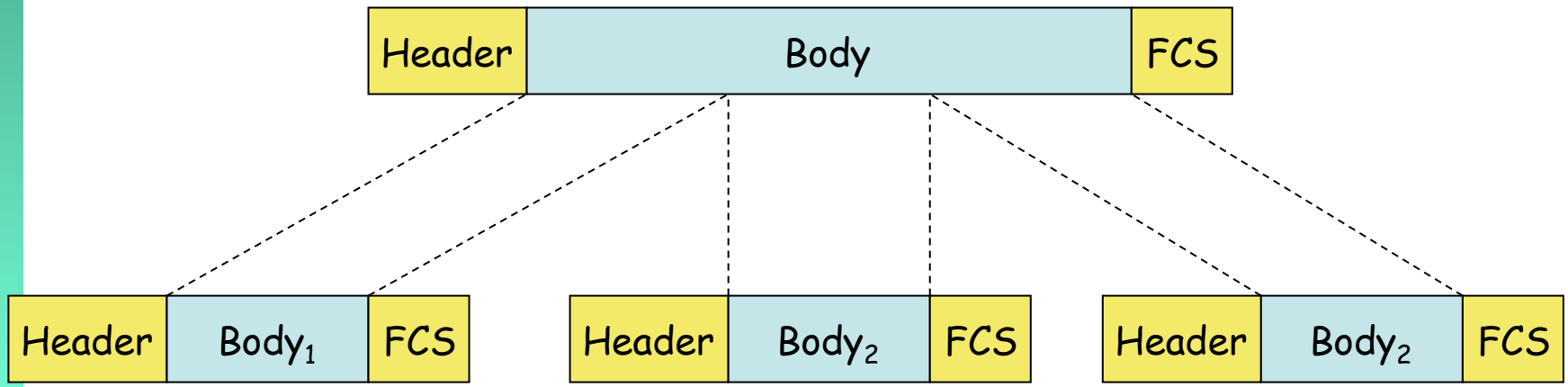
Tecnologías Wi-Fi (y 2)

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

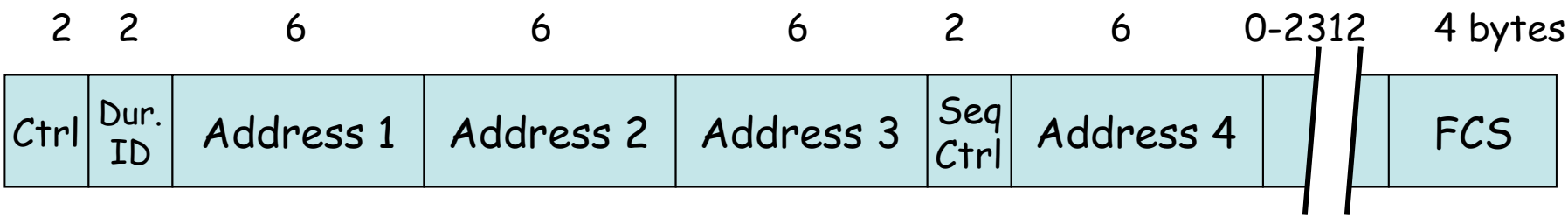
Redes de Banda Ancha
5º Ingeniería de Telecomunicación

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 las tramas



Frame Control field

Protocol Version

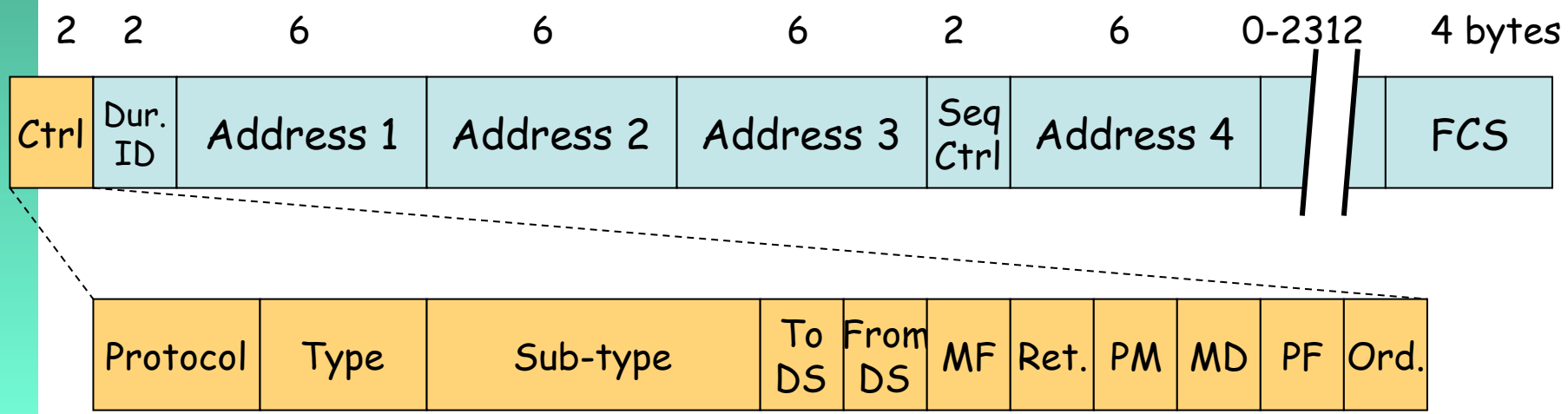
- Versión del 802.11 MAC (hoy hay solo uno de código 0)

