

# Capítulo 2

## Estándar IEEE 802.11

---

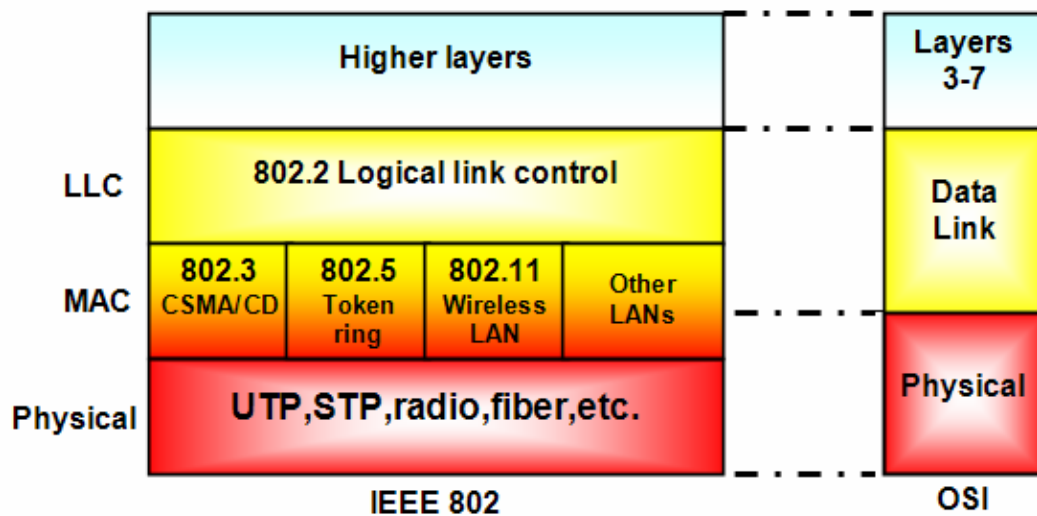
### 2.1 El proyecto 802

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. Eso permite a diversos técnicos poder realizar el mismo producto y venderlo competitivamente. Generalmente resulta ser determinante para una empresa o coalición de empresas que, creyendo en una tecnología, la realizan, y cuando ésta ha triunfado, llega a ser un estándar [4].

Los estándares de las redes LAN están definidos por los comités de la IEEE (*Institute for Electrical and Electronics Engineers*), bajo el nombre de IEEE 802 [4]. El modelo de referencia a capas de este proyecto 802, reportado en la figura 2.1, define tres estratos [5]:

- *Logical Link Control, LLC*: que gestiona los enlaces lógicos de nivel 2 y proporciona una interfaz común para el nivel de red, ocultando las diferencias relativas a la topología y a las técnicas de acceso al canal;

- *Medium Access Control, MAC*: que se preocupa de controlar y administrar el acceso al medio físico en el caso en el que venga compartido por más nodos (como un cable coaxial o el aire), buscando evitar las colisiones;
- *Físico, PHY*: cuya tarea es hacer de interfaz de las estaciones con el medio de propagación (codificación/decodificación de los bits transmitidos/recibidos, etc.).

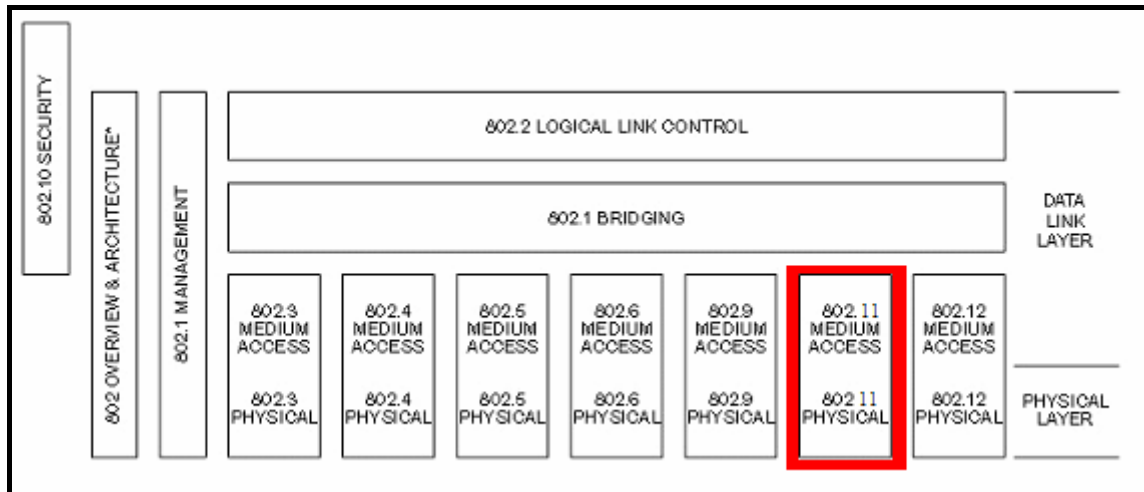


**Figura 2.1:** Estructura del proyecto IEEE 802

Como se puede notar, las funciones del nivel físico IEEE 802 constituyen un subconjunto del estrato físico OSI, en cuanto una parte del nivel MAC desarrolla funciones relacionadas al estrato físico adoptado, mientras la parte restante del nivel de control de acceso al medio y del nivel LLC desarrollan, en conjunto, las funciones típicas de la capa de enlace de datos del modelo OSI [4].

El proyecto IEEE 802 define distintas arquitecturas de redes LAN, y estas se diferencian por la modalidad de implementación del nivel físico y del nivel MAC, dado que el LLC es común a todas las redes. Viene estandarizado con la sigla IEEE 802.X y cubren todos los aspectos generales del sistema y de implementaciones de las diversas arquitecturas de red local (figura 2.2); esas son [4] [13]:

- 802.1, *higher layer LAN protocols*: describe la arquitectura general del proyecto y el modelo de referencia.
- 802.2, *Logical Link Control, LLC*: es un estándar ya consolidado o que define protocolos y formatos para la gestión de las conexiones lógicas en una red local.
- 802.3, *Ethernet*: especifica las características de la red local con topología a bus más difusa al mundo y es un estándar en continua evolución.
- 802.4, *Token Bus*: es un estándar para redes a bus utilizadas preponderantemente para automatizaciones de fábrica, con control de acceso realizado mediante transferencia de token.
- 802.5, *Token Ring*: especifica las características de las redes a anillo con control de acceso.
- 802.6, *Metropolitan Area Network*: este estándar tiene como objetivo la especificación de una red a extensión metropolitana; según este estándar la red tiene una topología física constituida por dos buses unidireccionales, que transportan información en dirección opuesta, los cuales están conectados a todas las estaciones.
- 802.9, *Unified Integrated Services* sobre Backbone.
- 802.11, *Wireless LAN*: define la modalidad de interconexión entre estaciones utilizando el aire como medio de propagación, lo que constituye hoy uno de los estándares de mayor interés para la evolución de las tecnologías de interconexión en área local, gracias a su peculiaridad de no necesitar cableado alguno en el área geográfica cubierta.
- 802.12, *Demand Priority Access Method*.
- 802.14, *Cable TV*.



**Figura 2.2:** Estándar IEEE 802.X

A exclusión del estándar 802.2 perteneciente al LLC, todos los demás pertenecen al nivel MAC y al nivel físico del modelo ISO-OSI.

## 2.2 Estándar IEEE 802.11

El estándar 802.11 define la modalidad de interconexión entre estaciones en áreas limitadas utilizando el aire como medio de transmisión; constituye uno de los estándares de mayor interés para la evolución de las tecnologías de interconexión en áreas locales [4].

El nacimiento del estándar IEEE 802.11 no ha sido inesperado; existen cerca de 7 años de estudio hasta la primera versión del estándar aparecido en el 1997 [5]. Los dispositivos que implementaban esta primera versión explotaban la frecuencia ISM de 2.4GHz, alcanzando una tasa de bit de 1-2 Mbps. El estándar está en continua evolución, permitiendo velocidades de conexiones siempre más elevadas, gracias a las investigaciones de numerosos grupos de trabajo. En septiembre del 1999 fue ratificado el 802.11b [6] (conocido también como 802.11HR, de High Rate), a continuación fue ratificado también el 802.11a [7] y últimamente, en junio de 2003, el 802.11g [8]. Vemos mejor todos los estándares de la familia IEEE 802.11 en la siguiente tabla 2.A [9]:

**Tabla 2.A:** Estándares del IEEE 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	-----	-----

La versión original del estándar preveía un único estrato MAC que interactuaba con tres niveles físicos distintos PHY: dos posibles interfaces RF, operantes con técnica SSS (*Spread Spectrum Signals*) y una transmisión inalámbrica en el infrarrojo (IR) [5]. El protocolo a nivel MAC que viene usado desde todas las extensiones del 802.11 (incluida la versión original) es el CSMA/CA.

