# El estándar IEEE 802.11
# Wireless LAN

**Francisco López Ortiz**

**ÍNDICE**

## 1. ABSTRACT

Este artículo realiza un estudio sobre el funcionamiento de los protocolos IEEE802.11 que se centran en las LAN sin cables o Wireless LAN. En concreto, se detiene en el funcionamiento de capa física, especialmente la de tecnología DSSS y de acceso al medio. Por otra parte, estudia la arquitectura de los modos *ad-hoc* e infraestructura.

## 2. 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 de una extensión de éstas últimas se tratara, pero con la flexibilidad i movilidad que ofrecen las comunicaciones inalámbricas. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 el pasado 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. Otro de los estándares definidos y que trabajan en este mismo sentido es el ETSI HIPERLAN.

La norma 802.11 ha sufrido diferentes extensiones sobre la norma para obtener modificaciones y mejoras. De esta manera, tenemos las siguientes especificaciones:

- 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.

En este trabajo nos centraremos en el estudio del primero, el estándar IEEE 802.11. 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.

El presente trabajo está estructurado tal y como se indica a continuación: en el apartado 3 se presentan las generalidades de los sistemas WLAN mediante algunas definiciones y también lo dedicamos a las configuraciones de redes inalámbricas que podemos encontrar habitualmente. En el apartado 4 nos centramos en el nivel físico y

veremos qué soluciones nos aporta 802.11 en cuanto a tecnologías de modulación y gestión de la transmisión y recepción de datos. En el apartado 5 nos centraremos en el nivel MAC del estándar IEEE 802.11 y hacemos una breve descripción del algoritmo de acceso que se utiliza en este nivel: el algoritmo CSMA/CA. Finalmente, expondremos una conclusiones y bibliografía.

## 3. GENERALIDADES SOBRE REDES DE ÁREA LOCAL INALÁMBRICAS

### 3.1 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 10 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.

### 3.2 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.

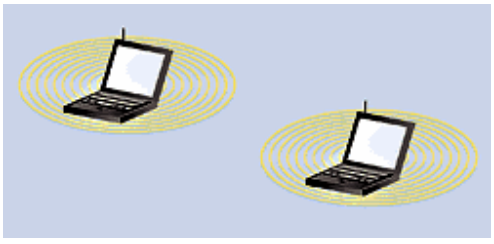
- Posibilidad de reconfiguración de la topología de la red sin añadir costes adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas 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.

### 3.3 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.

#### A. Peer to peer o redes ad-hoc

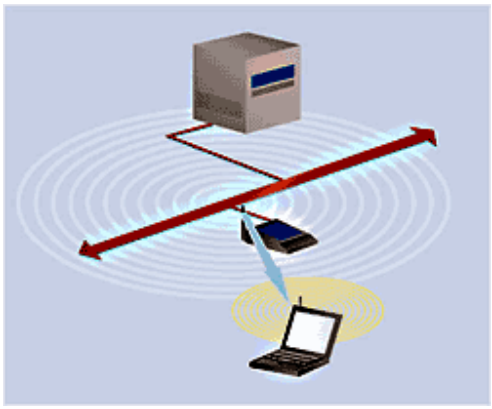
La configuración más básica es la llamada *de igual a igual* o *ad-hoc* y consiste en una red de dos terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. En la figura 3 mostramos un ejemplo. Para que la comunicación entre estas dos estaciones sea posible 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 i no requieren ningún tipo de gestión administrativa.



#### B. Modo Infraestructura

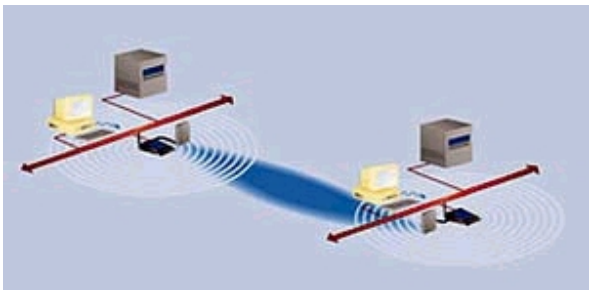
Para aumentar el alcance de una red del tipo anterior hace falta la instalación de un *punto de acces*o. Con este nuevo elemento doblamos el alcance de la red inalámbrica (ahora la distancia máxima permitida no es entre estaciones, sino entre cada estación y el punto de acceso). En la figura 4 mostramos 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.