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 *wireless bridge*



Frame Control field

More Fragments

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

Retry

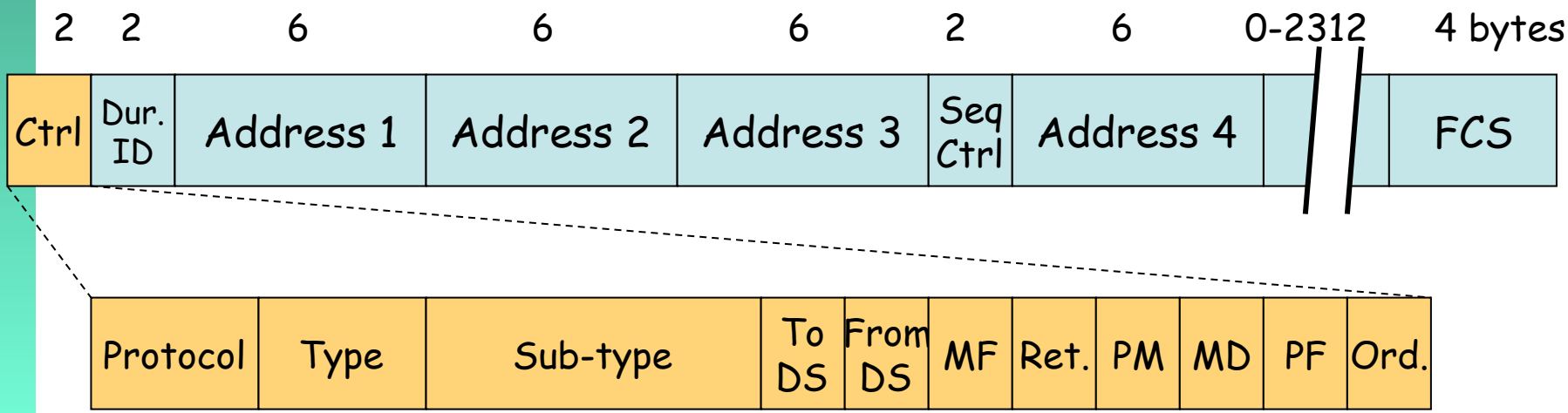
- Indica que es una retransmisión

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



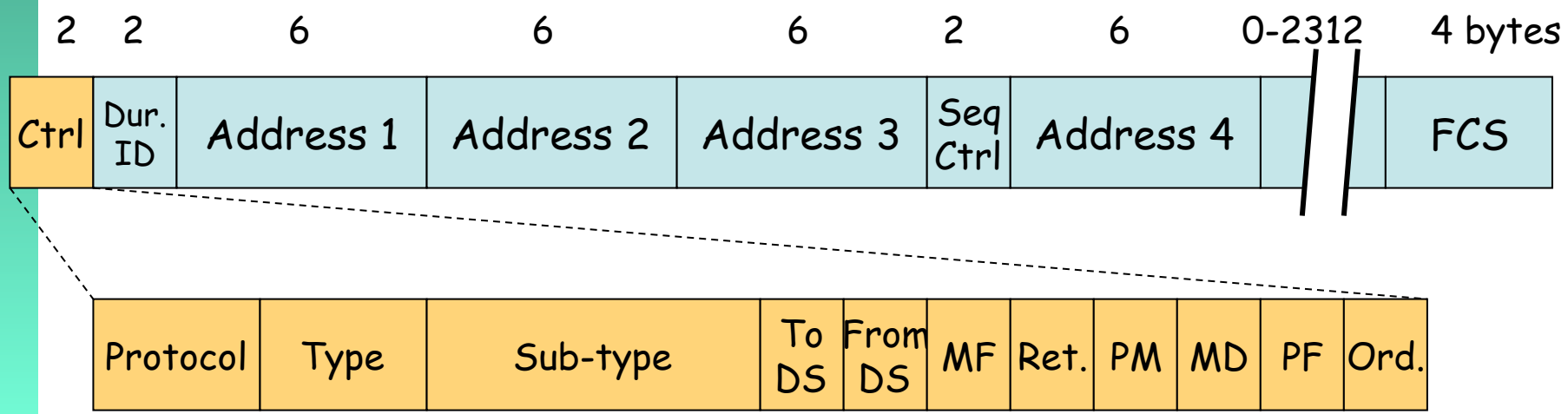
Frame Control field

Protected Frame

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

Order

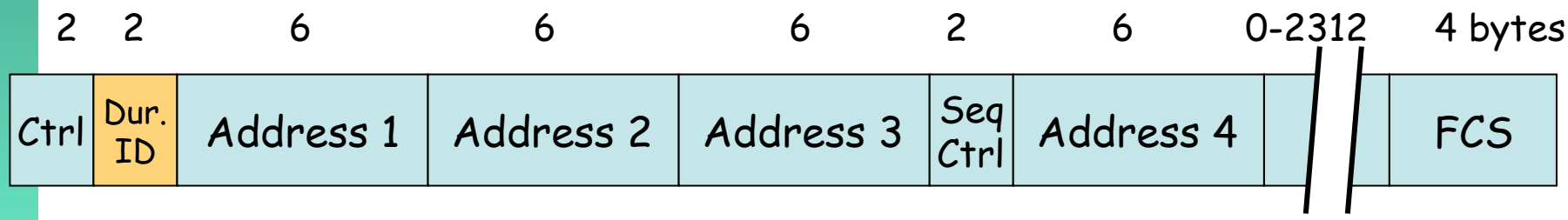
