta técnica consiste en la generación de un patrón de bits redundante llamado *señal de chip* para cada uno de los bits que componen la señal de información y la posterior modulación de la señal resultante mediante una portadora de RF. En recepción es necesario realizar el proceso inverso para obtener la señal de información original.
La secuencia de bits utilizada para modular cada uno de los bits de información es la llamada secuencia de Barker y tiene la siguiente forma:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

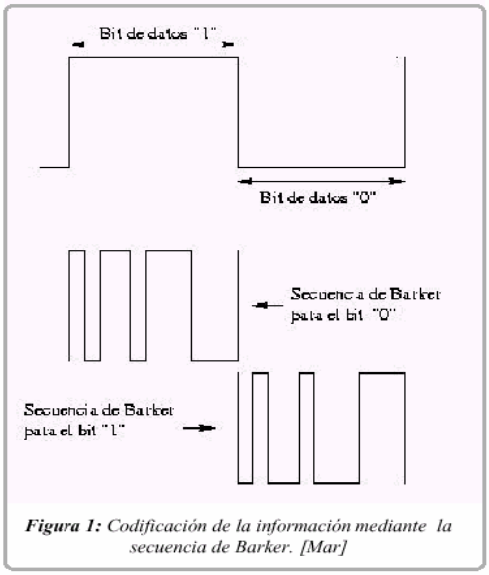


Figura 1: *Codificación de la información mediante la secuencia de Barker. [Mar]*

En la Figura 1 se muestra el aspecto de una señal de dos bits a la cual le hemos aplicado la secuencia de Barker. 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 proporcionando una velocidad de transferencia de 1 y 2 Mbps respectivamente.
En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa, DSSS, opera en el rango que va desde los 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho de banda total disponible de 83.5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de banda por canal de 5 MHz de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular. En el caso de España se utilizan los canales 10 y 11 ubicados en una frecuencia central de 2.457 GHz y 2.462 GHz respectivamente.
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. Esta independencia entre canales nos permite aumentar la capacidad del sistema de forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales. En el caso de España esta extensión de capacidad no es posible debido a que no existe el ancho de banda mínimo requerido (la información sobre la distribución de las frecuencias en distintas regiones del mundo se encuentra disponible en el estándar IEEE 802.11).

Tecnología de espectro ensanchado por salto en frecuencia (FHSS) (Frequency Hopping Spread Spectrum)

La tecnología de espectro ensanchado por salto en frecuencia consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time* y inferior a 400ms. Pasado este tiempo se cambia (hops) la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de

información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.
Cada una de las transmisiones a una frecuencia concreta se realiza utilizando una portadora de banda estrecha que va cambiando (saltando) a lo largo del tiempo. Este procedimiento equivale a realizar una partición de la información en el dominio temporal.
El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer. La ventaja de estos sistemas frente a los sistemas DSSS es que con esta tecnología podemos tener más de un punto de acceso en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan la misma frecuencia portadora en un mismo instante de tiempo.

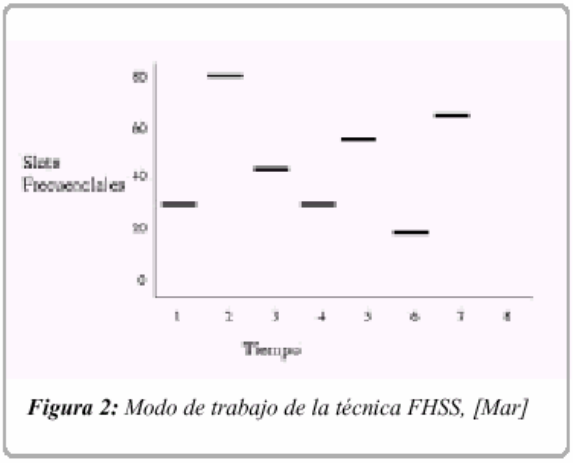
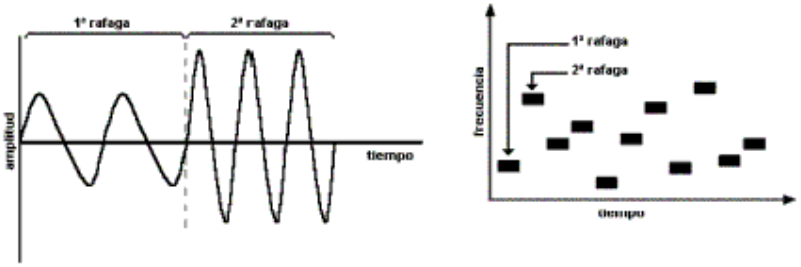


Figura 2: *Modo de trabajo de la técnica FHSS, [Mar]*



Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación el efecto global es que aunque vamos cambiando de canal físico con el tiempo se mantiene un único canal lógico a través del cual se desarrolla la comunicación.
Para un usuario externo a la comunicación la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. El estándar IEEE 802.11 describe esta tecnología mediante la modulación en frecuencia FSK, Frequency Shift Keying, y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps bajo condiciones de operación óptimas también especificadas en la norma.