### C. 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 6. 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.



## 4. NIVEL FÍSICO. ARQUITECTURA Y TECNOLOGÍAS DE MODULACIÓN

En este apartado realizaremos una revisión de la arquitectura de la capa de nivel físico, donde nos centraremos en describir ligeramente el funcionamiento de la capa de convergencia, fundamentalmente resaltando el proceso de transmisión y recepción de y las técnicas de modulación utilizadas por 802.11 y 802.11b.

## 4.1 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.

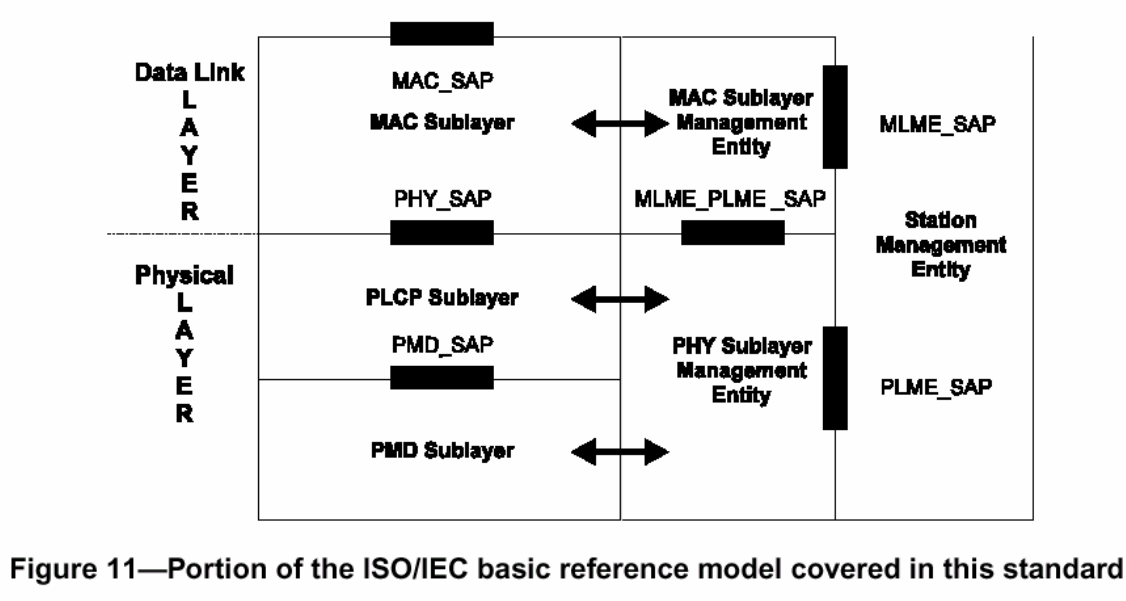



**Figure 11—Portion of the ISO/IEC basic reference model covered in this standard**

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.

## 4.2 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)

A.1 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

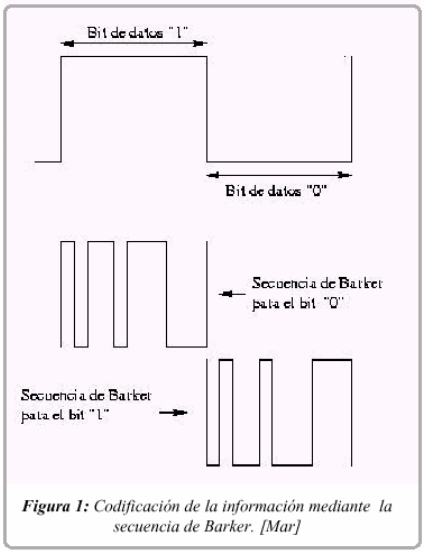



***Figura 1:*** *Codificación de la información mediante la secuencia de Barker. [Mar]*

En la Figura 1 mostramos 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 unas velocidades 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).

