WIRELESS LANs: 802.11

Ana Hernández Rabal

Índice

- Introducción
- Topologías WLAN
- IEEE 802.11 Capas
  - Capa física
  - Capa de enlace
- 802.11 Mecanismo de acceso al medio
  - CSMA/CA
  - MACA (Multiple Access CA)
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)
- Formato trama
- Tipos de tramas:
  - Gestión
  - Control
  - Datos

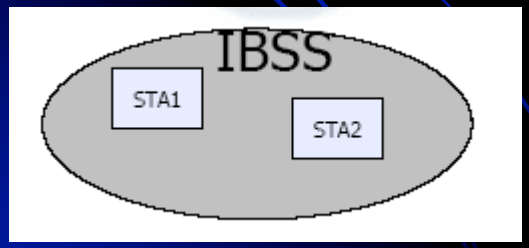
Introducción

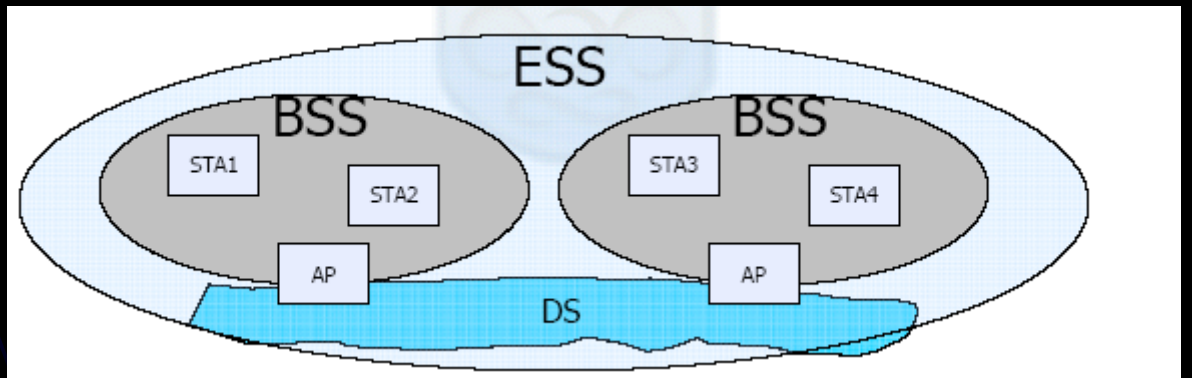
Wireless Local-Area Network

- Ondas de radio de alta frecuencia
- Caracteristicas WLANs:
  - movilidad
  - facilidad de instalación
  - flexibilidad
- Protocolo IEEE 802.11: capas física y de enlace de datos
  - 802.11a:54Mbps y 5GHz
  - 802.11b:11Mbps y 2.4GHz
  - 802.11g:54Mbps y 2.4GHz

