

# TEMA 2

## REDES DE ÁREA LOCAL

PARTE I: LANs CABLEADAS

PARTE II: LANs INALÁMBRICAS



# *TEMA 2. PARTE I*

## *LANs CABLEADAS*



# Contenido del Tema 2. Parte I: LANs cableadas

1. Generalidades de las Redes de Area Local (LAN)
2. El modelo de referencia IEEE 802.x
  3. El protocolo de acceso al medio en Ethernet/IEEE 802.3
  4. Estándares físicos IEEE 802.3
  5. Formato de la trama Ethernet
6. Interconexión entre LANs
7. Topologías LAN con bucles
8. LANs conmutadas
9. LANs virtuales (VLANs)
10. Referencias



# 1. Generalidades de las Redes de Area Local

Concepto de LAN

Modos de caracterización de las LANs

LANs P2P y MP

Medios de transmisión

Técnicas de control de acceso al medio

# Concepto de red de área local (LAN)



- Una red de área local es una red de ordenadores restringida a una superficie geográfica limitada (casa, oficina, laboratorio, edificio,.....)
  - Las LANs pueden usar dos topologías de transmisión: multipunto y punto a punto, pero, normalmente, se suelen emplear las primeras con modo de transferencia de difusión
  - La velocidad de las LAN es muy superior a las WAN



# Modos de caracterización de las LAN



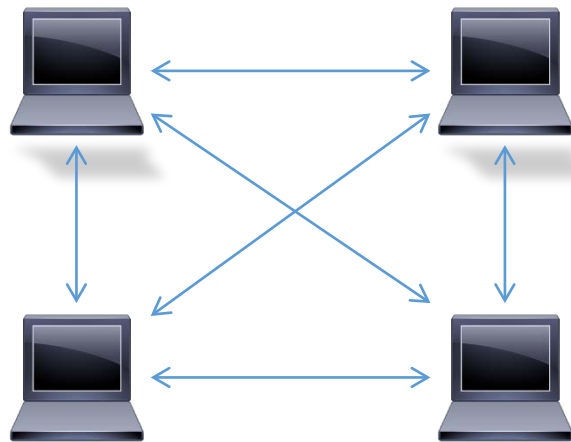
- Según la Topología: Forma de disponer los enlaces y los nodos de la red.
- Medios de transmisión: Tipo de conexión física entre las distintas estaciones o equipos de la red (cable coaxial, trenzado, FO, *Wireless*).
- Control de acceso al medio: Modo de acceso de las estaciones al medio compartido (Aloha, CSMA)



# LANs con enlaces Punto a Punto (P2P)



- En la red LAN con enlaces Punto a Punto todas las computadoras actúan como clientes o servidores no dedicados.
  - Desventajas: El fallo de un solo nodo en la red puede hacer que toda la red entre en fallo
  - El alto número de enlaces la convierte en costosa



Complejidad de la LAN P2P	
Nº nodos	Nº Enlaces
2 nodos	1 enlaces
3 nodos	3 enlaces
4 nodos	6 enlaces
10 nodos	45 enlaces
100 nodos	4.950 enlaces
1.000 nodos	499.500 enlaces
10.000 nodos	49.995.000 enlaces
100.000 nodos	4.999.950.000 enlaces

$$C_{m,2} = \frac{m!}{2(m-2)}$$

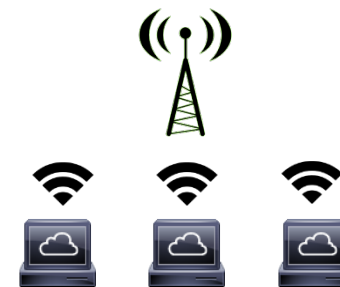
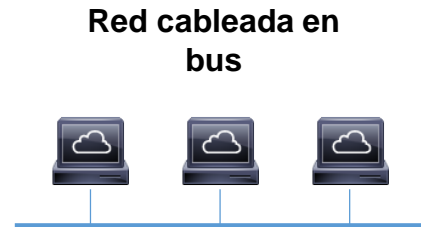
# LANs con enlaces Multipunto (MP)



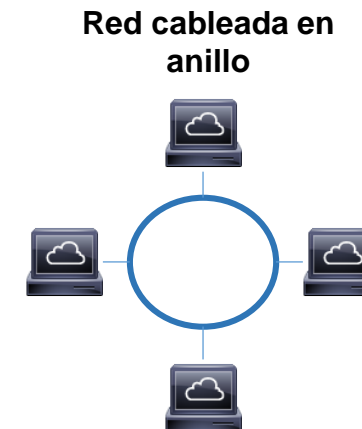
■ Las topologías multipunto son típicas de las LANs

■ Características:

- Los datos emitidos por un transmisor son recibidos por cualquier terminal conectado a la red
- El medio físico (canal) es compartido mediante Técnicas de Acceso al Medio
- No hay conmutación



Red inalámbrica

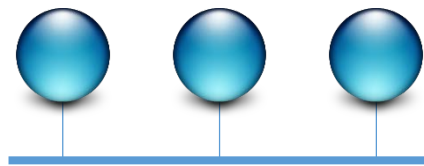




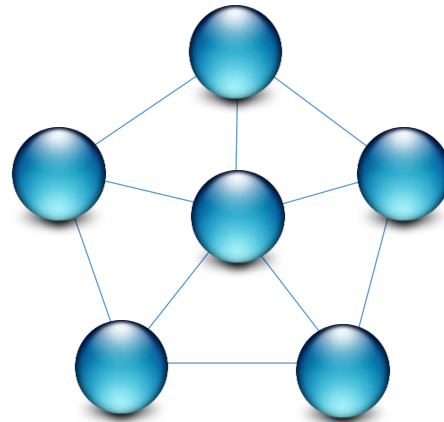
# Topologías de red con las LANs



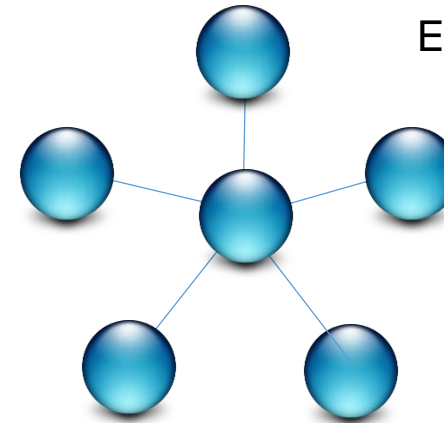
Bus



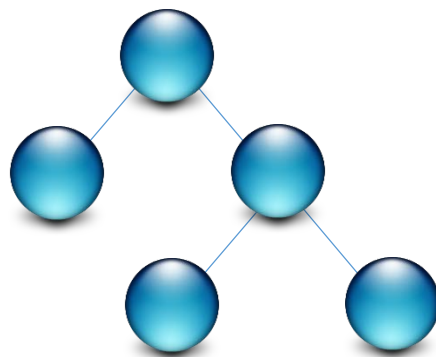
Mallada



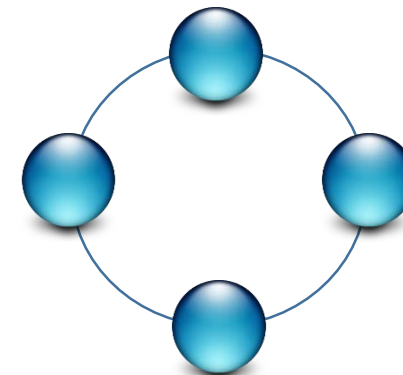
Estrella



Árbol



Anillo



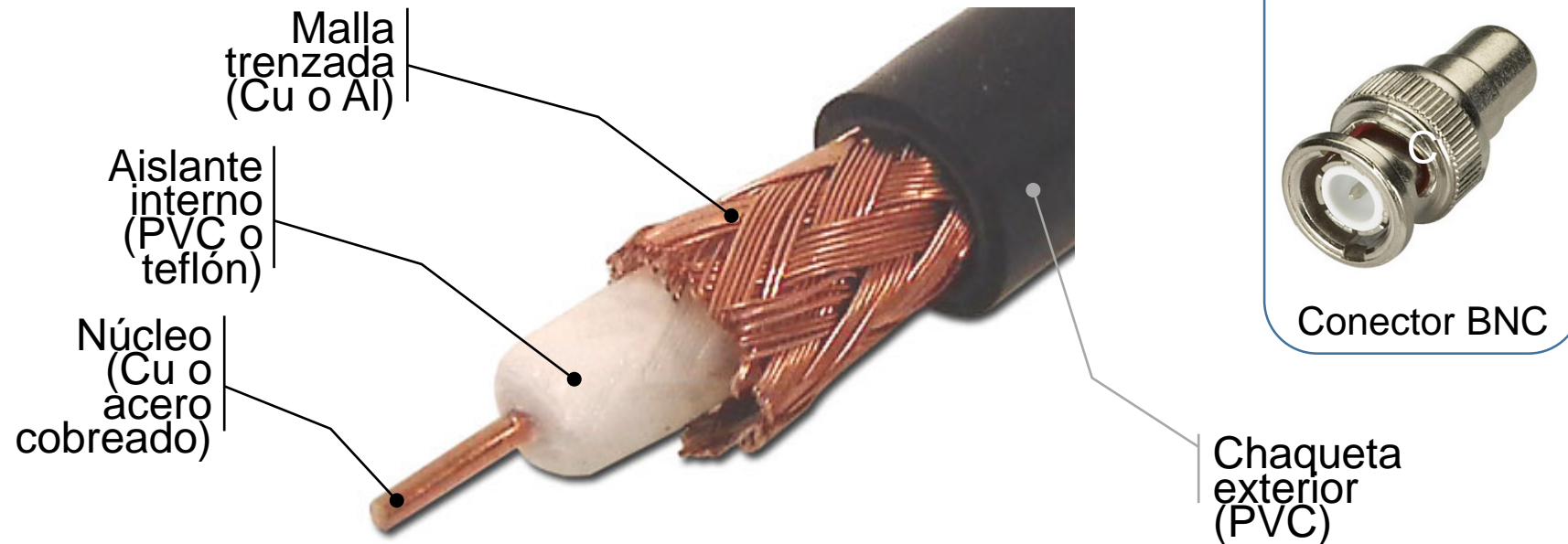
# Medios de transmisión

## Cable coaxial



### ■ Características:

- Velocidad: 10 Mbps
- Impedancia: 50 ohms (digital)
- Distancias: 100m (10base2) y 500m (10base5)



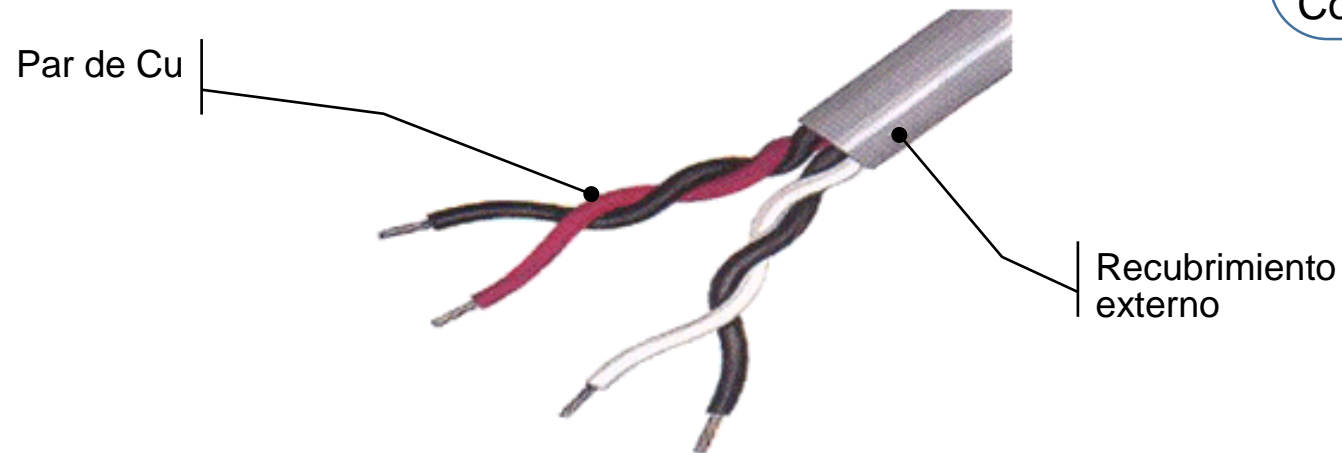
# Medios de transmisión

## Par trenzado



### ■ Características

- Velocidad: hasta 10 Gbps
- Pares trenzados de cobre
- Distancias: 100 mts
- Conector RJ45
- 2 clases: apantallado (STP) y no apantallado (UTP)



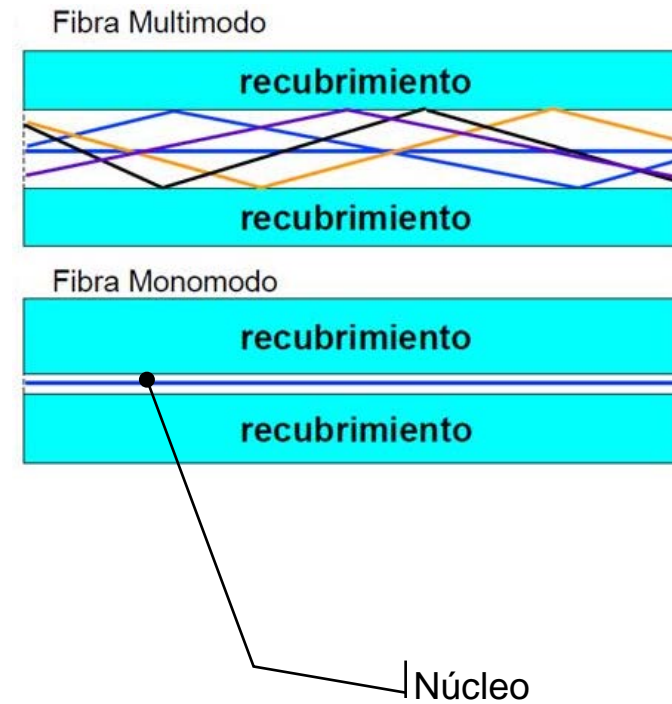
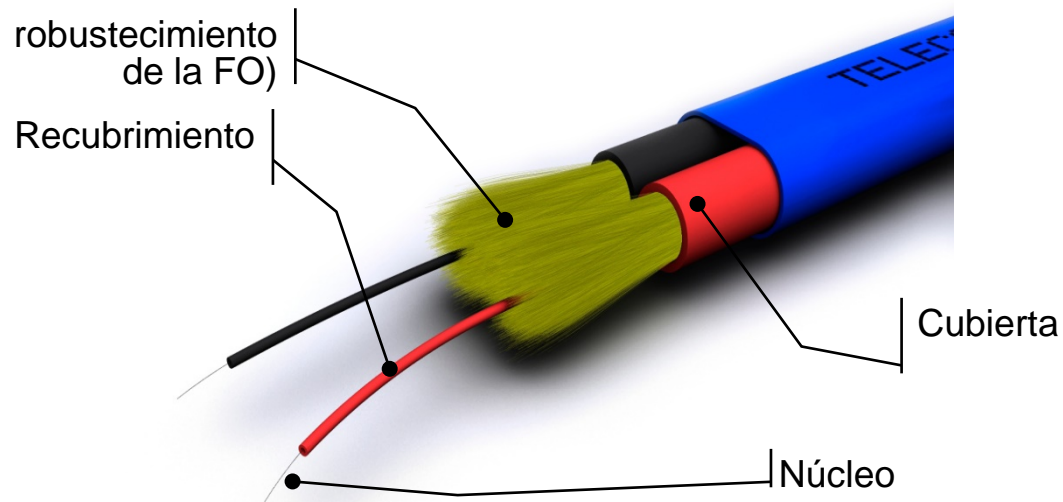
# Medios de transmisión

## Fibra óptica



### ■ Características

- Velocidad: hasta 100 Gbps
- Tipos: monomodo y multimodo
- Fuente de luz: laser o LED
- Distancias: 400 Kms (FO monomodo)
- Flexible y ligera

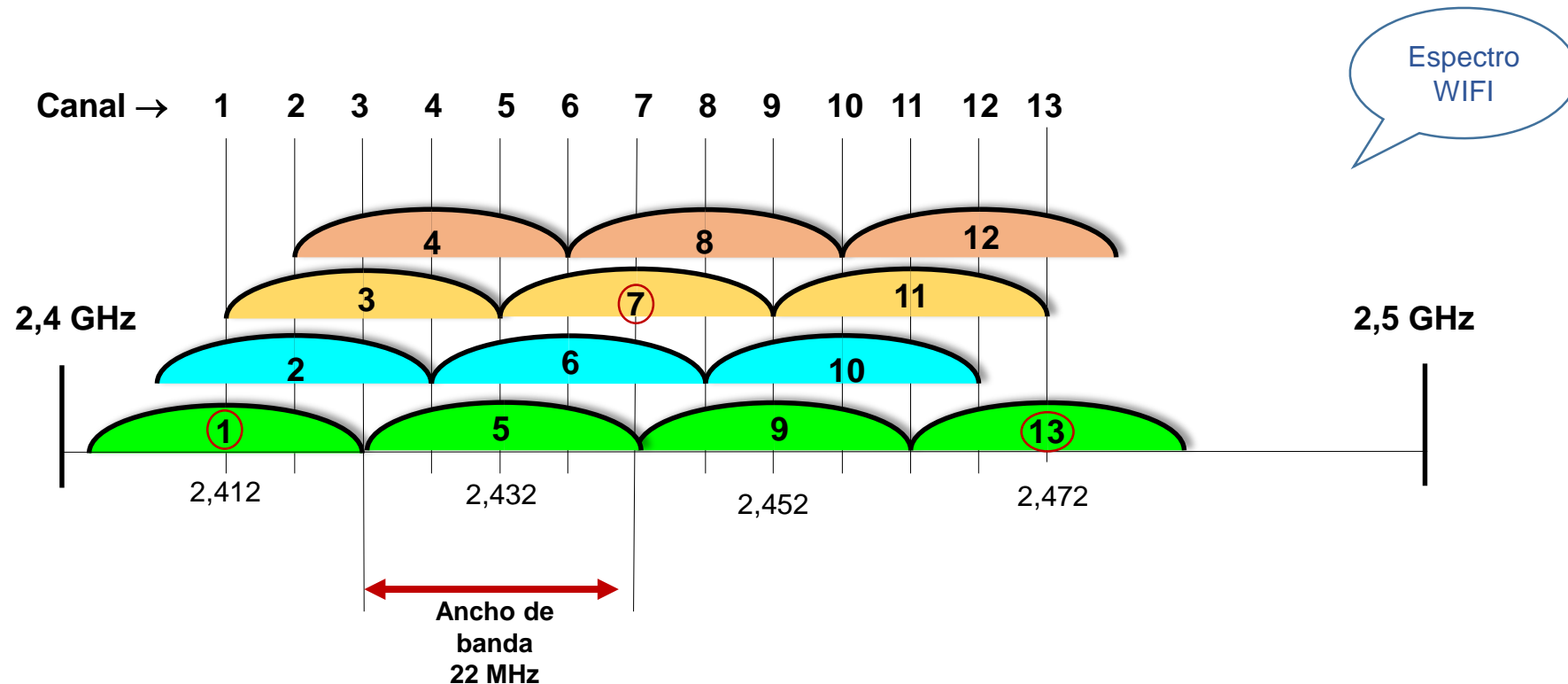


# Medios de transmisión

## Inalámbricos



- La transmisión inalámbrica consiste en unas técnicas de modulación en la banda ISM de 2,4 Ghz junto con los protocolos definidos en el estándar IEEE 802.11 que permiten la comunicación de dispositivos electrónicos y su conexión a Internet



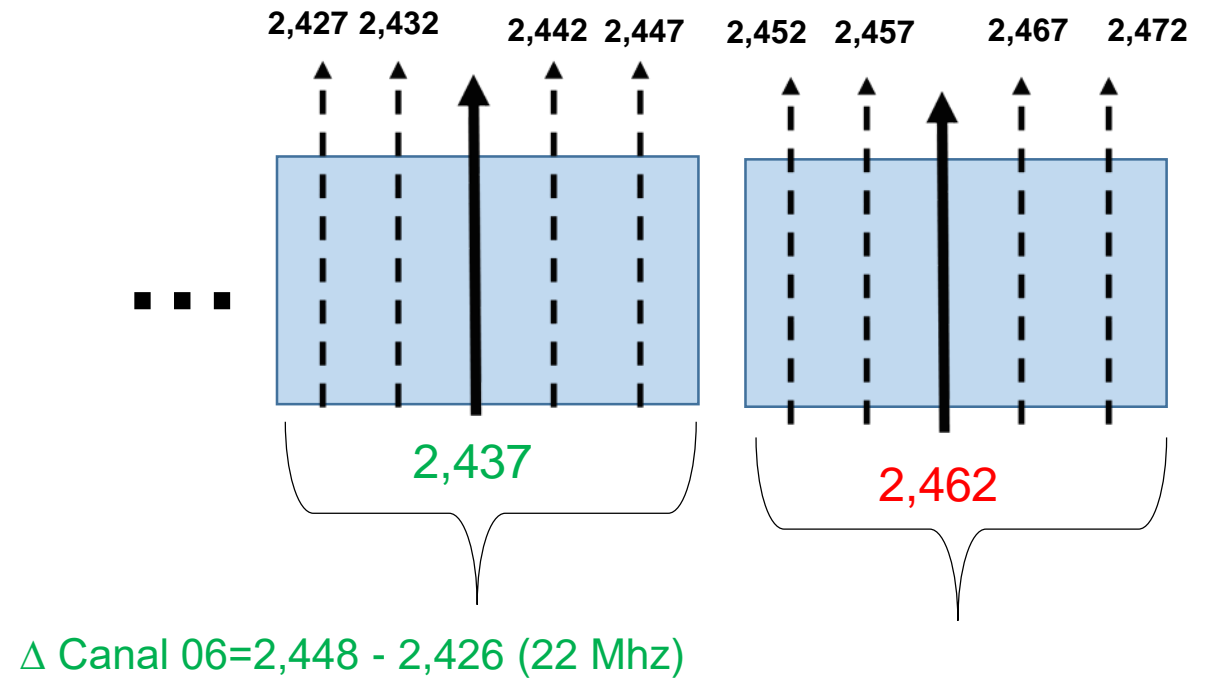


# Asignación canales IEEE 802.11

## FRECUENCIAS CENTRALES

- Canal 01: 2,412 Ghz
- Canal 02: 2,417 Ghz } + 5Mhz
- Canal 03: 2,422 Ghz
- Canal 04: 2,427 Ghz
- Canal 05: 2,432 Ghz
- Canal 06: 2,437 Ghz
- Canal 07: 2,442 Ghz
- Canal 08: 2,447 Ghz
- Canal 09: 2,452 Ghz
- Canal 10: 2,457 Ghz
- Canal 11: 2,462 Ghz
- Canal 12: 2,467 Ghz
- Canal 13: 2,472 Ghz

Se hace necesaria una separación de al menos 4 canales entre los elegidos con el fin de evitar interferencias entre canales adyacentes (por ejemplo: C06 y C11)



Δ Canal 11=2,451 - 2,473 (22 Mhz)

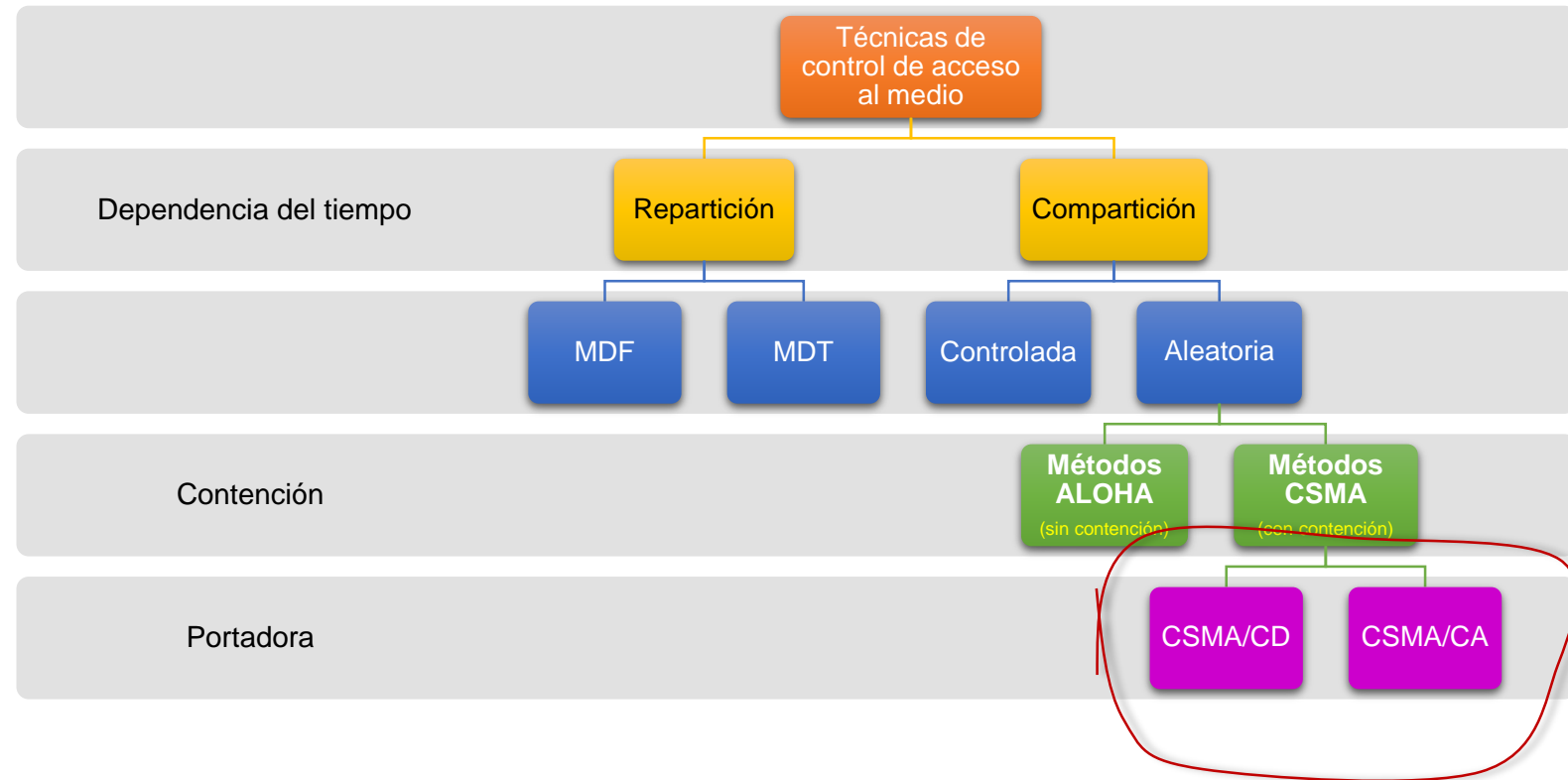


# LANs multipunto

## Técnicas de acceso al medio



- El control de acceso al medio es el conjunto de **mecanismos y protocolos** a través de los cuales varios "equipos" (dispositivos de red, ordenadores, teléfonos móviles, etc.) se ponen de acuerdo para compartir un medio de transmisión común



CD: collision detection; CS: carrier sense

CSMA: Carrier Sense Multiple Access; MDT: Multiplexión por división de tiempo; MDF: Multiplexión por división de frecuencia

# Tecnologías de compartición del medio



- Las técnicas de compartición del medio permiten que varios nodos de la LAN se comuniquen por un solo medio de comunicaciones y son las siguientes:
  - La **técnica de acceso aleatorio o de contención**: cada nodo puede enviar datos a los demás nodos conectados al medio de comunicaciones en cualquier momento.
  - La **técnica de acceso controlado**: cada nodo tiene su propio tiempo para utilizar el medio. Los dispositivos de red toman turnos para acceder al medio. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino y haya sido procesada por el destino.

# Control de acceso al medio

## Protocolos de acceso aleatorio



- En las técnicas denominadas de **acceso aleatorio o de contención**, no existe un tiempo preestablecido o predecible para que las estaciones transmitan, sino que las transmisiones se organizan aleatoriamente. En este sentido, las estaciones **compiten** para conseguir el acceso al medio (**contención**).
  - La principal ventaja de las técnicas de contención es su sencillez, porque pueden ser fácilmente implementadas. Estas técnicas funcionan eficientemente bajo carga a moderada, pero el rendimiento cae rápidamente bajo carga pesada.