### A.2 Tecnología de espectro ensanchado per salto en frecuencia (FHSS)

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 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.

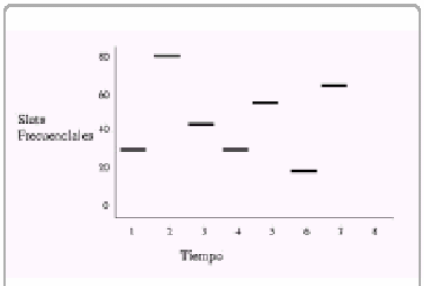



***Figura 2:*** *Modo de trabajo de la técnica FHSS, [Mar]*

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 FHSSS 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 rma.

**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, es decir, a unas frecuencias de emisión que se sitúan entre los 3,15·10e14 Hz y los 3,52·10e14 Hz. 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.

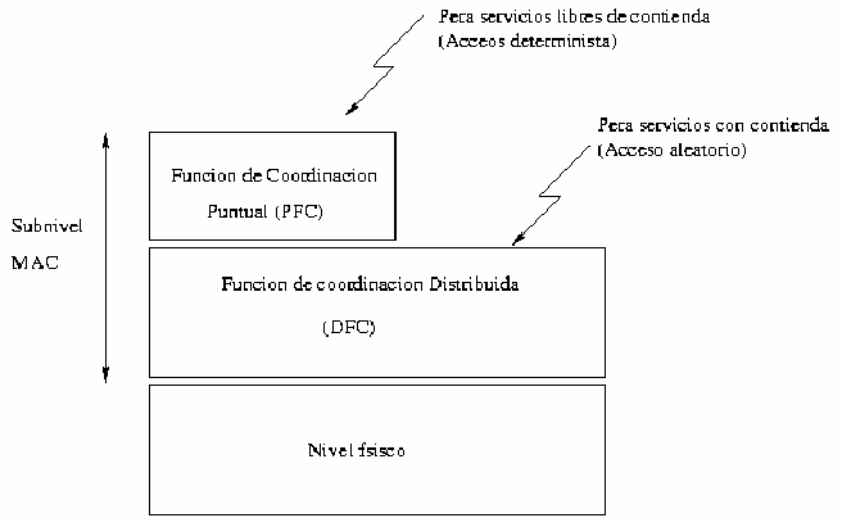
## 5. NIVEL DE ACCESO AL MEDIO (MAC)

Los diferentes métodos de acceso de IEEE802 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.

### 5.1 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.




#### 5.1.1 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

#### 5.1.1.1 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).

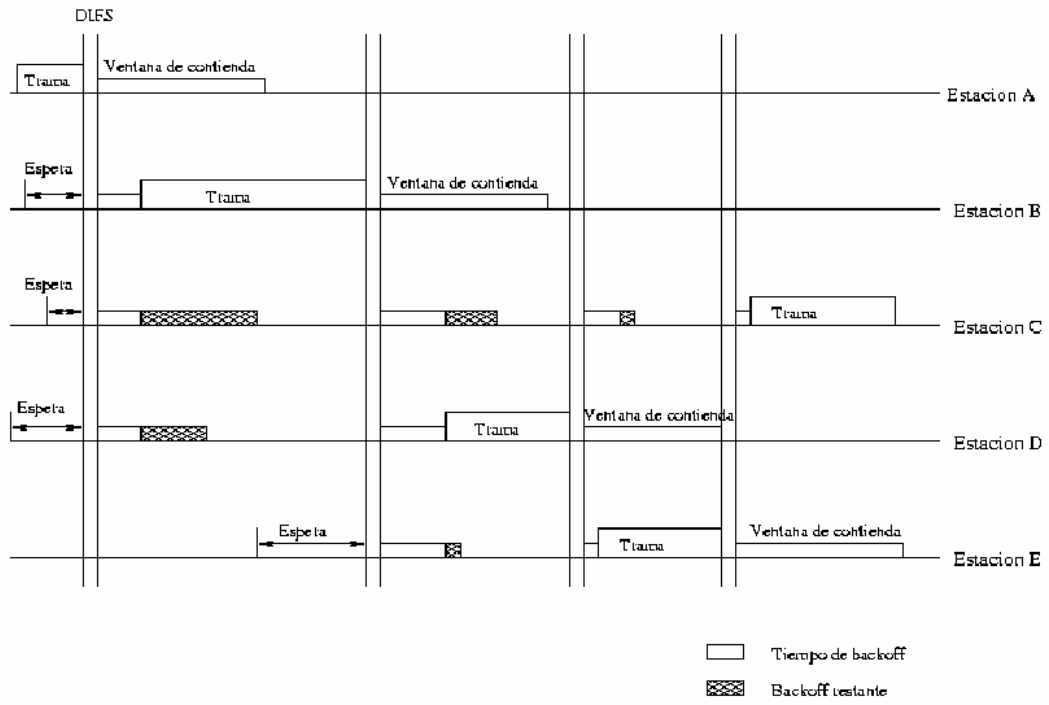
2.- Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada *espaciado entre tramas* (IFS).

