Wireless lans – IEEE 802.11

Unidad 2.1

Contents

[Funcionamiento básico 2](#_Toc115625337)

[Modelo OSI 3](#_Toc115625338)

[Bandas de operación (2.4 y 5GHz) 3](#_Toc115625339)

[CSMA/CA: Control del acceso al medio en wireless 4](#_Toc115625340)

[Qué problema resuelve 5](#_Toc115625341)

[Mecanismos 6](#_Toc115625342)

[DCF (función de control distribuida) 6](#_Toc115625343)

[PCF (función de control puntual) 9](#_Toc115625344)

[Trama wireless 10](#_Toc115625345)

[Frame control 11](#_Toc115625346)

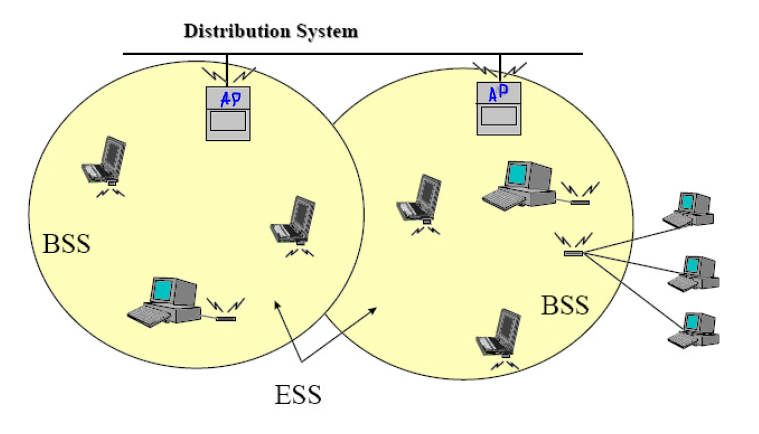
[Fragmentación y reensamblado 12](#_Toc115625347)

[Proceso de asociación a una red wireless 12](#_Toc115625348)

[Protección 13](#_Toc115625349)

[Normas 802.11 (A, B, G, N, AC) 13](#_Toc115625350)

# Funcionamiento básico

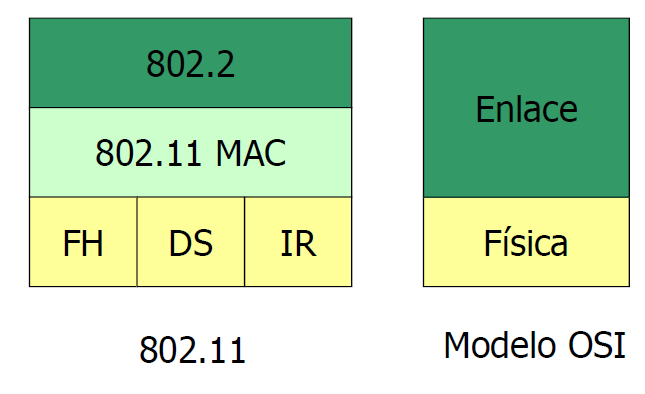


Wireless está definida en la IEEE 802.11.

* El access point (AP) es un dispositivo con una antena que cubre un área determinada llamada BSS (Basic Service Set). El Access Point está enchufado, tiene potencia para transmitir.
* Las terminales remotas se conectan al AP.
* El Access Point da servicio de integración hacia un sistema de distribución (DS – Distribution System). Es decir vincula los dispositivos a un switch conectado a recursos cableados. (usu. una LAN cableada)
* Cuando hay dos o más access point (AP), sus BSS conforman un Extended Service Set (ESS). Aquí cada dispositivo conectado al AP tiene acceso al mismo sistema de distribución.
* Los dispositivos en una red wireless no se comunican entre ellos, sino que se comunican a través del AP.
* Las terminales andan a batería, por lo que tienen que ahorrar energía.

**Redes ad-hoc:** Son aquellas que puedo formar entre por ejemplo dos laptop conectadas de forma wireless. En este caso uno de los dispositivos asume el rol de Access Point (AP). La forma de operación es idéntica al del modo infraestructura.

# Modelo OSI



La **capa de enlace** (capa 2 del modelo OSI) se encuentra dividida en dos subcapas.

