

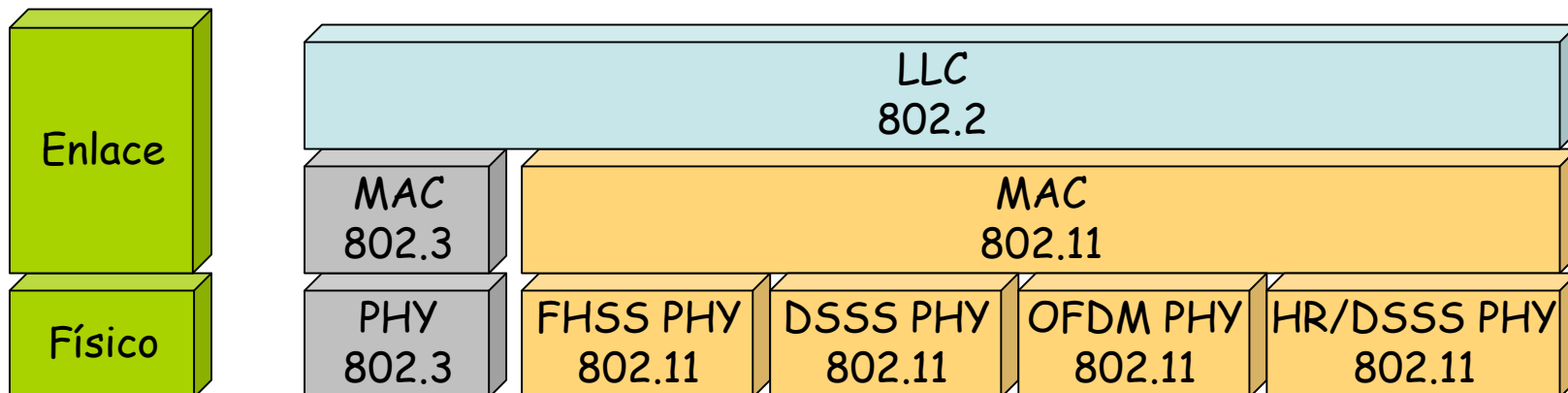
# Tecnologías Wi-Fi

Area de Ingeniería Telemática  
<http://www.tlm.unavarra.es>

Redes de Banda Ancha  
5º Ingeniería de Telecomunicación

# Estándar Wireless LANs

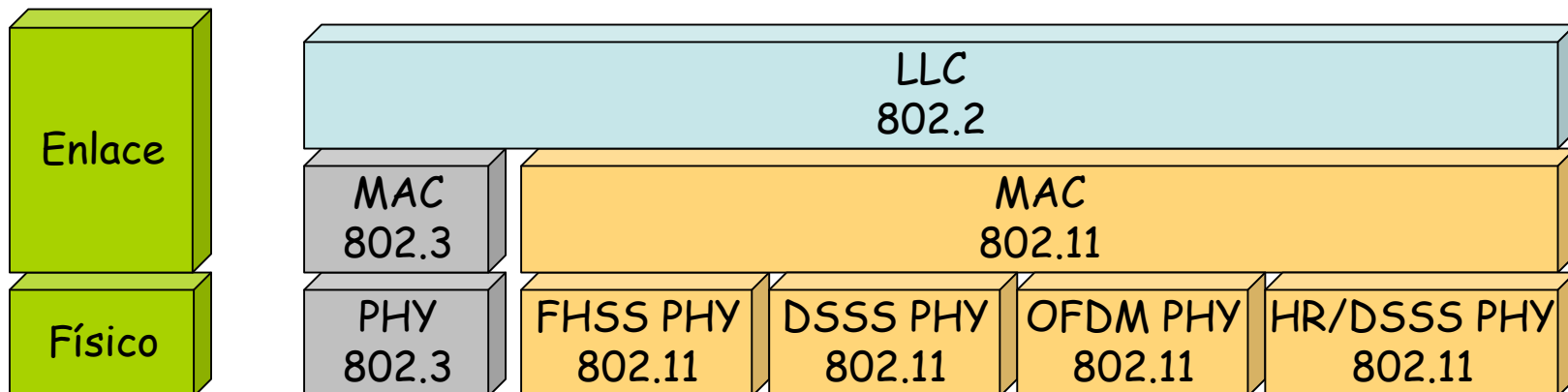
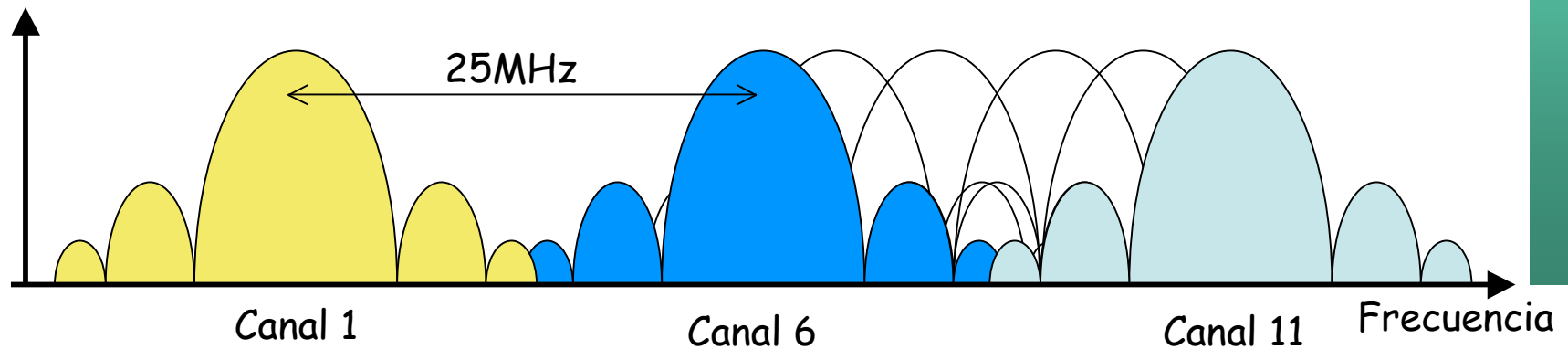
- IEEE 802.11 (1999)
- LAN basada en medio inalámbrico
- Certificación de la Wi-Fi Alliance (<http://www.wi-fi.org/>)
- Hay diferentes niveles físicos posibles
- MAC 802.11 es común a todos ellos
- MAC intenta ofrecer un acceso justo al medio
- El nivel físico está dividido en dos subniveles:
  - PLCP: Physical Layer Convergence Procedure
  - PMD: Physical Medium Dependent



# Nivel físico

## 802.11b

- HR/DSSS = *High Rate Direct-Sequence Spread Spectrum* (hasta 11Mbps)
- En EEUU 11 canales (14 en Japón, 12 en Europa-ETSI)
- BW aprox. de un canal menor de 25MHz (atenuación mayor de 30dB)
- Separación entre canales de 5MHz
- Canales 1-6-11 tienen ya escasa interferencia



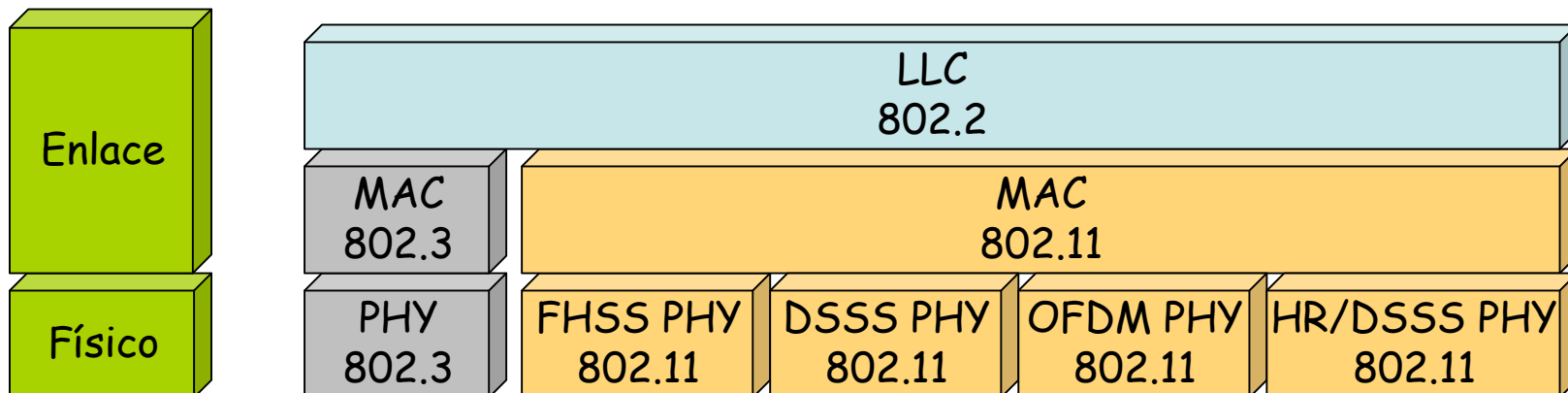
# Nivel físico

## 802.11a

- OFDM = *Orthogonal Frequency Division Multiplexing*
- Hasta 19 canales que no se solapan

## 802.11g

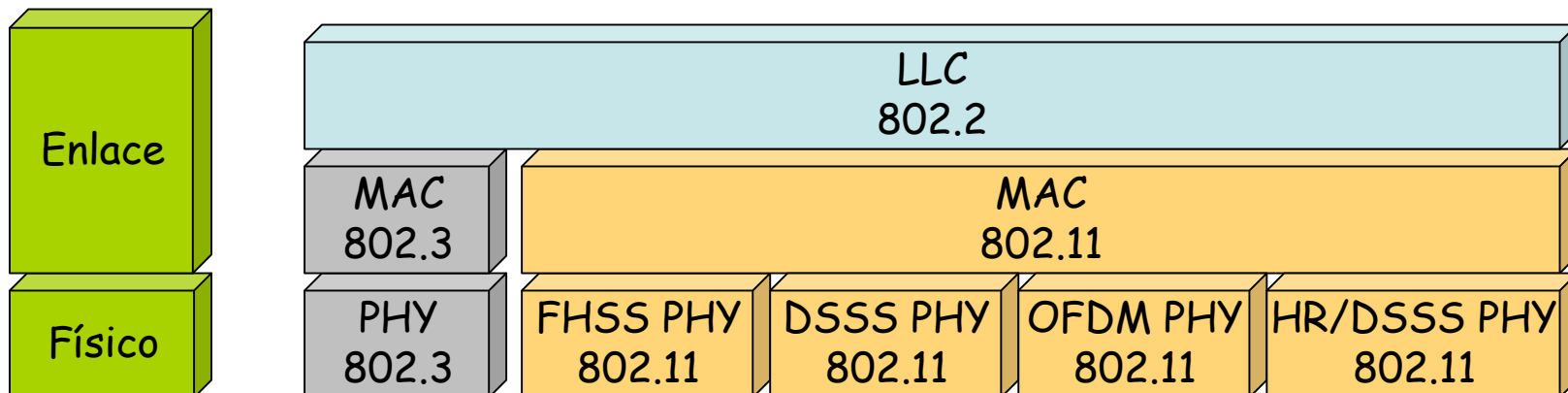
- OFDM = *Orthogonal Frequency Division Multiplexing*
- Compatible con 802.11b



# Nivel físico

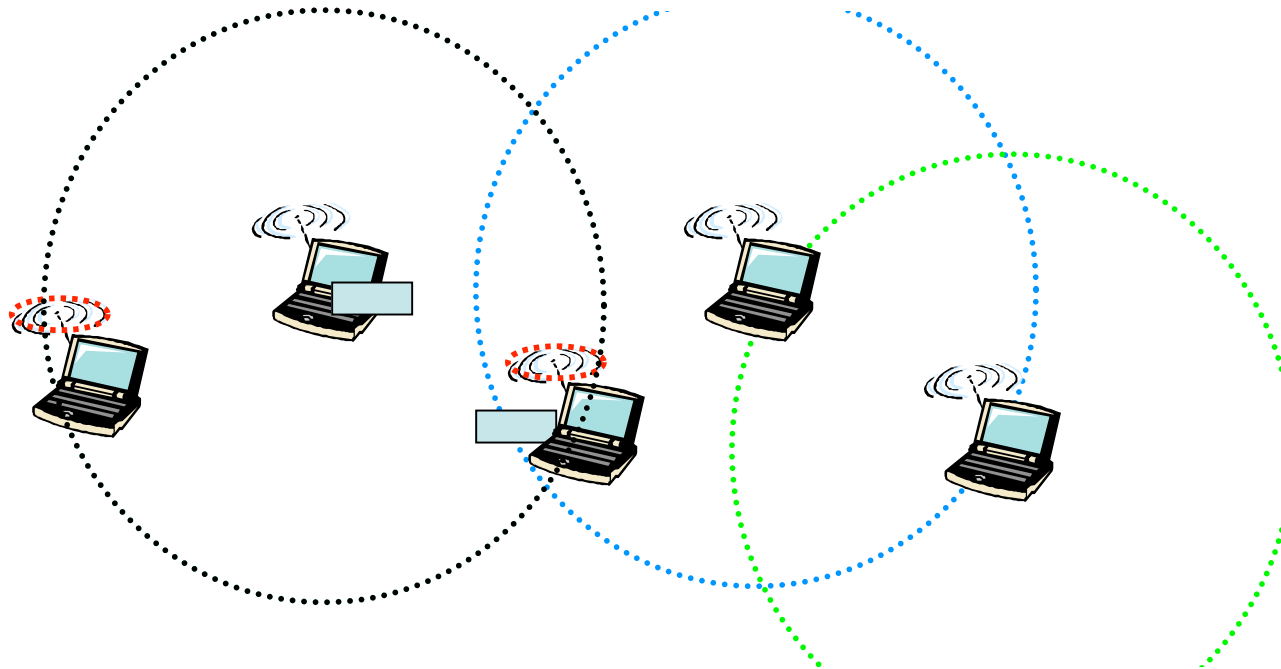
- Emplean bandas que no requieren licencia
  - 2.4 - 2.5 GHz es la *C-Band Industrial, Scientific and Medical (ISM)* (Por ejemplo los hornos microondas, algunos teléfonos inalámbricos, etc)
  - *Unlicensed National Information Infrastructure bands* (en torno a 5GHz)

Estándar	Velocidad Máx	Frecuencia
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	¿ 540 Mbps ?	¿ 2.4 ó 5 GHz ?