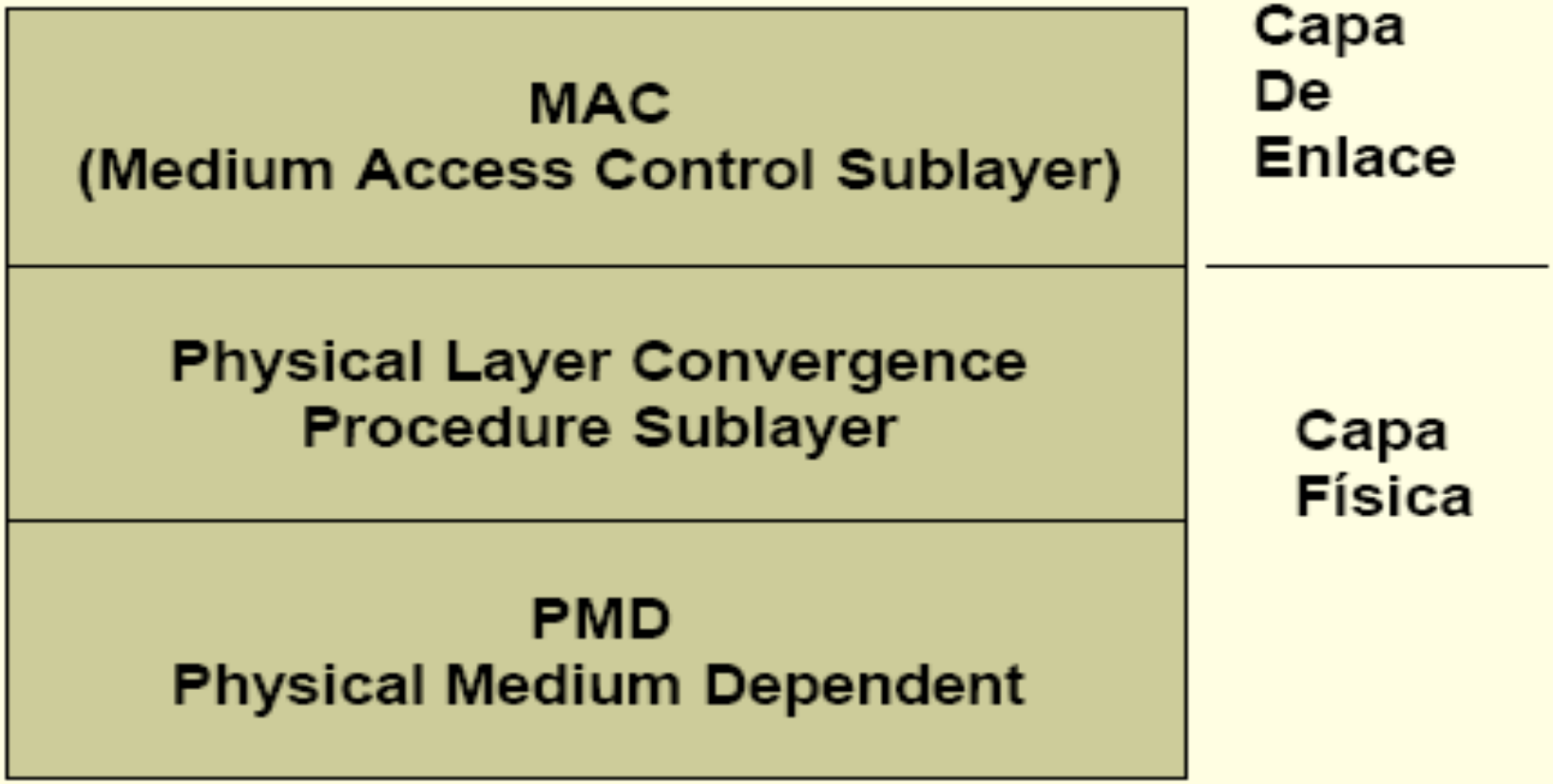
Topologías WLAN

- Independent Basic Service Set (IBSS) (Redes Ad-Hoc)
  - Las estaciones se comunican directamente. Cobertura limitada.
- Basic Service Set o Infraestructura (BSS)
  - Utiliza los AP (punto de acceso) para todas las comunicaciones.
  - Ocupa más capacidad. Todas las estaciones dentro del alcance del AP, pero no hay restricción en la distancia.
  - Los AP saben cuando una estación entra en modo ahorro de energía y almacenan las tramas.
- Extended Service Set o Infraestructura (ESS)
  - Infraestructura de múltiples BBS interconectadas por el sistema de distribución (DS) a través de un AP. Cable, FO, Inalámbrica…





IEEE 802.11 Capas



Capa física

- La capa PHY está dividida en dos subcapas
  - PLCP: Physical layer convergence procedure
    - Trata las tramas de la MAC (MPDU) y las pone en el formato adecuado para la PMD
  - PMD: Physical medium dependent sublayer
    - Define características y métodos tx/rx a través del medio inalámbrico.

Capa física

- Modulación y señalización de la transmisión de datos

Modo	Frecuencia	Velocidad	Modulación
DSSS	2.4 GHz (ISM)	1 Mbps 2 Mbps	DBPSK DQPSK
FHSS	2.4 GHz (ISM)	1 Mbps 2 Mbps (opc.)	2-GFSK 4-GFSK
DFIR	Infrarrojos (850-950 nm)	1 Mbps 2 Mbps (opc.)	PPM

802.11 Mecanismo de acceso al medio

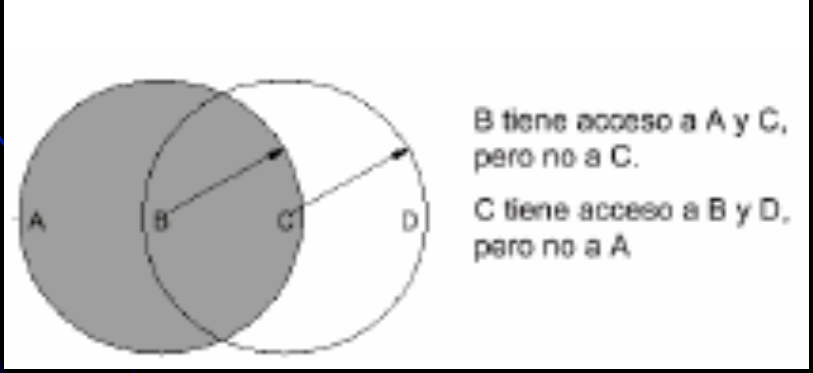
- Funciones Principales de la Capa MAC
  - Soporta dos modos de funcionamiento
    - DCF (Distributed Coordination Function)
      - Obligatoria
      - Ad-hoc e infreatructura
    - PCF (Point Coordination Function)
      - Opcional
      - Infraestructura
  - Gestión de acceso basado en el protocolo CSMA/CA (Carrier Sense Multiple Access / Collison Avoidance)
  - Gestión de movilidad y servicios de red (asociación, re-asociación, etc…)
  - Gestión de potencia
  - Funciones de seguridad (encriptación y autentificación)
  - Segmentación y reensamblado

CSMA/CA

- En redes wireless, no se puede escuchar y transmitir a la vez. No se detectan colisiones, intentar evitarlas.
- Funcionamiento de CSMA/CA:
  - Antes de tx, estación testea el medio (libre/ocupado).
  - Si no está ocupado, espera un tiempo IFS.
  - Si estaba ocupado o lo está en este tiempo, espera hasta que este libre.
  - Finaliza espera por medio ocupado y se ejecuta el algoritmo de Backoff, con una espera aleatoria uniforme en el intervalo de contienda (CW).
  - Se espera reduciendo el Backoff múltiplo de slots times (Al menos IFS). Si llega a cero, tx; Si alguien tx (No IFS) se para descuento.

Problemas CSMA/CA

- Nodos ocultos
  - Estación cree que el canal esta libre pero ocupado por otra que no oye.
- Nodos expuestos
  - Estación cree que el canal esta ocupado, pero esta libre, la estación que oye no le interfería.



Solución MACA (Multiple Access CA)

- Tx y Rx intercambian frames antes de tx.
- Tx envia RTS (Request to Send) con tiempo que ocupará medio.
- El Rx contesta con CTS (Clear to Send), repitiendo tiempo.
- Comportamiento nodos:
  - Al ver RTS, hay que esperar al CTS, y si no llega CTS, puede transmitir.
  - Al ver CTS, esperar longitud.
- La colisión de RTS/CTS se evita con CSMA/CA.