* 802.2 🡪 LLC común a LAN y wireless.
* 802.11 MAC 🡪 especifico a inalámbrico

Tres variantes en la **capa física (1)**. Son técnicas de modulación.

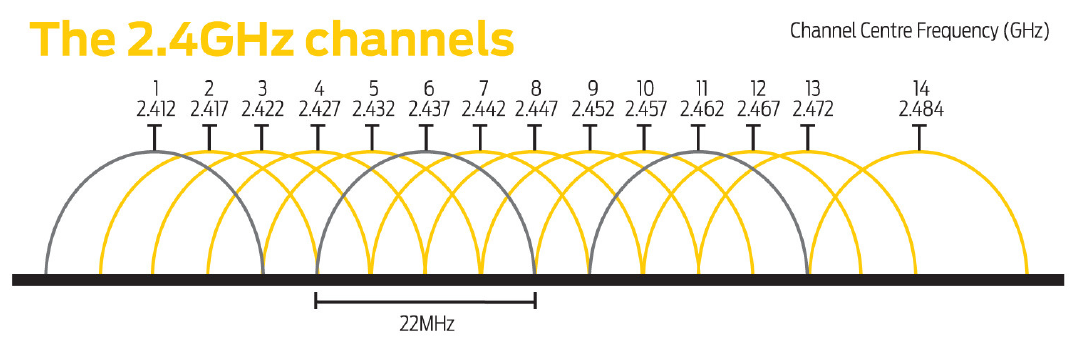
* Infrarrojo (no hay muchas implementaciones para esto, muy limitado)
* DS - Secuencia Directa
* FH - Frequency Hopping / Salto de frecuencia

# Bandas de operación (2.4 y 5GHz)

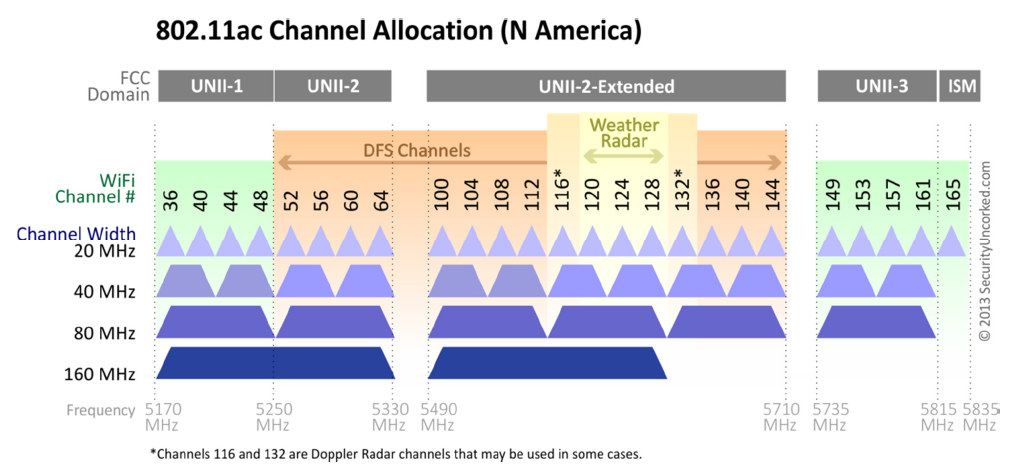
El medio usa el espectro radioeléctrico. Es un medio FINITO por lo tanto, hay que regular dicho espacio radioeléctrico. Se van asignando permisos para transmitir en las distintas bandas.

Para uso hogareño se usan las Bandas  Licenciadas que son de uso público. Están expuestas a interferencias.

|  |  |  |
| --- | --- | --- |
| Bandas | **2.4Ghz** | **5Ghz** |
| Canales | 14 canales de 22Mhz (depende de cada país). | Muchos más (165+) de 20MHz cada uno |
| Solapamiento entre canales | Sí | No |
| Canales que no se solapan | 1, 6 y 11 | Ninguno se solapa entre sí |
| Otros | Para implementar múltiples AP que cubran una misma área, deberá definirse a cada uno en canales diferentes. De lo contrario, van a ocupar el mismo ancho de banda y van a interferirse mutuamente. | Permite hacer backlink. Esto consiste en ir agregando canales (uniendo) de manera de obtener canales de 40Mhz hasta 160Mhz |
| Alcance | Mayor alcance | Menor alcance (porque a mayor frecuencia, hay mayor atenuación) |
| Capacidad / Ancho de banda | Menor | Mayor AB |



**Canales 5GHz:**



# CSMA/CA: Control del acceso al medio en wireless

La capa MAC (Control de Acceso al Medio) en wireless se hace con CSMA/CA.