## 2.3 Topología de red del 802.11

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. 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 [9]. El estándar prevé dos funciones de coordinación [9]:

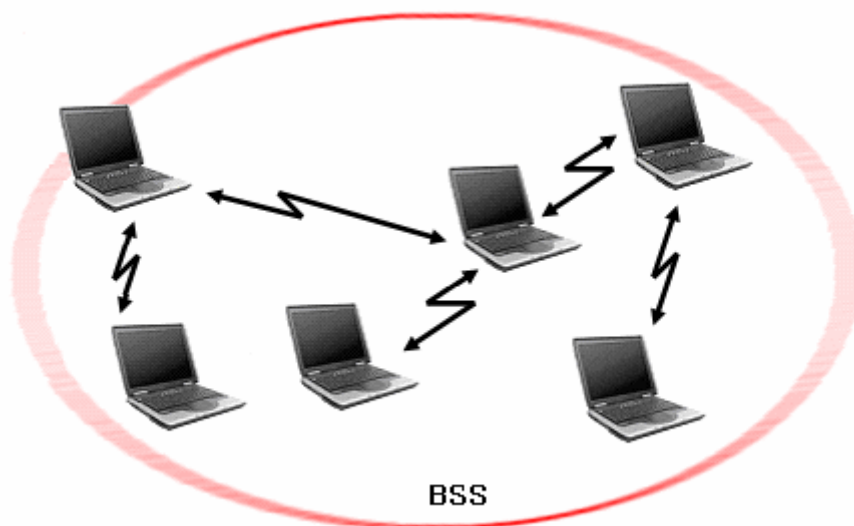
- DCF (*Distributed Coordination Function*), de tipo distribuida;
- PCF (*Point Coordination Function*), que se basa sobre un único nodo de coordinación.

El estándar prevé que más BSS puedan ser conectadas con una dorsal (*backbone*) llamada *Distribution System* (DS) dentro de una ESS, 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 presentes en una BSS pueden comunicarse directamente entre ellas [9].

El estándar soporta las dos siguientes topologías de red [1] [5]:

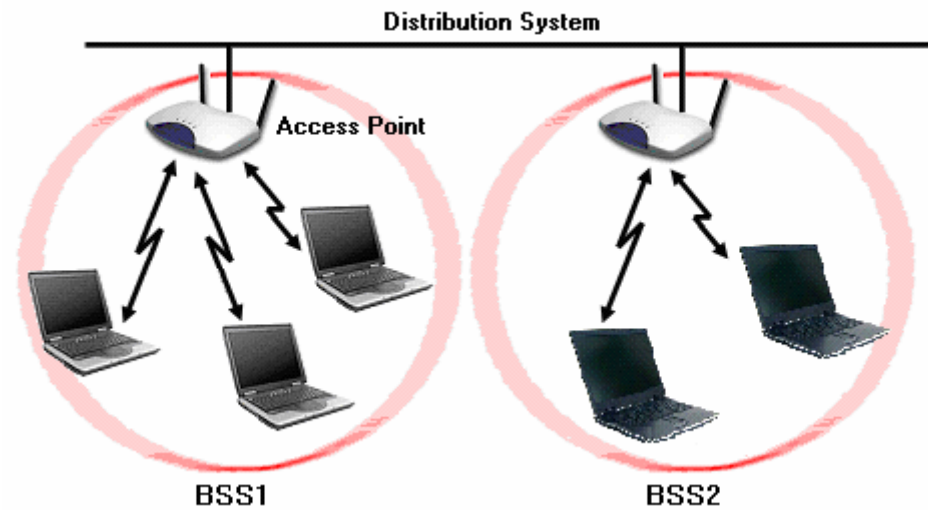
- Redes IBSS (*Indipendent Basic Service Set*)
- Redes ESS (*Extended Service Set*)

En las redes IBSS, cada estación puede comunicar directamente con otra perteneciente a la misma BSS sin que el tráfico sea llevado hacia cualquier AP o a través de más estaciones intermedias. Un ejemplo se muestra en la figura 2.3. El concepto IBSS se avecina mucho a las características de una red ad-hoc, en cuanto a que su objetivo es aquel de hacer comunicar las estaciones directamente entre ellas, sin tener que acceder a redes dotadas de infraestructura (de las redes wireless ad-hoc se discutirá ampliamente más adelante).



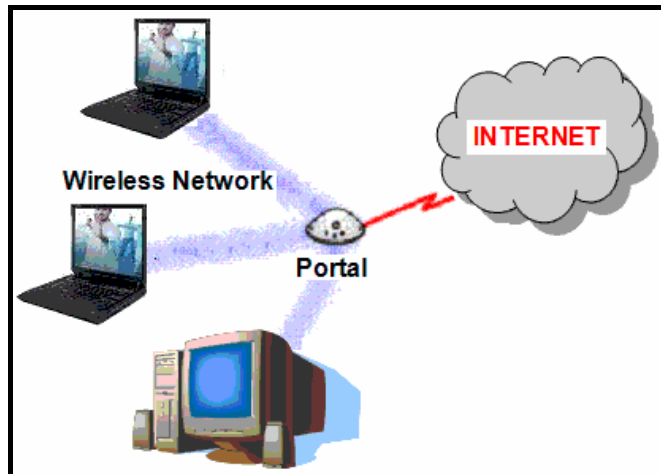
**Figura 2.3:** Ejemplo de red IBSS

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 2.4). Este se ocupa de transferir al MAC 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.



**Figura 2.4:** Ejemplo de red ESS

A través de dispositivos llamados *portal*, una ESS puede proporcionar también un acceso a Internet mediante la integración lógica entre una wireless LAN y una tradicional LAN cableada. Las redes ESS, sin embargo, no entran en el conjunto de las redes ad-hoc en cuanto necesitan una infraestructura fija.



**Figura 2.5:** Acceso a Internet

## 2.4 El nivel MAC para el 802.11

### 2.4.1 Formato de las tramas del MAC 802.11

La arquitectura lógica del estándar IEEE 802.11 está definida por el nivel MAC PHY de la pila ISO-OSI.

Esta clase de diseños a niveles es común a todas las modernas arquitecturas de red; lo que varía de una a otra es el número de niveles, su nombre y la entidad contenida. La finalidad de cada nivel es aquella de proporcionar servicios a las entidades del nivel superior, enmascarando el modo en las que son implementadas. A excepción del nivel más alto, un nivel  $N$  proporciona servicios de su nivel a las entidades del nivel  $N+1$ . Las entidades de nivel  $N$ , excepto el nivel físico, usan para comunicarse un servicio del nivel  $N-1$ . Las entidades de nivel físico se comunican directamente a través de los medios de transmisión que los interconectan. Entidades pertenecientes al mismo nivel, sobre sistemas distintos, se llaman *peer-entities*.

Por lo tanto, dados dos sistemas, ningún dato es transferido directamente desde un nivel  $N$  a otro nivel  $N$ ; de hecho, cada nivel transmite datos e información de control a aquel inferior. En el nivel físico se efectúan las transmisiones.



El bloque de datos que se trasfiere en estas operaciones constituye la trama (*frame*). Esta representa la unidad informativa del nivel MAC de cada estación en la cual vienen encapsulados los datos de usuario del nivel superior (LLC).

Cada trama de nivel MAC comprende un conjunto de campos que se suceden con un orden preestablecido en todos ellos [5] [4]: una cabecera (MAC *header*); el cuerpo de la trama (*frame body*), de longitud variable (máximo 2312 byte) que contiene informaciones específicas en base al tipo de trama; un FCS (*Frame Check Sequence*) que contiene un código de redundancia cíclica (*CRC*) a 32 bit.

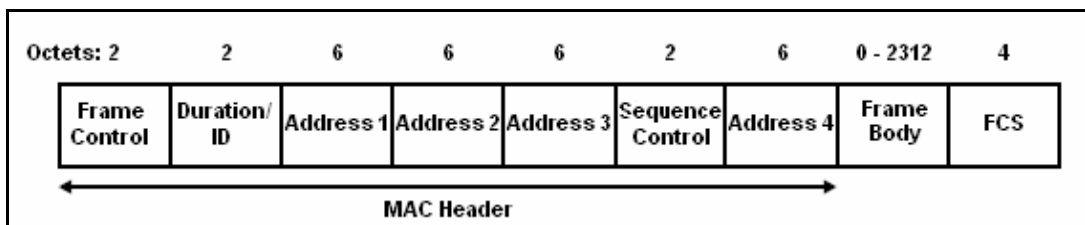


Figura 2.6: Formato general de la trama MAC 802.11

Examinamos ahora los campos que componen la cabecera del MAC:

- **FRAME CONTROL:** este campo contiene las informaciones de control estructuradas como vienen mostradas en la figura 2.7. Eso comprende:

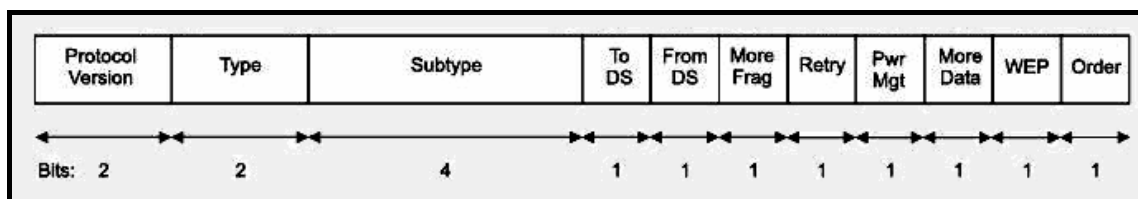


Figura 2.7: Formato del campo Frame Control.