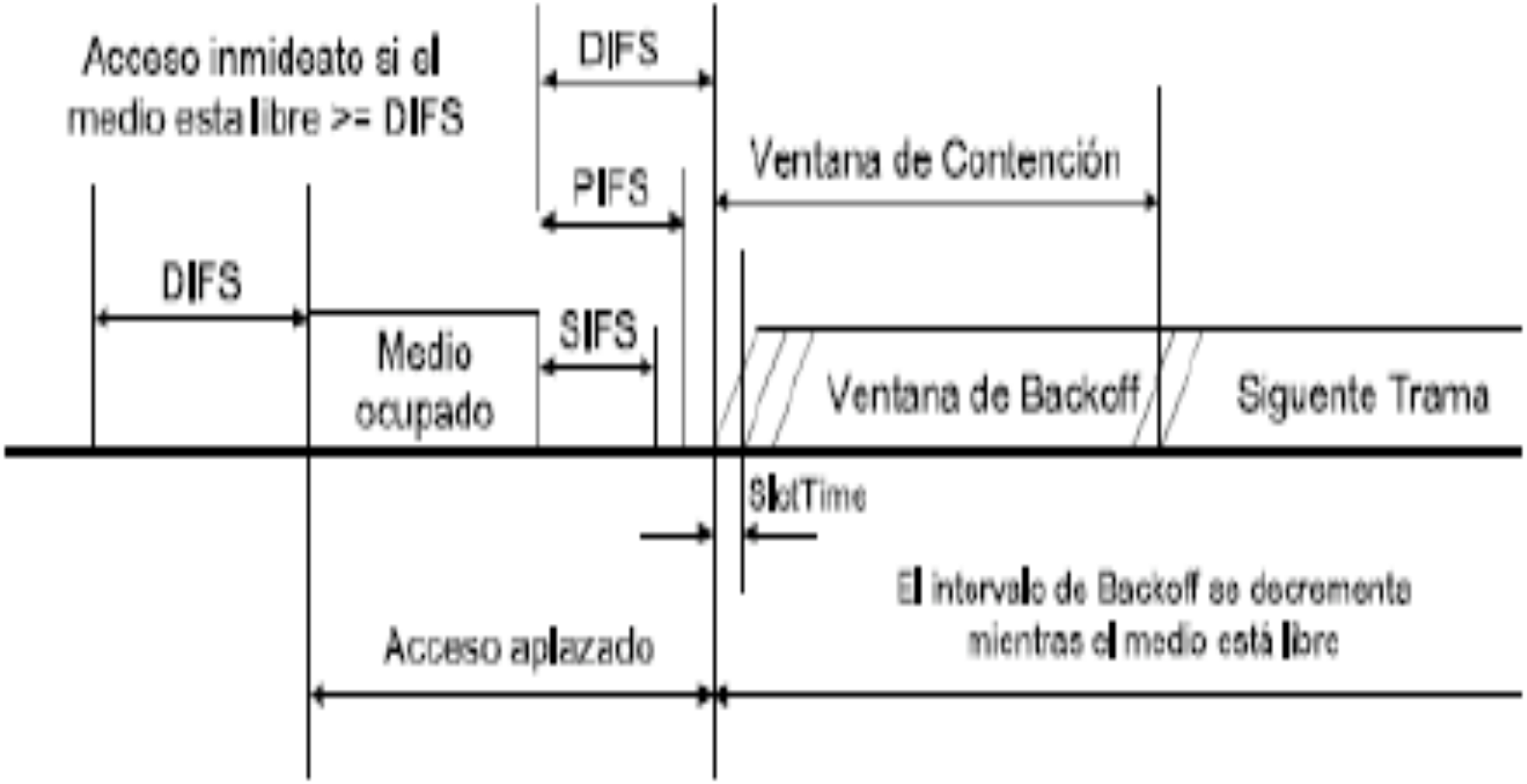
Distributed Coordination Function (DCF)

- Función de coordinación: Determina cuando una estación puede tx/rx.
- Tx asíncrona
- DFC:
  - Utiliza MACA (CSMA/CA con RTS/CTS)
  - Necesario ACKs, provocando retx. si no se recibe
  - Campo duration/ID tiempo reserva t(tx) + ACK
  - Implementa fragmentación de datos
  - Concede prioridad mediante espaciado de tramas (IFS)
  - Soporta Broadcast y Multicast sin ACK

Espaciado entre tramas (1)

- Intervalo entre tramas IFS. Estación escucha durante IFS antes de tx.
- Espacidos según prioridad
  - SIFS (short): Tx ACKs, fragmentos. Usado por el punto de coordinación (PC) para estaciones envíen síncrono.
  - PIFS (PFC): Estaciones para conseguir prioridad en períodos libres de contienda. PC para ganar contienda.
  - DIFS (DFC): Tiempo habitual contiendas MACA.
  - EIFS (Extended):Cuando llega trama errónea.

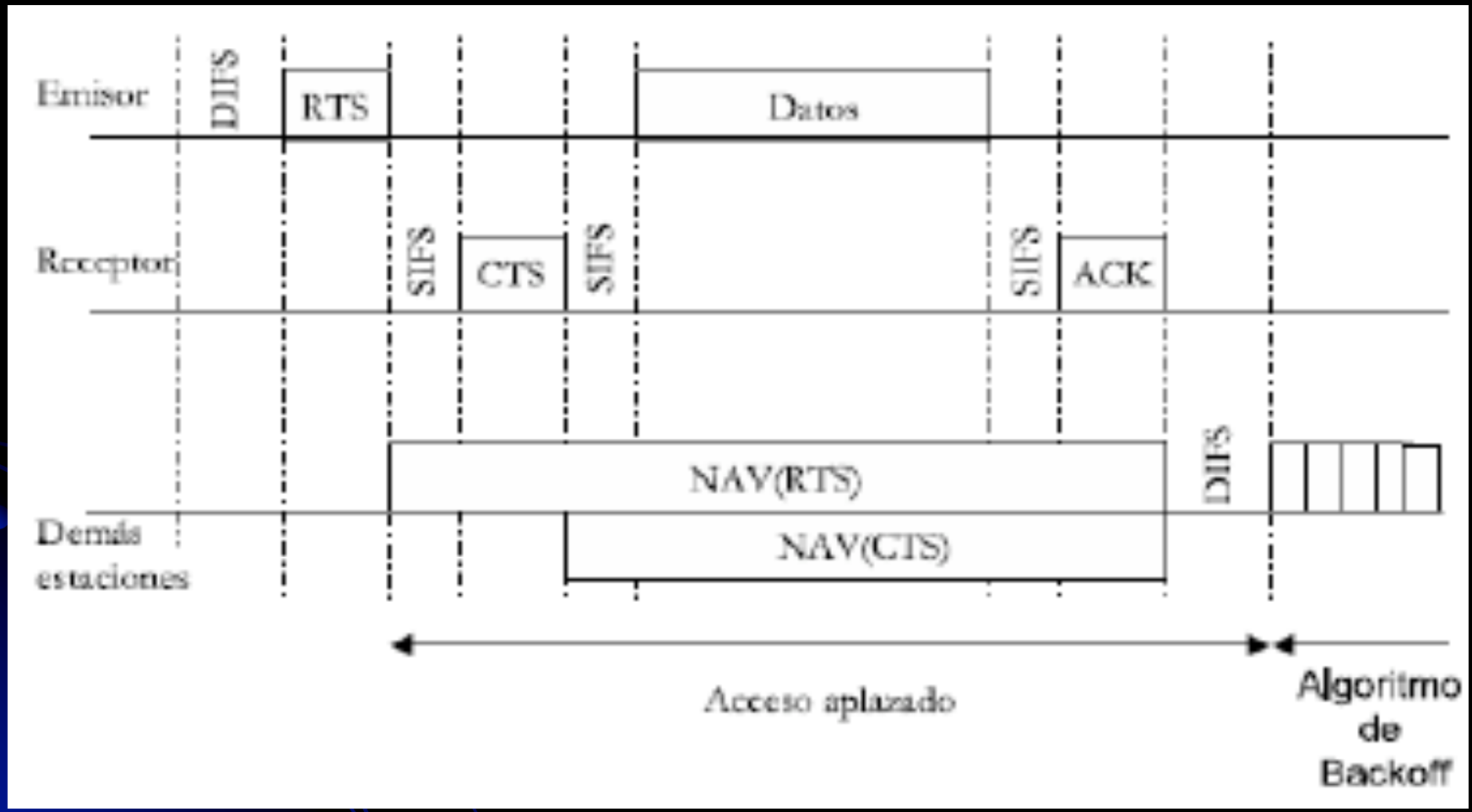
Espaciado entre tramas (2)