B- Tecnología de infrarrojos

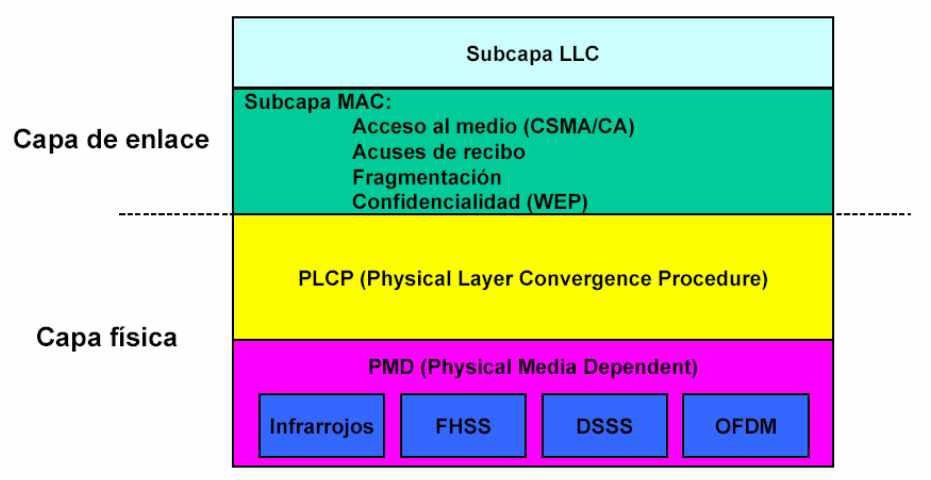
Una tercera tecnología, de momento no demasiado utilizada a nivel comercial para implementar WLANs, es la de infrarrojos. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los

infrarrojos no pueden pasar a través de objetos opacos pero se pueden reflejar en determinadas superficies.
Las longitudes de onda de operación se sitúan alrededor de los 850-950 nm. Los sistemas que funcionan mediante infrarrojos se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

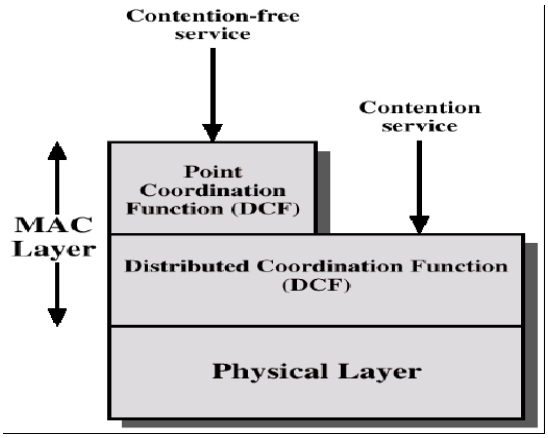
- ✓ Sistemas de corta apertura, de haz dirigido o de visibilidad directa que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.
- ✓ Sistemas de gran apertura, reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio. La norma IEEE 802.11 especifica dos modulaciones para esta tecnología: la modulación 16 ppm y la modulación 4 ppm proporcionando unas velocidades de transmisión de 1 y 2 Mbps respectivamente. Esta tecnología se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados como puede ser una aula concreta o un laboratorio.

NIVEL DE ACCESO AL MEDIO (MAC)

Los diferentes métodos de acceso de IEEE 802 están diseñados según el modelo OSI y se encuentran ubicados en el nivel físico y en la parte inferior del nivel de enlace o subnivel MAC.
Además, la capa de gestión MAC controlará aspectos como sincronización y los algoritmos del sistema de distribución, que se define como el conjunto de servicios que precisa o propone el modo infraestructura. Por último, veremos el aspecto y los tipos de tramas MAC.



Descripción Funcional MAC.



La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas: la función de coordinación puntual (PCF) y la función de coordinación distribuida.

DFC Función de Coordinación Distribuida

Definimos *función de coordinación* como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de contienda por el medio.
El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles no tolerados por los servicios síncronos.

Las características de DFC las podemos resumir en estos puntos:

- ✓ Utiliza MACA (CSMA/CA con RTS/CTS) como protocolo de acceso al medio
- ✓ Necesario reconocimientos ACKs, provocando retransmisiones si no se recibe
- ✓ Usa campo Duration/ID que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre
- ✓ Implementa fragmentación de datos
- ✓ Concede prioridad a tramas mediante el espaciado entre tramas (IFS)
- ✓ Soporta Broadcast y Multicast sin ACKs

Protocolo de Acceso al medio CSMA/CA y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance). Este algoritmo funciona tal y como describimos a continuación:

1. Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).
2. Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).

3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.
4. Una vez finaliza esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de Backoff, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo 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 que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.
5. Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS, el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

Sin embargo, CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas que intentaremos resolver con alguna modificación. Los dos principales problemas que podemos detectar son:

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

La solución que propone 802.11 es MACA o Multi Access Collision Avoidance.

