

Tema 7: Nivel de enlace de datos



Objetivos

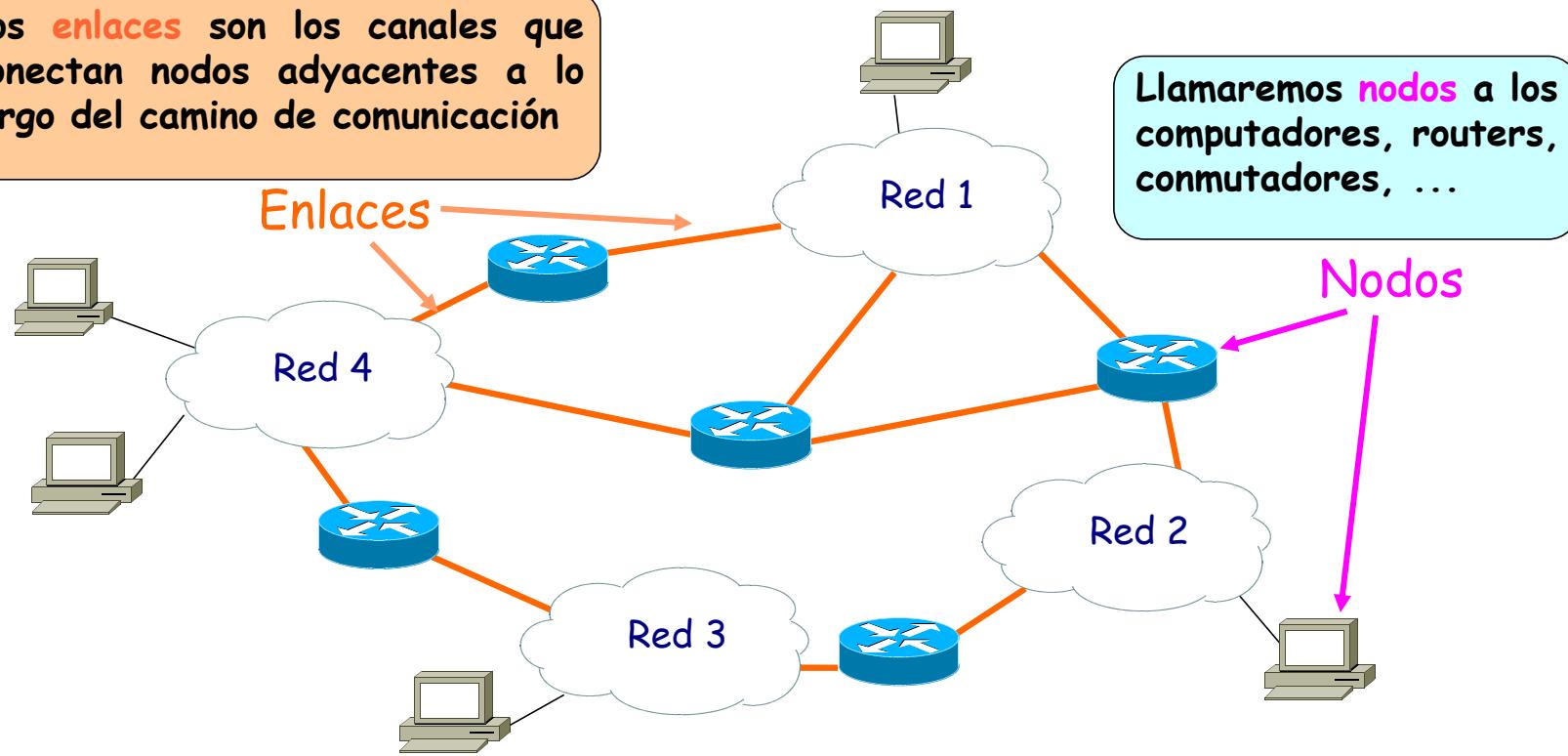
- Describir los servicios que **puede** ofrecer un protocolo de enlace de datos
- Diferenciar los métodos para la detección y corrección de errores
- Analizar los protocolos de acceso al medio en enlaces de difusión
- Justificar la necesidad del direccionamiento a nivel de enlace
- Describir el funcionamiento de las principales tecnologías de redes de área local (LANs): ámbito de aplicación y topologías
- Describir los estándares de redes de área local más utilizados: IEEE 802.3 (ethernet) e IEEE 802.11 (wi-fi)
- Describir los conceptos básicos sobre la interconexión de LANs y diferenciar los principales dispositivos de interconexión

Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

Terminología

Los **enlaces** son los canales que conectan nodos adyacentes a lo largo del camino de comunicación



El **nivel de enlace** tiene la responsabilidad de transferir datos desde un nodo al nodo adyacente a través del enlace que los une

Comparación entre niveles

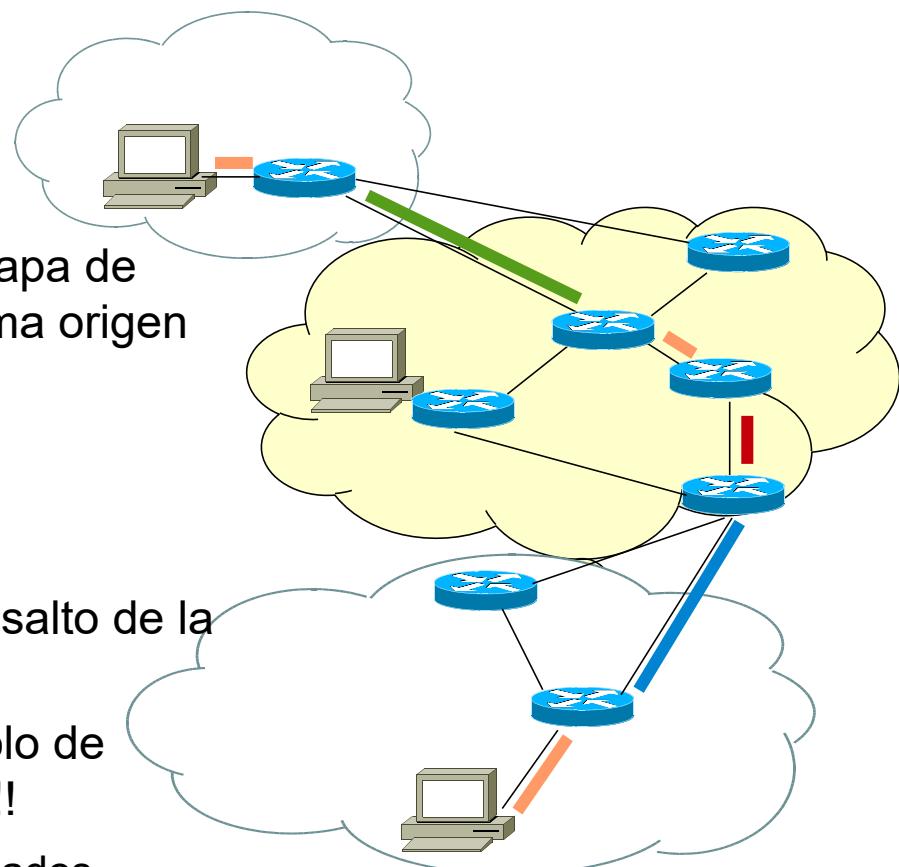
- Tarea que realiza:

- **Capa de red:**

- **De extremo a extremo**
 - Mover segmentos de la capa de transporte desde el sistema origen hasta el sistema destino

- **Capa de enlace:**

- **De nodo a nodo**
 - Cómo enviar en cada salto de la ruta
 - ¡¡En cada salto el protocolo de enlace puede ser distinto!!
 - Los servicios proporcionados también

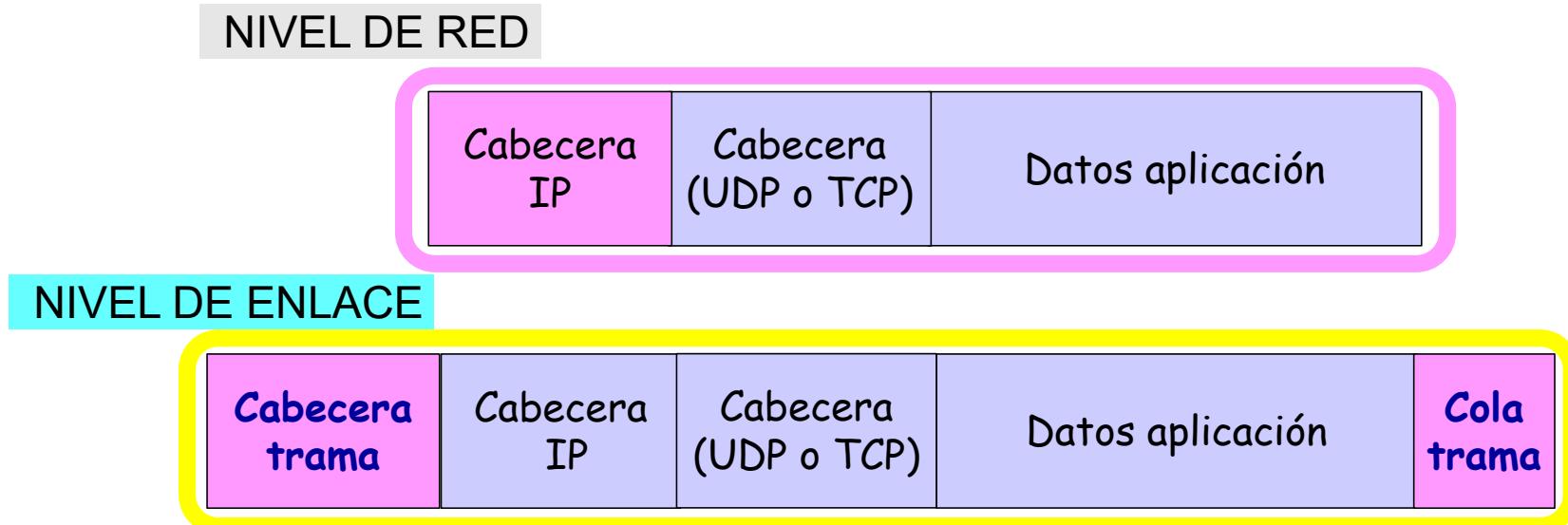


Capa de enlace: contexto

- Capa lógica por debajo del nivel de red y por encima del nivel físico
- Principal objetivo:
 - Conseguir **comunicación eficiente entre dos nodos directamente conectados**
- Cada protocolo de enlace puede proporcionar servicios diferentes
 - Ejemplo: puede o no proveer transferencia fiable sobre el enlace
- Unidad de transferencia: **trama**

Encapsulamiento de un datagrama

- Los datagramas IP se encapsulan en **tramas**



Servicios de la capa de enlace (I)

- Puede ofrecer:
 - Delimitación de la trama
 - El formato de la trama depende del protocolo de enlace utilizado
 - Control de flujo
 - Ajustar velocidades entre transmisor y receptor adyacentes
 - Gestión del canal
 - Acceso al medio
 - Define las reglas para poder transmitir una trama en el enlace
 - Trivial en un medio no compartido
 - Complejo en un enlace compartido
 - Comunicación simplex, half-duplex y full-duplex

Full-duplex, Half-duplex, simplex

Quien puede usar el medio de transmisión en un instante dado:

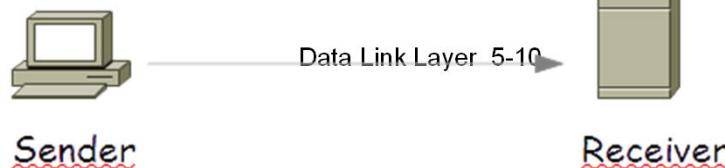
- full-duplex



- half-duplex



- simplex

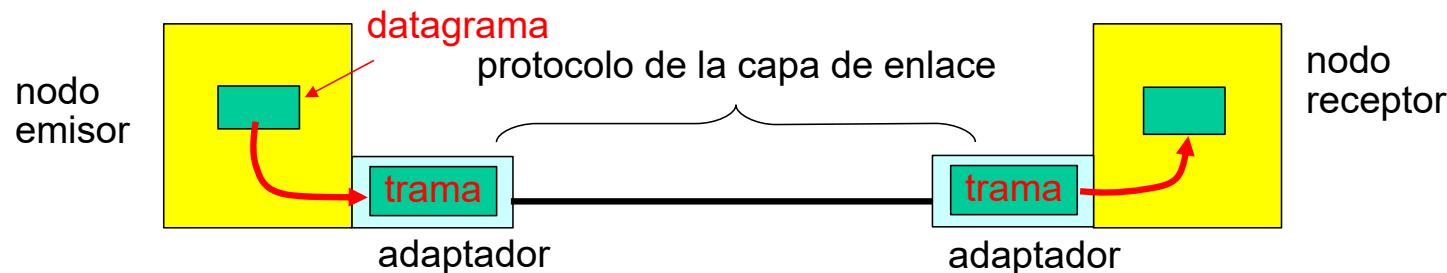


Servicios de la capa de enlace (II)

- Detección de errores
 - Mecanismos para detectar/corregir errores en los bits transmitidos
 - Usualmente, algoritmos sofisticados e implementados en hardware
- Entrega segura
 - Dos opciones para la corrección de errores:
 - Se detecta y corrige el error sin retransmitir la trama
 - El error se corrige mediante retransmisión
 - ¿Vale la pena duplicar este servicio (nivel enlace y red)?
 - No suele usarse si la tasa de error es baja (ej. Fibra óptica)

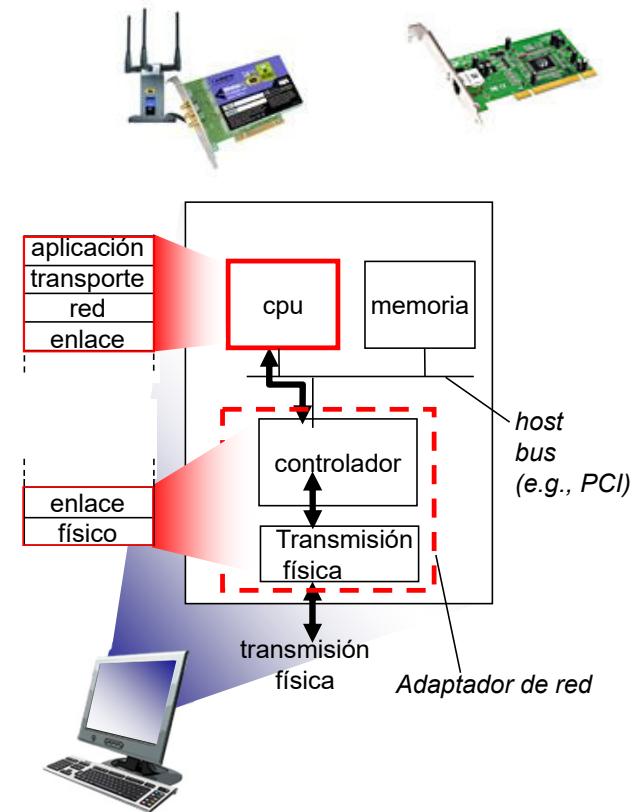
¿Dónde se implementa la capa de enlace?

- En **todos** los hosts
- En un **adaptador de red**, también denominado tarjeta de interfaz de red o NIC (*Network Interface Card*), o en un chip
 - Implementa las capas de enlace de datos y capa física
- El adaptador de red encapsula el datagrama en una trama y lo transmite por el enlace



Adaptador de red

- Muchas veces se integra en la placa base
 - Físicamente, forma parte del nodo
 - Comparte con el nodo la alimentación y los buses y está bajo su control
 - La capa de red delega completamente en el adaptador la tarea de transmitir el datagrama a través del enlace
 - Se encarga de (si el protocolo de enlace proporciona ese servicio):
 - Control de error
 - Entrega segura
 - Acceso al medio

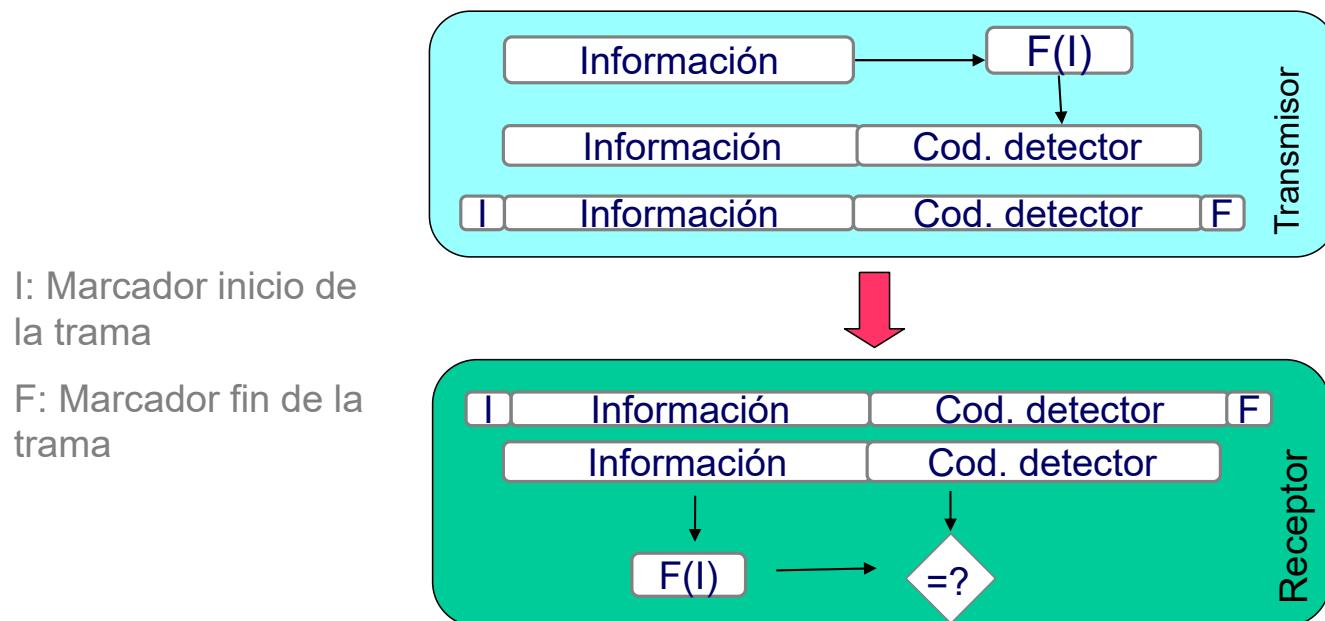


Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

Códigos detectores de error

- Permiten al receptor determinar algunas veces, **¡¡no siempre!!**, si hubo errores en la transmisión
- Normalmente cubren la cabecera y los datos



Códigos detectores de error

- Ningún método detecta el 100% de los errores ... pero los hay mejores y peores
- Veremos:
 - Paridad
 - Suma de comprobación de internet (*checksum*)
 - Comprobaciones de redundancia cíclica

Paridad Simple

- Cálculo del bit de paridad:
 - Añadir a cada código de 7-bits, 1 bit de paridad para conseguir un nº par/impar de unos en cada byte:
 - bit de paridad = 1 ó 0 para hacer que:
 - Paridad Par/Impar: nº par/impar de 1s en cada byte a transmitir.
 - Ejemplo:

Información a transmitir:
0100101

Con paridad **par**: 0100101**1**

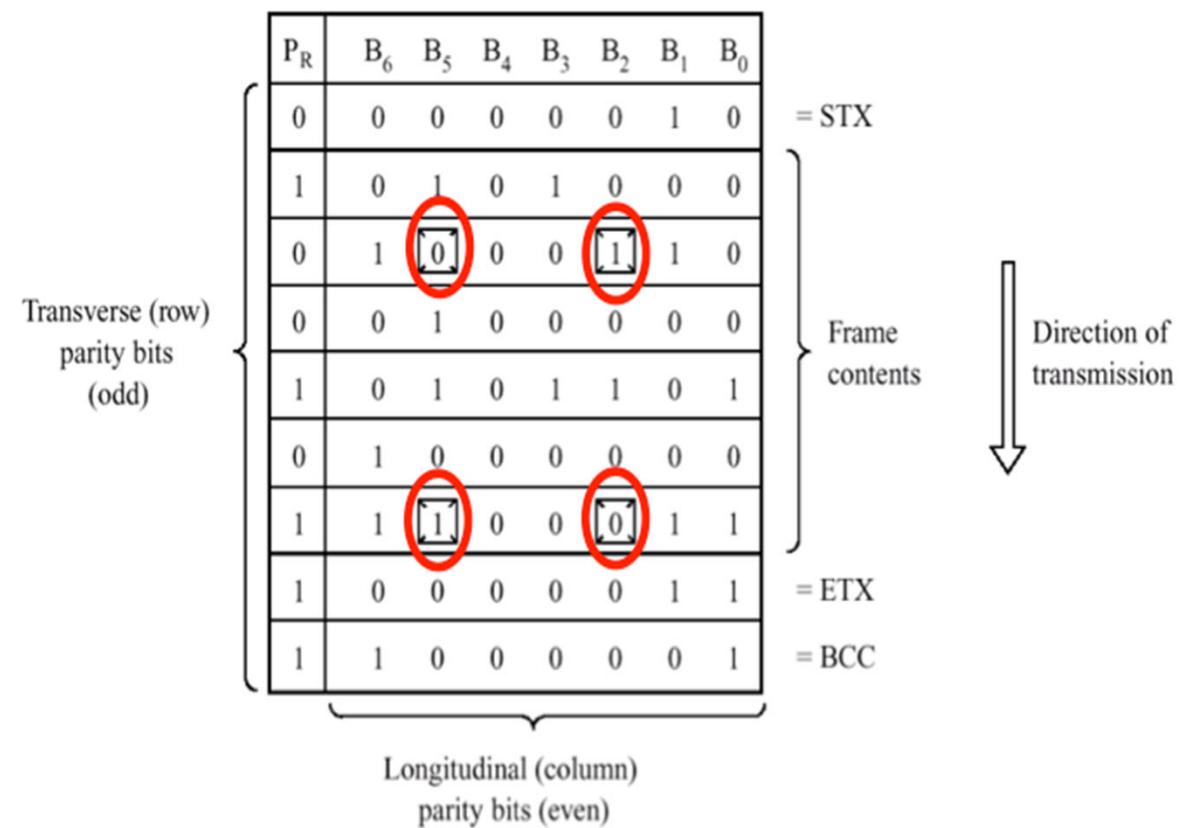
Con paridad **ímpar**: 0100101**0**

- Paridad par/ímpar: sólo permite detectar un nº ímpar de errores de bits

Paridad

- Se puede aplicar:

- A todos los datos (poco potente)
- Ordenando los datos en bloques
- **0** Errores no detectados



Suma de comprobación (*CheckSum*) de Internet

Emisor:

- Los bytes de datos se suman como **enteros de 16-bits**
- El **complemento a 1** de la suma es la suma de comprobación a transmitir

Receptor:

- Vuelve a realizar la suma de los datos
- Comprueba si el resultado obtenido es el mismo que el recibido:
 - NO – error detectado
 - SI – no se detecta error

- Implementado generalmente en software
- Empleado en el nivel de transporte y en el de red
- Problema:

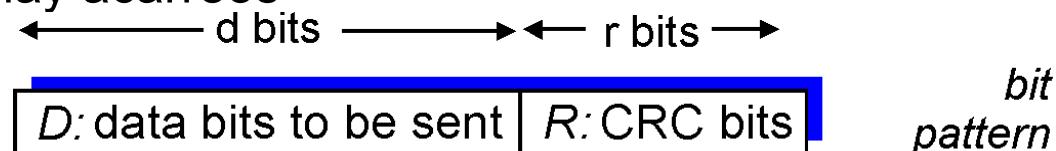
Datos binarios	Valor del CheckSum	Datos binarios	Valor del CheckSum
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
Total	7	Total	7

Ejemplo de cálculo de suma de comprobación

- Dado un paquete de 48 bits, lo dividimos en tres palabras de 16 bits:
 - 0110011001100110
 - 0101010101010101
 - 0000111100001111
- La suma de las dos primeras palabras sería:
 - 0110011001100110
 - 0101010101010101
 - 1011101110111011
- Sumando la tercera "palabra" al resultado anterior tenemos
 - 1011101110111011
 - 0000111100001111
 - **1100101011001010**
- La suma en complemento a uno se obtiene invirtiendo ceros y unos: **1100101011001010** seria **0011010100110101**. Que sería el *checksum*.
- Al llegar al receptor las cuatro palabras de 16 bits, incluyendo el *checksum* se suman y el resultado debe ser 1111111111111111. Si alguno de los bits es cero: ¡¡error!!

Códigos de Redundancia Cíclica: CRC

- Se tratan los bits de datos, **D**, como números binarios
- Se elige un patrón (generador) de $r+1$ bits, **G**
- Objetivo: Elegir r bits de CRC, **R**, tal que:
 - $\langle D, R \rangle$ sea exactamente divisible por G (en aritmética módulo 2)
 - El receptor conoce G, divide $\langle D, R \rangle$ por G. Si el resto no es cero se detecta el error
- Emplea aritmética polinomial en módulo 2
 - No hay acarreos



$$D * 2^r \text{ XOR } R \quad \text{mathematical formula}$$

Ejemplo CRC

Emisor:

- Calcula R como:

$$R = \text{resto de } \left(\frac{D * 2^r}{G} \right)$$

D = 101110 → d = 6 bits

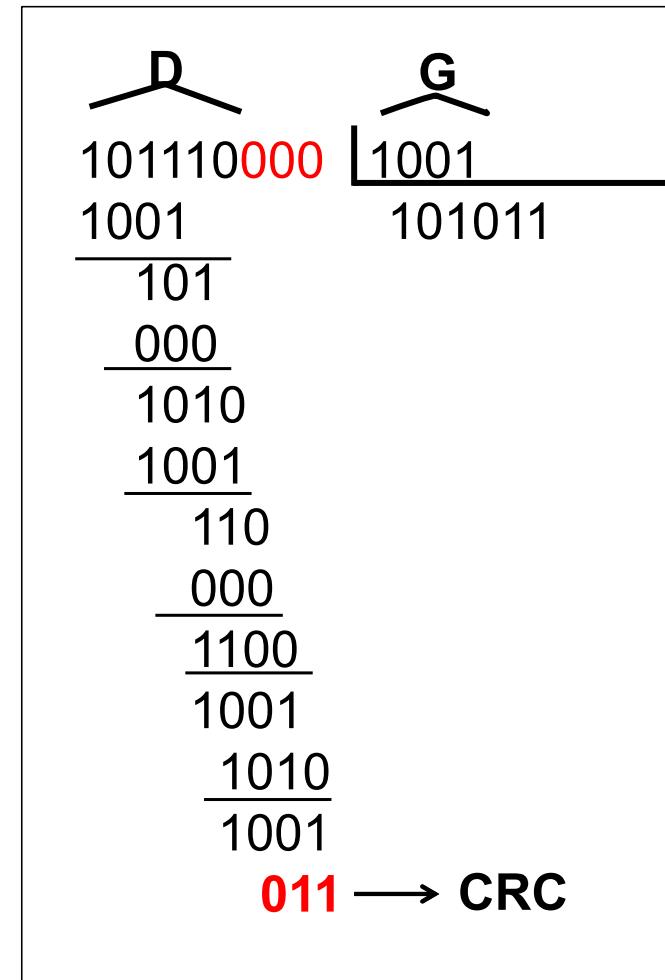
G = 1001 → r = 3 bits

- Envía D+R:

$$\begin{array}{r} \text{Datos + CRC} = 101110\boxed{011} \\ \hline \text{D} \quad \text{R} \end{array}$$

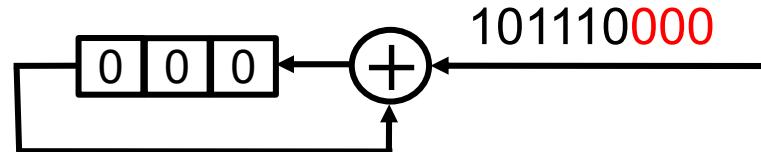
Receptor:

- Divide los datos recibidos (D+CRC) por el G acordado
- Si el resto = 0 → Datos recibidos sin error!!

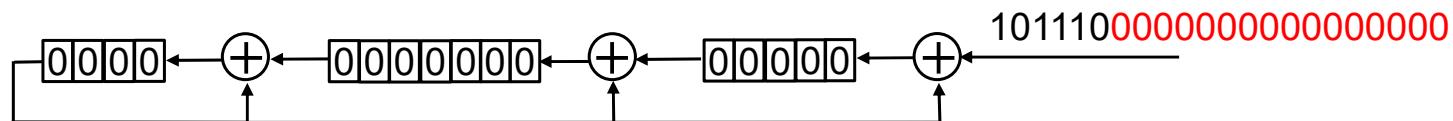


Implementación de los CRCs

- Los fundamentos matemáticos de los CRC son complejos ... pero la implementación hardware es muy sencilla
 - Bastan registro(s) de desplazamiento y puertas XOR
 - Las posiciones a '1' son precedidas por una XOR, menos la última que se realimenta a todas las XOR
 - Para el ejemplo anterior ($x^3 + 1$):



- Para un CRC más complejo ($x^{16} + x^{12} + x^5 + 1$):



CRC

- Muy potente
 - Con un generador de grado r ($r+1$ bits) se puede detectar:
 - TODAS las ráfagas de error de longitud $\leq r$
 - TODOS los errores que afectan a un número impar de bits
 - Bajo suposiciones apropiadas, ráfagas de longitud superior a $r+1$ con probabilidad 1- 0.5
- Ampliamente usado en la práctica en capa enlace (p.ej., Ethernet, 802.11 WiFi, ATM)
 - Se han definido estándares internacionales de generadores (G) para CRC de 8, 12, 16 y 32 bits
 - $G_{\text{CRC-32}} = 100000100110000010001110110110111$ (33 bits)

Corrección de errores

- Para poder corregir los errores se pueden emplear dos estrategias:
 - FEC (*Forward Error Correction*)
 - Añade información que permitirá al receptor reconstruir la información correcta
 - Detección + recuperación
 - ARQ (*Automatic Repeat Request*)
 - El emisor tiene que retransmitir la información dañada
 - Detección + reenvío

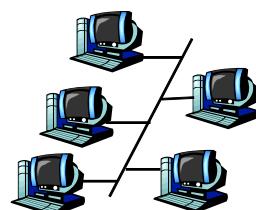
!!!Estudiadas en el tema 4 !!!!

Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

3. Enlaces y protocolos de acceso múltiple

- Existen dos tipos de enlaces de red:
 - Punto a punto
 - Acceso telefónico cableado
 - Red Ethernet (actualmente)
 - De difusión (cable o medio compartido)
 - Ethernet (en sus orígenes)
 - 802.11 (LAN inalámbrica)



Cable
compartido



802.11 WiFi



Redes vía
satélite

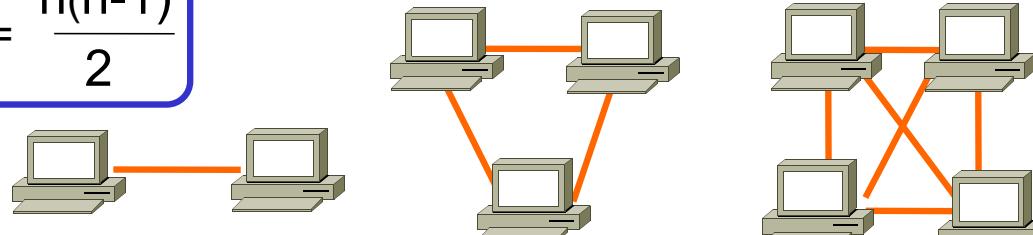


Grupo de personas
en una reunión

Enlaces punto a punto

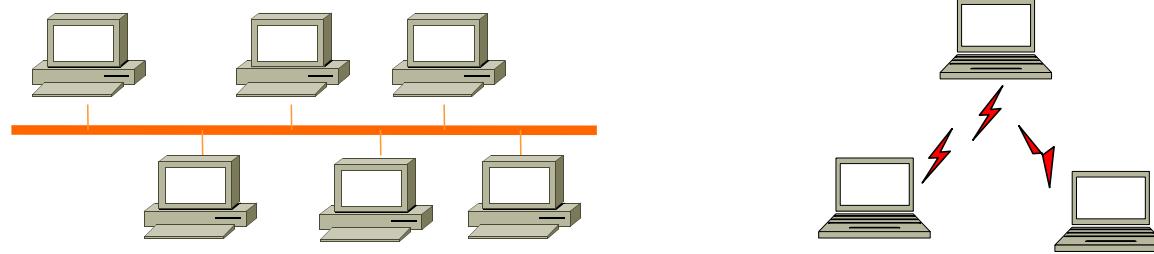
- Enlaces dedicados entre cada dos nodos, un único emisor y un único receptor
 - Ventaja:
 - Canales no compartidos: seguridad y privacidad
 - Inconveniente
 - Cuando crece el número de nodos (n) se requieren muchos enlaces

$$\text{Conexiones} = \frac{n(n-1)}{2}$$

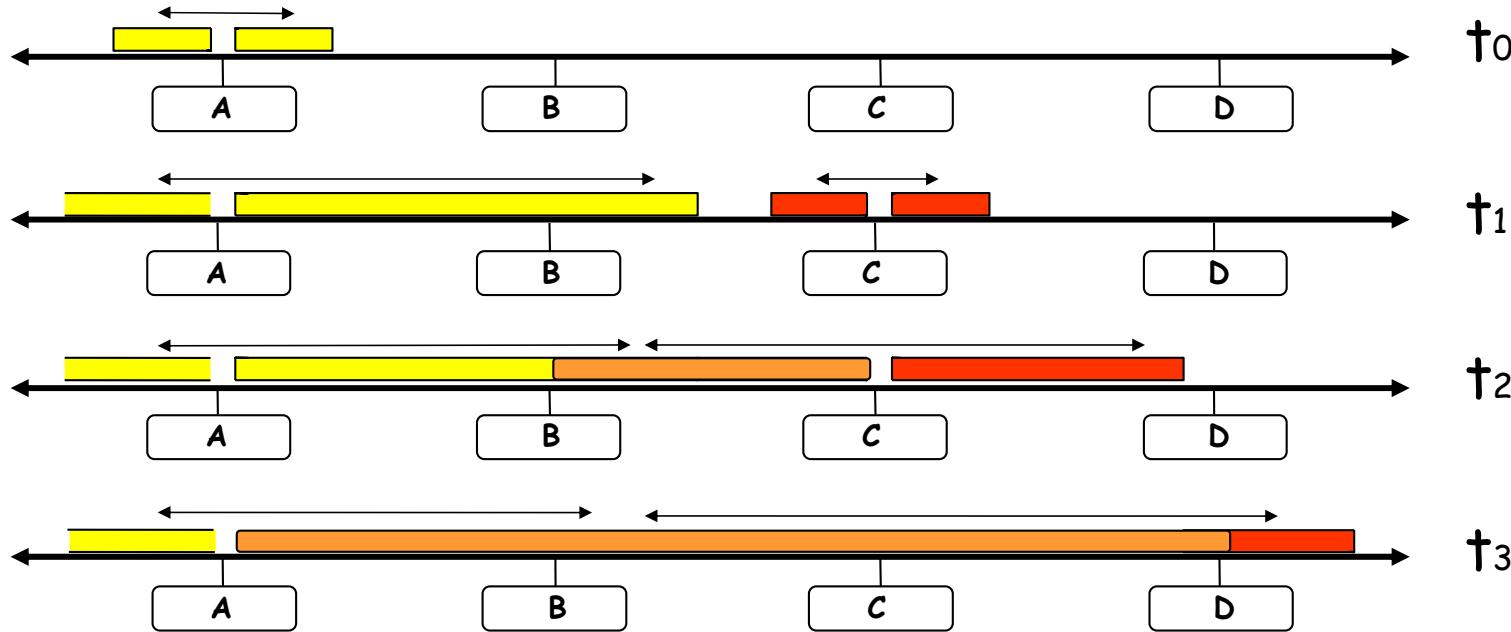


Enlaces de difusión

- Usan un canal de difusión compartido entre varios nodos
 - Sólo un nodo debe utilizar el enlace para transmitir con éxito
- Si dos o más nodos transmiten simultáneamente:
 - ¡¡Interferencias!!
 - **Colisión** si un nodo recibe dos o más señales al mismo tiempo
- Necesidad de un **protocolo de control de acceso al medio**
 - Algoritmo distribuido que determina cómo los nodos comparten el canal, i.e., determina cuándo un nodo puede transmitir
 - ¡¡No hay canal “en otra banda” para coordinación!!



Colisión de tramas



- Durante una colisión:
 - Todas las tramas implicadas se pierden
 - El canal de comunicación está desaprovechado

Características de un protocolo de acceso múltiple ideal

- **Equitativo:**
 - Dado un canal de difusión con un ancho de banda de R bps:
 - Cuando un nodo tiene datos para transmitir, puede hacerlo a una tasa de R bps
 - Cuando M nodos tienen datos para transmitir, cada uno de ellos puede hacerlo a una tasa media de R/M bps
- **Descentralizado:** no hay ningún nodo maestro que pueda ser el punto de fallo de toda la red
- **No requiere un reloj global**
- **Simple**, que no sea costoso de implementar

Taxonomía de los protocolos MAC (Media Access Control)

- Tres grandes clases:

- **Partición estática del canal**

- Se divide el canal en pequeños "trozos" (ranuras de tiempo, frecuencia)
 - Cada trozo se asigna en exclusiva a un nodo
 - Ejemplos: TDM, FDM

- **Acceso aleatorio:**

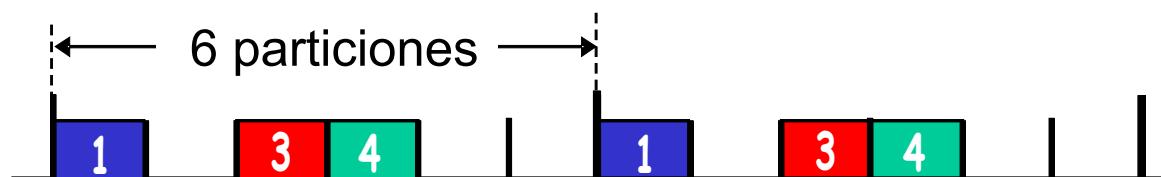
- El canal no está preasignado, pueden producirse colisiones
 - Hay que recuperarse de las colisiones
 - Ejemplos: CSMA/CD, CSMA/CA

- **Acceso por turnos:**

- Acceso al canal coordinado (por turnos) para evitar colisiones
 - Ejemplo: paso de testigo

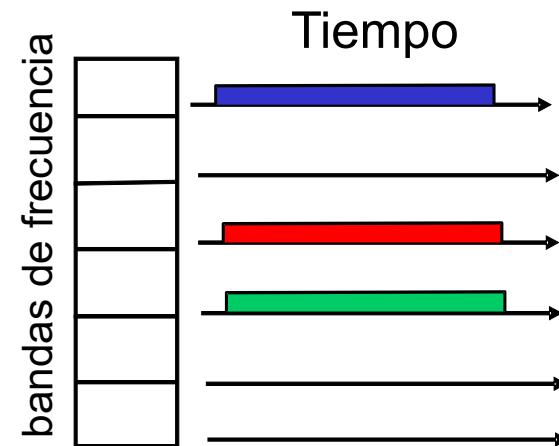
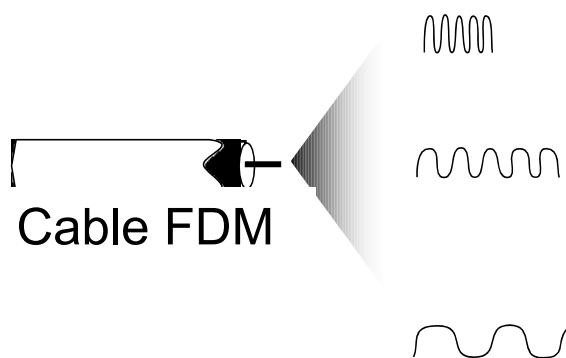
Protocolos de partición del canal

- Multiplexación por división el tiempo (TDMA: *Time Division Multiple Access*)
 - Se divide el uso del canal en marcos temporales
 - Cada marco temporal se divide en N particiones de tiempo (en una red con N nodos)
 - Se asigna una partición de longitud fija a cada nodo
 - Las particiones que no se usan se pierden
 - Ejemplo: 6 nodos, donde solo los nodos 1, 3 y 4 tienen paquetes para transmitir



Protocolos de partición del canal

- Multiplexación por división en frecuencia (FDM: *Frequency Division Multiple Access*)
 - Se divide el ancho de banda del canal en bandas de frecuencia
 - A cada nodo se le asigna una de las bandas de frecuencia
 - El ancho de banda en las bandas de frecuencia que no se usan se pierden
 - Ejemplo: 6 nodos, donde solo los nodos 1, 3 y 4 tienen paquetes para transmitir

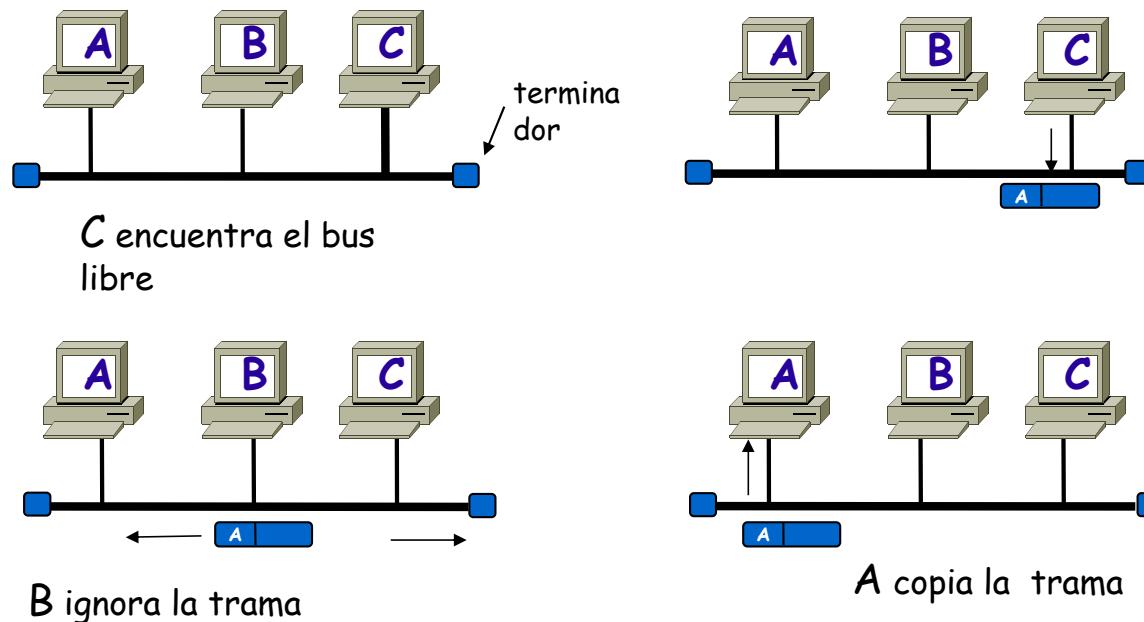


Protocolo de acceso aleatorio

- Cuando un nodo tiene paquetes para enviar:
 - Transmite utilizando todo el ancho de banda del canal
 - No hay coordinación entre nodos
 - Si dos nodos transmiten a la vez se produce una **colisión**
- Los protocolos de acceso aleatorio especifican:
 - Cómo detectar colisiones
 - Cómo recuperarse de una colisión (e.g., vía retransmisiones retardadas)
- Ejemplos de protocolos MAC de acceso aleatorio:
 - ALOHA
 - ALOHA ranurado
 - CSMA, **CSMA/CD, CSMA/CA**
 - (**CSMA: CARRIER SENSE MULTIPLE ACCESS**)

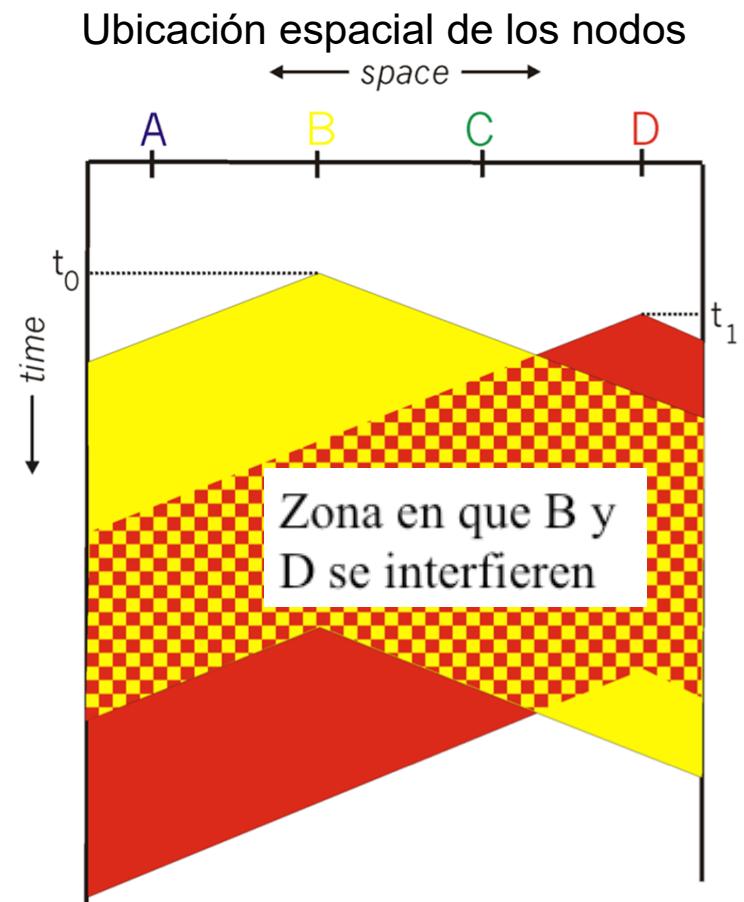
CSMA (*Carrier Sense Multiple Access*)

- CSMA escucha la señal portadora antes de transmitir (*Carrier Sense*):
 - Canal libre: transmite la trama entera
 - Canal ocupado: retrasa la transmisión
 - Analogía humana: *¡no interrumpir mientras otros hablan!*



Colisiones en CSMA

- Pueden ocurrir colisiones a causa del retardo de propagación
 - Más probables cuanto mayor sea el retardo
- En ese caso:
 - El paquete se descarta
 - El tiempo de transmisión del paquete se desaprovecha



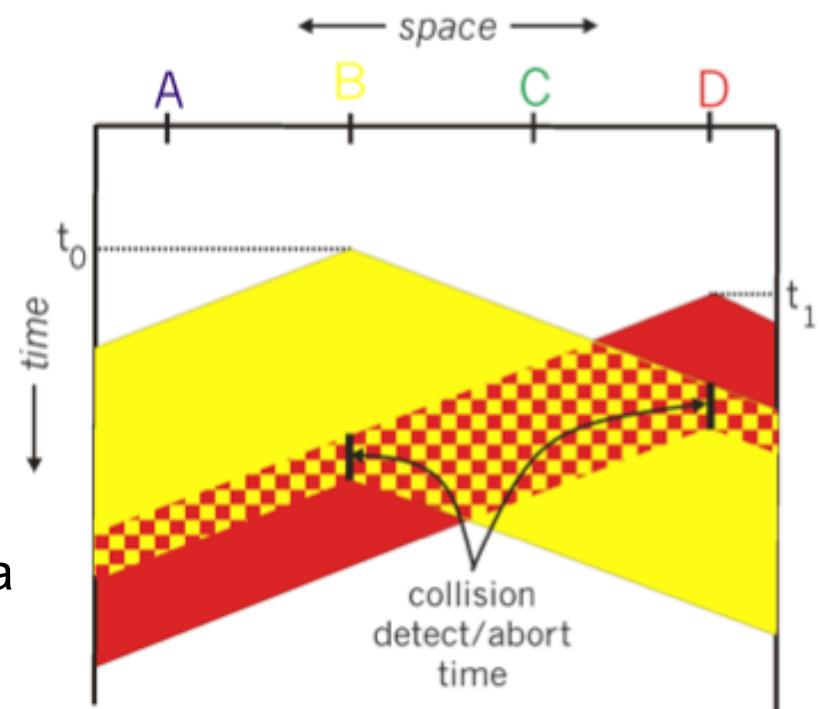
CSMA/CD (Detección de colisiones)

- CSMA/CD: detección de señal, similar a CSMA

- Mientras se transmite se comprueba si se produce una colisión (CSMA/**CD: Collision Detection**)
 - Las colisiones se detectan rápidamente
 - Si se detecta una colisión se aborta la transmisión, reduciendo el mal uso del canal

- Detección de colisiones:

- Fácil en LANs cableadas: se mide la potencia de la señal, se compara señales transmitidas con recibidas
- Difícil LANs inalámbricas: receptor apagado mientras se transmite



Algoritmo CSMA / CD

- Escuchar si el canal está libre antes de intentar la transmisión
- Si dos estaciones transmiten a la vez, siguen existiendo colisiones

```
mientras se tengan tramas por enviar
    Mientras el canal esté ocupado
        bucle de espera;
        /* canal libre */
        << transmitiendo >>
        si ocurre una colisión
            parar transmisión
        entonces se espera un tiempo aleatorio*
fin mientras
```

* *binary exponential backoff*

Binary Exponential Backoff

```
-> colisión i <-  
si i <= 10 entonces  
    elige un numero n entre 0 y ( $2^i - 1$ )  
    espera n time-slots  
    reintenta enviar  
sino si i <= 16 entonces  
    elige un numero n entre 0 y ( $2^{10} - 1$ )  
    espera n time-slots  
    reintenta enviar  
sino si i > 16 entonces  
    error  
fin
```

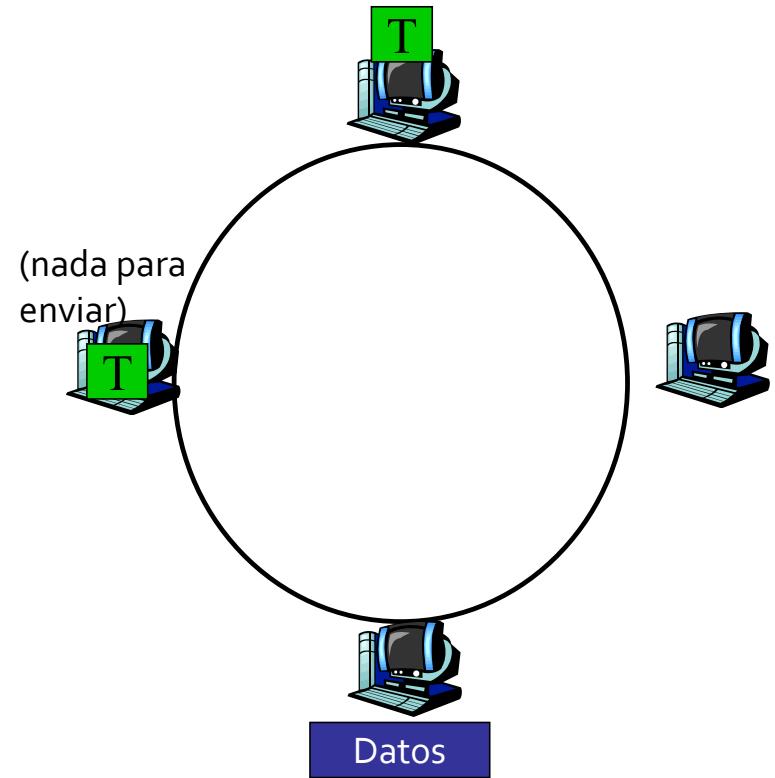
time-slots = tiempo de transmisión de 512 bits

Comparación de protocolos de acceso

- Protocolos de partición de canal:
 - Eficientes con carga alta
 - Ineficientes en condiciones de carga baja:
 - Sólo se asigna el $1 / N$ del ancho de banda disponible ¡aunque haya un único nodo activo!
- Protocolos de acceso aleatorio:
 - Eficientes con carga baja:
 - Un nodo dispone del canal (completo) cuando lo necesita
 - Con carga alta :
 - Sobrecarga por colisiones
- **Protocolos de acceso por turnos**
 - Buscan lo mejor de las otras dos aproximaciones

Protocolos de acceso por turnos: Paso de testigo

- Cuando un nodo quiere transmitir, ha de esperar a tener el testigo
- Paso de testigo
 - El testigo se pasa de un nodo al siguiente secuencialmente
 - Cuando un nodo recibe el testigo
 - Si tiene tramas que transmitir, transmite hasta un máximo y después pasa el testigo al siguiente nodo
 - Si no tiene tramas que transmitir pasa el testigo
- Permite un control de acceso descentralizado, equitativo y flexible
- **Problema:** ¡¡si un nodo falla, toda la red puede fallar!!



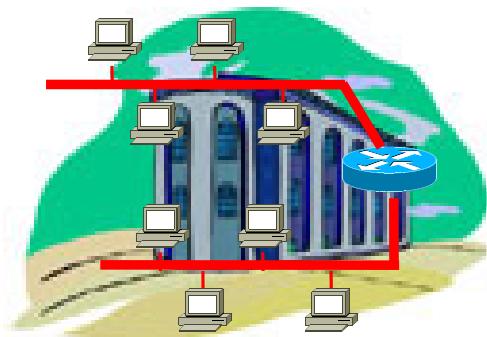
Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

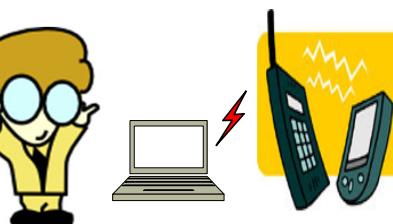
Clasificación de redes



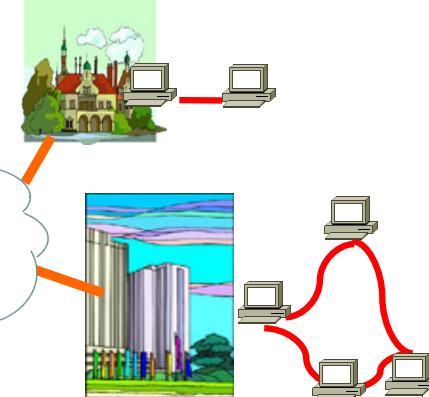
WAN (Wide Area Network)



LAN (Local Area Network)



MAN (Metropolitan Area Network)



Red pública
de la ciudad

PAN (Personal Area Network)

Características de la LAN

- Cubren un área geográfica moderada
 - Aunque sedes separadas pueden comunicarse mediante redes privadas virtuales (VPN)
- Son propiedad de la organización que posee los dispositivos conectados
 - Que también utiliza y administra la LAN
- Transmisión:
 - Altas velocidades y tasas de error bajas
- Las principales tecnologías LAN empleadas se basan en protocolos IEEE:
 - Protocolos IEEE 802.3 (Ethernet)
 - Protocolos IEEE 802.11 (Wi-Fi)

4. Direccionamiento del nivel de enlace

Este apartado se estudiará en la práctica 6

- Direcciones físicas IEEE (o direcciones MAC, hardware o Ethernet)
 - Función: utilizadas para enviar /recibir tramas entre interfaces conectados a la misma red física (misma red IP)
 - 48 bits en ROM de la tarjeta de red
 - Se expresan en hexadecimal: : 1A-2F-BB-76-09-AD
 - Tipos de direcciones:
 - Unicast: receptor individual
 - Broadcast: para todos los nodos. Todo a 1's. (FF:FF:FF:FF:FF:FF)
 - Multicast: para un conjunto de nodos. 1's en la cabecera de la dirección

Direcciones físicas IEEE

- Todas las redes IEEE comparten el mismo esquema de direcciones
 - IEEE 802.3 (ethernet), IEEE 802.11 (wi-fi)
- Se garantiza que las direcciones son únicas (independientemente de marcas y redes)
 - Cada fabricante compra uno o varios bloques
- Son direcciones planas → portables
 - El adaptador se puede llevar de una LAN a otra manteniendo su dirección MAC (diferencia con direcciones IP)

Octetos: 0 1 2 3 4 5
0011 0101 0111 1011 0001 0010 0000 0000 0000 0000 0000 0000 0001

1^{er} bit: (I/G Address Bit: 0=Individual; 1=Group)

2^{do} bit: (U/L Address Bit: Universally (0) /Locally (1) Administered)

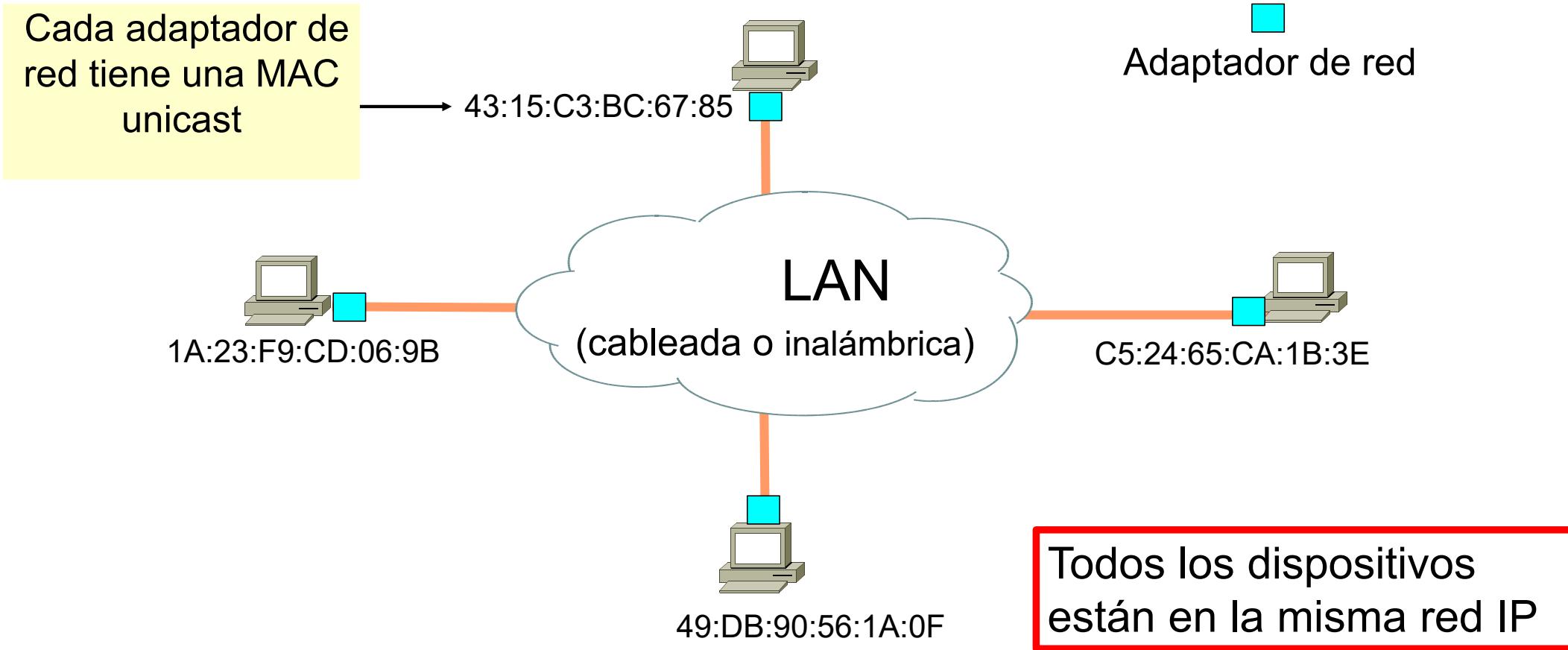
Representación hexadecimal:

AC : DE : 48 : 00 : 00 : 80



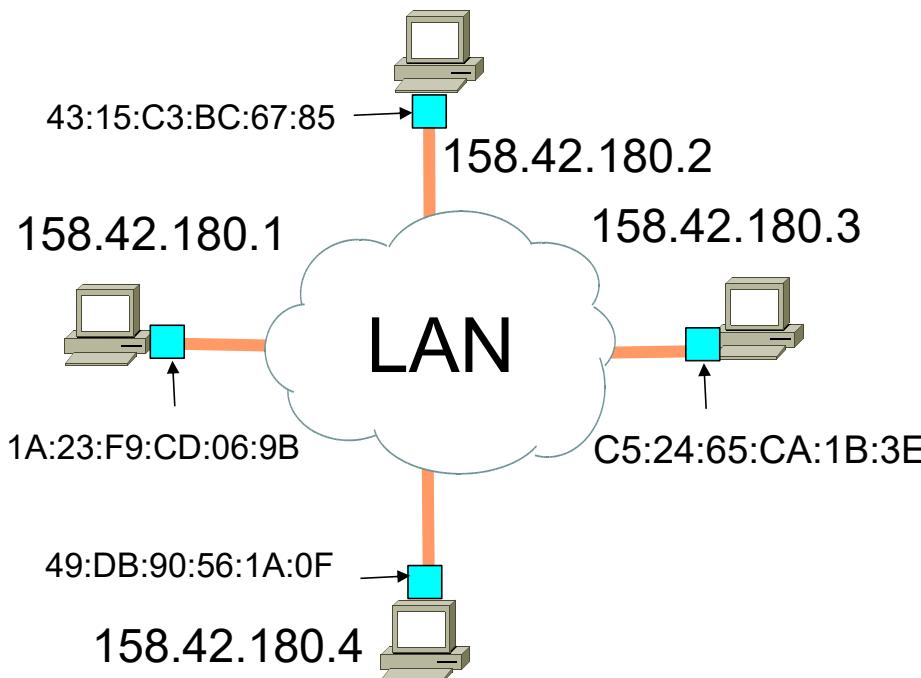
Organizationally Unique Identifier asignado por IEEE

Direcciones físicas unicast



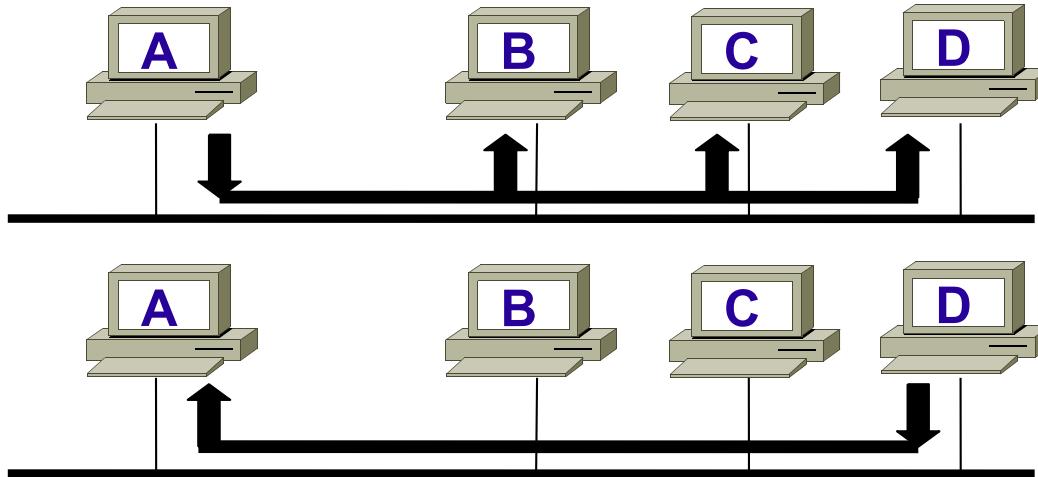
ARP: Address Resolution Protocol

¿Cómo determinar la dirección MAC sabiendo la dirección IP del host?