- Si se emplea ordenamiento estricto de las tramas



Frame Control field

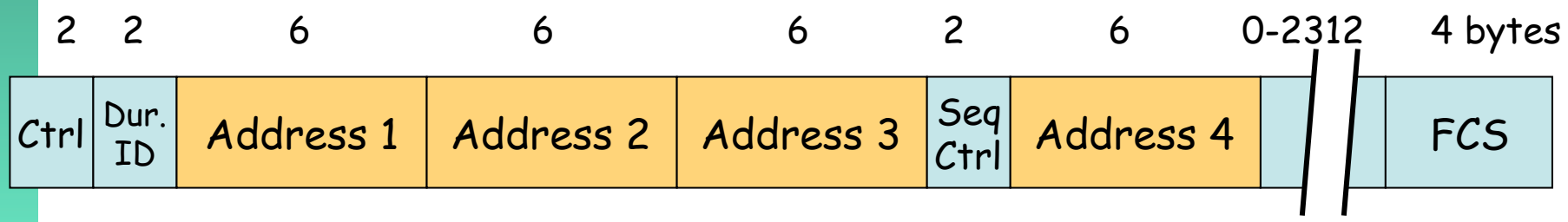
Duration/ID

- 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)



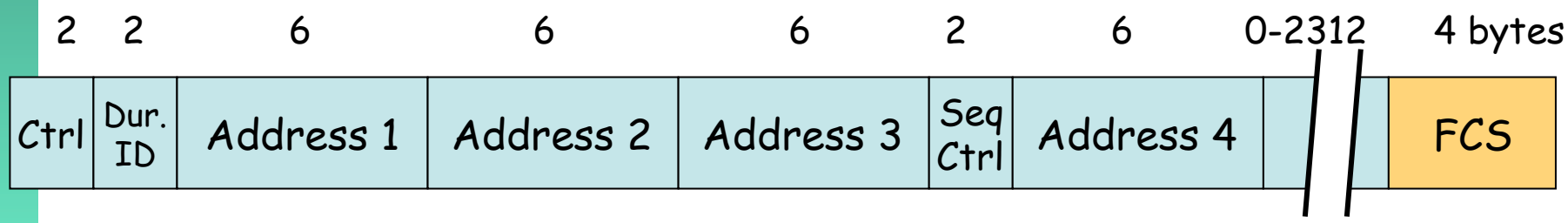
Direcciones

- 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

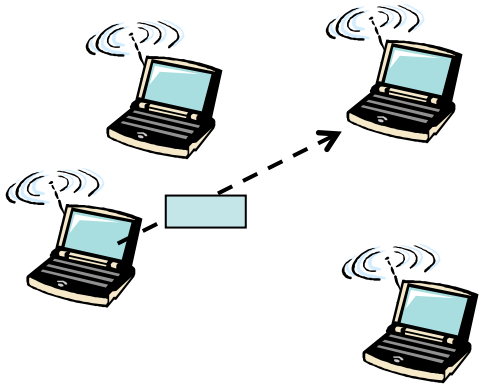
- Cyclic Redundancy Check (CRC)
- Mismo método que en 802.3
- Como cambia la cabecera debe recalcularlo el AP