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.

Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo. Por otra parte, el valor del slot time es 20μseg.




En la figura podemos ver un ejemplo de funcionamiento de acceso CSMA/CA.

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 MultiAccess 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.

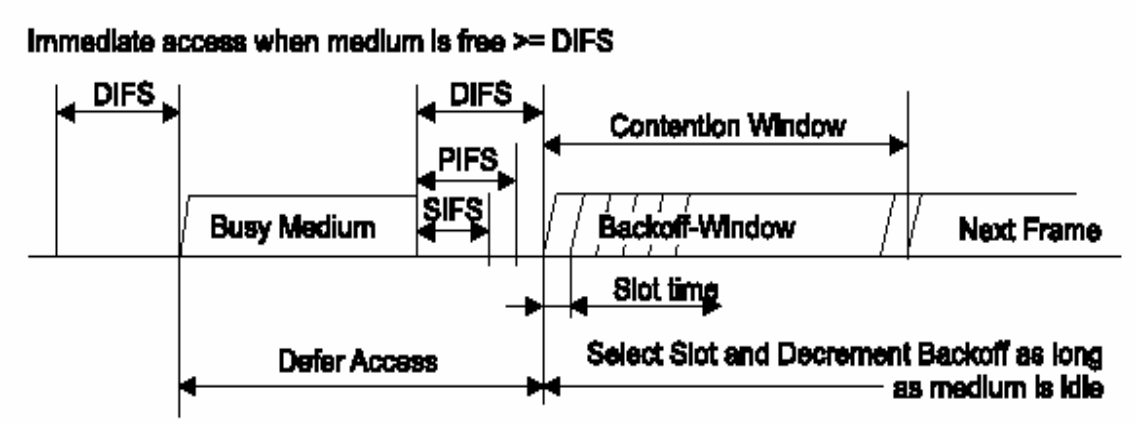
Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- 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.

#### 5.1.1.2 Espaciado entre tramas IFS

El tiempo de intervalo entre tramas se llama IFS. Durante este periodo mínimo, una estación STA estará escuchando el medio antes de transmitir. Se definen cuatro espaciados para dar prioridad de acceso al medio inalámbrico. Veámoslos de más cortos a más largos:



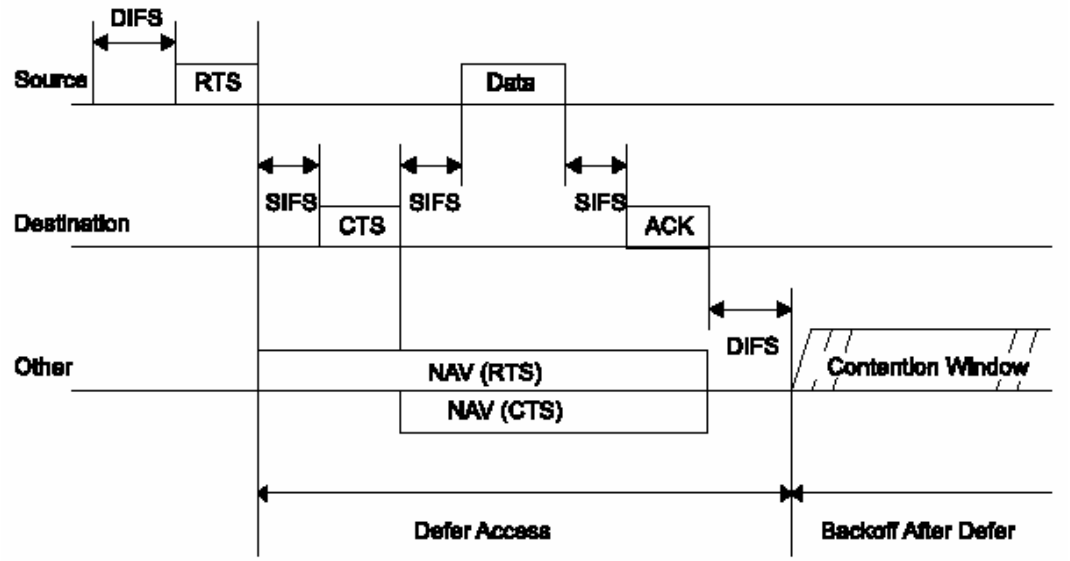

- SIFS (Short IFS). Este es el periodo más corto. Se utiliza fundamentalmente para transmitir los reconocimientos. También es utilizado para transmitir cada uno de los fragmentos de una trama. Por último, es usado por el PC o Point Control para enviar testigo a estaciones que quieran transmitir datos síncronos
- PIFS (PCF). Es utilizado por STAs para ganar prioridad de acceso en los periodos libres de contienda. Lo utiliza el PC para ganar la contienda normal, que se produce al esperar DIFS.
- DIFS (DCF). Es el tiempo de espera habitual en las contiendas con mecanismo MACA. Se utiliza pues para el envío de tramas MAC MPDUs y tramas de gestión MMPDUs.
- EIFS (Extended IFS). Controla la espera en los casos en los que se detecta la llegada de una trama errónea. Espera un tiempo suficiente para que le vuelvan a enviar la trama u otra solución.

#### 5.1.1.3 Conocimiento del medio

Las estaciones tienen un conocimiento específico de cuando la estación, que en estos momentos tiene el control del medio porque está transmitiendo o recibiendo, va a finalizar su periodo de reserva del canal.

Esto se hace a través de una variable llamada NAV (Network Allocation Vector) que mantendrá una predicción de cuando el medio quedará liberado.

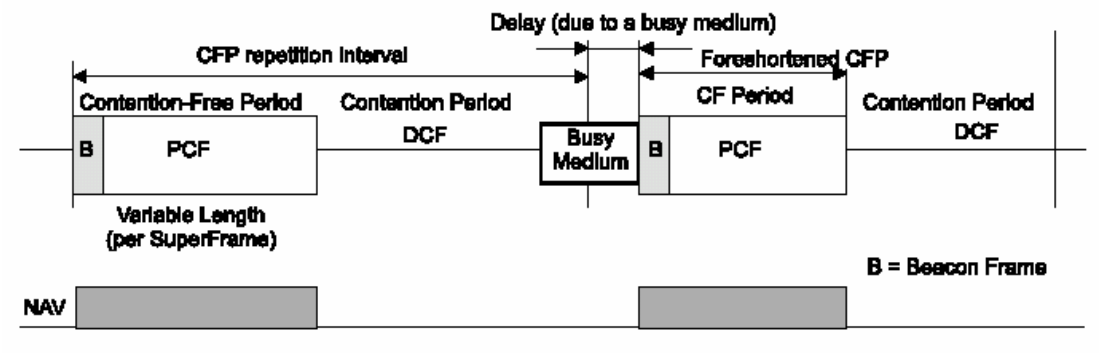
Tanto al enviar un RTS como al recibir un CTS, se envía el campo Duration/ID con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo Duration/ID. En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.