- Cada nodo IP (host o router) de la LAN tiene una tabla ARP
- Tabla ARP: relaciona direcciones IP ↔ MAC para algunos nodos de la LAN
 - < IP address; MAC address; TTL >
 - TTL (Time To Live): tiempo de expiración para el mapeo (típicamente 20 min)
 - Mismo nombre pero no confundir con TTL en encabezado IP

Funcionamiento de ARP



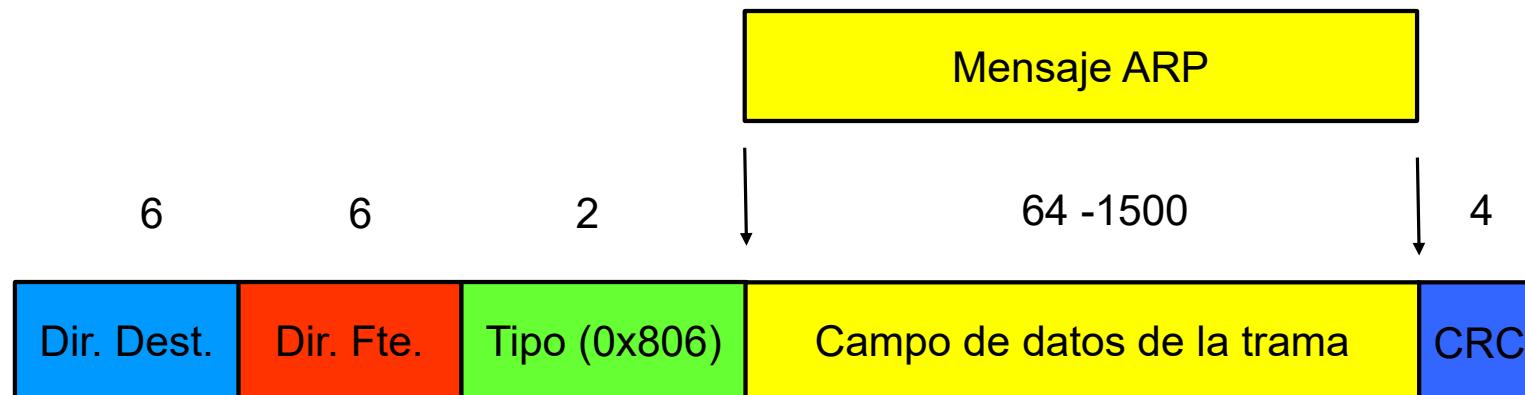
¡La consulta es por difusión!

¡La respuesta NO!

- El host **A** guarda el par IP_D - MAC_D en su tabla ARP hasta que la información caduque
 - La información caduca a menos que sea refrescada
- El host **D** también añade el par IP_A - MAC_A a su tabla ARP si no lo tenía aún
 - Si ya tenía una entrada IP_A la refresca (y en caso necesario actualiza MAC_A)
- Los nodos **B** y **C**, al recibir la petición (difusión) de A, aunque no contestarán, actualizarán el TTL (y en caso necesario la MAC_A) de sus tablas para la entrada IP_A *si ya la tenían registrada*. Si no la tenían no la añadirán a su tabla. ¡Pensad el motivo....!
- ARP es “plug-and-play”: los nodos crean sus tablas de ARP sin intervención de los administradores

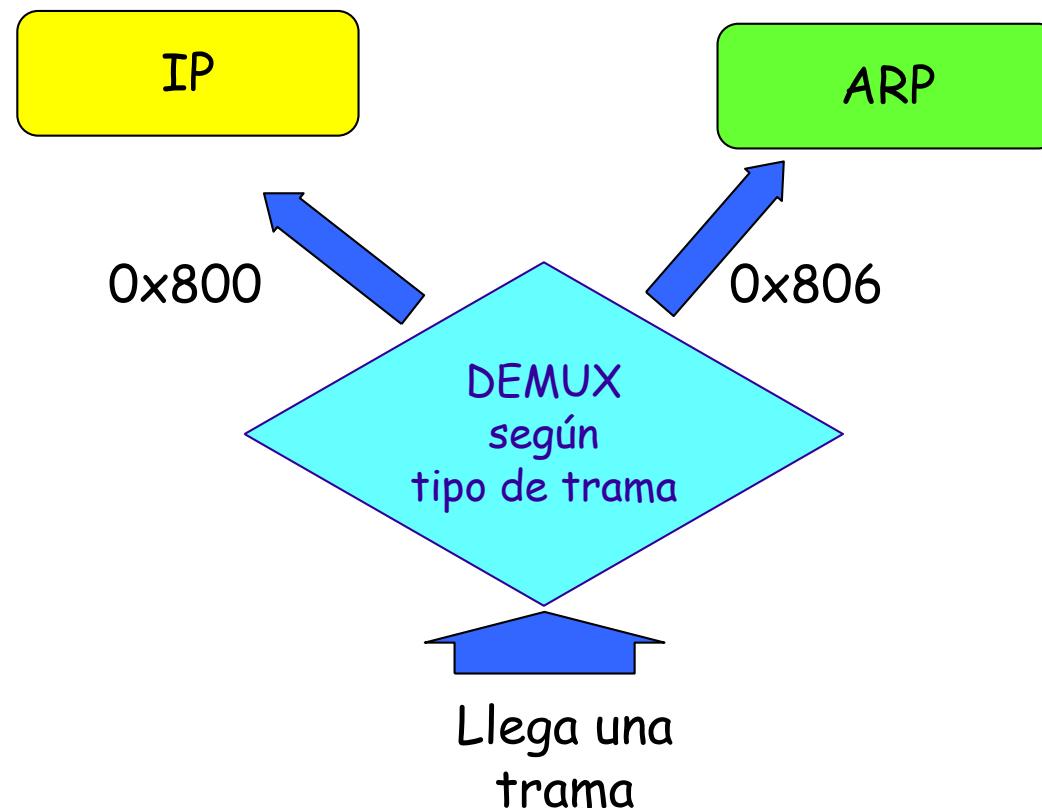
Encapsulado ARP

- El mensaje ARP se envía en el campo de datos de una trama
- Un campo en la cabecera de la trama permite identificar el tipo de mensaje (en el caso Ethernet para ARP 0x806).



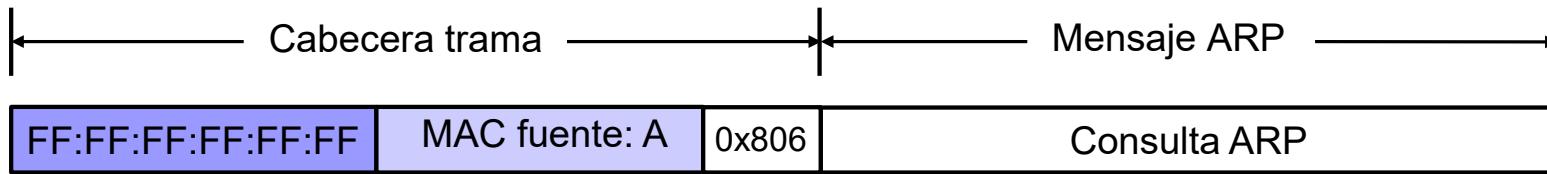
Demultiplexación

- Se entrega al módulo que corresponde según el tipo de trama

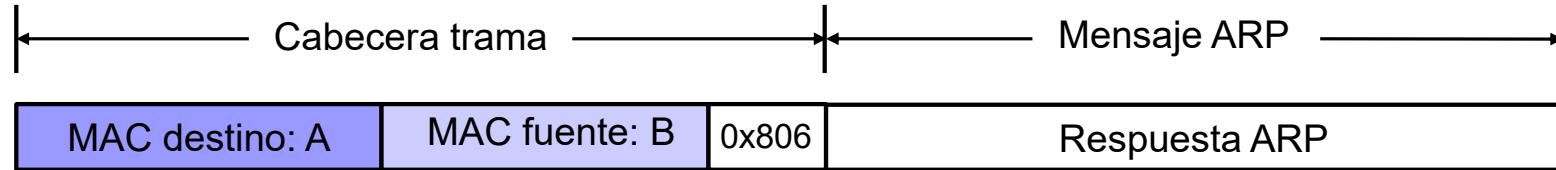


Información en mensajes ARP

- Información en un mensaje de petición ARP
 - Dirección física de A, dirección IP de A, dirección IP de B

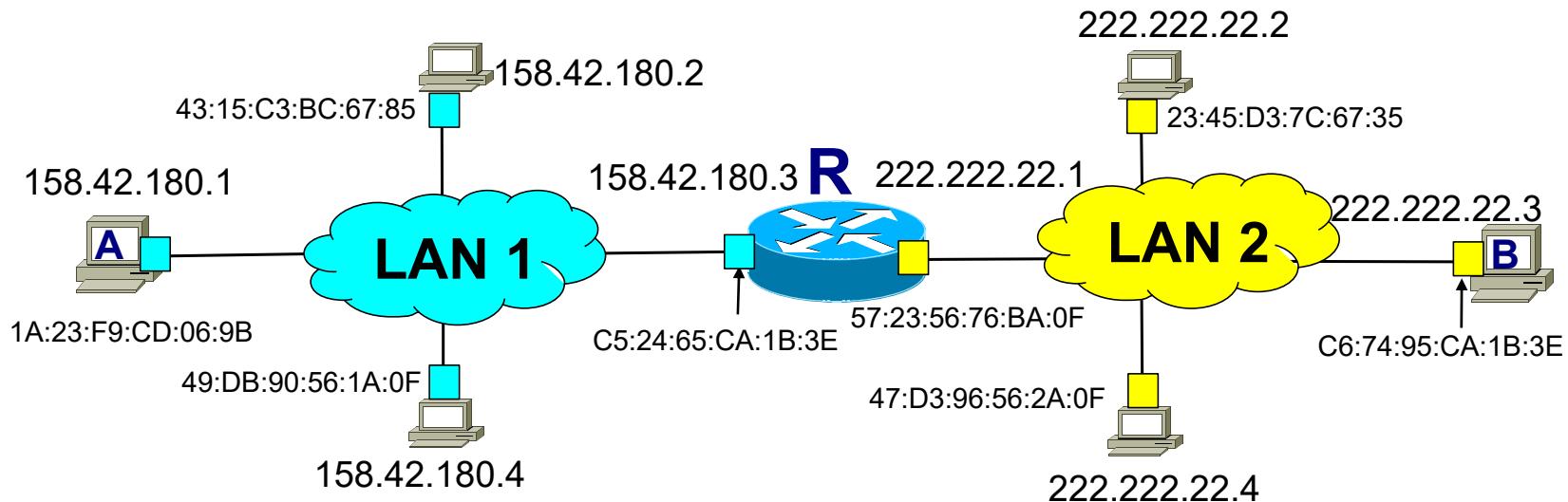


- Información en un mensaje de respuesta ARP
 - Contesta B, añadiendo su dirección física



ARP es local a la red

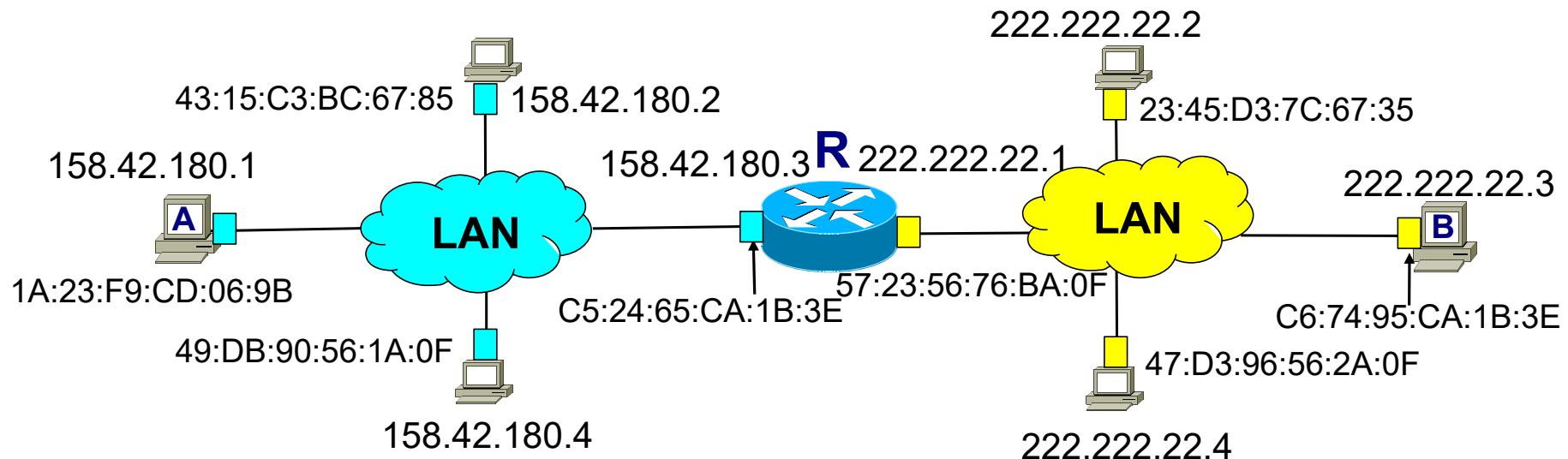
- La resolución de direcciones físicas es **local a la red**
 - Un computador sólo necesita averiguar la dirección física de otro si ambos comparten la **misma red física (LAN 1 o LAN 2)**



¡¡Dos tablas ARP en R, una por cada LAN!!

Reenvío fuera de la red

- **A** envía un datagrama a **B**, del cual conoce su dirección IP



- Dos tablas ARP en **R**, una por cada LAN

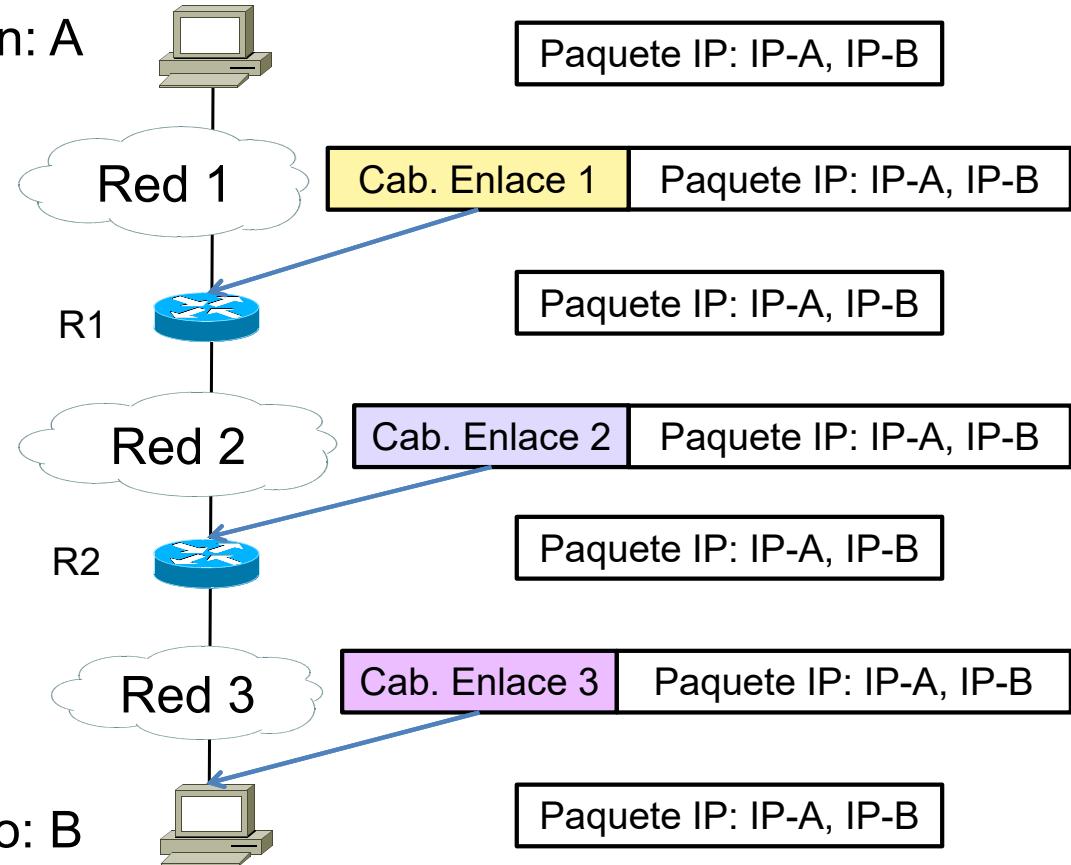
Direcciones MAC y encaminamiento

- El adaptador de red reconoce y procesa las tramas destinadas a él (con su dirección física):
 - Individual (**unicast**)
 - De grupo (multicast o **broadcast**)
- En el encaminamiento utilizaremos los 2 tipos de direcciones:
 - Direcciones IP en la cabecera del **datagrama**
 - Direcciones físicas en la cabecera de la trama

Transmisión a través de internet

Host origen: A

- En cada salto se extrae el datagrama y se descarta la trama
- Nueva trama en el salto siguiente



Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

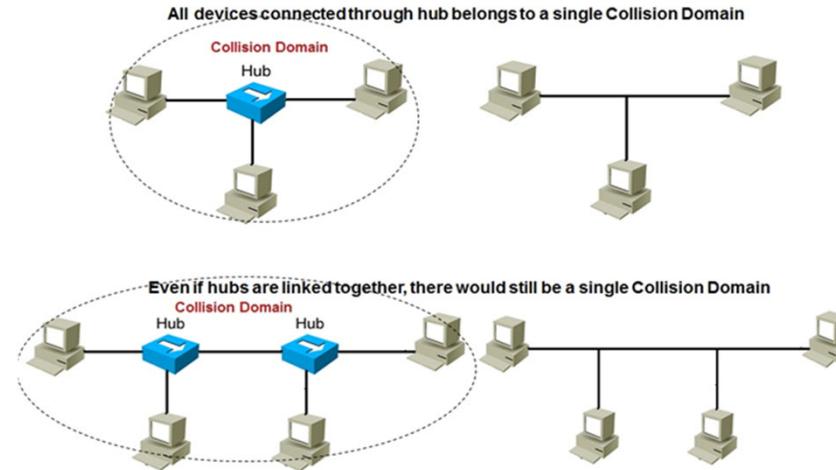
Dispositivos de interconexión

5	Aplicación	
4	Transporte	
3	Red	<i>Encaminador (Router)</i>
2	Enlace de datos	<i>Conmutador (Switch)</i>
1	Físico	<i>Repetidor (Hub)</i>

Conceptos previos

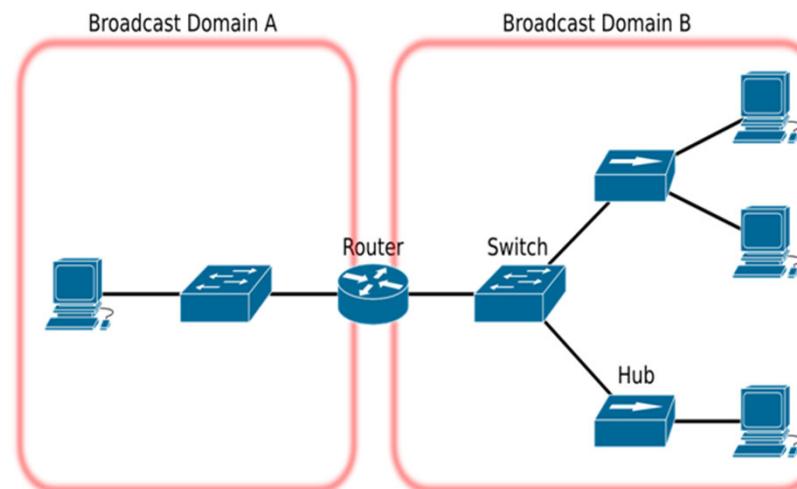
- **Dominio de colisión:**

- Conjunto de estaciones que se ven afectadas por una colisión (tanto si participan en ella como si no)



- **Dominio de difusión:**

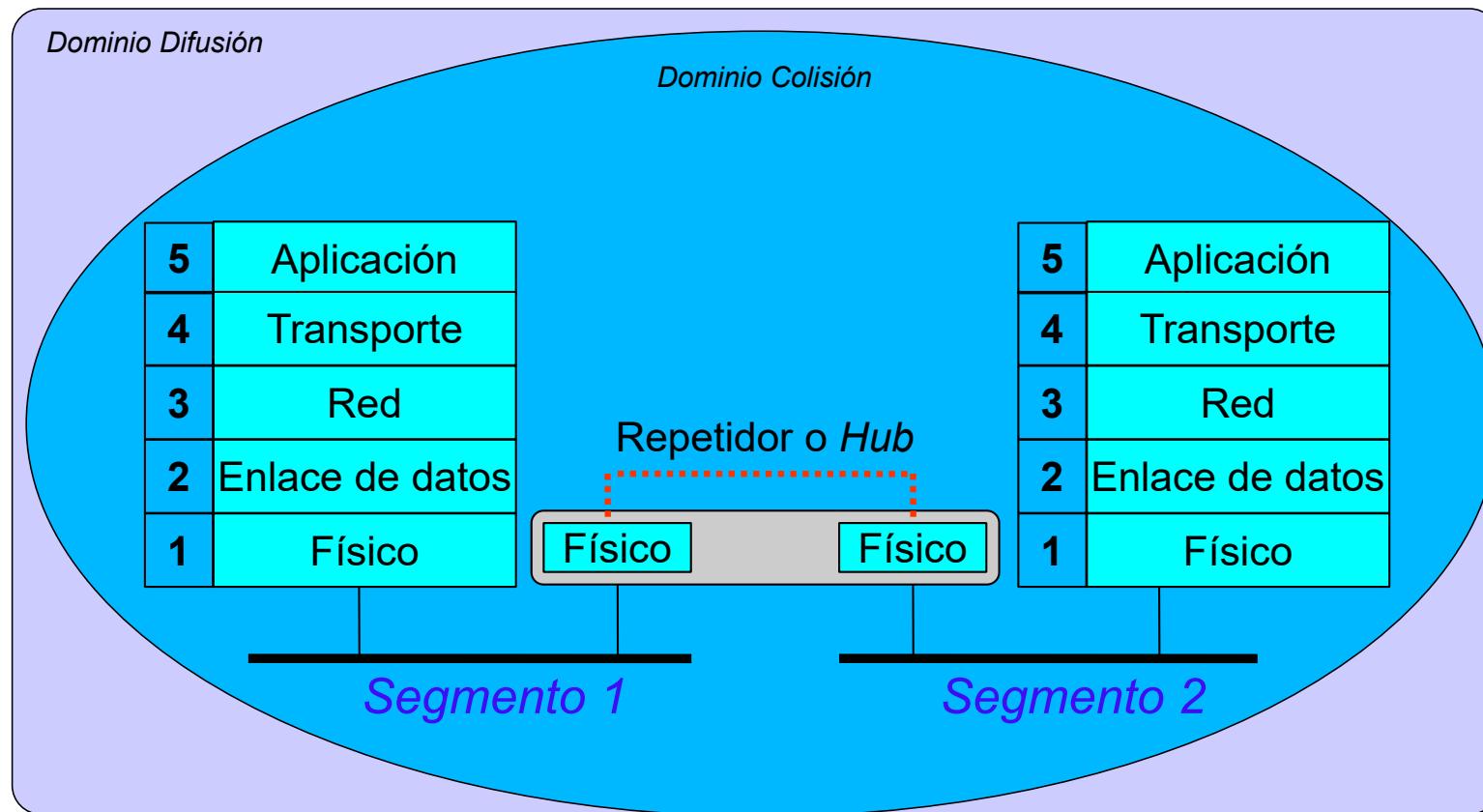
- Conjunto de estaciones que recibe una difusión efectuada por alguna de ellas



Repetidores/*Hubs*

- La señal transmitida se atenúa con la distancia
- Repetidor: dispositivo electrónico que regenera la señal
 - Interconectan dos o más segmentos LAN a nivel físico
 - **No entiende el formato de la trama, ni las direcciones físicas:** copia cualquier señal eléctrica (colisiones también)
- Concentradores (*hubs*): son repetidores multipuerto
- Los **repetidores/hubs no separan los dominios de colisión**
 - No CSMA / CD en el hub: los NIC en los nodos tienen que detectar colisiones

Esquema: Repetidores



Switch (Comutador)

- Dispositivo de capa de enlace de datos
- El switch almacena la trama que recibe por un puerto y la **retransmite selectivamente** por otro(s), cuando es necesario (difusión, destino en otro segmento, destino desconocido)
 - No analizan los datos de la trama, sólo las direcciones MAC
 - Son *plug & play*, aprenden solos
 - **No hay que configurarlos**
- **Transparentes**
 - Los nodos no son conscientes de su presencia
 - No modifican las direcciones de las tramas (ni fuente ni destino)
- Interconectan segmentos de una misma LAN
- **Separan los dominios de colisión pero no separan los dominios de difusión**

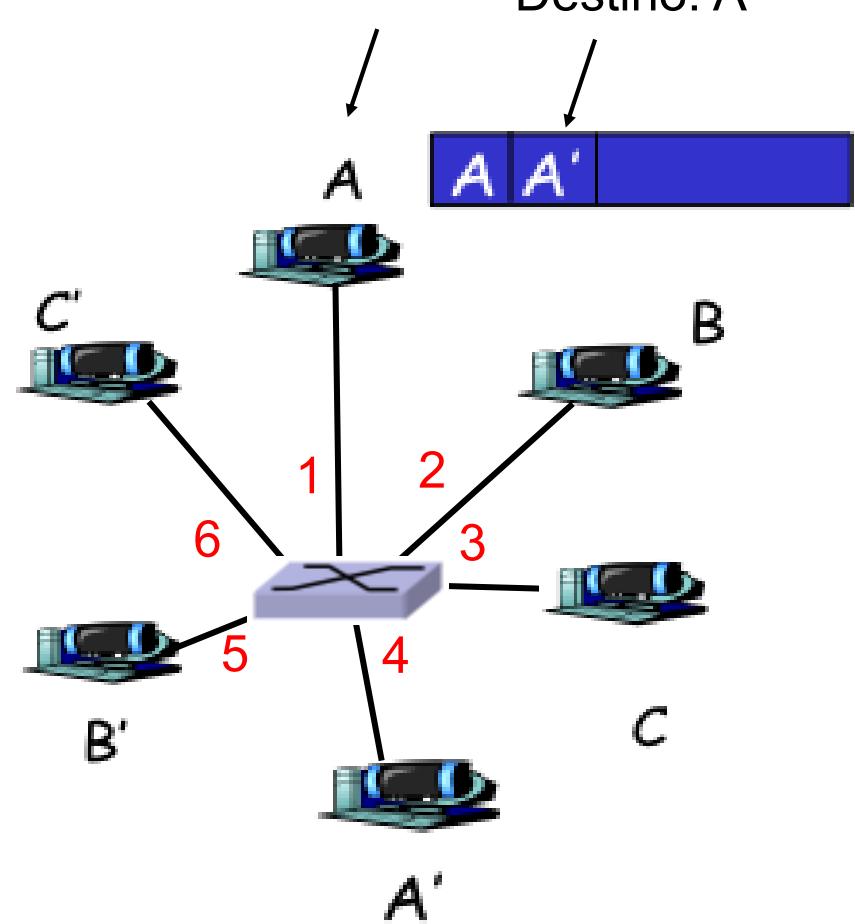
Commutadores: auto-aprendizaje

- El commutador **aprende** qué hosts pueden alcanzarse mediante qué interfaces
 - Cuando recibe una trama, “aprende” **la dirección origen** de la trama **y el puerto** por el que entró
 - Anota la información en la tabla de retransmisión