Direcciones

IBSS (Ah-hoc)

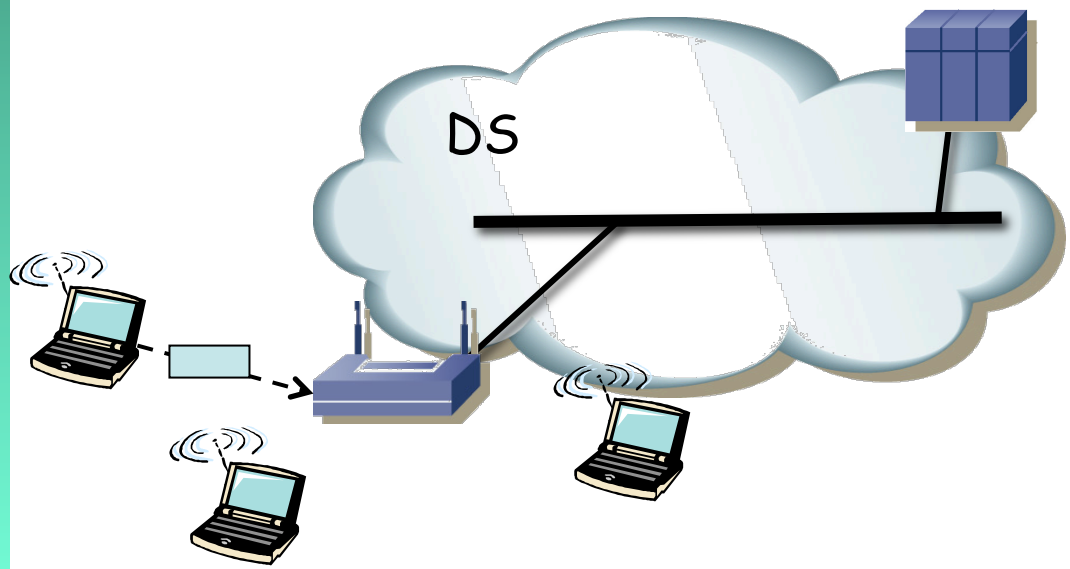
- ToDS = FromDS = 0
- Address 1 (receptor) = Dirección destino
- Address 2 (transmisor) = Dirección origen
- Address 3 = BSSID
- Address 4 = No usada



Direcciones

BSS

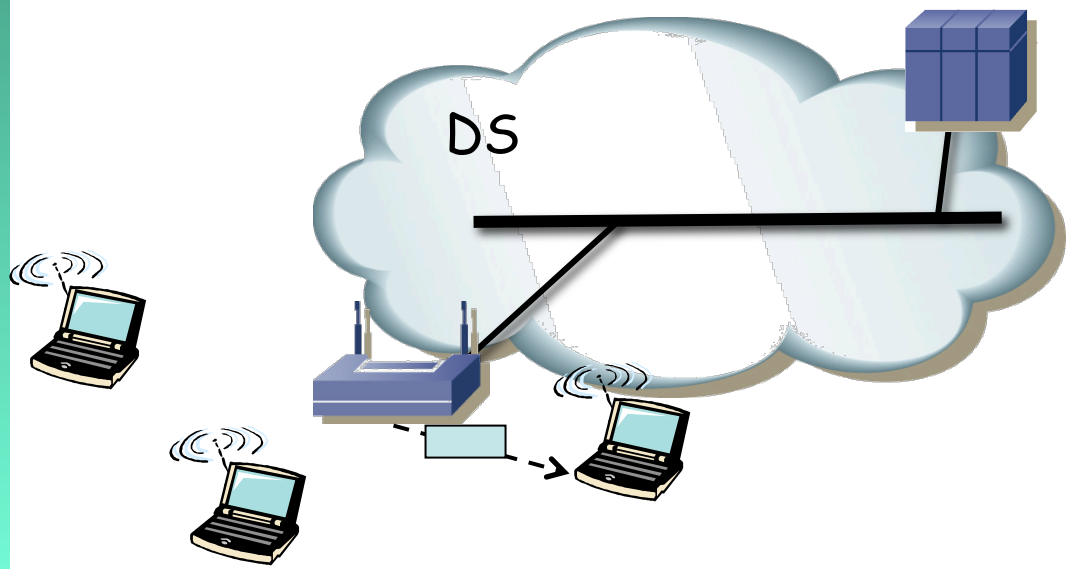
- Hacia el AP (ToDS = 1, FromDS = 0)
  - Address 1 (receptor) = BSSID
  - Address 2 (transmisor) = Dirección origen
  - Address 3 = Dirección destino (MAC estación destino)
  - Address 4 = No usada