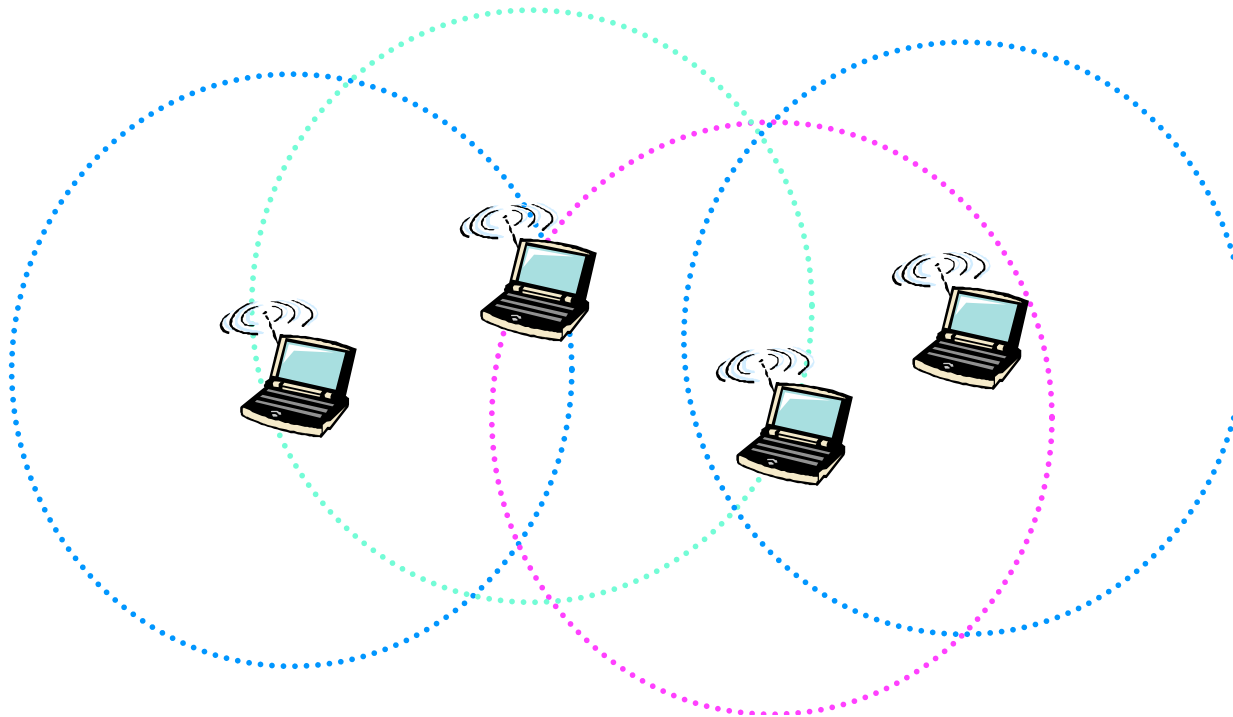
# Wireless LANs

- Para el usuario una WLAN funciona como una Ethernet compartida
- MAC 802.11 intenta ofrecer un acceso justo al medio
- Las estaciones no poseen la capacidad de detectar colisiones (no CSMA/CD)
- Los dispositivos hacen broadcast de la señal de radio
- Un receptor puede estar en el alcance de varios transmisores
- El transmisor antepone a su transmisión un *Service Set Identifier (SSID* ó *BSSID)*
- El receptor usa el SSID para filtrar las señales que desea recibir



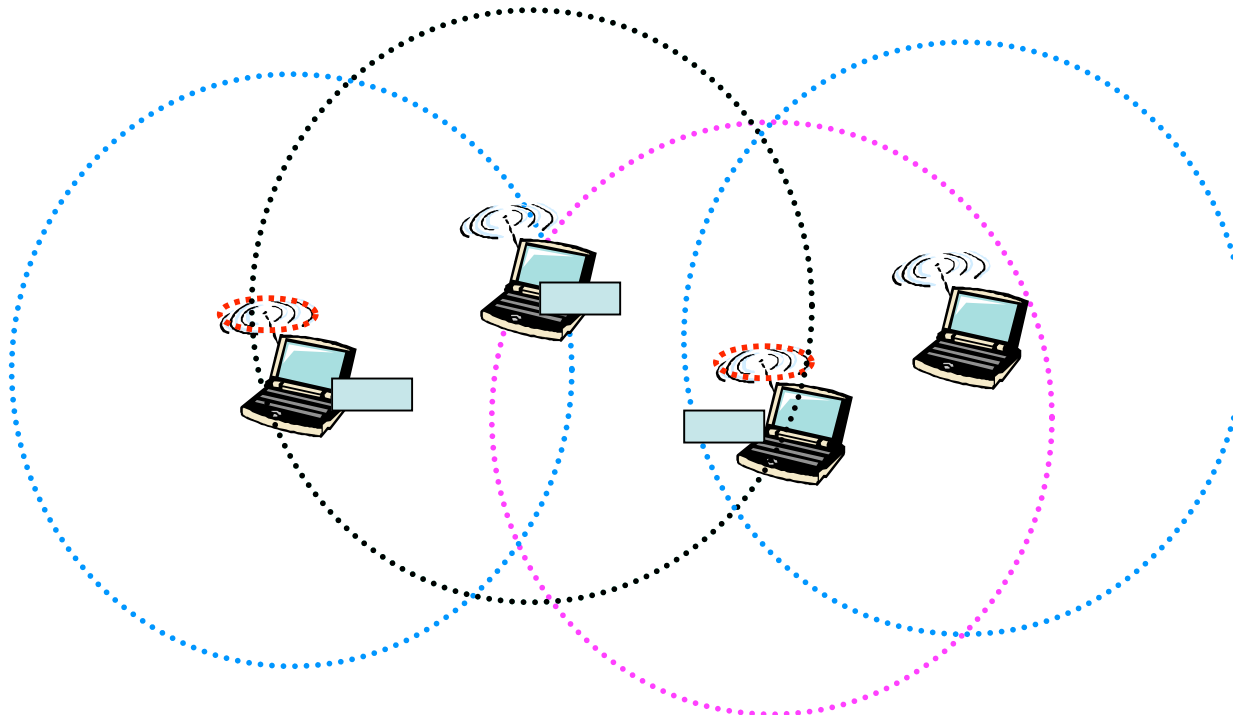
# Topologías

- Topologías:
  - *Independent Basic Service Sets (IBSSs) o Ad Hoc BSS*
  - *Basic Service Sets (BSSs) o Infraestructure BSS*
  - *Extended Service Sets (ESSs)*
- Un *Service Set* es una agrupación lógica de dispositivos



# IBSS

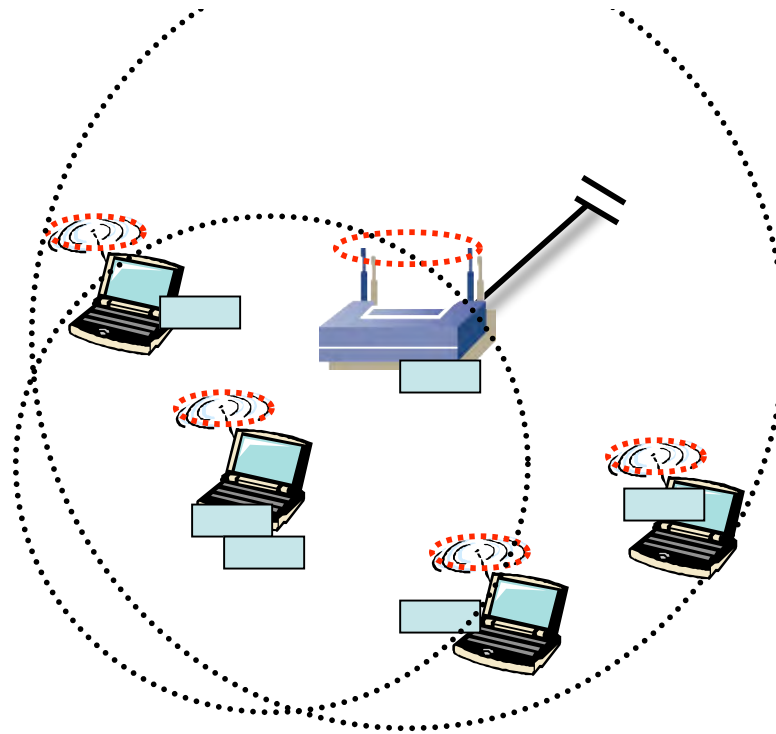
- *Independent Basic Service Set* ó *Ad-hoc network*
- Grupo de estaciones 802.11 comunicándose directamente entre ellas
- Es una WLAN *peer-to-peer*
- Generalmente pequeñas y duran poco tiempo
- No hay límite al número de miembros
- En ocasiones algunos miembros no pueden comunicarse con todos los demás
- BSSID es elegido al azar (número de 48bits empezando por 10)





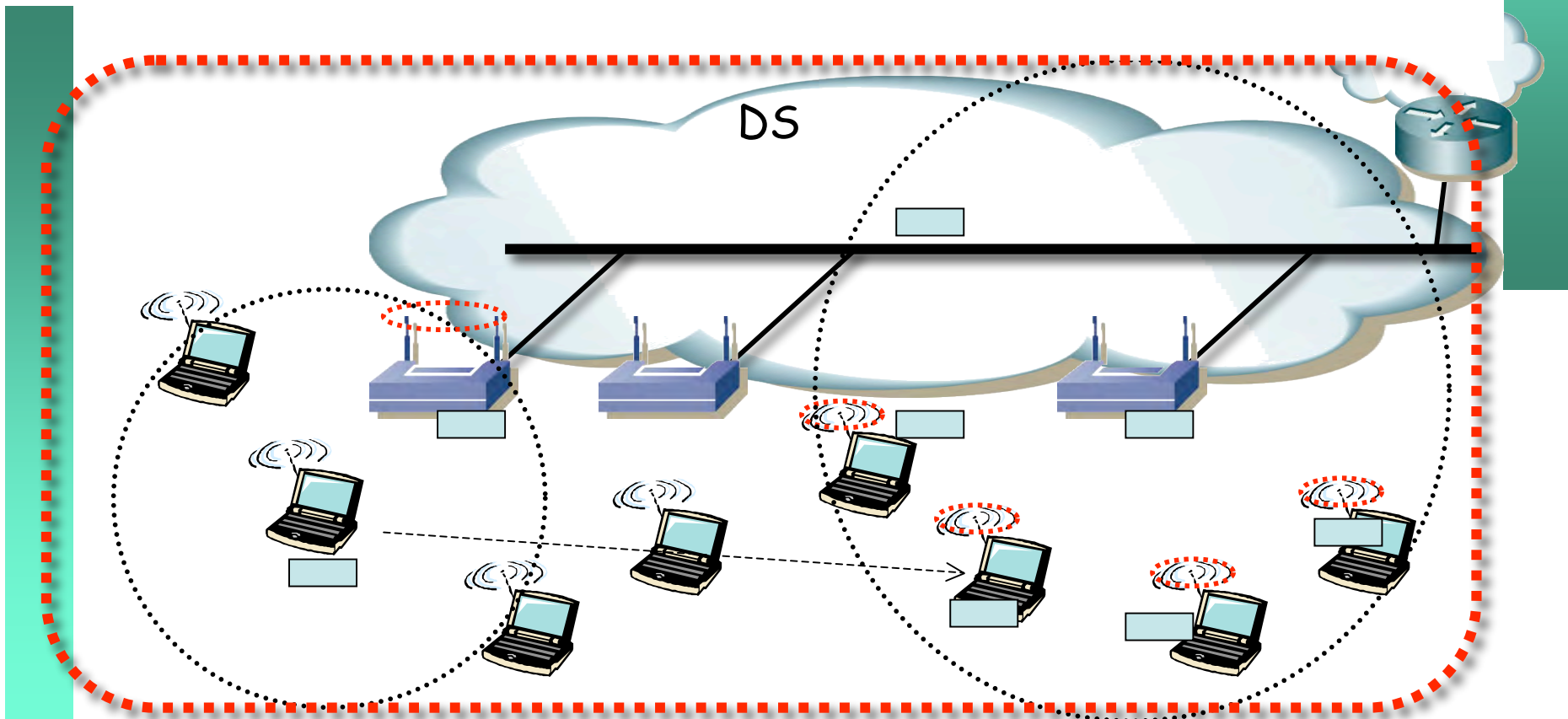
# BSS

- *Basic Service Set* o *Infraestructura BSS*
- Incluye una estación especializada: *Access Point (AP)* (Punto de acceso)
- Los clientes no se comunican directamente sino a través del AP
- El AP puede incluir un *uplink* que conecta a red cableada
- BSSID es la MAC Wi-Fi del AP



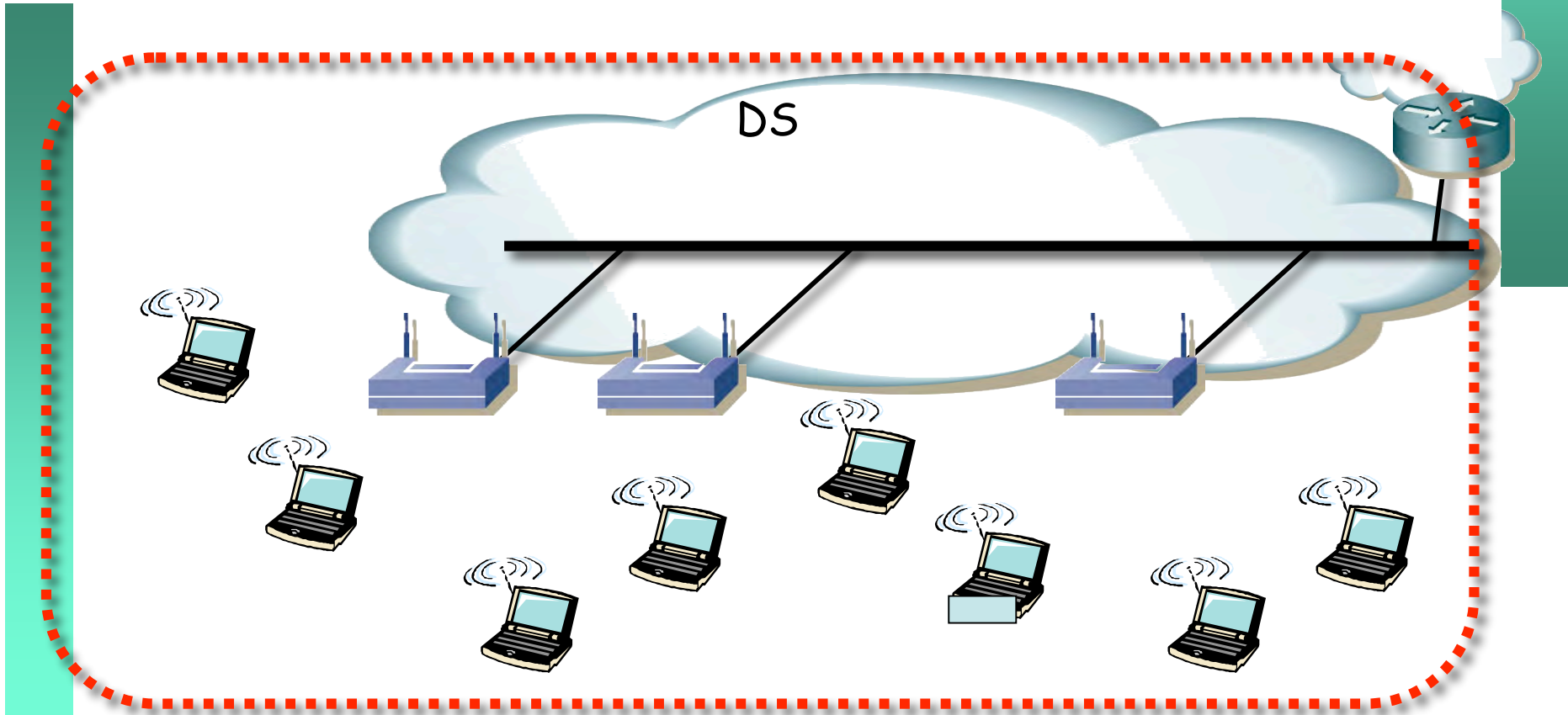
# ESS

- *Extended Service Set*
- Varias BSS conectadas por sus interfaces de *uplink*
- Todas empleando el mismo ESSID
- Se intercomunican a través del *Distribution System (DS)*