Dir MAC	interfaz	TTL
A	1	60

Tabla de reenvío
(initialmente vacía)

Fuente: A Destino: A'



Filtrado y reenvío de tramas

- Cuando un switch recibe una trama:

- Anota en la tabla la MAC origen (“aprende”)
 - Si la MAC ya aparecía, prolonga su TTL
- Busca en su tabla usando la **dirección MAC destino**
 - if** encuentra entrada para el destino

then {

if destino está en segmento desde donde llegó la trama,
then descarta trama

else reenvía la trama a la interfaz indicada

} else {

Inundación

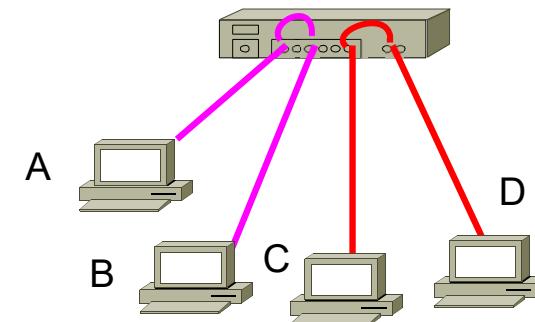
}



Reenvía por todos los interfaces
excepto el de llegada

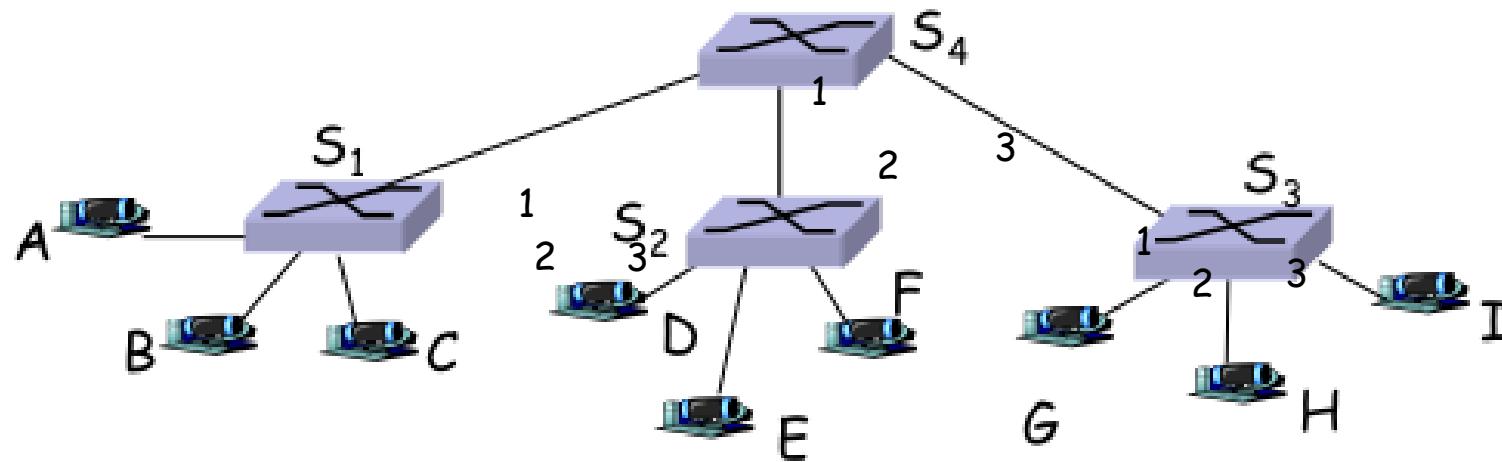
Switches: transmisiones simultáneas

- Permiten transmisiones simultáneas entre varios dispositivos (comunicación *full-duplex*)
 - Comunicación simultánea entre A-B y C-D sin problemas
 - Disponen de *buffers* para almacenar las tramas. No se producen colisiones
 - Mejora de prestaciones respecto a las redes de difusión
- Pueden conectar segmentos de red con distinto ancho de banda



Interconexión de commutadores

- Los commutadores pueden conectarse de forma jerárquica

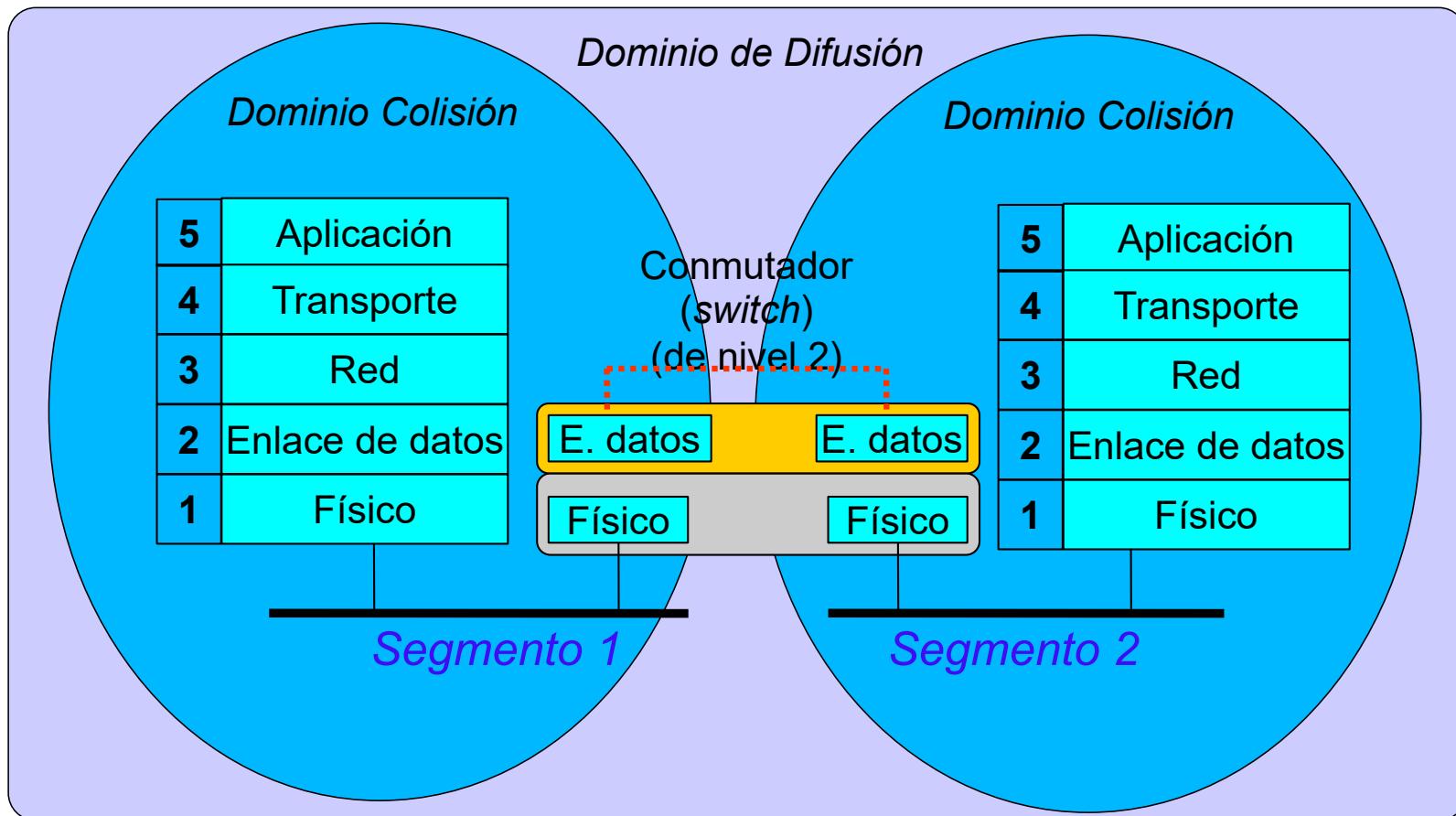


- Cuando se envía una trama desde A a G, ¿cómo sabe S_1 a quién debe enviar la trama?
- ¡¡Auto-aprendizaje!!

Comutadores: limitaciones

- Los comutadores **no separan los dominios de difusión**
 - Escalabilidad limitada
 - La cantidad de difusiones aumenta con el número de *hosts*
 - Las difusiones interrumpen a todos los hosts
 - Un *host* mal configurado (generando difusiones) entorpece todo un dominio de difusión

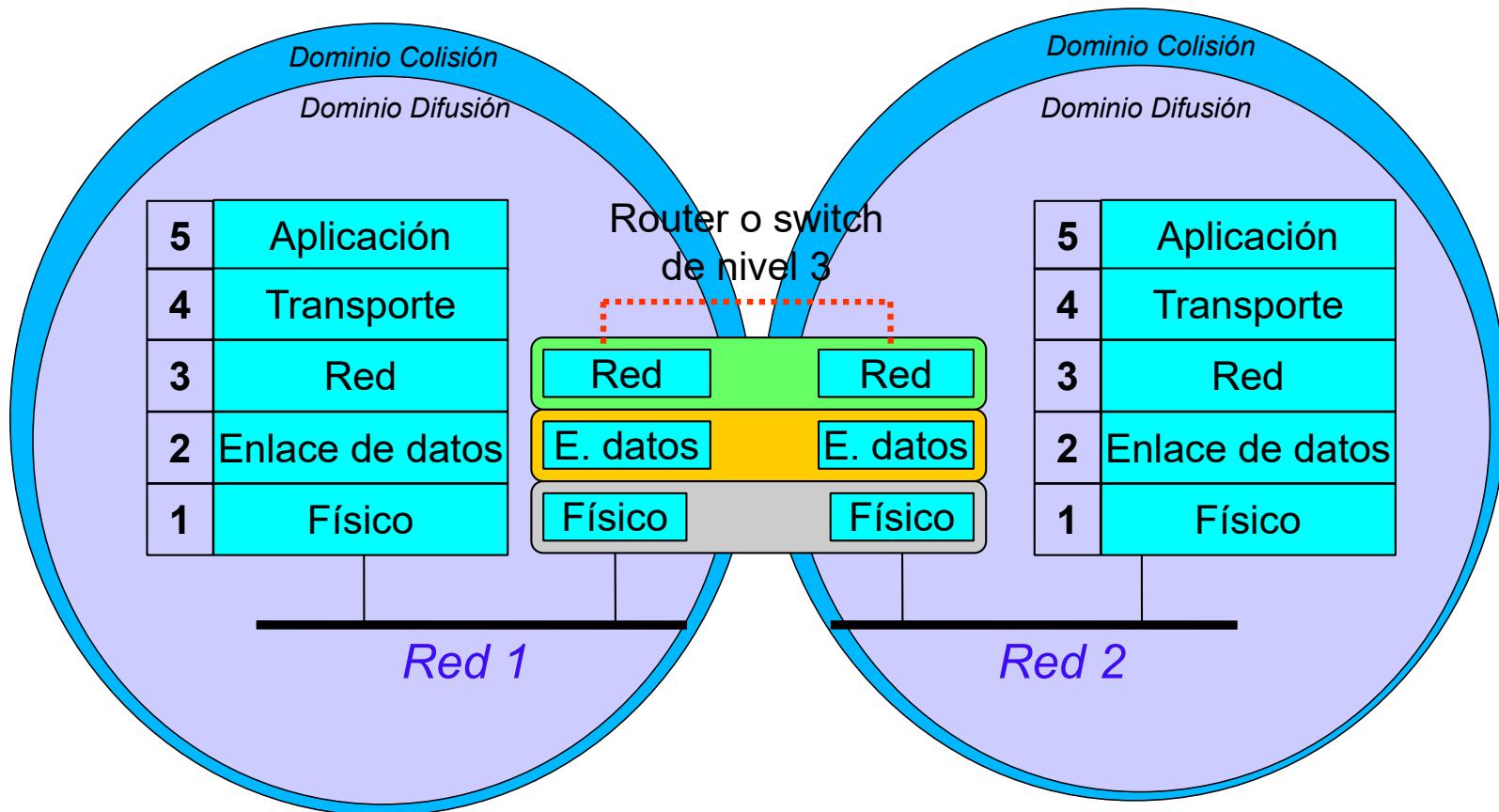
Esquema: commutador



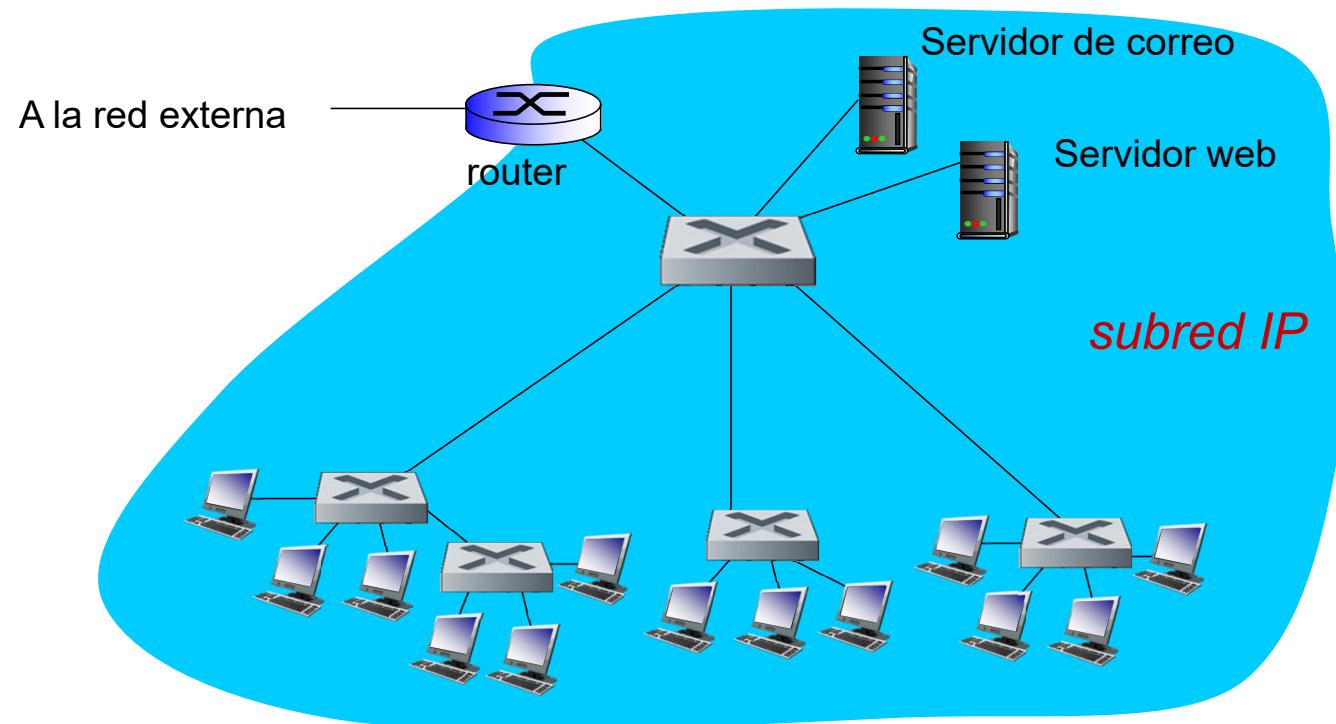
Routers

- Permiten la interconexión de redes de igual o distinta tecnología de nivel de enlace
- Las decisiones de encaminamiento se toman basándose en las direcciones IP
- Los routers separan los dominios de difusión y colisión
 - Cada puerto: un dominio de difusión
- Realizan un procesamiento software de los paquetes recibidos:
 - Decremento TTL, cálculo del checksum, fragmentación, generación paquetes ICMP, algoritmos de encaminamiento
 - Modifica la dirección origen de la trama original por la suya
- Tanto ellos como los host conectados a ellos necesitan ser configurados con su dirección IP

Esquema: Router



Redes institucionales



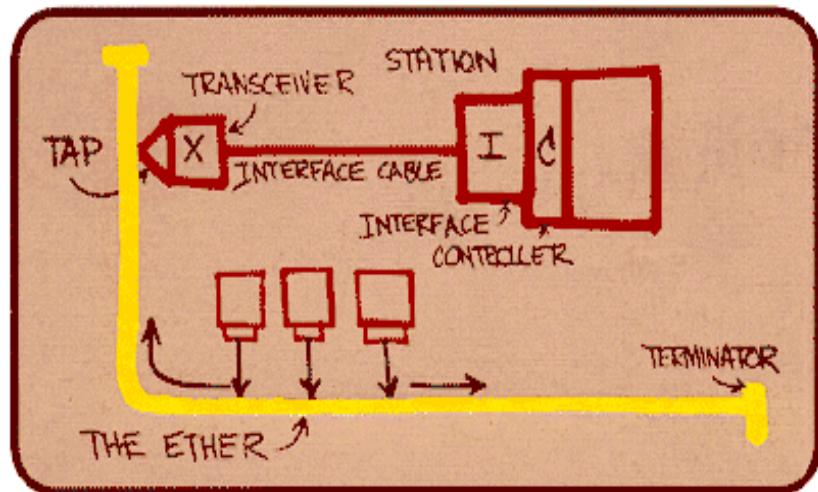
Índice

1. Introducción y servicios del nivel
Contexto y terminología
Servicios del nivel de red
2. Detección y corrección de errores
Paridad, *Checksum* y CRCs
3. Acceso al medio
Canales punto a punto y multipunto
Partición estática: MDT, MDF
Acceso aleatorio: CSMA, CSMA/CD
Protocolos por turnos: *Token Bus/Token Ring*
4. Direccionamiento del nivel de enlace
Práctica 6: Direcciones MAC y ARP
Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
Repetidores y concentradores (*Hubs*)
Comutadores (*Switches*)
Interconexión de comutadores
Auto-aprendizaje de comutadores
Comutadores y encaminadores
6. Ethernet
Estructura de la trama
Algoritmo CSMA/CD ethernet
Nivel físico: medios.
Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
Introducción
Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
El problema del terminal oculto – CDMA
Redes Wi-Fi 802.11
Arquitectura, asociación con punto de acceso
802.11: acceso múltiple, CSMA/CA, RTS-CTS
802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
Práctica 7: Cortafuegos IPTABLES
Práctica 8: Análisis de tráfico Wi-Fi 802.11

LAN cableadas: Ethernet

IEEE 802.3 (Ethernet)

- Tecnología LAN cableada “dominante”
- ¡Barata!
- Fácil de administrar
- Evolución de velocidad de funcionamiento: 10Mbps - 10Gbps

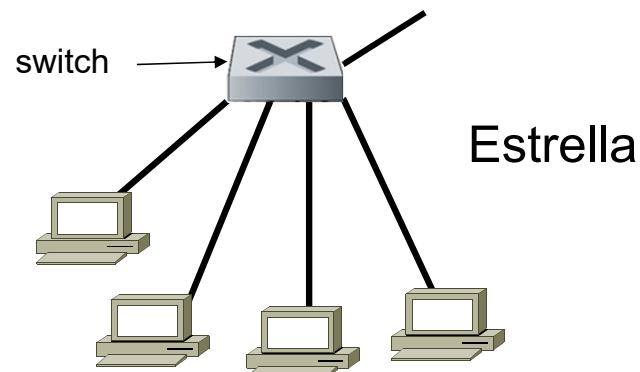
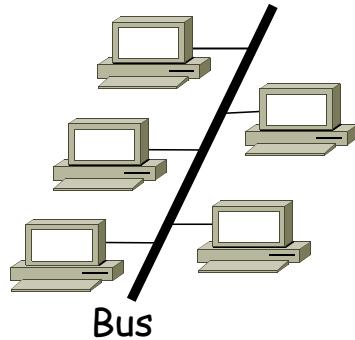


Esquema Ethernet de Metcalfe

En 2010 se aprobaron los nuevos estándares IEEE para trabajar a 40 Gbps y 100 Gbps!!

Topología en estrella

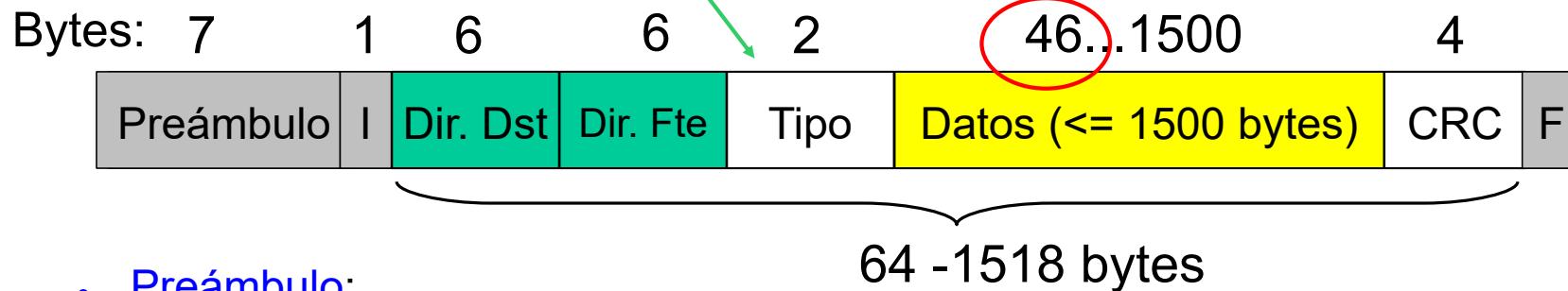
- Topología de bus popular a mediados de los 90
- Actualmente, **topología en estrella**
 - Varias estaciones conectadas a un punto central, utilizando cada una un enlace punto a punto
 - El punto central puede ser:
 - Concentrador (*hub*): estrella de difusión (ya en desuso)
 - **Comutador (*switch*)**: estrella comutada



Formato de trama Ethernet

IEEE 802.3: longitud [0..1500]

Ethernet DIX: tipo [1536..65536] 0x600..0xFFFF



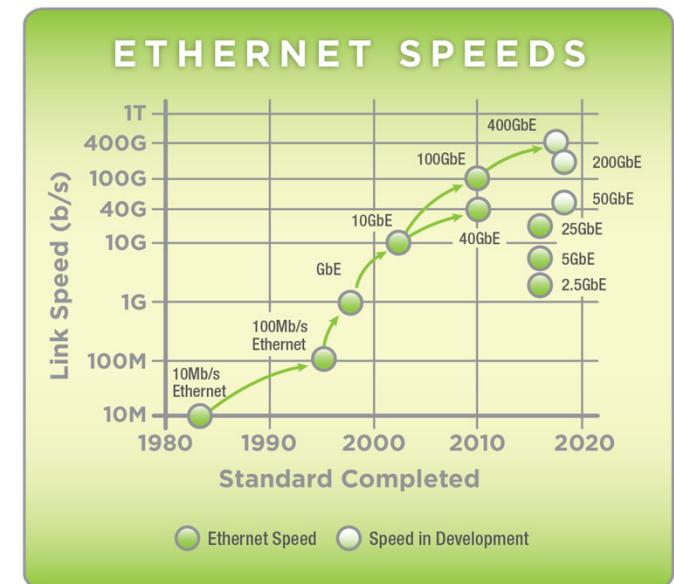
- **Preámbulo:**
 - 7 bytes con el patrón 10101010
 - Se utiliza para sincronizar emisor y receptor con el reloj del emisor
- **Delimitador de inicio de trama (I):**
 - 1 byte con patrón 10101011
- **CRC:** no incluye los bits de preámbulo
- **Delimitador de final de trama (F):** silencio de 96 bits

Ethernet: sin conexión, sin garantías

- No utiliza conexiones
 - Las tramas se envían directamente y son independientes
- Sin garantías: no utiliza reconocimientos
 - Si el contenido de una trama se pierde sólo podrá recuperarse si se utiliza un protocolo de nivel superior con garantías, como TCP
- En topologías de difusión, control de acceso al medio mediante CSMA/CD con *binary exponential backoff*

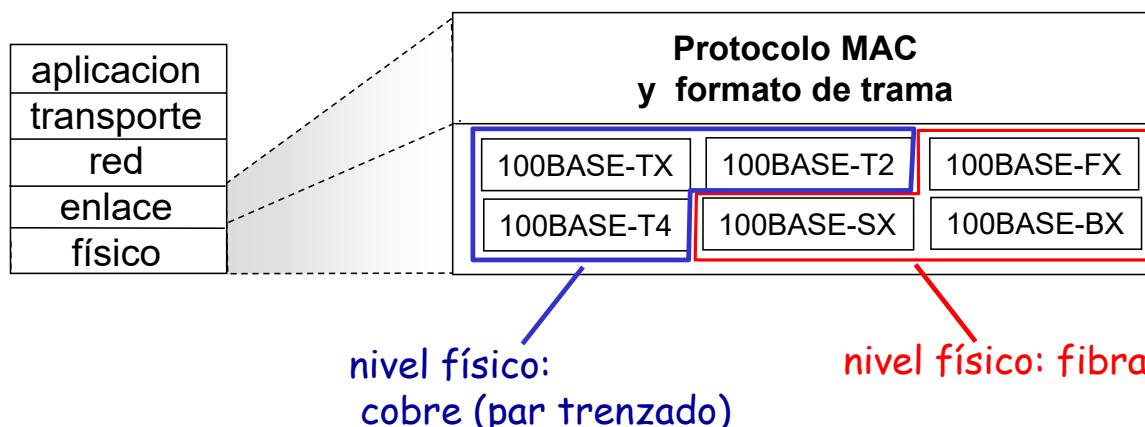
Tecnologías Ethernet

- Diferentes velocidades:
 - 10 Mbps (IEEE 802.3)
 - 100 Mbps (IEEE 802.3u) Fast Ethernet
 - 1.000 Mbps (IEEE 802.3z) 1 Gigabit Ethernet
 - 10.000 Mbps (IEEE 802.3ae) 10 Gigabit Ethernet
 - 40.000/100.000 Mbps (IEEE 802.3ba) 40/100 Gigabit Ethernet
- Características comunes:
 - Mecanismo de entrega sin garantía (best-effort)
 - Servicio sin conexión y entrega no fiable
 - Control de acceso al medio aleatorio (si se requiere)
 - CSMA/CD

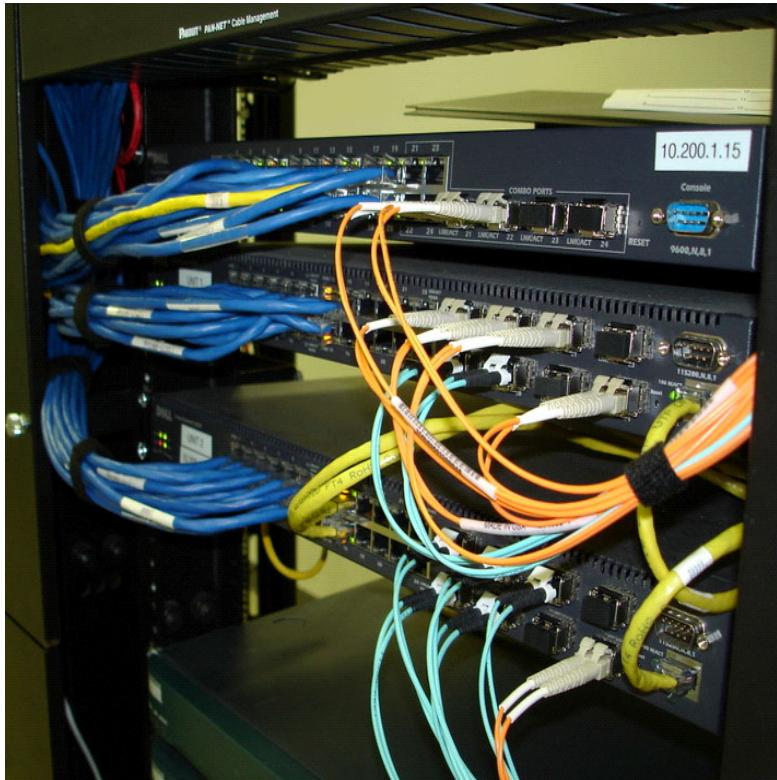


Ethernet: medios de transmisión

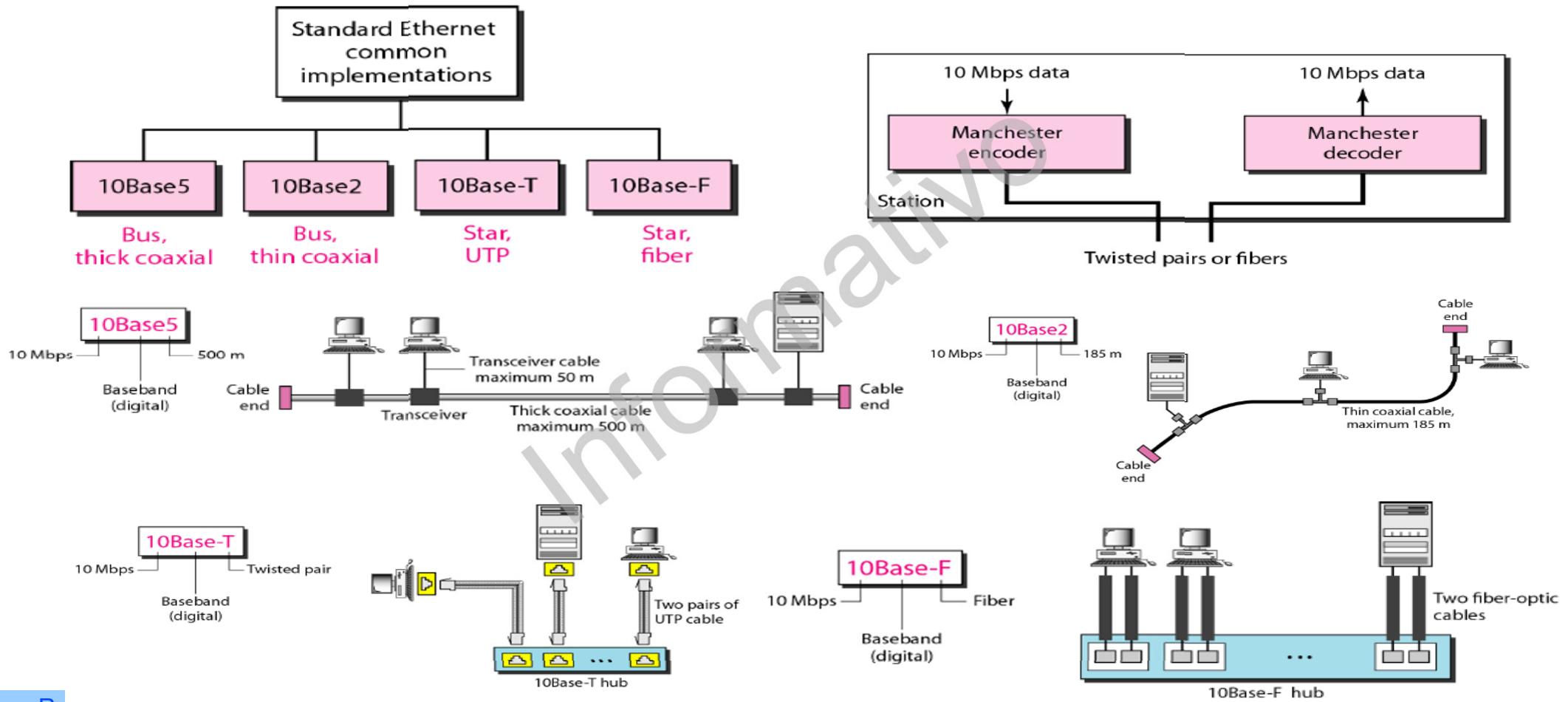
- Soporte a todas las velocidades sobre diferentes medios de transmisión:
 - Par trenzado (10Base-T, 100Base-T4, 100Base-TX, 10GBase-T, etc.)
 - Fibra óptica (10Base-F, 100BaseFX, etc.)
 - Inicialmente, también coaxial (10Base2), hoy en desuso
- Se definen distancias máximas de los enlaces dependientes del medio de transmisión empleado