### 5.1.2 PFC  Función de Coordinación Puntual

Por encima de la funcionalidad DCF se sitúa la función de coordinación puntual, PCF, asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. El estándar IEEE 802.11, en concreto, define una técnica de interrogación circular desde el punto de acceso para este nivel. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio. En la figura 8 mostramos la relación entre estos dos modos de operación.

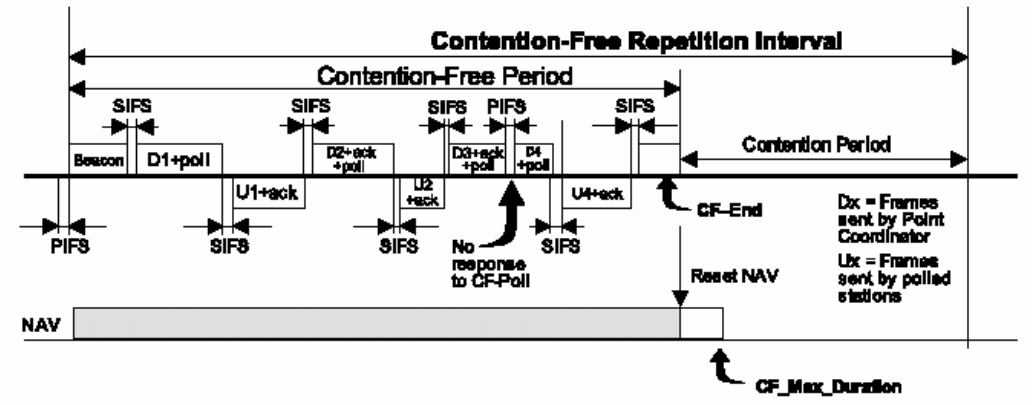
Estos dos métodos de acceso pueden operar conjuntamente dentro de una misma celda o conjunto básico de servicios dentro de una estructura llamada *supertram*a. Un parte de esta *supertrama* se asigna al periodo de contienda permitiendo al subconjunto de estaciones que lo requieran transmitir bajo mecanismos aleatorios. Una vez finaliza este periodo el punto de acceso toma el medio y se inicia un periodo libre de contienda n el que pueden transmitir el resto de estaciones de la celda que utilizan técnicas deterministas.




Un aspecto previo a comentar el funcionamiento de PFC es que es totalmente compatible con el modo DFC, observándose que el funcionamiento es transparente para las estaciones. De esta manera, una estación se asociará (se dará de alta en un modo infraestrucutra) de modo que pueda actuar en el periodo CFP, declarándose como CF-Pollable, o por el contrario, se situará su NAV según las indicaciones del punto de coordinación.

Existe un nodo organizador o director, llamado punto de coordinación o PC. Este nodo tomará el control mediante el método PIFS, y enviará un CF-Poll a cada estación que pueda transmitir en CFP, concediéndole poder transmitir una trama MPDU. El PC mantendrá una lista Pollable donde tendrá todos los datos de las estaciones que se han asociado al modo CF-Pollable. La concesión de transmisiones será por riguroso listado y no permitirá que se envíen dos tramas hasta que la lista se haya completado.

El nodo utilizará una trama para la configuración de la supertrama, llamada Beacon, donde establecerá una CFRate o tasa de periodos de contienda. Pese a que el periodo de contienda se puede retrasar por estar el medio ocupado, la tasa se mantendrá en el siguiente periodo con medio libre.



Como podemos observar, la transmisión de CF-Polls espera un tiempo SIFS. También podemos ver que si una estación no aprovecha su CF-Poll se transmite a la siguiente en el listado Pollable.

Las estaciones que no usen el CF, situarán su NAV al valor del final del CF y luego lo resetearán para poder modificarlo en el periodo de contienda en igualdad de condiciones.

Un problema importante que podemos encontrarnos en solapamiento de redes wireless ocurrirá cuando varios sistemas con coordinación puntual compartan una tasa CFRate semejante. Una solución suele ser establecer un periodo de contienda entre PCs para ganar el medio esperando un tiempo DIFS+ BackOff (1-CWmin). Sin embargo, podemos encontrarnos con mayores dificultades que exigirían un estudio diferenciado.