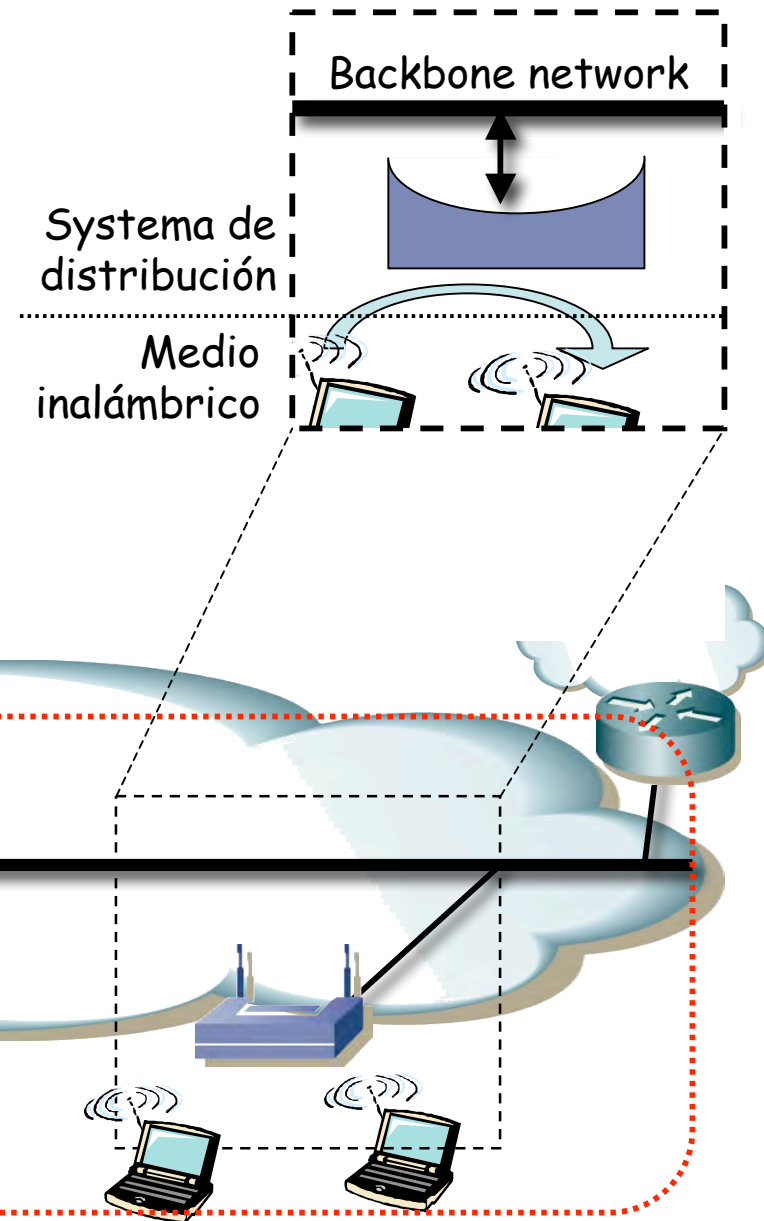
# ESS

- El DS normalmente está creado en base a una Ethernet
- Podría emplearse un DS inalámbrico (*WDS = Wireless Distribution System*)
- En cualquier caso debe ser una LAN (nivel 2)
- El AP actúa como un puente



# ESS

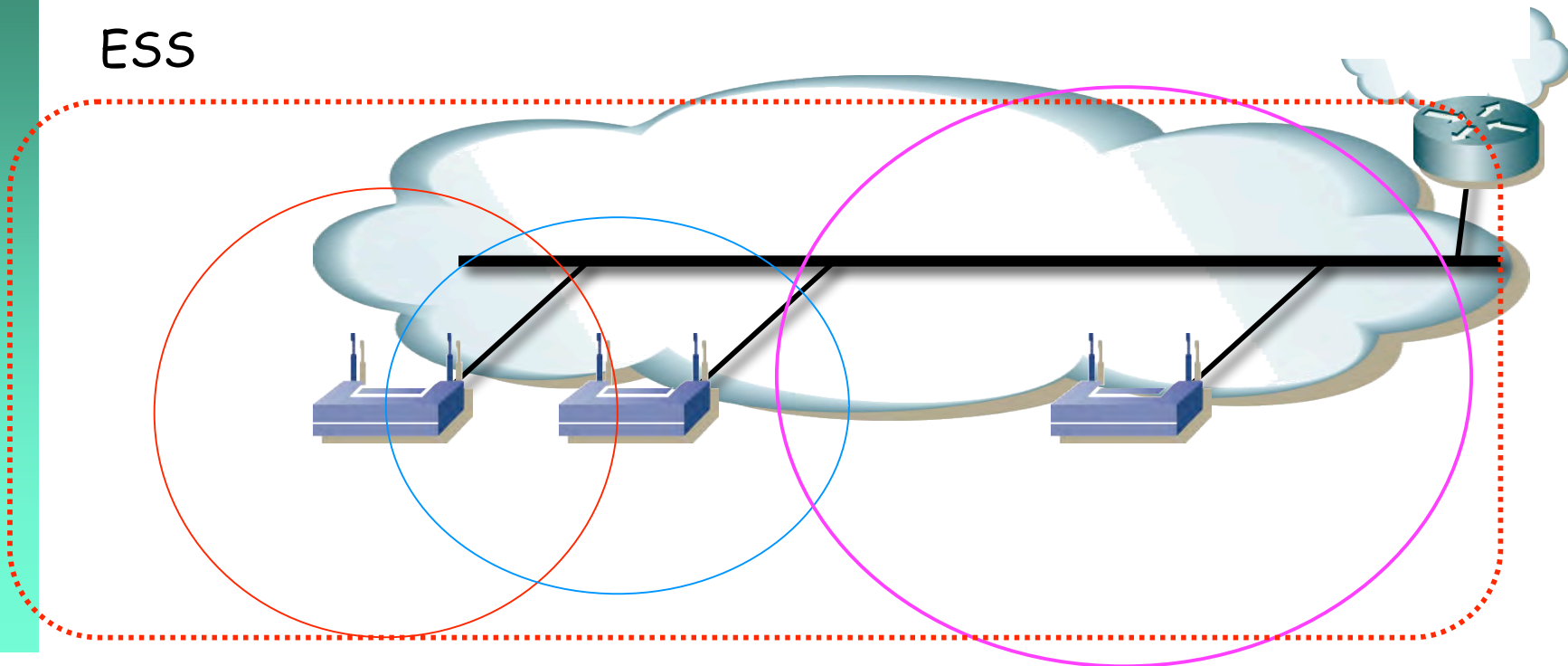
- La Ethernet no forma entera el DS, es solo el *DS medium*
- En realidad, la comunicación entre estaciones inalámbricas atraviesa el DS



# Movilidad

- 802.11 ofrece movilidad en el nivel de enlace
- Transparente para los niveles superiores
- Todo el contenido de un ESS es la misma LAN
- El ESS sabe hacer llegar una trama a donde esté el destino

ESS

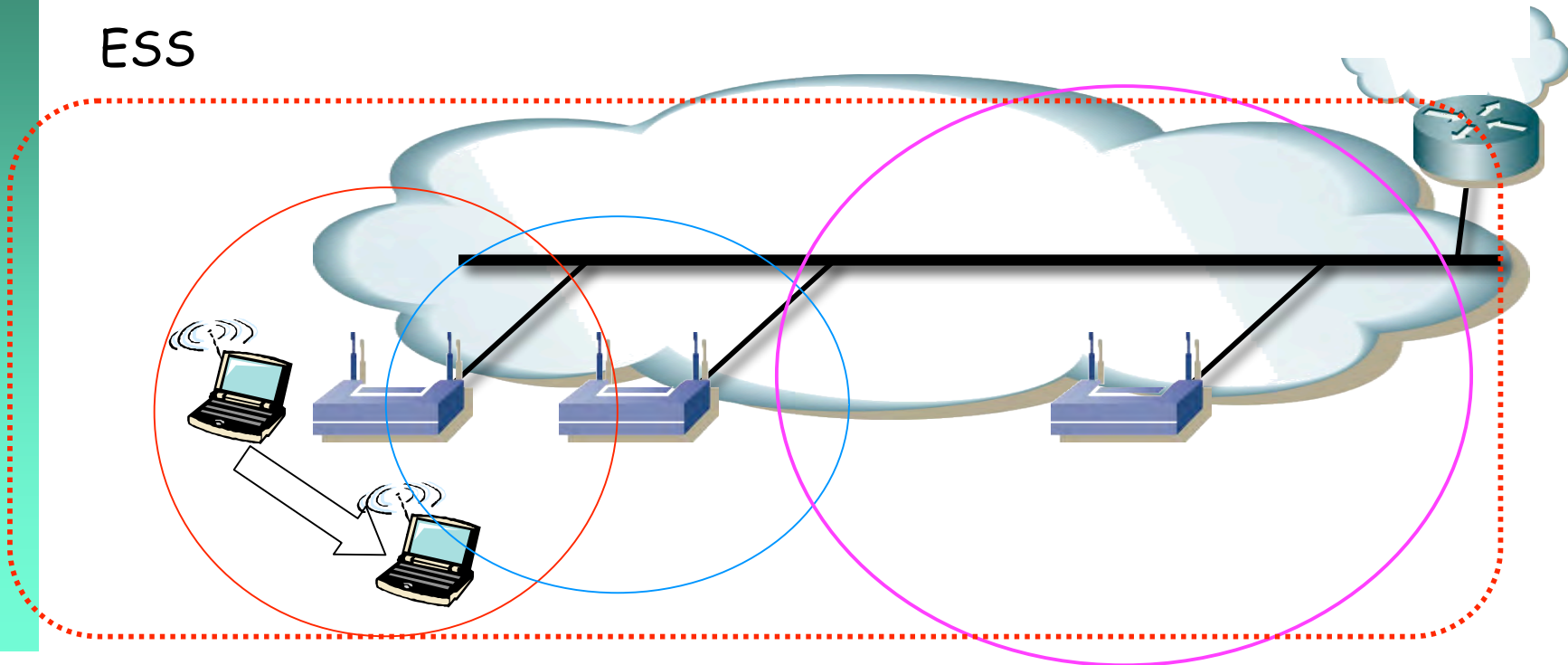


# Movilidad

## Sin transición

- Estaciones se mueven dentro del área de cobertura de un mismo AP

ESS

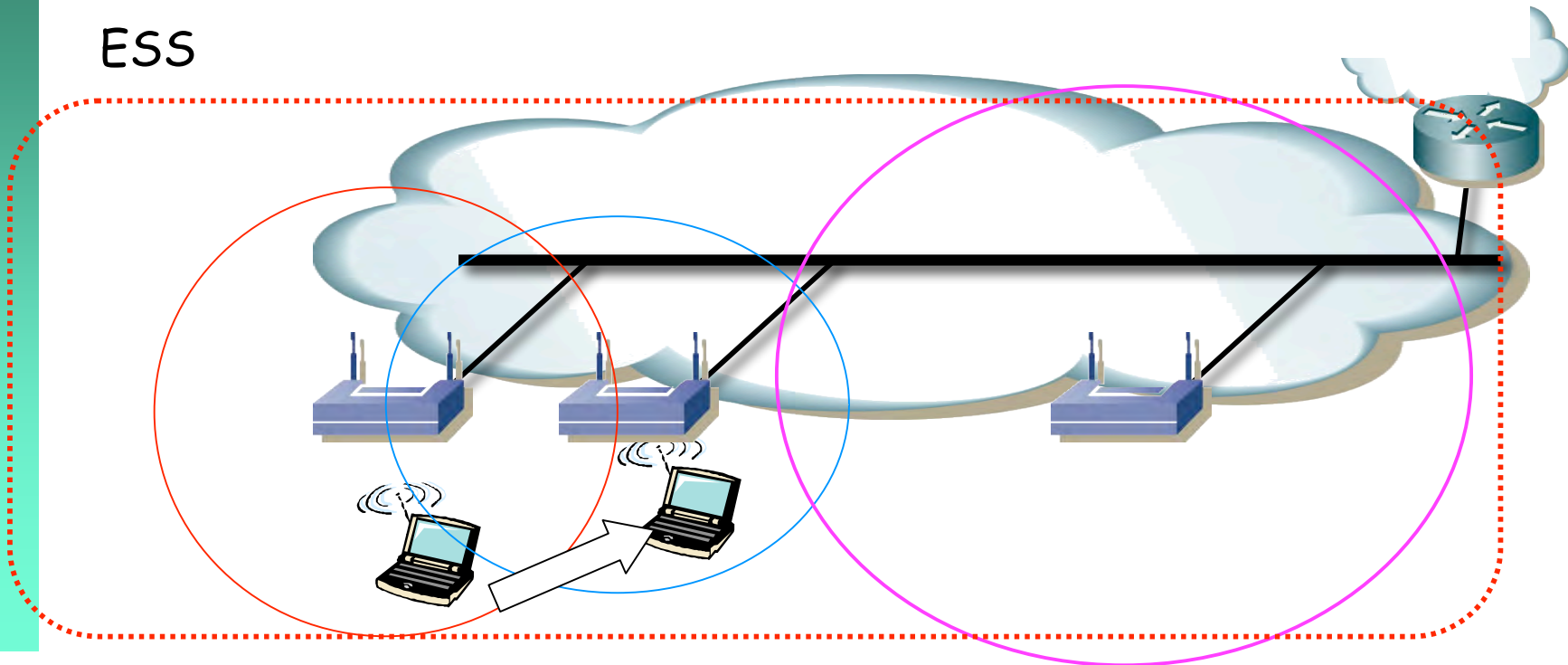


# Movilidad

## Transición BSS

- Estaciones se mueven dentro de un mismo ESS cambiando de AP
- Reasociación, normalmente al detectar otro AP con más potencia
- Requiere cooperación entre los APs para conocer a cuál se encuentra asociado el usuario
- Durante bastante tiempo esa cooperación no estuvo estandarizada. Hoy en 802.11F