- Protocol Versión: es un campo de longitud 2 bit, su valor por defecto es 0 y todos los demás valores están reservados para versiones futuras del protocolo.

- Type y Subtype: el campo Type tiene longitud 2 bit y el Subtype 4 bit. Juntos identifican si la trama es de gestión, de control o de datos. 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 [5]:
  - Trama de *datos (Data Frames)*: para la transmisión de las unidades informativas.
  - Trama de *control (Control Frames)*: para el control del acceso al medio.
  - Trama de *gestión (Management Frames)*: utilizadas para intercambiar información sobre la gestión de la conexión.
- To DS: es un campo de 1 bit, y vale 1 para las tramas destinadas al DS, sino 0.
- From DS: es un campo de 1 bit, y vale 1 para las tramas provenientes de un DS, sino un 0.
- More Fragments: es un campo de 1 bit, y vale 1 en todas las tramas de datos o de gestión que tienen fragmentos de la MSDU, sino vale 0.
- Retry: es un campo de 1 bit, y vale 1 en todas las tramas de datos o de gestión que son retransmitidas en un mismo frame, sino vale 0. Esta información la usan las estaciones receptoras para eliminar las tramas duplicadas.
- Power Management: es un campo de 1 bit e indica el estado de energía en la que se encontrará la estación después de haber completado la secuencia de intercambios de tramas.
- More Data: es un campo de longitud 1 bit y si está a 1 indica que hay otras MSDU que están para ser enviadas a la estación receptora.
- WEP: está puesto a 1 si el campo frame body contiene informaciones que están codificadas mediante algoritmo WEP.
- Order: si está puesto a 1 indica a la estación receptora que procese los datos según el orden de llegada.

- **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-Poll el campo contiene un identificador de asociación de la estación que ha transmitido la trama.

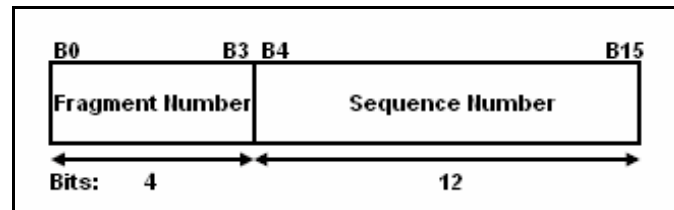
- **ADDRESS 1, 2, 3 y 4:** son cuatro campos que contienen una dirección en el formato de la trama MAC y se utilizan para indicar el Basic Service Set Identifier (BSSID), el Destination Address (DA), el Source Address (SA), el Receiver Address (RA) y el Transmitter Address (TA). En la interpretación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

**Tabla 2.B:** Interpretaciones de los campos Address1, 2, 3 y 4 en función de To DS y From DS.

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.

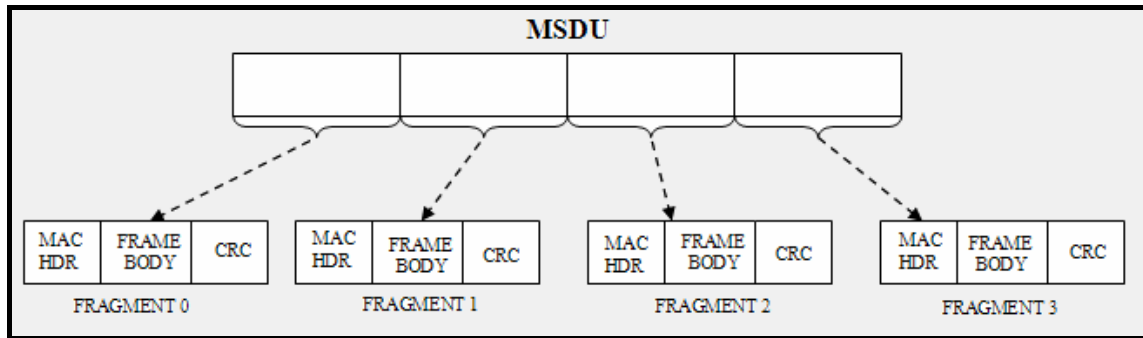
- **SEQUENCE CONTROL:** es un campo de 16 bit que a su vez está formado por dos campos, como se puede ver en su formato expuesto en la figura 2.8.



**Figura 2.8:** El campo Sequence Control.

- 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.
- Fragment Number: indica el número del fragmento de una MSDU. Vale 0 para el primer fragmento y se queda igual en todas las retransmisiones del mismo segmento.

Una trama muy larga puede ser dividida en fragmentos más pequeños (figura 2.9), 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.



**Figura 2.9:** Fragmentación de una trama.

- **FRAME BODY:** es un campo de longitud variable; su longitud mínima es de 0 byte y la máxima de 2312 byte. Estas contienen información específica al tipo de trama.
- **FCS:** campo de 32 byte que contiene el código CRC a 32 bit que viene calculado sobre todos los campos de la cabecera más el campo Frame Body.

### 2.4.2 Acceso al medio en el IEEE 802.11

En una red gobernada por un protocolo de acceso casual al medio, no hay preasignaciones de banda a las individuales estaciones, más bien, cada una de ellas accede al canal independientemente de las otras. Para evitar transmitir simultáneamente a otra estación y causar una *colisión*, los terminales que trabajan en una red inalámbrica deben necesariamente regular el acceso al canal. Tal comportamiento se hace necesario por las características de compartir el medio físico utilizado para el intercambio de información [4].

Así como en la red cableada, se hacen necesarias las políticas de contienda del medio de transmisión entre estaciones para administrar los posibles eventos de conflictos. El nivel MAC se encarga de la entrega de las unidades informativas de nivel superior (LLC) entre estaciones origen y destino, garantizando el éxito de la transferencia y ocupándose de la gestión de la denominada lógica de coordinación para acceso al medio.

Como ya hemos dicho, la función de coordinación podría ser constituida por la lógica de coordinación llamada DCF (*Distributed Coordination Function*) que es de tipo distribuida, o de la PCF (*Point Coordination Function*) que se basa sobre un único nodo de coordinación (este último procedimiento no será tratado en este proyecto dado que estamos orientados al estudio de redes privadas de un control centralizado) [1] [5]. El estándar define, además, dos diferentes intervalos de tiempo: el CP (*Contention Period*) durante el cual la red usa el DCF, y el CFP (*Contention Free Period*) durante el cual viene utilizado el PCF [5].

La técnica DCF usa el protocolo CSMA/CA con los ACK y un tiempo casual de backoff, asegurando la interoperatividad entre estaciones que transmiten con tasa de datos distintas.

#### **2.4.2.1 El protocolo CSMA/CA**

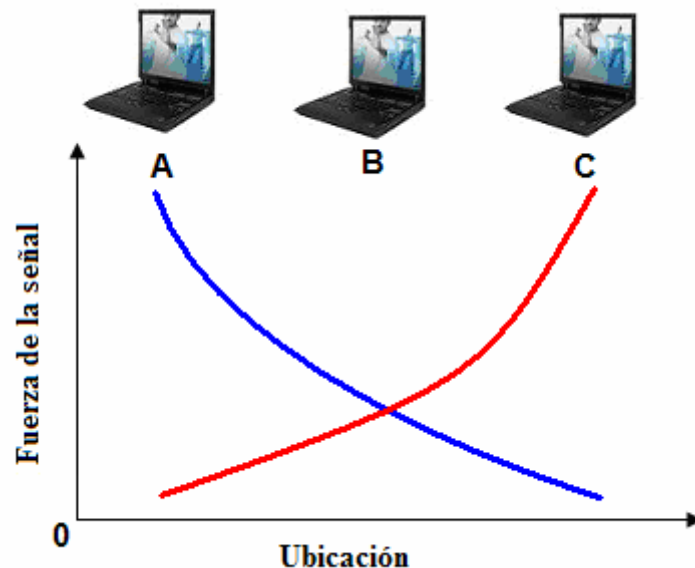
El protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) pertenece a la clase de protocolos de acceso (CSMA) que efectúan un *sensing* (revelación) del canal antes de iniciar una transmisión [4]. En el estándar 802.11, la capa física sondea el nivel de energía sobre la frecuencia radio para determinar si hay o no transmisión [10]. Eso prevé que la capa física “pruebe” el canal de transmisión y proporcione esta información al protocolo MAC [10]: la estación podrá transmitir sólo si el canal está libre, sino, esperará a que lo esté, buscando evitar de este modo las colisiones.