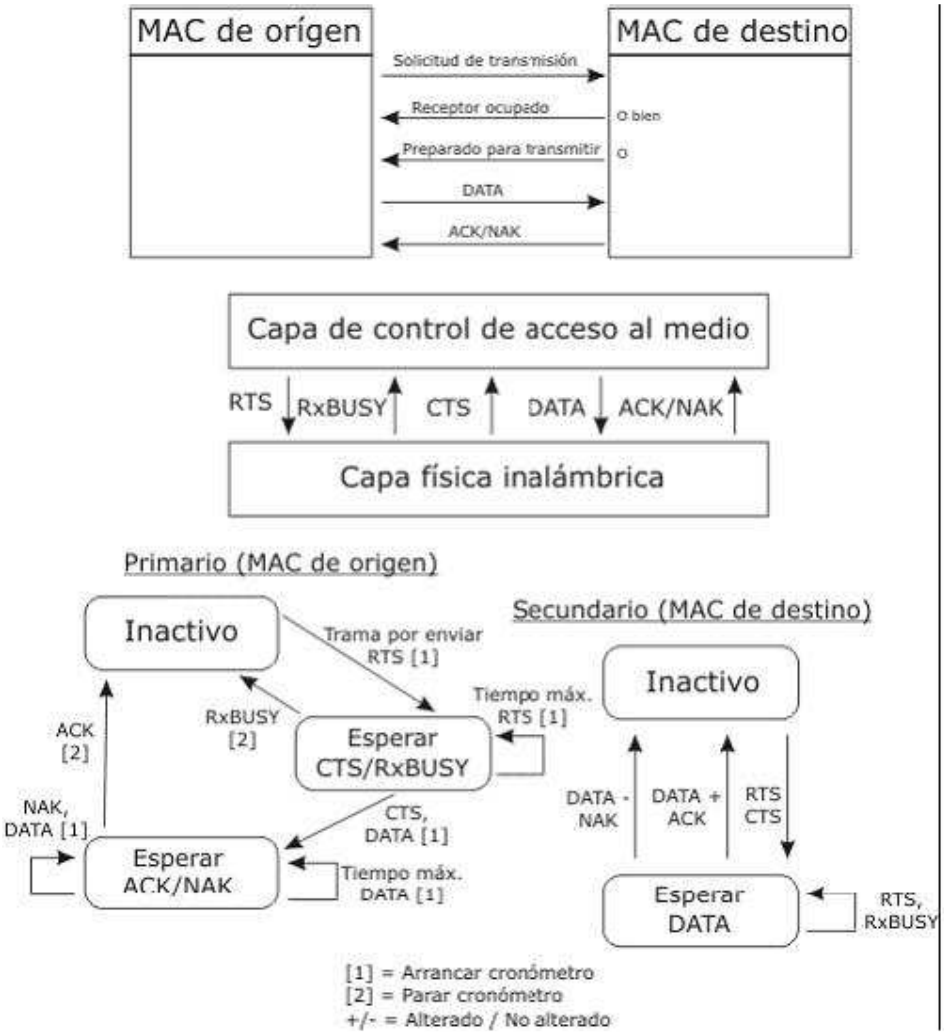
Según este protocolo, antes de transmitir el emisor envía una trama RTS (Request to Send), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (Clear to Send), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS
- Al escuchar un CTS, hay que esperar según la longitud

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

ACK Acuse de Recibo
NAK Negative Acuse de Recibo



Los intervalos interframe del nivel MAC 802.11

Las tramas del nivel MAC están espaciadas en el tiempo a intervalos llamados IFS (InterFrame Space). El uso de los IFS en el estándar 802.11 permite a las estaciones separar estas tramas entre ellas. El estándar 802.11 prevé cuatro IFS distintos, permitiendo obtener un acceso al medio con diferentes niveles de prioridad y separar las tramas de estaciones diversas. La duración del IFS está determinada a partir del valor de particulares atributos relativos al nivel físico implementado pero es independiente de la tasa de bit de las estaciones. Estos están ordenados a continuación, del más breve al más largo:

SIFS (Short IFS): es el más breve intervalo de tiempo definido. Viene utilizado para transmitir sobre el medio, sin efectuar la contienda, tramas de ACK, CTS o las MPDU que constituyen roturas de fragmentos, o para responder a un polling durante la modalidad PCF. En IEEE 802.11a e IEEE802.11n a 5GHz el SIFT es de 16 micro segundos, con un aSlotTime de 9 micro segundos.

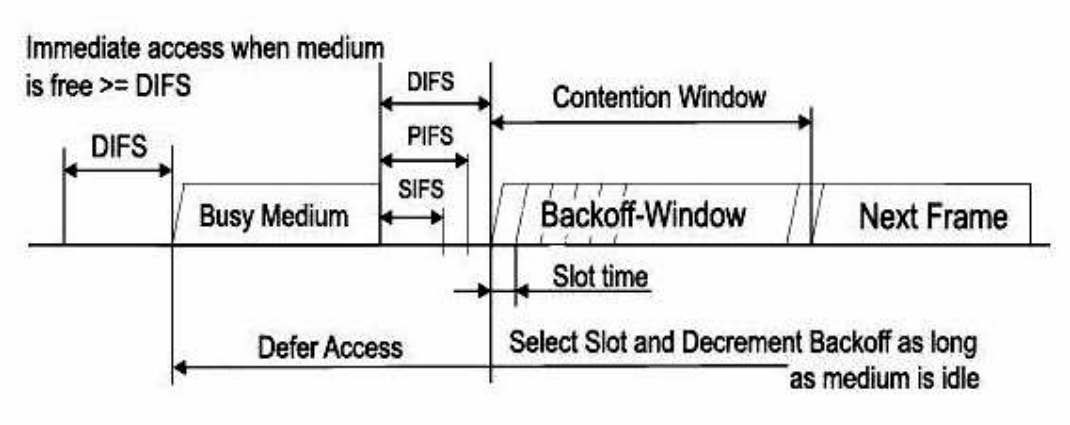
En IEEE 802.11g e IEEE802.11n a 2.4GHz el SIFT es de 20 micro segundos, con un aSlotTime de 10 micro segundos.