Acceso aleatorio

# Control de acceso al medio

## Protocolos de acceso controlado



- En las técnicas denominadas de **acceso controlado** cada nodo tiene su propio tiempo (turno) para utilizar el medio.
  - Los nodos toman turnos para acceder al medio. Cuando un dispositivo coloca una trama en los medios, ningún otro dispositivo puede hacerlo hasta que la trama haya llegado al destino



Acceso controlado

# Control de acceso al medio

## Protocolos de acceso aleatorio



- Aloha Simple
  - Las estaciones transmiten en cualquier instante.
- Aloha Ranurado
  - Las estaciones transmiten durante unas determinadas ranuras, intervalos o slots de tiempo.
- CSMA: *Carrier Sense Multiple Access*
  - Las estaciones "escuchan" la portadora por si hay alguna otra estación transmitiendo antes de transmitir ellas mismas.
- CSMA/CD: *Carrier Sense Multiple Access/Collision Detection*
  - Las estaciones "escuchan" la portadora antes de transmitir, y detectan colisiones durante la transmisión.
- CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*)
  - Acceso múltiple con escucha de portadora y evasión de colisiones



## 2. El modelo de referencia IEEE 802.x

El modelo de referencia IEEE 802.x

IEEE 802.x vs OSI

IEEE 802.x. Encapsulado

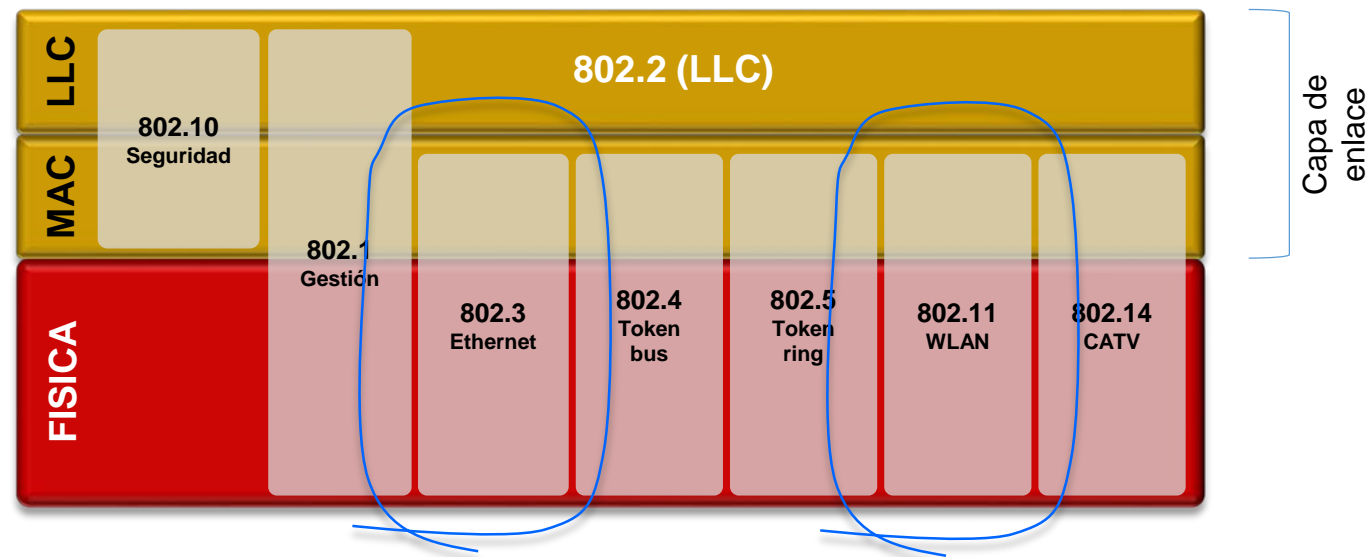
Servicios de las capas MAC y LLC



# Modelo de referencia IEEE 802.x



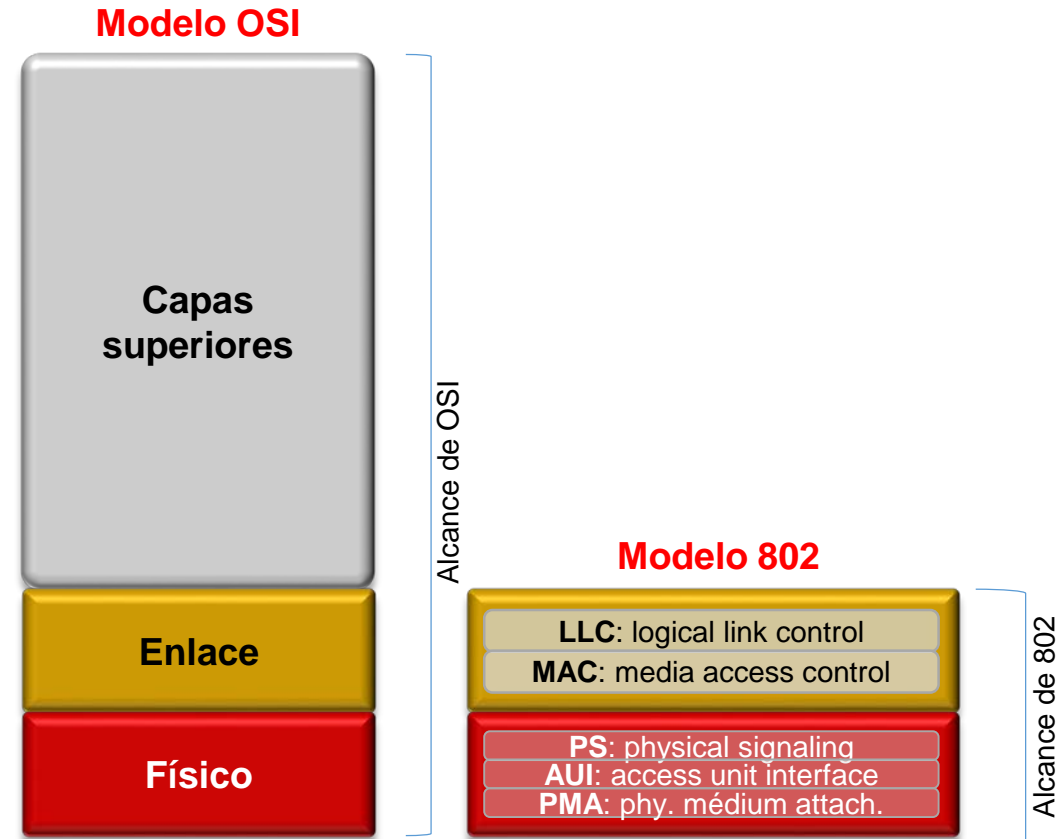
- El conjunto de estándares IEEE 802 define los dos niveles mas bajos del modelo OSI y está dirigido a redes LAN y MAN



# El modelo de IEEE 802.x vs. OSI

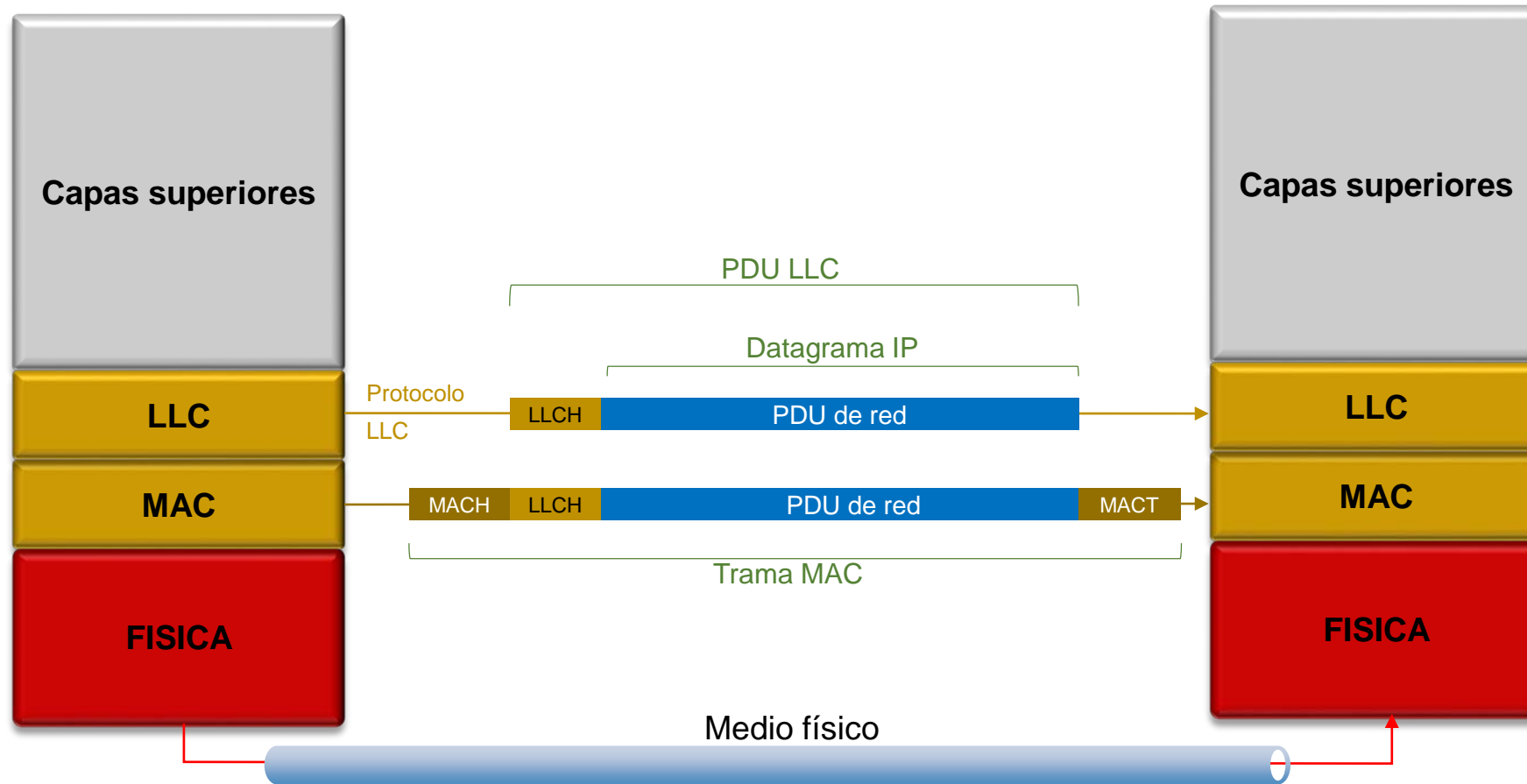


- El objetivo de la familia de estándares IEEE 802 fue conseguir un modelo multifabricante para el diseño de LANs
- Durante el desarrollo de IEEE 802 se siguió el modelo OSI. Aunque se decidió descomponer las capas 1 y 2.



# Modelo de referencia IEEE 802.x

## Encapsulado



# Modelo de referencia IEEE 802.x

## Servicios de las subcapas LLC y MAC



### Subcapa LLC (803.2)

- **Gestión del enlace de datos**
- Es servidora o proveedora de servicios de la capa de red
- Direccinamiento
- Secuenciación
- **Tiene 3 tipos de servicios:**  
LLC1 (no fiable, sin conexión, CLNS), LLC2 (fiable, orientada a conexión, CONS), LLC3 (sin conexión y reconocimiento de datos recibidos)

### Subcapa MAC (802.3) CSMA/CD

- Depende de la topología
- Regula el acceso de las estaciones al medio
- Sincronismo de trama
- Direccinamiento físico
- Detección de errores
- El servicio que ofrece al subnivel LLC, es no fiable y no orientado a conexión.



# 3. El protocolo de acceso al medio en Ethernet/IEEE 802.3

Introducción a Ethernet

El protocolo de acceso al medio CSMA

El protocolo de acceso al medio CSMA/CD

Ventana de colisión

El algoritmo de retardo exponencial

# Introducción a Ethernet



- Ethernet fue introducido en el mercado en 1980 por XEROX<sup>1</sup> y se estandarizó en 1983 como **IEEE 802.3**
- El acceso al medio compartido es por detección de la onda portadora y con detección de colisiones (**CSMA/CD**)
  - La capa física de Ethernet ha evolucionado durante el tiempo desde el cable coaxial al par trenzado e interfaces de fibra óptica, con velocidades de 10 Mbps hasta 100 Gbps



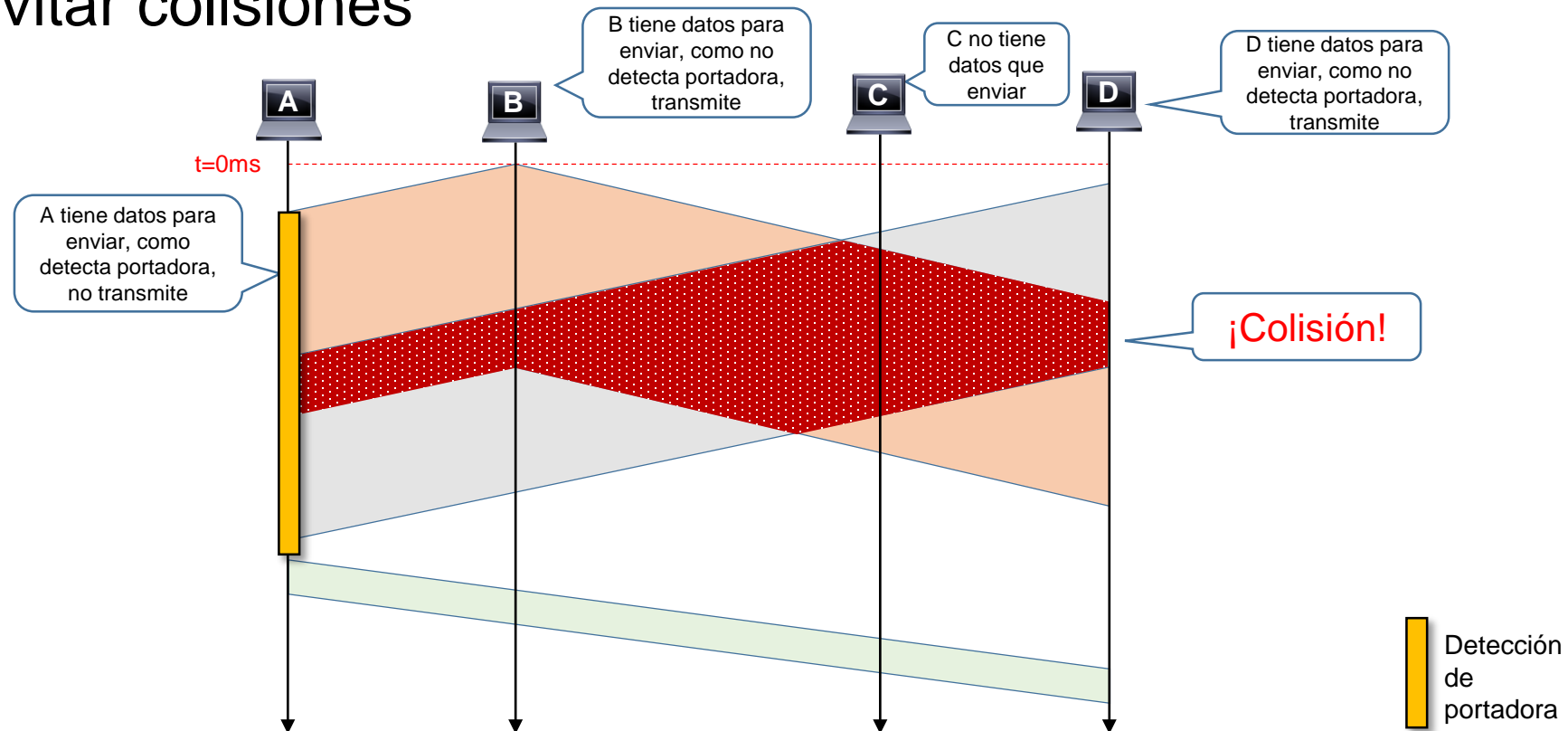
1. Robert Metcalfe fue el coinventor de Ethernet





# Protocolo de acceso al medio CSMA

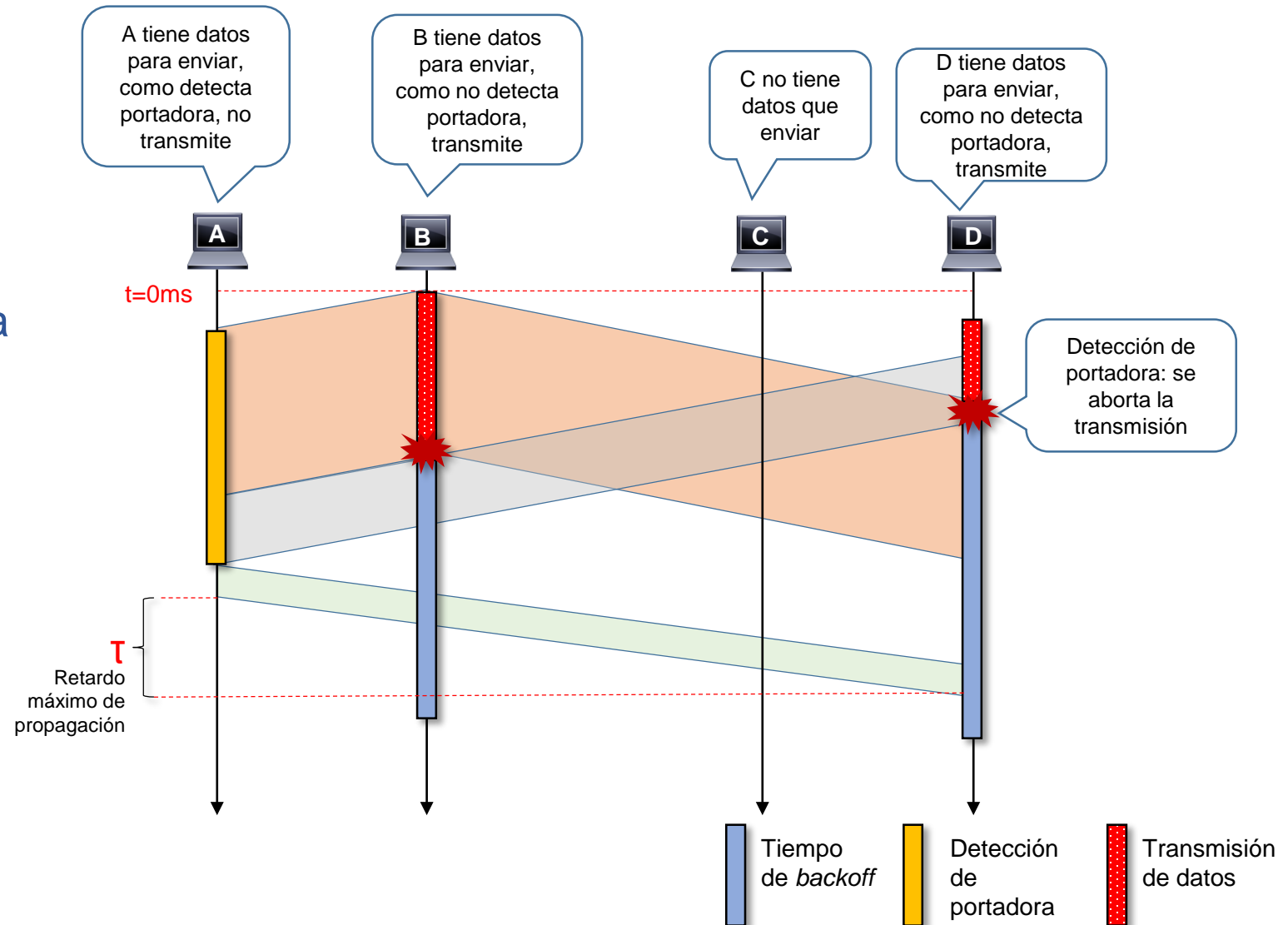
- Se entiende por *Acceso Múltiple por Detección de Portadora (CSMA)* a escuchar el medio, antes de transmitir, para saber si existe presencia de portadora ocupando el canal, con el fin de evitar colisiones



# Protocolo de acceso al medio CSMA/CD

■ En el caso de CSMA con detección de portadora el algoritmo es el siguiente:

- 1) Si el medio se encuentra libre se transmite.
- 2) Si está ocupado se continúa escuchando hasta que se libere; en este caso se transmite inmediatamente.
- 3) Si durante esta transmisión se detecta colisión se aborta la transmisión.
- 4) Tras el aborto se espera una cantidad aleatoria de tiempo conocida como espera (*backoff*), intentando transmitir de nuevo a continuación (paso 1).

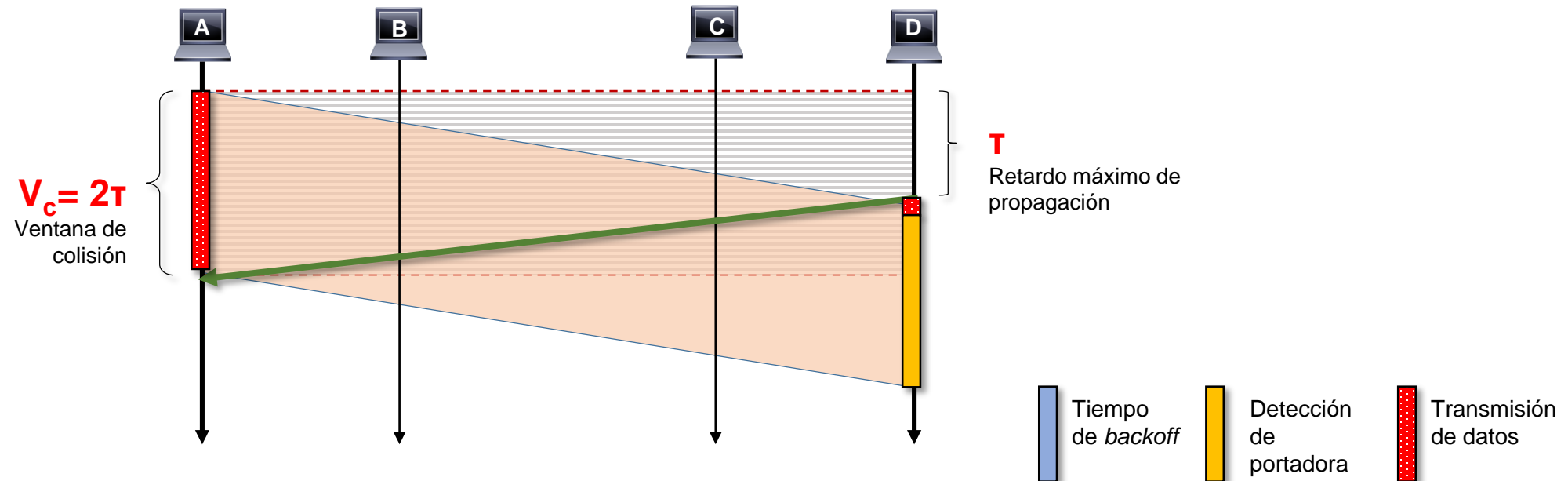


# Protocolo de acceso al medio CSMA/CD

## Ventana de colisión

### ■ Ventana de colisión (o tiempo de reacción)

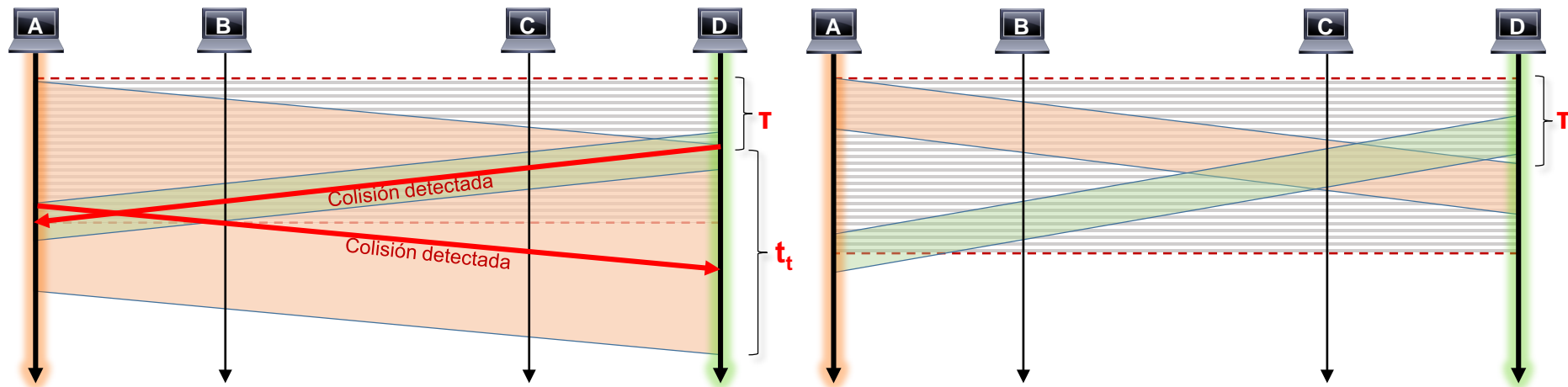
- Dados los ordenadores situados en los extremos opuestos de la red (A y D), el doble del tiempo transcurrido desde que A empieza a transmitir el primer bit hasta que lo recibe D es lo que se denomina **ventana de colisión ( $V_c$ )**.
- Dicho de otro modo: es el tiempo que A tarda en detectar una colisión en el caso peor, que es aquel en el que D empieza a transmitir justo cuando pasan exactamente  $T_{sgs}$ . Evidentemente, D se da cuenta de la colisión inmediatamente, pero hasta que no pasan otros  $T_{sgs}$ , A no se entera



# Protocolo de acceso al medio CSMA/CD

## Tamaño mínimo de la trama Ethernet (IEEE 802.3)

- El estándar Ethernet fija el tamaño mínimo de trama para que se pueda detectar la colisión, ya que si finalizara la transmisión demasiado pronto dejaría de escuchar y por tanto no vería si hay o no colisión.
  - En el estándar 802.3 fija la longitud la trama mínima a 64 bytes (512 bits).
  - Esto implica que el tiempo para detectar la colisión ( o **tiempo de reacción**) en una red de 10Mbps es de  $51,2 \mu\text{s}$



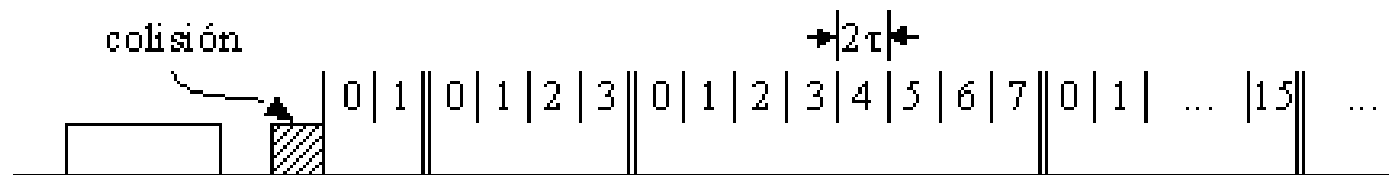
Trasmisión superior al tiempo de reacción  
 $t_t > t_R = 2\tau \Rightarrow$  colisión detectada

Trasmisión inferior al tiempo de reacción  
 $t_t < t_R = 2\tau \Rightarrow$  colisión no detectada

# Protocolo de acceso al medio CSMA/CD

## Algoritmo de retardo exponencial (BEB)

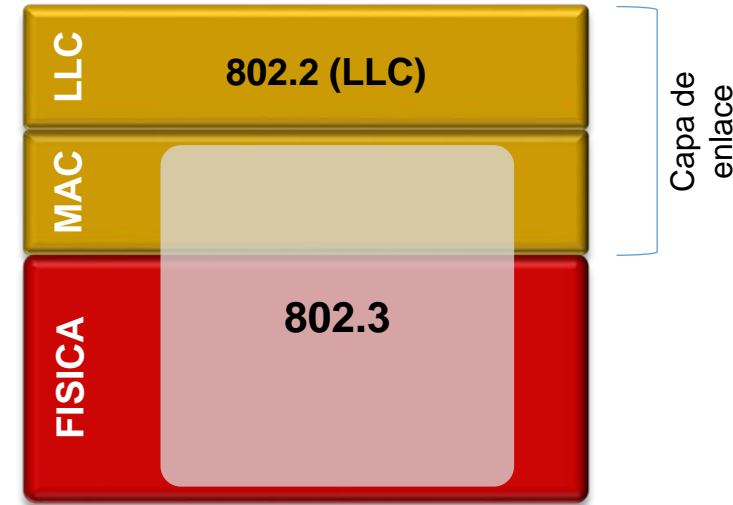
- Si se produce una colisión, se deja de transmitir, y se resuelve la espera mediante la técnica BEB (*Binary Exponential Backoff*):
  - Se divide el tiempo posterior a una colisión en ranuras de duración  $2\tau$ , que es el intervalo de vulnerabilidad (donde  $\tau$  retardo máximo de propagación)
- Se define una ranura de tiempo como el tiempo que la señal tarda en ir y volver, y debe ser igual al tiempo de transmisión de una trama mínima de 512 bits
  - A 10 Mbps es de  $51,2 \mu\text{s}$  y a 100 Mbps:  $5,12 \mu\text{s}$
- Tras la colisión:
  - Las estaciones involucradas vuelven a intentar transmitir en una de las 2 ranuras siguientes, de forma aleatoria. Si se vuelve a producir una colisión, esas estaciones intentarán transmitir en una de las 4 ranuras siguientes ...
  - Si se siguen produciendo colisiones, el intervalo de espera sigue creciendo hasta el décimo intento, a partir del intento 10 y hasta el 15, no se aumenta el número de ranuras.
  - A partir del intento 16, se descarta la trama.



# Generalidades sobre IEEE 802.3 [1]



- En 1973, Robert Metcalfe (de Xerox) presenta la patente de ETHERNET.
- ETHERNET II, fué desarrollado en el año 1979 por la cooperación entre *Digital Equipment Corporation, Intel y Xerox*, iniciales que dieron su nombre al prefijo DIX de dicho sistema.
- En 1983 se publica la norma IEEE 802.3 y esta se utiliza para referirse, comúnmente, a ETHERNET





# Generalidades sobre IEEE 802.3 [2]



■ Con el nombre IEEE 802.3 coexisten varios estándares: 10BASE2, 10BASE5, 10BASEX, 100BASEF, etc.