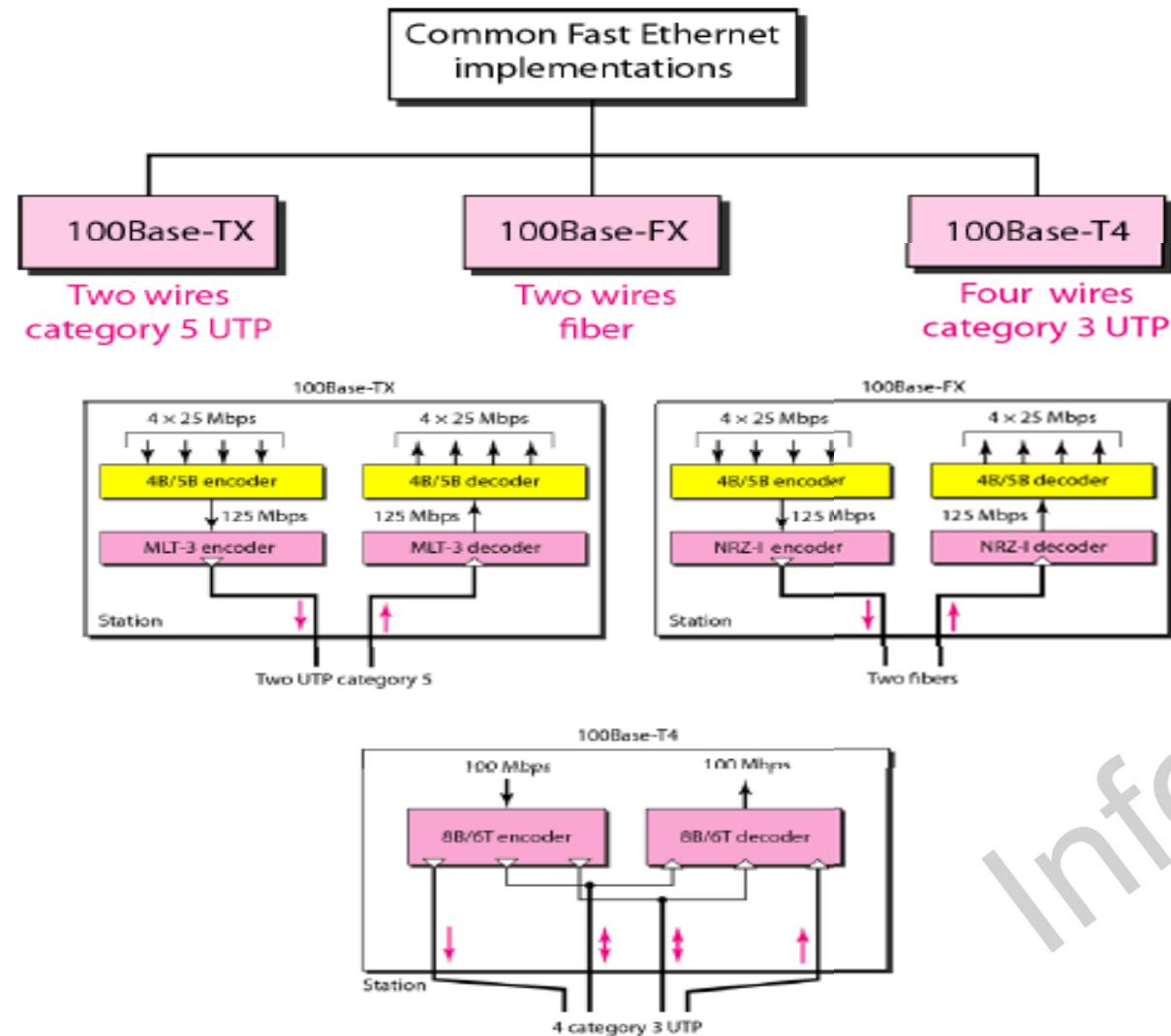
Fibra óptica y par trenzado



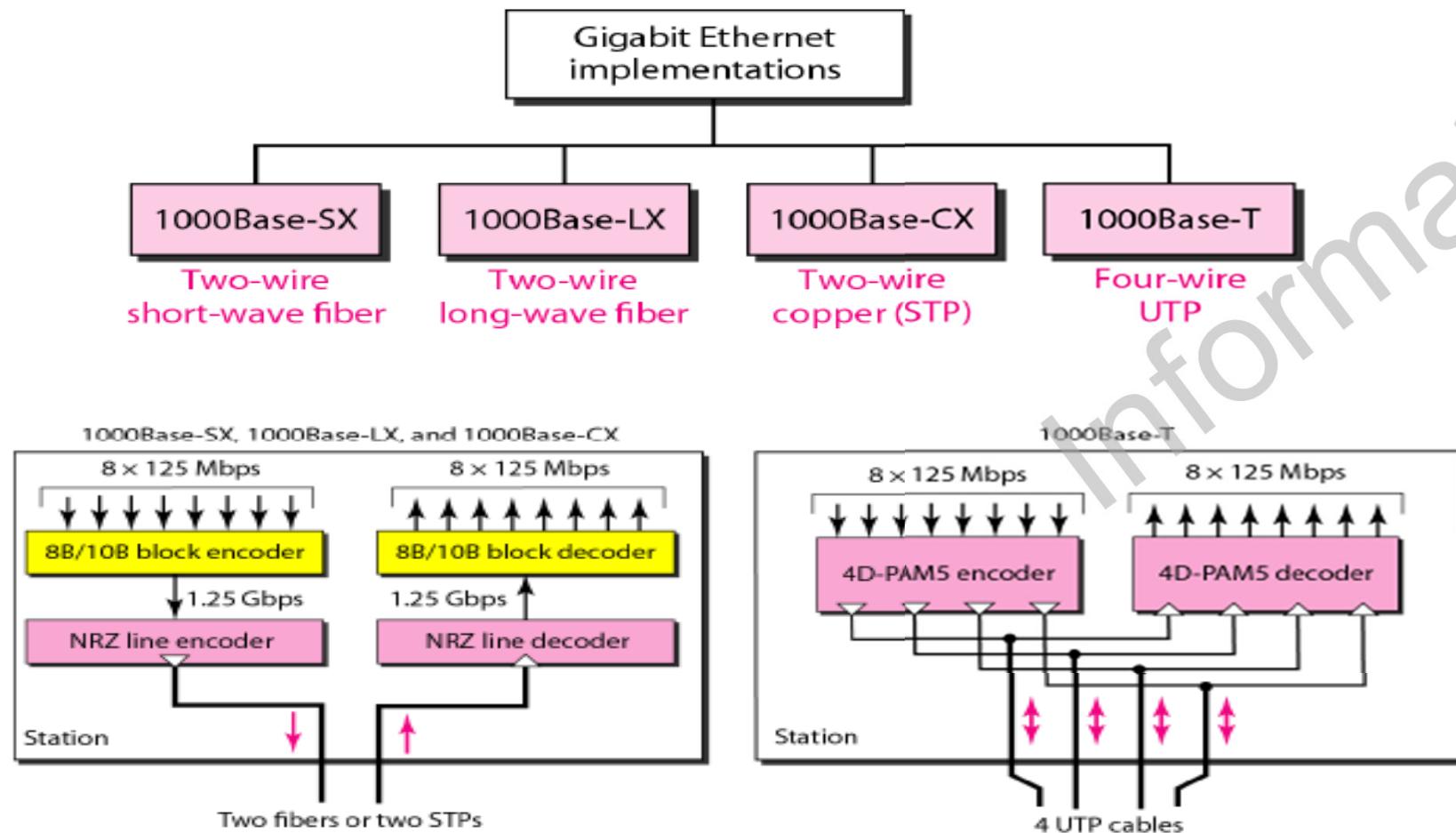
Ethernet a 10 Mbps: IEEE 802.3



Ethernet a 100 Mbps: IEEE 802.3u Fast Ethernet



Ethernet a 1000 Mbps: IEEE 802.3z Gigabit Ethernet



Configuración mixta. Negociado automático

- Los fabricantes han desarrollado adaptadores 10/100Mbps, 100/1000Mbps, ... para par trenzado
- El negociado automático permite a un par de nodos que comparten un enlace negociar las opciones de funcionamiento
- Como mínimo determinará la velocidad a la que deben funcionar

Gigabit Ethernet

- Compatible con 10Base-T y 100Base-T
- Uso principal para interconectar switches de redes Fast Ethernet
- Negociado automático obligatorio
- 10 Gigabit Ethernet:
 - Uso principal como backbone de redes 1Gigabit Ethernet
- 25GbE, 50GbE, 100GbE, 200GbE
 - Uso en Centros de Proceso de Datos

Índice

1. Introducción y servicios del nivel
 - Contexto y terminología
 - Servicios del nivel de red
2. Detección y corrección de errores
 - Paridad, *Checksum* y CRCs
3. Acceso al medio
 - Canales punto a punto y multipunto
 - Partición estática: MDT, MDF
 - Acceso aleatorio: CSMA, CSMA/CD
 - Protocolos por turnos: *Token Bus/Token Ring*
4. Direcccionamiento del nivel de enlace
 - **Práctica 6: Direcciones MAC y ARP**
 - Enrutamiento de paquetes a una LAN externa
5. Dispositivos de interconexión de nivel de enlace
 - Repetidores y concentradores (*Hubs*)
 - Comutadores (*Switches*)
 - Interconexión de comutadores
 - Auto-aprendizaje de comutadores
 - Comutadores y encaminadores
6. Ethernet
 - Estructura de la trama
 - Nivel físico: medios.
 - Fast Ethernet, Gigabit Ethernet, 10G
7. Redes inalámbricas
 - 1. Introducción
 - Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
 - Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
 - El problema del terminal oculto – CDMA
 - 2. Redes Wi-Fi 802.11
 - Arquitectura, asociación con punto de acceso
 - 802.11: acceso múltiple, CSMA/CA, RTS-CTS
 - 802.11: direccionamiento
8. Ejemplo: un día en la vida de una petición web.
 - **Práctica 7: Cortafuegos IPTABLES**
 - **Práctica 8: Análisis de tráfico Wi-Fi 802.11**

Tipos de redes inalámbricas

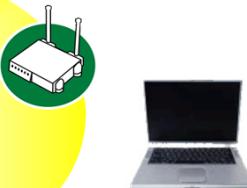
- Wireless Personal Area Network

WPAN:
RFID, Bluetooth,
ZigBee



- Wireless Local Area Network

WLAN (Wi-Fi):
IEEE 802.11



- Wireless Wide Area Network



WWAN
GSM, GPRS (2G)
UMTS (3G)
LTE/SAE (4G)

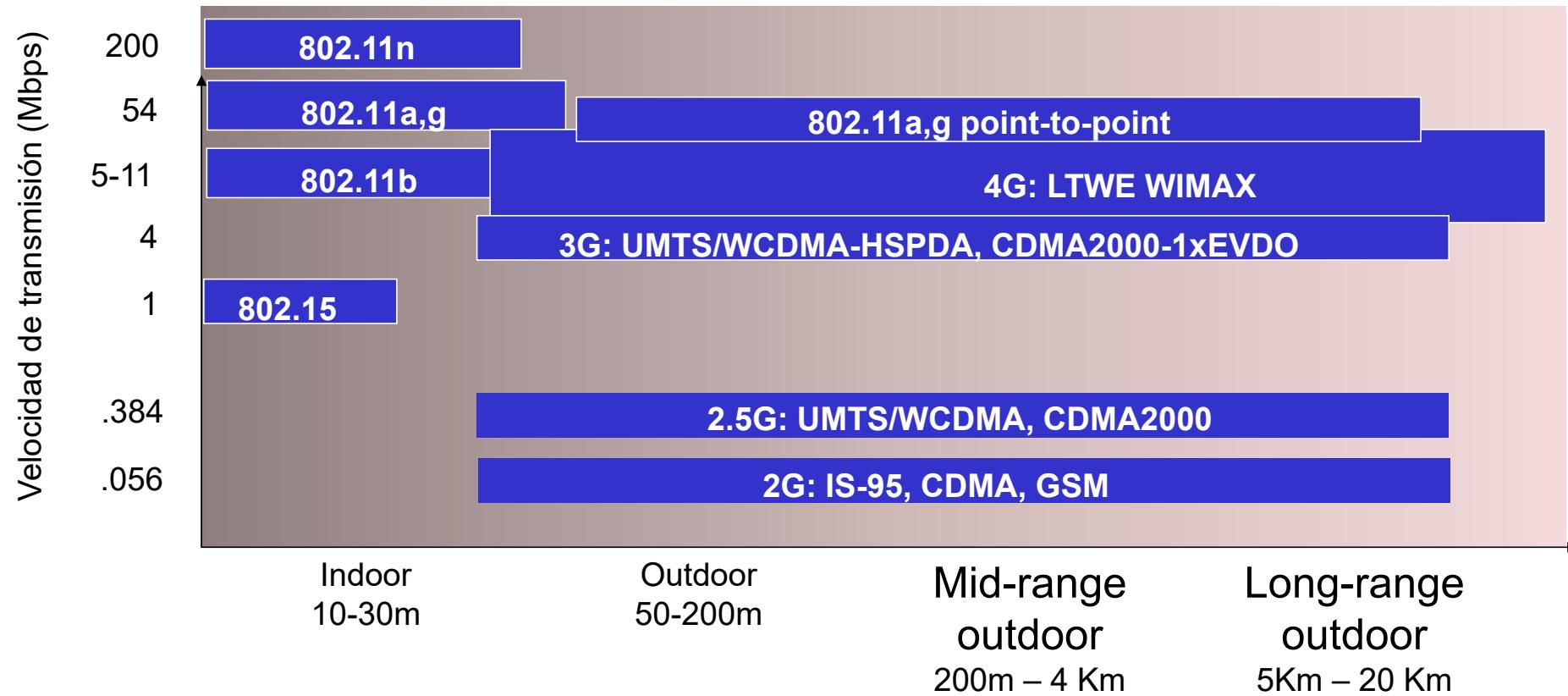
Telefonía

Wireless Metropolitan Area Network

WMAN (Wi-Max):
IEEE 802.16:
Teóricamente ofrece hasta 70 Mbps a una distancia de 50 km.

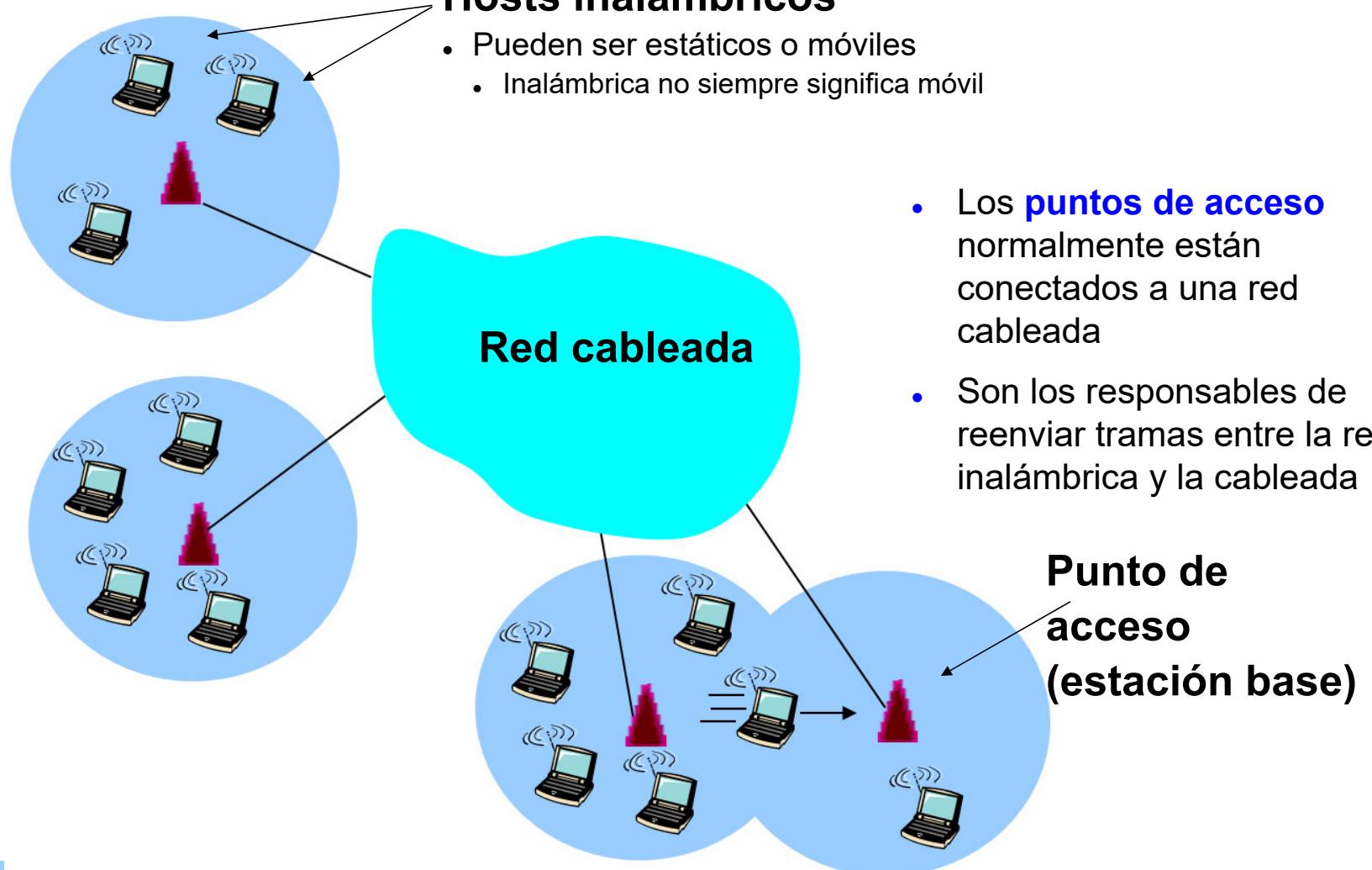


Comparativa de redes inalámbricas



[Kurose 2017]

Elementos de una red inalámbrica



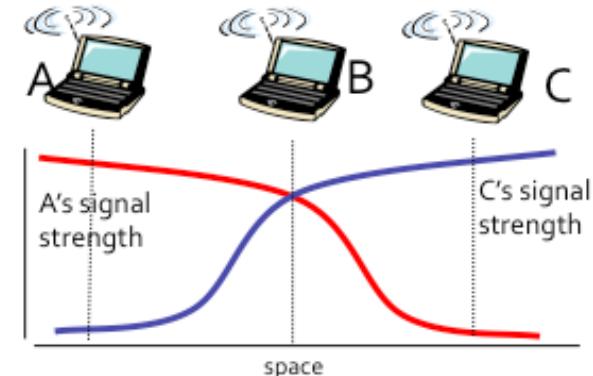
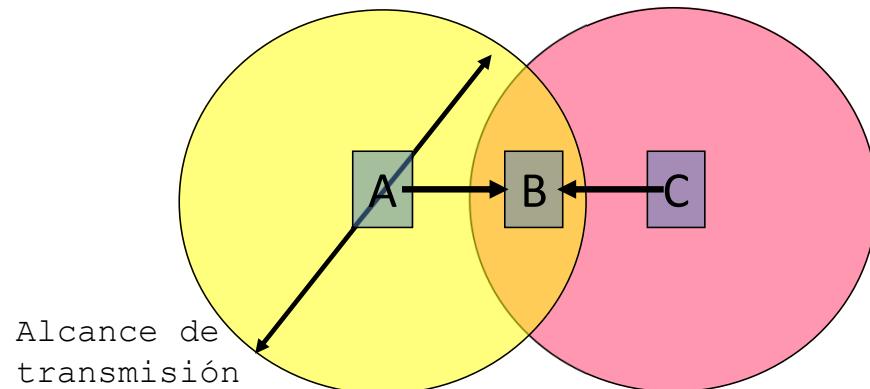
Diferencias entre redes cableadas e inalámbricas

- La potencia de la señal decrece con la distancia mucho más rápidamente
 - Las ondas de radio se atenúan mucho conforme se propagan. Pueden incluso llegar a desaparecer tras cierto recorrido
- Interferencias con otras fuentes de señal
 - Las frecuencias estándar para las redes inalámbricas están compartidas con las redes de telefonía móvil. Además, diversos aparatos como motores eléctricos también producen interferencias
- Propagación multicamino
 - Las señales de radio se reflejan en los objetos y en el suelo, llegando a la antena diferentes copias de la señal en momentos de tiempo ligeramente distintos

Todo esto hace que la comunicación inalámbrica sea mucho más difícil que la comunicación por cable

Problema del terminal oculto

- La señal transmitida tiene un alcance limitado
 - Puede que algunas estaciones no reciban la transmisión



- A y C no se escuchan:
 - (a) un obstáculo lo impide
 - (b) la señal no tiene suficiente potencia
- La detección de colisión no funciona entre ellas
- Pero B recibe las dos transmisiones solapadas

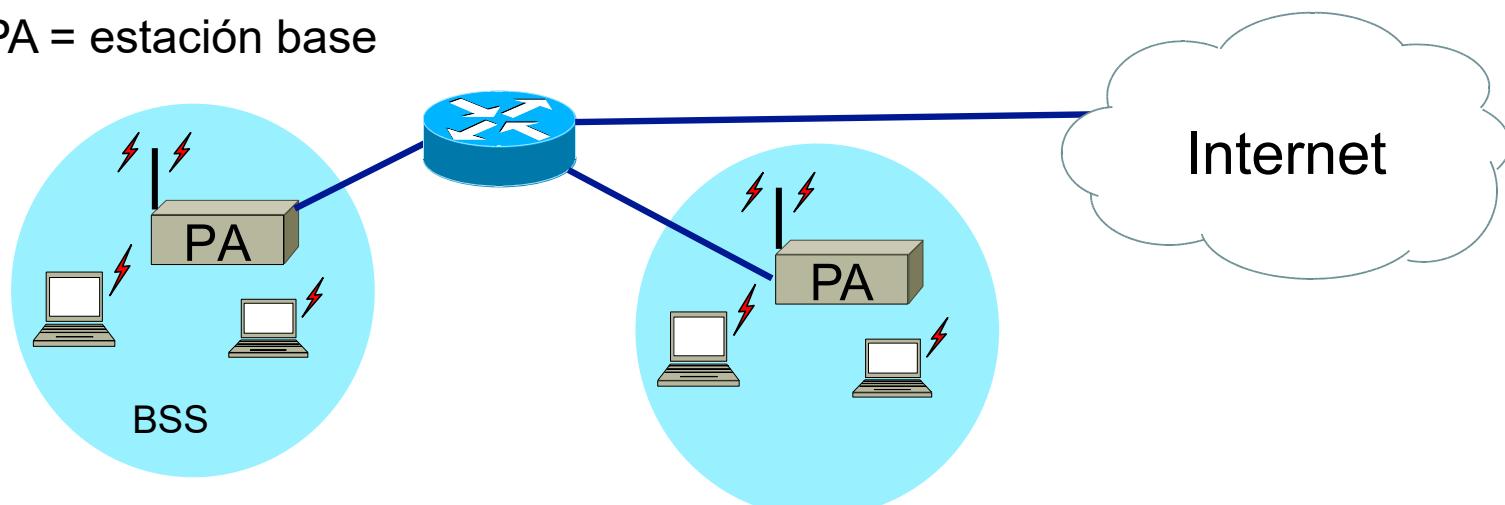
IEEE 802.11 (LAN inalámbrica)

Estándares IEEE 802.11	Rango de frecuencias	Velocidad de transmisión
802.11b	2.4 - 2.485 GHz	Hasta 11 Mbps
802.11a	5.1 - 5.8 GHz	Hasta 54 Mbps
802.11g	2.4 - 2.485 GHz	Hasta 54 Mbps
802.11n	2.4 – 2.485 Ghz 5.1 – 5.225 GHz	Hasta 600 Mbps* <small>* Usando 4 antenas (poco habitual)</small>
802.11ac	5.1 - 5.8 GHz	Hasta 7 Gbps* <small>* Usando 8 antenas</small>

- Características comunes:
 - Control de acceso al medio distribuido (CSMA/CA)
 - Mismo formato de trama
 - Pueden reducir su velocidad de transmisión para abarcar distancias mayores
 - Comparten la misma arquitectura
 - Compatibles si trabajan en la banda de frecuencias de 2,4 GHz (no todos)

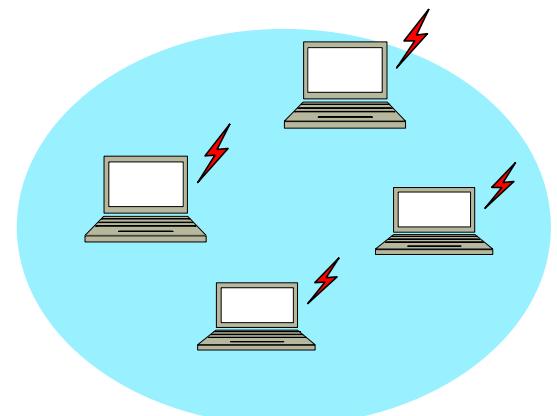
Arquitectura de las redes 802.11

- La señal transmitida decae con la distancia
 - El espacio se divide en áreas de alcance de la señal denominadas celdas (BSA: *Basic Service Area*)
 - Contiene una o más estaciones inalámbricas que pueden ser móviles o fijas (BSS: *Basic Service Set*)
 - Puede contener un punto de acceso (PA) que normalmente se conecta a una red cableada
 - PA = estación base



Modos de funcionamiento (I)

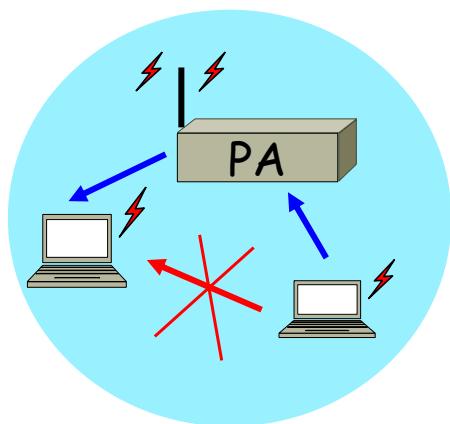
- En una celda, pueden coexistir simultáneamente 2 modos de funcionamiento:
 - Independiente:
 - **Redes ad-hoc** (p. e.: portátiles en clase)
 - No requiere instalar infraestructura
 - Limitado temporal y espacialmente
 - No tiene conexión al exterior
 - Las redes se forman “al vuelo”, cuando dispositivos móviles próximos se detectan
 - Control distribuido:
 - Las estaciones se comunican directamente unas con otras



Modos de funcionamiento (II)

- Con **infraestructura**:

- Las estaciones se comunican a través de un **punto de acceso (PA)**
 - Deben asociarse al PA para poder transmitir
- Configuración de un PA:
 - El administrador tiene que asignarle:
 - Un identificador, SSID (**Service Set IDentifier**), que identificará a la red (p.ej., UPVNET)
 - La frecuencia de la señal a utilizar (nº de canal)
 - Posible interferencia con puntos de acceso (PA) vecinos



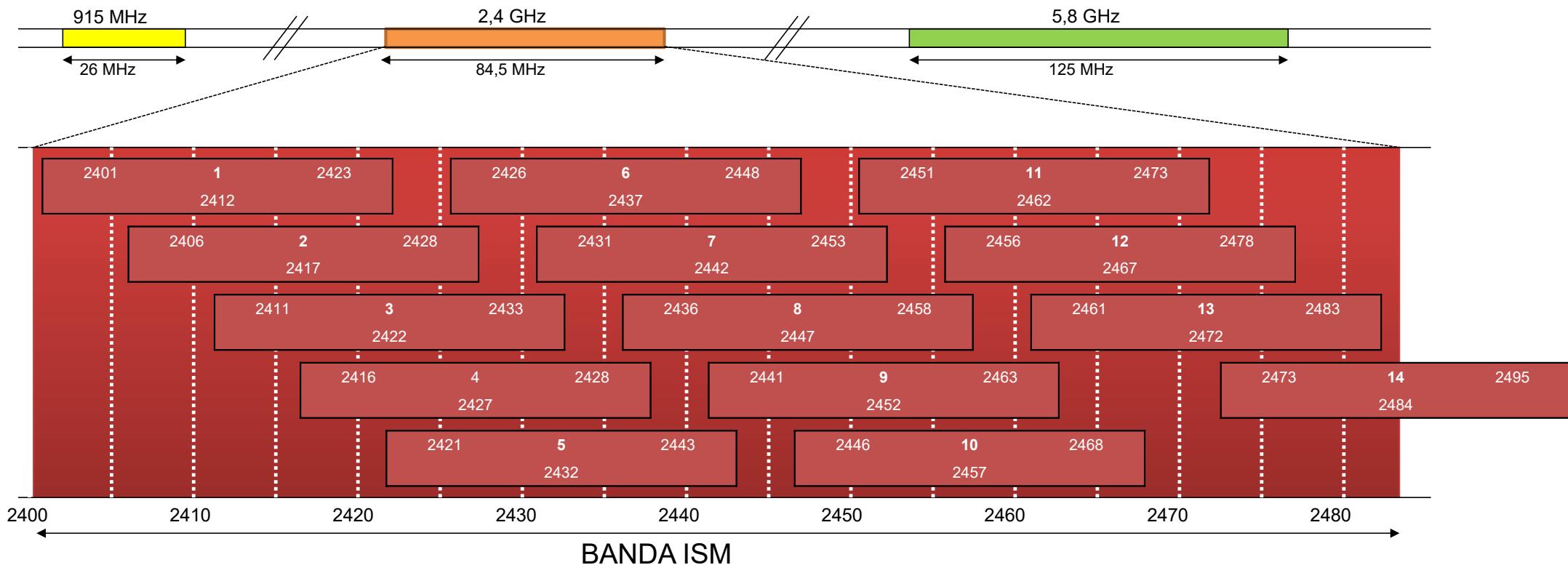
Distribución de canales en frecuencia

- Ejemplo: canales en la banda de 2,4 GHz

- 14 canales de 22 MHz

- En Europa disponibles sólo [1-13]