PIFS (PCF IFS): es un intervalo de tiempo usado exclusivamente en la modalidad PCF. Su duración es función del aSlotTime, unidad temporal definida a su vez por el tipo de nivel físico utilizado. El PIFS está ligado al SIFS por la siguiente relación y su duración es tal para proporcionar una prioridad de acceso al canal.

PIFS = aSlotTime + SIFS > SIFS

DIFS (DCF IFS): viene utilizado por las estaciones que operan en modalidad DCF para transmitir tramas de datos MPDU (MAC Protocols Data Units) o tramas de gestión (MMPDU, MAC Management Protocol Data Unit). Se relaciona con el PIFS como sigue:

DIFS = aSlotTime + PIFS > PIFS



Formato de las tramas MAC

Las tramas MAC contienen los siguientes componentes básicos:

- ✓ una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia
- ✓ un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama
- ✓ un secuencia checksum (FCS) que contiene un código de redundancia CRC -32 de 32 bits

Las tramas MAC se pueden clasificar según tres tipos:

- ✓ Tramas de datos.
- ✓ Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda
- ✓ Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

El formato de la trama MAC genérica tiene el siguiente aspecto:

Octetos:	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Body	FCS
	MAC Header							*Body*	*FCS*

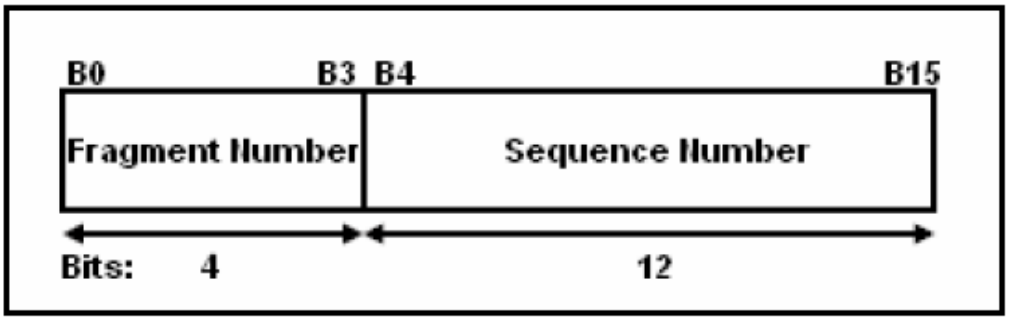
Los campos que componen esta trama son:

- ✓ Campo de control. Merece examinar aparte. Lo haremos más abajo.

- ✓ Duration/ID. es un campo de longitud 16 bit e indica el tiempo (en microsegundos) por el cual el canal estará ocupado hasta que llegue una transmisión correcta de una MPDU. En las tramas de control de tipo Power Save el campo contiene un identificador de asociación de la estación que ha trasmitido la trama.
  En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación.

- ✓ Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- ✓ Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando. Es un campo de 16 bit que a su vez está formado por dos campos, como se puede ver en su formato expuesto en la figura.

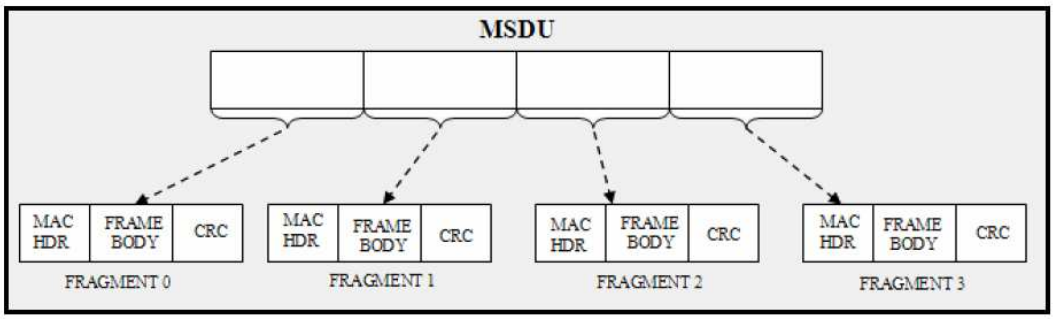


Fragment Number: indica el número del fragmento de una MSDU (MAC Service Data Unit). Vale 0 para el primer fragmento y se queda igual en todas las retransmisiones del mismo segmento.

Sequence Number: indica el número de secuencia de una MSDU que le viene atribuido por un contador de incremento unitario 4096.

El Sequence Number permanece invariante en todas las retransmisiones y para todos los fragmentos de una MSDU.