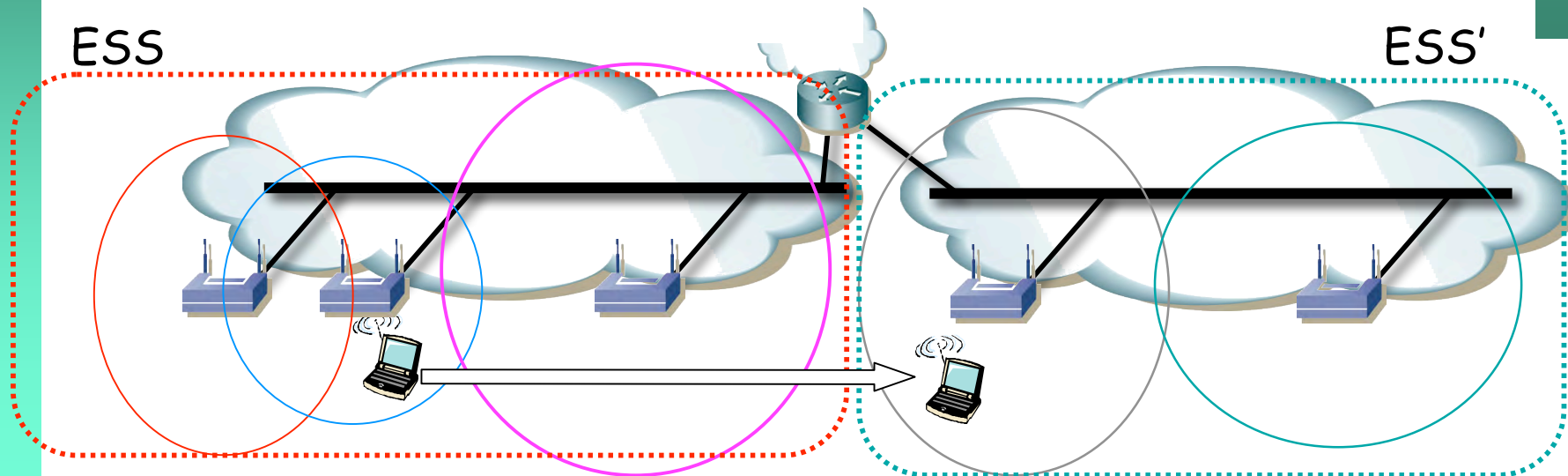
ESS



# Movilidad

## Transición ESS

- De un ESS a otro distinto
- No soportado por 802.11
- Comunicación de capas superiores se ve interrumpida
- Se creará una nueva asociación y nueva configuración de red
- Para TCP/IP existe la posibilidad de *Mobile IP*

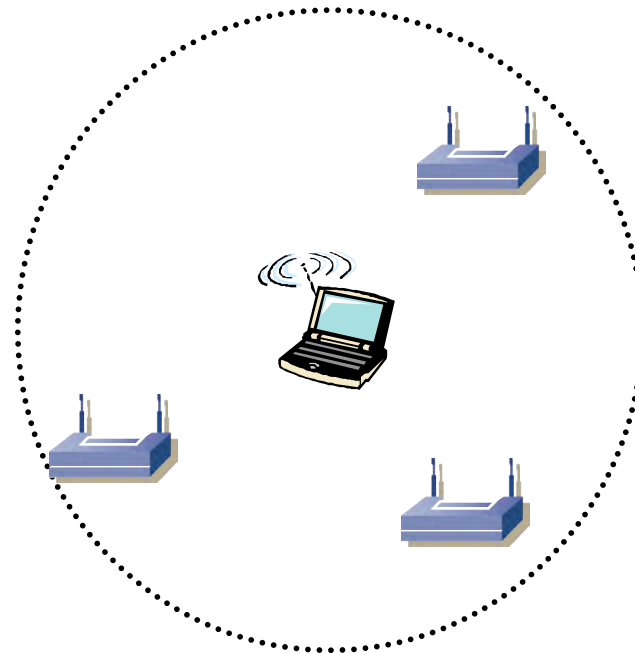




# Unirse a un BSS

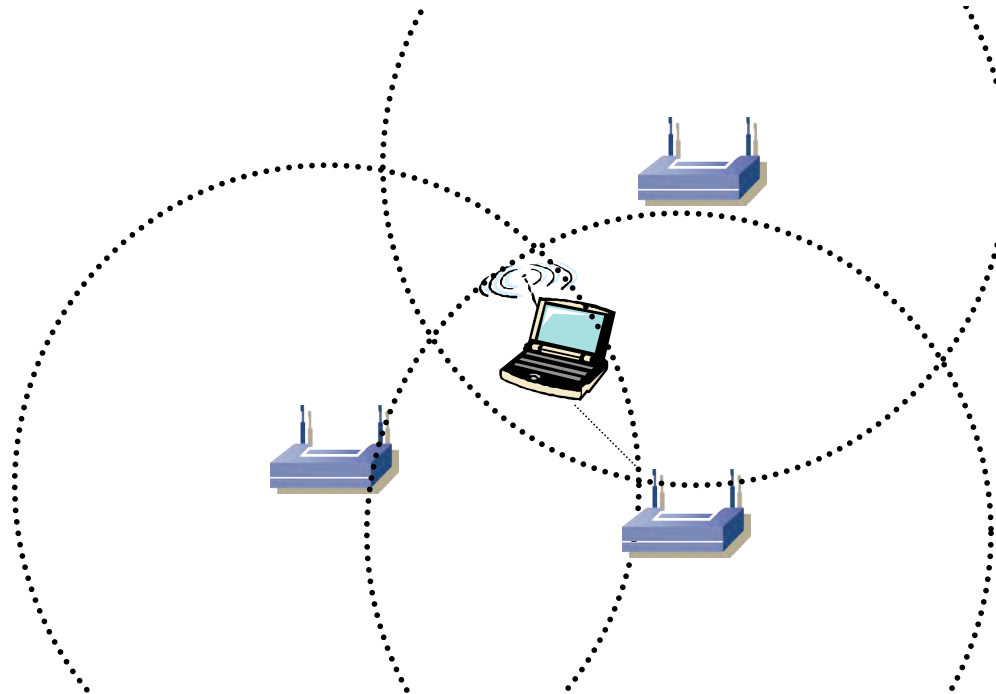
## Proceso de sondeo

- Usuario envía una trama de sondeo (*probe*)
- Normalmente en todos los canales que soporta
- A la menor velocidad soportada (1Mbps)
- Incluye información sobre las velocidades que soporta y el SSID al que pertenece



# Unirse a un BSS

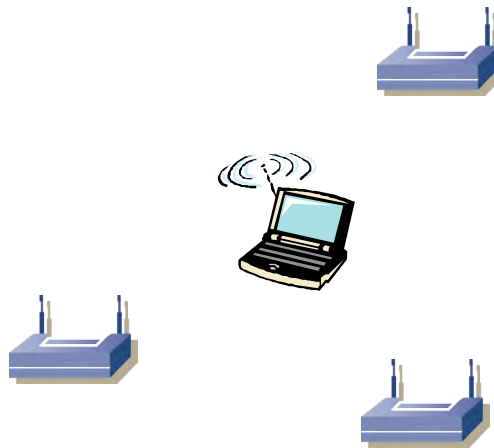
- APs responden (*probe response*)
- El cliente averigua:
  - Potencia de señal con cada uno
  - SSID de cada uno
  - Velocidades soportadas
- Cliente selecciona a cuál asociarse



# Unirse a un BSS

## Proceso de autenticación

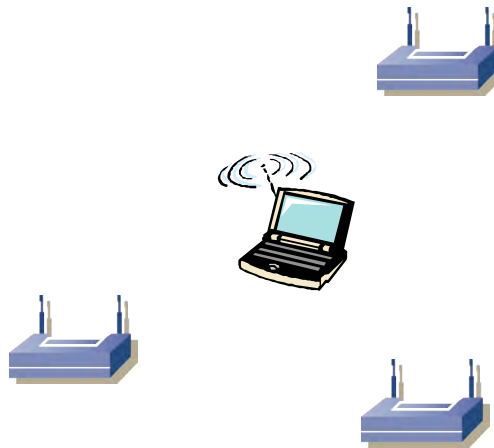
- En la asignatura “*Gestión y Seguridad en Redes de Ordenadores*”



# Unirse a un BSS

## Proceso de asociación

- Cliente envía una trama de solicitud de asociación (*association request*)
- El AP responde (*association response*) con un aceptación o rechazo
- AP asigna un *puerto lógico* al cliente (*AID, Association Identifier*)



# Servicios ofrecidos por 802.11

## Asociación

- Estación móvil se registra en un AP

## Autenticación

- Puede darse varias veces pero al menos antes de la asociación

## Distribución

- Una trama aceptada por el AP emplea este servicio para entregarla al destino
- Determina dónde está el destino
- Toda comunicación a través del AP emplea el servicio de distribución (incluido entre estaciones asociadas al mismo AP)

## MSDU delivery

- *MAC Service Data Unit* delivery
- Hacer llegar los datos al destino

# Servicios ofrecidos por 802.11

## Reasociación

- Movilidad entre BSS de un ESS

## Desasociación

- Abandonar la red

## Desautenticación

- Termina la autenticación y con ello la asociación

## Confidencialidad

- Encriptación de las tramas

## Integración

- Permite conectar el DS a una red no 802.11

# Servicios ofrecidos por 802.11

## TPC

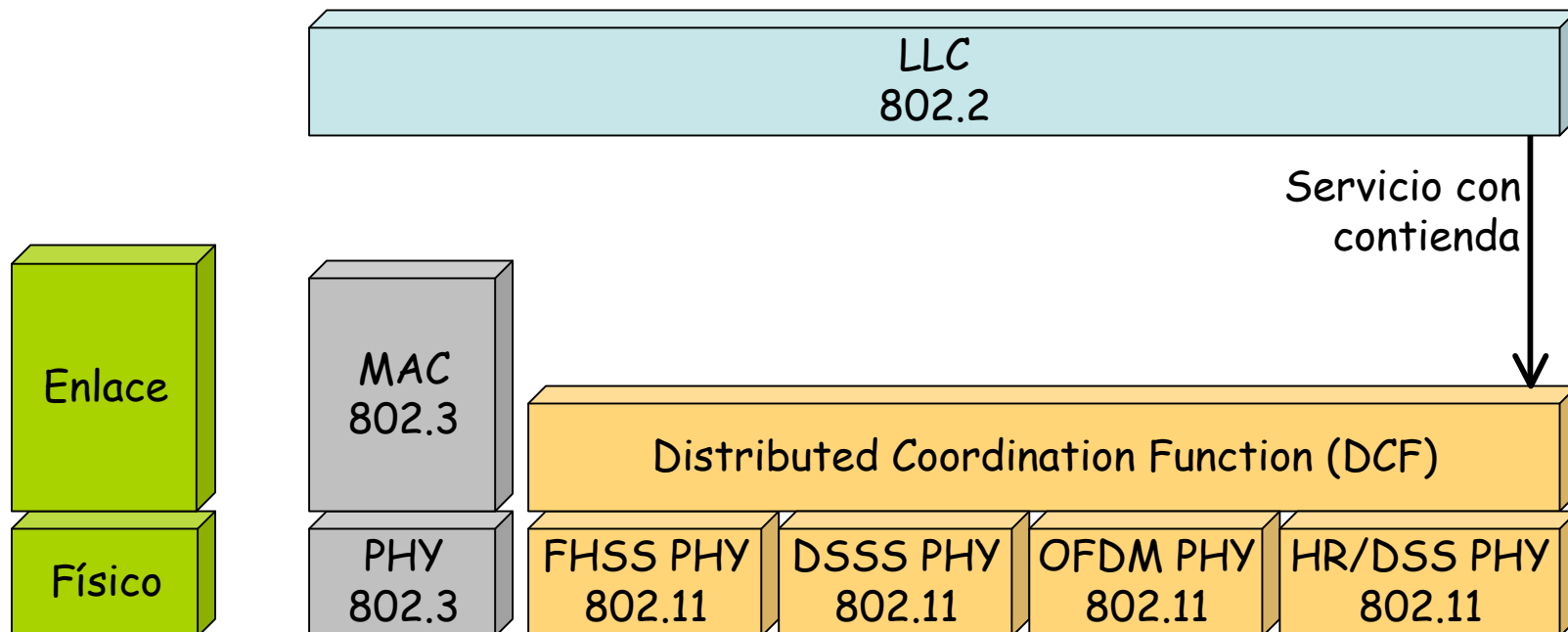
- *Transmit Power Control*
- 802.11h, para reducir interferencias en 802.11a