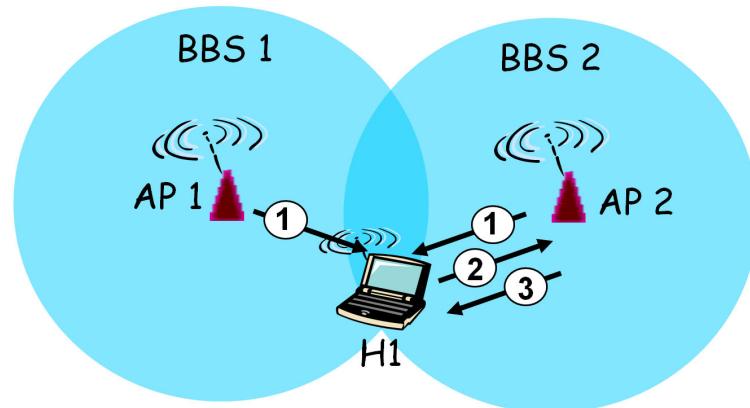
Frecuencia inicial	Número de canal	Frecuencia final
Frecuencia central		



Asociación a un PA

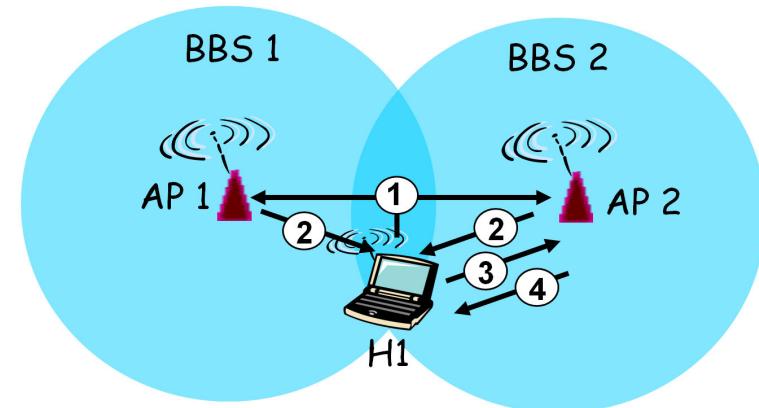
- Cada PA envía periódicamente una trama de ofrecimiento de asociación (**beacon frames**):
 - Incluye el SSID y la dirección MAC del PA
- Una estación móvil
 - Selecciona un PA e intenta asociarse a él
 - Los PAs pueden solicitar la **autentificación** de la estación:
 - Por dirección MAC
 - Por nombre de usuario y contraseña para permitir la asociación
 - Cuando la estación queda asociada a un PA debe obtener una dirección IP de la subred del PA (normalmente mediante DHCP)
 - A nivel de red el PA es transparente (los demás hosts/routers en Internet no ven el PA)

Asociación a un PA pasivo y activo



Exploración Pasiva:

- (1) Los PA envían beacon frames
- (2) El host H1 envía una petición de asociación al PA seleccionado
- (3) El PA seleccionado contesta con una respuesta de asociación

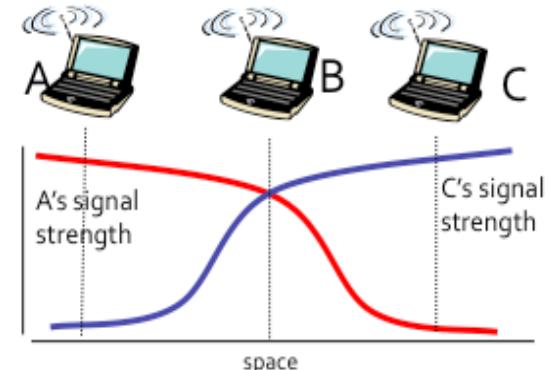


Exploración Activa:

- (1) El host H1 envía por difusión una trama de sondeo
- (2) Los PA responden a la trama de sondeo
- (3) El host H1 envía una petición de asociación al PA seleccionado
- (4) El PA seleccionado devuelve una respuesta de asociación

¿Qué tipo de protocolo MAC es adecuado?

- Medio compartido con posibilidad de colisiones
 - ¿Es adecuado CSMA/CD?
 - Detección de portadora
 - Si el emisor escucha el canal antes de transmitir, ¿qué información obtiene?
 - Detección de colisión
 - ¿Dónde se producen las colisiones?
 - ¿Cómo las podemos detectar?



Acceso al medio en redes inalámbricas

- 802.11: **CSMA** (*Carrier Sense Multiple Access*)
 - Comprobar el canal antes de transmitir
 - Si está ocupado esperar a que quede libre
- En las redes 802.11 no hay detección de colisión
 - Son difíciles de detectar mientras se transmite debido a la baja potencia de la señal recibida
 - Las estaciones funcionan en modo half-dúplex
 - No se pueden detectar todas las colisiones (problema del terminal oculto)
 - Objetivo: evitar colisiones **CSMA/CA** (**Collision Avoidance**)

CSMA/CA

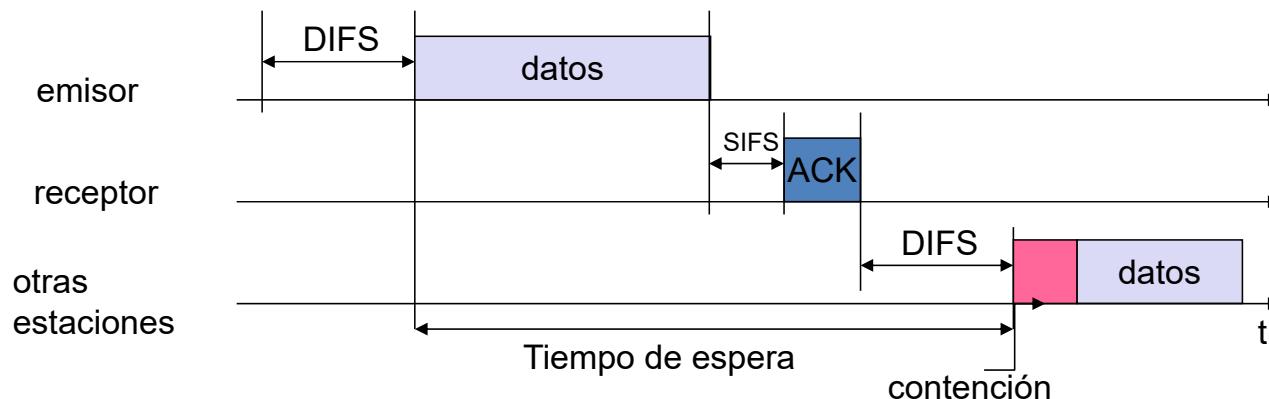
(Carrier Sense Multiple Access with Collision Avoidance)

CSMA/CA emisor

- Si detecta el canal libre durante **DIFS** segundos:
 - Transmite la trama completa (sin escuchar)
- Si detecta el canal ocupado sigue escuchando:
 - Cuando queda libre espera un tiempo aleatorio (alg. *Backoff*)

CSMA/CA receptor

- Si trama recibida OK, **devuelve ACK** despues de **SIFS** segundos (ACK necesario y obligatorio debido al problema de la estación oculta)



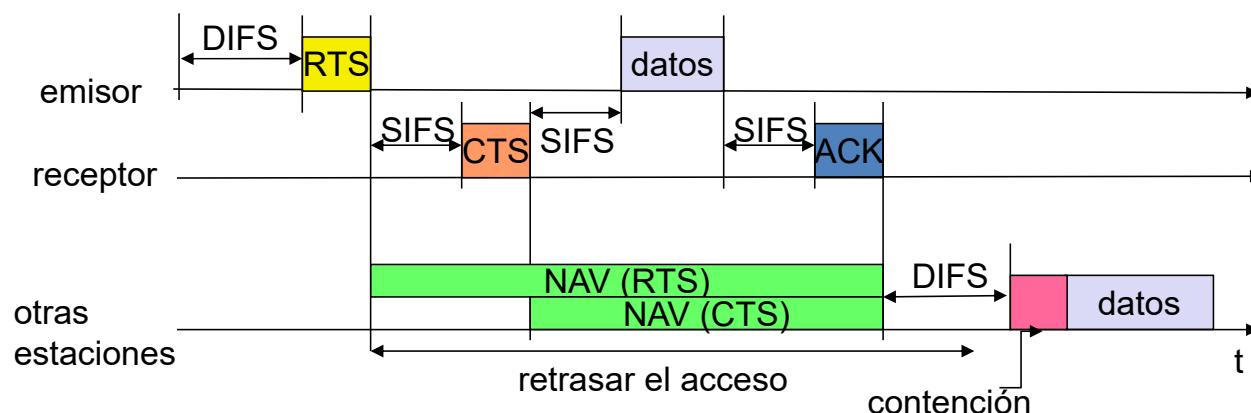
DIFS: Distributed Inter-frame Space

SIFS: Short Inter-frame Space

DIFS > SIFS

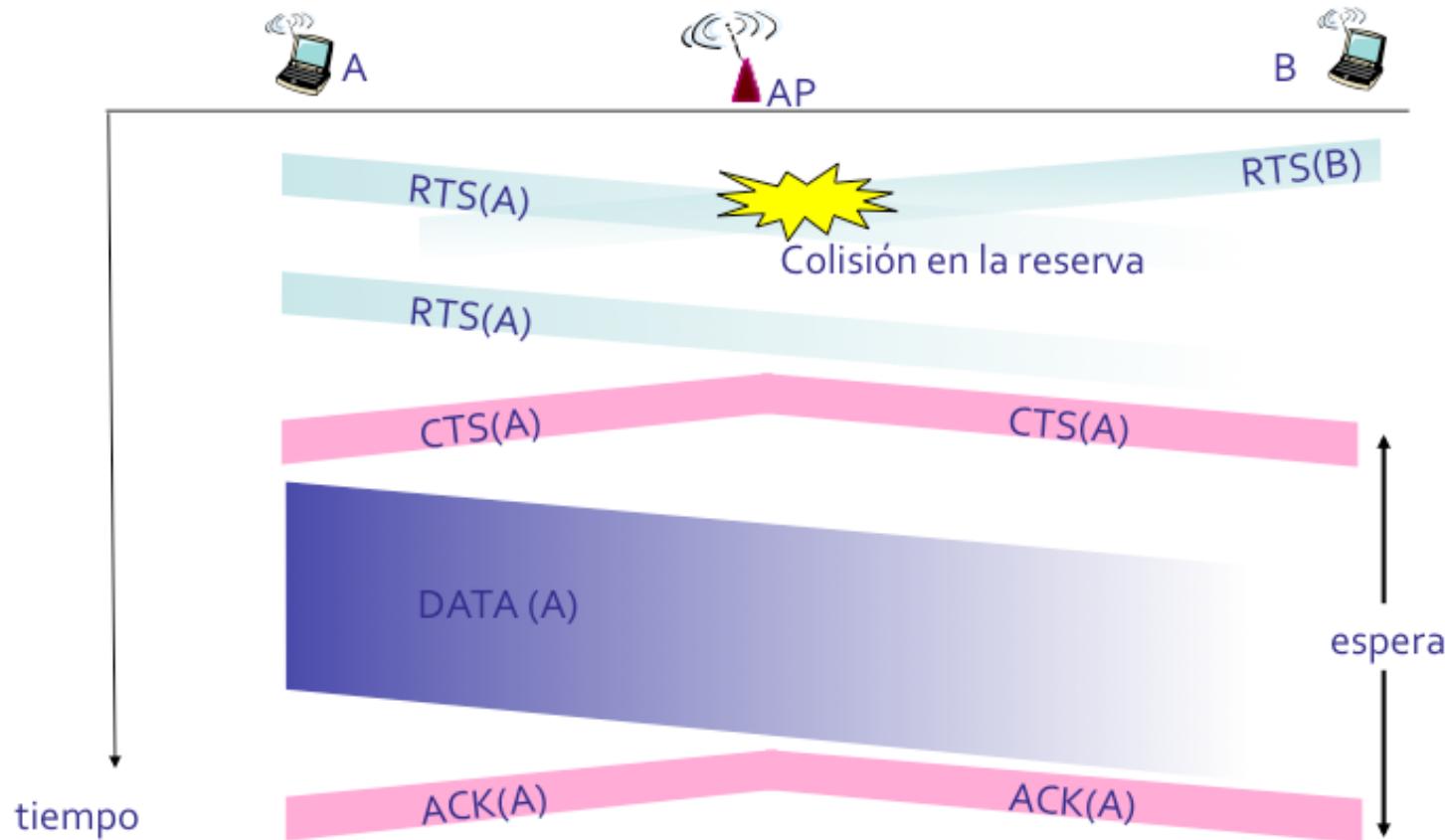
CSMA/CA: Evitación de colisión (poco empleado)

- Una estación solicita al PA transmitir una trama de datos enviando por difusión una trama **RTS** (Request To Send)
 - En la trama RTS se indica el tiempo necesario para transmitir la trama de datos completa
- El PA contesta enviando por difusión una trama **CTS** (Clear To Send) que:
 - Permite transmitir a la estación solicitante
 - Prohibe a las otras otras estaciones transmitir durante el tiempo indicado
- Sólo se realiza el intercambio de tramas RTS/CTS cuando el tamaño de la trama de datos a enviar supera un umbral definido en la estación
 - **RTS/CTS normalmente no se utiliza** (umbral>MTU)

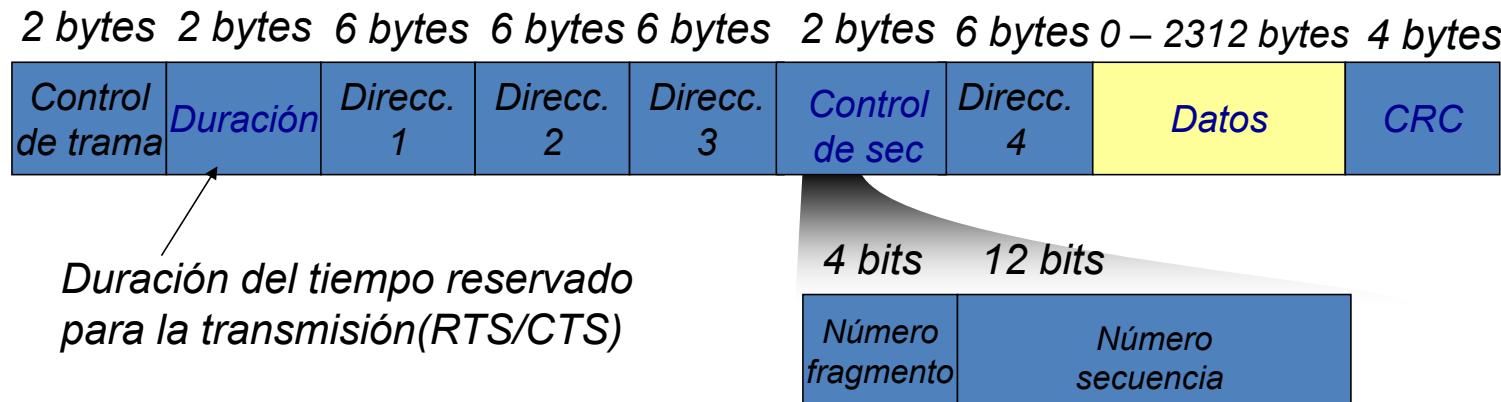


Network Allocation Vector (NAV): Campo que indica el tiempo que el canal estará ocupado.

Evitación de colisiones: intercambio RTS-CTS

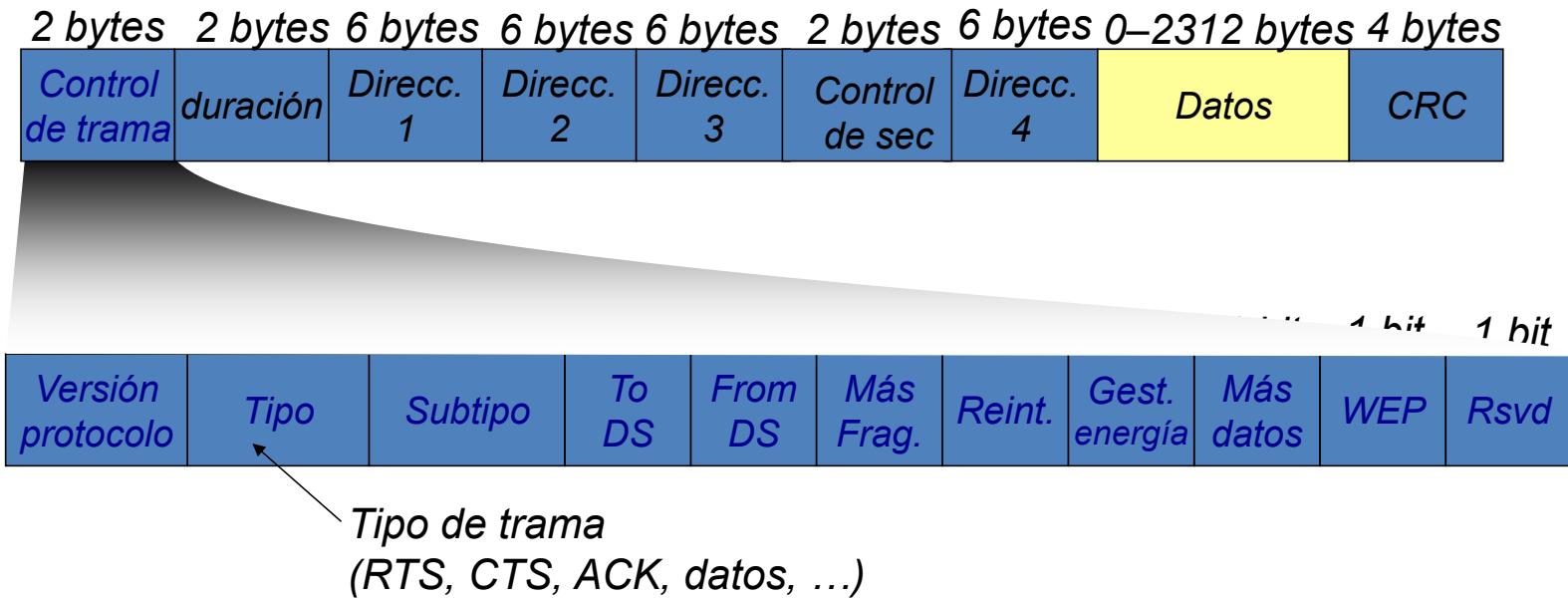


Formato de trama 802.11



- Duración / ID de conexión:
 - Si se usa como un campo de duración, indica el tiempo (en microsegundos) que se asignará el canal para la transmisión exitosa de una trama MAC. En algunas tramas de control, este campo contiene un identificador de asociación o conexión.
- Control de secuencia:
 - Contiene un subcampo de número de fragmento de 4 bits, usado para fragmentación y reensamblaje, y un número de secuencia de 12 bits usado para numerar tramas enviadas entre un transmisor y receptor dados.
- Datos de la trama:
 - Puede contener datos del protocolo del siguiente nivel LLC (que contienen datos de nivel de red, por ejemplo) o información de control MAC.
- CRC: comprobación de redundancia cíclica de 32 bits.

Formato de trama 802.11



❖ Control de Trama:

- Indica el tipo de trama (control, gestión o datos) y proporciona información de control. La información de control incluye si la trama va hacia o desde un DS (Sistema Distribuido), información de fragmentación e información de privacidad

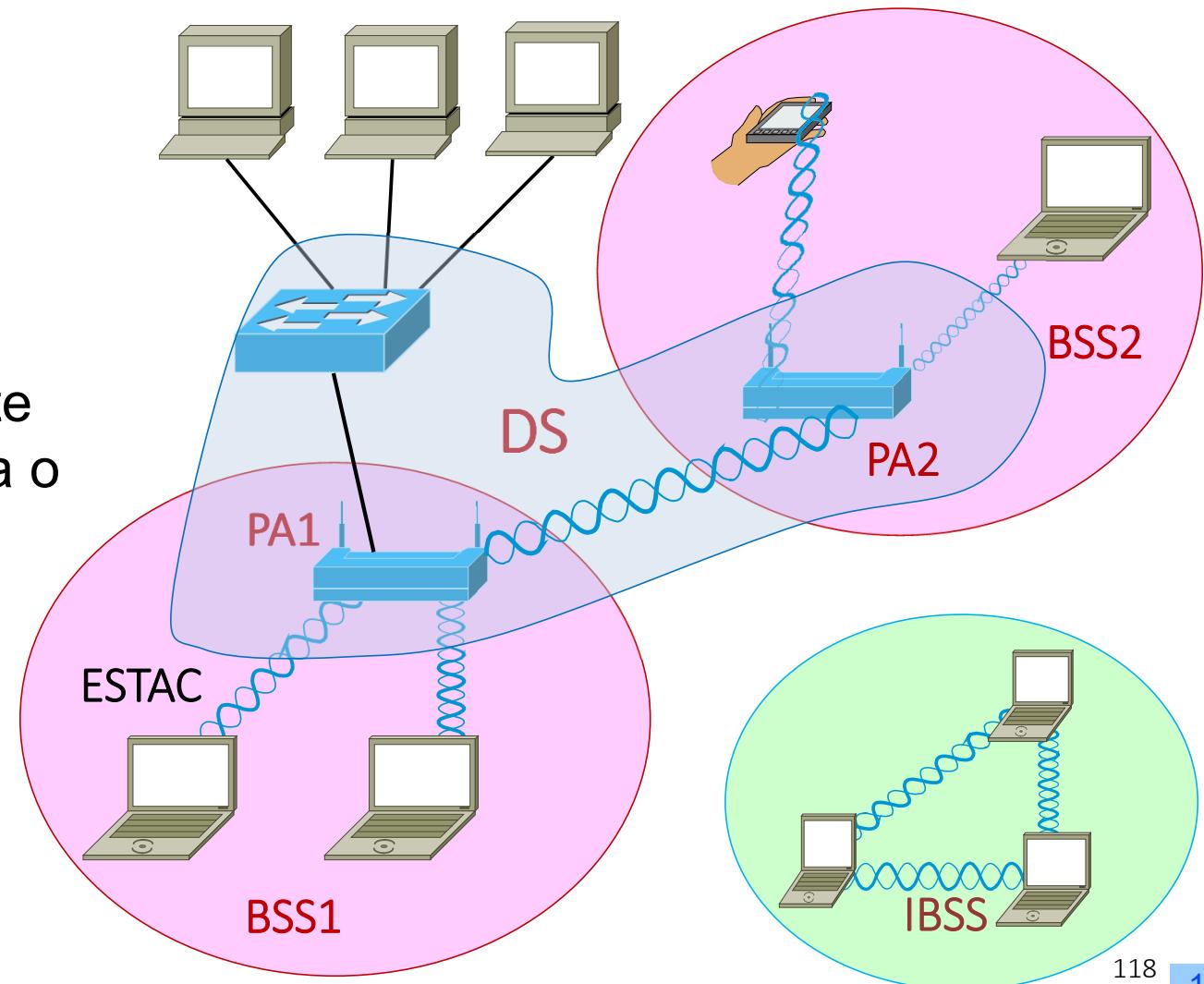
Formato de trama 802.11: tipos de tramas

- *Tramas de Control*
 - RTS / CTS / ACK
 - CF-Poll / CF-End
- *Tramas de gestión*
 - **Beacons** : tramas de invitación a la asociación (*beacon frame*) que anuncian la existencia de una red, utilizadas en el escaneo pasivo
 - **Probe Request/Response**: utilizadas en el escaneo activo
 - **Association Request/Response**
 - **Dissociation/Reassociation**
 - **Authentication/Deauthentication**
- *Tramas de datos*

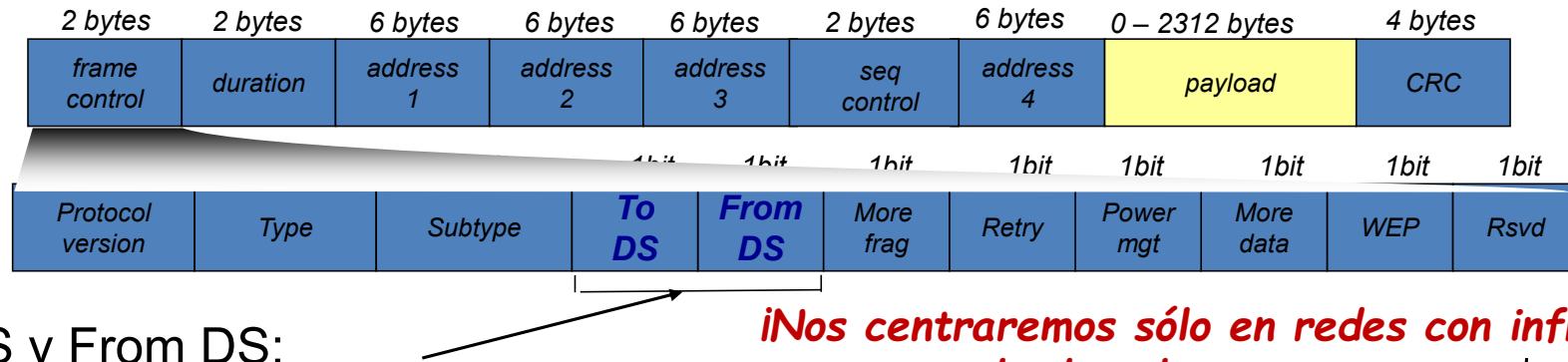
¿Qué es un DS en IEEE 802.11?

Sistema de distribución
(*Distribution System*, DS)

Conjunto de servicios que permite
conectar un PA a la red cableada o
varios PA entre sí



Trama 802.11: direccionamiento



- To DS y From DS:

iNos centraremos sólo en redes con infraestructura y tramas de datos!