Una trama muy larga puede ser dividida en fragmentos más pequeños, cada uno de los cuales es transmitido de manera independiente a los otros y, por tanto, requiere de un propio ACK: el beneficio es evidente en el caso de intentos de transmisiones, algunas de las cuales, fallidas. Se hace entonces necesario retransmitir el único fragmento erróneo y no el entero MSDU. El inconveniente está representado en el aumento del overhead.



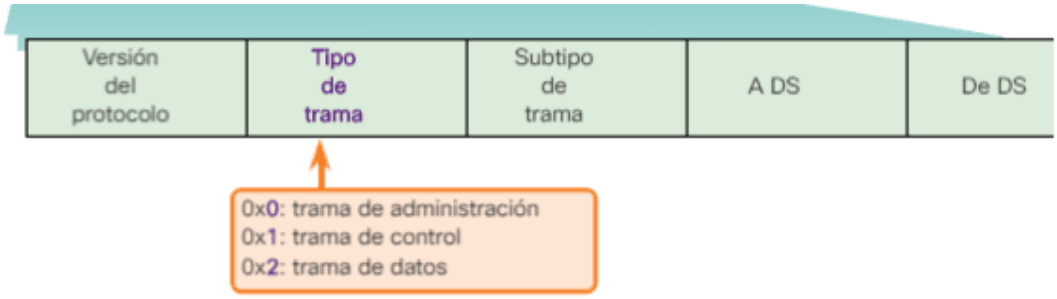
- ✓ Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- ✓ FCS. Contiene el checksum.

El **campo de control** de trama tiene el formato siguiente:

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More data	WEP	Order

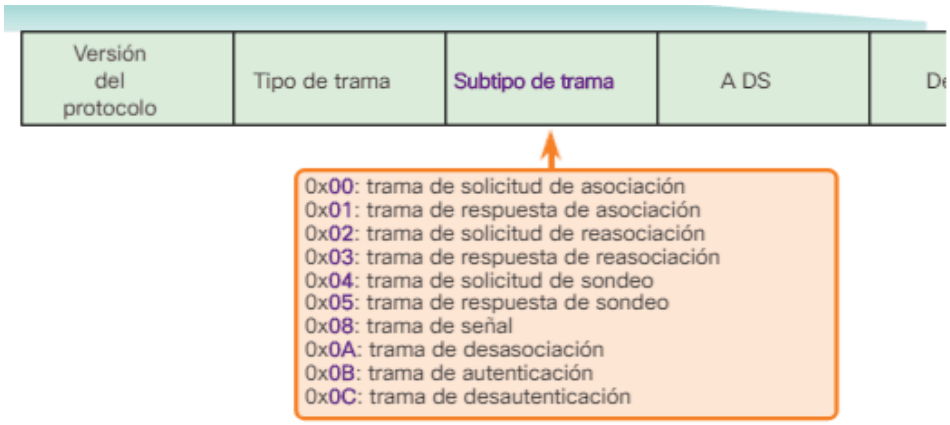
- ✓ Protocol Versión.
- ✓ Type/Subtype. Mientras tipo identifica si la trama es del tipo de datos, control o gestión.

  En particular, los valores del campo Type pueden ser 00 que identifica un Management frame, 01 para un Control frame, 10 para un Data frame y 11 si está reservado.



- ✓ el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.

Tramas de Administración:



Trama de solicitud de asociación: (0x00) se envía desde un cliente inalámbrico, permite que el AP asigne los recursos y sincronice. La trama transporta información sobre la conexión inalámbrica, incluso las velocidades de datos admitidas y el SSID de la red a la que se quiere asociar el cliente inalámbrico. Si se acepta la solicitud, el AP reserva memoria y establece una ID de asociación para el dispositivo.

Trama de respuesta de asociación: (0x01) se envía desde un AP hasta un cliente inalámbrico, contiene la aceptación o el rechazo de la solicitud de asociación. Si es una aceptación, la trama contiene información como una ID de asociación y las velocidades de datos admitidas.

Trama de solicitud de reasociación: (0x02) un dispositivo envía una solicitud de reasociación cuando sale del alcance del AP al que está asociado actualmente y encuentra otro AP con una señal más intensa. El nuevo AP coordina el reenvío de toda la información que todavía pueda contener el búfer del AP anterior.

Trama de respuesta de reasociación: (0x03) se envía desde un AP, contiene la aceptación o el rechazo de una trama de solicitud de reasociación de un dispositivo. La trama incluye la información requerida para la asociación, como la ID de asociación y las velocidades de datos admitidas.

Trama de solicitud de sondeo: (0x04) se envía desde un cliente inalámbrico cuando este requiere información de otro cliente inalámbrico.

Trama de respuesta de sondeo: (0x05) se envía desde un AP después de recibir una trama de solicitud de sondeo y contiene la información de capacidad, como las velocidades de datos admitidas.