Conocimiento del medio (1)

- Cada STA contiene el NAV (Network Allocation Vector) con una predicción de cuando quedará libre el medio.
- A enviar RTS o recibir CTS se envía/recibe la duración.
- Otras estaciones toman Duration/ID si es mayor que su NAV.

Conocimiento del medio (2)



Point Coordination Function (PCF) (1)

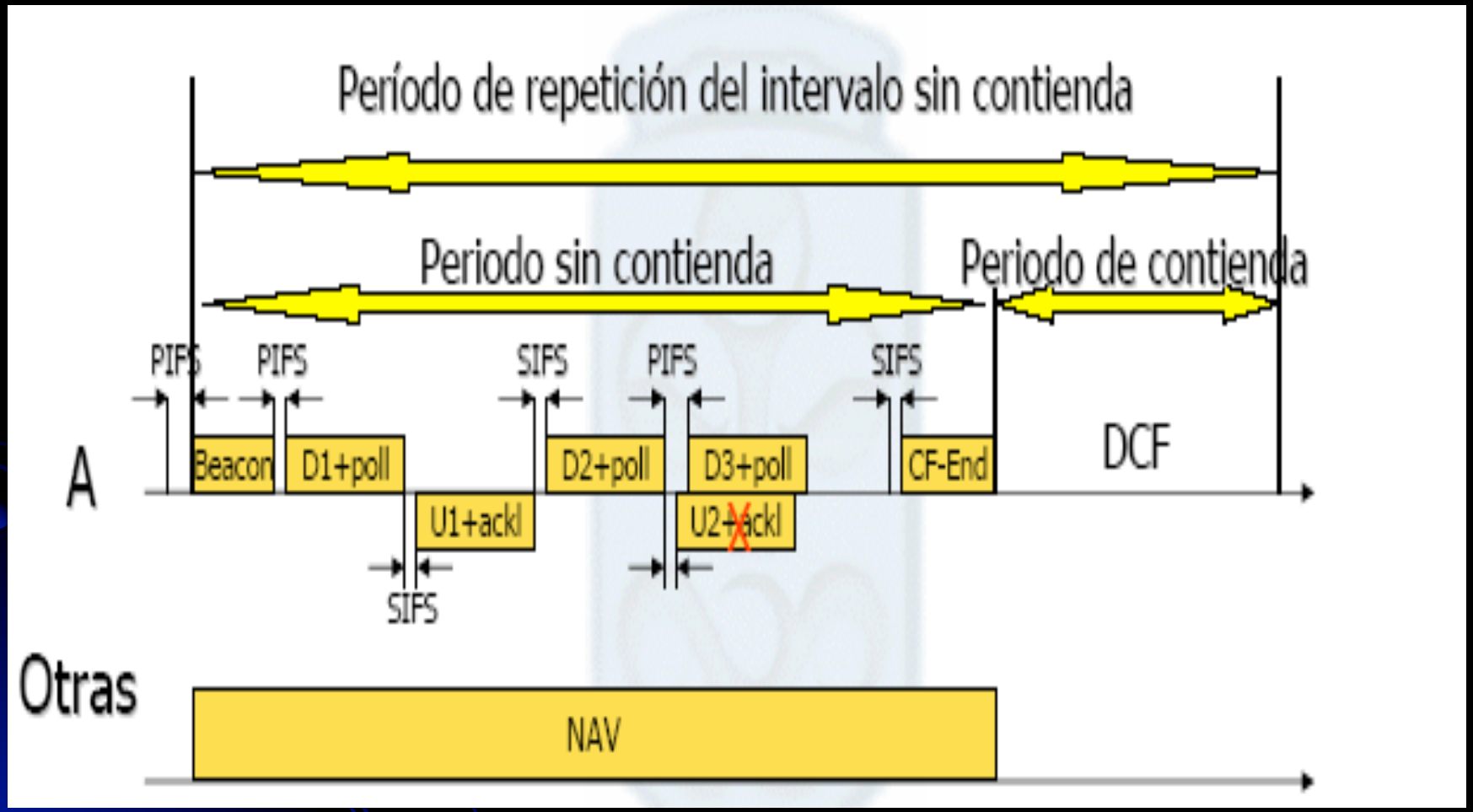
- Transmisiones libres de contienda con técnicas de acceso deterministas.
- Opera junto con DCF: supertrama
  - Una parte asignada al período de contienda: tx aleatoria.
  - Cuando acaba AP toma control, comienza período libre de contienda: tx determinista.
- PFC
  - PC gana el medio puesto que espera PIFS<DIFS
  - Trama Beacon indica duración CFP (Contention Free Period) y elemento DTIM.
  - Estaciones actualizan NAV.
  - Las estaciones pueden usar CFP (CF-Pollable) o situar su NAV al comienzo de la contienda según PC. (Asociación, también decide su inclusión en la Polling list)

Point Coordination Function (PCF) (2)

- El PC toma el control, enviando CF-Poll (puede contener trama datos o ack) a estación que podrá transmitir una trama MPDU: Data, Data+CF-ACK, CF-ACK, Null data.
- Lista estaciones CF-pollable (Polling list).
- CFP termina con trama CF-End
- El PC utilizara trama Beacon con CFRate o tasa de períodos de contienda. Longitud del CFP se puede retrasar, pero mantiene una tasa CFPRate.