Direcciones

BSS

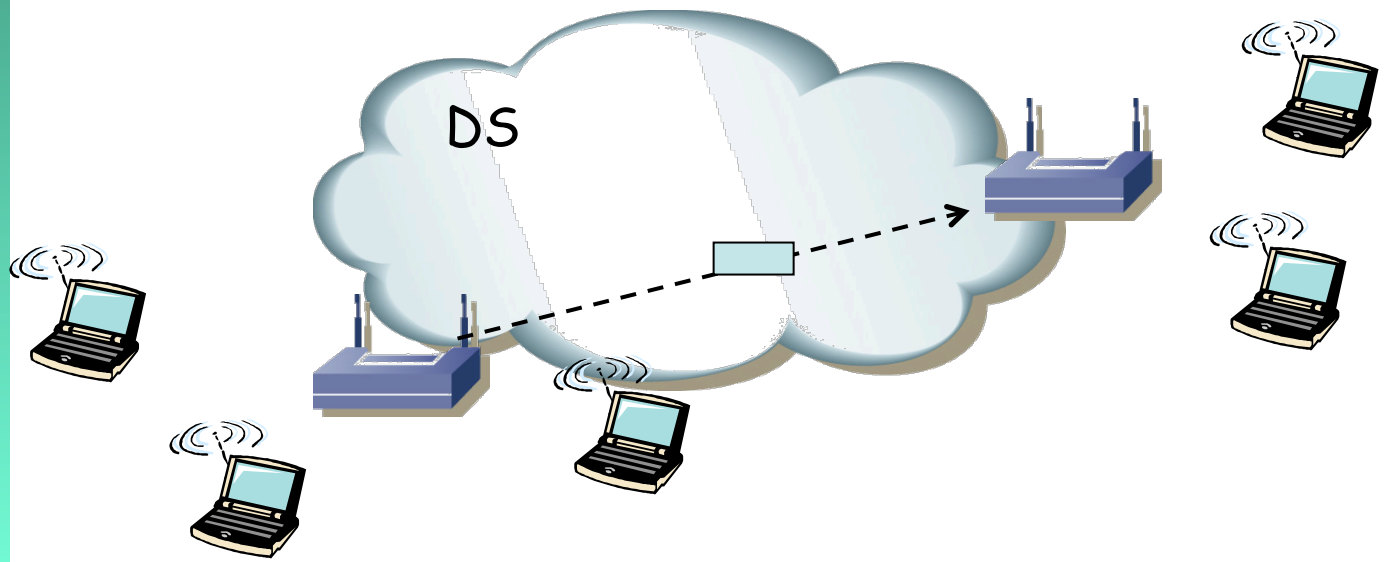
- Desde el AP (ToDS = 0, FromDS = 1)
  - Address 1 (receptor) = Dirección destino
  - Address 2 (transmisor) = BSSID
  - Address 3 = Dirección origen (MAC estación origen)
  - Address 4 = No usada



Direcciones

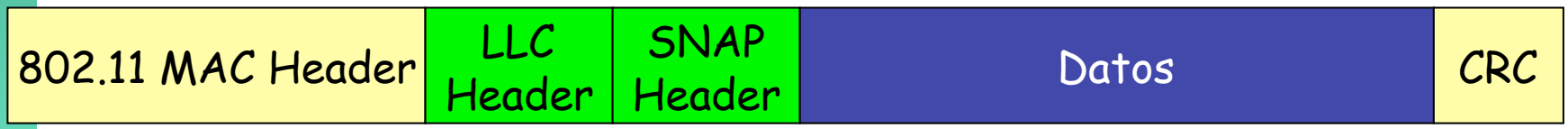
BSS

- 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)