## DFS

- *Dynamic Frequency Slection*
- Evitar radares en 5GHz

# Subnivel MAC

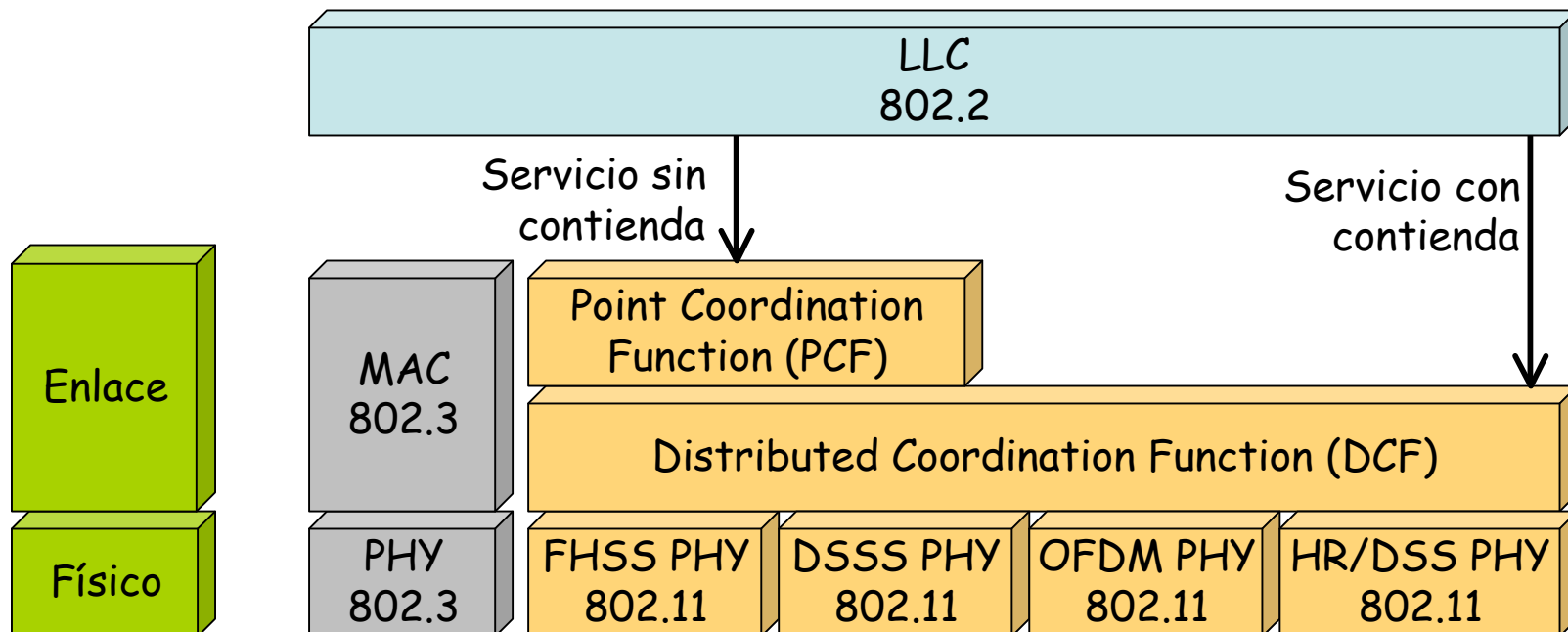
- IEEE 802.3 (Ethernet) usa CSMA/CD
- IEEE 802.11 (Wi-Fi):
  - DCF = *Distributed Coordination Function*
    - CSMA/CA = *Carrier Sense Multiple Access / Collision Avoidance*
    - *Mandatory*
    - Modo infraestructura o *ad-hoc*





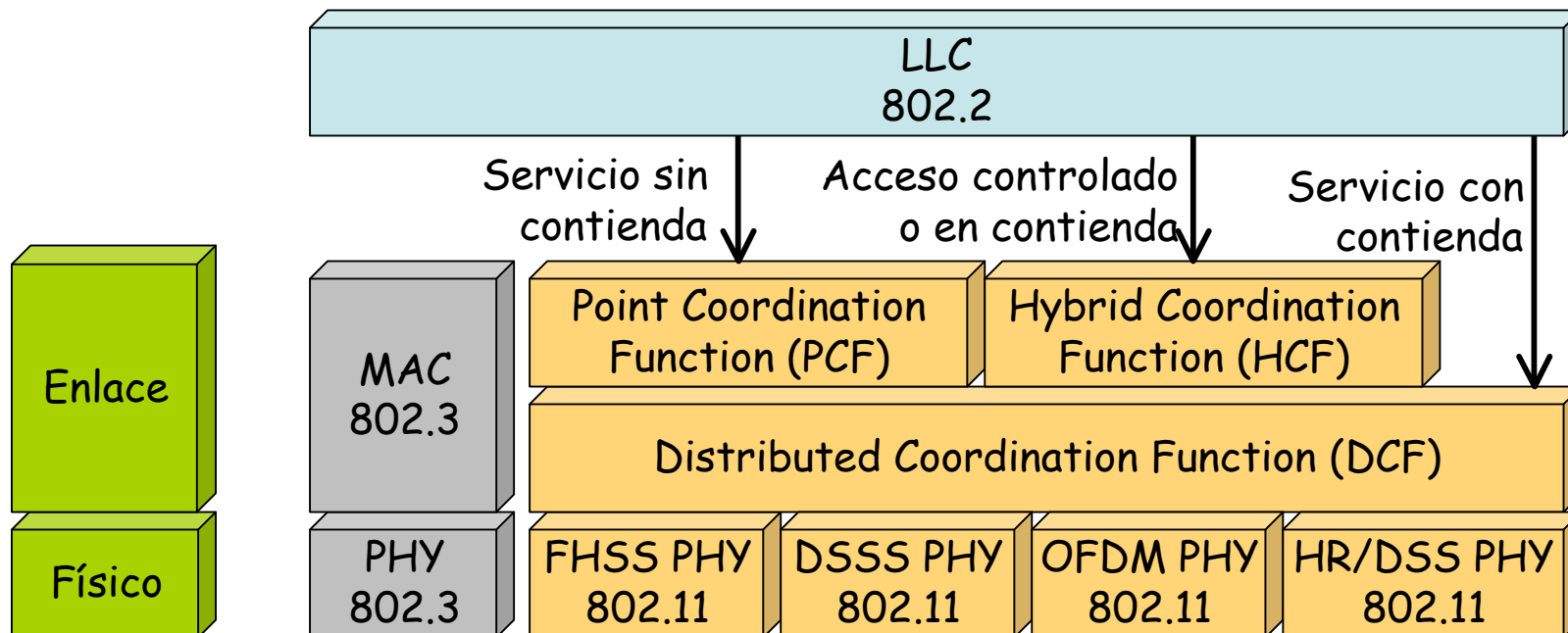
# Subnivel MAC

- IEEE 802.3 (Ethernet) usa CSMA/CD
- IEEE 802.11 (Wi-Fi):
  - PCF = *Point Coordination Function*
    - Solo para modo infraestructura
    - Sin contienda (hay un coordinador)
    - Poco implementada



# Subnivel MAC

- IEEE 802.3 (Ethernet) usa CSMA/CD
- IEEE 802.11 (Wi-Fi):
  - HCF = *Hybrid Coordination Function*
    - Permite QoS sin los requisitos rigurosos de PCF
    - 802.11e



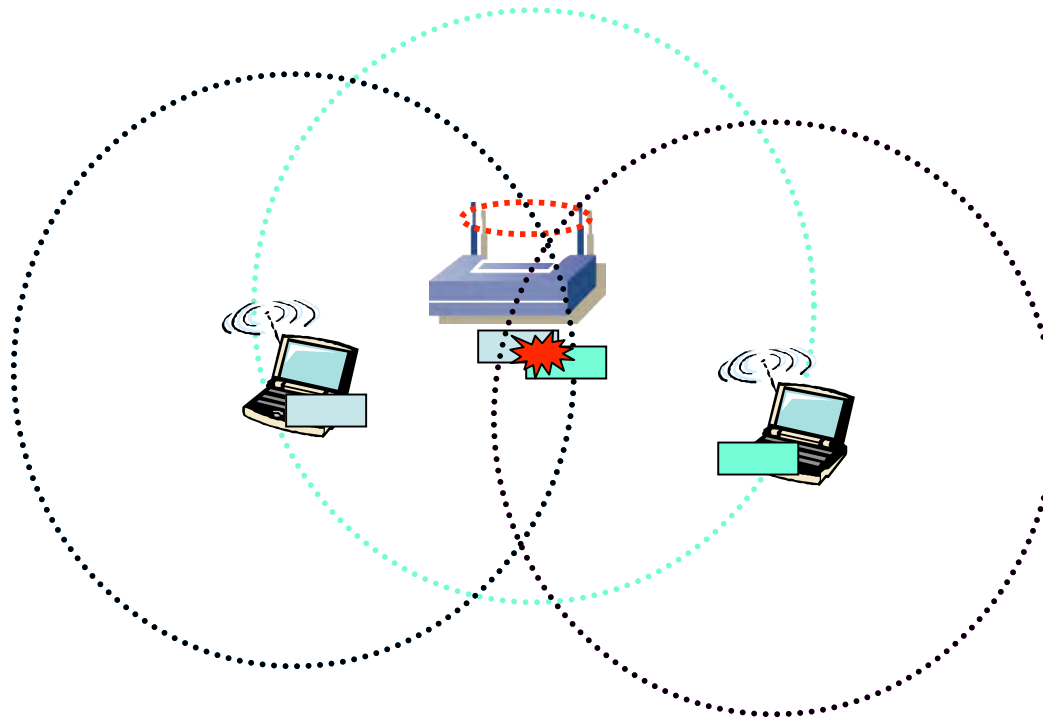
# Subnivel MAC

## Conveniente un cierto conocimiento en detalle:

- Para comprender las diferentes soluciones para hacer la red segura
- Para solucionar problemas de red (*packet sniffing*)
- Para poder optimizar parámetros de la misma
- Para ajustar parámetros de los drivers
- Para comprender las mejoras que se van ofreciendo en nuevos productos y estándares

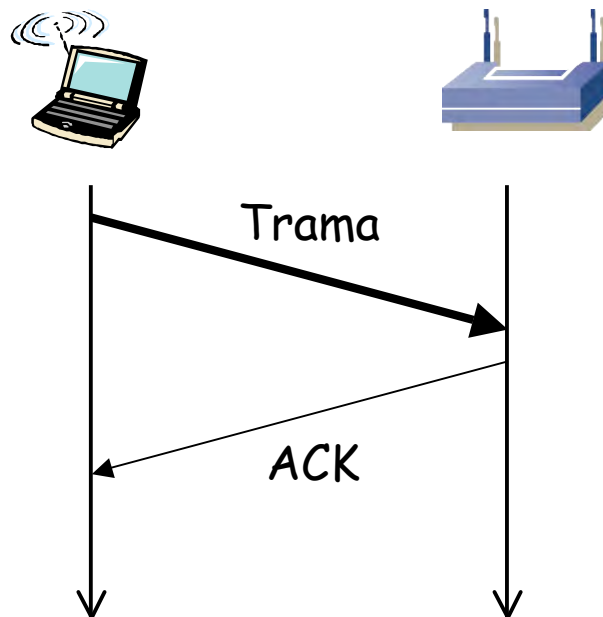
# MAC

- Emplea un método CSMA (*Carrier Sense Multiple Access*)
- ¿Detección de colisiones?
  - Puede que la trama que provoca la colisión en el receptor no lo haga en el emisor
  - Las estaciones no tienen la capacidad de detectar colisiones



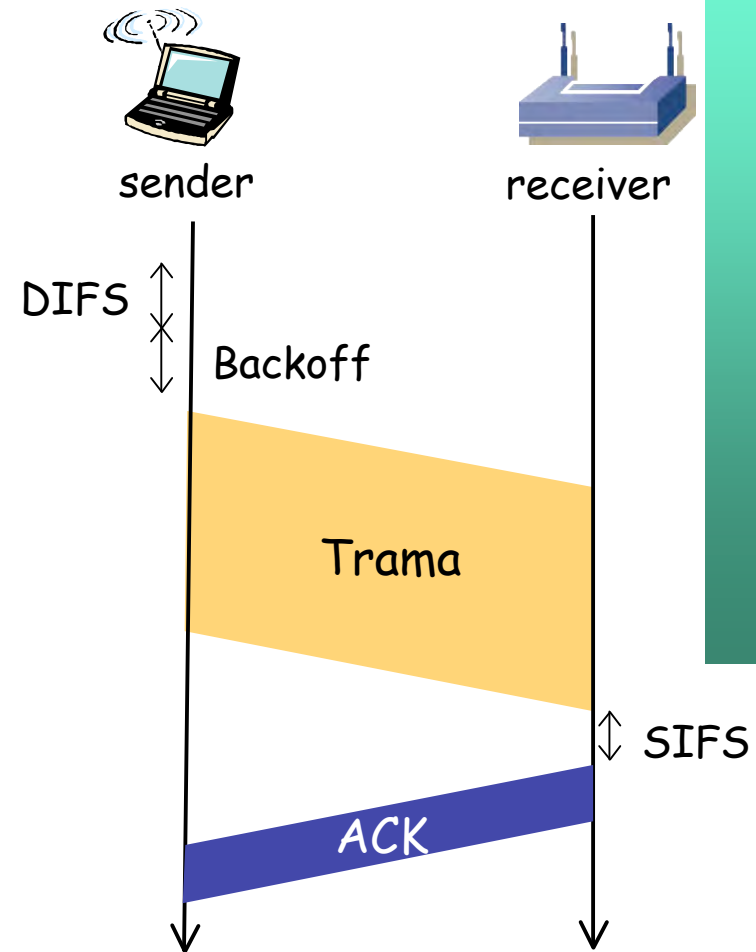
# MAC

- El ruido es difícil de controlar (bandas libres)
- 802.11 emplea confirmaciones positivas
- La secuencia de trama+ack es una operación atómica (todo o nada)
- Tramas a la MAC de broadcast no son confirmadas (ni multicast)



# CSMA/CA

- **Carrier Sense:** Si se detecta el medio inactivo durante el tiempo suficiente (DIFS) la estación puede enviar una trama
- **Random Backoff:** Genera un valor al azar de tiempo que espera (entre  $CW_{min}$  y  $CW$ )
- Si el medio sigue libre envía la trama
- Destinatario espera un tiempo (SIFS, con  $SIFS < DIFS$ ) y envía una confirmación
- Si no recibe ACK duplica  $CW$ , genera un nuevo backoff aleatorio, espera y retransmite