- Ocupan 1 bit cada uno. Indican la dirección en la que va la trama, si una trama de datos se dirige hacia un sistema de distribución (DS) o proviene de él.
 - Como en una red de infraestructura 802.11, todas las tramas se transmitirán a través del Punto de Acceso (PA), podemos ver los bits To DS y From DS como los bits que indican si la trama va hacia el Punto de Acceso o viene de él

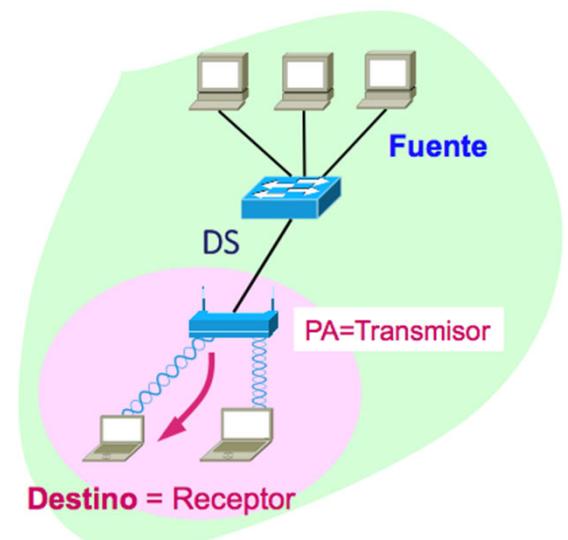
To DS	From DS	Significado	Modo
0	0	Una trama de datos dirigida de una STA a otra STA dentro del mismo IBSS, así como todas las tramas de gestión y control	Ad Hoc
0	1	Trama de datos enviada desde el DS	Infraestructura
1	0	Trama de datos destinada hacia el DS	Infraestructura
1	1	Trama del Sistema de distribución inalámbrico (Wireless distribution system (WDS)) siendo enviada desde un PA a otro PA	WDS

Trama 802.11: direccionamiento

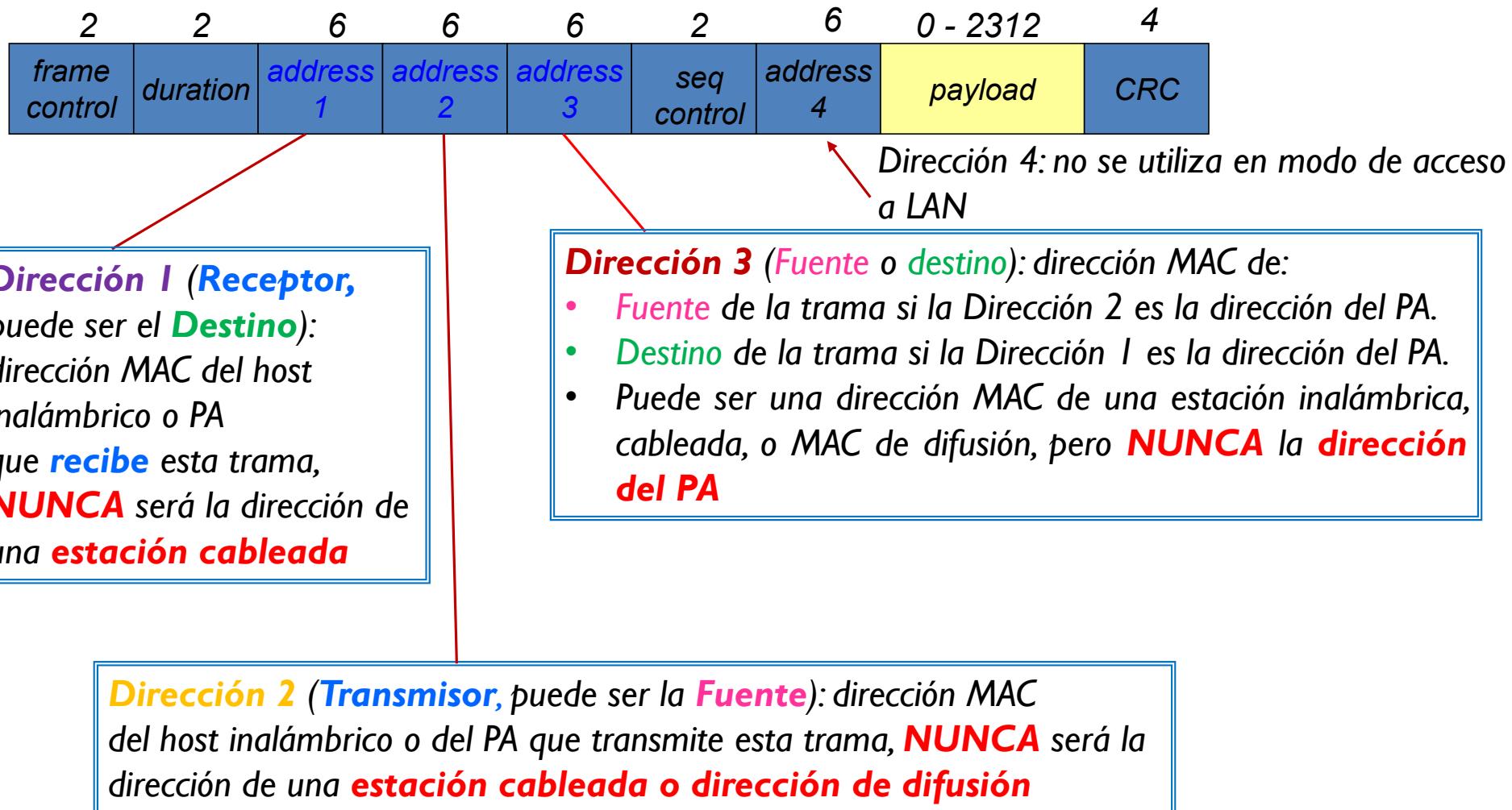
- En modo infraestructura
 - En 802.11 la transmisión de todas las trama se realizará a través del Punto de Acceso (PA) para llegar a cualquier otro host (inalámbrico, cableado o la interfaz del router)
 - Por lo tanto, el PA aparecerá en cada trama de datos 802.11 como transmisor o receptor
 - Sustituye la dirección MAC del remitente original de la trama (si PA actúa como transmisor) o del destino final de la trama (si PA actúa como receptor)
 - Para conservar la dirección MAC de la trama del remitente original o el destino final, se utilizará un tercer campo de dirección

Trama 802.11: direccionamiento

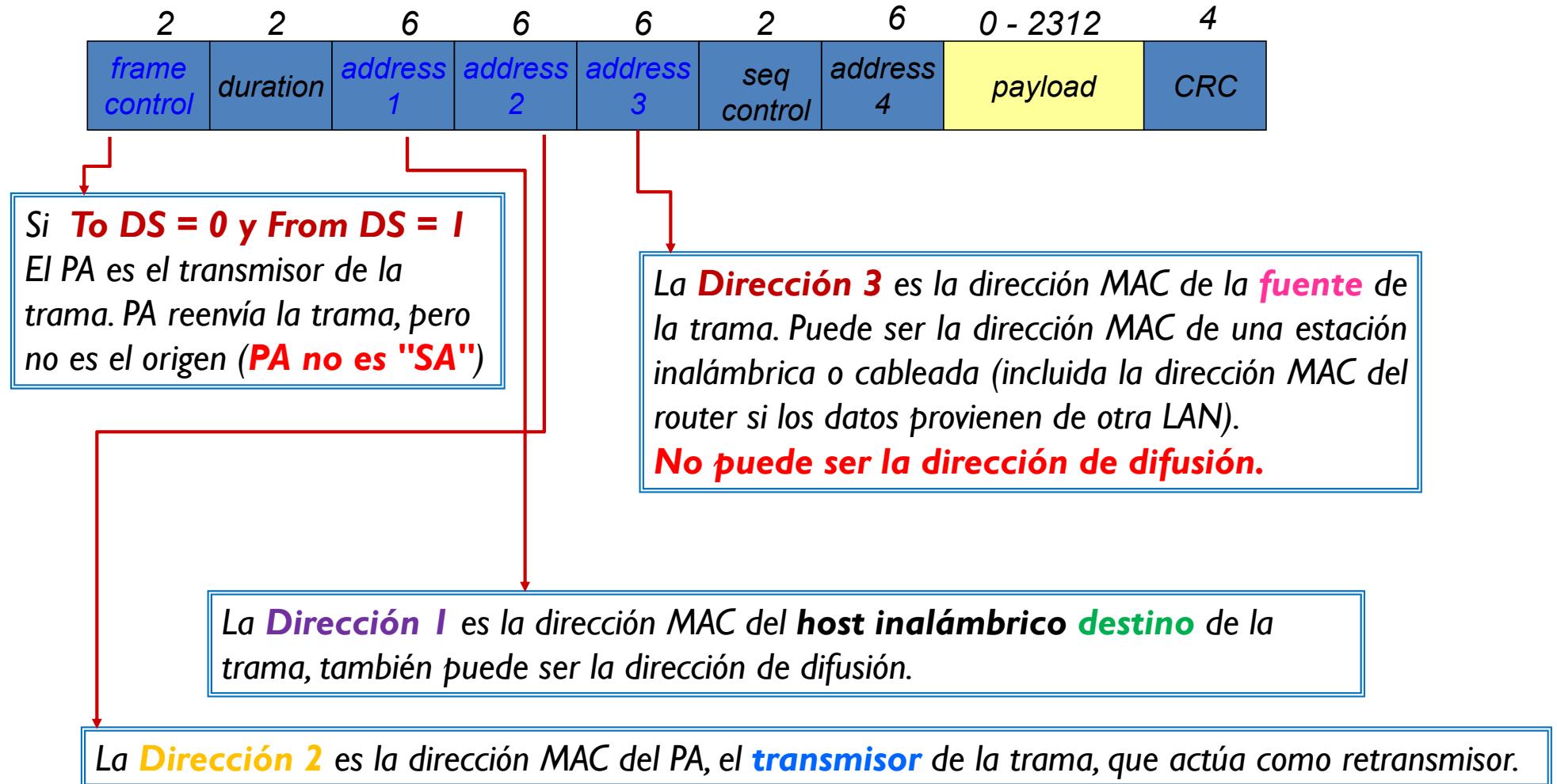
- Nomenclatura:
 - “Dirección destino” o “DA” (*Destination Address*) es la MAC del destino final de la trama
 - Procesará el paquete contenido en la trama
 - “Dirección fuente” o “SA” (*Source Address*) es la MAC de la fuente original de la trama
 - “Dirección del receptor” o “RA” (*Receiver Address*) es la MAC que identifica al dispositivo inalámbrico que es el destinatario inmediato de la trama
 - “Dirección del transmisor” o “TA” (*Transmitter Address*) es la MAC que identifica al dispositivo inalámbrico que está transmitiendo la trama
- Campos de dirección:
 - **Dirección 1** sólo puede ser “Receptor” (inalámbrico)
 - Si “Receptor” ≠ PA entonces “Receptor” = “Destino”
 - **Dirección 2** solo puede ser “Transmisor” (inalámbrico)
 - Si “Transmisor” ≠ PA entonces “Transmisor” = “Fuente”
 - **Dirección 3** solo puede ser “Fuente” o “Destino”
 - En modo infraestructura no habrá aparecido en los otros campos



Trama 802.11: direccionamiento

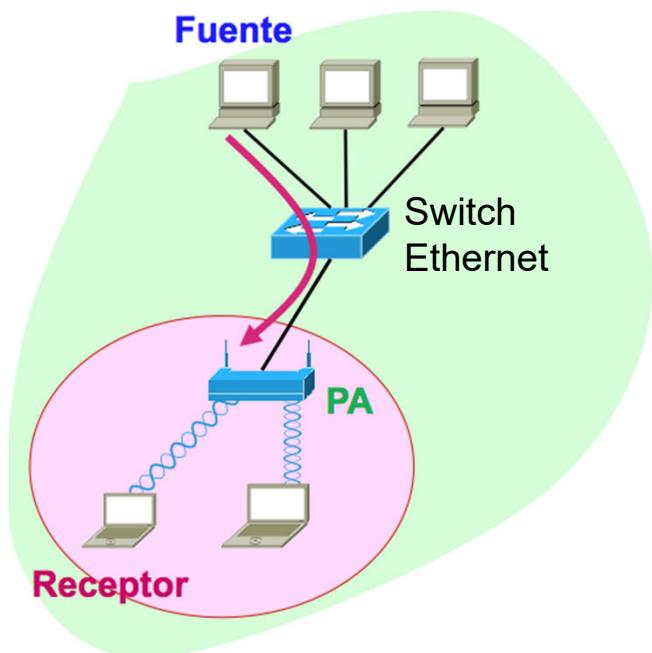


Trama 802.11: direccionamiento



Transmisión desde red cableada a red inalámbrica – paso 1

Trama en red IEEE 802.3 (Ethernet) desde Fuente a PA



Destinada a **receptor** (en red wi-fi):

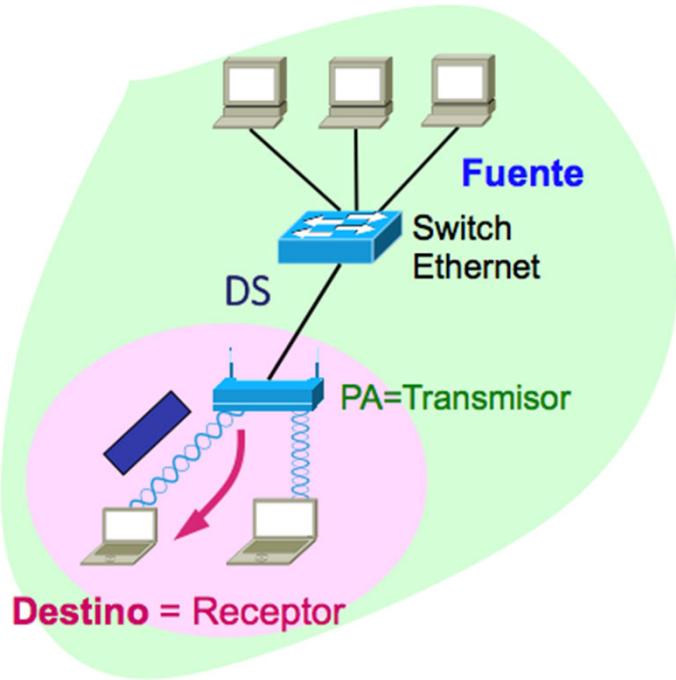
Trama 802.3



¡El PA es transparente desde la red Ethernet!

- Permite la comunicación entre la red inalámbrica y la cableada:
 - Recibe las tramas Ethernet destinadas a la red inalámbrica y genera las tramas inalámbricas (IEEE 802.11)
 - Recibe las tramas inalámbricas (IEEE 802.11) destinadas a la red cableada y genera tramas Ethernet

Transmisión desde red cableada a red inalámbrica – paso 2



Trama en red IEEE 802.11 (wifi) desde PA a Destino

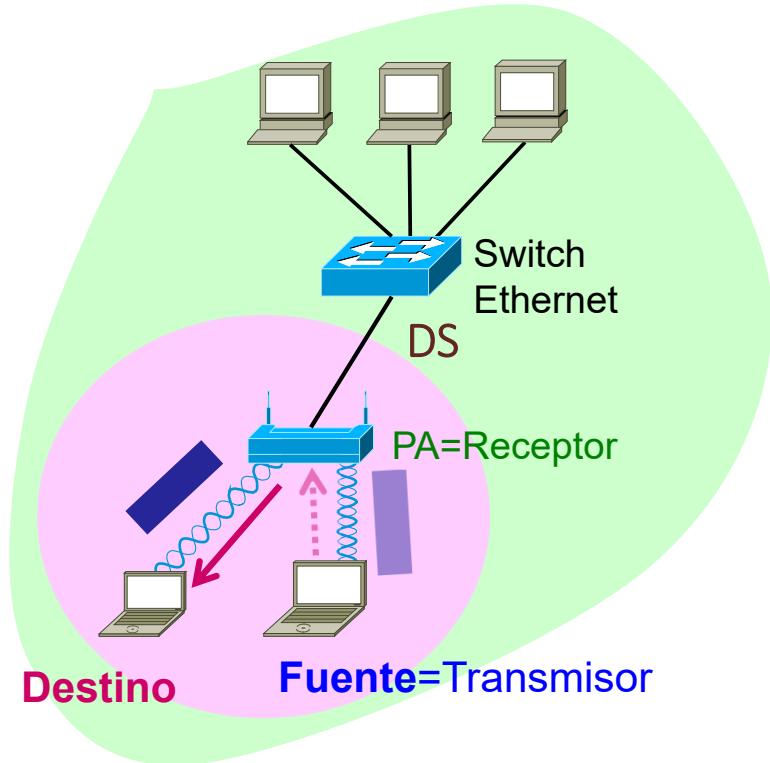
To DS = 0, From DS = 1

- Generación de la trama inalámbrica (IEEE 802.11) a partir de la trama Ethernet en el PA
 - Dirección 1: MAC estación inalámbrica receptora
 - Dirección 2: MAC estación inalámbrica transmisora (MAC_PA)
 - Dirección 3: MAC fuente del paquete

a de

To DS	From DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	1	MAC_Receptor	MAC_PA (BSSID)	MAC_Fuente	No se usa

Transmisión entre estaciones inalámbricas – paso 2



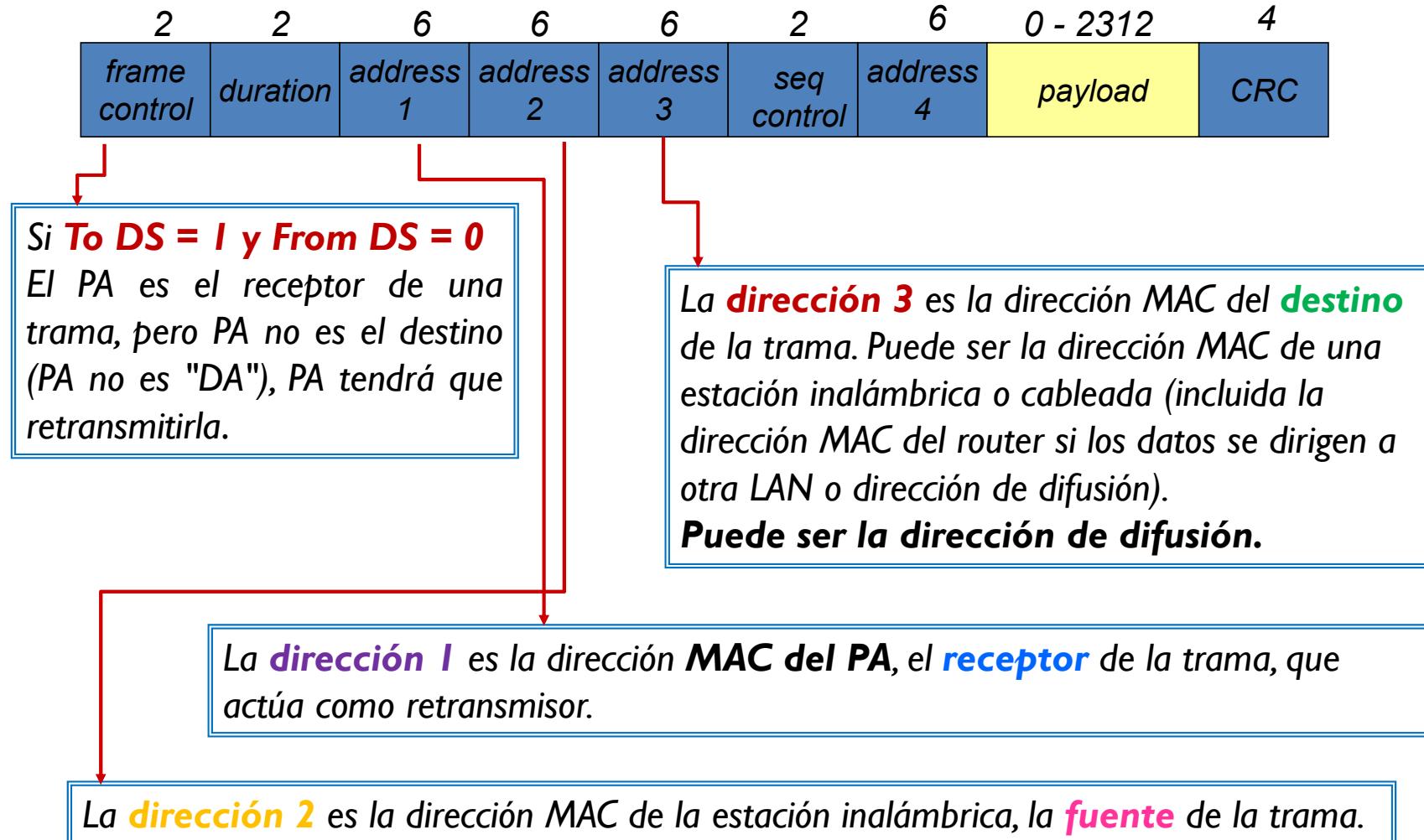
To DS = 0, From DS = 1

- Generación de la trama inalámbrica (IEEE 802.11) desde PA a Receptor
 - Dirección 1: MAC estación inalámbrica receptora
 - Dirección 2: MAC estación inalámbrica transmisora (MAC_PA)
 - Dirección 3: MAC fuente del paquete

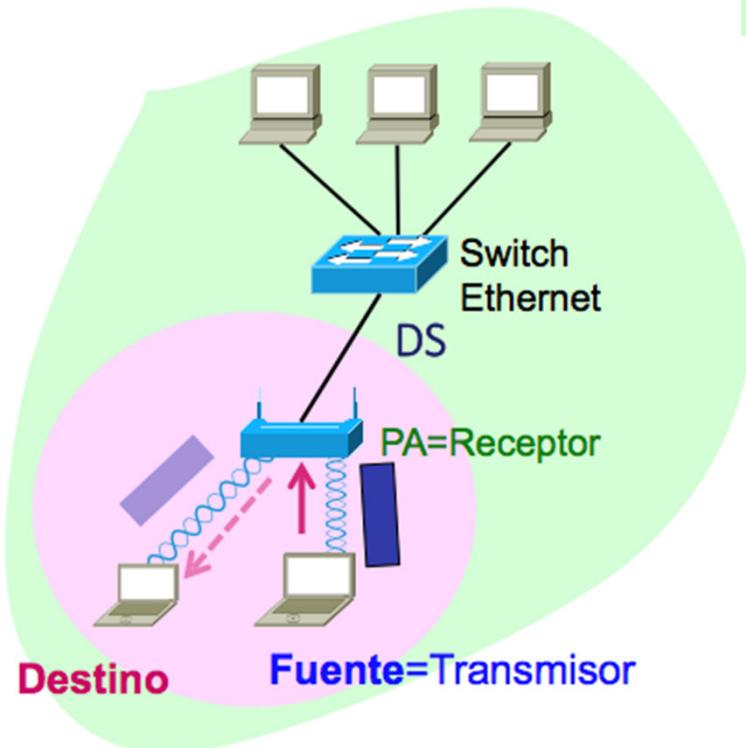
a de

To DS	From DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	1	MAC_Receptor	MAC_PA (BSSID)	MAC_Fuente	No se usa

Trama 802.11: Direccionamiento



Transmisión entre estaciones inalámbricas – paso 1



To DS = 1, From DS = 0

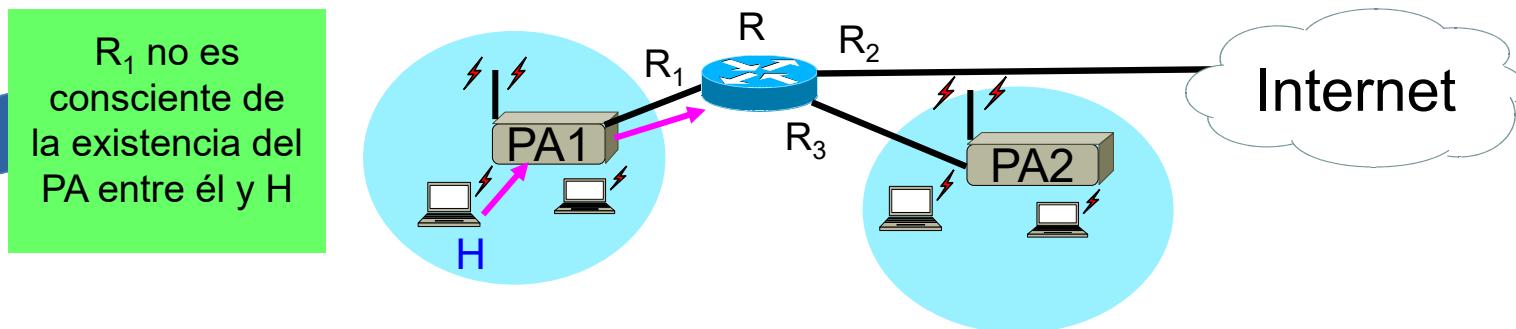
- Generación de la trama inalámbrica (IEEE 802.11) desde fuente a PA
 - Dirección 1: MAC estación inalámbrica receptora (MAC_PA)
 - Dirección 2: MAC estación inalámbrica transmisora (fuente)
 - Dirección 3: MAC destino del paquete

a de

To DS	From DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
1	0	MAC_PA (BSSID)	MAC_Transmisor	MAC_Destino	No se usa

Otro ejemplo

- H transmite un datagrama a R₁



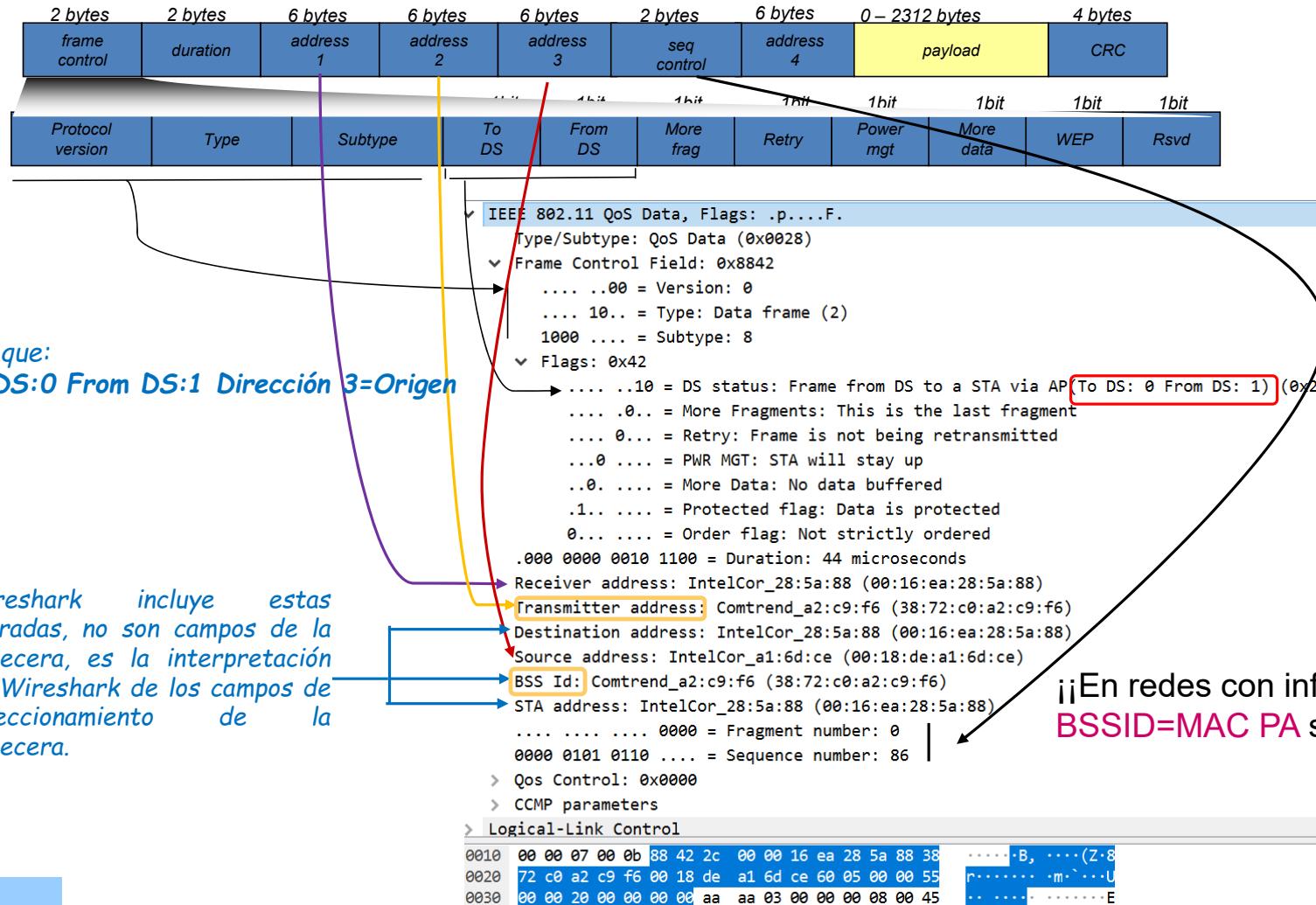
- H mediante ARP averigua la MAC de R₁
- H envía la trama IEEE 802.11 a PA1, llenando los campos de direcciones:
 - Dir. 1: Dir. MAC de PA1 (antena receptora)
 - Dir. 2: Dir. MAC de H (antena transmisora)
 - Dir. 3: Dir. MAC de R₁ (destino final de la trama)
- PA recibe la trama IEEE 802.11, genera una trama IEEE 802.3 (Ethernet):
 - Dir. destino: Dir. MAC R₁
 - Dir. fuente: Dir. MAC de H

To DS = 1, From DS = 0

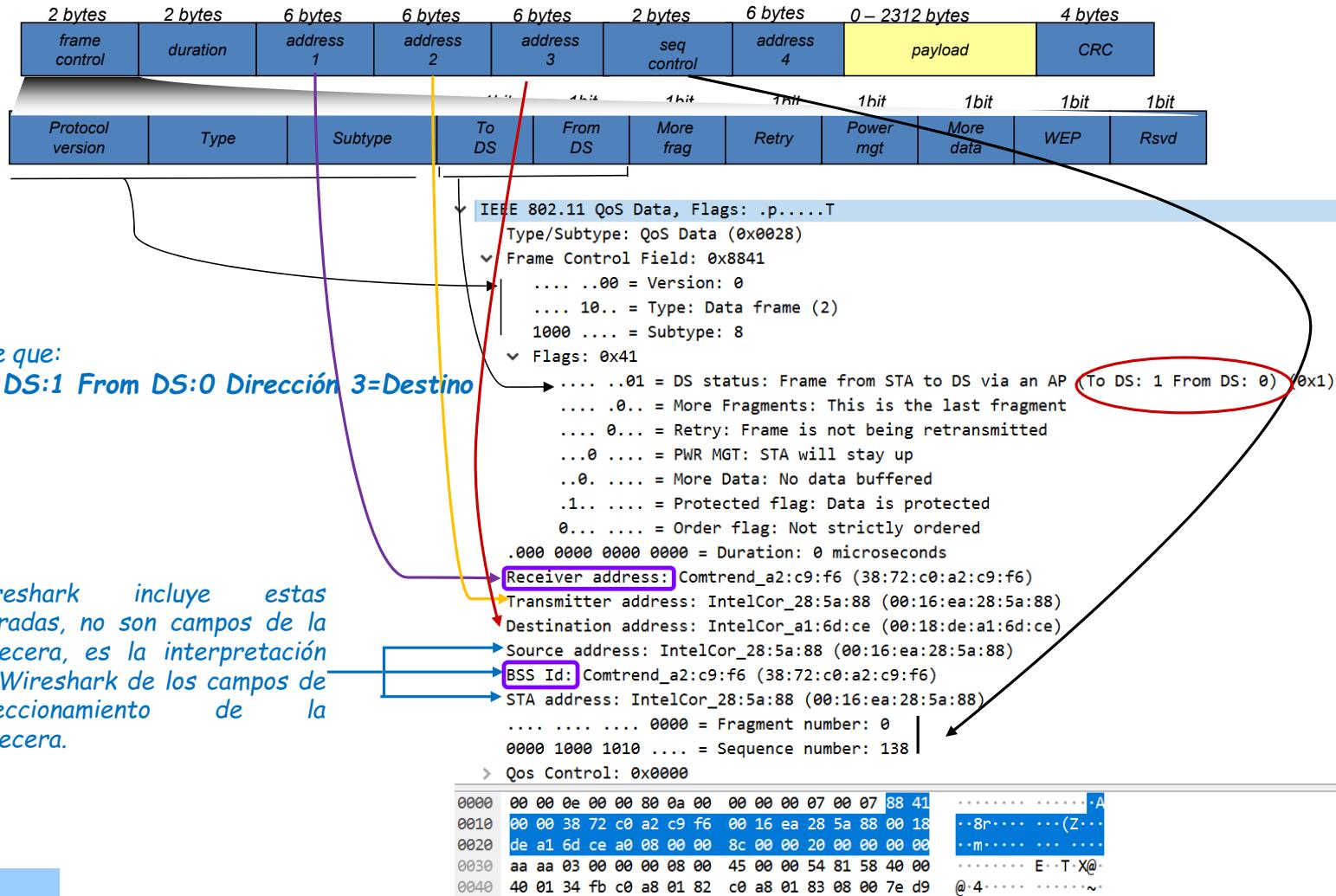
Trama 802.11: Wireshark

- En las capturas de Wireshark veremos algunas entradas que no son campos de la cabecera 802.11.
- Wireshark incluye entradas para interpretar los campos de direccionamiento de la cabecera.
 - Siempre incluye:
 - Id. de BSS: es la dirección MAC del punto de acceso (PA)
 - Dirección de STA: es la dirección MAC de la estación que captura el tráfico
 - Dependiendo de:
 - Si PA está actuando como receptor de la trama (RA)
 - La dirección 1 contiene PA
 - Wireshark añade la entrada de la dirección fuente (*Source address*)
 - Si PA está actuando como transmisor de la trama (TA)
 - La dirección 2 contiene PA
 - Wireshark añade la entrada de la dirección destino (*Destination address*)