A la clase de los protocolos CSMA pertenece también el CSMA/CD (*CSMA with Collision Detection*), utilizado en el estándar 802.3 y en todas las redes Ethernet cableadas, el cual prevé que una estación que está transmitiendo sobre el canal libre escuche aquello que efectivamente está sobre el canal: de hecho podría existir una colisión debida al hecho que dos o más estaciones hubiesen sentido el canal libre en el mismo momento. Sin embargo, el CSMA/CA del 802.11, a diferencia del CSMA/CD, no implementa la revelación de las colisiones por, al menos, dos motivos: la capacidad de percibir las colisiones requiere la posibilidad tanto de enviar como de recibir al mismo tiempo y eso puede ser costoso; pero más importante es el hecho que aunque se

revelaran las colisiones y al momento del envío no revelara alguna, una colisión se podría verificar siempre al receptor [10].

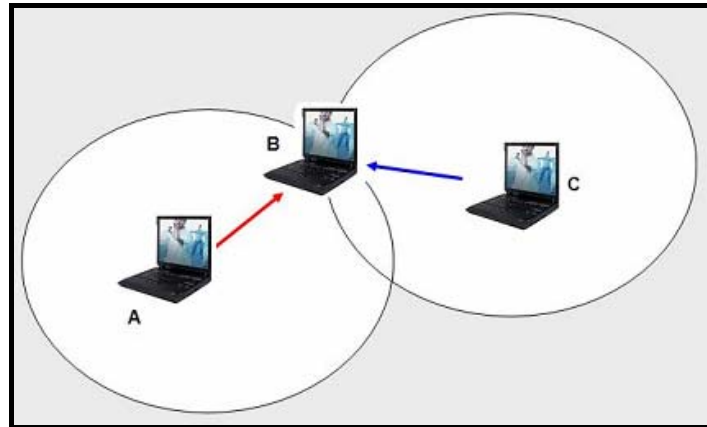
Esta última situación deriva de algunos problemas particulares del medio de transmisión sin cables [10] [11]:

- *El problema de la atenuación (fading)*: debido a la atenuación de la señal cuando se propaga a través del aire, dos estaciones pueden transmitir simultáneamente hacia el mismo nodo y provocar en el receptor colisiones no advertidas. Esto se esquematiza en el gráfico de la figura 2.10:



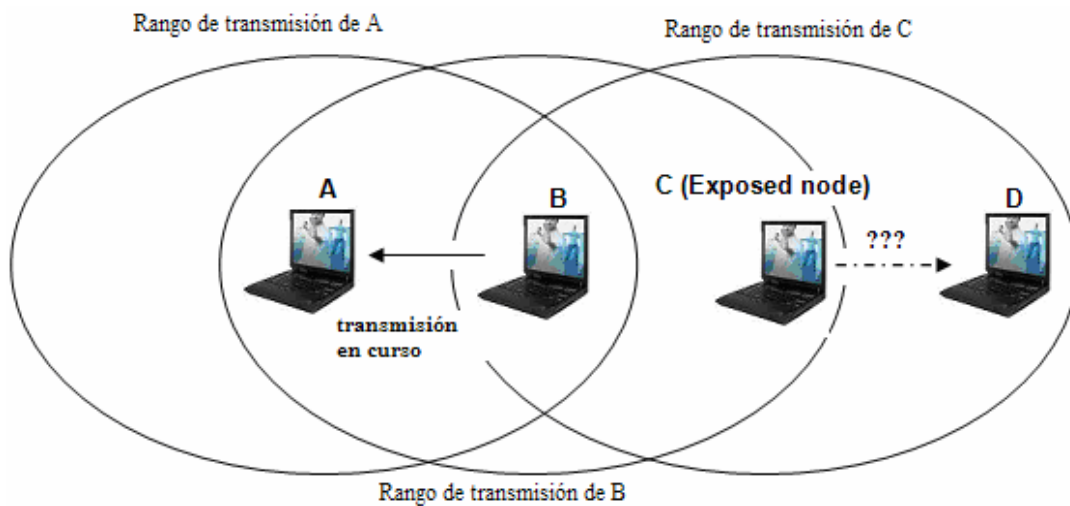
**Figura 2.10:** Problema de la atenuación

- *El problema del terminal oculto (hidden terminal problem)*: los obstáculos físicos en el ambiente (por ejemplo una montaña) o la distancia pueden hacer que la estación A compruebe el canal, lo encuentre libre e inicie una transmisión hacia el nodo B que está ya recibiendo una trama desde otra estación C. A B le llegan dos paquetes desde nodos diferentes provocando así una colisión.



**Figura 2.11:** Problema del terminal oculto

- *El problema de la estación expuesta (exposed node)*: haciendo referencia a la figura 2.12, se nota que B está transmitiendo una trama a A; el nodo C (nodo expuesto) no puede transmitir hacia D porque siente el canal ocupado por la transmisión de B (se encuentra en su radio de acción), aunque su transmisión no creara una colisión en A. Este problema lleva a una baja utilización de la banda disponible [12].



**Figura 2.12:** Problema del nodo expuesto

A continuación se tratará la manera de limitar estos problemas.



#### 2.4.2.2 Los intervalos *interframe* del nivel MAC 802.11

Las tramas del nivel MAC están espaciadas en el tiempo a intervalos llamados IFS (*InterFrame Space*) [5]. 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 [5]:

- *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.
- *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 (2.1) y su duración es tal para proporcionar una prioridad de acceso al canal.

$$\text{PIFS} = \text{aSlotTime} + \text{SIFS} > \text{SIFS} \quad (2.1)$$

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

$$\text{DIFS} = \text{aSlotTime} + \text{PIFS} > \text{PIFS} \quad (2.2)$$

- *EIFS (Extended IFS)*: se utiliza solamente en modalidad DCF cada vez que el nivel físico lo indica, para el nivel superior (MAC), que verifican los errores en la transmisión. Este intervalo se relaciona con los otros mediante la siguiente función:

$$EIFS = SIFS + [8 * dimension ACK (\mu s) + dimension PLCP Preamble (\mu s) + dimension PLCP Header (\mu s)] + DIFS \quad (2.3)$$

donde  $EIFS > DIFS$ .

En la figura 2.13 se representan las relaciones temporales entre estos valores y se esquematiza el denominado procedimiento de backoff [5].

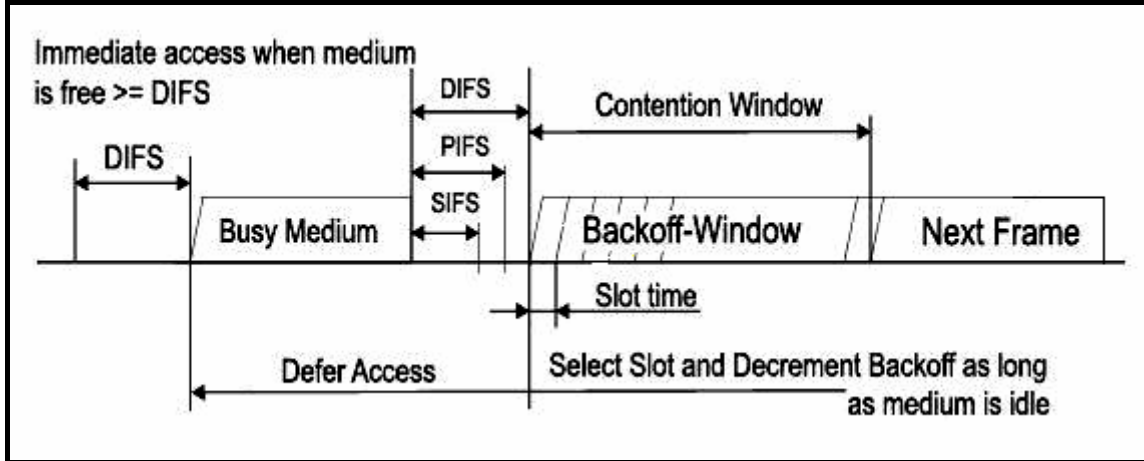


Figura 2.13: Relaciones entre IFS

### 2.4.2.3 El procedimiento del *backoff*

El procedimiento del *backoff* [5] (tiempo de espera) viene llevada a cabo en estas situaciones:

- Inmediatamente después de que la estación, comprobando el medio antes de la transmisión de la trama, haya sentido el canal ocupado;
- Cuando una trama debe ser retransmitida;
- Después de las transmisiones llevadas a cabo con éxito en particulares tramas (aquellas con el bit More Fragments igual a 0 o aquellas con el campo Subtype igual al PS-Poll).