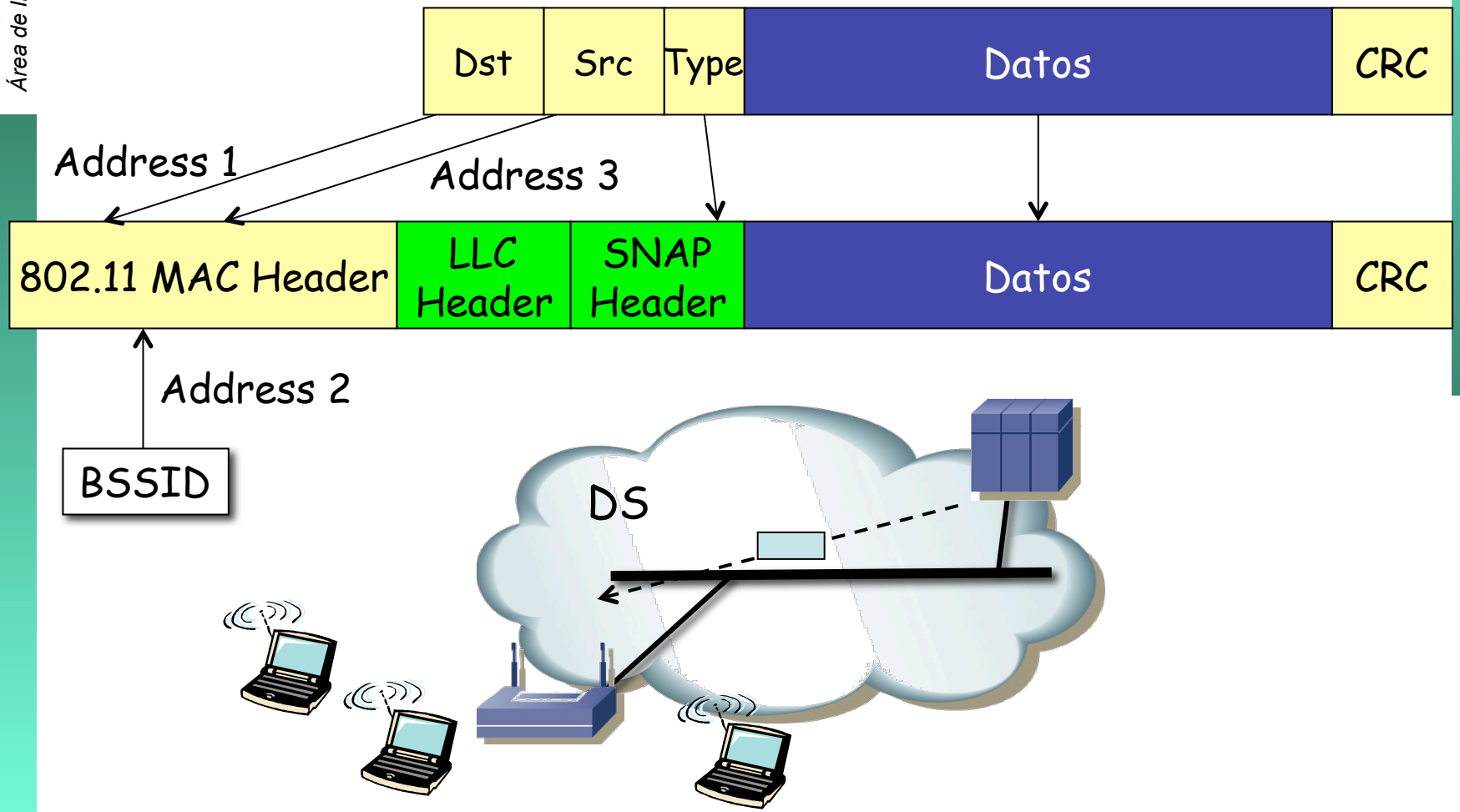
Encapsulado

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



DS Ethernet

- Bridge DS → BSS

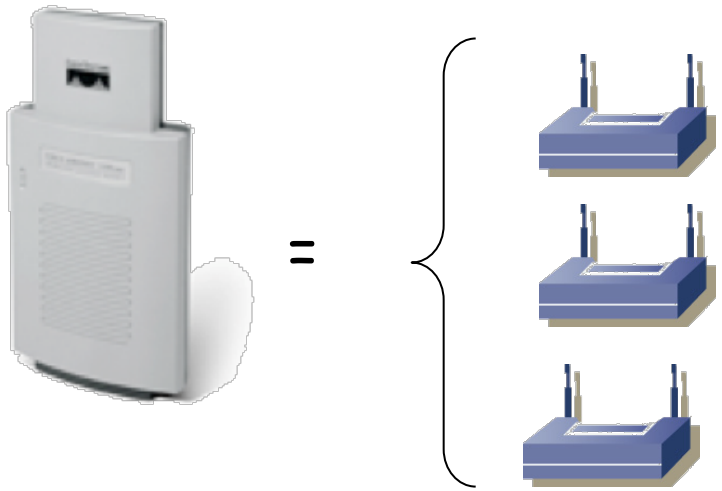


PCF

- *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*)