- Estos normalizan el nivel MAC y físico.
- En todos ellos el protocolo de acceso al medio es CSMA/CD





# 4. Estándares físicos IEEE 802.3

Clasificación de las redes Ethernet

Subcapas físicas de IEEE 802.3

Estándares físicos IEEE 802.3

10Base5

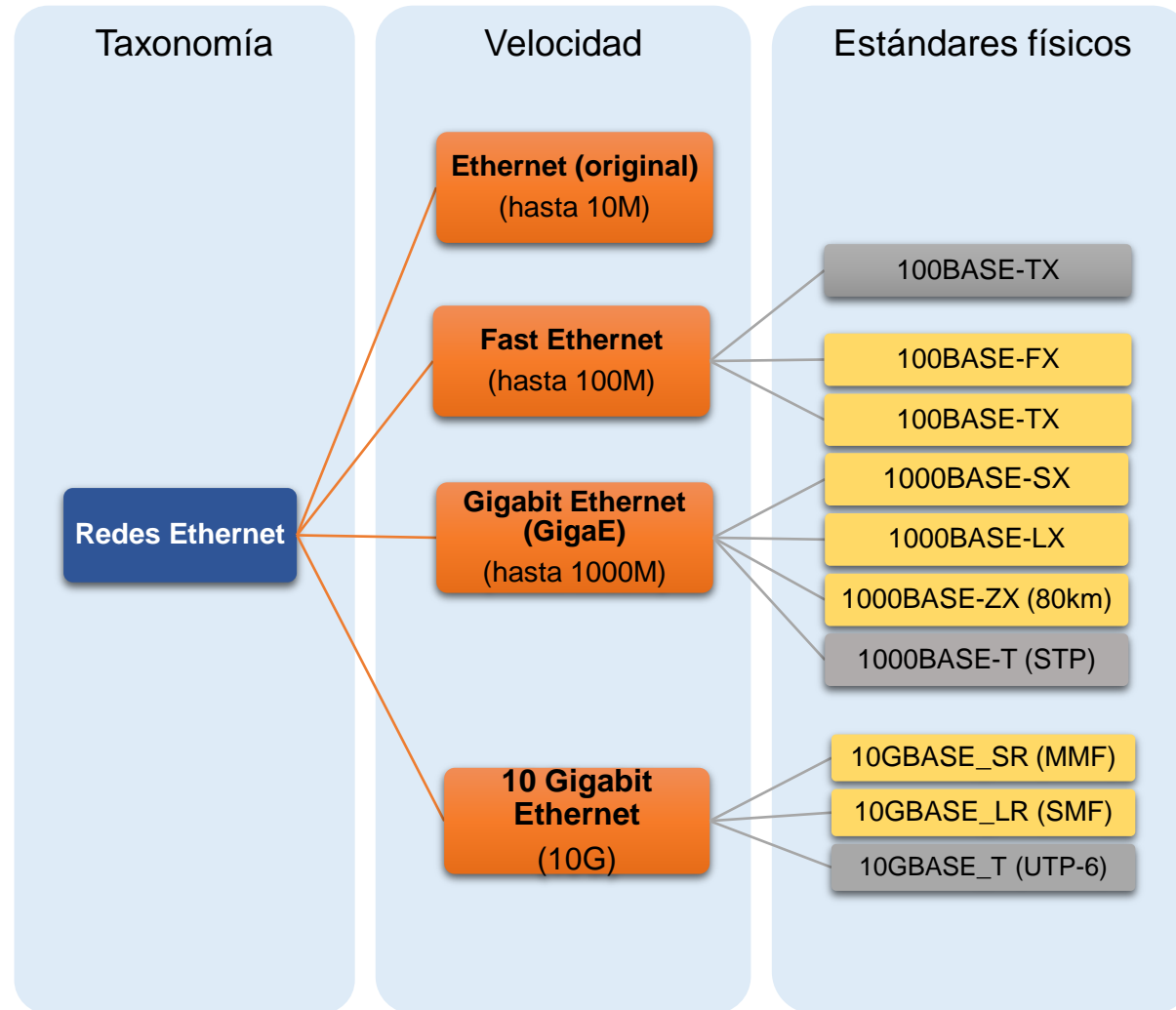
10Base2

10BaseT

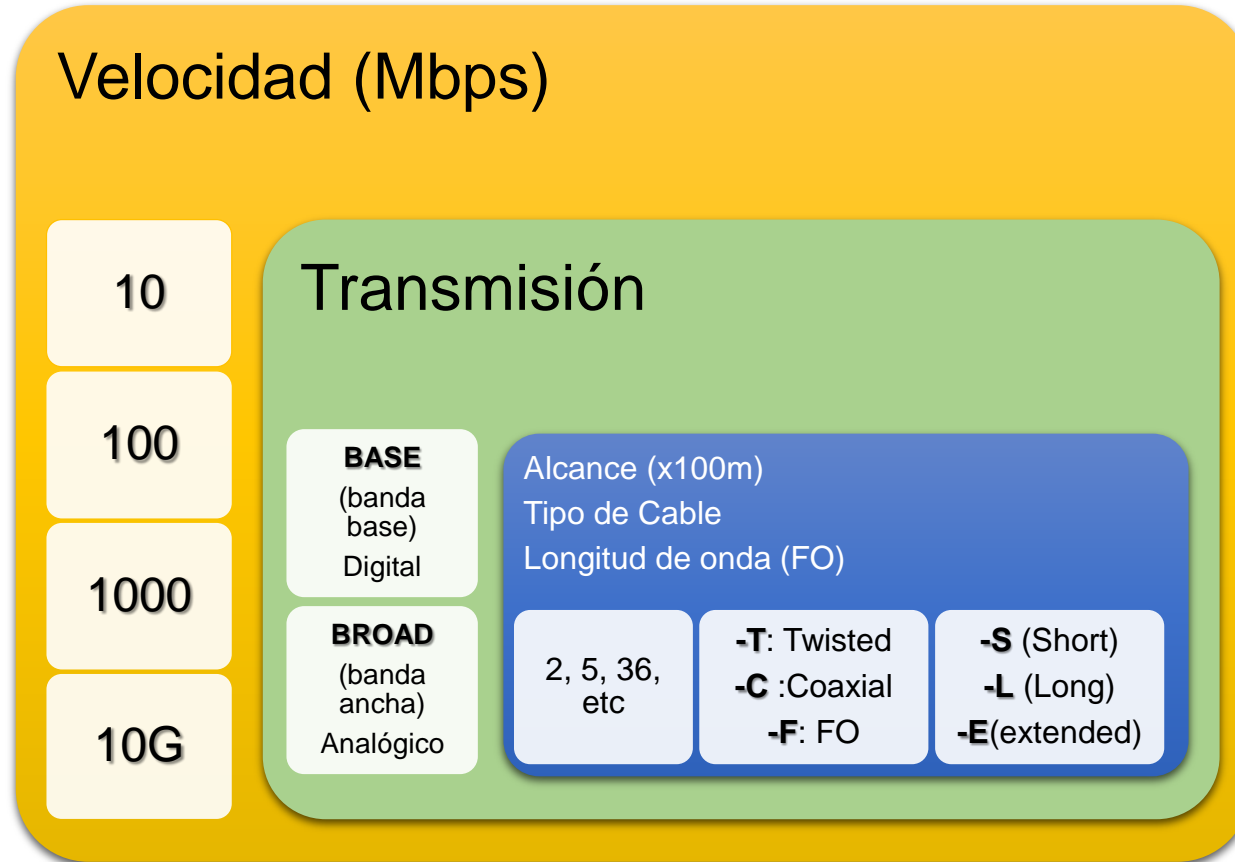
1000BaseX

10GBaseSR

# Clasificación de las redes Ethernet



# Denominación informal de los estándares físicos de las LANs Ethernet



## Ejemplos:

10BASE5

10BASE-T (cobre, 100m)

10GBASE-T (Cu cat6)

10BASE-S (FO multimodo)

10BASE-L (FO monomodo)

10BROAD36 (3,6km, coax)

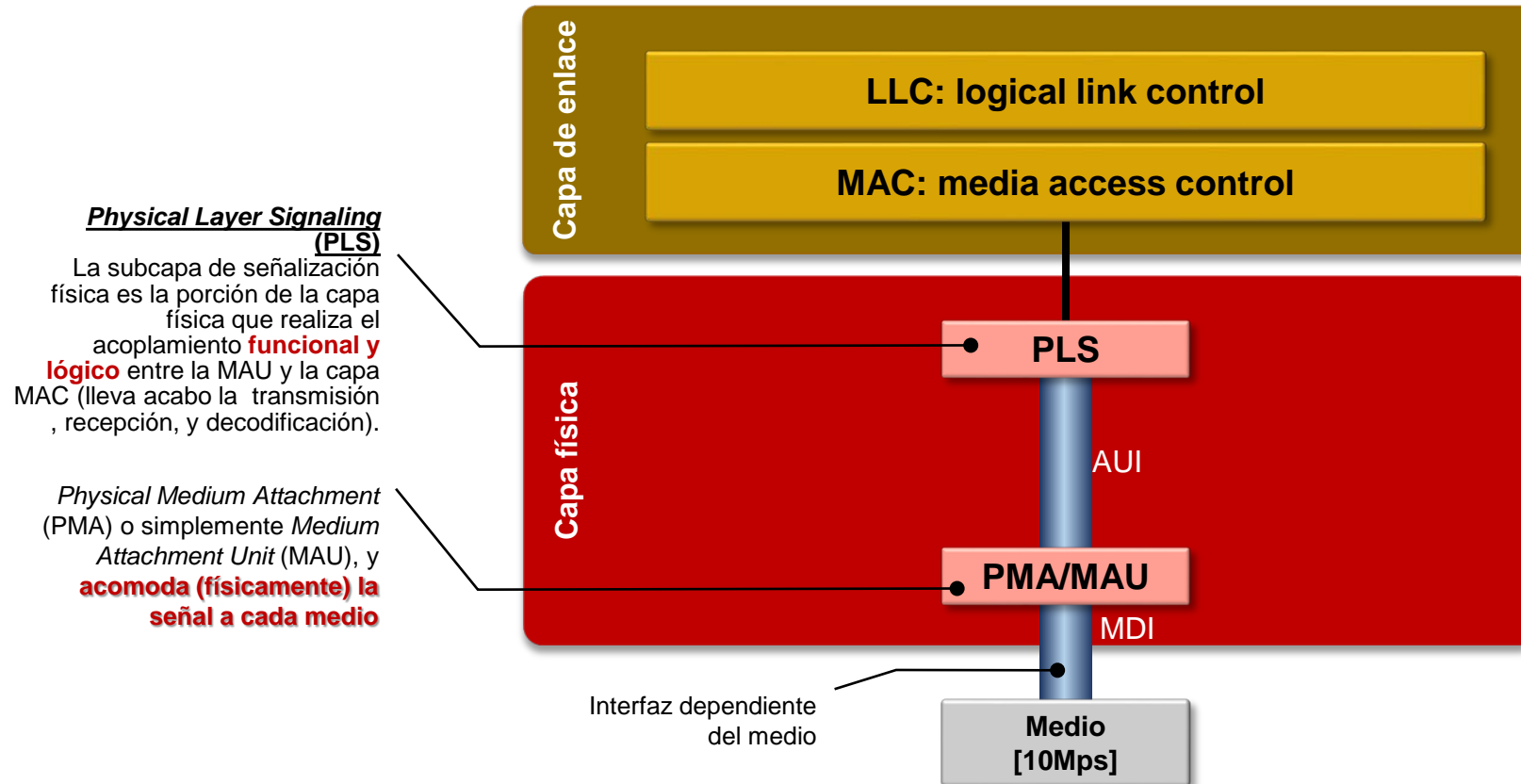
100BASE-TX (cobre[2])

# El modelo de IEEE 802.x

## Subcapas del nivel físico



Modelo 802



Media dependant interface (MDI)

Physical Layer Signaling (PLS)

Attachment Unit Interface (AUI)

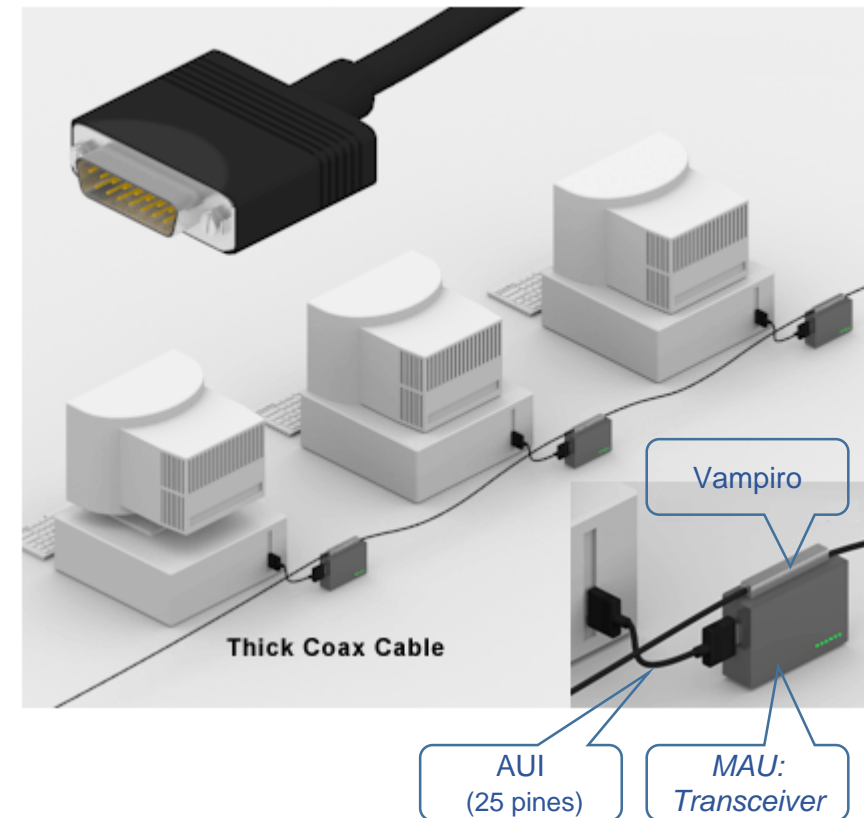
Physical Medium Attachment (PMA)

# Estándares físicos de las LANs

## IEEE 802.3 (10Base5)



- Fue la primera red Ethernet (IEEE 802.3; 1983) y era conocida como Ethernet de cable grueso (*Thick Ethernet*)
  - Muy fiable
  - Topología en Bus.
  - La señal es sacada del bus mediante conexiones vampiro
  - Longitud total máxima de los segmentos de 500m unidos: 2.500 metros
  - Número máximo de equipos por segmento: 100 por especificación



Physical Layer Signaling (PLS)  
Attachment Unit Interface (AUI)  
Physical Medium Attachment (PMA)

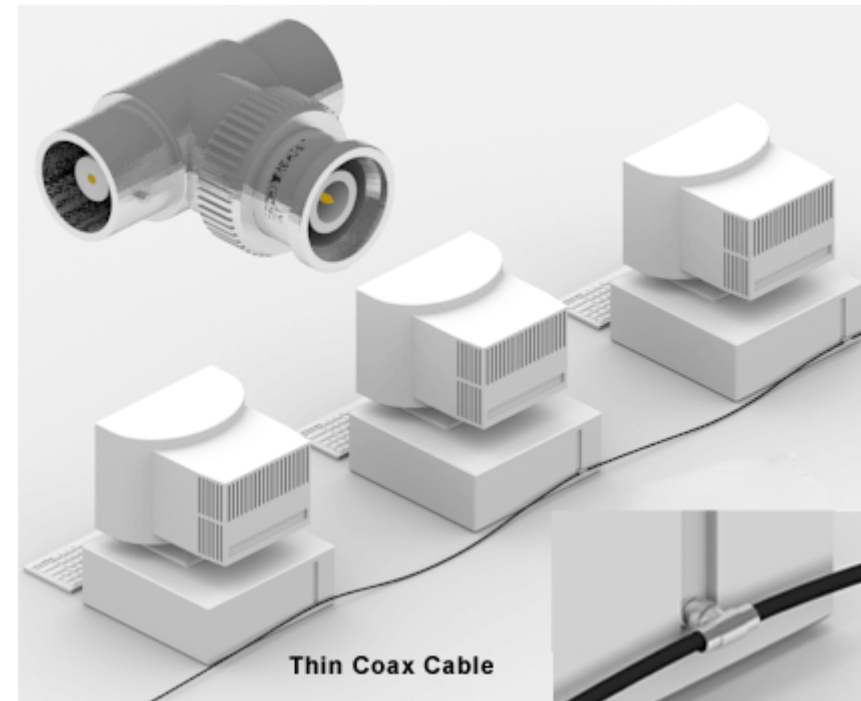


# Estándares físicos de las LANs

## IEEE 802.3a (10Base2)



- Conocida como Ethernet de cable fino (*Thin Ethernet*)
  - Muy fiable
  - Topología en Bus.
  - La señal es sacada del bus un conector BNC en forma de T.
  - Los cables coaxiales pueden tener una longitud máxima de 185 metros .
  - Número máximo de equipos por segmento es de 30.
  - Coste bajo.



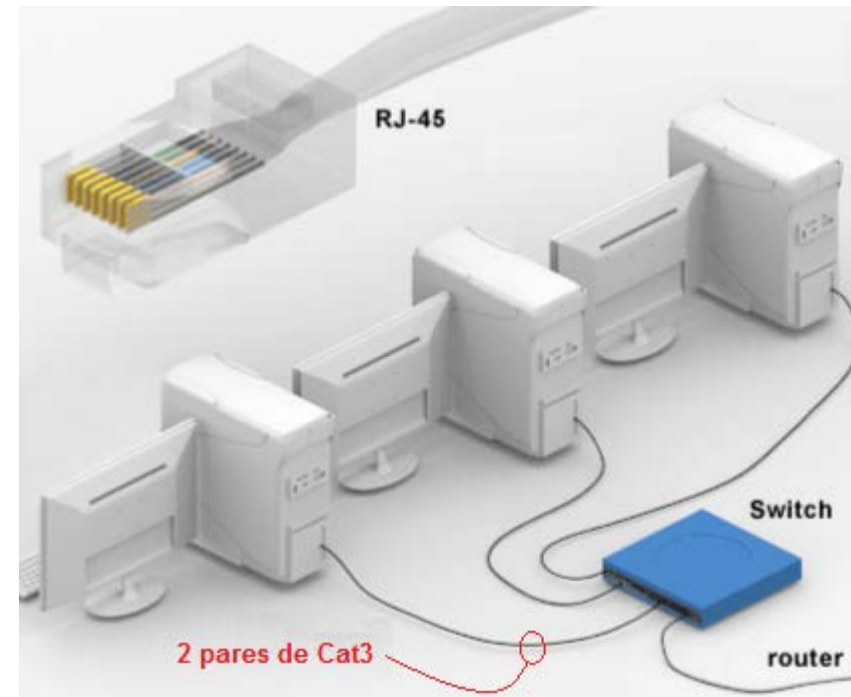
# Estándares físicos de las LANs

## IEEE 802.3b (10Base-T)



### ■ Es el estándar mas común (1990)

- Cable par trenzado UTP CAT3 (2 pares).
- **Conectores RJ45**
- Topología en estrella con *hub* o *switch*
- Cada segmento: 100m. Longitud máxima 2,5 km (con repetidores)
- Hasta 1024 estaciones
- Coste bajo.



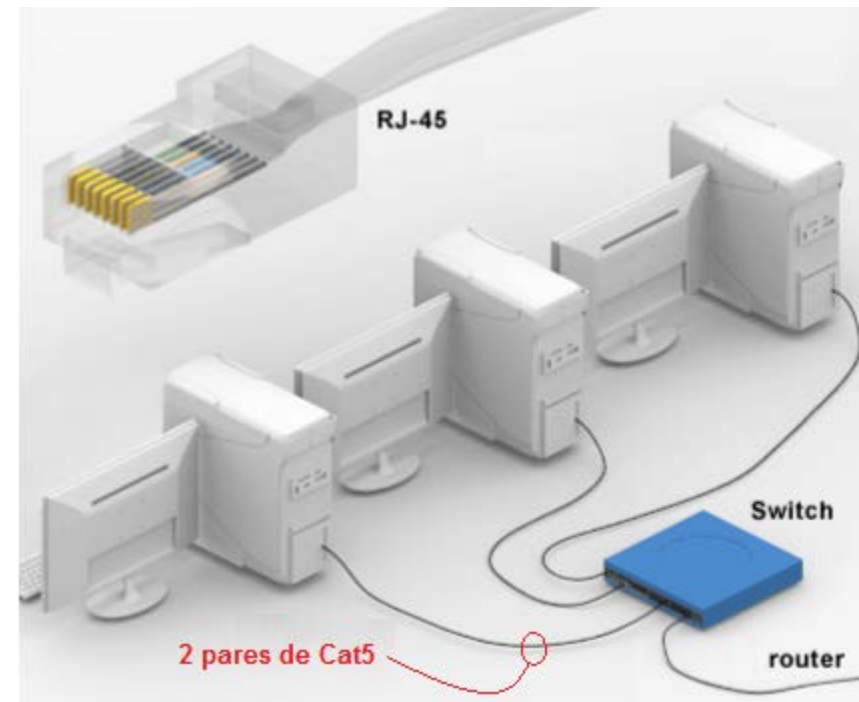
# Estándares físicos de las LANs

IEEE 802.3u (100Base-TX). Fast Ethernet



## ■ Es muy similar a 10Base-T (1995)

- Cable par trenzado UTP CAT5 (2 pares).
- Conectores RJ45
- Topología en estrella con *hub* o *switch*
- Longitud máxima 2,5km. Cada segmento: 100m.
- Número máximo de equipos por dominio de colisión es de 1024.
- Coste bajo.

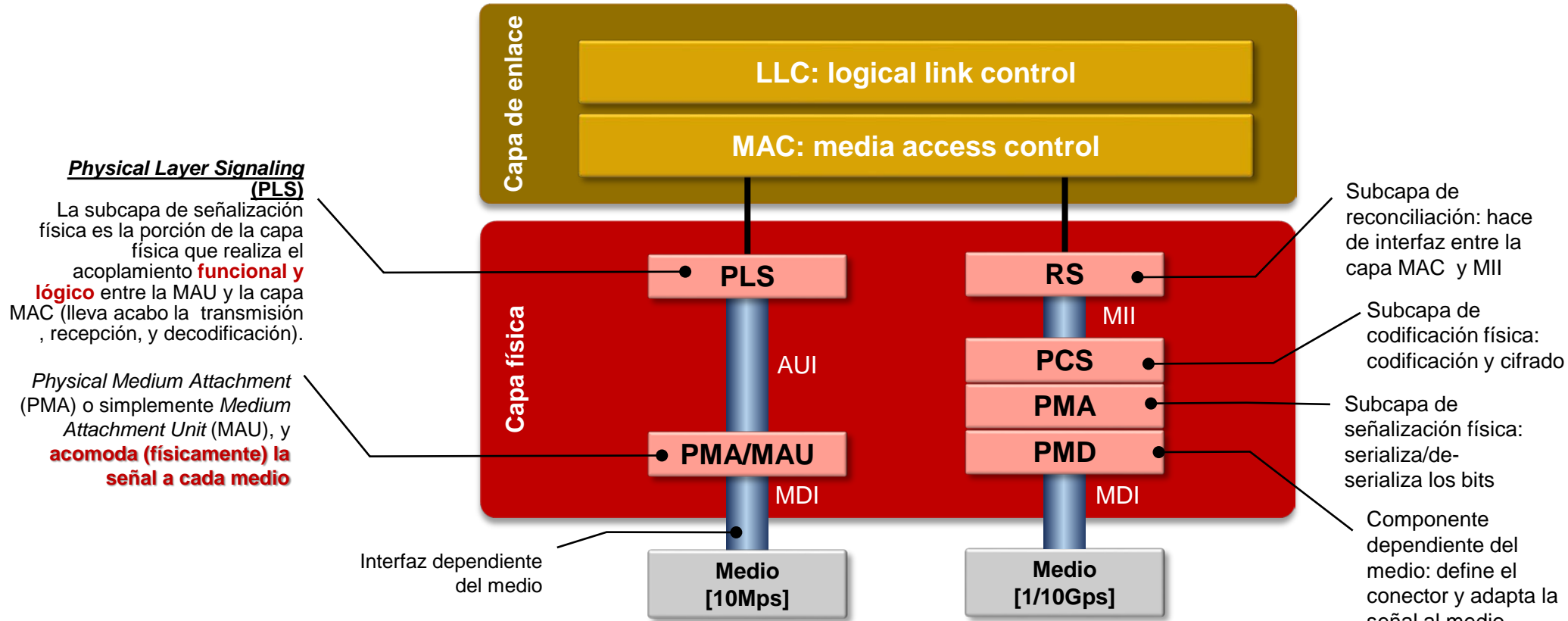


# El modelo de IEEE 802.x

## Subcapas del nivel físico por encima de 10Mbps



Modelo 802



- Media dependant interface (MDI)
- Physical Layer Signaling (PLS)
- Attachment Unit Interface (AUI)
- Physical Medium Attachment (PMA)

# Estándares físicos de las LANs

## IEEE 802.3ab ampliado (1000BASE-X)



- Gigabit Ethernet es una *Fast Ethernet* supercargada. Su estrategia es la misma que *Fast Ethernet*.
- La compatibilidad hacia atrás facilita la migración

IEEE 802.3ab

1000BASE-SX	1000BASE-LX	1000BASE-CX	1000BASE-T
<ul style="list-style-type: none"><li>• MMF</li><li>• Primera ventana a 850 nm</li><li>• Long. de onda pequeñas</li><li>• Hasta 500m</li></ul>	<ul style="list-style-type: none"><li>• MMF</li><li>• Segunda ventana a 1300 nm</li><li>• Mayores long. de onda</li><li>• Hasta 5km</li></ul>	<ul style="list-style-type: none"><li>• Cobre</li><li>• Cable apantallado</li><li>• Hasta 25m</li></ul>	<ul style="list-style-type: none"><li>• Cobre</li><li>• UTP Cat5</li><li>• Hasta 1000m</li></ul>

# Estándares físicos de las LANs

## IEEE 802.3ae (10GBASE-X)



- **10 Gigabit Ethernet** es el estándar más reciente (año 2002) y más rápido de los estándares Ethernet. IEEE 802.3.
- Es un protocolo *full-duplex* y no requiere de CSMA / CD.

10GBASE-SR	10GBASE-LR	10GBASE-ER	10GBASE-T
<ul style="list-style-type: none"><li>• MMF</li><li>• Primera ventana a 850 nm</li><li>• Long. de onda pequeñas</li><li>• Hasta 26-82m</li></ul>	<ul style="list-style-type: none"><li>• SMF</li><li>• Segunda ventana a 1310 nm</li><li>• Mayores long. de onda</li><li>• Hasta 10km</li></ul>	<ul style="list-style-type: none"><li>• SMF</li><li>• ventana a 1550 nm</li><li>• Hasta 40m</li></ul>	<ul style="list-style-type: none"><li>• Cobre</li><li>• UTP Cat6, ó 7</li><li>• Hasta 100m</li></ul>

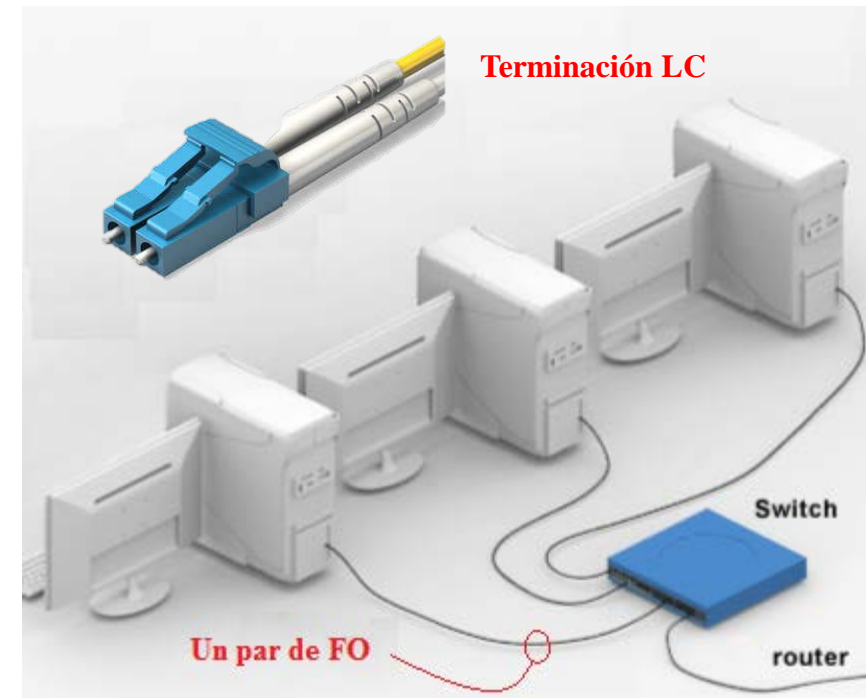


# Estándares físicos de las LANs

## IEEE 802.3ae (10GBase-SR)



- Entre los estándares de FO es el más utilizado
  - FO Multimodo (850 nm)
  - Los conectores son tan variados como sus aplicaciones
  - Topología en estrella con *switch*
  - La longitud máxima, dependiendo del tipo de FO, puede llegar a 300m
  - En su rango es el más barato.





# 5. Formato de la trama Ethernet

Formato de la trama MAC

Formato de la trama IEEE 802.2

Formato de la trama IEEE 802.2 con SNAP

Diferencias entre Ethernet II y 802.3

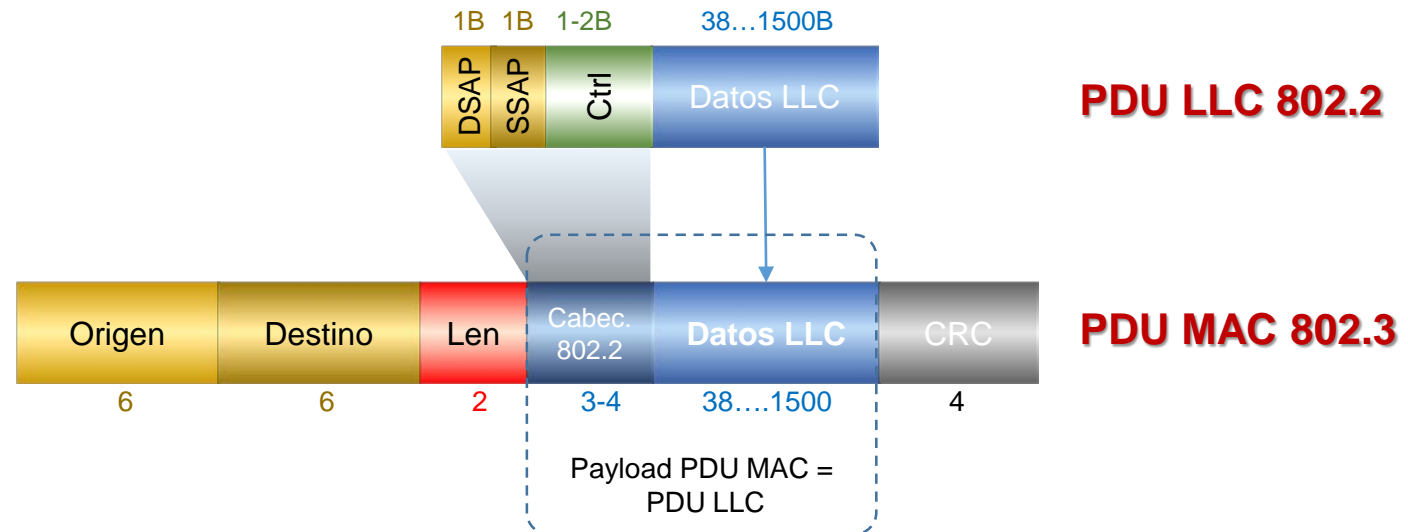
# Formato de la trama MAC

## Ethernet II y IEEE 802.3



- **Preámbulo** (7 octetos): 1010...10 para sincronizar los relojes.
- **SFD** (*start of frame delimiter*): Delimitador de principio de trama (1 octeto: 10101011)
- **Origen/Destino**: son direcciones MAC
- **Longitud de datos/Tipo de Protocolo** (802.3/Ethernet II).
- **Datos** (0-1500 octetos. Mínimo 46 bytes => longitud mínima de la trama 64 bytes). Si no llega a 46 se hace un Relleno (*Padding*): asegura que el tamaño mínimo de la trama sea de 512 bits (46+18=64 octetos, no incluido el preámbulo).
- **CRC (Cyclic Redundancy Coding)**, 4 octetos): control de errores.