Acceso múltiple por detección de portadora con evitado de colisiones. Consiste en escuchar durante un periodo de tiempo antes de transmitir. Las implementaciones de este protocolo tratan de evitar las colisiones en todo lo posible.

## Qué problema resuelve

En redes cableadas, se usa CSMA/CD (Carrier Sense Multiple Access / Colision **Detection**)

Pero en entornos wireless, el ancho de banda (AB) es mucho menor y la radiofrecuencia está expuesta a más interferencia.

Por eso se usa: CSMA/CA. (Carrier Sense Multiple Access / Colision **Avoidance**).

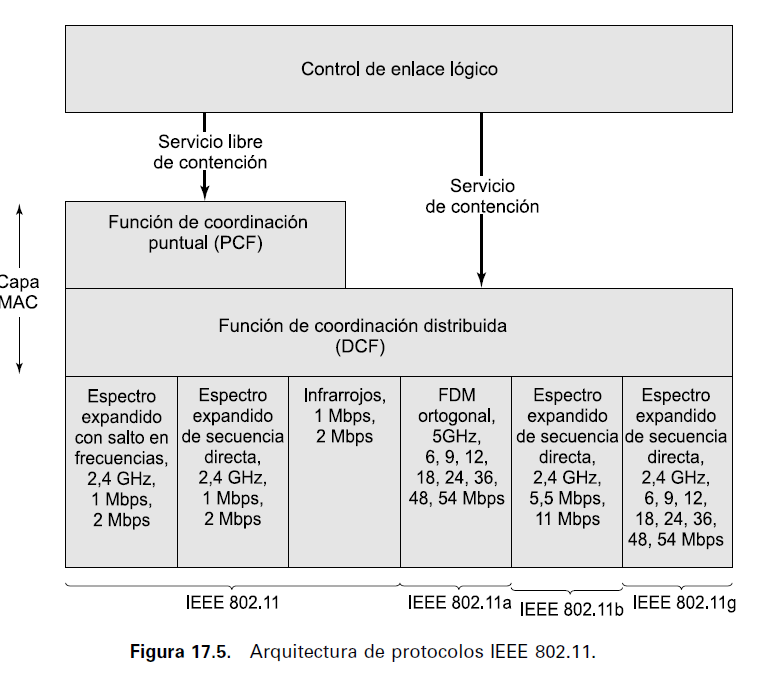
**Problema del nodo oculto:**

En una red wireless, las terminales se conectan directamente al AP. No se escuchan entre sí. Esto podría darse por un impedimento físico (pared) que no les permite escucharse entre sí directamente, pero no es problema mientras puedan escuchar al AP.

Por eso, no es posible que las terminales detecten colisiones, por eso se busca evitarlas.

CSMA/CA resuelve este problema.

## Mecanismos



### DCF (función de control distribuida)

No tiene control central. Cada estación escucha el medio y trata de transmitir.

#### Variante: DCF con RTS/CTS

Siglas: Distributed Coordination Function with Request to Send/Clear to Send

Esta variante sigue existiendo. Se sigue usando cuando la trama a transmitir es muy larga, se reserva el medio.