- Solapamiento PCs
  - Si varios PC transmiten a CPFRates semejantes, hay riesgo de colisión de CF
  - Usaremos CSMA/CA sobre DIFS+BackOff(1-Cwmin)

Point Coordination Function (PCF) (3)



Sincronización

- Una función de sincronización (TSF) mantiene los relojes de las estaciones sincronizados
- Modo Infraestructura: el AP controla el TSF, enviada a las estaciones en los beacons, que siempre lo aceptarán
- Modo Ad-Hoc: el intervalo de Beacon (TBTT) lo establece la estación.
- La sincronización puede ser activa (Probe Response) o pasiva

Proceso de prueba

- Estación manda **Probe Request** por cada canal que se puede usar (velocidades, topologia…)
- Probe request:
  - SSID element: Identificador de la estación con el ha sido configurado.
  - Support rates element: Velocidades de datos que la estación soporta.
- AP recibe, chequea FCS y replica trama en **Probe Response.**
- Probe response:
  - Timestamping field: Valor TSFTIMER, para sincronizar estación con AP.
  - Beacon interval field: Unidades de tiempo (UT=1024us) entre beacons.
  - Capability information field: Capabilities capas MAC y PHY.
  - SSID element: Identificador que configura el AP.
  - Support rate element: Velocidades de datos que AP soporta.
  - PHY parameter set element: Para secuencia directa y salto en frecuencia da información a nivel físico de la estación.

Autenticación

- Entre estaciones en una red Ad-hoc hoc.
- Entre estación y AP en una red infraestructura.
- Dos mecanismos:
  - Open System:
    - Algoritmo nulo, cualquier estación se puede autentificar enviando una trama (**Authentication**).
  - Shared key:
    - Clave compartida de 40 ó 104 bits.
    - Algoritmo WEP (Wired Equivalent Privacy).
    - No es seguro. Inversible captando cantidad suficiente de tramas.
- Alianza WIFI desarrolló WPA (Wifi Protect Access). Incorpora TKIP (Protocolo Temporal de Intercambio de Claves) más robusto que RC4 de WEP.

Asociación (1)

- Estación envia petición asociación (**Association request**) al AP.
- El AP responde con una trama (**Association response**), indicando las capacidades de la BSS y aisgnándole un identificador de asociación “Assciation ID”.
- La respuesta de asociación será asentida por la estación.
- El AP aceptará la asociación si la estación está previamente autentificada. Si no rechazará, indicando la razón.
- El AP informará al Sistema de Distribución de la asociación de la estación.

Asociación (2)

- Association request:
  - Listen interval: Informa al AP cada cuanto tiempo despertará la estación del Power Save.
  - SSID element: Identificador de la estación para el AP, aceptará o no la trama si lo conoce.
  - Support rates element: Velocidades de datos que la estación soporta.
- Association response:
  - Status code.Codigo de estado resultado de una respuesta de asociación.
  - Association ID: Lo necesita la estación cuando opera en Power Save. El AP lo utiliza para avisar de las tramas almacenadas.
  - Support rate element: Velocidades de datos que AP soporta.

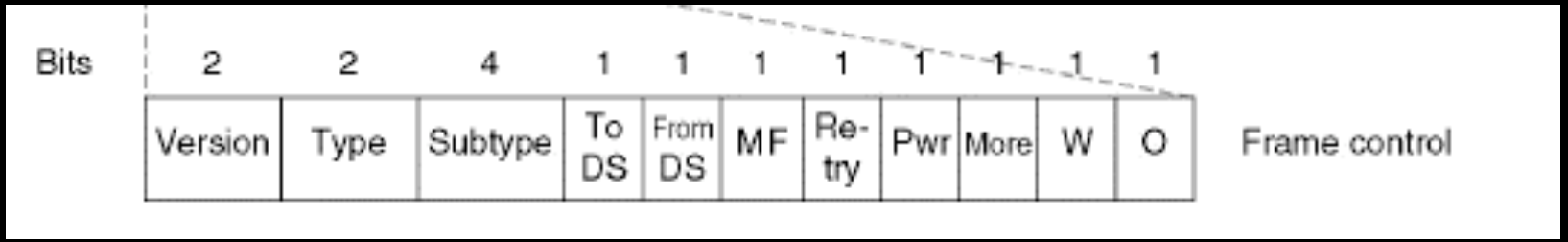
Gestión de potencia

- Redes infraestructura
  - Una estación puede operar en modo Power-Save o Awake (Despierto).
  - El AP no transmitirá tramas de forma normal a las estaciones en modo Power-Save. Las irá almacenando.
  - Dentro de las tramas Beacon se inserta un TIM (mapa de indicación de tráfico), que refleja qué estaciones tienen tramas pendientes en el AP.
  - Las estaciones en modo PS, despertarán periódicamente y escucharán tramas Beacon.
  - La estación enviará al AP una trama PS-Poll cuando sepa que existen tramas pendientes para ella. El AP responde con la trama almacenada.
  - La estación saldrá del modo PS indicándoselo al AP en un bit del campo control de trama de las tramas que envíe.
  - La estación cambiará su estado al recibir respuesta.

Formato trama: Cabecera de control (1)

- **Versión del Protocolo:** Versión MAC 802.11 que se utiliza en el resto de trama. 0 indica la MAC 802.11.
- **Type:** 00= Management, 01=Control, 10=Data, 11=Reserved.
- **Subtype:** Definen el detalle del servicio (Association request y response, reassociation request y response, Beacon, Power Save, RTS, CTS, ACK, CF, etc...).