Multi-BSS APs

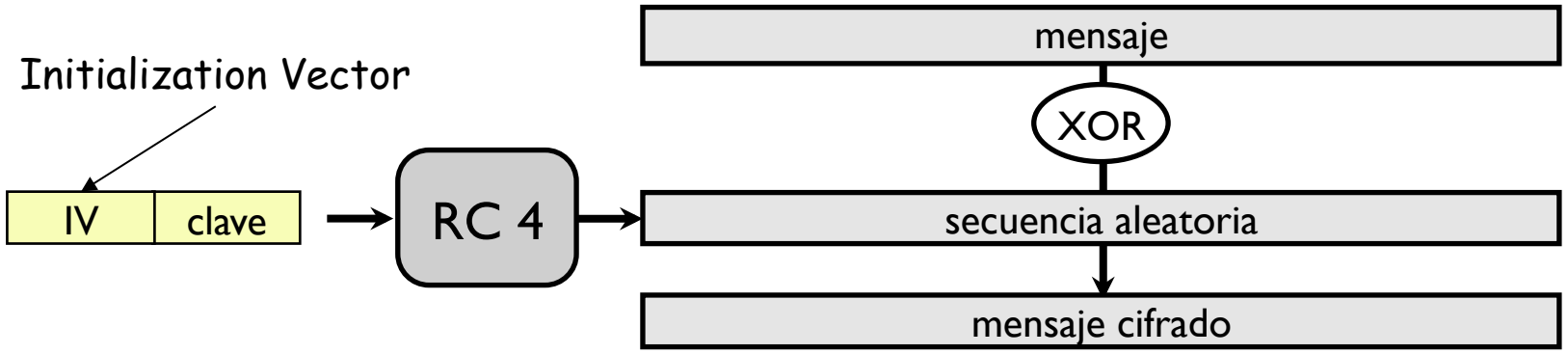
- Circuitos integrados para 802.11 originalmente soportaba un solo BSS
- Hoy en día son capaces de gestionar más de uno, con diferente SSID
- *Virtual Access Points*



Seguridad en WiFi

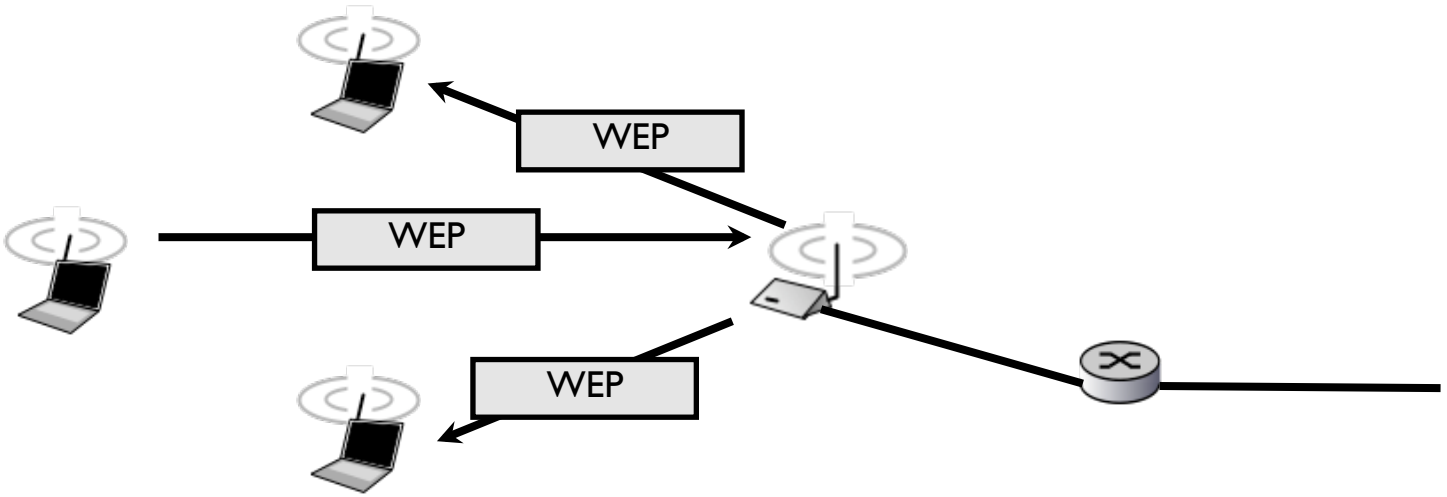
Wired Equivalent Privacy (WEP)

- Conseguir el mismo nivel de privacidad que en una red de cable
- Proteger la confidencialidad de los datos (cifrarlos)
- Proteger la integridad de los mensajes
- Se utiliza el algoritmo de cifrado RC4 (tipo clave secreta)
- Serie pseudo-aleatoria a partir de la clave secreta (40 ó 104 bits)
- El mensaje se cifra con una clave de la misma longitud que el mensaje pero que depende de la clave original
- Intenta un cifrado de Vernan: cifrar con una secuencia aleatoria tan larga como el mensaje
- Algoritmo RC4 es un generador de secuencia pseudoaleatoria a partir de una semilla
- "IV" diferente para cada trama, va con ella en claro (24 bits)