Hay dos valores a tener en cuenta antes de empezar:

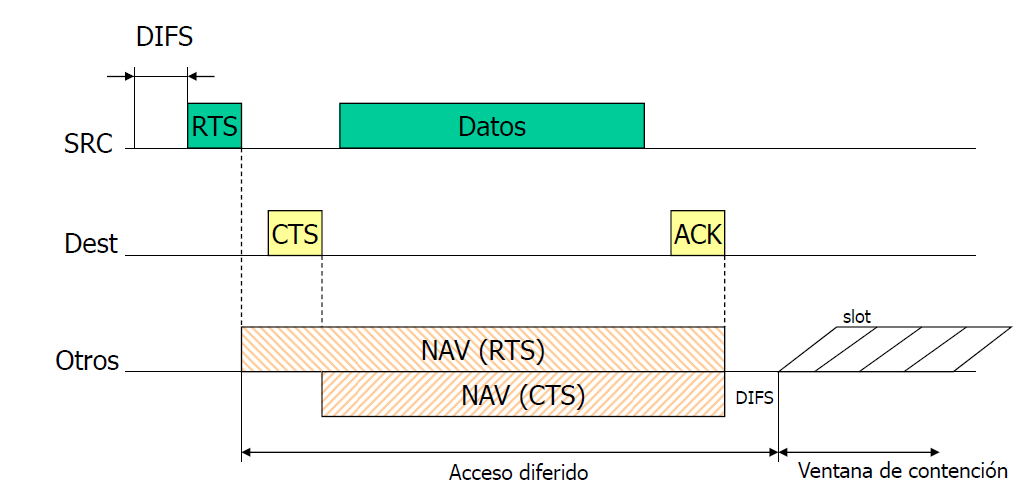
* DIFS (Distributed Inter Frame Space): tiempo determinado que se requiere que el medio haya pasado libre antes de pedir transmitir.
* NAV (Network Allocation Vector): contador de tiempo que indica cuánto falta para terminar una transmisión (de RTS a ACK). Si es 0, el medio está libre.

Para transmitir:

* La terminal se fija si NAV está en 0 (el medio está libre)
* Escucha el medio durante un intervalo de tiempo determinado DIFS (Distributed Inter Frame Space).
* Si el medio está libre, la estación va a transmitir una trama conocida como **RTS** (ready to send) y “reserva el medio”.
* Recibe un **CTS** (clear to send) del AP.
* Transmite los datos.
* El receptor verifica el CRC y enviá un **ACK** (confirmación de recepción de la trama – diferente de redes cableadas!). Si no llega el ACK, se vuelve a intentar la transmisión.

Mientras, las demás terminales conectadas al AP:

* Setean el NAV (Network Allocation Vector).
  + Cuando escuchan el RTS (si lo escuchan), setean el NAV con un valor de tiempo que toman de la trama RTS. El **emisor incluyó en esa trama el intervalo de tiempo que necesita emitir** (recibir el CTS, transmitir los datos, recibir el ACK y x tiempo más tarde libero el medio)
  + Todas van a escuchar el CTS. En el **CTS** el AP le indica cuanto **tiempo le queda al emisor** del tiempo que solicitó en el RTS, y en base a eso setean el NAV.

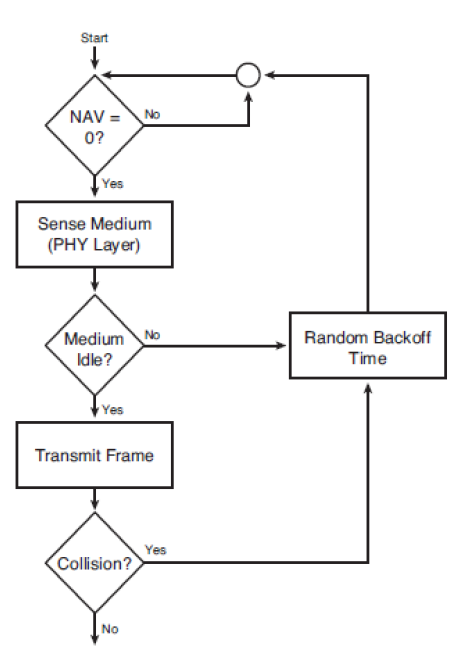


*Línea de tiempo – Dest = AP // SRC = emisor*

Este método con confirmaciones se lo llamo **DCF** (función de control distribuida) **con RTS/CTS**, y se realizaban por el **problema del nodo oculto** (una estación no escucha el RTS, por una interferencia por ejemplo una pared). Luego se dieron cuenta que ese problema no ocurría frecuentemente y que la solución **bajaba mucho la performance**, por lo que pasaron el mecanismo de **RTS/CTS opcional.**

#### Variante: DCF sin RTS/CTS

No hay control central del medio. No reserva el medio cuando empieza a transmitir, sino que transmite cuando el medio está libre.