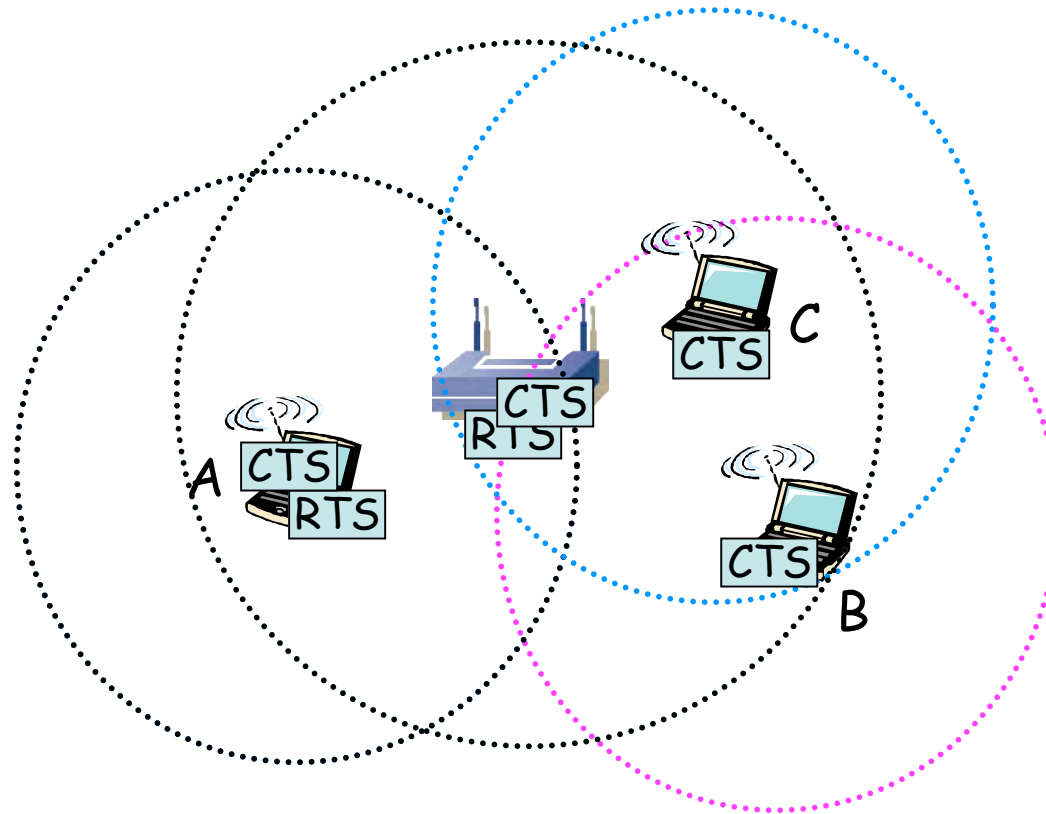


DIFS = DCF Interframe Space  
 SIFS = Short Interframe Space

# Terminal oculto

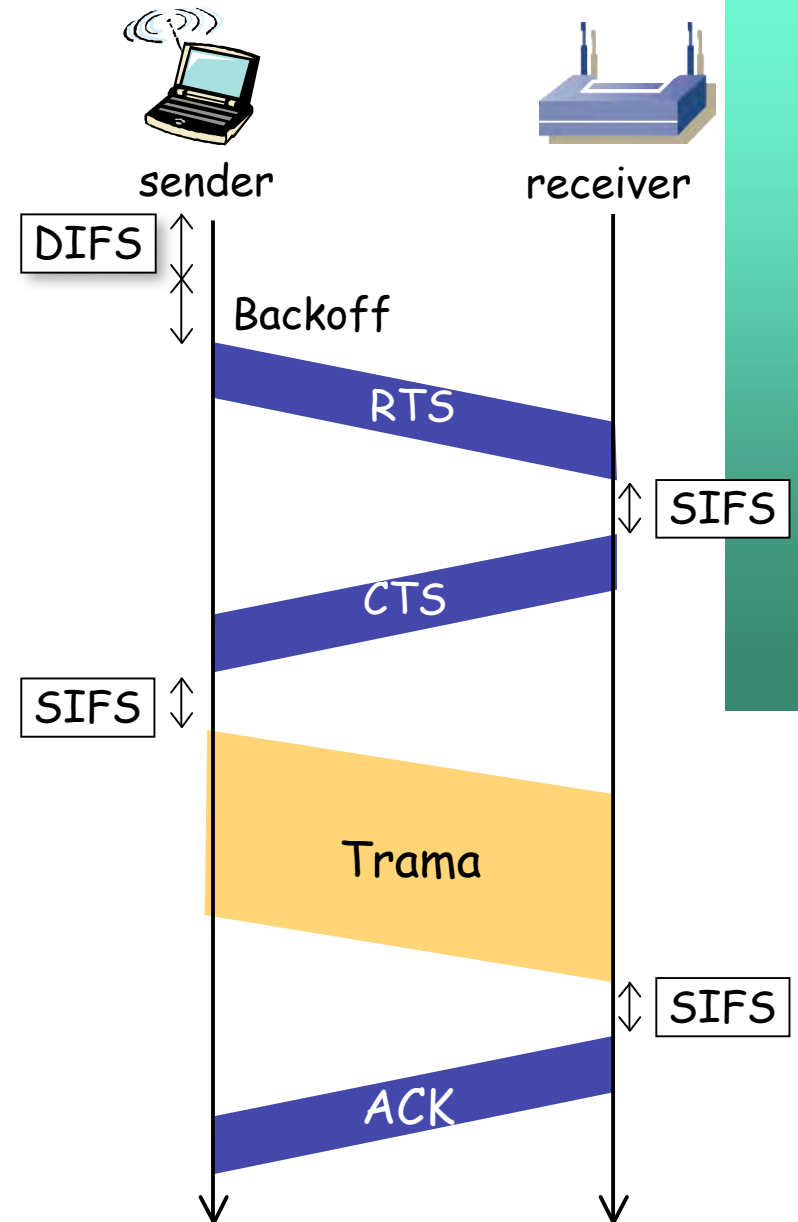
## Collision Avoidance

- Reservar previamente el canal con una trama corta (menor probabilidad de colisión)
- *Request-To-Send* (RTS) (puede colisionar)
- *Clear-To-Send* (CTS) (nadie más transmite)



# CSMA/CA

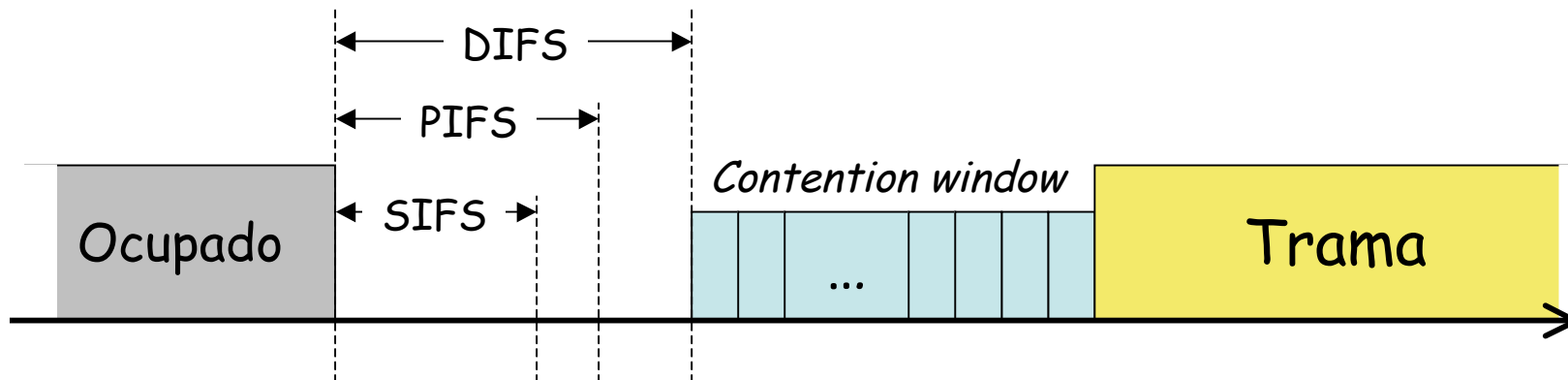
- DIFS > SIFS
- RTS/CTS consume capacidad
- Utilizado en entornos con frecuente contienda
- Generalmente solo para tramas grandes
- Throughput obtenible limitado
- Unos 4-6Mbps en 802.11b a 11Mbps
- Unos 30Mbps en 802.11g y 802.11a a 54Mbps





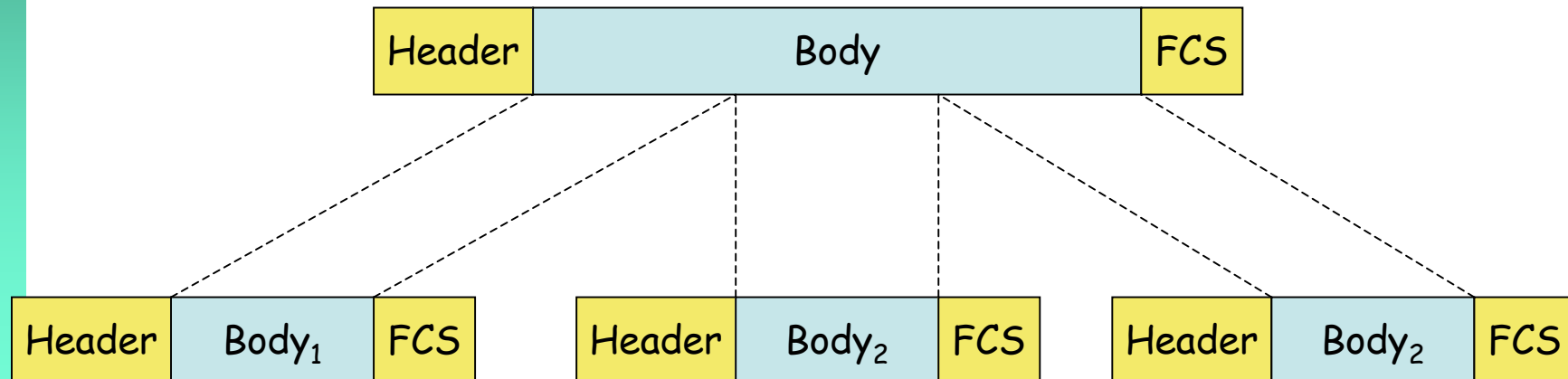
# Tiempos entre tramas

- SIFS = Short InterFrame Space
  - Tramas de la máxima prioridad
  - Al transcurrir SIFS  $\mu$ s puede empezar transmisión con lo que el medio pasa a estar ocupado
- PIFS = PCF InterFrame Space
- DIFS = DCF InterFrame Space
- EIFS = Extended InterFrame Space
  - No es un valor fijo
  - Empleado tras un error en la transmisión

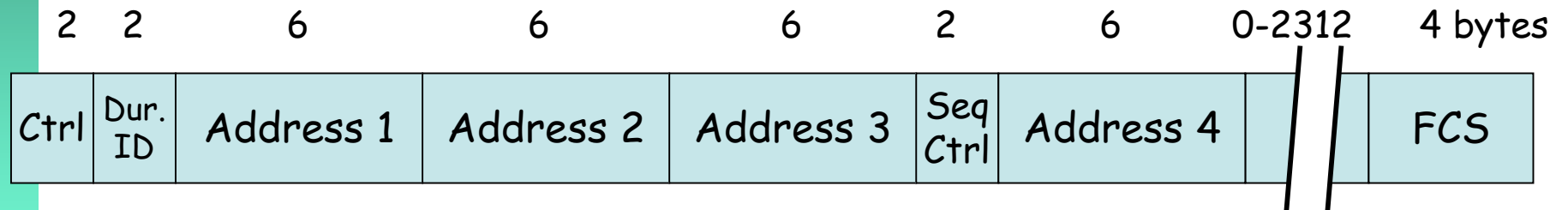


# Fragmentación

- Servicio ofrecido en el nivel de enlace
- Divide trama grande en más pequeñas
- Cada fragmento es confirmado por separado
- El transmisor no libera el medio hasta enviar todos los fragmentos
- Aumenta la fiabilidad en la transmisión
- Solo se aplica a tramas *unicast*
- Atención a las diferencias con la fragmentación en el nivel de red



# Formato de trama



# Frame Control field

## Protocol Version

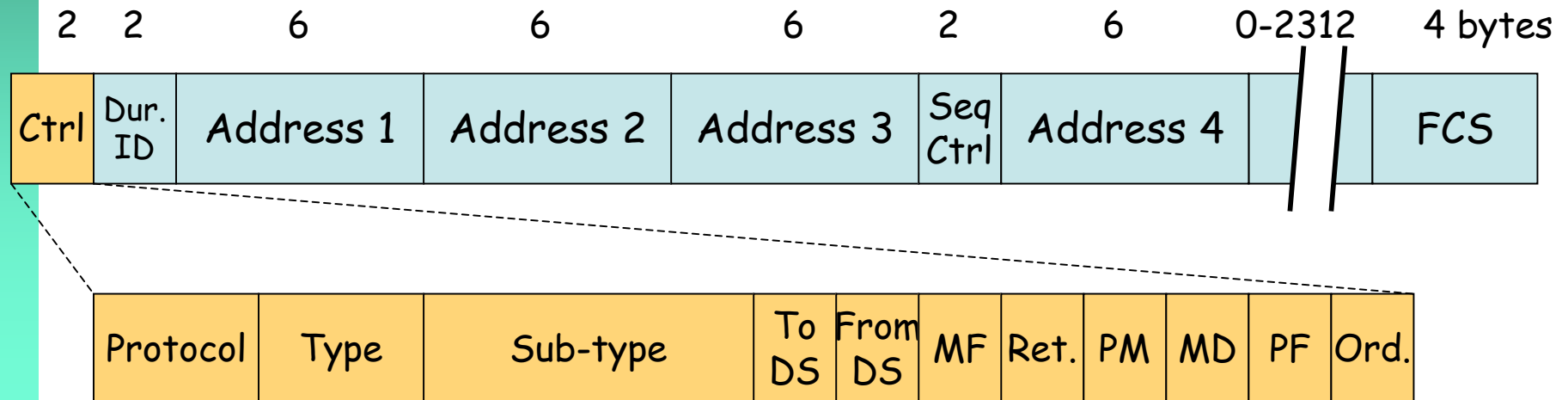
- Versión del 802.11 MAC (hoy hay solo uno de código 0)

## Type and Subtype fields

- Tipo de trama
- Hay varias tramas para gestión

## ToDS and FromDS

	ToDS=0	ToDS=1
From DS=0	Tramas de control. Datos en un IBSS	Datos destinados al DS
From DS=1	Datos originados en el DS	Datos en un <i>wireless bridge</i>