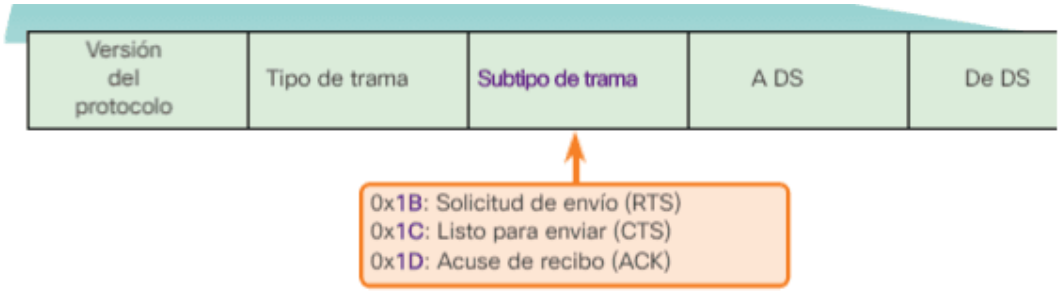
Trama de señal: (0x08) se envía periódicamente desde un AP para anunciar su presencia y proporcionar el SSID y otros parámetros configurados con anterioridad.

Trama de desasociación: (0x0A) se envía desde un dispositivo que desea finalizar una conexión. Permite que el AP detenga la asignación de memoria y quite el dispositivo de la tabla de asociación.

Trama de autenticación: (0x0B) el dispositivo emisor envía al AP una trama de autenticación que contiene su identidad.

Trama de desautenticación: (0x0C) se envía desde un cliente inalámbrico que desea finalizar la conexión de otro cliente inalámbrico.

Tramas de Control



Trama de Solicitud de envío (RTS): las tramas RTS y CTS proporcionan un esquema optativo de reducción de colisiones para los AP con clientes inalámbricos ocultos. Un cliente inalámbrico envía una trama RTS como primer paso en el enlace de dos vías, lo cual se requiere antes de enviar tramas de datos.

Trama de Listo para enviar (CTS): un AP inalámbrico responde a una trama RTS con una trama CTS. Proporciona autorización para que el cliente inalámbrico que realizó la solicitud envíe tramas de datos. La trama CTS contribuye a la administración del control de colisiones al incluir un valor de tiempo. Este retraso minimiza la probabilidad de que otros clientes transmitan mientras lo hace el cliente que realizó la solicitud.

Trama de Acuse de recibo (ACK): después de recibir una trama de datos, el cliente inalámbrico receptor envía una trama ACK al cliente emisor si no se encuentran errores. Si el cliente emisor no recibe una trama ACK en un plazo predeterminado, reenvía la trama.

Las tramas de control son fundamentales para la transmisión inalámbrica y desempeñan una función importante en el método de contienda de los medios que usan las tecnologías inalámbricas, conocido como "**acceso múltiple por detección de portadora y prevención de colisiones**" (CSMA/CA).

- ✓ ToDS/FromDS. Son Campos de 1 bit. Identifican si la trama si envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero.

  To DS: vale 1 para las tramas destinadas al DS, sino 0.

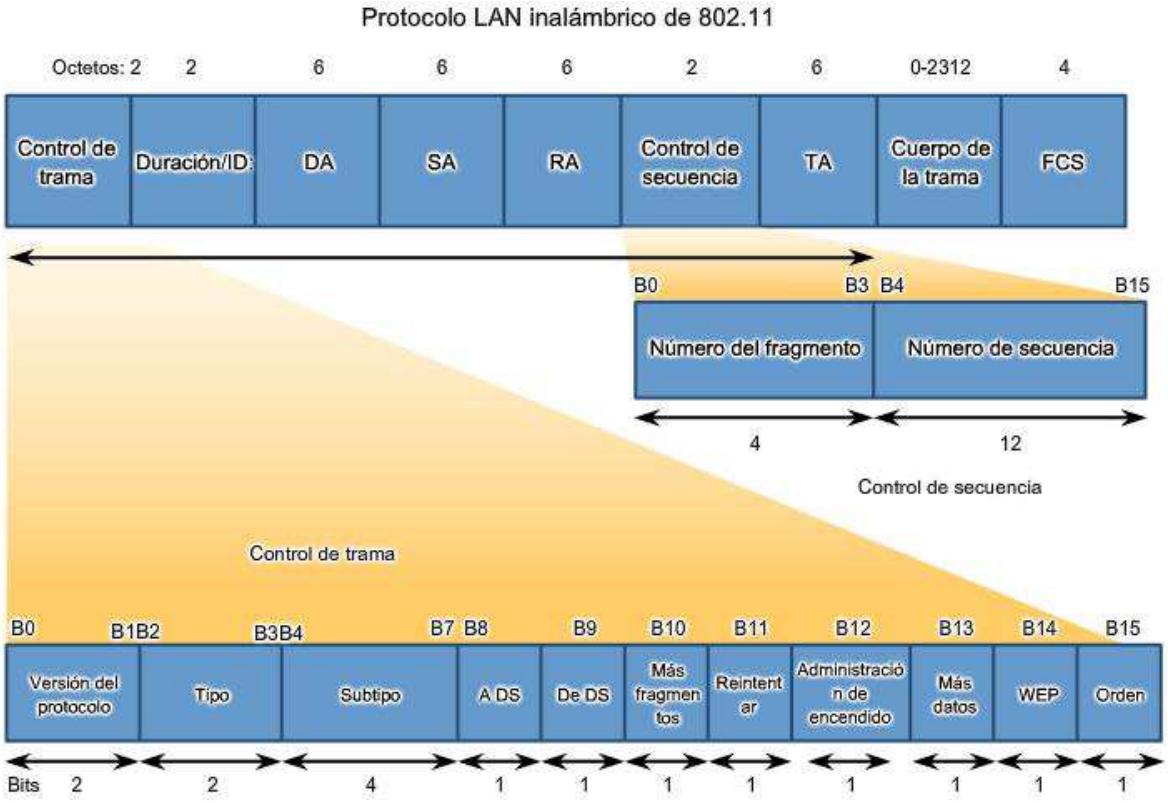
  From DS: vale 1 para las tramas o provenientes de un DS, sino un 0.