Una estación que quiere transmitir:

* Se fija si el **NAV** (vector de asignación de red) está en 0. Si no está en cero, significa que alguien está transmitiendo y entonces espera.
* Cuando el NAV llegó a 0, escucha el medio por un intervalo **DIFS** que no haya nadie transmitiendo.
* Después del intervalo DIFS
  + El medio se ocupó: se ejecuta el mecanismo de backoff exponencial (timer random para evitar colisión).
* El medio está libre, **transmite la trama**. Dentro de la trama, el campo Duration/ID indica eltiempo utilizado para calcular el **NAV time**.
* Después de transmitir, podría haber colisión:
  + Si el emisor recibe el **ACK** significa que la transmisión fue hecha correctamente.
  + Si no lo recibe, o reciba un NACK (la trama llegó dañada), en ese caso debo volver a retransmitir luego de un tiempo aleatorio.

El **algoritmo exponencial binario** (**backoff**, tiempo de espera random para volver a transmitir) debe ejecutarse en cada uno de los siguientes casos:

* Cuando escucha el medio y este está ocupado.
* Después de una retransmisión.
* Después de una transmisión exitosa.

### PCF (función de control puntual)

Variación del DCF.

Beneficio: el tiempo de espera para transmitir tiene un límite. Tengo garantizado que me toque. En DCF, una estación sensa el medio sin saber cuándo va a poder transmitir. Acá se le garantiza un momento.

**En PCF el AP va a ir alternando periodos de DCF (distribuido) con periodos de PCF (puntual).**

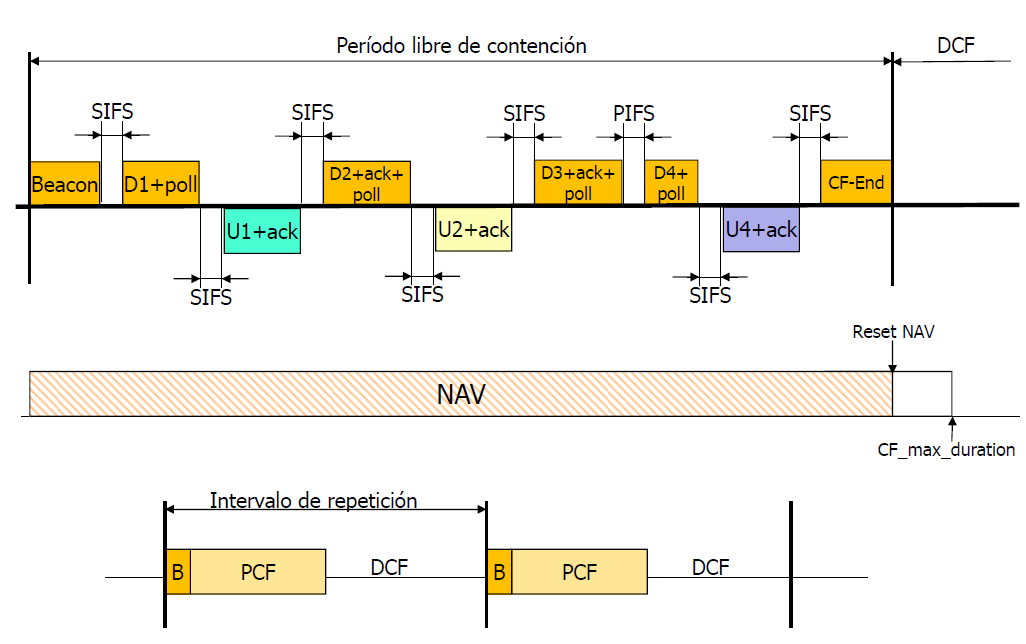
* Durante un intervalo de tiempo el acceso el medio funciona con [DCF](#_Variante:_DCF_sin) (el que puede transmitir transmite, sino espera, etc)
* **Pero durante el período PCF, el AP determina quién transmite**
* Una vez finalizado este periodo, vuelve al periodo DCF y así sucesivamente.