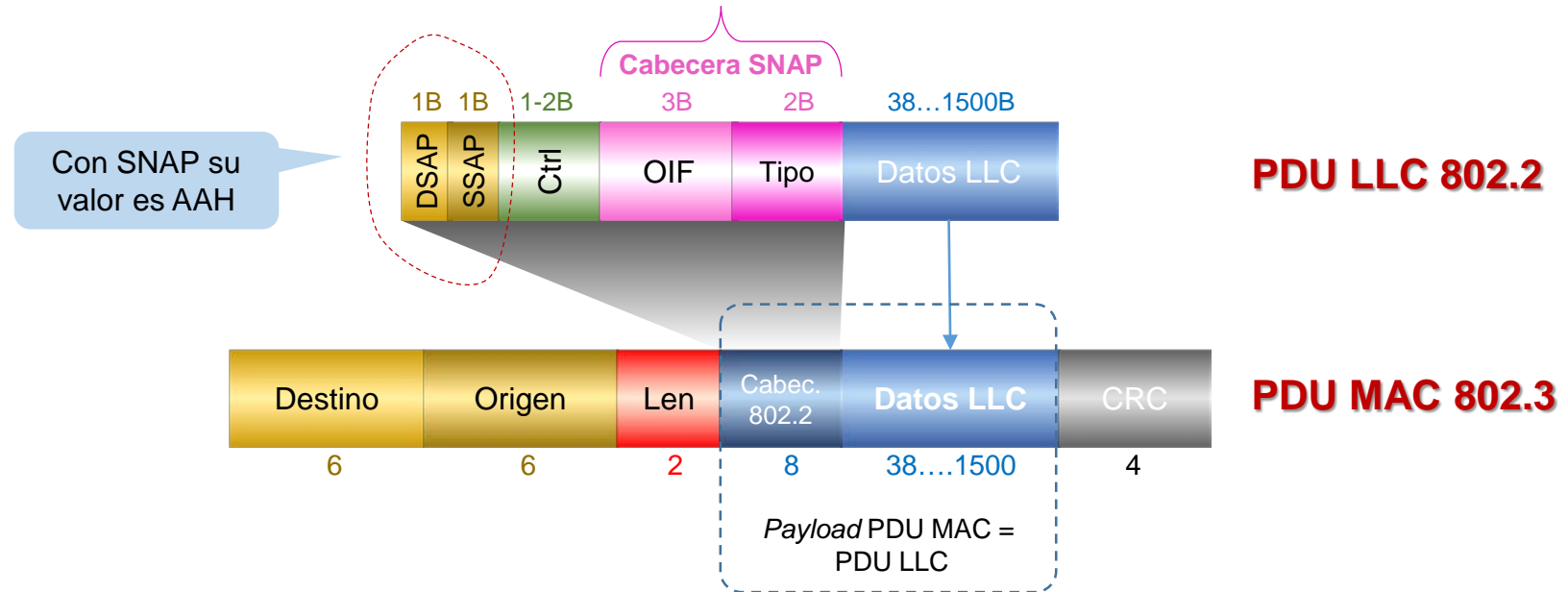
# La trama IEEE LLC 802.2 vs. MAC 802.3



- **DSAP** (1 octeto): Destino de *SAP*, es un campo que simplemente actúa como un puntero a un búfer de memoria en la estación receptora.
- **SSAP** (1 octeto): El SSAP o Fuente de *Service Access Point*, es análogo a la DSAP, y especifica el punto de acceso de servicio (SAP) del proceso de envío.
- **Control** (2 octetos): Especifica el tipo de trama LLC que se trata.
- **Datos** (0-1500 octetos. Mínimo 46 bytes => longitud mínima de la trama 64 bytes).

# Formato de la trama IEEE 802.2

## Alternativa con SNAP



- Nuevos campos (cabecera SNAP):
- OIF (3 octetos): *Organization Identifier Field* o código del proveedor.
- Tipo (2 octetos): Identifica al protocolo de nivel superior dentro de un fabricante. Se le suele llamar *Ethertype*.

*El Subnetwork Access Protocol (SNAP) es un protocolo recogido por la norma IEEE 802 que permite direccionar diferentes protocolos utilizando un SAP.*

*Aunque apenas se ha implementado en Ethernet, si se usa en FDDI y en token ring, y IEEE 802.11*



# Diferencias entre Ethernet y IEEE 802.3



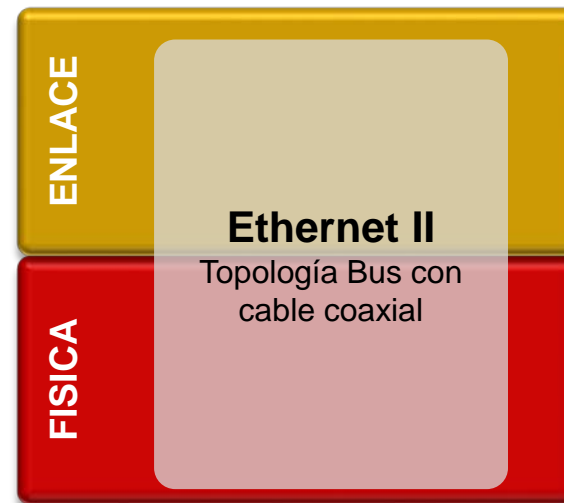
## Similitudes

- Protocolo de acceso al medio CSMA/CD
- Topología lógica “bus”

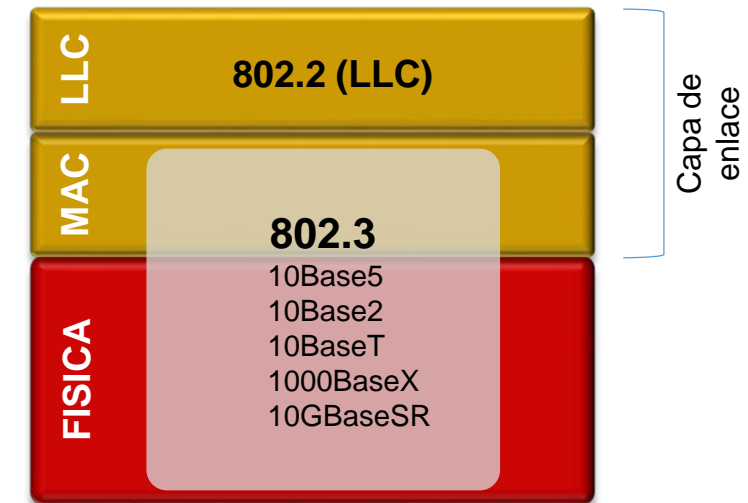
## Diferencias

- Ethernet II solo especifica el cable coaxial
- 802.x divide la capa de enlace en dos subniveles
- El formato de la cabecera de las tramas de enlace es diferente
- El estándar DIX está obsoleto aunque aún se puede ver en las redes

### Modelo Ethernet II (DIX)



### IEEE 802.x







# 6. Interconexión entre LANs

Concepto de interconexión de redes

Interconexión a nivel físico

Interconexión a nivel de enlace

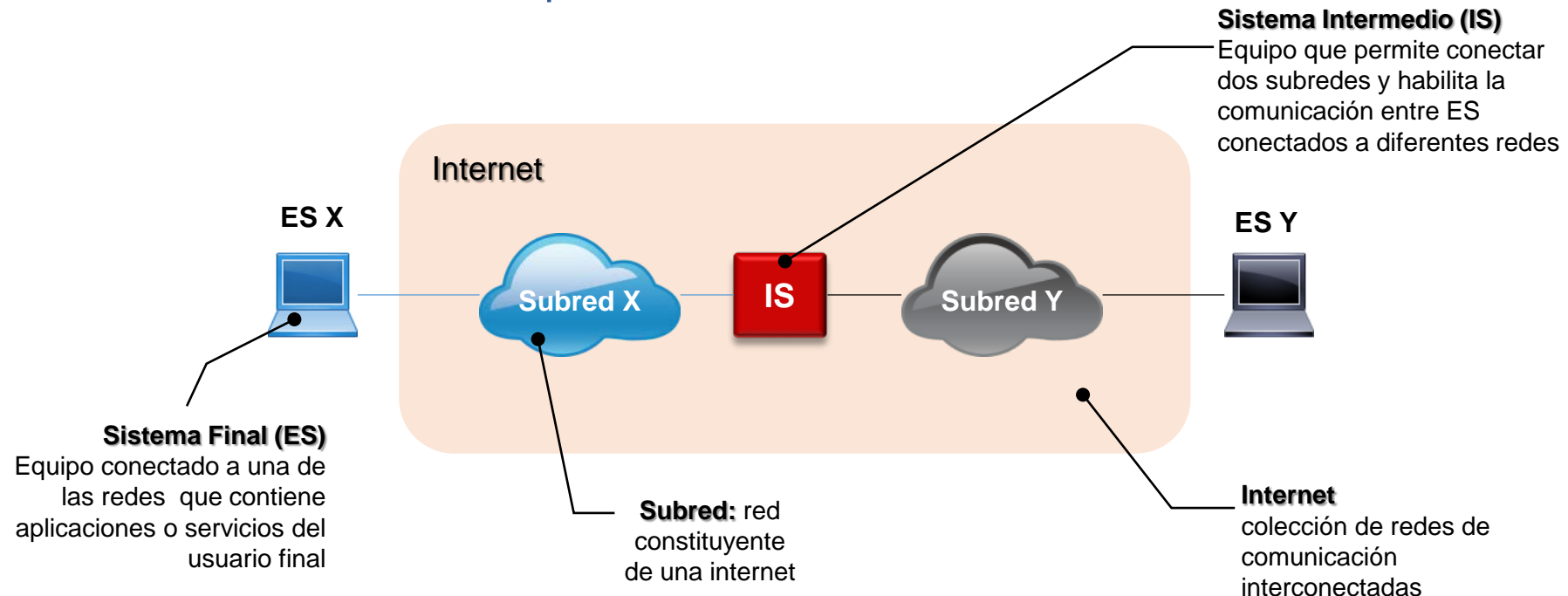
Casos de estudio

Características y funcionalidades de los puentes

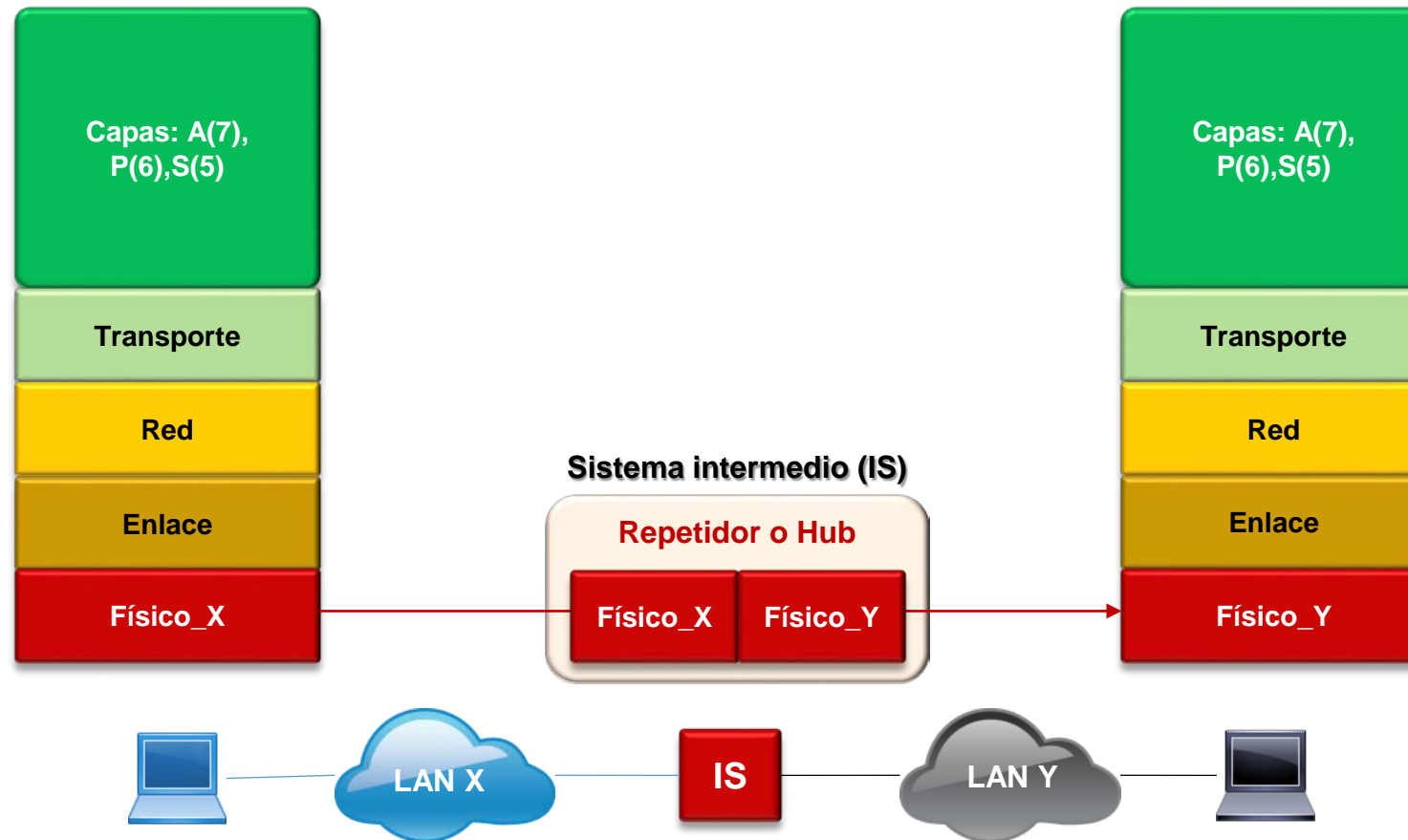
# Concepto de interconexión de redes



- La interconexión de redes (*internetworking*) es la conexión física y lógica entre dos o más redes (con tecnologías y diseños diferentes).
  - Su objetivo es facilitar que los usuarios de cualquier red se puedan comunicar con los usuarios de las demás redes, y dar acceso a los servicios ofrecidos por las distintas redes.

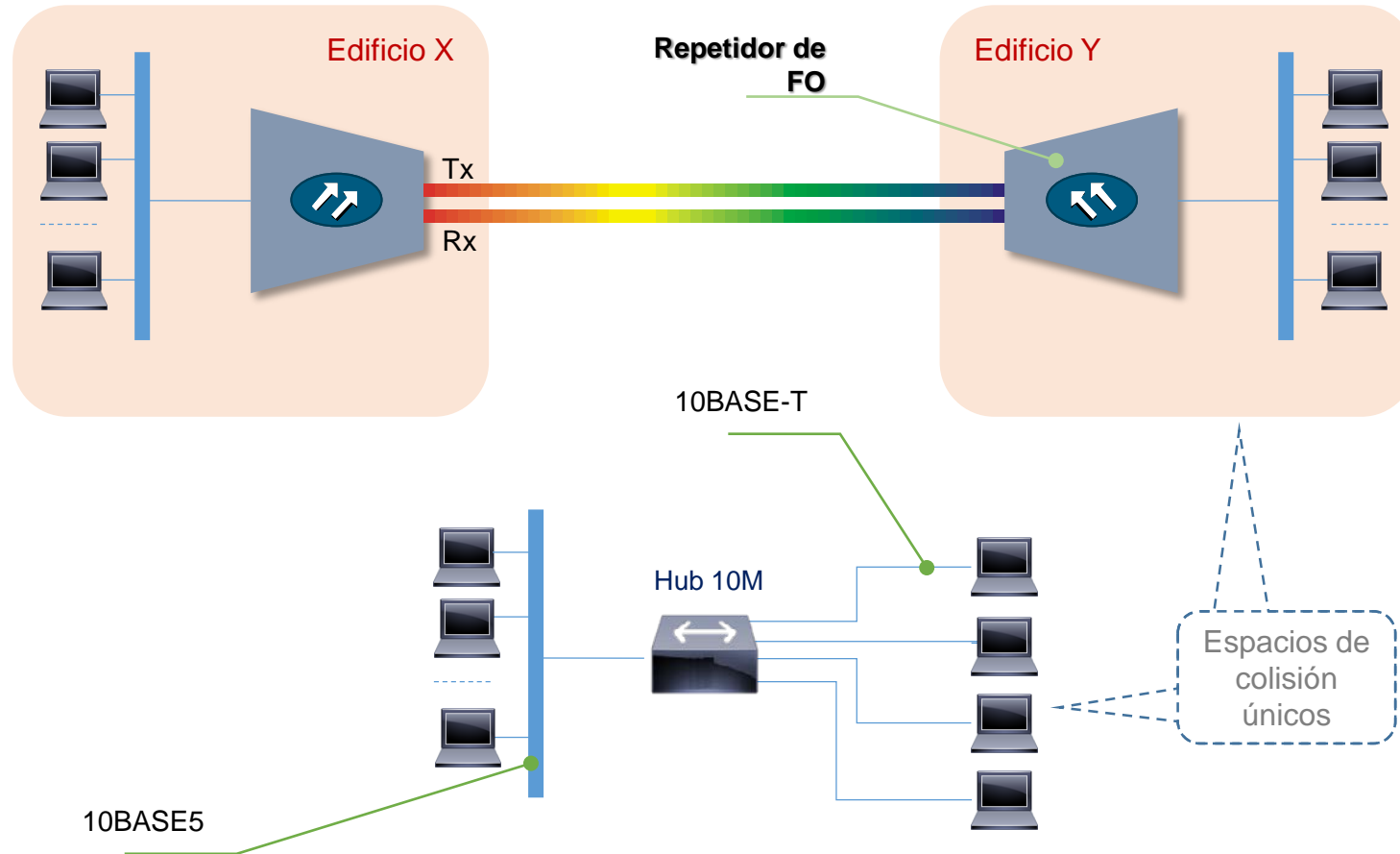


# Interconexión a nivel físico



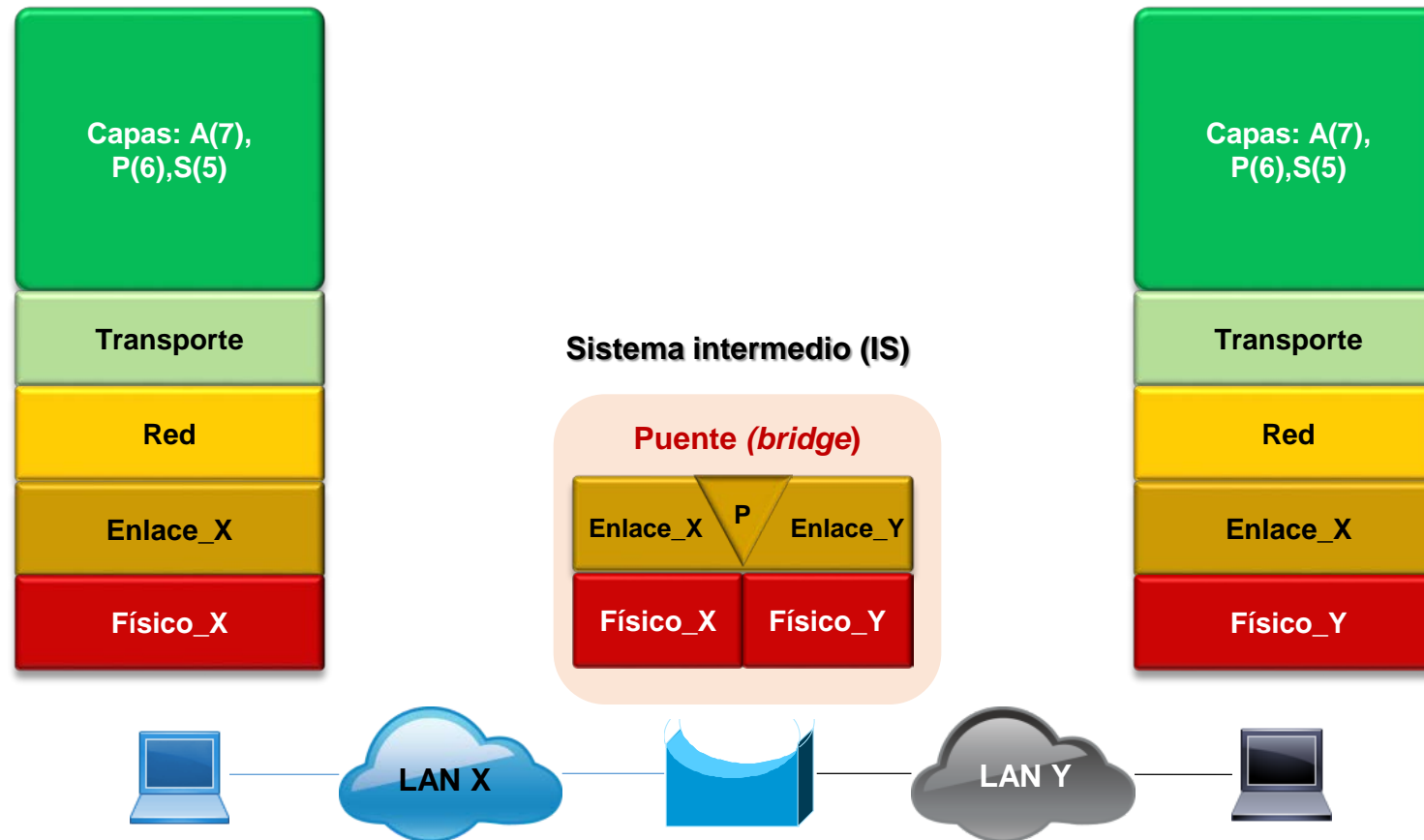
# Interconexión a nivel físico

## Ejemplos



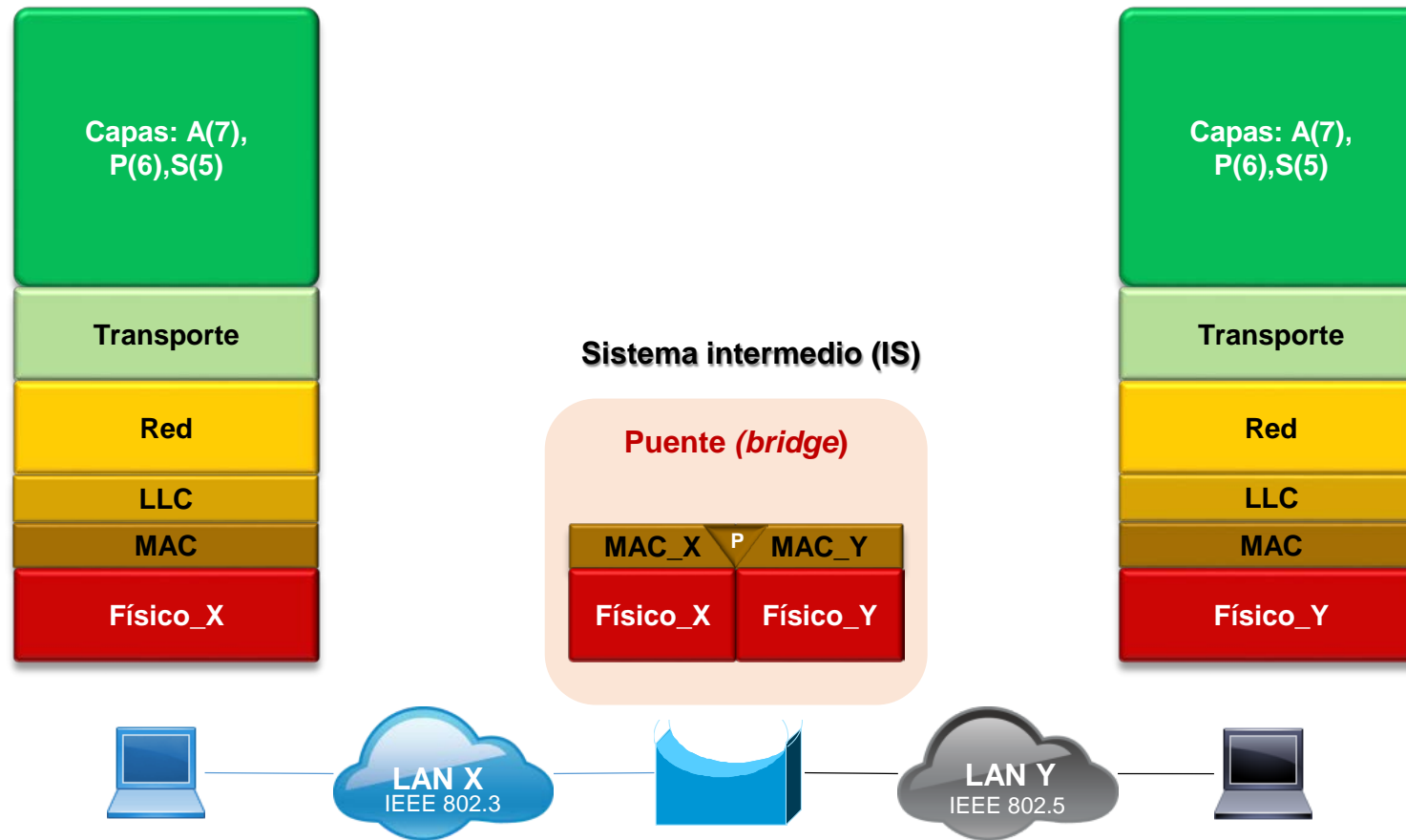
# Interconexión a nivel de enlace

## Ethernet DIX. Puente heterogéneo



# Interconexión a nivel de enlace

## IEEE 802.3. Puente heterogéneo





# Características y funcionalidades de los puentes

## Funciones

- Lectura de todas las tramas transmitidas (**modo promiscuo**)
- Retransmisión selectiva de las tramas leídas (**encaminamiento y direccionamiento**)
- Conexión de mas de 2 LANs

## Ventajas

- Fiabilidad, gracias a la división en **segmentos** (espacios de **colisión**)
- Prestaciones, ya que los segmentos mas pequeños son mas eficientes
- Mayor alcance
- Transparentes para las estaciones (a nivel MAC). *Plug & Play*

## Aplicación

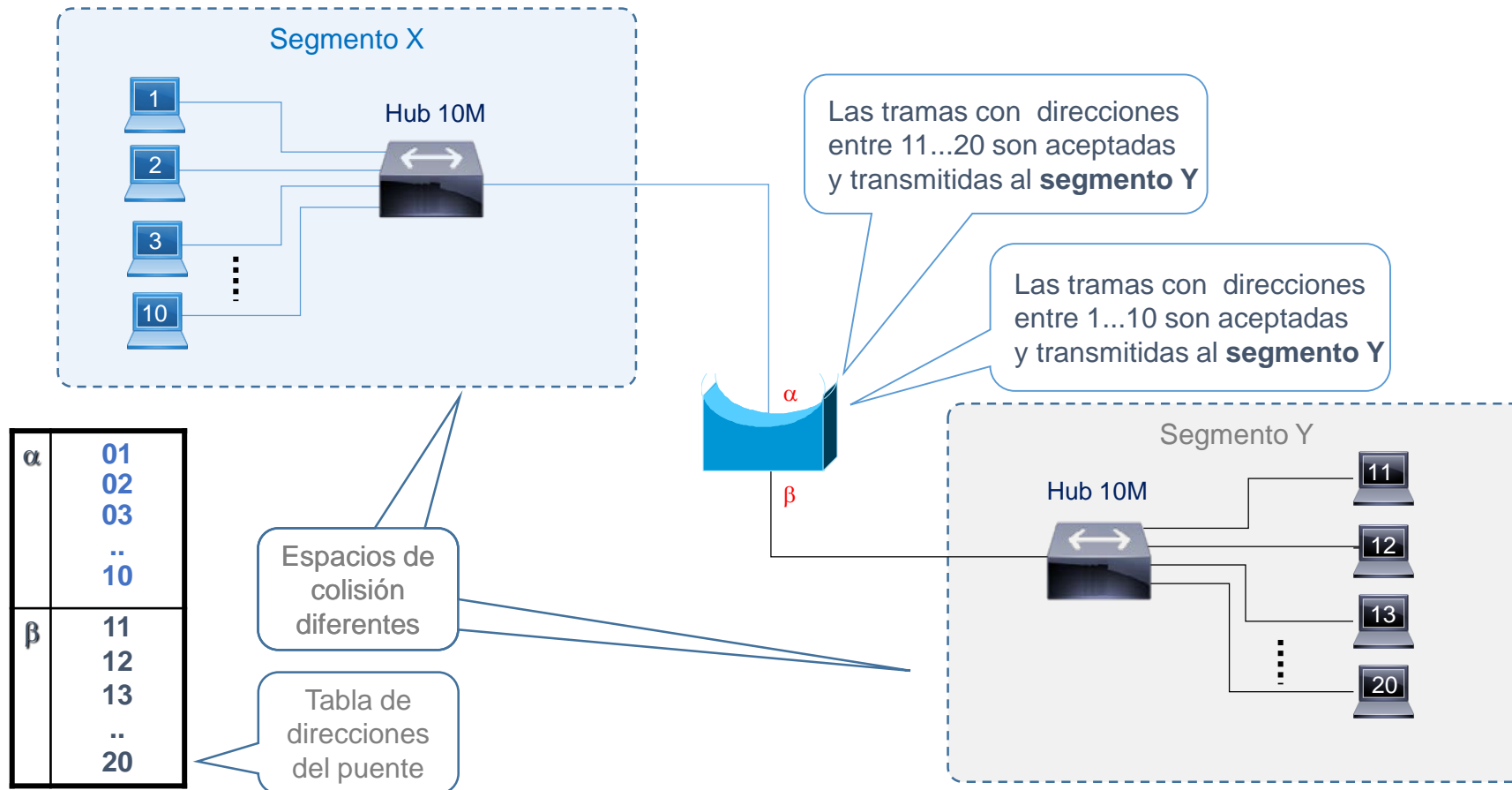
- En la interconexión de LANs que utilizan protocolos idénticos o similares (físico y MAC).
- Filtrado

## Diseño

- Memoria suficiente
- Control de bucles (***Spanning tree protocol***)