Cada estación que intenta iniciar una transmisión debe primero efectuar el *carrier-sense* (comprobación del canal), y sólo después de haber sentido el canal libre por un tiempo mayor o igual a un DIFS (o a un EIFS, en el caso de que una transmisión anterior no haya sido completada con éxito) podría transmitir una trama. Por lo tanto, en el caso en que el canal resultase ocupado, la estación debería retrasar la transmisión hasta que el canal quede libre mediante un DIFS o un EIFS, según los casos. Además, para precaver la posibilidad de colisión con otras estaciones que queriendo transmitir habían igualmente sentido libre el canal con un DIFS o un EIFS, viene calculado un tiempo casual de backoff, es decir, un posterior tiempo de espera.

El tiempo de backoff generado casualmente, indica cuanto tiempo debe esperar la estación después de que el canal se sienta libre con un DIFS o un EIFS. El valor del backoff viene calculado según la siguiente expresión:

$$\text{Backoff Time} = \text{Random}() * \text{aSlotTime} \quad (2.4)$$

donde,

- *Random()* es un número entero pseudocasual extraído de una distribución uniforme en el intervalo  $[0, CW]$ , donde *CW* (*Contention Window*) es

un número entero expresado entre dos parámetros característicos del nivel físico llamados  $aCW_{min}$  y  $aCW_{max}$ .

$$aCW_{min} \leq CW \leq aCW_{max} \quad (2.5)$$

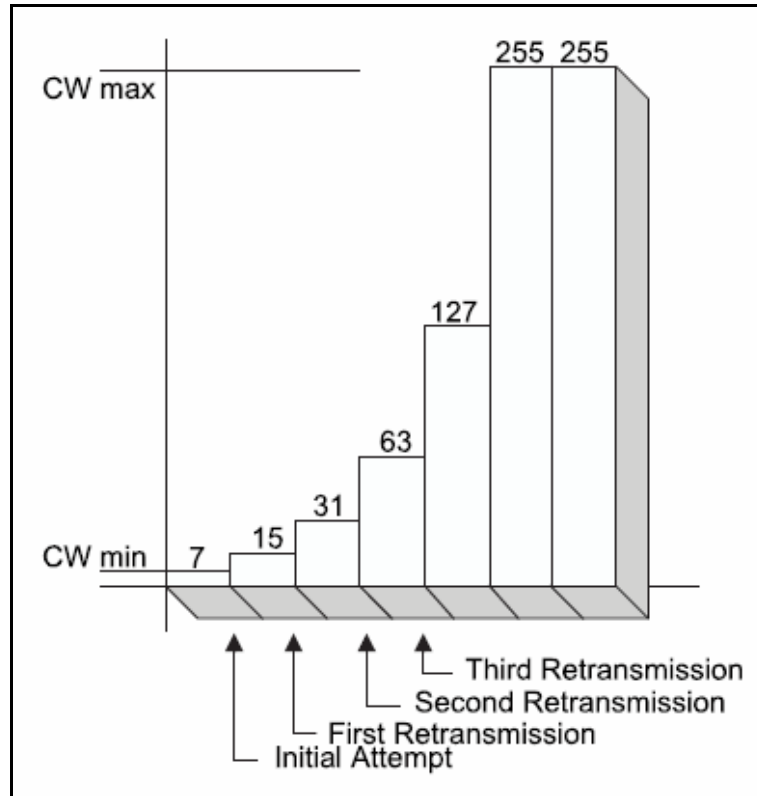
○ *aSlotTime* es el parámetro que define la duración del *time slot* (tiempo de slot) a nivel físico, y depende de la particular tecnología de transmisión utilizada (50 $\mu$ s para el Frequency Hopping Spread Spectrum, 20 $\mu$ s para el Direct Sequence Spread Spectrum, 8 $\mu$ s para el Infrarrojo).

Después de haber esperado que el canal quedase libre mediante un DIFS o un EIFS, la estación, para poder transmitir su trama, debe decrementar un contador llamado *Backoff Timer*, que parte del valor del Backoff Time (calculado con la fórmula 2.4) y decrece en una unidad con cada intervalo de *aSlotTime*. Durante este decremento, la estación sigue sondeando el canal para tener en cuenta si, mientras tanto, cualquier otra estación ha ocupado el medio. En el caso en el que esto ocurra, todas las estaciones detienen el decremento y el valor del contador viene congelado para utilizarlo como valor inicial en la próxima contienda, garantizando a las relativas estaciones un tipo de prioridades de acceso al medio. Cuando el Backoff Timer se pone a cero, la estación podrá transmitir su trama ocupando el canal. Sin embargo se podrá verificar que dos estaciones, habiendo generado el mismo número de backoff, inician a transmitir simultáneamente sobre el canal, provocando una colisión de la cual se perciben no recibiendo la trama ACK de confirmación.

El parámetro CW varía dinámicamente en cada una de las estaciones con el intervalo [ $aCW_{min}$ ,  $aCW_{max}$ ]. Se parte de un valor inicial igual a  $aCW_{min}$  y viene incrementado exponencialmente al verificarse una colisión, hasta alcanzar el valor  $aCW_{max}$ , según la siguiente expresión:

$$CW = 2 * CW + 1 \quad (2.6)$$

En cambio, si la transmisión de la trama va a buen fin (recepción del ACK), entonces CW vuelve a configurarse como  $aCW_{min}$ .



**Figura 2.14:** Incremento exponencial de CW

#### 2.4.2.4 DCF (Distributed Coordination Function)

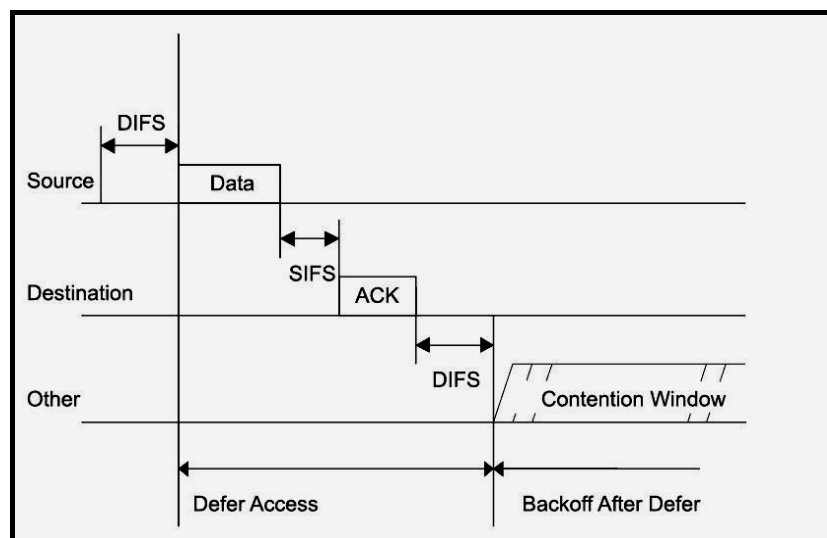
El DCF [1] [5] representa el principal método de acceso al canal en una red wireless y viene utilizado para la transferencia asíncrona de los datos en modalidad *best-effort*, es decir, sin garantizar la QoS (Quality of Service). El DCF es la única modalidad prevista por las redes IBSS y por todas las redes privadas de un control centralizado (como por ejemplo la red wireless ad-hoc). Se utiliza en el intervalo temporal CP (*Contention Period*) y proporciona un método que consiente a las estaciones de acceder en modo justo (fair) al canal.

Se ha dicho ya que cada estación con intención de transmitir una MSDU debe participar en la disputa por el canal, también para las que deben retransmitir, y que la modalidad DCF se basa en el CSMA/CA, donde la operación fundamental a completar es el carrier-sense. En el estándar IEEE 802.11 viene definida las dos modalidades de la

comprobación del canal: una clase a nivel físico (*physical carrier sensing*) y otra en el subnivel MAC (*virtual carrier sensing*) [1] [5].

El physical carrier sensing advierte de la presencia de otros usuarios IEEE 802.11 analizando los paquetes recibidos mediante la interfaz. A su vez, sondea el nivel de energía sobre la frecuencia radio para determinar si hay o no una transmisión en curso, proporcionando esta información al nivel MAC [10].