### 5.2 Formato de las tramas MAC

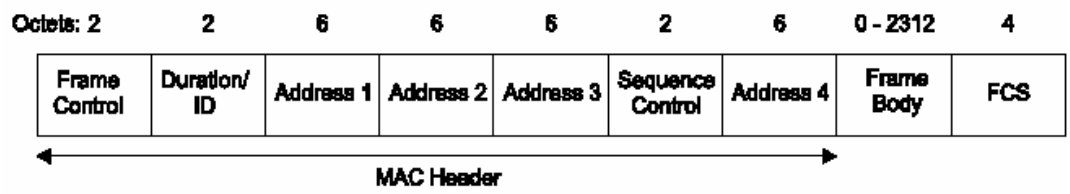
Las tramas MAC contienen los siguientes componentes básicos:

- 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 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.

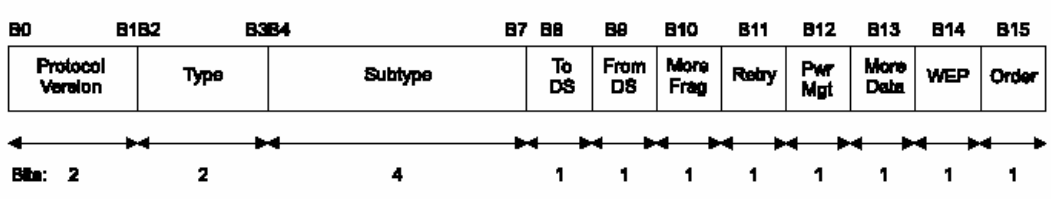
El formato de la trama MC genérica tiene el siguiente aspecto:



Los campos que componen esta trama son:

- Campo de control. Merece examinar aparte. Lo haremos más abajo.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una 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.
- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

Los campos de control de trama tienen el formato siguiente:



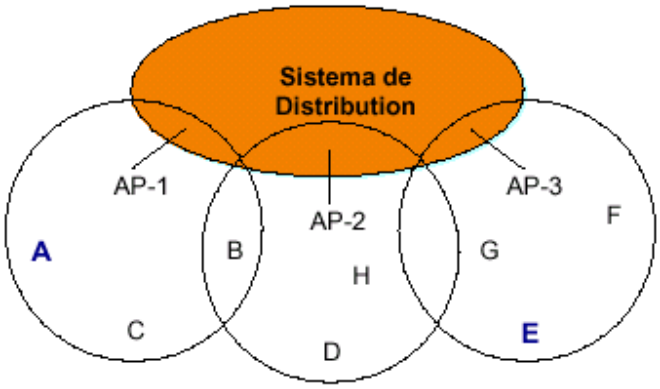

- Versión.
- Type/Subtype. Mientras tipo identifica si la trama es del tipo de datos, control o gestión, el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- ToDS/FromDS. Identifica si la trama si envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. 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.
- 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, en el cual no nos detendremos.

### 5.3 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 podemos ver un ejemplo de transmisión del nodo A al nodo E.




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

**5.4 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.

### 5.4.1 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.

## 5.5 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.

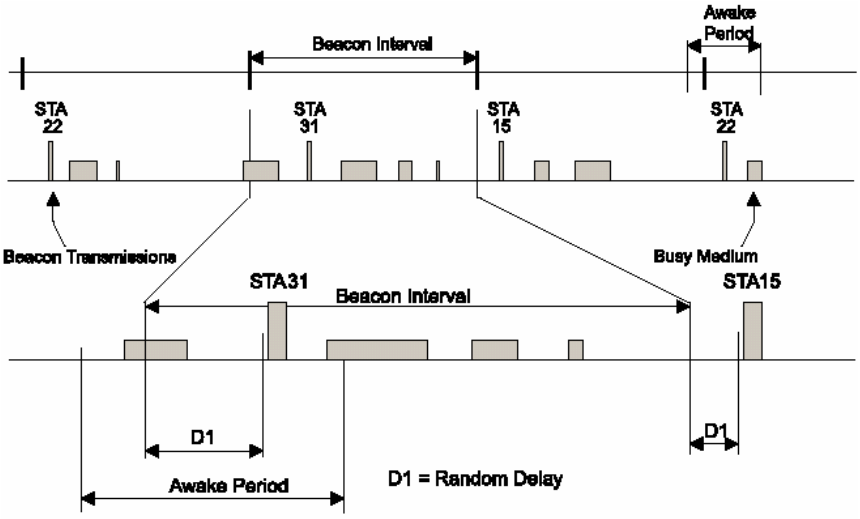
### 5.5.1 Sincronización

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.