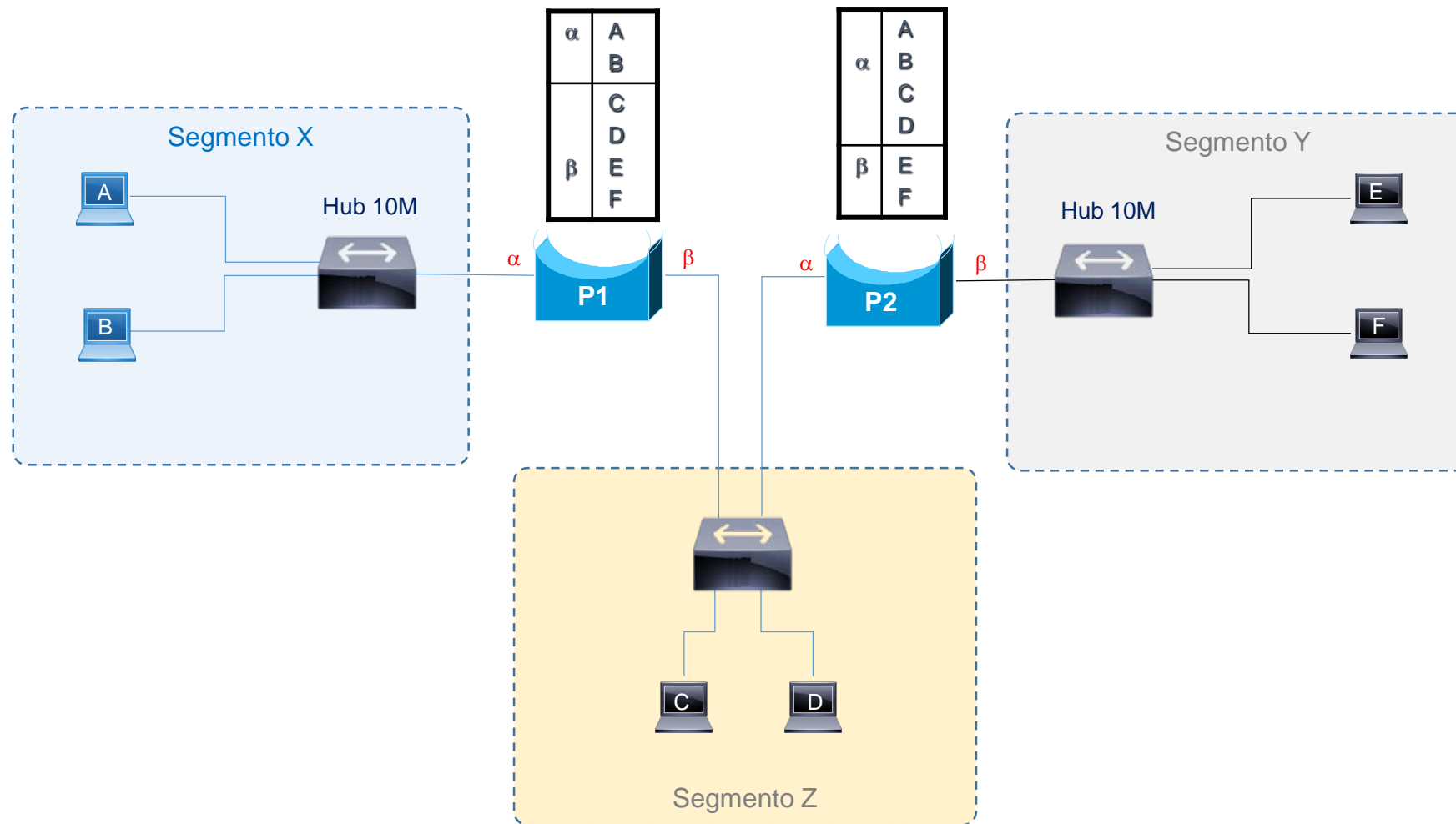
# Caso de estudio 1

## Interconexión de 2 segmentos LAN



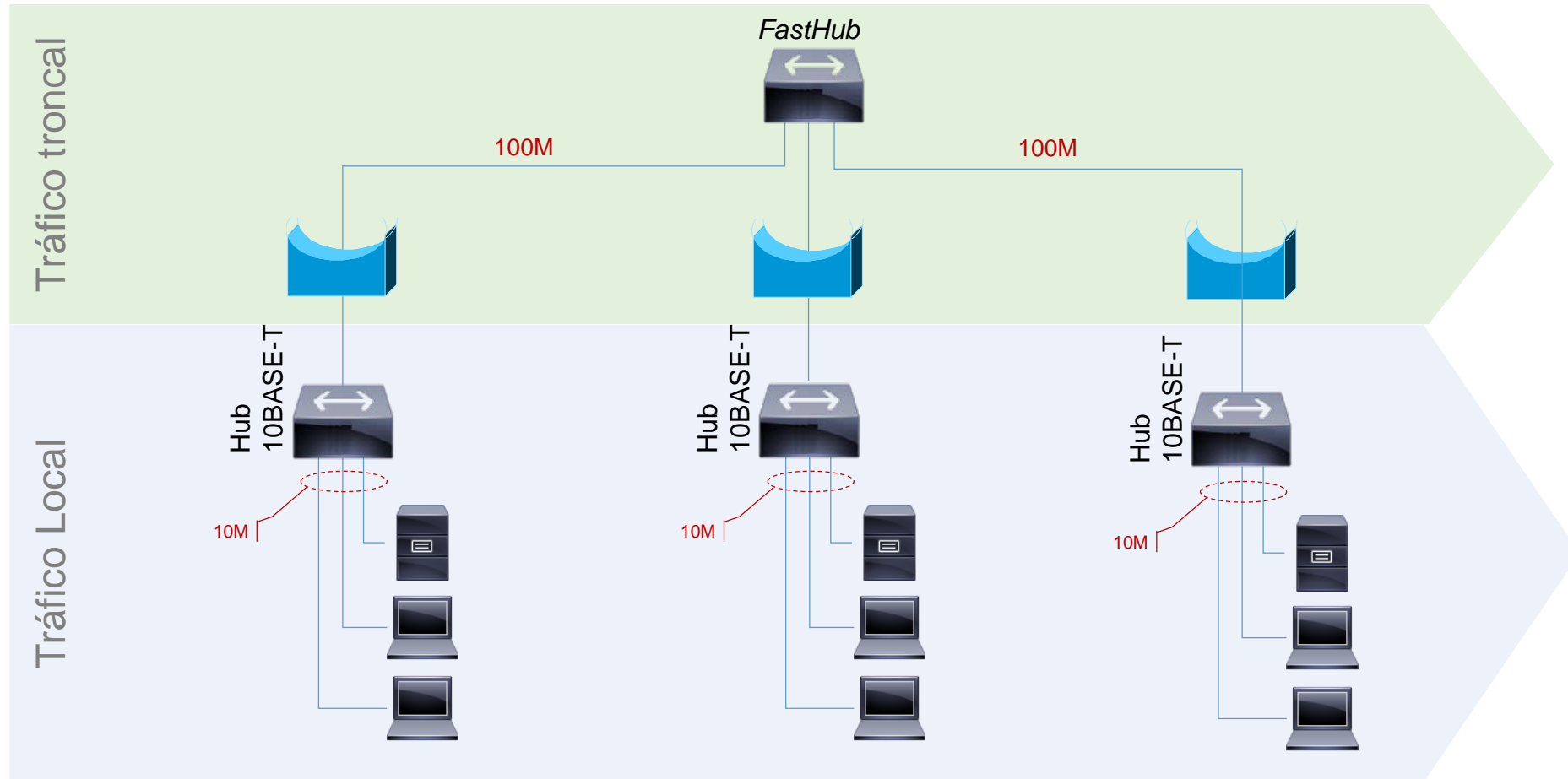
# Caso de estudio 2

## Interconexión de 3 segmentos con 2 puentes



# Caso de estudio 3

## Arquitectura de red troncal





# 7. Topologías LAN con bucles

El problema de los bucles

Representación de las redes como grafos

El protocolo STP

El algoritmo STP

En caso de estudio

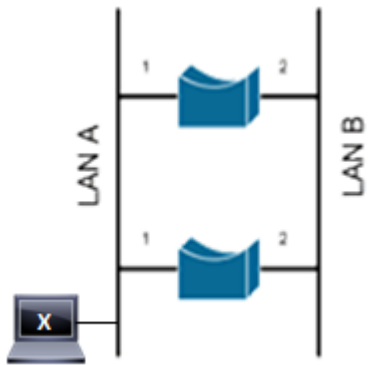
# El problema de los bucles



## ■ En una red existe un bucle cuando hay más de una conexión o camino entre dos nodos

- Aunque esta duplicidad de las conexiones es atractiva porque da redundancia, el bucle conduce a tormentas de difusión (véase el ejemplo)
- La solución es permitir los bucles físicos y crear una topología lógica libre de bucles mediante el protocolo STP

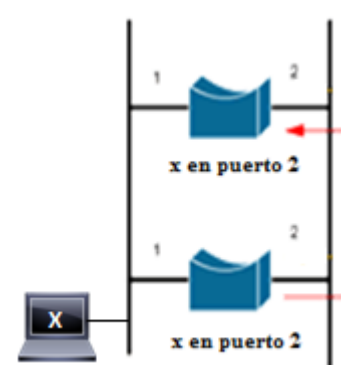
1) Los puentes no tienen ninguna entrada en su tabla de direcciones MAC.



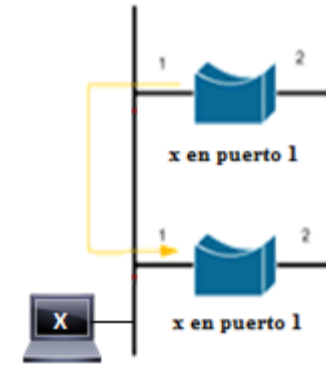
2) Una estación transmite un paquete con dirección MAC de origen X, los puentes guardan en la memoria que la estación con MAC = X se encuentra conectada al puerto 1 y proceden al *flooding*



3) Pero uno de los puentes va a ser el primero que transmitirá el paquete recibido en la LAN A a la LAN B, lo que hará que el otro puente interprete que la estación X se encuentra en la LAN B y guardará el paquete en la cola de la LAN A para el correspondiente *flooding*.



4) Ese puente envía el paquete de la LAN B a la LAN A y el otro puente renueva la entrada que dice que la estación X se encuentra en A y lo envía a la LAN B, este paquete será enviado a la LAN A por el otro puente y así sucesivamente

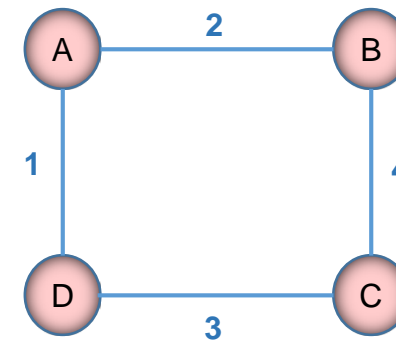
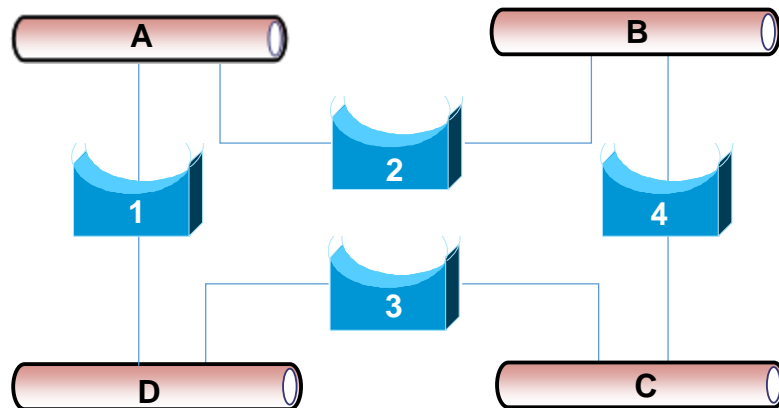




# Representación de las redes como grafos



- La red se puede representar como un **grafo**, donde cada **nodo** se corresponde con un segmento LAN y los **arcos** son los dispositivos (*bridges, switches*) que conectan 2 segmentos

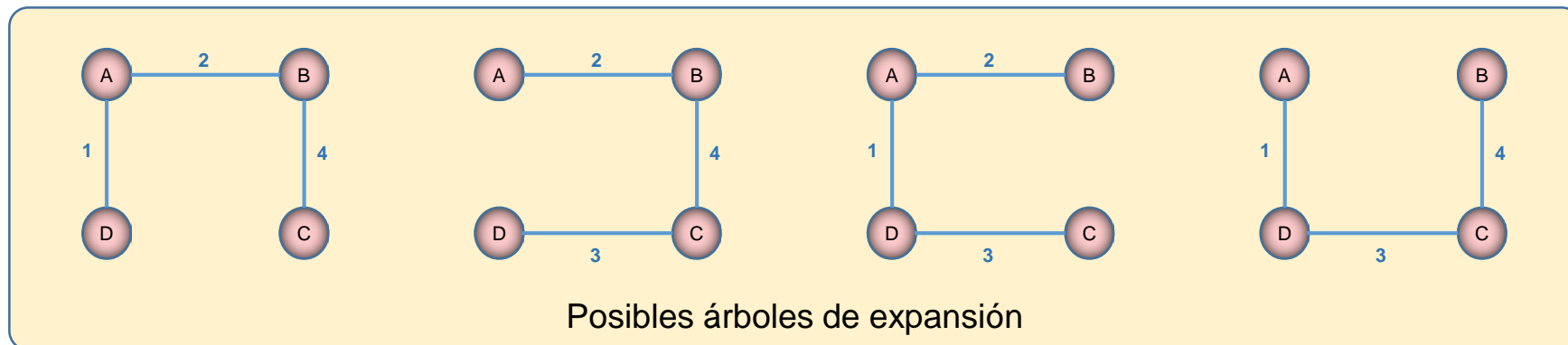
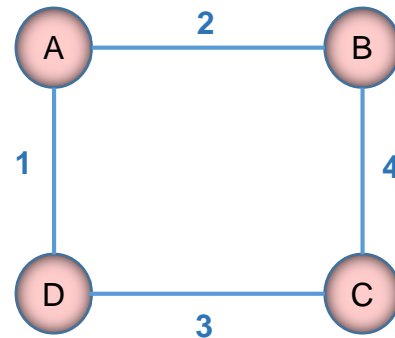


# El protocolo STP

*Spanning tree protocol (IEEE 802.1d)*



- El algoritmo STP transforma la red física, en la que existen bucles, en una red lógica en forma de árbol (llamado *árbol de expansión*), o sea libre de bucles.

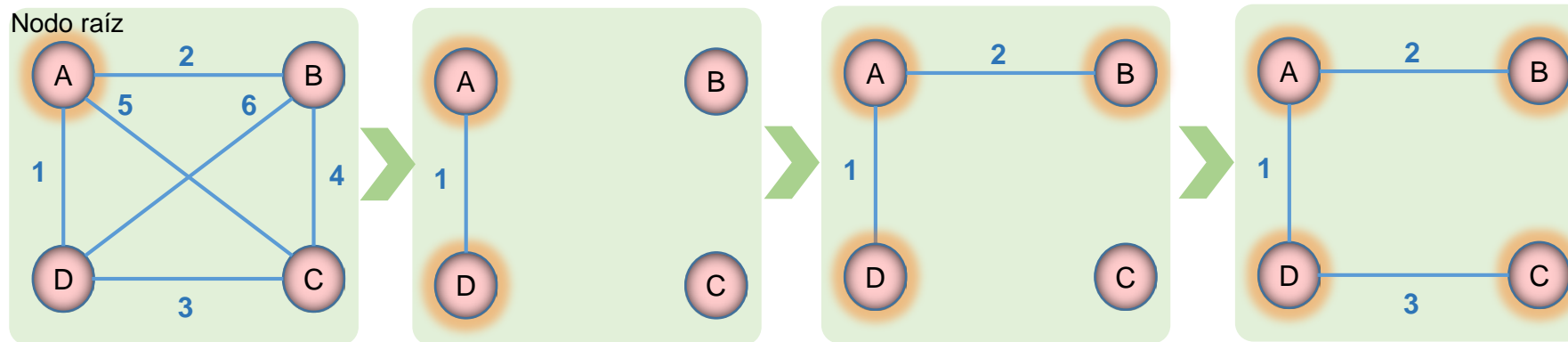


# El algoritmo STP

## Spanning tree protocol



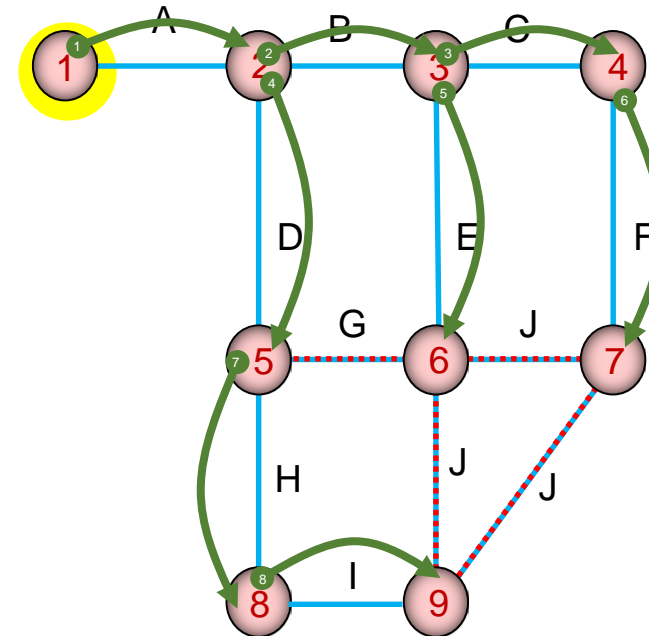
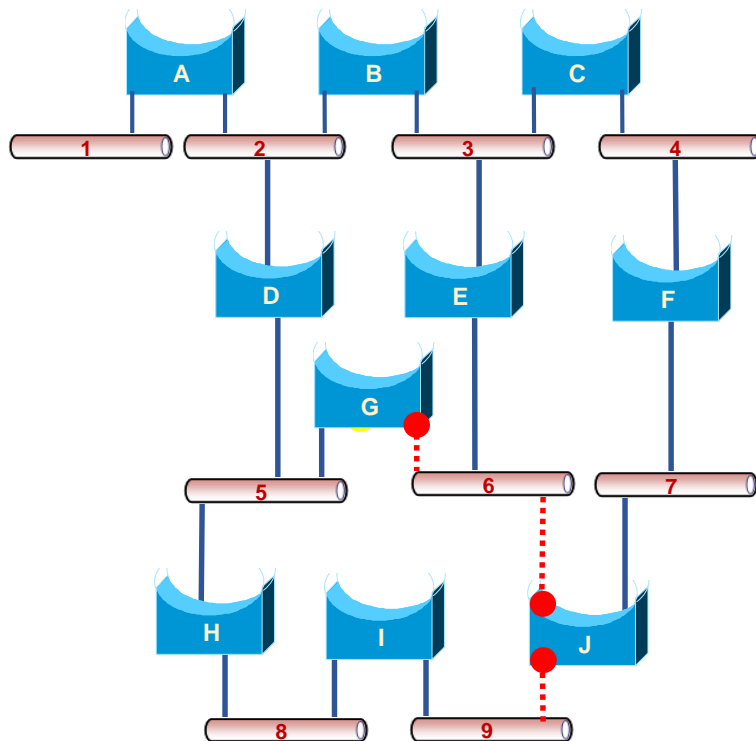
- El algoritmo STP es el mas habitual para determinar el árbol de expansión mínimo (el de menor coste). Su desarrollo es el siguiente:
  - 1. Se marca un nodo cualquiera que será el nodo de partida (**nodo raíz**).
  - 2. Seleccionamos la **arista** de menor valor en el **nodo marcado** anteriormente, y marcamos el otro nodo en el que incide.
  - 3. Repetir el paso 2 siempre que la arista elegida enlace un nodo de los marcados y otro que no lo esté.
  - 4. El proceso termina cuando tenemos todos los nodos del grafo marcados.



# Caso de estudio de STP



- En la red mostrada, a la que se aplica el algoritmo STP, el conjunto de puentes  $\mathbb{B} = \{A, B, C, D, E, F, H, I, J\}$  es tal que el de menos coste es "A", después le sigue "B", etc. Y, finalmente, el de mas coste es "J".
  - Se supone que el nodo inicial o vértice es "1"



● Puerto bloqueado



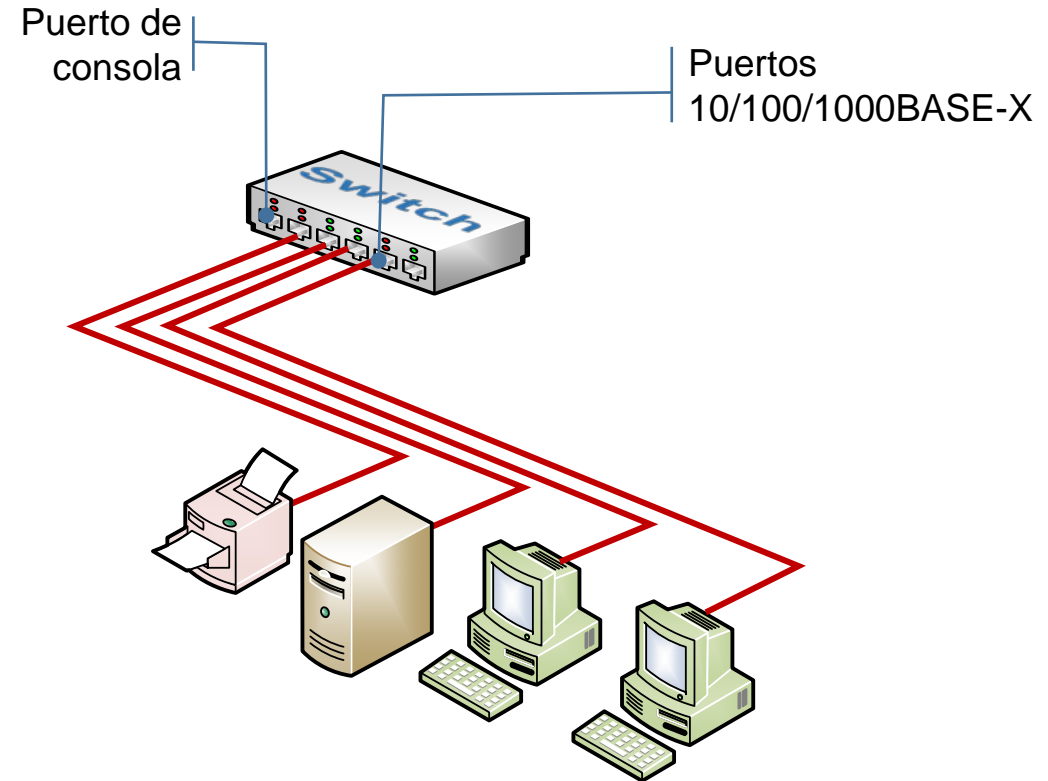
# 8. LANs conmutadas

Los conmutadores Ethernet  
Modos de funcionamiento de los  
conmutadores  
Casos de estudio

# Los conmutadores o *switches* Ethernet



- Los Conmutadores Ethernet (N2) son puentes de múltiples puertos que realizan la conmutación de forma muy rápida gracias a implementaciones en hardware con ASICs (*Application Specific Integrated Circuit*)
- Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino
- Los puentes han sufrido un retroceso comercial debido a las mayores prestaciones ofrecidas por los conmutadores



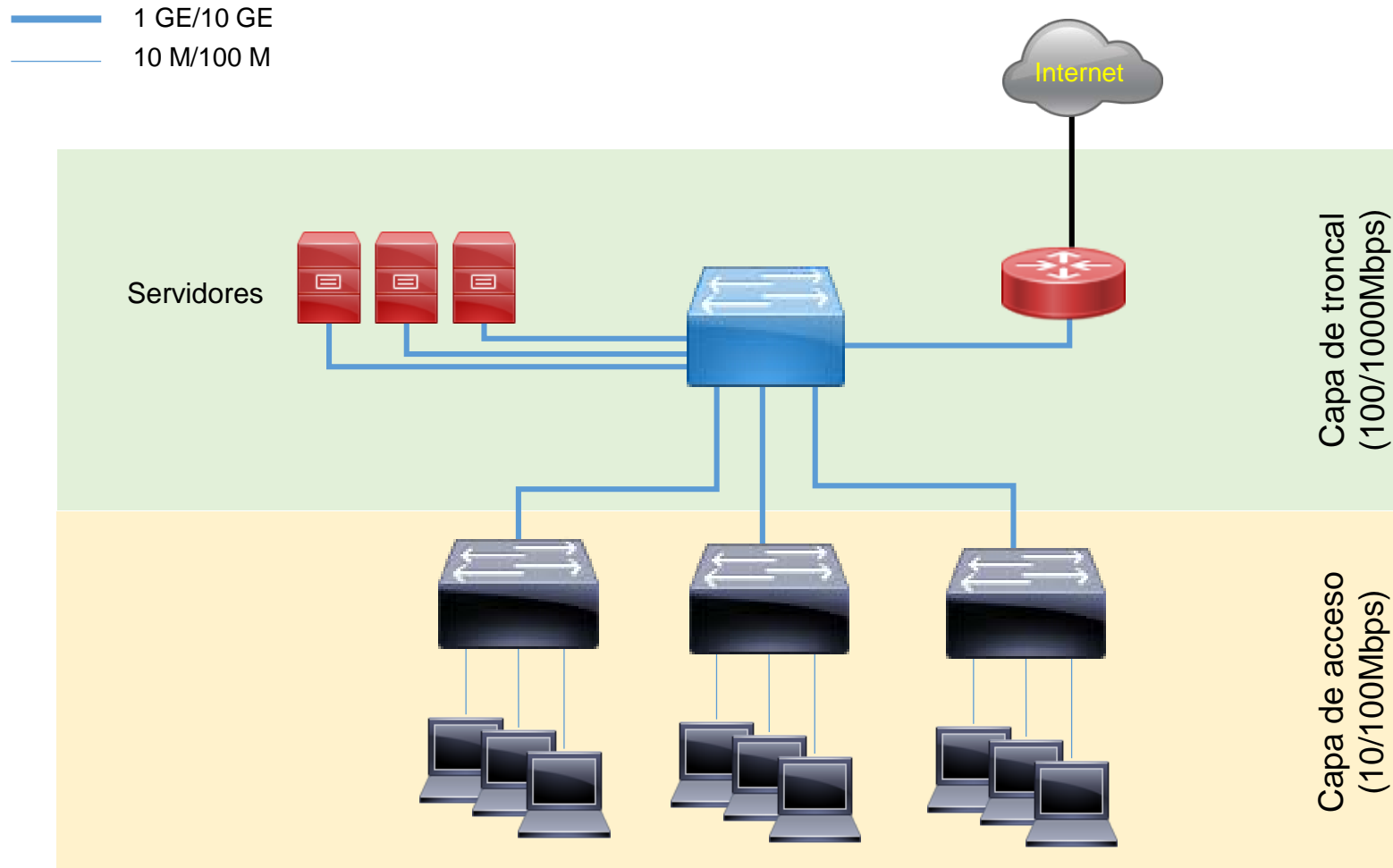


# Modos de funcionamiento de los conmutadores

- Almacenamiento y reenvío (*Store-and-Forward*):
  - El conmutador recibe la trama en su totalidad, la almacena, comprueba el CRC y la retransmite si es correcta (si no la descarta).
    - ✓ De uso común en oficinas y empresas.
- Conmutación de conexión directa (*cut-through*):
  - El conmutador empieza retransmitir la trama tan pronto ha leído la dirección de destino (6 primeros bytes). Aunque el CRC sea erróneo la trama se retransmite. **Menor latencia** que almacen./reenvío.
    - ✓ De aplicaciones muy específicas y especializadas
- Híbrido:
  - Usa cut-through inicialmente, pero si detecta que una estación genera tramas erróneas pasa a modo *almacenamiento/reenvío* para las tramas que vienen de esa dirección MAC.
    - ✓ De aplicaciones muy específicas y especializadas

# Caso de estudio

## LAN jerárquica conmutada

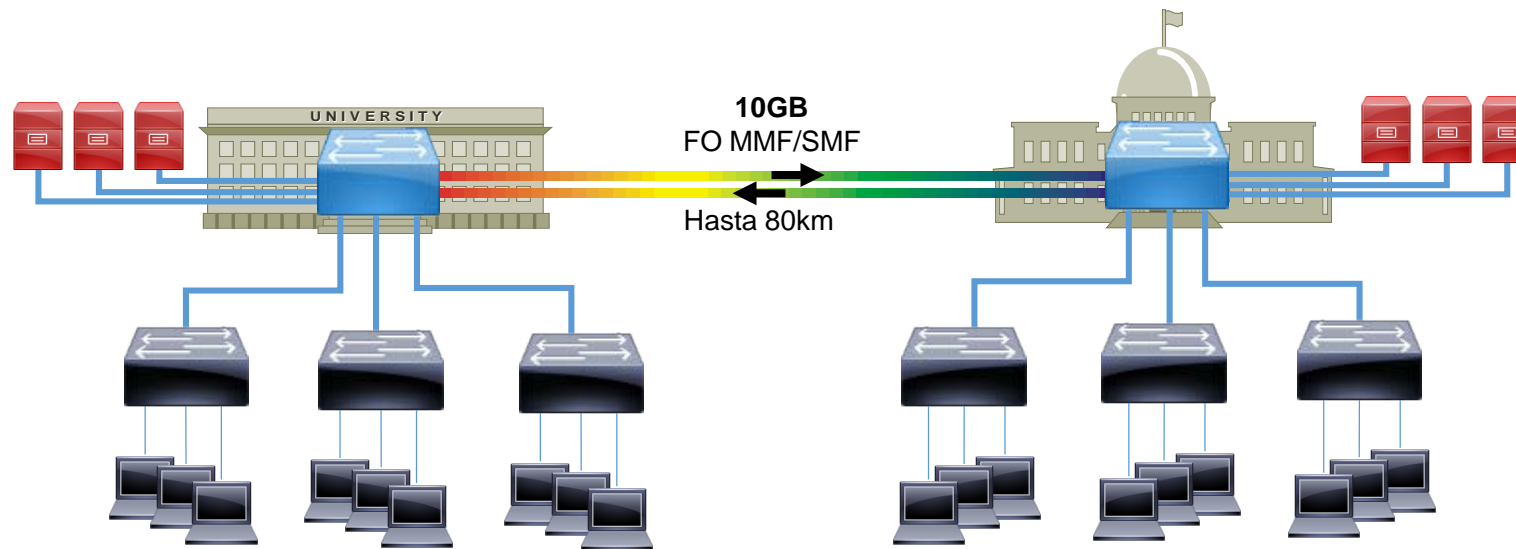


# Caso de estudio

## LAN conmutada metropolitana



- Una red Ethernet tradicional es semi-duplex: una estación puede transmitir una trama o recibirla, pero no ambas cosas simultáneamente
- Ethernet full-dúplex es un enlace punto a punto entre nodos (de conmutadores entre si o entre conmutadores y ordenadores).
- Se desactiva el CSMA/CD. No hay colisiones.