Cómo es un período PCF:

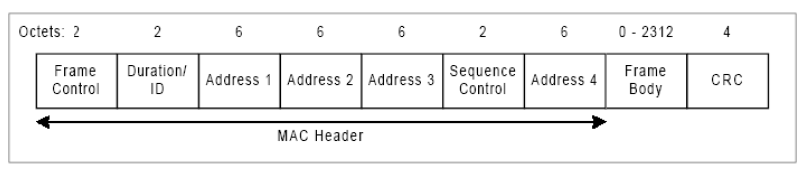
* El beacon anuncia el comienzo de un intervalo PCF. Durante ese intervalo, el AP sondea / hace poll entre los dispositivos asociados, si tienen algo para transmitir.
* Si ante el poll, una estación tiene algo para transmitir (U1 en el ejemplo), transmite. Después el AP vuelve a hacer poll con la siguiente estación. Si un nodo no tiene nada para transmitir, el AP pasa a la siguiente estación.
* Cuando termina el período PCF, se envía un nuevo beacon para indicar que se pasa a DCF.

Intervalos:

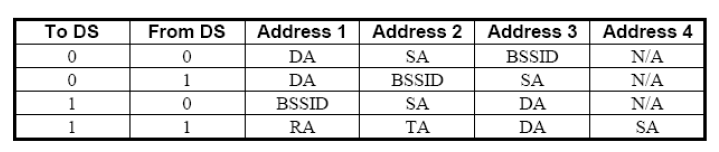
* DIFS: Distributed Inter Frame Space (DCF). En PCF nunca va a haber un periodo DIFS sin transmisión.
* SIFS: Short Interframe Space. Tiempo entre una trama y otra del PCF. SIFS < DIFS (para que nadie empiece a transmitir)
* PIFS: tiempo que espera AP por una transmisión después de un poll. Después pasa al próximo poll.



# Trama wireless



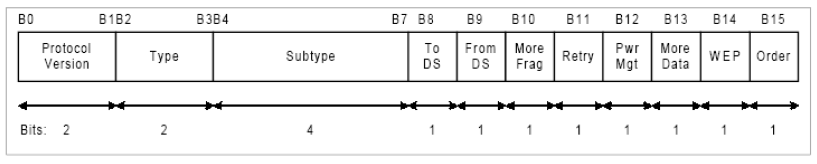
Los campos son:

* [Frame Control](#_Frame_control).
* **Duration/ID:** intervalo de tiempo utilizado para calcular el **NAV time**.
* **Address fields:** son 4 campos, aunque la mayoría de las veces se transmiten sólo 3. Los valores de cada dirección dependen de los valores de los campos ToDS y FromDS en Frame Control (to/from Distributed System, o sea, enviado al AP o por el AP).  
  
  + DA: Destination adress (destino final de la transmisión)
  + SA: Source Addresss (dirección de origen real, la que inicia la transmisión)
  + BSSID: ID del BSS.

Si ToDS = FromDS = 1 (transmisión de un AP a otro):

* + RA: Receiver Address. El dispositivo que va a recibir esa trama
  + TA: Transmitter Address. AP que transmite el mensaje.
* **Sequence Ctrl:** identifica el fragmento.
* **Frame body:** Datos
* **CRC:** 32-bit.

## Frame control



Frame control tiene 2 octetos (16 bits) que se usan para:

* Protocol versión
* Type. Las tramas pueden ser de **tipo/subtipo:**
  + Administración: petición/confirmación de asociación, autenticación, Beacon (mini trama que se envía continuamente).
  + Control: RTS, CTS, ACK (otras asociadas con PCF?).
  + Datos.
* Subtype
* ToDS/FromDS:
  + ToDS: vale 1 cuando la trama se envía al AP (DS es distributed system, refiere la línea que está conectado el AP).
  + FromDS: vale 1 cuando la trama viene de un AP (1 a de un terminal).
  + Combinaciones:
    - From: 0 / To: 0 significa que el host envía autenticación al AP (no pasa al cableado, por ej la contraseña).
    - From: 1 / To: 1 es para por ejemplo, wireless bridge.
* More Fragments (MF): indica que hay más fragmentos pertenecientes a la misma trama.
* Retry: indica que esta trama ya ha sido transmitida. Sirve para descartar duplicados en caso que se pierda el ACK.
* Power Mgmt: Cuando una estación envía una trama con el bit de power management encendido, significa que se está por ir a dormir. Con esa info, el AP acumulará mensajes para esa estación hasta que se despierte. Cuando se despierte, va a enviar el PSPoll (power safe poll) al AP para avisarle que está despierta y que le puede mandar todo.   
  El AP puede pedir que todas estén despiertas en cierto tiempo.  
  El AP está enchufado, pero las estaciones andan a batería. Entonces cada tanto las estaciones apagan el aparato de transmisión para ahorrar energía. Al conectarse con el AP, indican cada cuanto hacen esto, y el AP está enterado de todo. Si tuviera que transmitir un broadcast, tiene que saber cuándo están todas despiertas al mismo tiempo.
* More Data: ídem, el AP indica a la estación que tiene más fragmentos para ella. Sirve para indicarle a la estación que no se duerma porque el AP tiene más datos que enviarle.
* WEP (Wired Equivalent Privacy): Privacidad equivalente al cableado. Indica que el campo de datos está encriptado. Esto ya no se usa, porque hoy en día es fácilmente quebrable por fuerza bruta.

# Fragmentación y reensamblado

La capa de red, en función a la tasa de error (BER, de capa 1), va a ir controlando el tamaño de la trama a transmitir (**cuanto más grande es el BER, más subdividida en fragmentos debe estar la trama para retransmitir el menor tamaño posible**). Se transmite un fragmento a continuación del otro.

En redes cableadas, el BER es ínfimo. En wireless, es mucho más alta.

Para esto se usan los campos More Data y/o More Fragments del Frame Control.

# Proceso de asociación a una red wireless

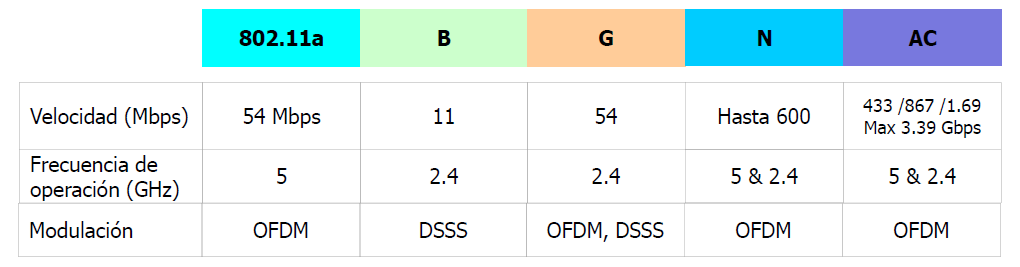
Para incorporarse a una celda, una estación debe completar los siguientes **pasos**:

* **Sincronización:** por medio de los “**Beacon frames**” transmitidos por el AP. El AP envía 10 Beacon frames por segundo.
* **Autenticación:** intercambio de información (**clave**) entre el AP y el terminal.
* **Asociación:** se **vinculan la terminal al AP**. A partir de este momento puede comenzar a transmitir. El AP toma nota del MAC (esto después sería visible si el AP se conecta a una red cableada).

# Protección

Se utiliza el protocolo WEP (wired equivalent privacy) para evitar la intercepción de la información. Y para limitar el acceso de los terminales a un determinado AP.

# Normas 802.11 (A, B, G, N, AC)



Las normas wireless difieren entre sí en: velocidad, frecuencia de operación y modulación.

A operaba en 5GHz, B y G, en 2.4, y N y AC en ambas bandas a la vez.

Velocidad de transmisión: La velocidad real (throughput) es mucho menor

* A: no se usó mucho. SE necesitaba una antena diferente para cada banda. Interoperabilidad entre A y B fue conflictiva.
* G: logra la misma velocidad que A en 2.4, y el AP podía tomar estaciones en B y G a la vez (interoperabilidad).
* N: opera en ambas bandas a la vez.
* AC: opera en ambas a la vez.