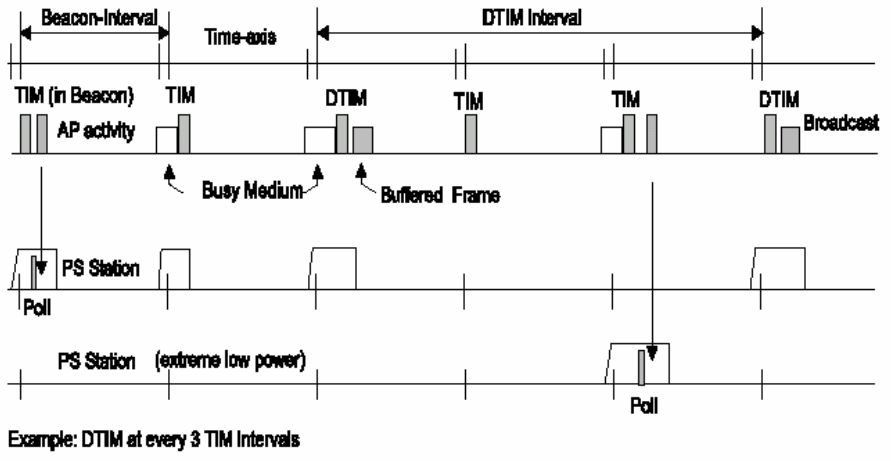
### 5.5.2 Gestión de Potencia

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.



## 6. CONCLUSIONES

Diferentes estudios sobre el algoritmo CSMA/CA para cada uno de los diferentes medios físicos demuestran que, si bien para carga baja se comportan de manera similar, a carga alta el medio infrarrojo se comporta mejor que el DSSS, y éste a su vez mejor que el FHSS, pero cuando nos movemos en condiciones de propagación ideales. En cambio, la introducción de un retardo sitúa a FHSS como la mejor solución, seguida de DSSS e IR.

Desde el punto de vista de la seguridad, se ha criticado mucho el algoritmo WEP de encriptación y actualmente se están utilizando otro tipo de soluciones a nivel más alto de capa. Parece ser que aunque la encriptación se haya modificado para el uso de claves de 128bits, el algoritmo utiliza cuatro claves de cifrado, lo cual hace sencillo el hacking y cracking por un intruso.

Como conclusión general al uso de esta tecnología, podemos decir que hay diferentes especificaciones que probablemente sobrepasen a la especificación 802.11. De hecho, actualmente está muy extendido el uso de 802.11b que alcanza velocidades de 5.5 y 11 Mbits.

## 7. BIBLIOGRAFIA


Estándares IEEE http://standards.ieee.org/db
+ IEEE802.11 Wireless LAN Medium Access (MAC) and Physical Layer (PHY)
+ IEEE802.11b Higher-Speed Physical Layer Extension in the 2.4GHz Band

Sistemas de Comunicación 1 Wireless LAN. Javier Cañas. Universidad Técnica Federico Santa María. (presentación en diapositivas)

Wireless LAN: Redes inalámbricas por Fernando Plaza Mesas http://www.arturosoria.com/

Estudio del rendimiento del algoritmo CSMA/CA IEEE802.11 con diferentes niveles físicos. Miquel Oliver Riera, Ana Escudero Quesada. Grupo de comunicaciones móviles y banda amplia

Redes de Área Local Inalámrbricas según el estándar IEEE802.11. Miquel Oliver, Ana Escudero

Seguridad y soluciones en IEEE802.11b. White Paper PROXIM.