MMF: Multimode fibre  
SMF: Single mode fibre



# 9. Redes LAN virtuales (VLANs)

Concepto de VLAN

Ventajas de las VLANs

Modificación de la trama MAC

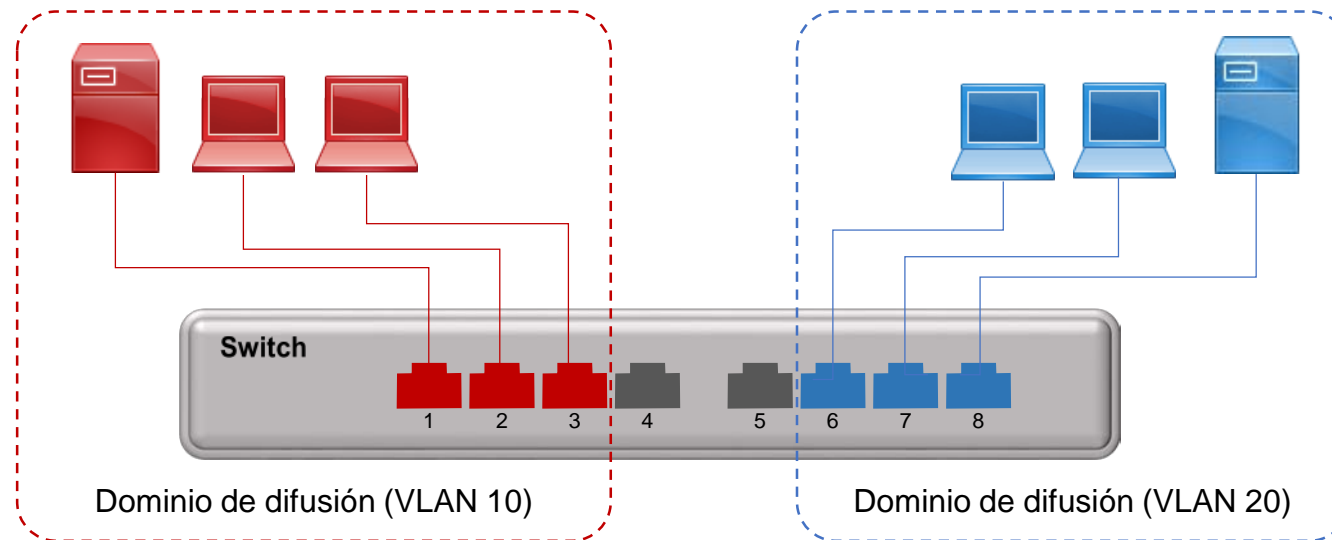
Caso de estudio

Pros y contras

# Concepto de VLAN

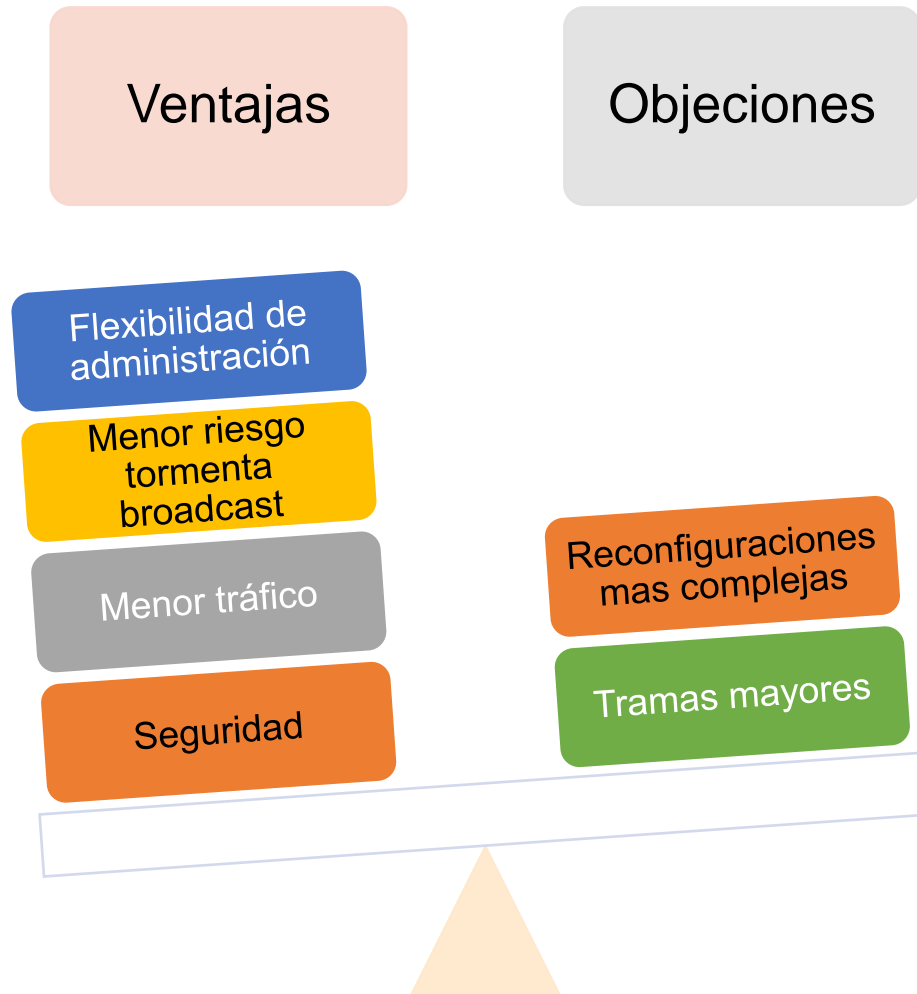


- La VLAN es una tecnología que permite crear redes lógicas independientes dentro de una misma red física.
  - Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.
  - Todas las estaciones de trabajo y los servidores de una VLAN comparten sus recursos, independientemente de la localización de su conexión física.
- Por tanto, las VLAN suponen una segmentación de la red basada en dominios *broadcast*.



VLAN	Puertos
10	1,2,3
20	6,7,8

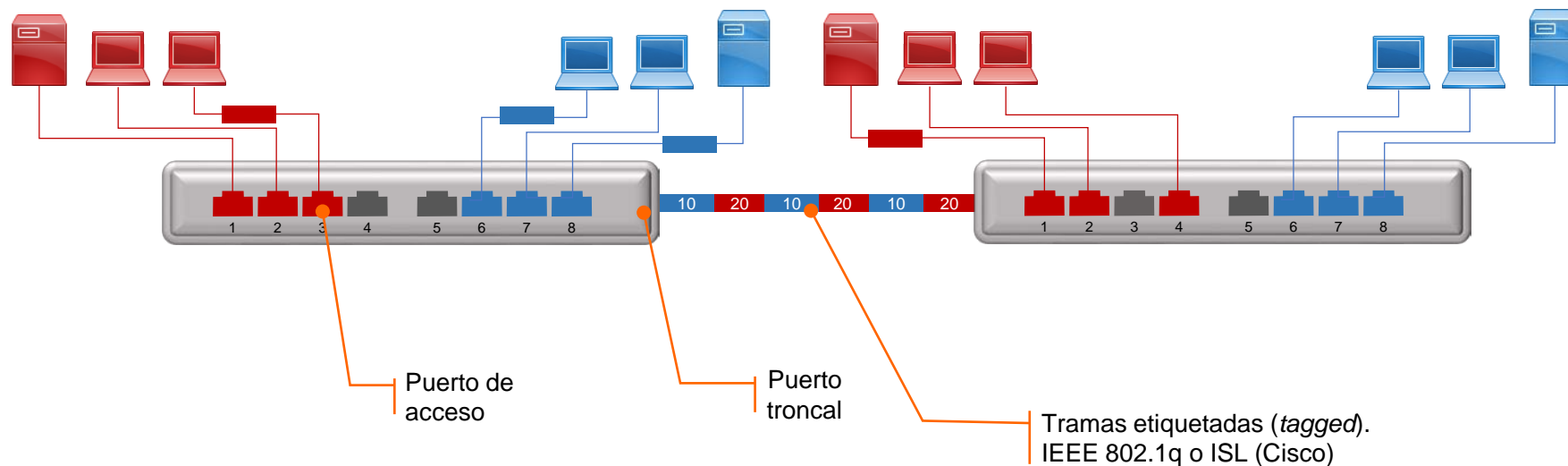
# Ventajas de las VLAN



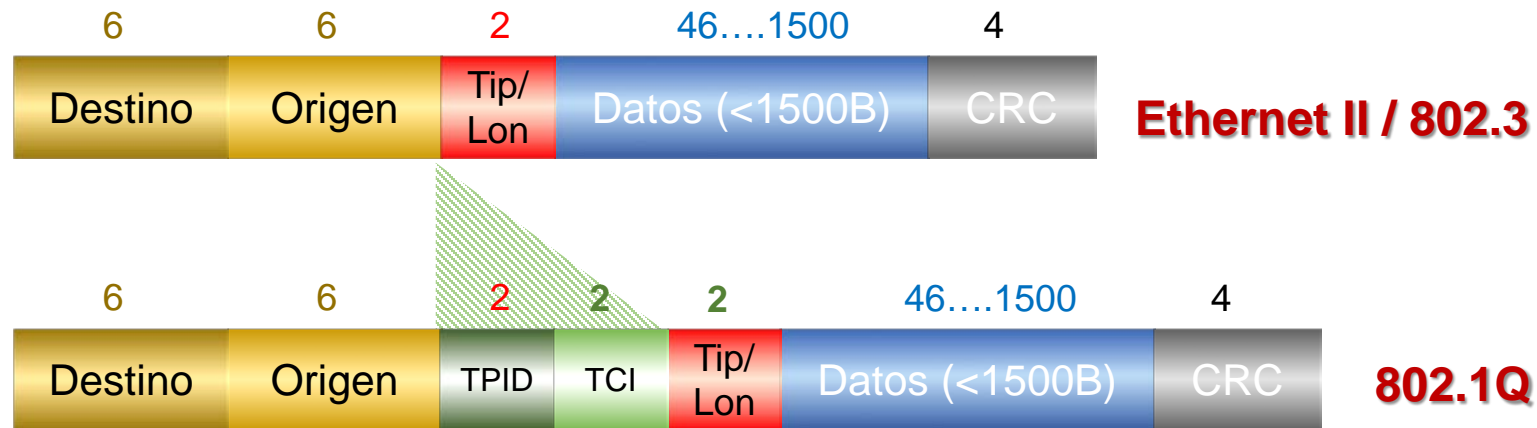


# Concepto de puerto *trunk* y puerto de acceso

- Un **puerto *trunk*** (puerto de enlace troncal) es un puerto capaz de transportar tráfico para varias o todas las VLAN accesibles por un conmutador en particular.
- En cambio, un **puerto de acceso**, es aquél que lleva sólo el tráfico hacia y desde la VLAN específica asignada al mismo.
- El puerto troncal marca las tramas con etiquetas especiales que las identifican (ya sean etiquetas ISL o etiquetas 802.1Q). Por el contrario, un puerto de acceso no proporciona tales etiquetas, porque son innecesarias.



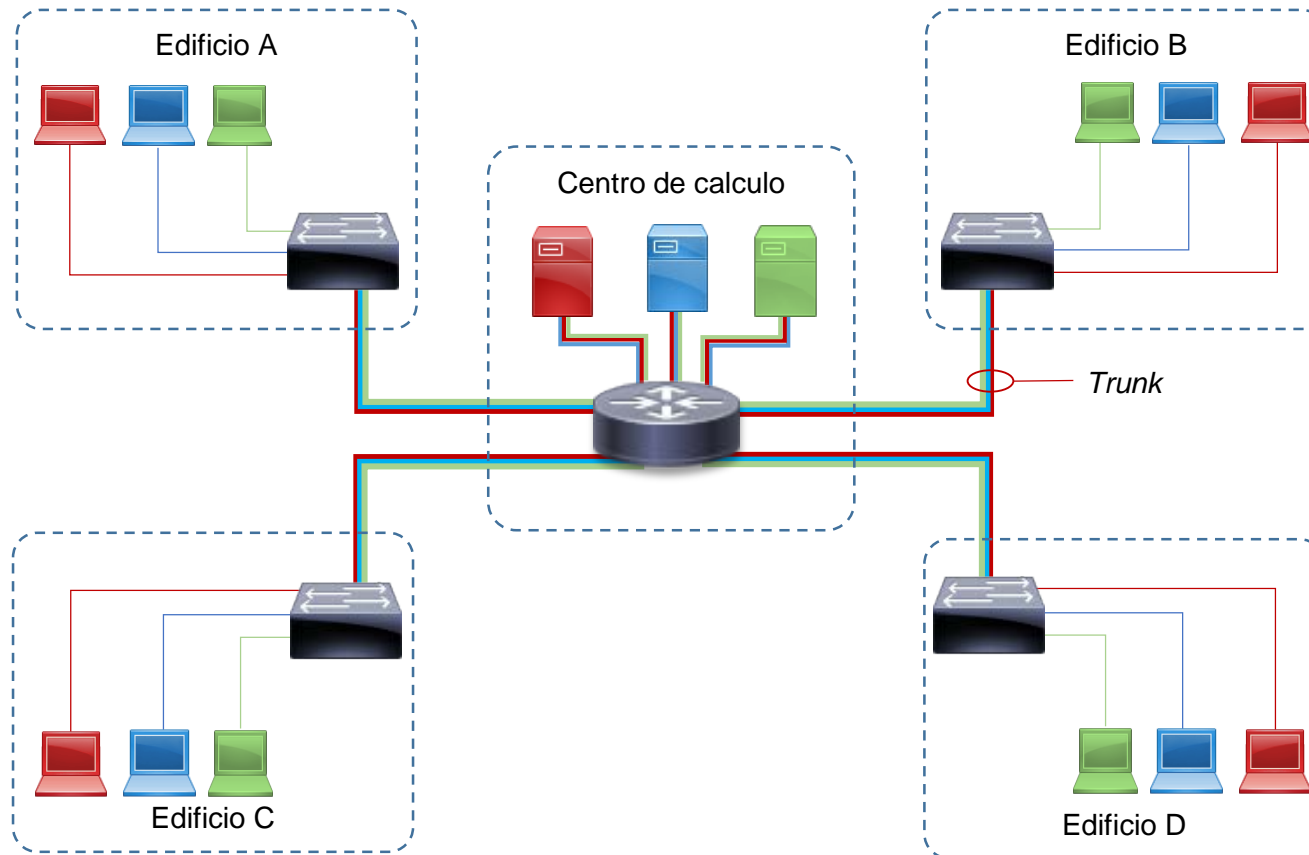
# Modificación de la trama MAC para las VLANs



- Tag Identificador de protocolo (TPID): es un campo de 2 octetos con un valor igual a 0x8100 con el fin de identificar una trama IEEE 802.1Q.
- Información de control del Tag (TCI): Contiene el Punto de código de prioridad (PCP): un campo de 3 bits que se refiere a la prioridad. El CFI (*Canonical Format Indicator*) que indica el formato de direcciones MAC. Finalmente, el Identificador de VLAN (VID), 12 bits

# Caso de estudio de VLANs

## Red de campus



VLAN Alumnos

VLAN investigación

VLAN administración



Switch-router



Commutador N2

# Redes de área local

## Pros y contras



### Coste

Fácil configuración y ampliación del sistema

Velocidad

Compartición de recursos costosos

Multifabricante.



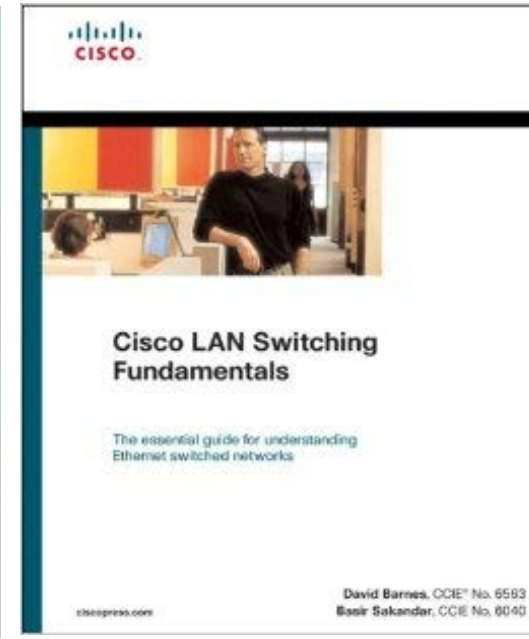
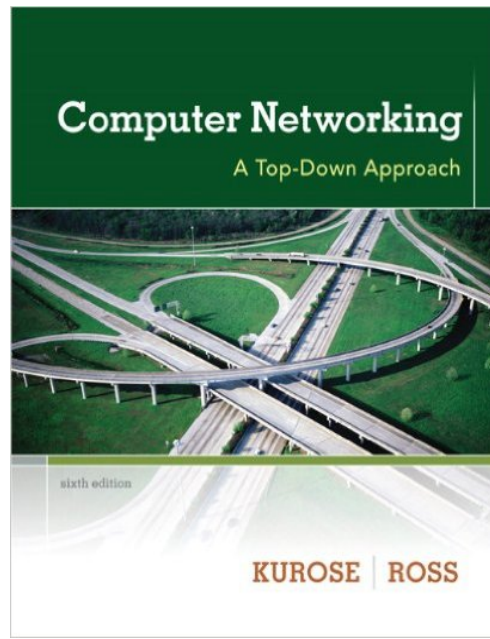
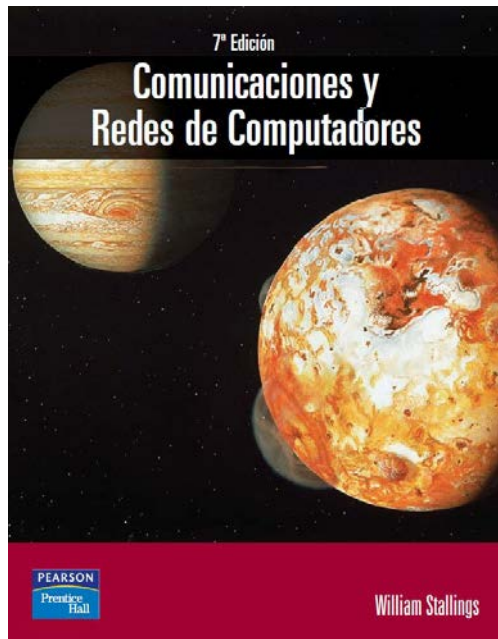
### QoS

Limitación geográfica

Integridad y seguridad de los datos distribuidos

Dificultad de administración y gestión remota de equipos(\*).

# Referencias



- [1] William Stallings: *Comunicaciones y Redes de Computadores*. (7ª ed 2004). Prentice Hall
- [2] J Kurose & K Ross: *Computer Networking a Top Down Approach* (6ª ed 2013)
- [3] David Barnes & Basir Sakandar: *Cisco LAN Switching Fundamentals* (1ª ed 2005). Cisco Press

# *TEMA 2. PARTE II*

## *LANs INALÁMBRICAS*





# Contenido del Tema 2. Parte II: LANs inalámbricas



1. Generalidades de las LANs inalámbricas
2. El protocolo de acceso al medio CSMA/CA
3. El estándar IEEE 802.11
4. La capa física
5. Casos de estudio
6. Referencias



# 1. Generalidades de LANs inalámbricas

Concepto de WLAN

Sistemas de transmisión inalámbricos

Modos de operación

Arquitectura de IEEE 802.11

Componentes de las WLANs

Evolución de la estandarización WLAN

IEEE 802.11 y Wi-Fi™

# Concepto de WLAN

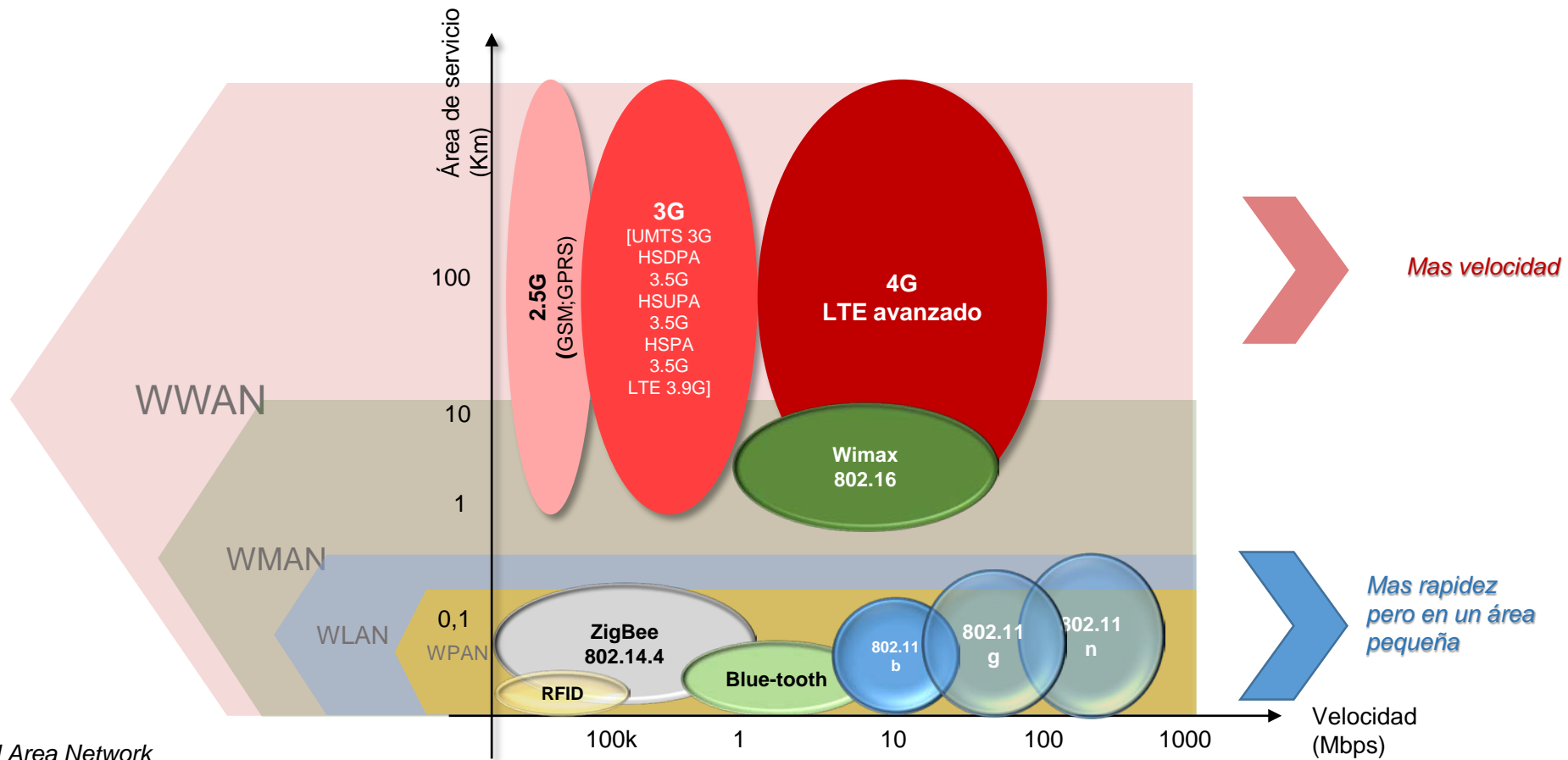


- Una red de área local inalámbrica ( WLAN ) es una [red informática inalámbrica](#) que conecta dos o más dispositivos utilizando un mecanismo inalámbrico de comunicaciones, dentro de un [área limitada](#), como una casa, una escuela, un laboratorio de computación, o un edificio de oficinas.
- La mayoría de las WLAN modernas están basadas en estándar [IEEE 802.11](#) y se comercializan bajo la marca [Wi-Fi](#).



# Sistemas de transmisión inalámbricos

## Evolución



WPAN: Wireless Personal Area Network  
 RFID: Radio Frequency IDentification  
 LTE: Long Term Evolution

# WLAN

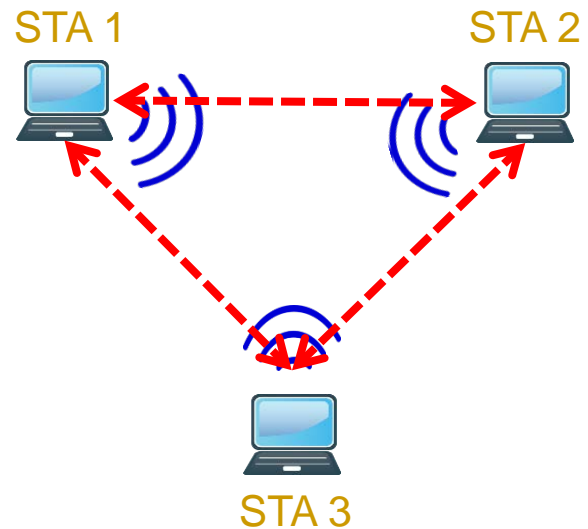
## Modos de operación



### Modo ad hoc

Conjunto de estaciones que comunican entre sí.

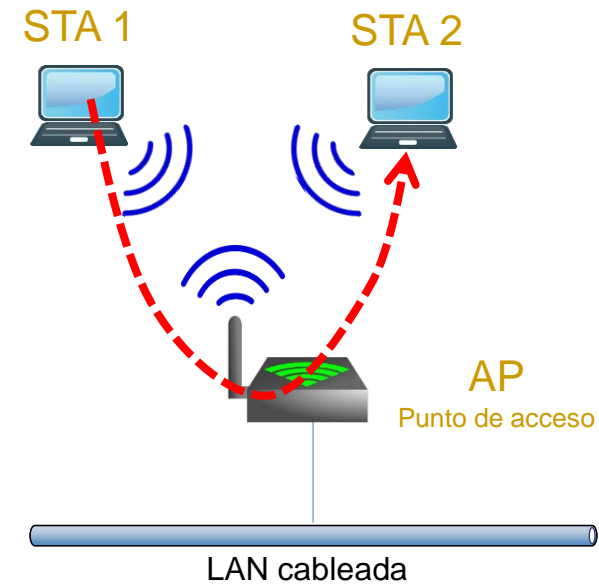
**Topología mallada**



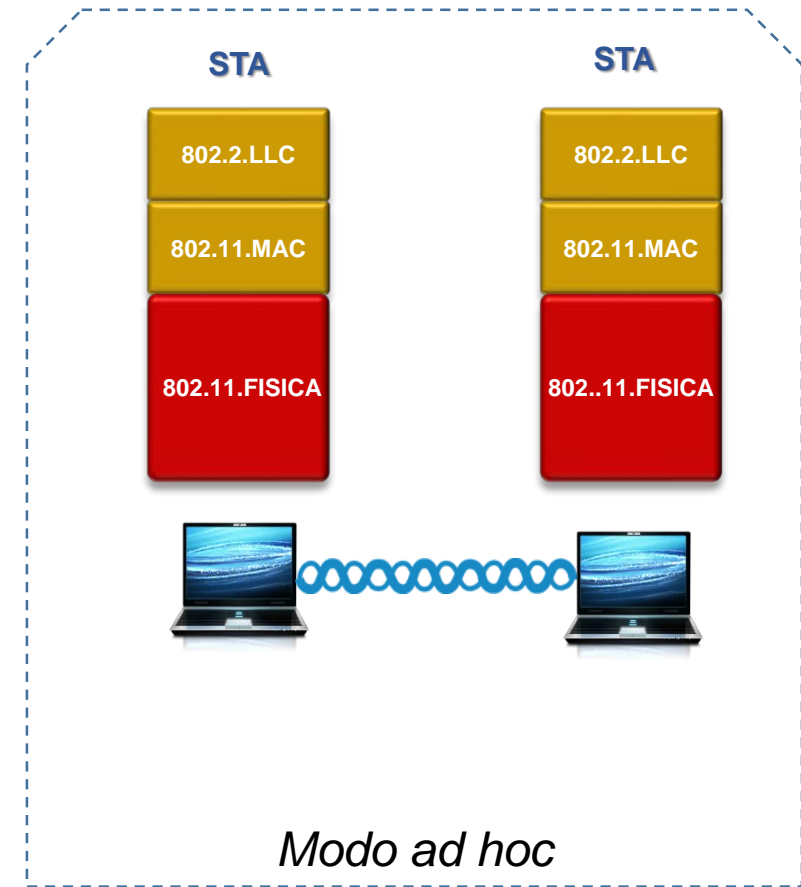
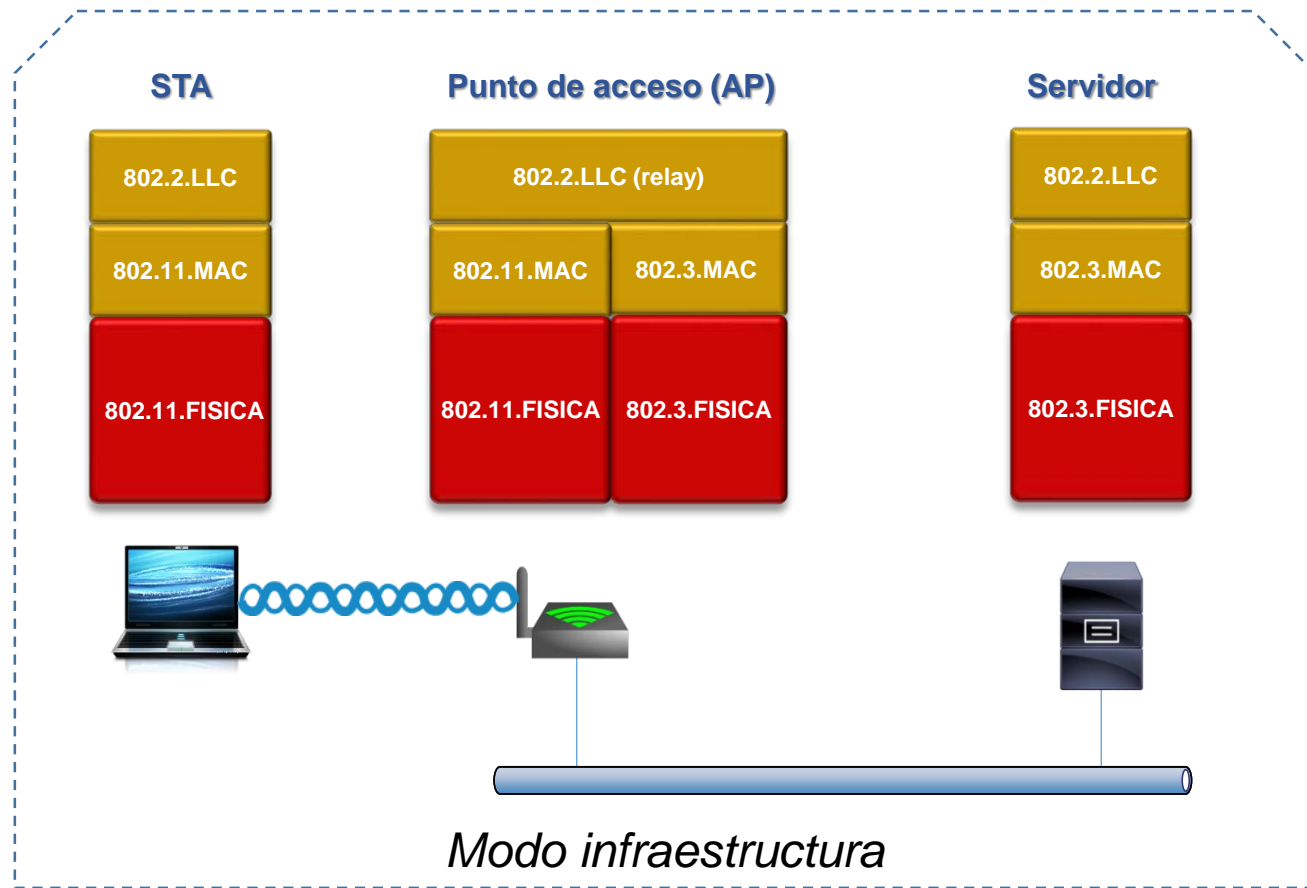
### Modo infraestructura

Una estación actúa como *hub* (AP)

**Topología en estrella**



# Arquitectura de IEEE 802.11





# Componentes de las WLAN

## Modo infraestructura



### STA (Station)

Cualquier equipo capaz de conectar inalámbricamente con un AP

### AP (Access point)

Estación que da conexión inalámbrica a las STAs asociadas.