# Frame Control field

## More Fragments

- 0 en el último
- Normalmente se usa la MTU de Ethernet y no hay fragmentación

## Retry

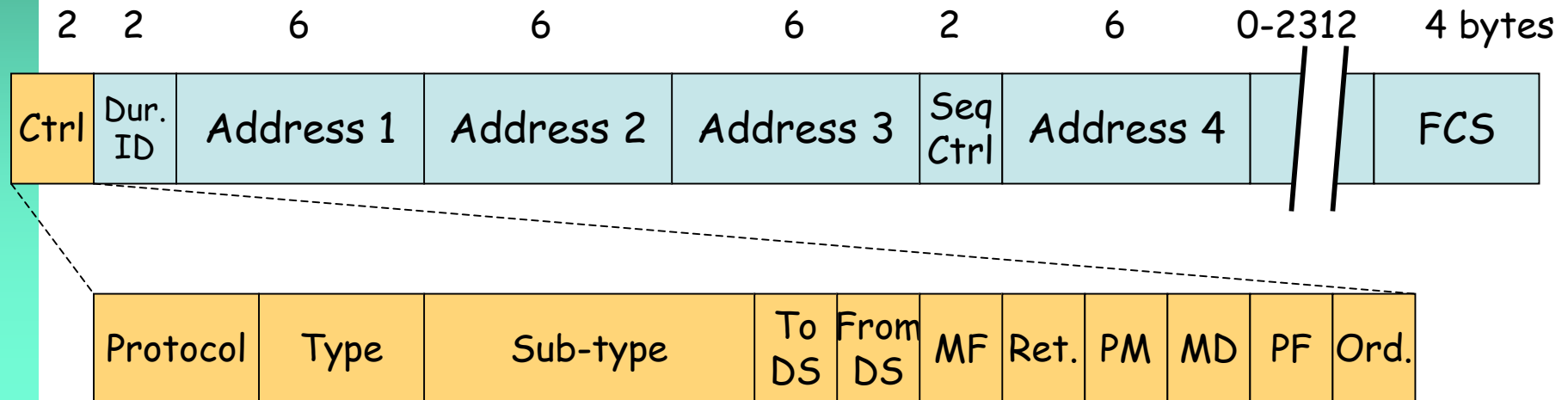
- Indica que es una retransmisión

## Power Management

- Indica (con 1) que tras esta trama la estación pondrá el interfaz en ahorro de energía

## More Data

- El AP indica a la estación que tiene más datos para ella, que no entre en ahorro de energía



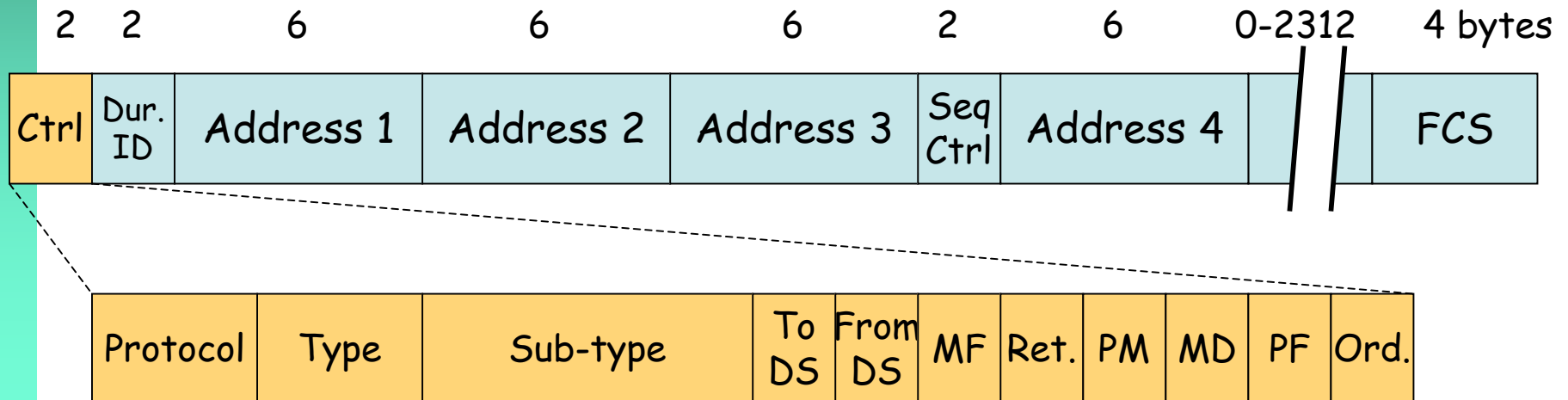
# Frame Control field

## Protected Frame

- Indica si la trama va encriptada en el nivel de enlace

## Order

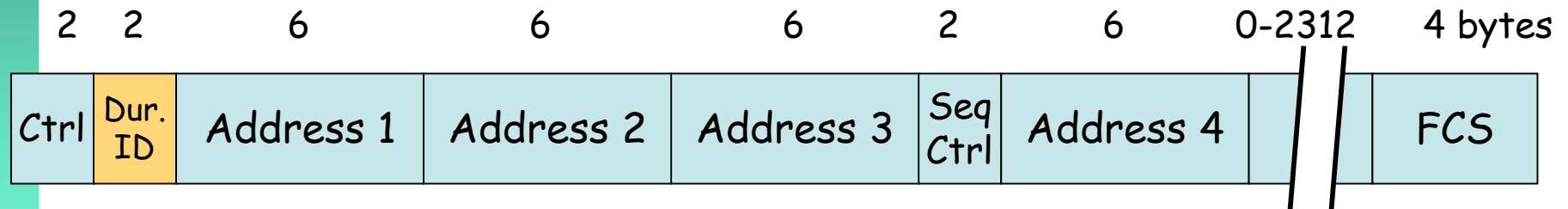
- Si se emplea ordenamiento estricto de las tramas



# Frame Control field

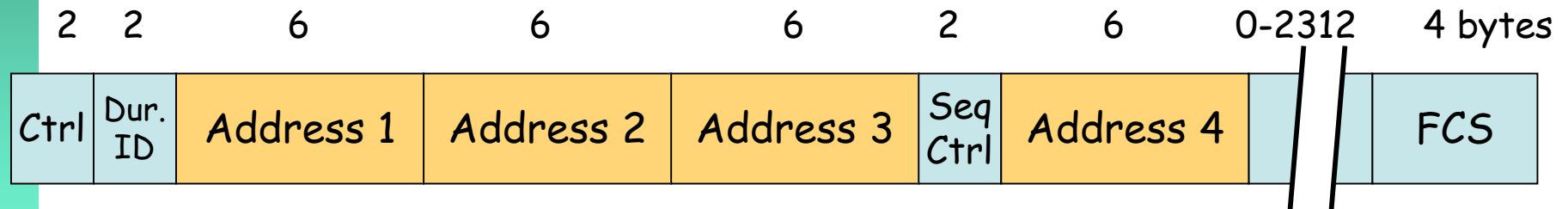
## Duration/ID

- Tiempo que el medio estará ocupado por la transmisión de la trama
- Una estación en ahorro de energía envía periódicamente una trama solicitando las tramas acumuladas en el AP para ella (entonces este campo es el ID de su asociación con el AP)



# Direcciones

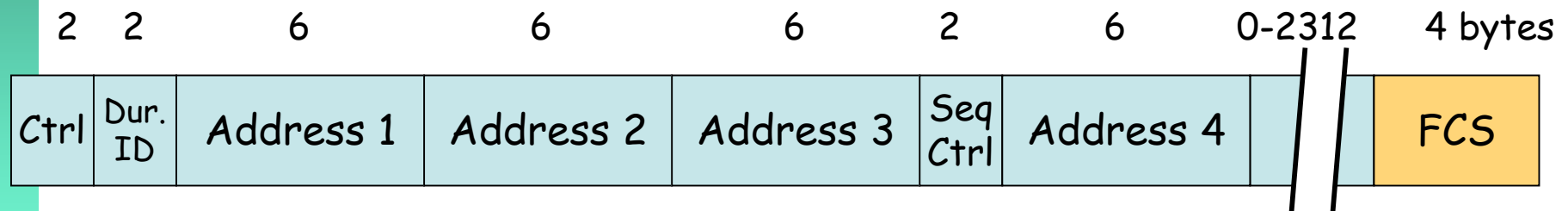
- Hasta 4 direcciones (depende del tipo de trama)
- Mismo espacio de direcciones que 802.3
- *BSSID*: MAC del interfaz Wi-Fi del AP identifica al BSS





# FCS

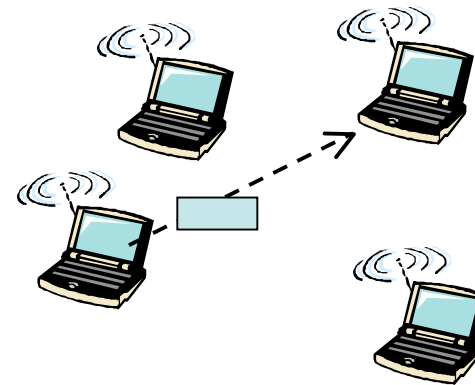
- Cyclyc Redundancy Check (CRC)
- Mismo método que en 802.3
- Como cambia la cabecera debe recalcularlo el AP



# Direcciones

## IBSS (Ad-hoc)

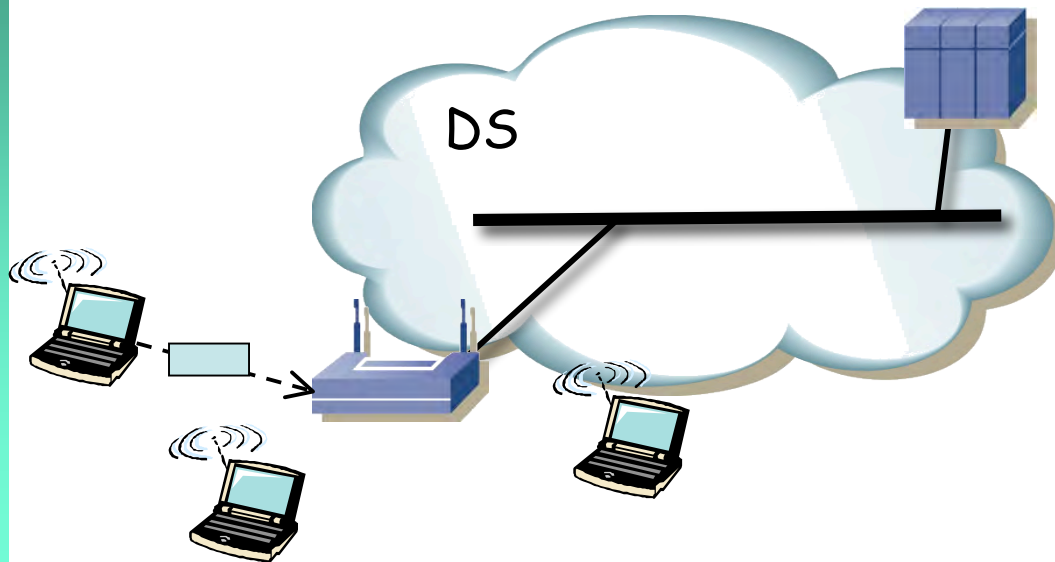
- ToDS = FromDS = 1
- Address 1 (receptor) = Dirección destino
- Address 2 (transmisor) = Dirección origen
- Address 3 = BSSID
- Address 4 = No usada



# Direcciones

## BSS

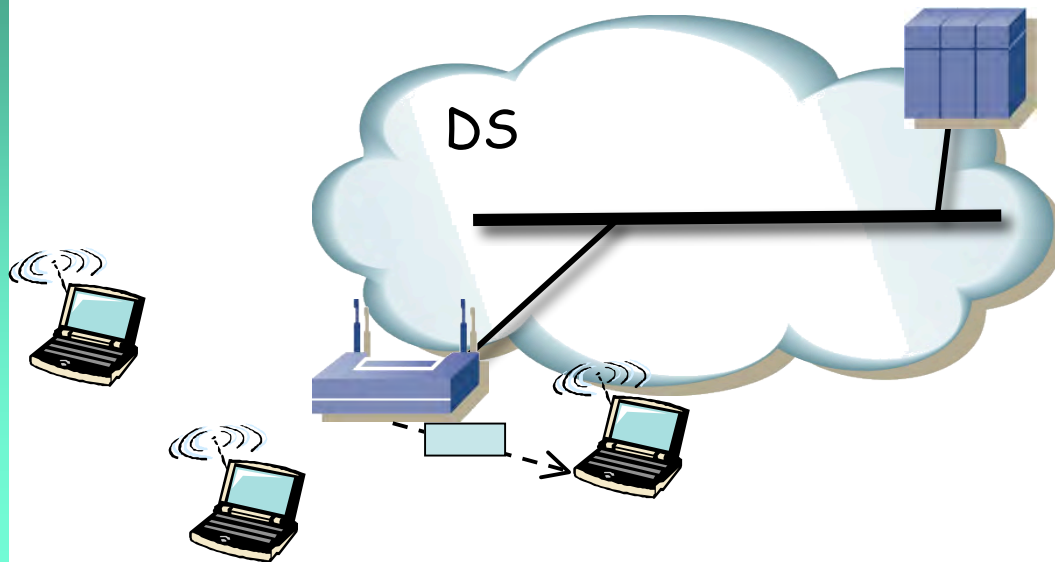
- Hacia el AP (ToDS = 1, FromDS = 0)
  - Address 1 (receptor) = BSSID
  - Address 2 (transmisor) = Dirección origen
  - Address 3 = Dirección destino (MAC estación destino)
  - Address 4 = No usada



# Direcciones

## BSS

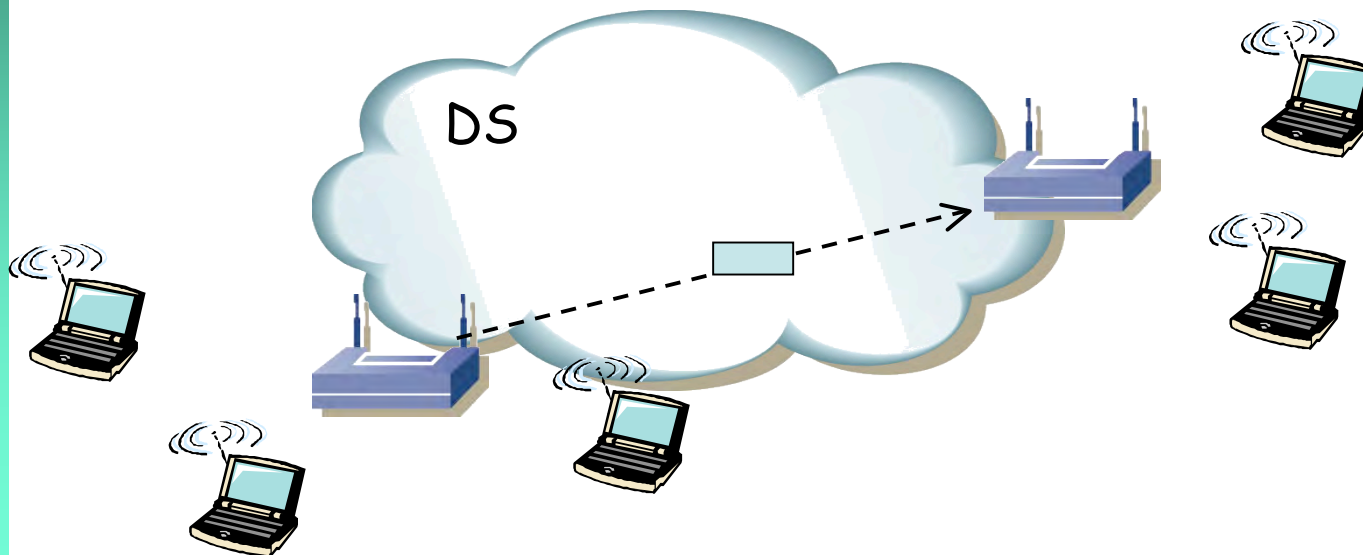
- Desde el AP (ToDS = 0, FromDS = 1)
  - Address 1 (receptor) = Dirección destino
  - Address 2 (transmisor) = BSSID
  - Address 3 = Dirección origen (MAC estación origen)
  - Address 4 = No usada