Trama 802.11: Wireshark

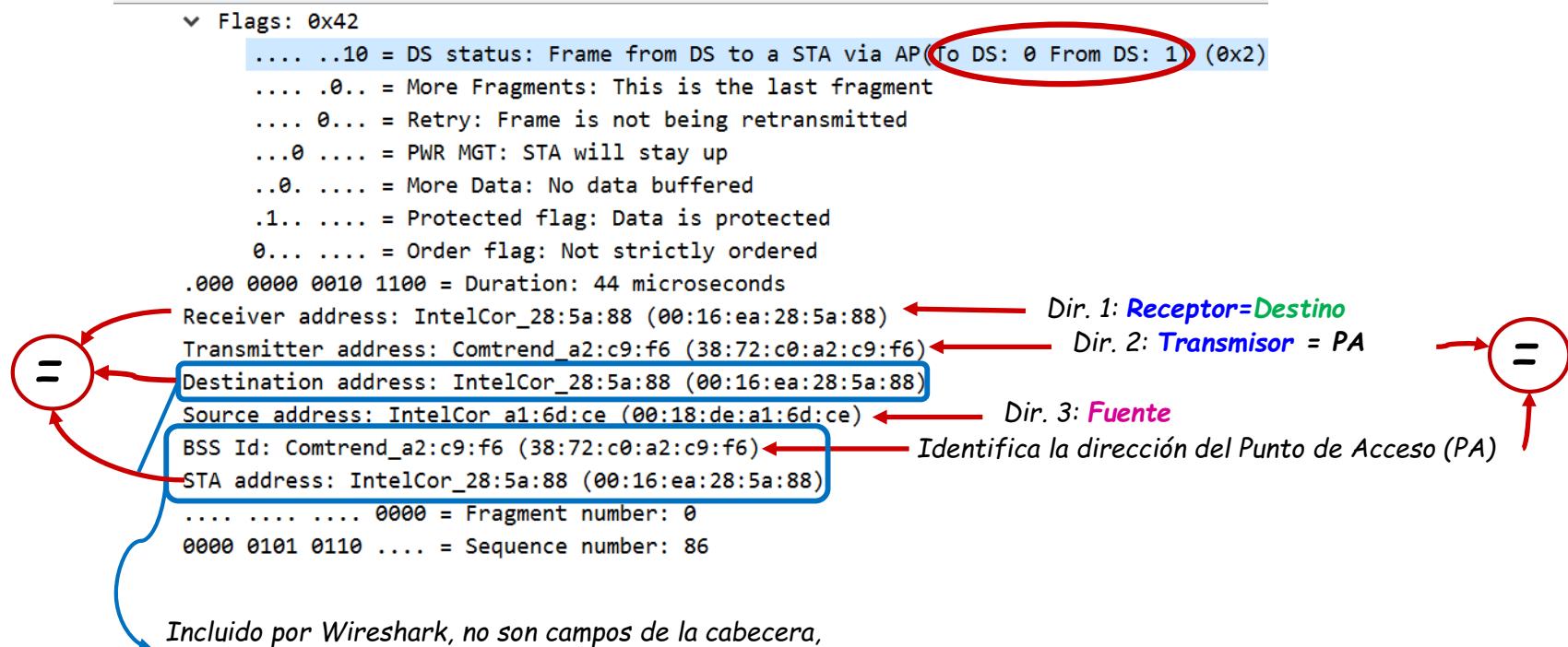
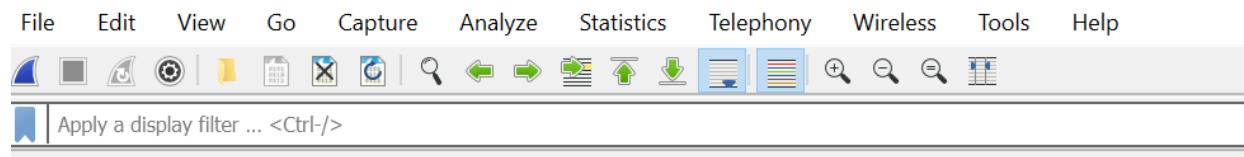


Trama 802.11: Wireshark



Trama 802.11: Wireshark

To DS	From DS	Significado	Modo
0	1	Trama de datos proviene del DS	Infraestructura



Trama 802.11: Wireshark

To DS	From DS	Significado	Modo
1	0	Trama de datos destinada al DS	Infraestructura

wifi2wifi_2.pcap

No. Time Source Destination Protocol Length Info

8	1.238100	IntelCor_28:5a:88	Broadcast	ARP	94	Who has 192.168.1.131
9	1.238509	IntelCor_a1:6d:ce	IntelCor_28:5a:88	LLC	96	S, func=SREJ, N(R)=69

Flags: 0x41

-01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
-0. = More Fragments: This is the last fragment
- 0.... = Retry: Frame is not being retransmitted
- ..0 = PWR MGT: STA will stay up
- ..0. = More Data: No data buffered
- .1... = Protected flag: Data is protected
- 0.... = Order flag: Not strictly ordered
- .000 0000 0000 0000 = Duration: 0 microseconds

Receiver address: Comtrend_a2:c9:f6 (38:72:c0:a2:c9:f6) ← Dir. 1: Receptor=PA →

Transmitter address: IntelCor_28:5a:88 (00:16:ea:28:5a:88) ← Dir. 2: Transmisor=Fuente →

Destination address: IntelCor_a1:6d:ce (00:18:de:a1:6d:ce) ← Dir. 3: Destino →

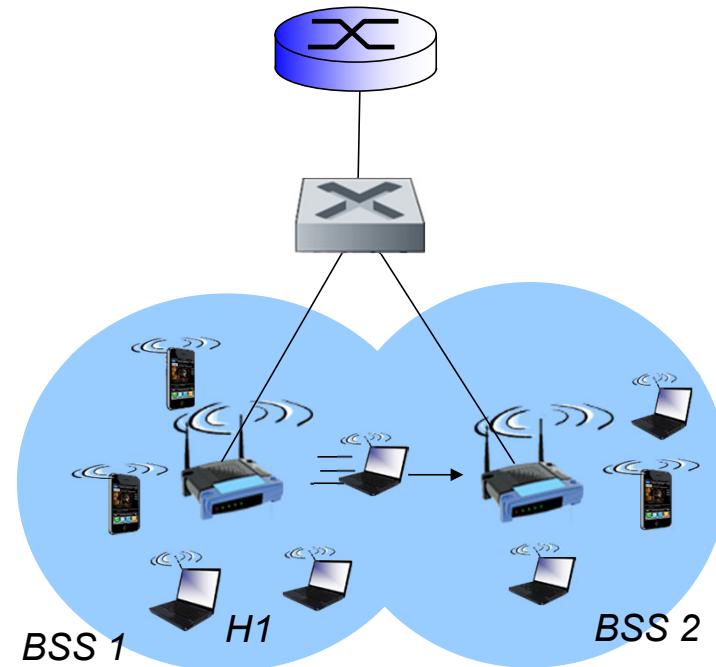
Source address: IntelCor_28:5a:88 (00:16:ea:28:5a:88)

BSS Id: Comtrend_a2:c9:f6 (38:72:c0:a2:c9:f6) ← Identifica la dirección del Punto de Acceso (PA) →

Incluido por Wireshark, no son campos de la cabecera, es la interpretación de Wireshark de los campos de direccionamiento de la cabecera.

802.11: movilidad dentro de la misma subred

- H1 permanece en la misma subred IP: la dirección IP no se modifica, mantiene la misma
- Comutador (*switch*): ¿a qué PA está asociado H1?
 - Autoaprendizaje: el conmutador verá la trama de H1 y "recordará" qué puerto del conmutador puede utilizar para alcanzar a H1

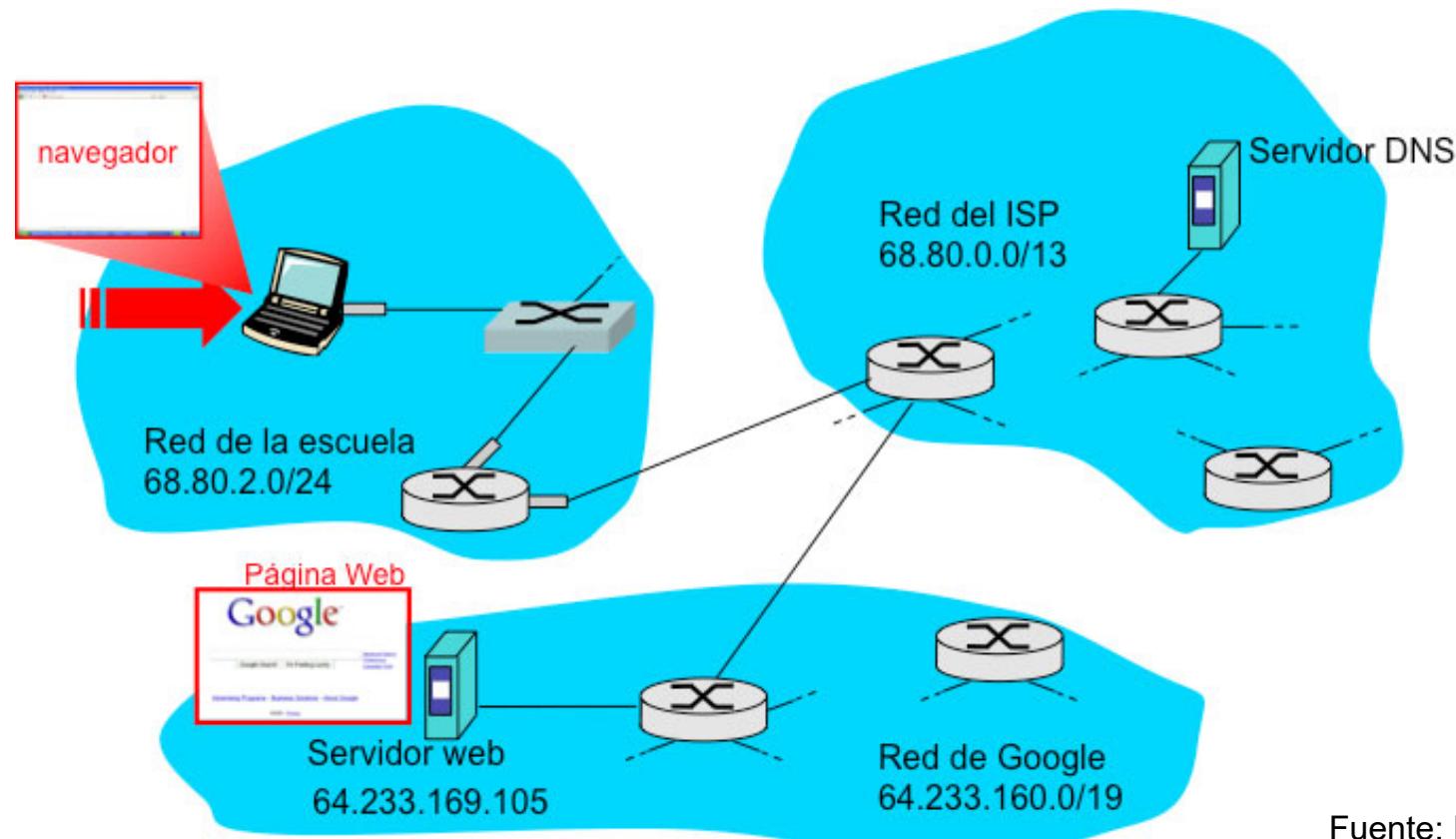


Índice

1. Introducción y servicios del nivel
 - Contexto y terminología
 - Servicios del nivel de red
 2. Detección y corrección de errores
 - Paridad, *Checksum* y CRCs
 3. Acceso al medio
 - Canales punto a punto y multipunto
 - Partición estática: MDT, MDF
 - Acceso aleatorio: CSMA, CSMA/CD
 - Protocolos por turnos: *Token Bus/Token Ring*
 4. Direccionamiento del nivel de enlace
 - Práctica 6: Direcciones MAC y ARP**
 - Enrutamiento de paquetes a una LAN externa
 5. Dispositivos de interconexión de nivel de enlace
 - Repetidores y concentradores (*Hubs*)
 - Conmutadores (*Switches*)
 - Interconexión de conmutadores
 - Auto-aprendizaje de conmutadores
 - Conmutadores y encaminadores
 6. Ethernet
 - Estructura de la trama
 - Algoritmo CSMA/CD ethernet
 - Nivel físico: medios.
 - Fast Ethernet, Gigabit Ethernet, 10G
 7. Redes inalámbricas
 - Introducción
 - Elementos de una wi-fi: infraestructura y ad-hoc. Un único salto y varios.
 - Diferencias con las redes cableadas: pérdida de potencia, interferencias, multipath
 - El problema del terminal oculto – CDMA
 - Redes Wi-Fi 802.11
 - Arquitectura, asociación con punto de acceso
 - 802.11: acceso múltiple, CSMA/CA, RTS-CTS
 - 802.11: direccionamiento
 8. Ejemplo: un día en la vida de una petición web.
- Práctica 7: Cortafuegos IPTABLES**
- Práctica 8: Análisis de tráfico Wi-Fi 802.11**

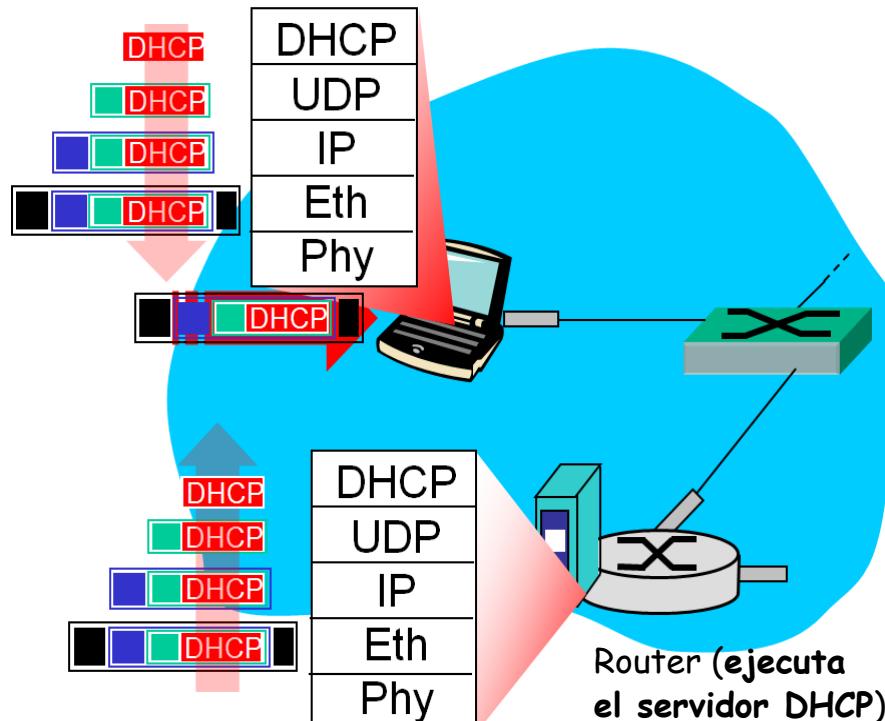
Un día en la vida de una petición web: escenario

Un estudiante conecta su portátil a la red del campus y solicita la página web www.google.com



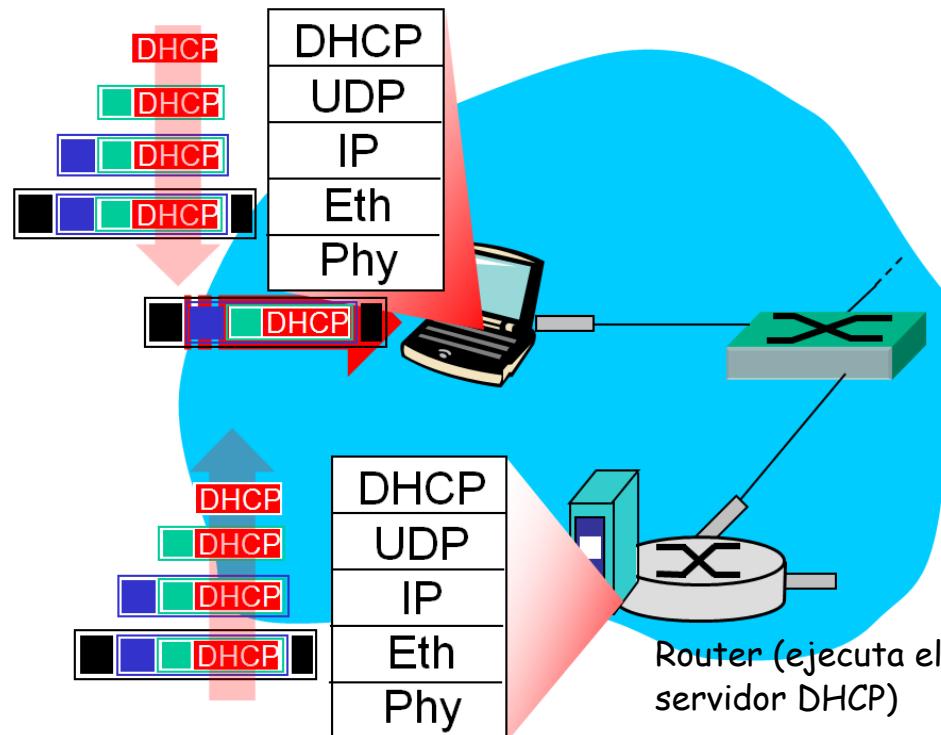
Fuente: Kurose & Ross

Obteniendo la configuración de red



- El portátil necesita 3 direcciones IP:
 - Una para él
 - IP del router
 - IP de un servidor DNS
- Las obtiene mediante **DHCP**
- La petición **DHCP Discover** se encapsula en **UDP**, que se encapsula en **IP** y finalmente en **Ethernet**
- La trama Ethernet **se difunde** (FF:FF:FF:FF:FF:FF) en la LAN y llega al servidor DHCP
- De la trama Ethernet se extrae el datagrama IP, el datagrama UDP y la petición DHCP

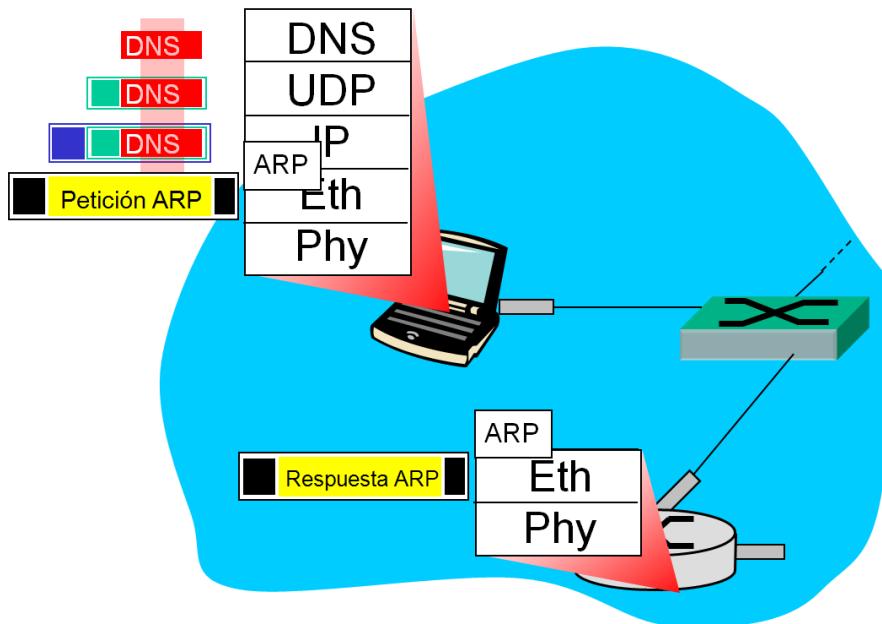
Diálogo DHCP



- El servidor DHCP contesta con el mensaje **DHCP Offer** proponiéndole una dirección IP
- El portátil la acepta y devuelve el mensaje **DHCP Request**
- El servidor DHCP finaliza la petición con el mensaje **DHCP ACK**
- Nótese que el switch aprende la localización de los host y por tanto ya conoce la ubicación del portátil

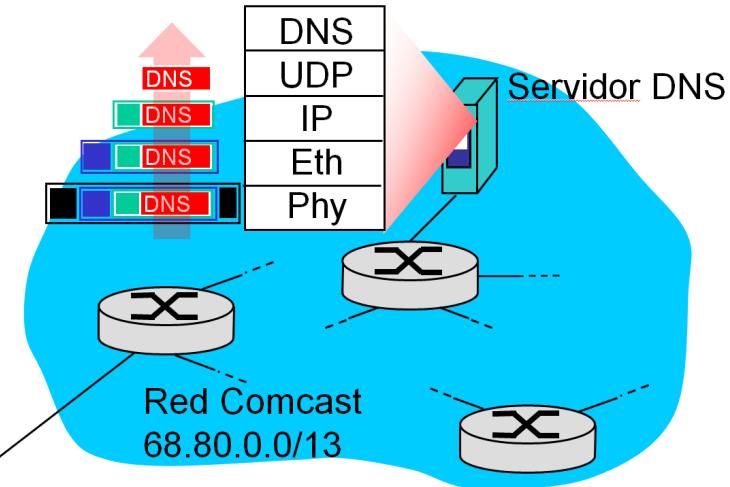
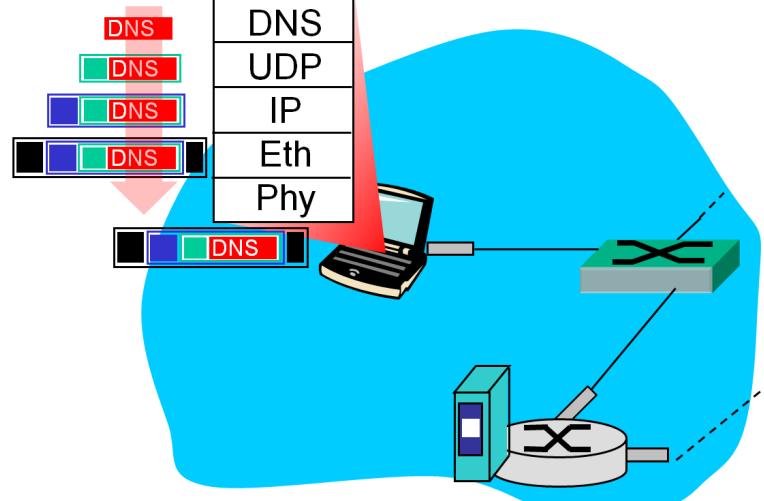
El cliente ya tiene su dirección IP
y conoce el DNS y el router de su red

ARP (antes de DNS y de HTTP)



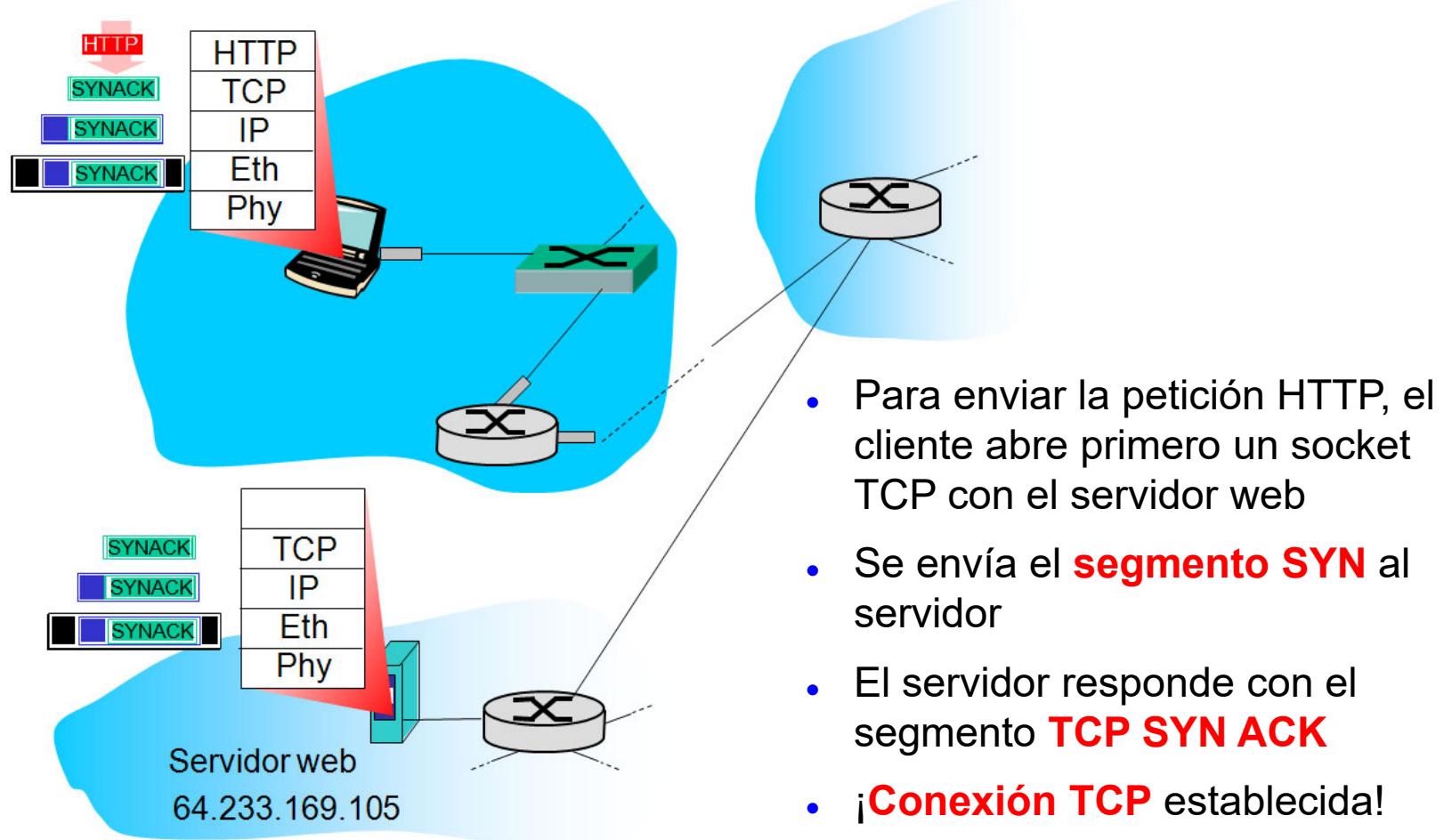
- Antes de enviar la petición HTTP, se necesita la dirección IP de www.google.com: **DNS**
- La petición DNS se crea y encapsula en un datagrama UDP, que se encapsula en IP y luego en Ethernet
- Para enviar la trama al router, se necesita su dirección MAC: **ARP**
- La petición ARP se envía por difusión. El router contesta directamente al portátil
- El cliente conoce la MAC del router y envía la trama con la petición DNS

Uso del DNS

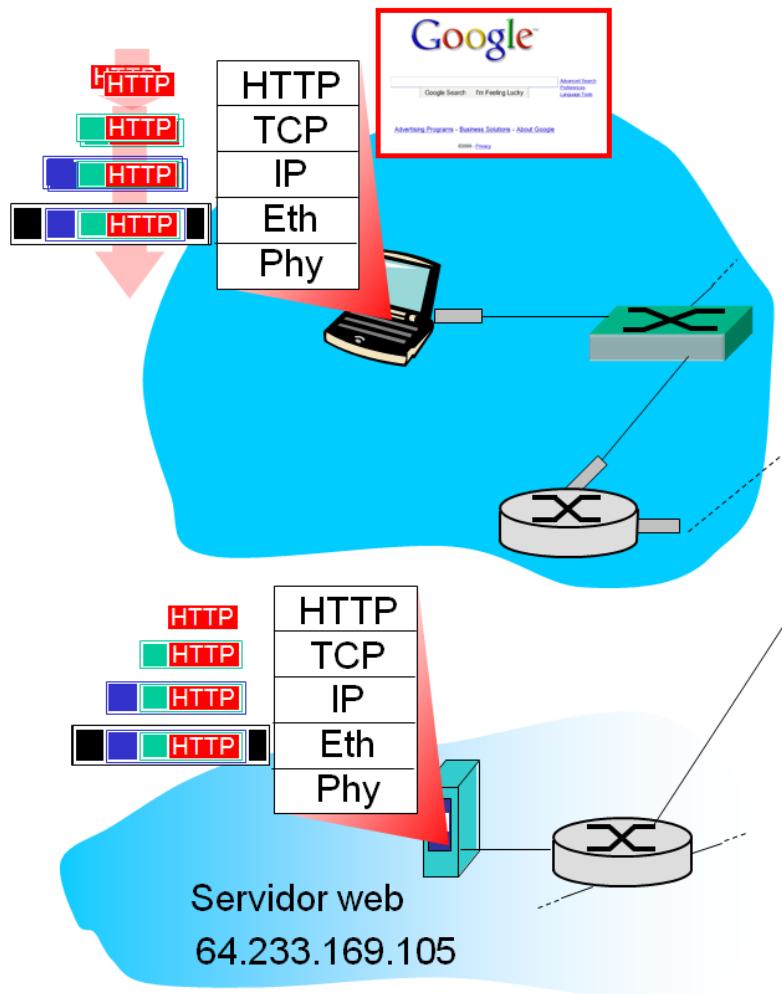


- El datagrama IP que contiene la petición DNS se envía a través del switch al router
- El datagrama IP se encamina hacia la red del ISP donde está el DNS (tablas de encaminamiento creadas usando RIP, OSPF y/o BGP)
- En el servidor DNS, la petición se extrae del datagrama
- El servidor contesta con la dirección IP buscada

Estableciendo la conexión TCP



Petición y respuesta HTTP



- La petición HTTP se envía a través del socket
- El datagrama que contiene la petición HTTP se encamina hacia el servidor
- El servidor responde con la **respuesta HTTP**, que contiene la página web
- La respuesta HTTP se encamina hacia el cliente