### BSS (Basic service set)

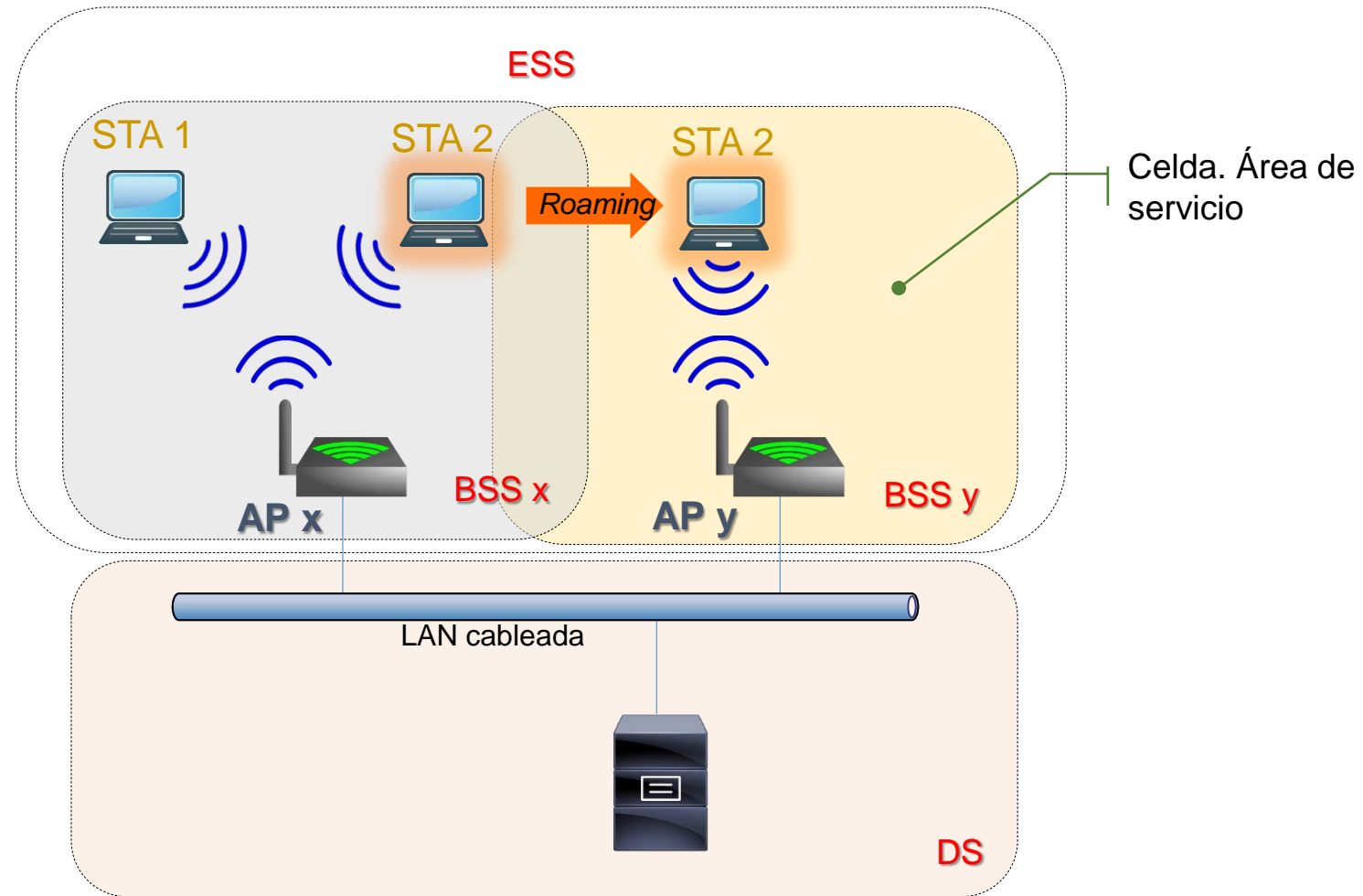
Es el conjunto de un AP con sus STAs asociados

### ESS (Extended service set)

Un ESS es un conjunto de 2 o más BSS integrados formando un único segmento de red lógico. Cada ESS está identificado por un SSID

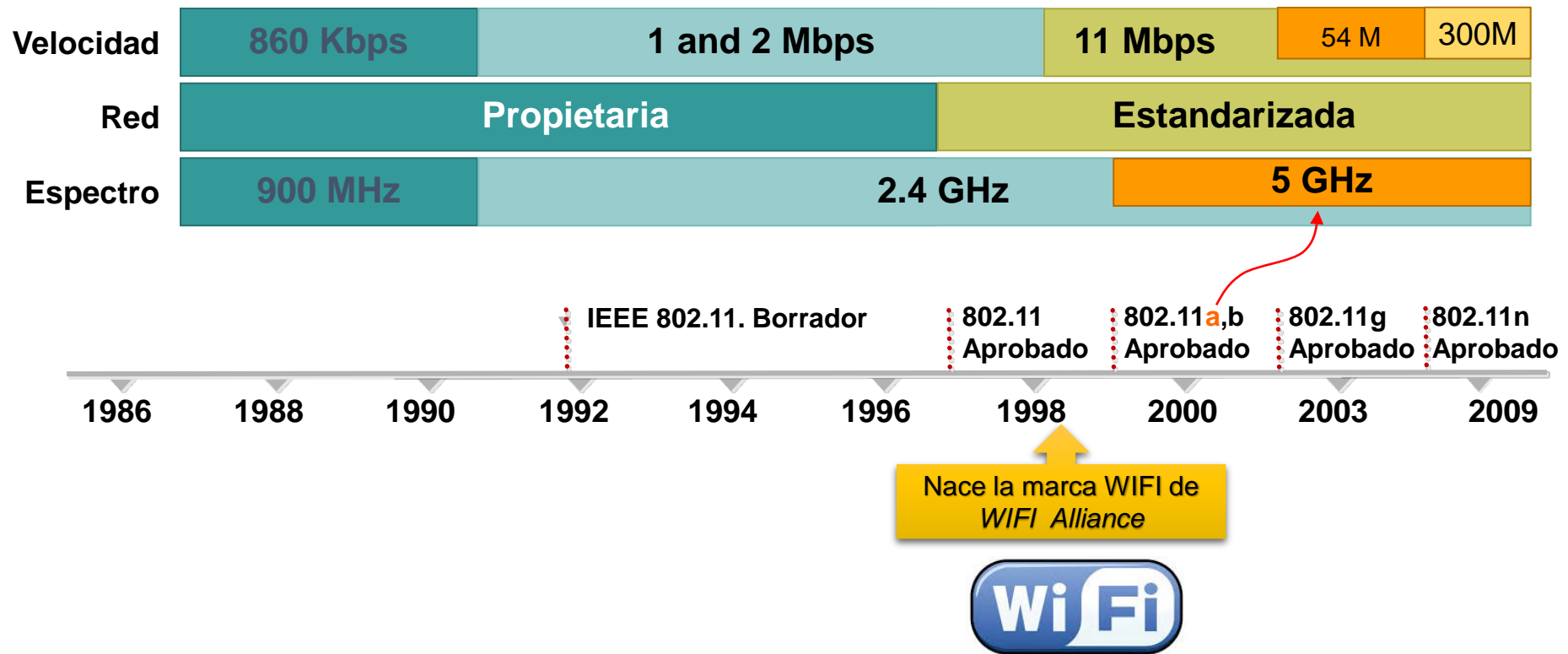
### DS (Distribution system)

Es el sistema que interconecta BSS



SSID (service set identifier)

# Evolución de la estandarización WLAN



# IEEE 802.11 y Wi-Fi™



## ■ Wi-Fi™ Alliance

- Wi-Fi es una marca comercial basada en el estándar IEEE 802.11
- La WECA (*Wireless Ethernet Compatibility Alliance*) nace en 1999 para la explotación commercial de la marca Wi-Fi
  - ✓ En 1999 cambió su nombre a *Wireless Fidelity Alliance*
- Está formada por +170 miembros (Lucent, Harris, Cisco, etc.)
- 350 productos certificados, aproximadamente

## ■ Misión

- Certificar la interoperabilidad de productos WLAN (802.11)
- Proporcionar un sello de aprobación
- Promover Wi-Fi™ como un estandar global





## 2. El protocolo de acceso al medio CSMA/CA

Modos de acceso al medio con CSMA/CA

Modo distribuido. Acceso básico

Modo distribuido. Acceso con RTS/CTS

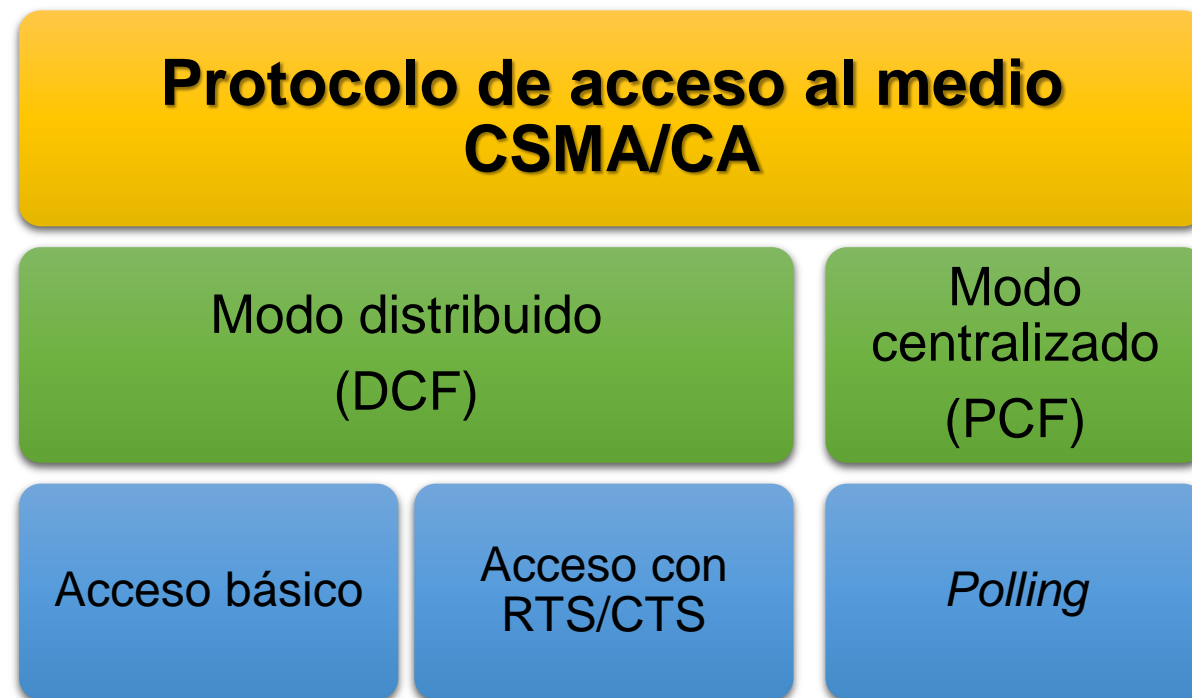
El problema de la estación oculta

Modo centralizado

Alternancia DCF y PCF

# Modos de acceso al medio con CSMA/CA

- En la arquitectura IEEE 802.11 el protocolo de acceso al medio es **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*) o también: **acceso múltiple con escucha de portadora y evasión de colisiones**.
  - CSMA/CA es una adaptación del protocolo CSMA/CD.

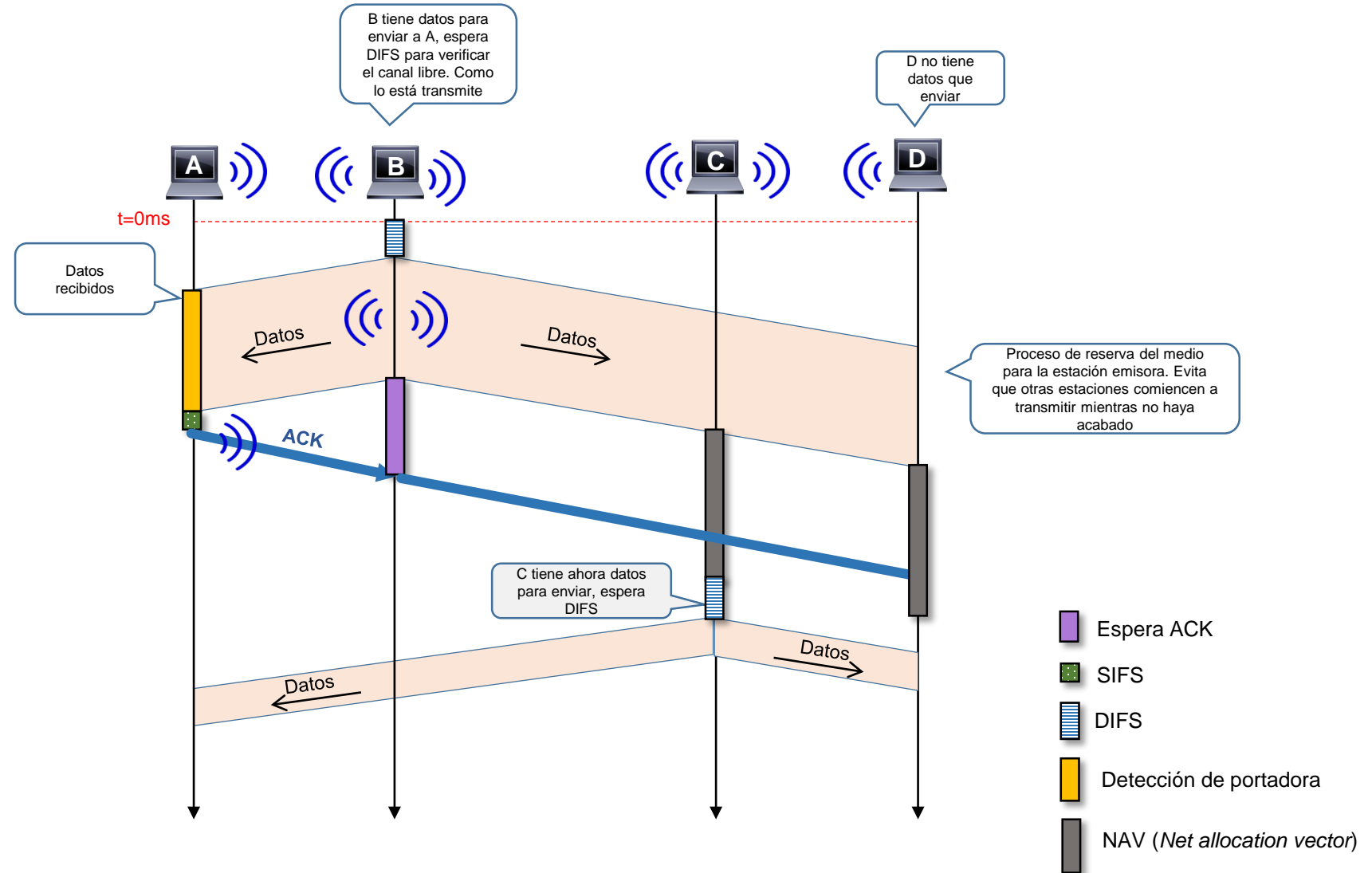




# El protocolo de acceso al medio CSMA/CA

## Modo distribuido (DCF). Acceso básico [1]

La estación que desea transmitir (B), debe escuchar el canal un determinado tiempo conocido como **DIFS** (*DCF Interframe Space*) para verificar que el canal esté libre. Si tras concluir DIFS sigue libre, transmite



SIFS (*Short Interframe Space*) = 10  $\mu s$  (para 802.11b)

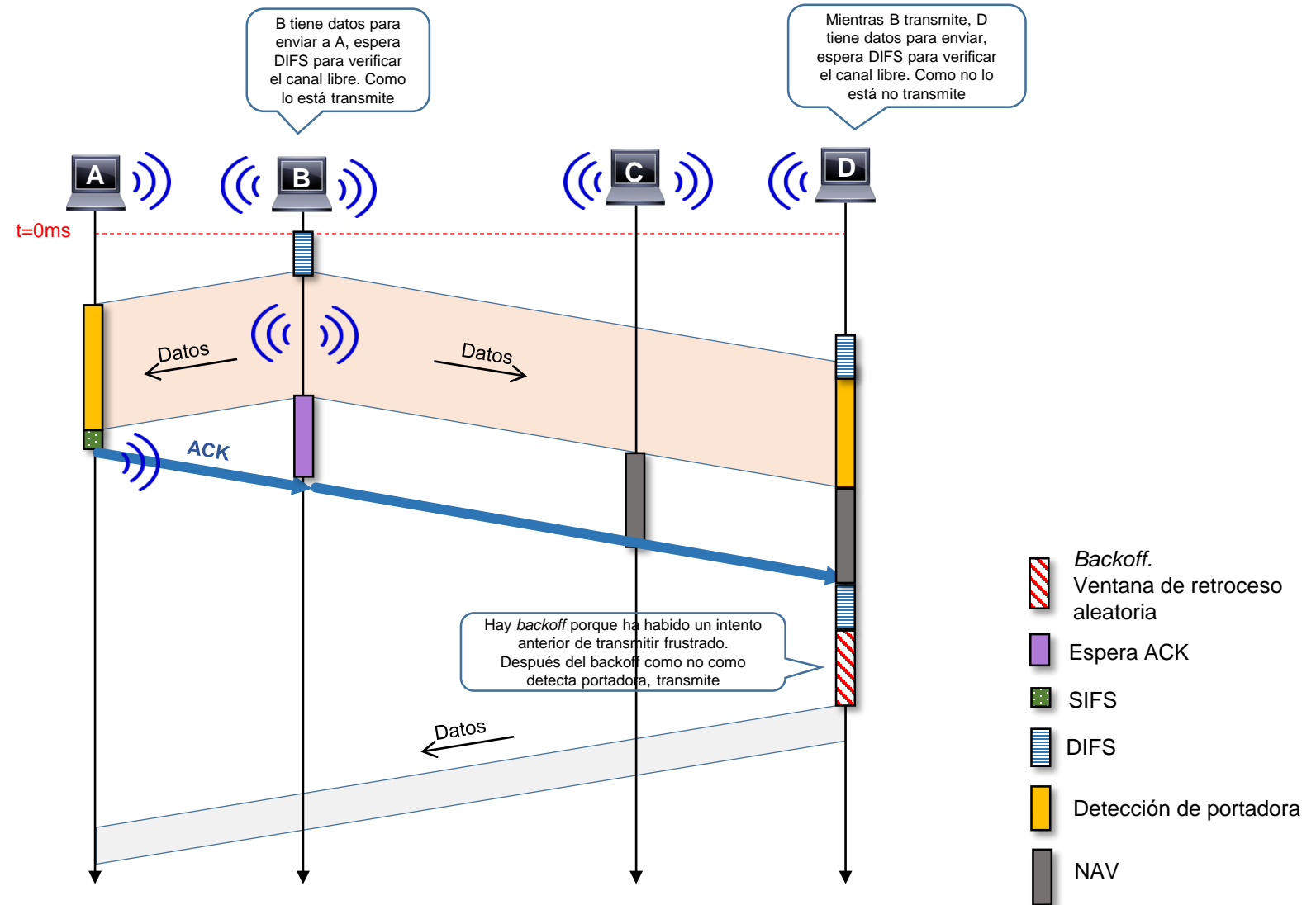
DIFS (*DCF Interframe Space*) = 50  $\mu s$  (para 802.11b)



# El protocolo de acceso al medio CSMA/CA

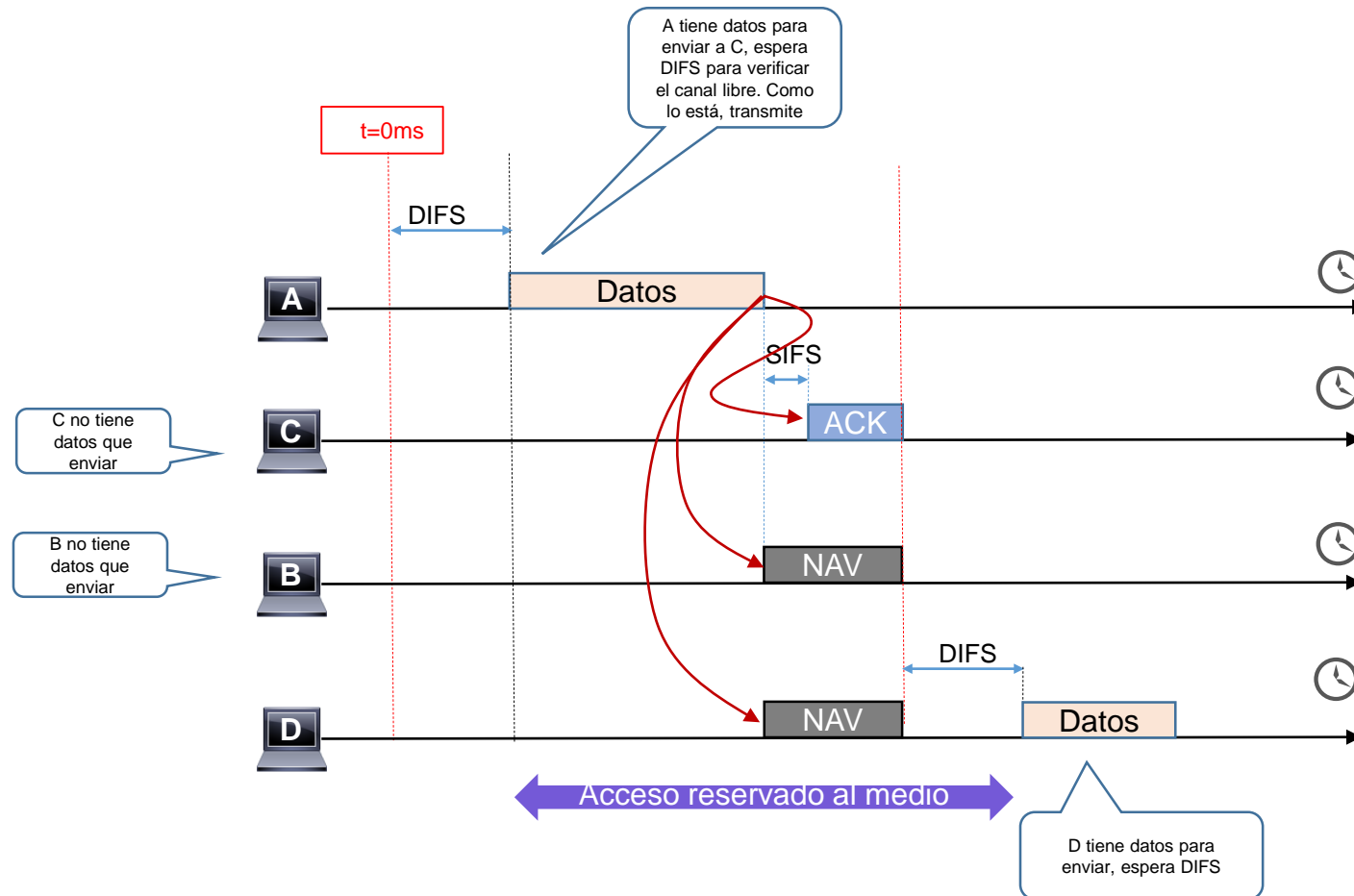
## Modo distribuido (DCF). Acceso básico [2]

- La estación que desea transmitir (D), tras esperar DIFS encuentra el medio ocupado (por STA B), entonces aplaza la transmisión y continúa escuchando hasta que la transmisión finaliza.
- Transcurrida la transmisión STA D espera otro DIFS, si el medio se encuentra libre realiza un retroceso exponencial binario y sondea el medio de nuevo; si está libre, transmite



# El protocolo de acceso al medio CSMA/CA

## Modo distribuido (DCF). Acceso básico [3]

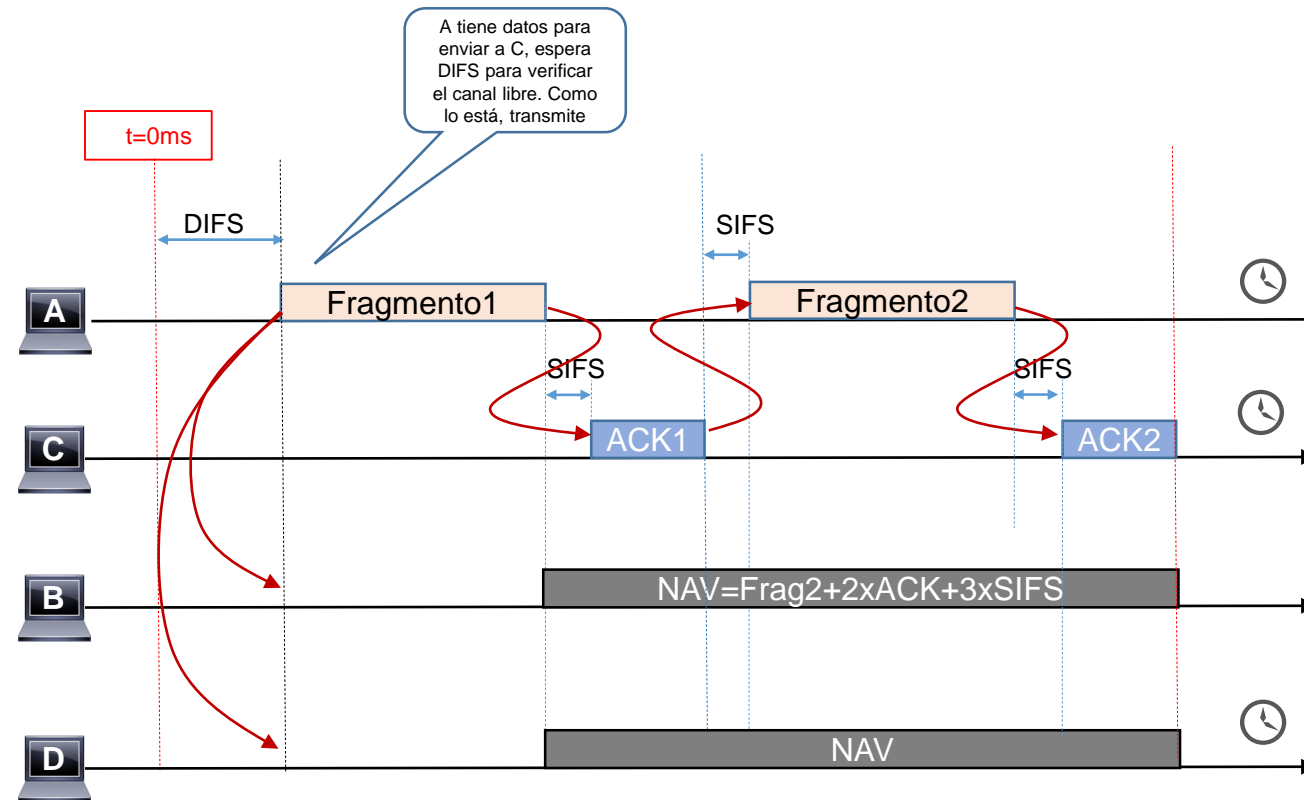


NAV: net allocation vector

# El protocolo de acceso al medio CSMA/CA

## Modo distribuido (DCF). Acceso básico [3]. Fragmentación

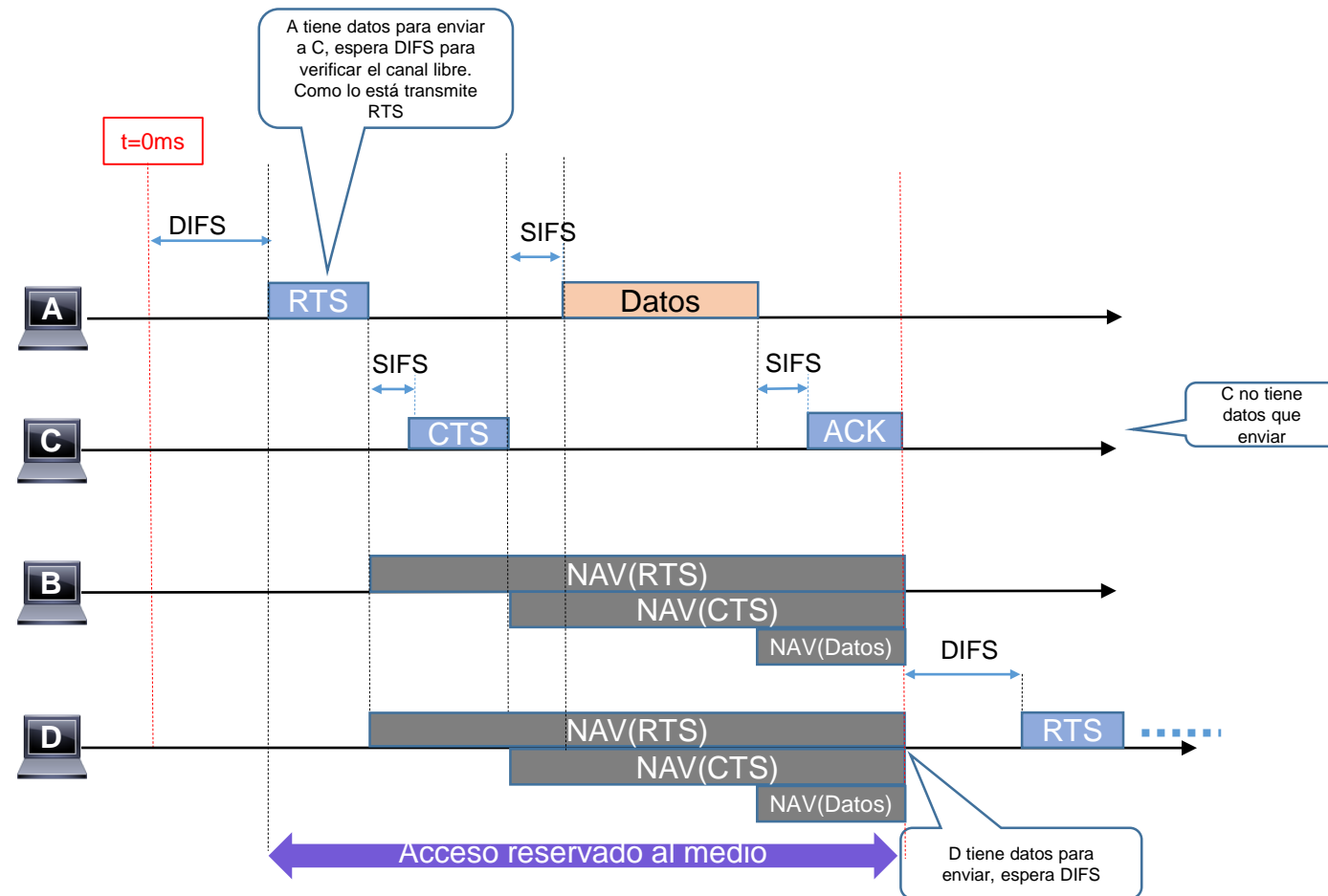
- El proceso de fragmentación divide las MSDU (MAC Service Data Units) en unidades más pequeñas para lograr MPDUs que tengan menos probabilidades de alteración durante la transmisión y así aumentar la confiabilidad de la red inalámbrica, ya que, a menudo, suele tener un nivel muy alto de interferencias