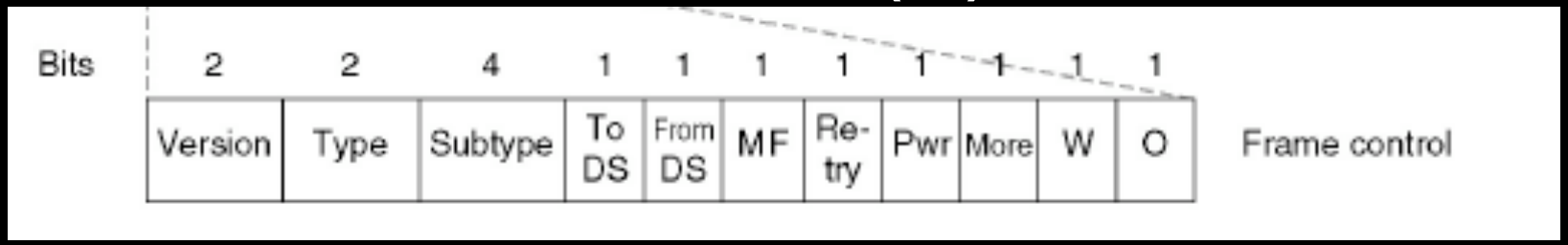
Formato trama: Cabecera de control (2)



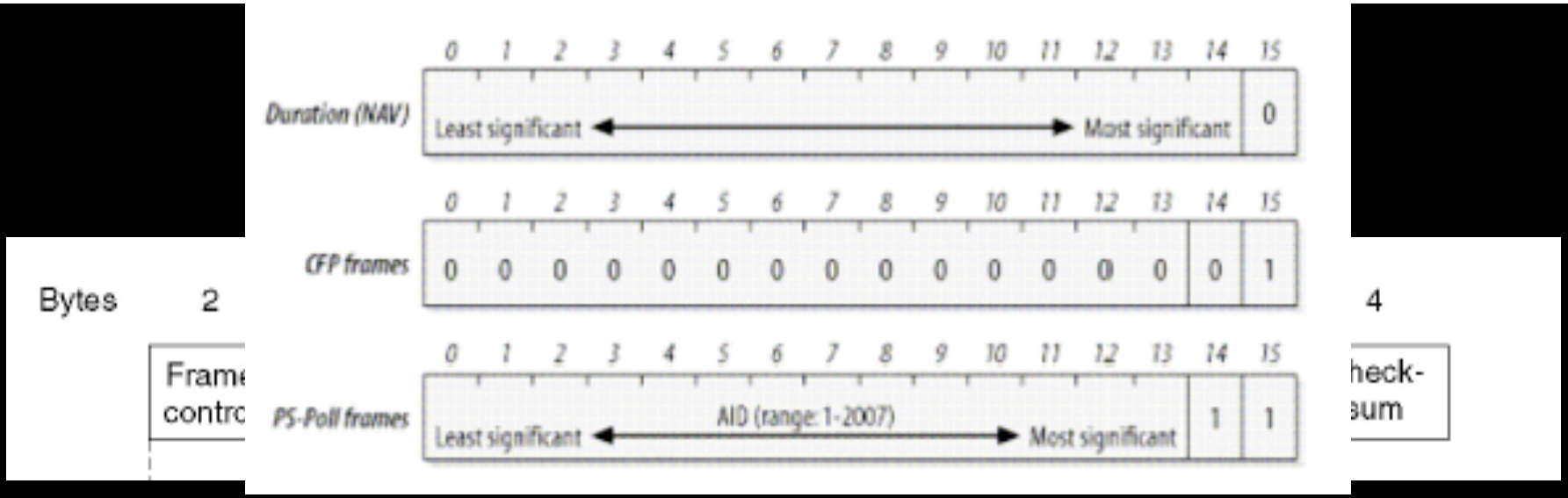
- **BITs de ToDS y FromDS:** Indican si la trama se destina al sistema de distribución. Todas las tramas en modo infraestructura tendrán uno de estos bits a 1

	To DS=0	To DS=1
From DS=0	All management and control frames Data frames within an IBSS (never infrastructure data frames)	Data frames transmitted from a wireless station in an infrastructure network
From DS=1	Data frames received for a wireless station in an infrastructure network	Data frames on a "wireless bridge"

Formato trama: Cabecera de control (3)



- **BITs de Fragmentación:** Trama fragmentada, todos los fragmentos menos el último tiene bit a 1. Trama no fragmentada el bit es 0.
- **BIT de Retransmisión:** 1 para trama retransmitida. Eliminar duplicadas.
- **BIT de Control de Potencia:** 1 la estación está en modo *power-saving*, 0 la estación está activa. Tramas tx por AP, el bit es 0.
- **Más BITs de Datos:** Fijado por el punto de acceso. Hay al menos una trama disponible destinada a una estación no activa.
- **BIT WEP:** 1 indica que la trama ha sido procesada con WEP (*Wired Equivalent Privacy*).
- **Otro BIT:** Procesado adicional en la tx y rx. 1 si utiliza ordenamiento estricto, 0 en otro caso.



- **Frame Control:** indica el tipo de trama: beacon, control, datos o gestión.
- **Duration/Connection ID**
  - **Duración: Fijando el NAV**

Bit 15 a 0. Campo D/I se utiliza para fijar el NAV. Nº de us que el medio permanecerá ocupado durante la tx.

  - **Tramas Transmitidas durante el Período de Contention-Free**

Bit 14 es 0 y el bit 15 es 1. Los demás bits son 0. El campo vale 32,768. Permite recuperar el NAV a estación que no ha recibido el *beacon.*

  - **Tramas PS-Poll**

Bits 14 y 15 a 1 en tramas *PS-Poll*. Las estaciones que se reactivan incorporan un Association Identity (AID) asignado a la estación por la BSS a la cual estaban asociada. Valor oscila entre 1 y 2007.

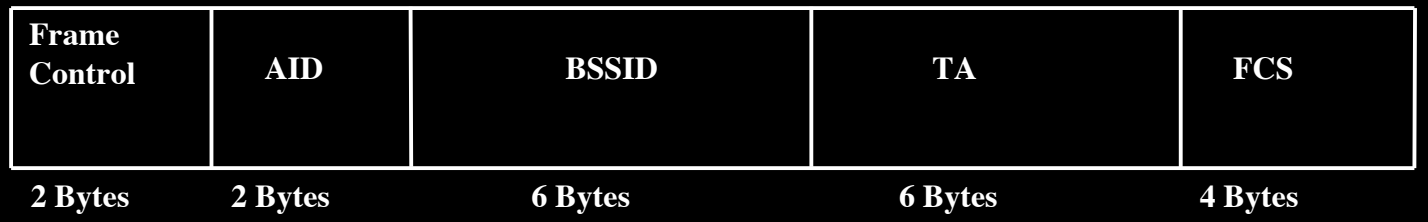
Formato trama (2)

- **Campo de Direcciones: D**irección de 48 bits. Si el primer bit es 0, *unicast*. Si el primer bit es 1, *multicast*. Si todos los bits 1, la trama es *broadcast*.
  - ***Dirección destino:*** *R*eceptor final de la trama.
  - ***Dirección de la fuente:*** *F*uente de la transmisión.
  - ***Dirección del receptor:*** Indica qué estación inalámbrica debe procesar la trama para encaminarla al destinatario.
  - ***Dirección del transmisor:*** Identifica la interfaz inalámbrica que transmite la trama al medio inalámbrico.
  - ***Identificador Basic Service Set (BSSID):*** Identifica las diferentes redes inalámbricas LAN ubicadas en la misma área.
    - Cada BSS tiene determinada un BSSID, un identificador de 48 bit que la distingue de otras BSS's.
    - En modo infraestructura la BSSID es la dirección MAC de la interfaz inalámbrica del punto de acceso que crea la BSS.
    - El BSSID todo 1´s dirección *broadcast*.