  El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS. (se muestra mas Adelante)

- ✓ Más fragmentos. Se activa si se usa fragmentación.

- ✓ Retry. Se activa si la trama es una retransmisión.

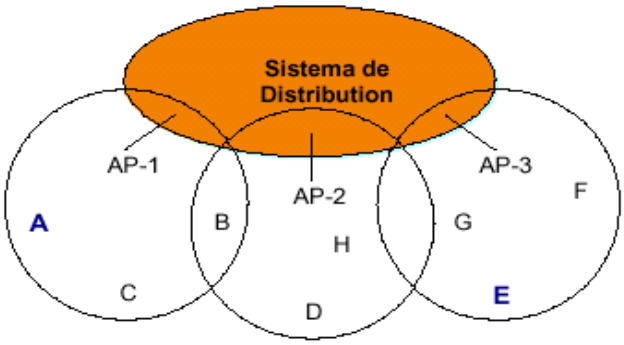
- ✓ Power Management. Se activa si la estación utiliza el modo de economía de potencia.
- ✓ More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso.
- ✓ WEP. Se activa si se usa el mecanismo de autenticación y encriptado.
- ✓ Order. Se utiliza con el servicio de ordenamiento estricto.



Direccionamiento en modo infraestructura

Veamos de manera específica como funciona el direccionamiento en modo infraestructura. Como hemos comentado con anterioridad, el caso más complejo de direccionamiento se produce cuando una estación quiere transmitir a otra ubicada en otro BSS o sistema de servicios básicos.
En este caso los campos ToDS=FromDS=1 y las direcciones de cada uno de los componentes por los que pasa la trama toman el siguiente valor en la trama MAC, quedando la dirección 1 como el nodo destino, la dirección 2 será la del punto de acceso final, la dirección 3 sería la del punto de acceso origen y por último, la dirección 4 sería la del nodo origen.

En la figura se puede ver un ejemplo de transmisión del nodo A al nodo E.



Addr1: nodo E, Addr2: AP-3, Addr3: AP-1
Addr4: nodo A

ADDRESS 1, 2, 3 y 4: son cuatro campos que contienen una dirección en el formato de la trama MAC y se utilizan para indicar el Basic Service Set Identifier (BSSID), el Destination Address (DA), el Source Address (SA), el Receiver Address (RA) y el Transmitter Address (TA). En la interpretación de los cuatro campos vienen también involucrados los campos To DS y From DS, como en la siguiente tabla:

To DS: vale 1 para las tramas destinadas al DS, sino 0.

From DS: vale 1 para las tramas provenientes de un DS, sino un 0.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Como se puede ver, si los campos To DS=0 y From DS=0, equivale decir que el DS no está involucrado en la comunicación. En el Address 1 se encuentra la dirección MAC de la estación destinataria y en el Address 2 la de la estación emisora. Así como, el Address 3 contiene el BSSID (que equivale a la dirección del AP en las redes ESS y a un número casual en las IBSS) y, por último, el Address 4 no se utiliza. De modo análogo se interpretan los demás casos.

Servicios del Sistema de Distribución. Asociación.

La especificación IEEE802.11 define el sistema de distribución como la arquitectura encargada de interconectar diferentes IBSS o redes inalámbricas independientes.
El componente fundamental de este sistema de distribución es el punto de acceso, y además la especificación define lo que llama los servicios de distribución que facilitan y posibilitan el funcionamiento en modo infraestructura. Se definirán servicios diferentes para cada componente, según se tratase de punto de acceso o estación.

Enumeraremos los servicios y expondremos el servicio de asociación, por su carácter básico. Los cinco primeros los implementa el punto de acceso y los cuatro últimos la estación. La especificación añade en algunos servicios la información necesaria para implementarlo pero no se detiene en esta implementación.

- ✓ Distribución. Se encarga de llevar un paquete del punto de acceso de origen al de destino.
- ✓ Integración. Se encarga de la función de pasarela con otros sistemas IEEE802.x.

En concreto, define el componente portal que se encargará de aspectos necesarios como redireccionamiento.

- ✓ Asociación. Servicio necesario para que una estación pueda adherirse al modo infraestructura y utilizar sus servicios.
- ✓ Reasociación. Consiste en el campo de punto de acceso al que se asocia la estación para adherirse al modo infraestructura. También se utiliza para modificar las características de la asociación.
- ✓ Autenticación y Deautenticación. Proceso necesario para que la estación se pueda conectar a la wireless LAN y consiste en la identificación de la estación.
- ✓ El proceso pues de conexión, pasa por la autenticación previamente a la asociación.
- ✓ Privacidad. Este servicio utilizará WEP para el encriptado de los datos en el medio.
- ✓ Reparto de MSDUs entre STAs. Este es el servicio básico de intercambio.