En el virtual carrier sensing, a nivel MAC, todas las estaciones presentes en la BSS escuchan las tramas que transitan sobre el canal y extraen de la trama el campo Duration/ID (a menos que no se trate de una trama transmitida durante el CFP, en el cual el campo Duration es puesto a 32768, o de tramas con Subtype igual a Power Save-Poll). Este campo contiene una información muy importante: el intervalo de tiempo en microsegundos, que una estación en espera de adjudicarse el canal debe atender antes de iniciar a sondearlo. Las estaciones vienen, por tanto, informadas sobre cuanto durará la transmisión en curso en el caso en que venga correctamente, del tal modo que no se compruebe inútilmente el canal. Estas, además, actualizan con la información adquirida un contador interno llamado NAV (Network Allocation Vector), que se decrementa hasta alcanzar el valor 0 cuando la transmisión correcta viene terminada. Se podrá reanudar a comprobar el canal cuando tanto el physical como el virtual carrier sensing indiquen que el canal esté libre. El virtual carrier sensing es, en cambio, una operación de percepción efectuada a un nivel más alto al precedente. Recapitulando las modalidades de acceso al canal según la DCF, se debe proceder como sigue:



**Figura 2.15:** Ejemplo de transmisión de una trama DATA y del relativo ACK.

Una estación que tuviese la necesidad de transmitir una trama, debe primero controlar que el medio no esté ocupado efectuando una medida de potencia de la señal presente en el canal (physical carrier sensing). Cuando esta condición viene verificada, la estación continúa para efectuar un control mediante un DIFS (o un EIFS); al término de este transcurso sucedido con éxito, la estación inicia la transmisión de los datos siguiendo el procedimiento mostrado en la figura 2.15. Si el canal, en cambio, resulta ocupado, se efectúa el virtual carrier sensing y se espera al reseteo del NAV para sondear de nuevo el canal. Suponiendo que el canal resulte libre por un tiempo DIFS, viene puesta en marcha el backoff [cfr. par. 2.4.2.3].

Viene pues generado el número casual del backoff time y después de haber sentido el canal libre por un DIFS (o un EIFS) se empieza a decrementar el backoff timer. Cuando este contador llegue a cero, la transmisión puede finalmente llevarse a cabo. La estación destinataria controla a su vez que los datos recibidos sean correctos según el algoritmo CRC y, por último, un SIFS restituye una trama ACK de confirmación.

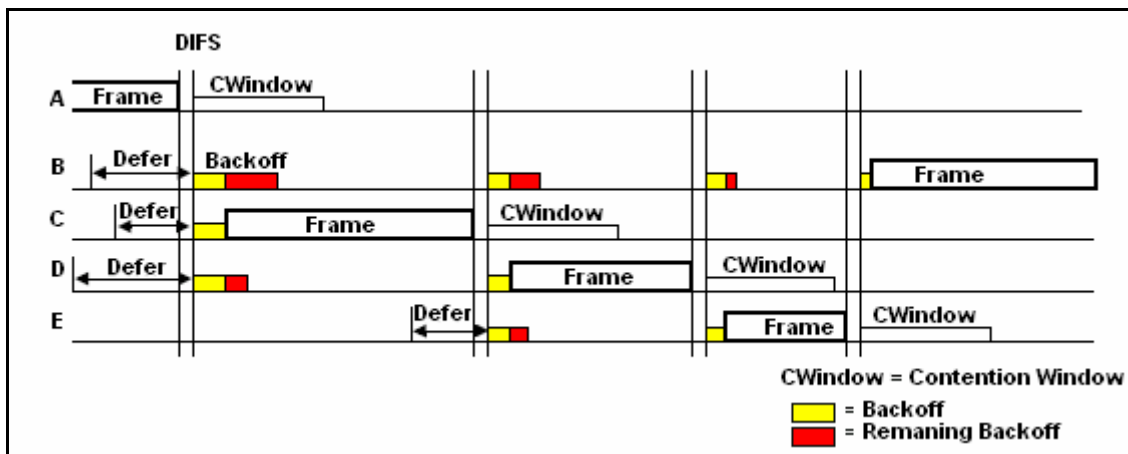


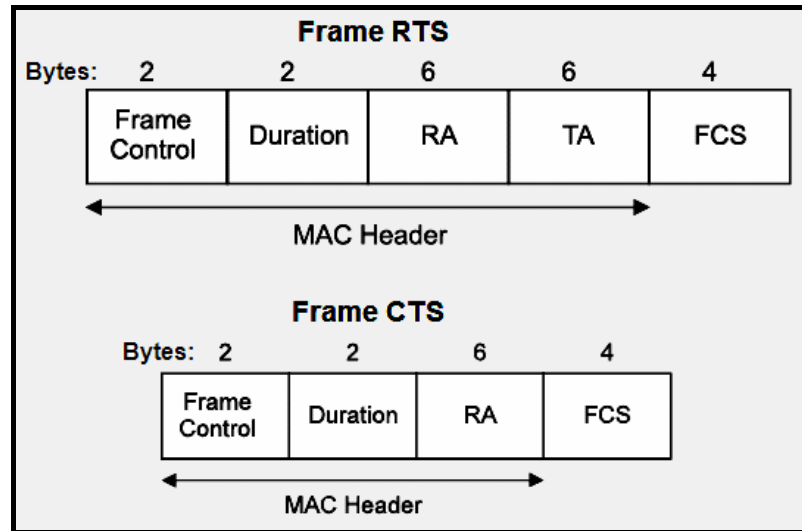
Figura 2.16: Ejemplo de aplicación del procedimiento de backoff.

#### 2.4.2.5 Las tramas RTS y CTS

El problema del terminal oculto [cfr. par. 2.4.2.1] es de fundamental importancia en las redes inalámbricas: el nodo oculto, puesto que se encuentra en proximidad a la estación que está recibiendo una trama y bastante lejano de aquella que lo está transmitiendo, no puede leer el campo Duration/ID transmitido en la trama, por lo tanto,

no actualiza su NAV. En este caso el mecanismo de virtual carrier sensing no tiene efecto y se verifica una colisión.

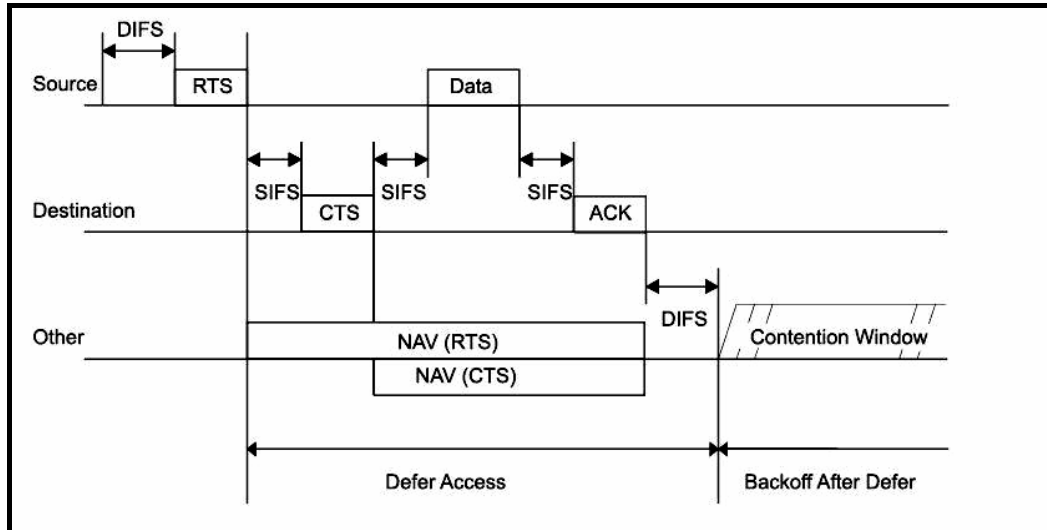
Para buscar limitar tal problema, el protocolo IEEE 802.11 puede utilizar una breve trama de control *petición de envío* (RTS, *Request To Send*) y una breve trama de *vía libre para el envío* (CTS, *Clear To Send*) para *reservar* el acceso al canal [10]. En la figura 2.17 se muestra el formato de las dos tramas:



**Figura 2.17:** Formato de las tramas RTS y CTS.

El mecanismo prevé que la estación, antes de transmitir la trama de datos, envíe al receptor la trama de control RTS, especificando en el campo Duration el tiempo total necesario para la transmisión de la trama de datos y del relativo frame ACK. El destinatario responde después de un SIFS con otra trama de control CTS, en el cual copia el campo de duración. Tal información consiente a todos los nodos que ven el intercambio de los dos paquetes de actualizar el NAV. Los nodos que ven solo el CTS (eventuales nodos escondidos), actualizan el NAV en un momento sucesivo respecto a aquellos que ven el RTS, como mostrado en la figura 2.18.