# Direcciones

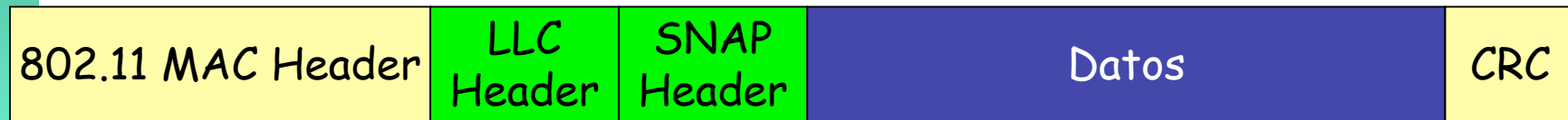
## BSS

- WDS (ToDS = 1, FromDS = 1)
  - Address 1 (receptor) = MAC AP destino
  - Address 2 (transmisor) = MAC AP origen
  - Address 3 = Dirección destino (MAC estación destino)
  - Address 4 = Dirección origen (MAC estación origen)



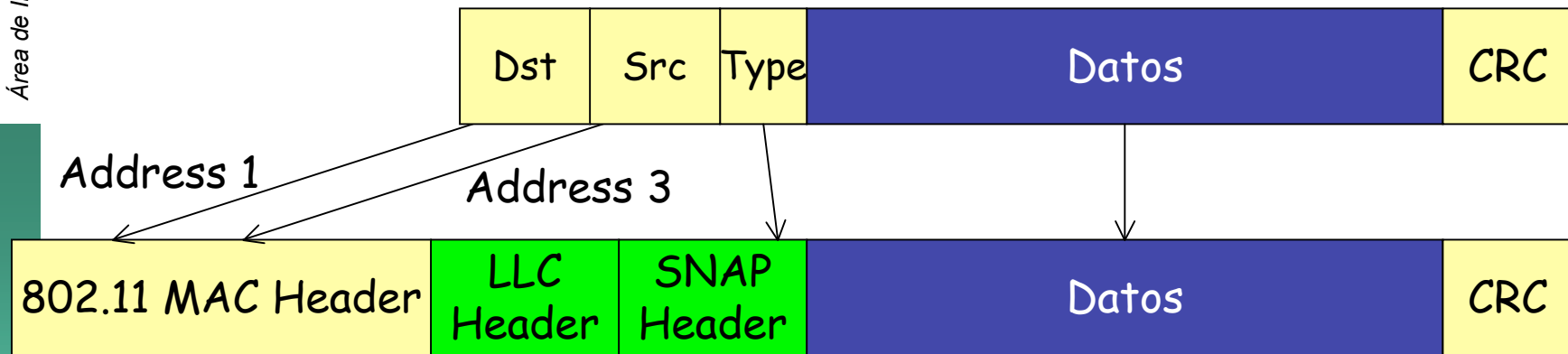
# Encapsulado

- Emplea LLC/SNAP
- Para paquetes IP dos alternativas
  - RFC 1042
  - IEEE 802.1H



# DS Ethernet

- Bridge DS → BSS

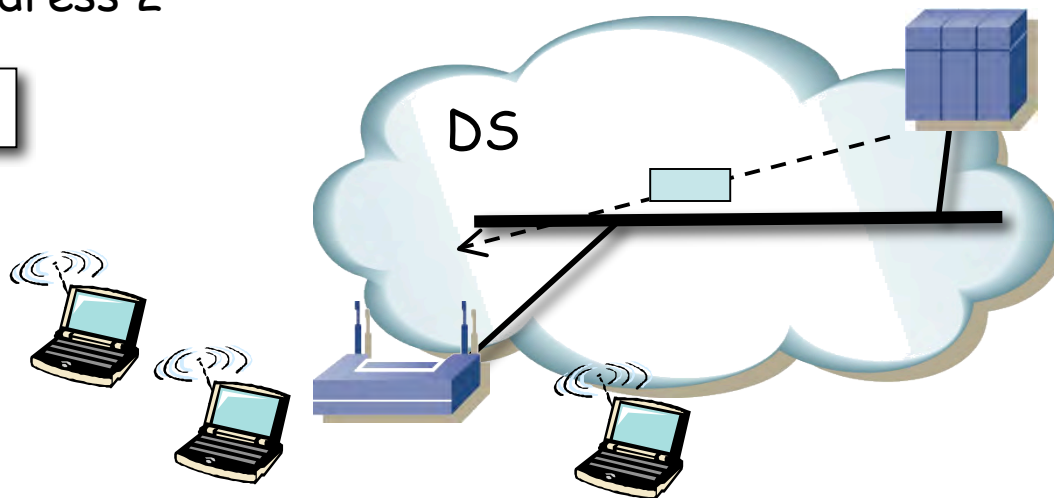


BSSID

Address 2

Address 1

Address 3



# PCF

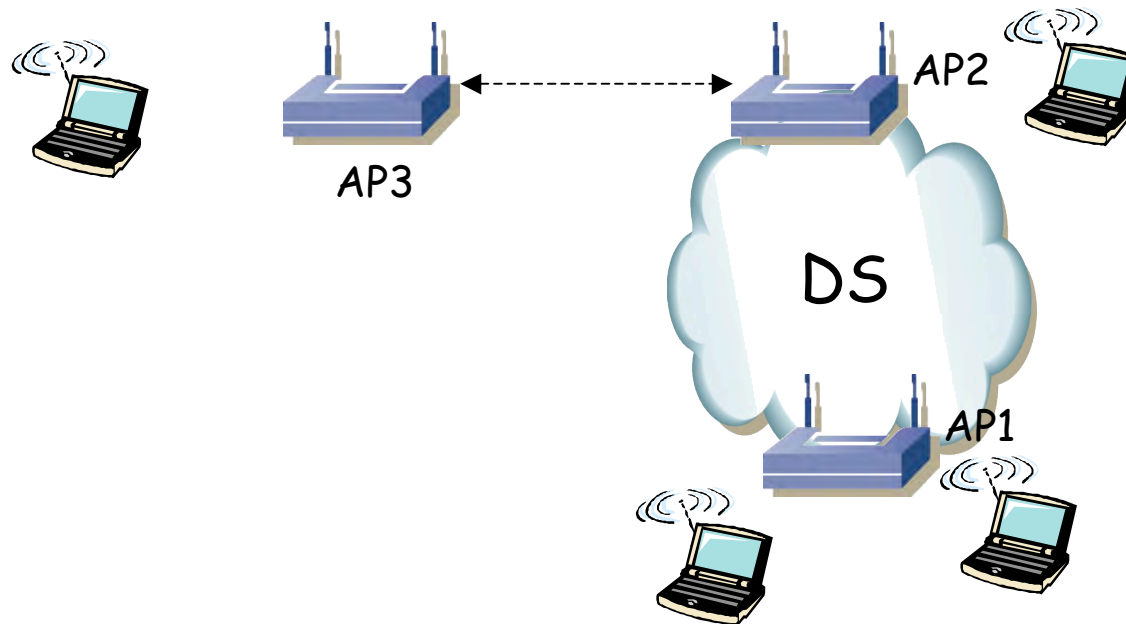
- *Point Coordination Function*
- Opcional
- Ofrece entrega de tramas sin contienda
- Solo para caso infraestructura (BSS)
- No implementada por la mayoría de los productos
- Funcionamiento:
  - En ciertos momentos comienza un *Contention Free Period (CFP)*
  - Marca el comienzo del CFP antes que una estación transmita con DCF porque emplea un tiempo menor (PIFS) de espera
  - El AP actuará enviando a las estaciones o solicitando tramas de ellas (*polling*)





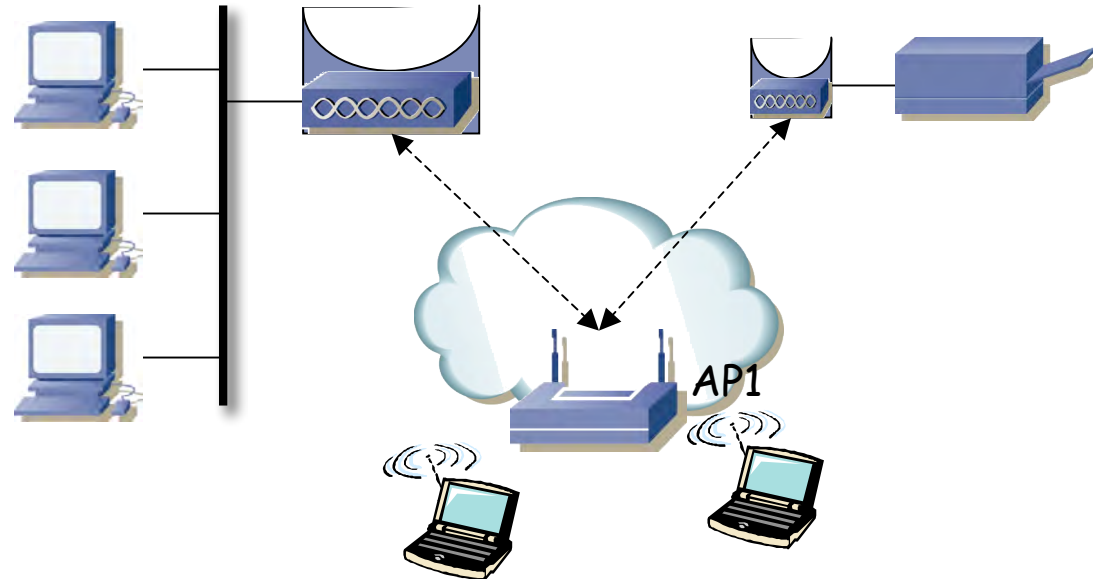
# Repeater AP

- AP que no puede conectarse al DS cableado
- Usuarios muy alejados llegan a AP3 pero no a AP2
- AP3 retransmite las tramas en el mismo canal
- Extiende el BSS y el dominio de colisión



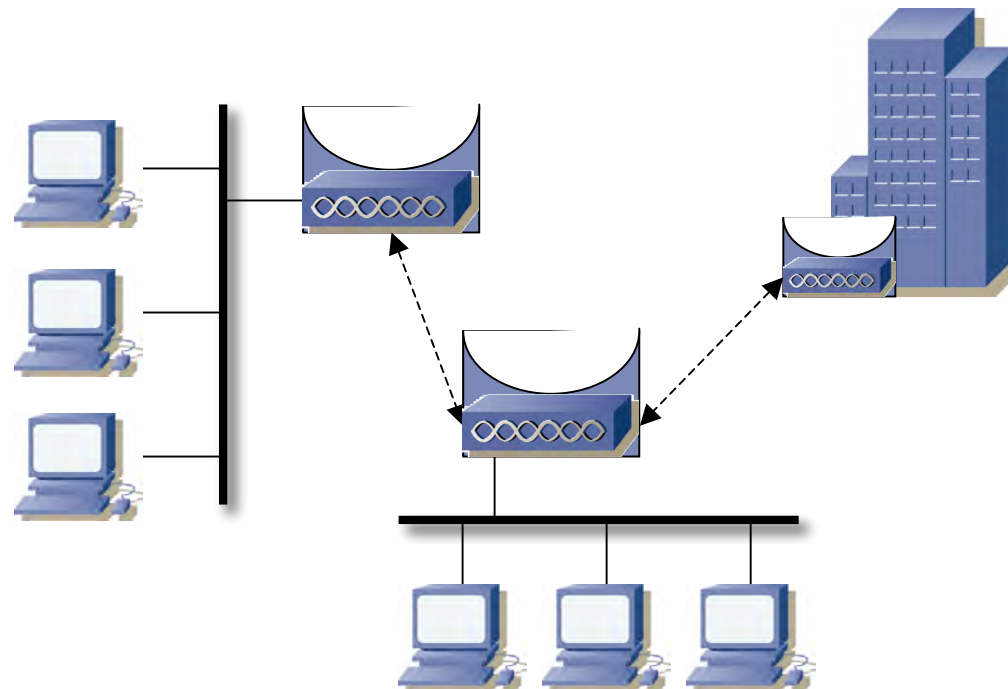
# Universal client / Workgroup bridge

- Incluir en la red inalámbrica dispositivos con interfaz alámbrico
- Alejados del DS
- *Universal Client*: Cuando se conecta un solo dispositivo
- *Workgroup Bridge*: Se conecta una pequeña red cableada



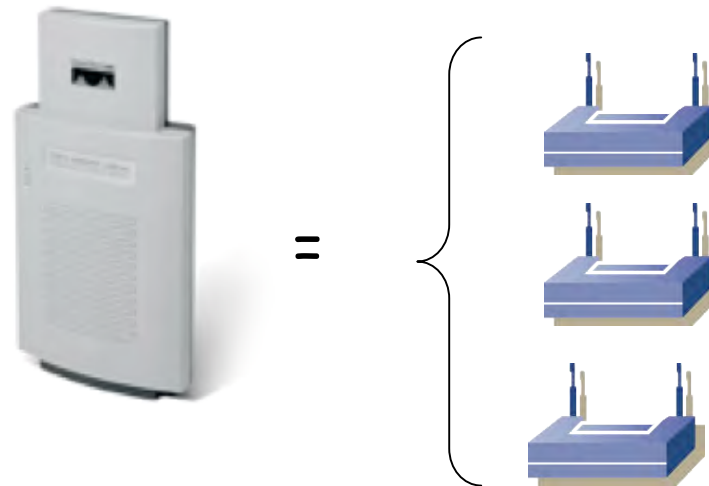
# Wireless Bridge

- Interconectar LANs mediante puentes
- Enlace entre los puentes es inalámbrico
- Generalmente redes grandes y distancias mayores de las habituales para WLAN
- Uno de los puentes actúa como AP y los otros como clientes



# Multi-BSS APs

- Circuitos integrados para 802.11 originalmente soportaba un solo BSS
- Hoy en día son capaces de gestionar más de uno, con diferente SSID
- *Virtual Access Points*



# Práctica 8

## *Configuración de Access Point y cliente WiFi*

- Parámetros de configuración de un AP comercial
- Configuración de cliente WiFi
- Router WiFi