Algoritmo de Asociación Activa.

Veremos como ejemplo como funciona el sencillo algoritmo de asociación activa, según la cual la estación utilizará las tramas de prueba y respuesta para mantenerse asociada a un punto de acceso que puede variar si tiene la condición de móvil.

El algoritmo consiste en los siguientes pasos:

- ✓ El nodo envía una trama de prueba (Probe)
- ✓ Los puntos de acceso alcanzados responden con una trama de respuesta (Response)
- ✓ El nodo seleccionará generalmente por nivel de señal recibida el punto de acceso al que desea asociarse, enviándole una trama de requerimiento de asociación
- ✓ El punto de acceso responderá con una respuesta de asociación afirmativa o negativa

La asociación activa implica que la estación continuará enviando este tipo de tramas y podrá provocar una reasociación en función de los parámetros de selección que él mismo utilice y defina.

Subnivel de Gestión MAC

La subcapa de gestión MAC implementa las siguientes funcionalidades:

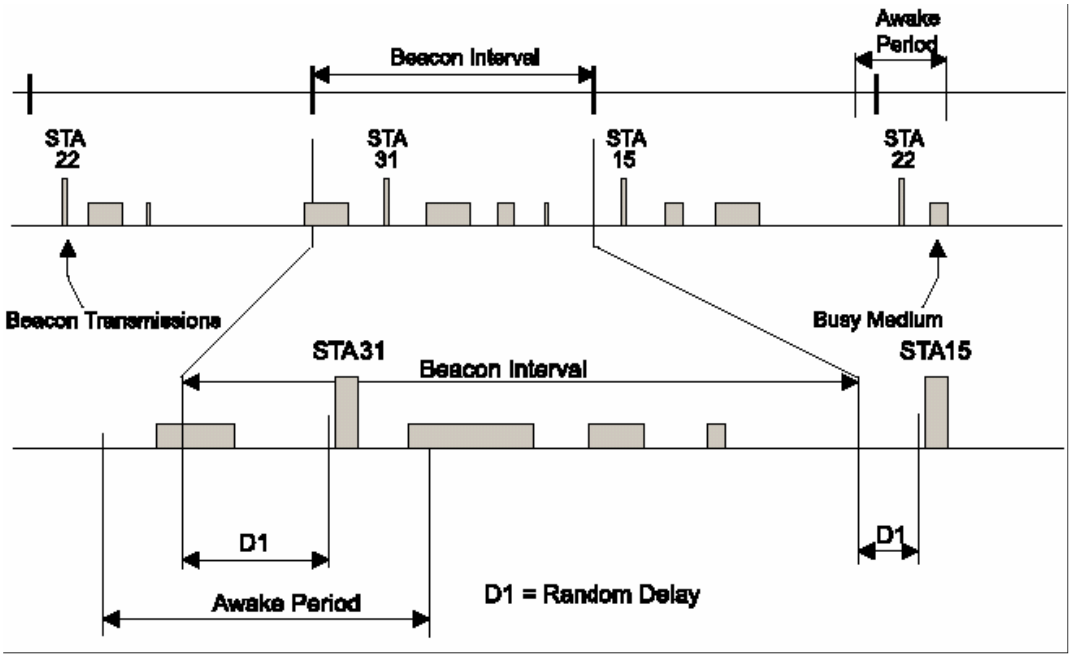
Sincronización.
Gestión de potencia
Asociación-Reasociación
Utiliza el MIB o Management Information Base

Describiremos los dos primeros puntos.

Sincronización

La sincronización se consigue mediante una función de sincronización (TSF) que mantendrá los relojes de las estaciones sincronizados. Según el modo de operación, distinguiremos el modo de funcionamiento.
En el modo infraestructura, la función de sincronización recaerá en el punto de acceso, de tal manera que el punto de acceso enviará la sincronización en la trama portadora o Beacon y todas las estaciones se sincronizarán según su valor.
En el modo ad-hoc, el funcionamiento es más complejo. Por una parte, la estación que instancie la red establecerá un intervalo de beacon, esto es, una tasa de transferencia de portadoras que permitan la sincronización.
Sin embargo, en este caso, el control está distribuido y entre todas las estaciones se intentará mantener la sincronización. Para ello, toda esta estación que no detecte en un determinado tiempo de BackOff una trama de sincronización, enviará ella misma una trama de portadora para intentar que no se desincronice la red.

En la figura podemos ver este funcionamiento.



Gestión de Potencia

Las estaciones en la red pueden adoptar un modo limitado de potencia. Este modo de funcionamiento implicará que la estación se "despertará" sólo en determinados momentos para conectarse a la red.
Estas estaciones se denominan PS-STAs (Power Save Station) y estarán a la escucha de determinadas tramas como la de portadora y poco más. 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.

El punto de acceso mantendrá almacenados los paquetes que le lleguen con destino a los nodos limitados de potencia. Por tanto, el punto de acceso mantendrá un mapa de paquetes almacenados y los destinos a quienes tendrá que repartirlos o enviarlos.
Cuando el punto de acceso decida enviarle el paquete lo hará enviándole una trama TIM o Traffic Indication Map a la estación para que despierte en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.