**Figura 2.18:** Ejemplo de utilización de las tramas RTS y CTS.

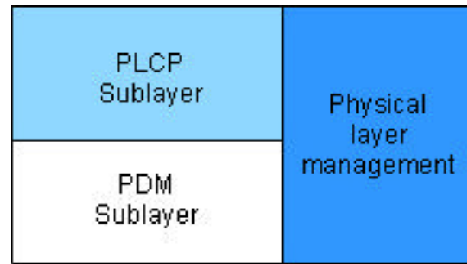
Ya que tanto el CTS como el ACK vienen enviados después de un intervalo SIFS, más breve respecto a un DIFS, estas tramas adquieren indirectamente una prioridad más alta respecto a otras tramas en el acceso al medio. Además, las colisiones debidas a la estación oculta son reducidas al intervalo de transmisión del RTS más un SIFS.

Debido al anterior *overhead* introducido, el intercambio de RTS/CTS no está siempre justificado, especialmente para tramas de datos de pequeñas dimensiones, mientras se considera ventajoso para paquetes más largos de un cierto valor umbral (*RTSThreshold*).

## 2.5 El nivel físico para el 802.11

El nivel físico [4], cuya estructura lógica viene reportada en la figura 2.19, se ocupa de efectuar las siguientes operaciones:

- Determinación del estado del canal (Carrier Sense);
- Transmisión de los datos sobre el canal;
- Recepción de los datos del canal.



**Figura 2.19:** Estructura lógica del nivel PHY

Describimos, por tanto, la estructura lógica reportada en la figura 2.19:

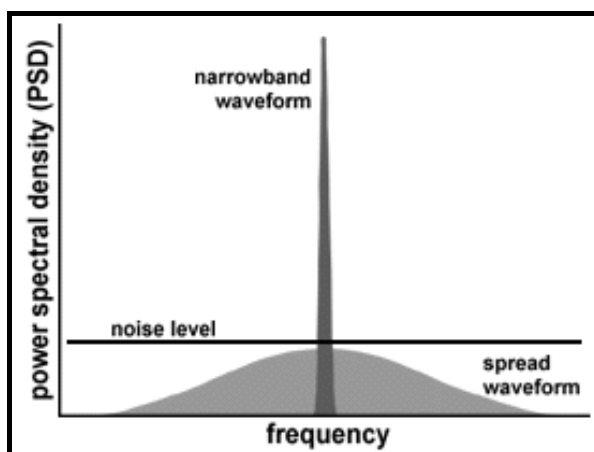
- El *Physical Layer Management* tiene la tarea de administrar el *PLCP Sublayer* y el *PDM Sublayer* haciendo de interfaz con el nivel MAC;
- El *PLCP Sublayer* convierte los paquetes provenientes del nivel MAC en PPDU (PLCP Protocol Data Unit). Esto mediante la agregación de un PLCP preamble y un PLCP header;
- El *PDM Sublayer* es el transductor hacia el canal. Este convierte la información en señal eléctrica, encargándose de la modulación y la demodulación.

En la primera versión del estándar IEEE 802.11 se incluyen tres diferentes implementaciones para el nivel físico [1] [5]: DSSS, FHSS, IR. Las sucesivas extensiones del estándar [6] [7], en cambio, han introducido el OFDM y una versión más veloz del DSSS denominada HR-DSSS (High Rate Direct Sequence Spread Spectrum). Estas representan fundamentalmente diversos tipos de modulación de señal permitiendo diversas frecuencias de transmisión.

1) Las redes basadas en rayos infrarrojos usan la tecnología *IR (InfraRed)*, la cual opera con longitud de onda comprendida en el rango que va de 850nm a 950nm. Esta está limitada a las instalaciones de redes en ambientes delimitados dados que los rayos infrarrojos no se propagan a través de objetos opacos (como las paredes). Sin embargo presenta la ventaja de no generar interferencia.

Las ondas de radio proporcionan la conectividad incluso en condiciones de no visibilidad. Las redes wireless basadas en ondas de radio utilizan las técnicas de modulación *SS (Spread Spectrum)*, las cuales distribuyen la potencia sobre una vasta

banda de frecuencia (figura 2.20) [1], de manera que la señal sea menos susceptible a la interferencia de lo que es con las convencionales técnicas de modulación radio. En otras palabras, a mayor banda consumida la señal obtenida es, por tanto, más simple de observar con el simple hecho de que el receptor conozca los parámetros spread spectrum empleados por el transmisor. Si el receptor no está sintonizado a la justa frecuencia, la señal se asimila al ruido.



**Figura 2.20:** Spread Spectrum (SS).

Existen dos tipos de tecnologías SS: *FHSS* (*Frequency Hopping Spread Spectrum*) y *DSSS* (*Direct Sequence Spread Spectrum*).

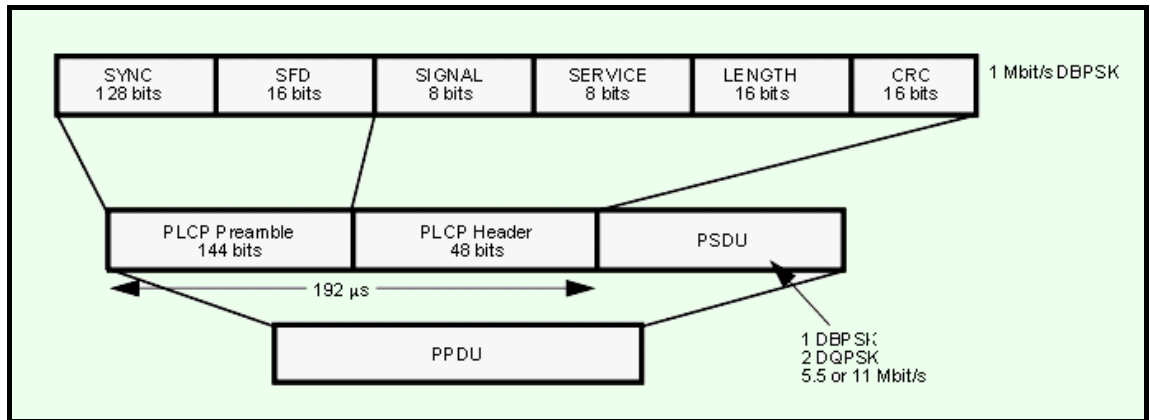
2) Los sistemas *FHSS* [14], durante el la transferencia de señales, “saltan” de una frecuencia a otra: realmente las estaciones transmiten uno o más paquetes de datos utilizando un transporte, después pasan a otra frecuencia y envían una o más tramas de datos y prosiguen de esta manera alternando un salto y una transmisión. El tiempo de permanencia en cada frecuencia está fijado y no puede superar los 400ms, pero la secuencia de los saltos es pseudocasual y advierte tanto al transmisor como al receptor. Los saltos de un canal a otro deben sucederse a una velocidad mínima de 2.5 saltos/seg. y deben estar distanciados en frecuencia al menos de 6MHz. La modulación prevista por el 802.11 es la *GFSK* (*Gaussian Frequency Shift Keying*) y las tasas de bits alcanzables con esta tecnología son 1Mbps y 2Mbps [1].

3) El *DSSS* [14] es una tecnología de transmisión a “frecuencia directa” a banda ancha: los bits informativos a transmitir están relacionados con una secuencia redundante de bit llamada “chipping code”, de tal manera que sea probable recuperar los

datos originales, incluso en la hipótesis de bit dañados, sin tener que recurrir a retransmisiones. El tipo de modulación depende de la velocidad de transmisión: para tasa de bit de 1Mbps se utiliza la modulación *DBPSK* (*Differential Binary Phase Shift Keying*), en la cual cada símbolo está compuesto por un solo bit; para tasa de bit de 2Mbps se utiliza, en cambio, la modulación *DQPSK* (*Differential Quadrature Phase Shift Keying*), que asocia a cada símbolo dos bits [1].

4) En el estándar IEEE 802.11b [6] viene introducido un nuevo tipo de modulación DSSS, *High Rate DSSS (HR-DSSS)* [14]. Mediante esto es posible aumentar el rendimiento de la fuente, permitiendo de tal manera, una transmisión a 1Mbps, 2Mbps, 5.5Mbps y 11Mbps. El throughput (cantidad de datos por segundo que se pueden transmitir) a 5.5 y 11Mbps se obtienen mediante la implementación de una codificación de tipo CCK (*Complementary Code Keying*), manteniendo, en cambio, para las frecuencias más bajas (1 y 2Mbps) los códigos normales del estándar original. Para la transmisión a 5.5Mbps vienen codificados símbolos de 4 bit, mientras que para las transmisiones a 11Mbps se codifican símbolos compuestos de 8 bit [1].