WEP

- Enviando con WEP
  - El terminal calcula CRC y cifra el paquete con WEP
  - El paquete se envía al access point
  - El access point lo descifra y si el CRC es inválido lo tira
  - El access point puede cifrarlo con otro IV y enviarlo



- Un intruso
  - No puede descifrar los paquetes que le llegan
  - No puede generar paquetes válidos para otros

Vulnerabilidades de WEP

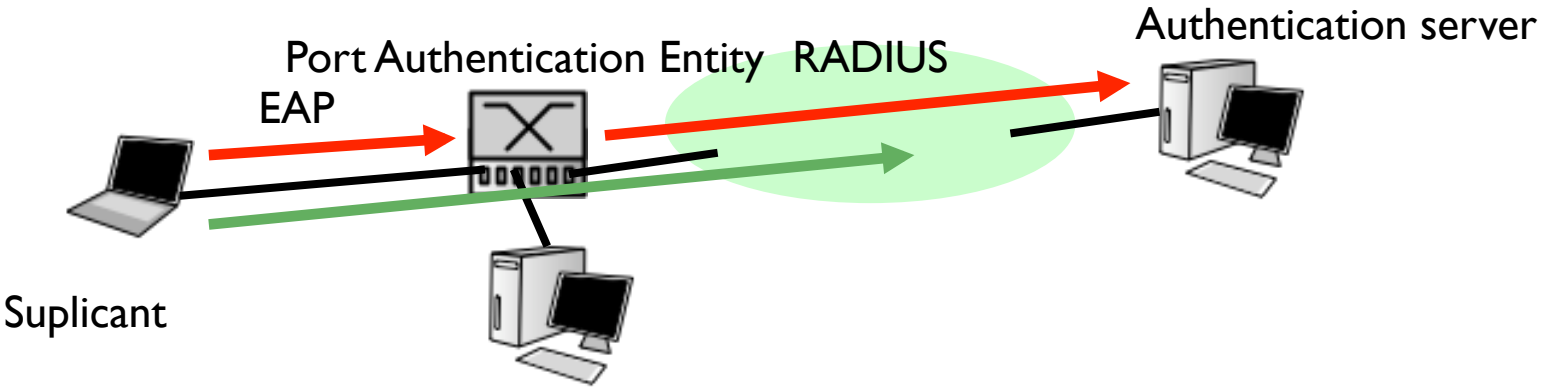
- Contra la confidencialidad
  - La clave se reutiliza (IV de 24 bits, solo hay que esperar 16.777.216 paquetes para que se repita)
  - RC4 tiene claves débiles: Algunos IVs generan claves en las que ciertas partes de la clave secuencia dependen solo de unos pocos bits de la clave original
  - Ataques de fuerza bruta (el secreto compartido depende de una clave introducida por el usuario)
- Contra la integridad
  - El CRC que se usa fue diseñado para detectar errores no para integridad así que no es un buen hash
  - No hay protección contra inyección de paquetes
  - Si repito un paquete que veo en el canal sigue siendo un paquete valido
- Contra la autentificación
  - Autentificación falsa
  - Ataques de desautentificación

Mejorando confidencialidad

- 802.11i, estándar del IEEE sobre seguridad mejorada en redes 802.11
- Añade:
  - Autentificación basada en 802.1x
  - 2 nuevos protocolos de cifrado para sustituir a WEP:
    - TKIP: protocolo basado en RC4 pero corrigiendo los problemas de WEP (iba a ser WEP2)
      - Fácil de cambiar en hardware que ya soporte WEP
    - CCMP: protocolo completamente rediseñado para nuevo hardware, basado en AES

Autentificación en 802.1x

- Ya había un estandar del IEEE para la autentificación en redes de tipo Ethernet (parte de 802.1)
- Arquitectura de autentificación 802.1x



  - El conmutador sólo acepta el tráfico 802.1x del suplicante
  - El suplicante se autentifica usando EAP en el servidor de autentificación
    - EAP over LAN : EAPOL para transmitir EAP en ethernet
    - el conmutador utiliza RADIUS para verificar la autenticación
  - Tras completar el proceso el PAE acepta todo el tráfico del suplicante

Comercialmente

- Nombres de la WiFi alliance para los equipos reales
- WPA (WiFi Protected Access)
  - Nombre comercial de TKIP
  - Se definió a partir del borrador de 802.11i cuando aún se trabajaba en el estándar
  - TKIP se implementó antes debido a que estaba basado en el hardware de WEP
- WPA2
  - 802.11i, con CCMP
- Ambos tienen dos formas de funcionamiento
  - WPA personal
    - Basado en secreto compartido (las claves se calculan a partir de una clave definida en los BSS y en los PCs)
  - WPA enterprise
    - Clave basada en TLS y certificados