Tramas de control

- Power save poll (PS-Poll)
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledgement (ACK)
- Contention-free End (CF-End)
- CF-End+contention-free acknowledgement (CF-End+CF-ACK)

Tramas de control: PS-Poll

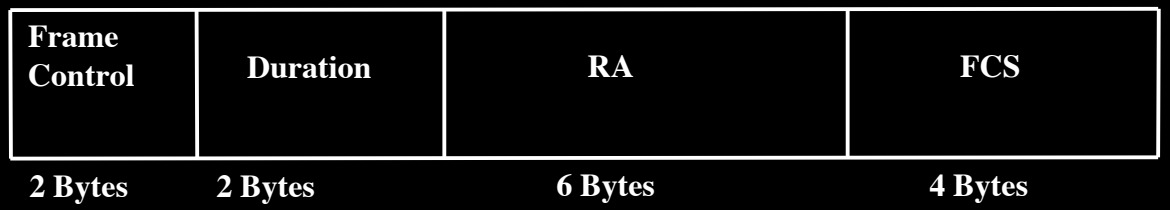


- Trama PS-Poll: La estación que esta en ahorro de energía solicita al AP tramas pendientes
  - AID: Association Identity (AID) de la estación.
  - BSSID: MAC del AP de la infraestructura.
  - TA: MAC de la estación inalámbrica en power-save.
  - FCS: Campo control de secuencia.

Tramas de control: RTS

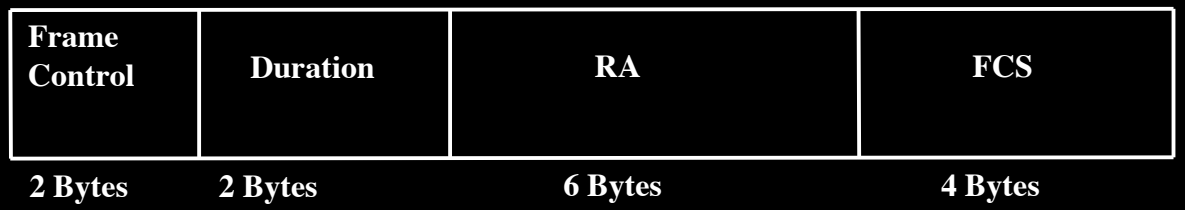
- Trama RTS: Solicitud de reserva del medio inalámbrico
  - Duration: Tiempo requerido por la estación en us. Incluye t(RTS) + t(CTS)+SIFS + t data+SIFS + ACK+SIFS
  - RA: MAC del receptor deseado.
  - TA: MAC del transmisor de la trama.
  - FCS: Campo control de secuencia.

Tramas de control: CTS



- Trama CTS: Respuesta al RTS, indica que el medio ha sido reservado por un tiempo
  - Duration: RTS Duration (us) - t(CTS)-SIFS
  - RA: MAC del receptor deseado.
  - FCS: Campo control de secuencia.

Tramas de control: ACK



- Trama ACK: La envía el rx al tx para indicar que ha recibido la trama
  - Duration: 0 normalmente, la trama ya incluía tiempo ACK+SIFS
  - RA: MAC del receptor deseado.
  - FCS: Campo control de secuencia.

Tramas de control: CF-End y CF-End+CF-ACK

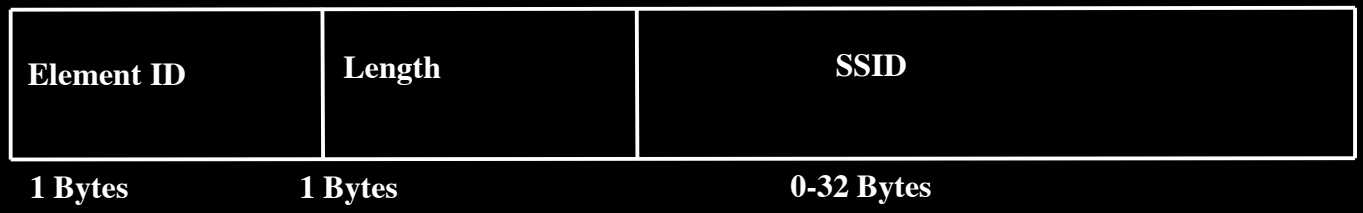
- Trama CF-End y CF-End+CF-ACK : Específicas de PFC. Indica final de período contention-free y CF-End+CF-ACK incluye un ACK de la última trama recibida por PC
  - Duration: 0.
  - RA: MAC del receptor deseado. En CF-End broadcast MAC.
  - BSSID: MAC del AP.
  - FCS: Campo control de secuencia.

Tramas de gestión

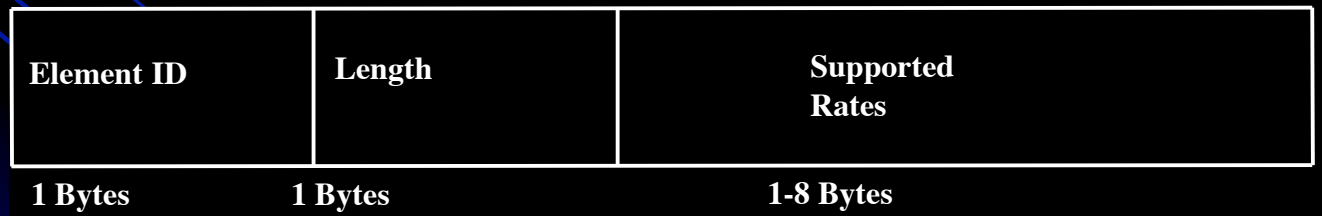
- Beacon
- Probe request
- Probe response
- Authentication
- Deauthentication
- Association request
- Association response
- Reassociation request
- Reassociation response
- Disassociation
- Announcement traffic indication