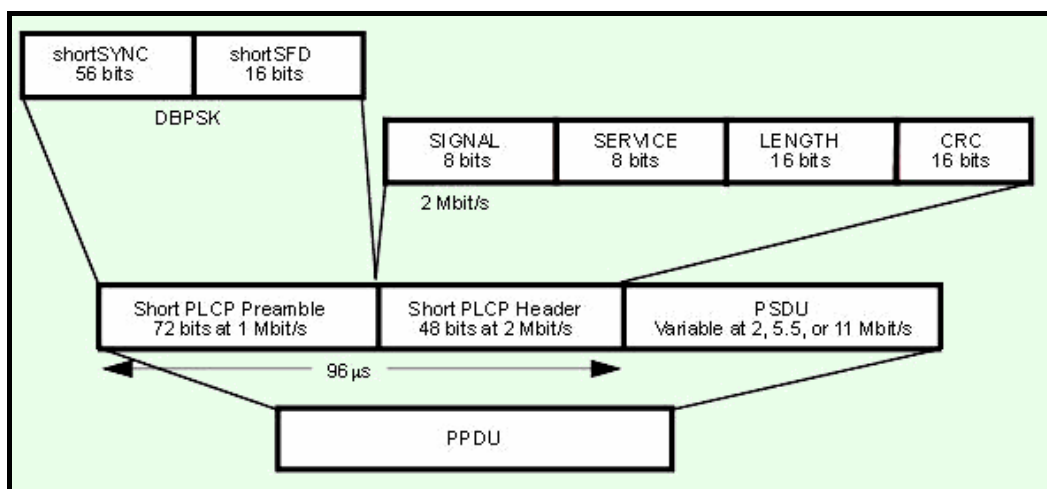
El estándar 802.11b ha definido dos formatos de PPDU [6]: una que recalca la definición dada por el 802.11, que por tanto hace posible la compatibilidad entre las dos versiones, y otra que busca optimizar las prestaciones y hace uso del Short PLCP. Nos referimos al primero con el nombre de formato de PPDU con Long PLCP y al segundo como formato del PPDU con Short PLCP. El formato que adopta el Long PLCP, sustancialmente igual al de la figura 2.21, viene repropuesto con las indicaciones de la duración del preámbulo y de los encabezamientos PLCP en la figura 2.22. Esto representa el formato PLCP que debe ser obligatoriamente soportado en cuanto que consiente la interoperabilidad con las especificaciones de la modulación DSSS a 1Mbps y a 2Mbps.



**Figura 2.21:** Formato de una PDU que usa el Long PLCP.

Como se puede ver en la figura 2.21, se necesitan siempre 192µs para transmitir el preámbulo y el encabezamiento PLCP mientras el PSDU puede ser transmitido a una de las velocidades consentidas. De todo lo dicho se evidencia que llega con transmitir a una tasa de bit de 1Mbps o 2Mbps para mantener la compatibilidad con las estaciones que adoptan el estándar 802.11 clásico [6].

En el formato que adopta el Short PLCP se ha reducida la longitud del preámbulo PLCP de 144 bit a 72 bit mientras permanece inalterada a 48 bit la longitud de la cabecera PLCP (figura 2.22).



**Figura 2.22:** Formato de una PDU que usa el Short PLCP.

El tiempo de transmisión del Short PLCP Preamble más el Short PLCP Header llega a 96 $\mu$ s que, respecto a los 192 $\mu$ s de la versión con Long PLCP, permite ahorrar otros 96 $\mu$ s por cada trama transmitida. Todo esto es obtenido gracias al uso del campo shortSYNC que es constituido por 56 bit en lugar de los 128 bit que usa el campo SYNC y a la transmisión del Short PLCP Header a 2Mbps y no a 1Mbps [6].

Es necesario precisar que este formato de PPDU es definido por el estándar 802.11b como opcional y observamos también que su implementación requiere que todas las estaciones tengan un *basic set rate* (grupo de velocidades que las estaciones pueden usar para recibir la trama) de, al menos, 2Mbps.

Si se usa tanto el Long PLCP como el Short PLCP, desde el punto de vista de la semántica de los campos, en el 802.11b no cambia nada respecto al 802.11, excepto por el hecho que ahora se usan 3 bits del campo SERVICE que antes estaban reservados. Estos bits tiene fines particulares entre los cuales podemos indicar: si el reloj del transmisor y aquel extraído de los símbolos transmitidos provienen del mismo oscilador, se redondea más o menos el valor del *length* (cuando se usa una velocidad superior a los 8Mbps) y la elección de la modulación a usar.

5) En el estándar 802.11a [7] viene introducida como técnica de modulación la OFDM (*Orthogonal Frequency Division Multiplexing*) [14]. Mediante esta técnica se obtienen diversos *throughput* (6, 9, 12, 18, 24, 36, 48, 54Mbps) transmitiendo en la banda de los 5GHz. El OFDM efectúa una separación de datos en transmisión generando dos cadenas. Estas contienen separadamente datos a una alta tasa de bit y a una baja tasa de bit. Para generar su suma se implementa en la fase de transmisión, la IFFT (Inverse Fast Fourier Transform), mientras que en fase de recepción se hace uso de la FFT (Fast Fourier Transform). Para evitar que se creen interferencias intersimbólicas, se introduce el Guard Time, intervalo en el cual el símbolo OFDM permanece periódico. Manteniendo una diferencia de un número entero de periodos al interno del periodo de integración de la FFT, se asegura la ortogonalidad entre ellos. La ortogonalidad derriba el problema de la interferencia intersimbólica, mientras, siendo la señal útil subdividida en más frecuencias, resulta más estable contra eventuales fenómenos de *multipath fading* (desvanecimientos multicaminos).

## 2.6 Otros estándares de las redes wireless

Paralelamente al estándar 802.11 se han desarrollado otros estándares menos conocidos pero que existen en el comercio y en proyectos como testimonio del éxito y la gran atención puestos hacia esta tecnología.

Los principales son [1]:

- Bluetooth
- HomeRF
- Hiperlan 1 e Hiperlan 2

### 2.6.1 Bluetooth

La tecnología *bluetooth* fue aprobada en el 1998 por Bluetooth SIG (Special Interest Group) [15], o sea, un consorcio de empresas y constructoras unidas al objetivo de desarrollar un estándar para la interconexión vía radio. Surgida para obviar los problemas de falta de compatibilidad entre periféricos digitales, usa potencias mas bajas respecto a los otros estándares, definiendo en realidad una PAM (Personal Area Network), es decir, un subconjunto de WLAN mas grandes. Todos los equipamientos Bluetooth predispuestos en un ambiente de trabajo están en condición de generar pequeñas redes de trabajo sin cables. De forma distinta a una LAN, los dispositivos interconectados no se limitan a los ordenadores sino que también comprenden dispositivos electrónicos como teléfonos móviles, auriculares, proyectores, escáner, videocámaras, cámaras de fotos, etc. Esta tecnología permite “comunicar” dispositivos hasta un número máximo de 16, atravesando ondas radioreceptoras a bajos radios emitidos por algunos transmisores presentes al interno de los equipamientos en la banda de frecuencia ISM (2.45Ghz – 2.56Ghz) con modulación FHSS (Frequency Hopping Spread Spectrum) o con GFSK (Gaussian Frequency Shift Keying) [1]. La velocidad máxima de transferencias de datos es igual a 1Mbps fullduplex con una cobertura de los 10 a los 100 metros.



### 2.6.2 HomeRF

Finalmente está el SWAP (Shared Wireless Application Protocol) creado por HomeRF Working Group [1] para la transmisión de datos en radiofrecuencia de dispositivos domésticos con una frecuencia de 2.4Ghz y una tasa de bits igual a 1.6Mbps. La *HomeRF* deriva de la integración entre la tecnología DECT (Digital Enhanced Cordless Telephony) y la LAN wireless. En ellos se utiliza el estándar IEEE 802.11 para los datos y la DECT para la voz. Soporta un protocolo de tipo TDMA (Time Division Multiple Access) para administrar voz y otros servicios críticos, y emplea una técnica del tipo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para garantizar una elevada tasa de datos. Su evolución 2.0 consentirá una tasa de datos de hasta 10Mbps y una transmisión datos/voz con un rango de 50 metros en modalidad *peer-to-peer* o *access point* [1].



### 2.6.3 Hiperlan 1 e Hiperlan 2

La ETSI-BRAN (European Telecommunications Standards Institute-Broadband Radio Access Network) ha intentado seguir las iniciativas estadounidenses al frente de las wireless LAN proponiendo dos soluciones propias denominadas Hiperlan (High Performance Radio Local Area Network), hasta ahora con escaso éxito [16] [17].



Hiperlan 1 es el nombre de un proyecto seguido por la ETSI en el 1992 para explotar la tecnología GSM en el mundo de las WLAN. Teóricamente alcanza una velocidad de 23.5Mbps a la frecuencia de 5Ghz, que en toda Europa ha estado reservado para esta finalidad. No existen productos comerciales y el proyecto está sustancialmente abortado.

Hiperlan 2 es una profunda revisión de la versión precedente y constituye la respuesta de la ETSI al 802.11a. Utiliza la gama de los 5Ghz para transmitir 54 Mbps. Aunque tampoco existen por ahora productos comerciales para esta tecnología.