Tramas de gestión: Info element (1)

- SSID IE
  - Si Length 0, broadcast SSID



- Supported Rates IE
  - Cada valor binario +500kbps



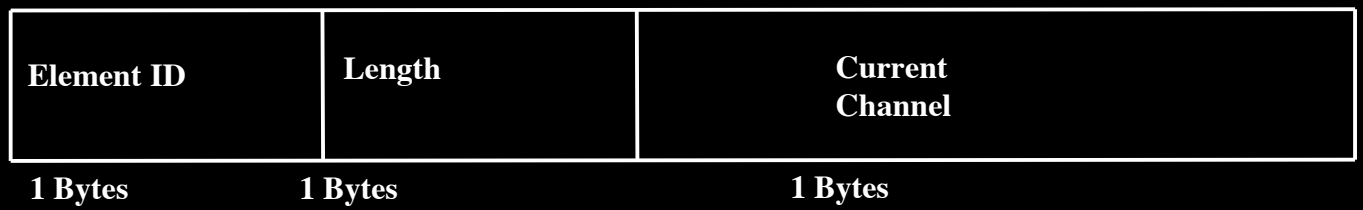
Tramas de gestión: Info element (2)

- FH Paremeter Set ID (Frecuency Hop)
  - Dwell time: el tiempo FH dwell en UT
  - Hop set: patrón de grupo de salto FH
  - Hop pattern: patrón individual de salto F
  - Hop index: índice de canal en uso dentro del patron de salto

Element ID	Length	Dwell Time	Hop Set	Hop Pattern	Hop Index
1 Bytes	1 Bytes	2 Bytes	1 Bytes	1 Bytes	1 Bytes

Tramas de gestión: Info element (3)

- DS Parameter Set ID
  - Current channel: canal en uso por la estación de secuencia directa



- CF Parameter Set ID
- TIM IE
- IBSS Parameter Set ID
- Challenge Text IE

Tramas de gestión: Fixed Fields (1)

- Authentication Algorithm Number Field
  - 0 autenticación abierta
  - 1 autenticación con clave compartida
  - Resto reservados
- Authentication Transaction Sequence Number Field
  - Paso actual en procesos de autenticación multipaso
- Beacon Interval Field
  - Uts entre beacons

Tramas de gestión: Fixed Fields (2)

- Capability Information Field
  - ESS: En tramas beacon y probe response, AP=1 y IBSS=0.
  - IBSS: En tramas beacon y probe response, IBSS=1 y ESS=0.
  - CF-Pollable
  - CF-Poll request
  - Privacy: Si WEP=1 si no 0.
- Current AP Adress Field
  - MAC AP al que esta asociado la estación.

Tramas de gestión: Fixed Fields (3)

- Listen Interval Field
  - Nº intervalos beacon para que estación despierte.
- Reason Code Field
  - Razón de deatenticación o desasociación sin petición.
- AID Field
  - Puerto lógico para la estación. Asignado por AP.
- Status Code Field
  - En tramas response indica exito o fallo de solicitud en trama request.
- Timestamp Field
  - Valore de TSFTIMER

Tramas de gestión: Tipos (1)

- Trama Beacon:
  - La envía el AP cada Beacon Interval.
  - Proporciona sincronización AP-estaciones
  - Contiene parámetros físicos.
  - En Power Save, si AP time tramas almacenadas.

Tramas de gestión: Tipos (2)

- Probe request

Frame Control	Duration	DA	SA	BSSID	Sequence Control	SSID IE	Supported Rates IE

- Probe response

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Time-stamp Field	Beacon Interval Field	Capability Information Field	SSID IE	Supported Rates IE	FH/DS Parameter Set IE	CF Parameter Set IE (Optional)	IBSS Parameter Set IE (Optional)

- Authetication

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Authetication Algoritm Numer Field	Authetication Transaction Sequence Numer Field	Status Code Field	Challenge Text IE (Optional)

Tramas de gestión: Tipos (3)

- Deauthetication

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Reason Code Field

- Association request

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Listen Interval Field	Current AP Address Field	SSID Field	Supported Rates IE

- Association response

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Status Code Field	AID Field	Supported Rates IE

Tramas de gestión: Tipos (4)

- Reassociation request

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Listen Interval Field	Current AP Address Field	SSID Field	Supported Rates IE

- Reassociation response

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Capability Information Field	Status Code Field	AID Field	Supported Rates IE

- Disassociation

Frame Control	Duration	DA	SA	BSSID	Sequence Control	Reason Code Field

Tramas de datos

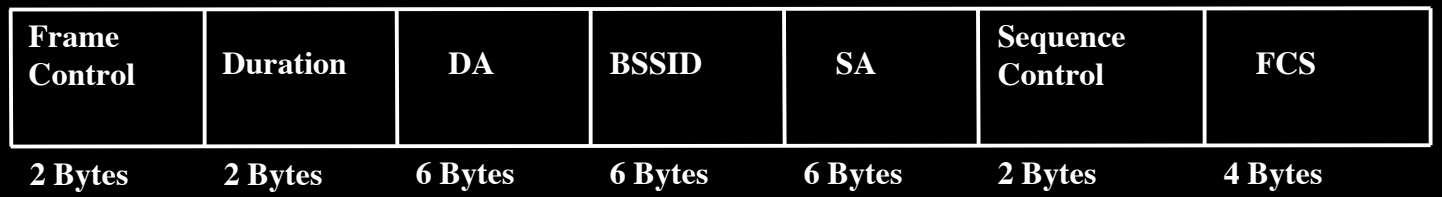
- Data
- Null data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- CF-ACK
- CF-Poll
- CF-ACK+CF-Poll

Tramas de datos: Data, Data+CF-ACK, Data+CF-Poll y Data+CF-ACK+CF-Poll

Frame Control	Duration	DA	BSSID	SA	Sequence Control	Payload	FCS
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	0-2312 Bytes	4 Bytes

- Diferente subtype para proporcionar las funcionalidades CF-ACK y/o CF-Poll requeridas por PCF

Tramas de datos: Null, CF-ACK, CF-Poll y CF-ACK+CF-Poll



- Trama Null data: igual trama data pero sin campo payload. Indica cambio en el bit de ahorro de potencia en el campo de trama de control.
- Diferente subtype para proporcionar las funcionalidades CF-ACK y/o CF-Poll requeridas por PCF