# El protocolo de acceso al medio CSMA/CA

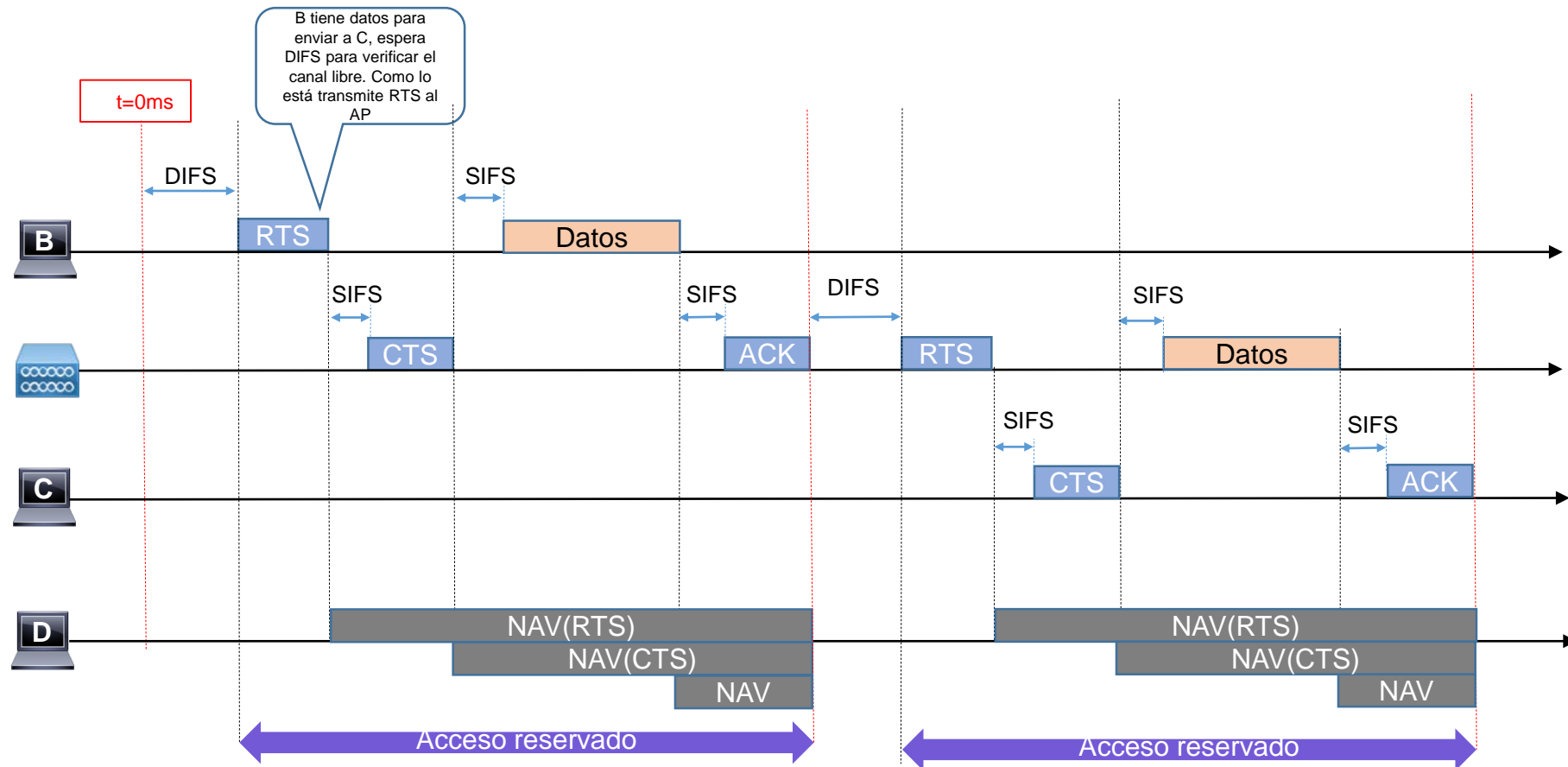
## Modo distribuido (DCF). Acceso con RTS/CTS

- El acceso RTS/CTS no es aleatorio (está libre de contienda) sino determinado
- El uso de RTS/CTS (es opcional y configurable) y se usa para transmitir muchos datos y evitar las colisiones
- El emisor antes de enviar los datos envía un RTS al receptor. El receptor responde con CTS (si está listo). Tras recibir CTS el emisor manda los datos.
  - Todas las estaciones que reciben RTS/CTS programan una espera (NAV) basada en la duración de las tramas de control



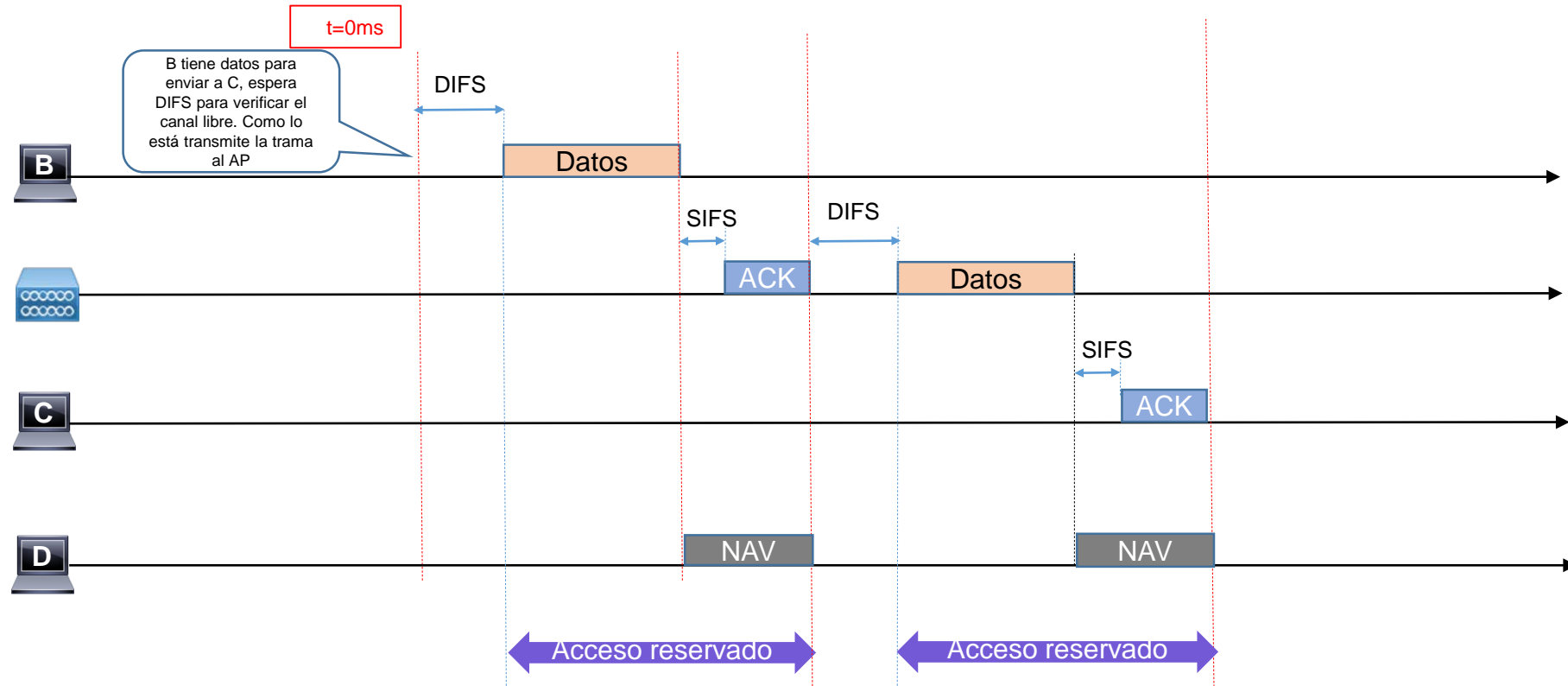
# El protocolo de acceso al medio CSMA/CA

## Modo distribuido (DCF). Acceso con RTS/CTS y AP



# El protocolo de acceso al medio CSMA/CA

## Modo distribuido. Acceso sin RTS/CTS y con AP





# Acceso distribuido básico vs RTS/CTS

Cuando el tamaño del paquete a enviar es mayor que un valor predeterminado (*threshold*) se activa automáticamente el modo RTS/CTS

DCF  
Acceso básico

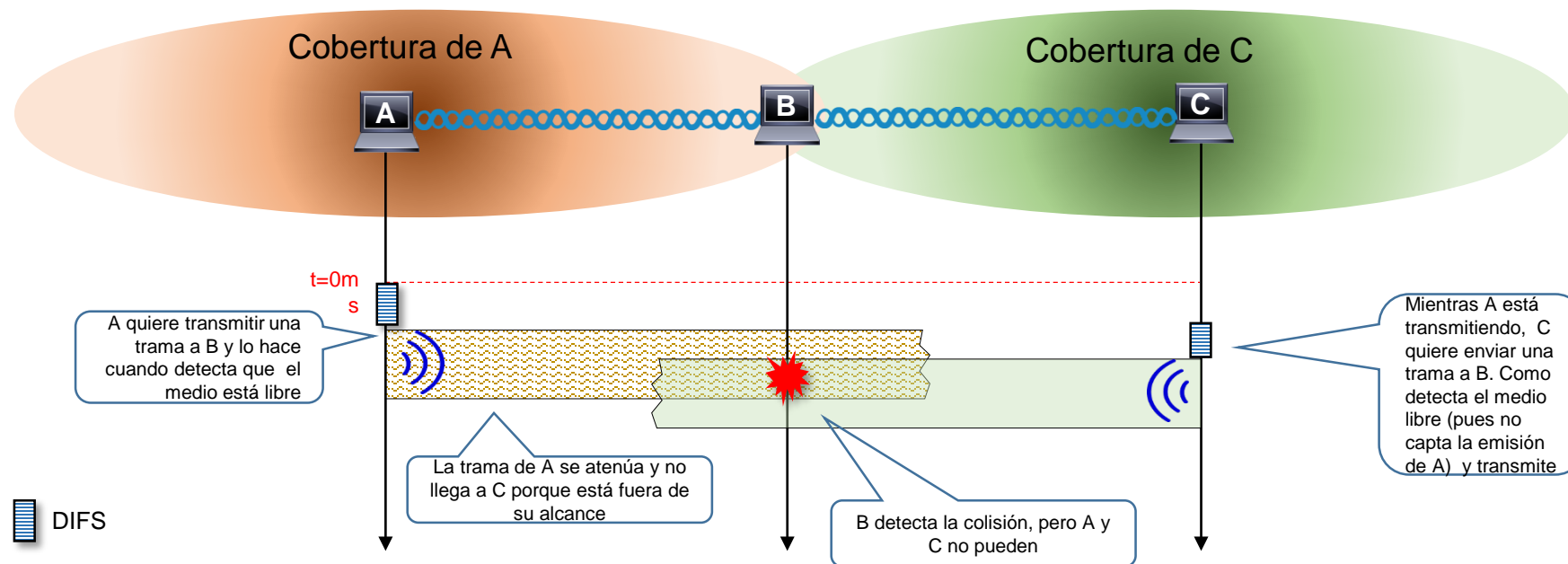
- Usado para tramas pequeñas de datos
- Problema del terminal oculto
- Inapropiado con muchas STAs

DCF  
Acceso  
RTS/CTS

- Para tramas de datos grandes
- Evita colisiones
- Resuelve el problema del terminal oculto
- Pero introduce sobrecarga (*overhead*)

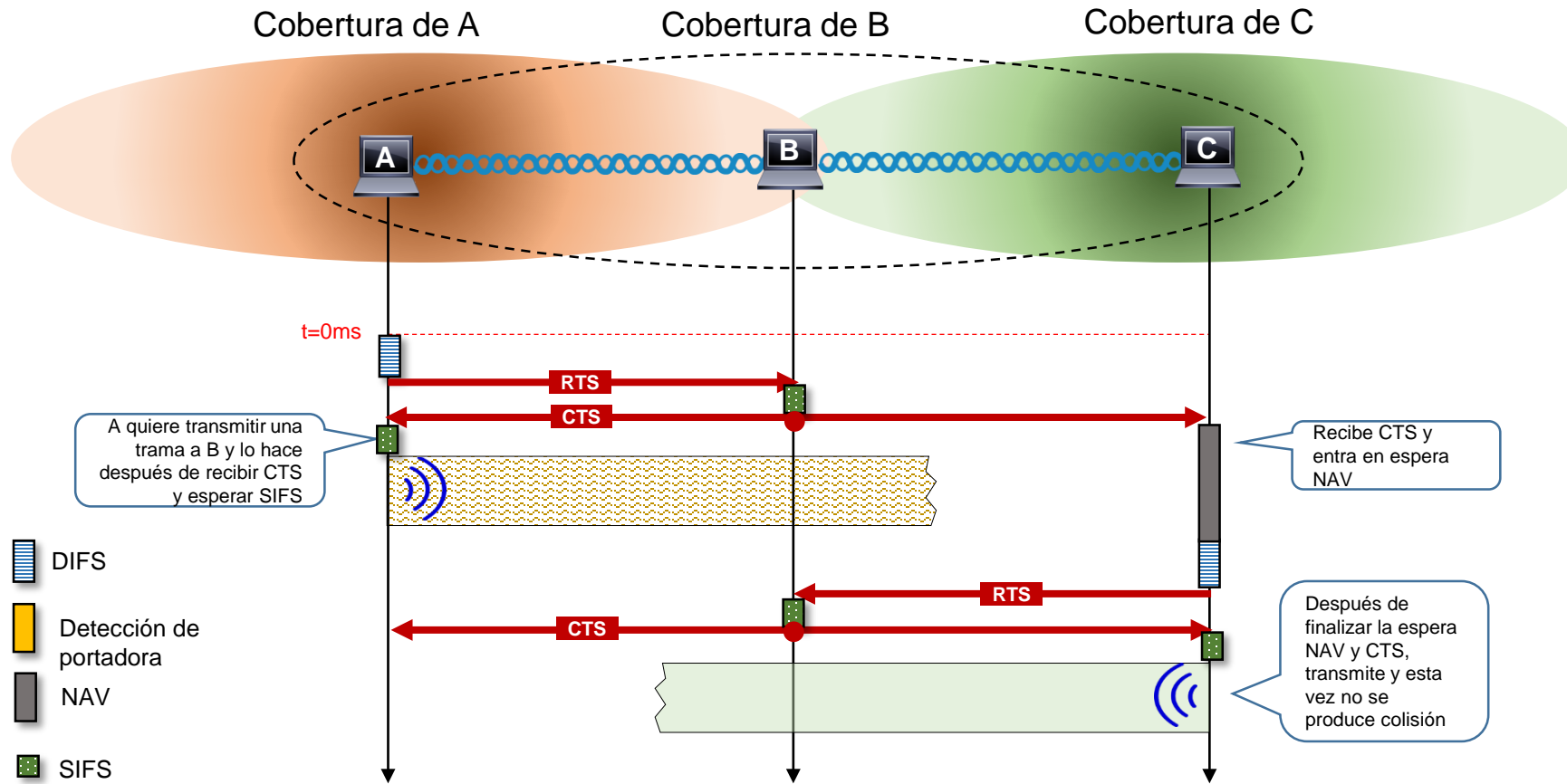
# El problema de la estación oculta

- El problema de la estación oculta consiste en que una estación (C) cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo (A) al que la estación no "escucha".



# El problema de la estación oculta

## Solución





# 3. El estándar IEEE 802.11

IEEE 802.11 vs. 802.3

La capa MAC

Tipos de tramas MAC

La trama baliza

Conexión a una WLAN

Formatos de las tramas MAC

La cabecera SNAP

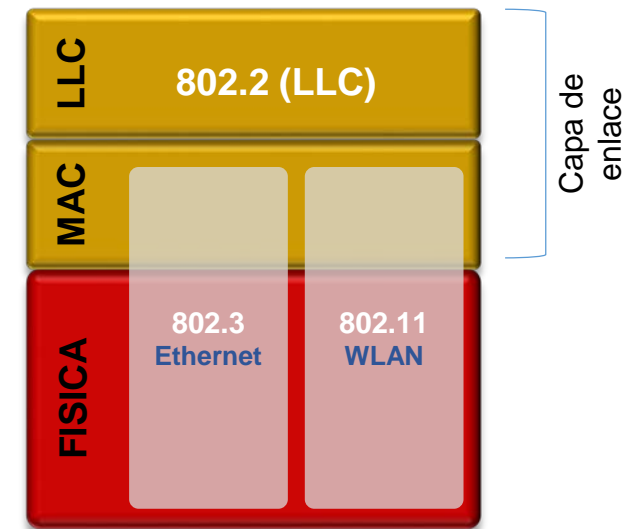
Encapsulación

# IEEE 802.11 vs. 802.3



- El estándar IEEE 802.11 es una parte de la arquitectura 802.x
  - Fue aprobado por el IEEE en el año 1997
- Su definición tiene como objetivo sustituir a las capas física y MAC del modelo IEEE 802.3 para adaptarlas al medio inalámbrico

## ARQUITECTURA 802.X

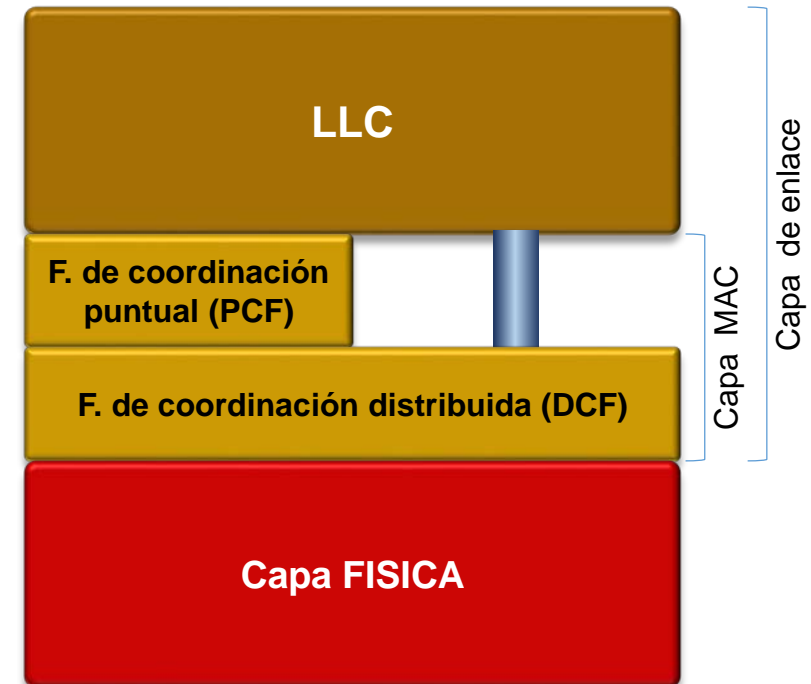


# IEEE 802.11

## La capa MAC



- La capa básica 802.11 MAC utiliza la **función de coordinación distribuida (DCF)** o la **función de coordinación puntual (PCF)** para el acceso al medio de las STAs
- La **función de coordinación distribuida (DCF)** está disponible en modo *ad hoc* y en modo infraestructura (**servicio con contención**).
  - Determina cuando una STA puede transmitir o recibir datos. No requiere AP
  - Se basa en **CSMA/CA** y opcionalmente en **802.11 RTS/CTS**
- La **función de coordinación puntual (PCF)** está disponible sólo en el modo "infraestructura" (**Servicio sin contención**)
  - Requiere la presencia de un AP que actúe como Nodo Coordinador (*Point Coordinator, PC*) para conseguir un servicio sin contención. En consecuencia tan sólo puede ser utilizada en redes con infraestructura
  - El AP debe decidir que estación, de entre todas las que forman la red, debe transmitir.
  - Proporciona QoS





# IEEE 802.11

## Tipos de tramas MAC



### ■ Datos

- Transportan datos de capas superiores.
- Diferentes tipos dependiendo de su función y tipo de servicio
  - ✓ Data, Data+CF-ACK, Data+CF-Poll, CF-ACK, CF-Poll, etc

### ■ Control

- Administran el acceso al medio y proporcionan fiabilidad MAC
  - ✓ RTS, CTS, ACK

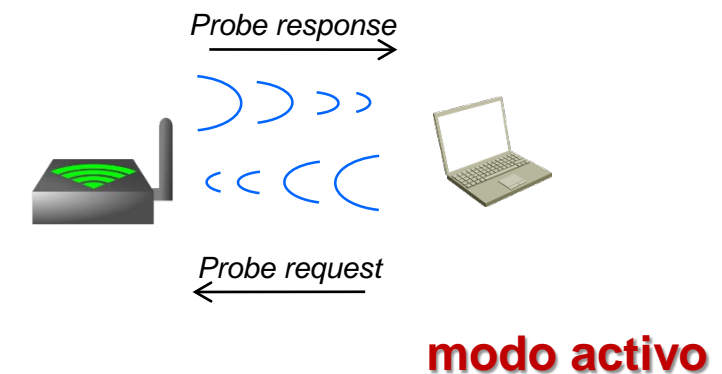
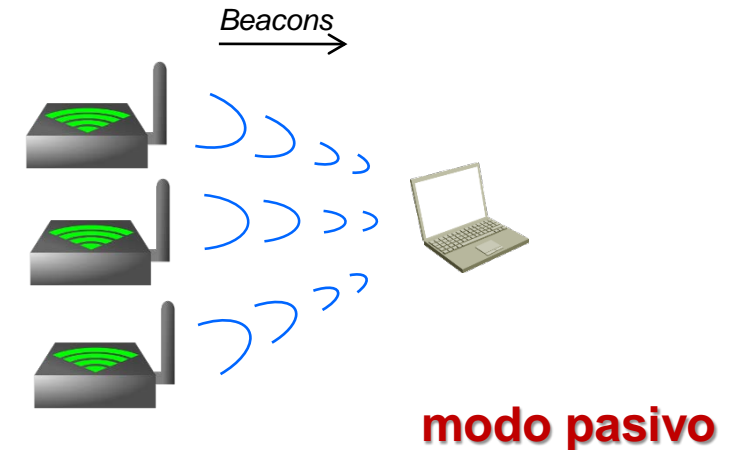
### ■ Gestión

- Proporcionan servicios específicos de las redes inalámbricas e inmediatos en las cableadas
  - ✓ Trama baliza (*beacon*)
  - ✓ Tramas de sonda petición/respuesta (*probe*)
  - ✓ Tramas de autenticación/de-autenticación
  - ✓ Tramas de asociación/ re-asociación/ des-asociación

# La trama baliza (*Beacon*)

- La trama *Beacon* es un tipo de trama de gestión emitida por los APs con destino *broadcast* que publica el **SSID** de la red a la que pertenece.
  - Típicamente se envían 10 veces por segundo
  - Un AP puede configurarse para que no envíe *beacons*, o para que los envíe ocultando su SSID.
  - Además del SSID, contiene información de las velocidades admitidas, autenticación, marca de tiempo para actualizar el reloj y otras datos.
- La STA puede disponerse para escuchar los *beacons* emitidos periódicamente (**modo pasivo**), o bien puede enviar un mensaje *probe request* sucesivamente por cada canal hasta que obtiene una trama de respuesta *probe response* que contiene el SSID esperado de un AP (**modo activo**).

El **SSID** (*Service set identification*) es un identificador (32 caracteres) que diferencia a una WLAN de otra, adjunto a la cabecera de los paquetes enviados por el medio, que el receptor utiliza para filtrar las señales recibidas y localizar las que quiere escuchar

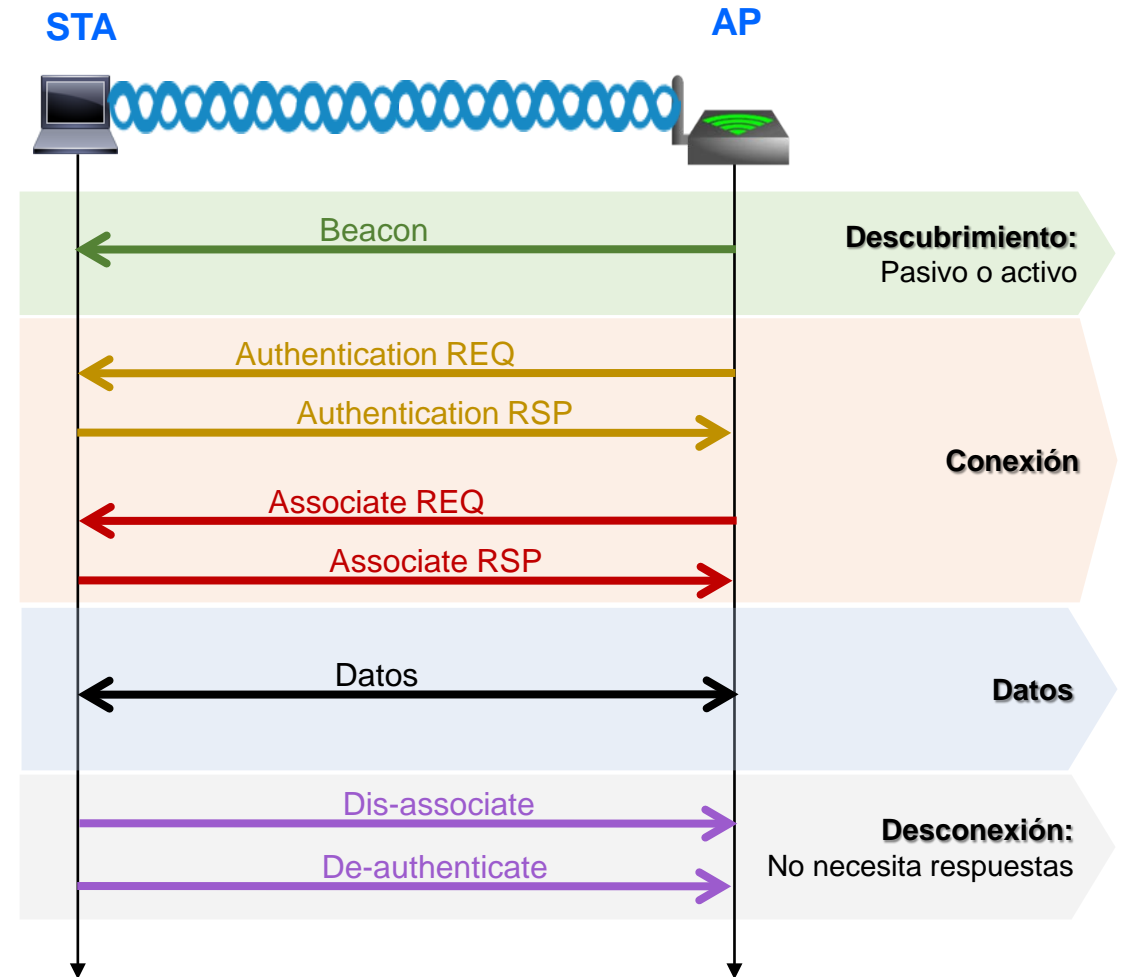


# Conexión a una WLAN

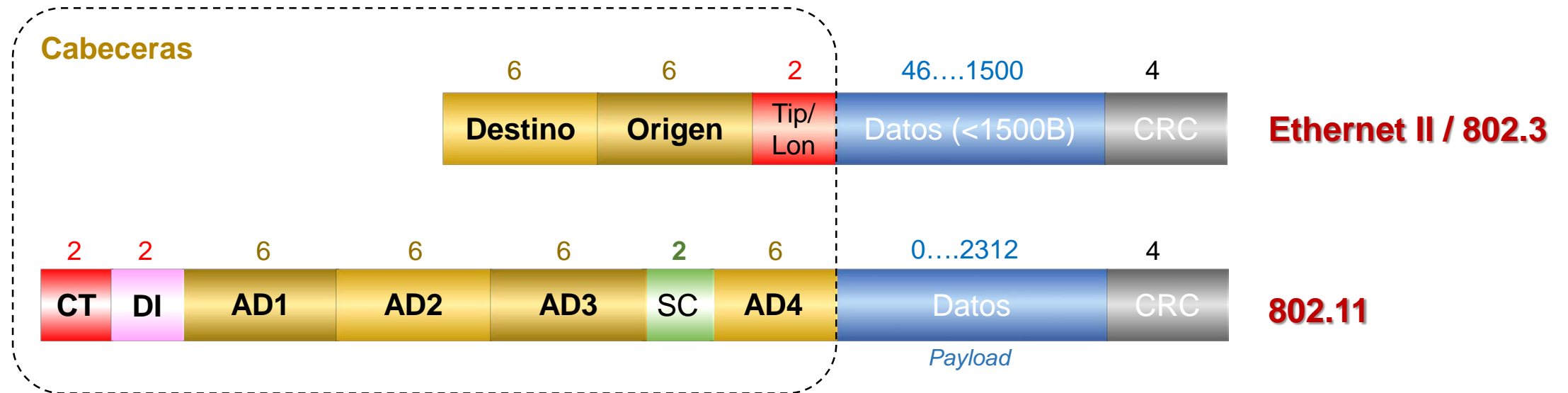


■ El proceso de conexión a una red 802.11 se llama “**asociación**” y equivale a conectarse por cable a un switch en una red Ethernet

- Como una WLAN esta expuesta a ataques se debe utilizar algún protocolo de protección, como WEP, WPA, etc.
- Cuando se utiliza protección, la red (el AP) obliga a las estaciones a autenticarse antes de asociarlas



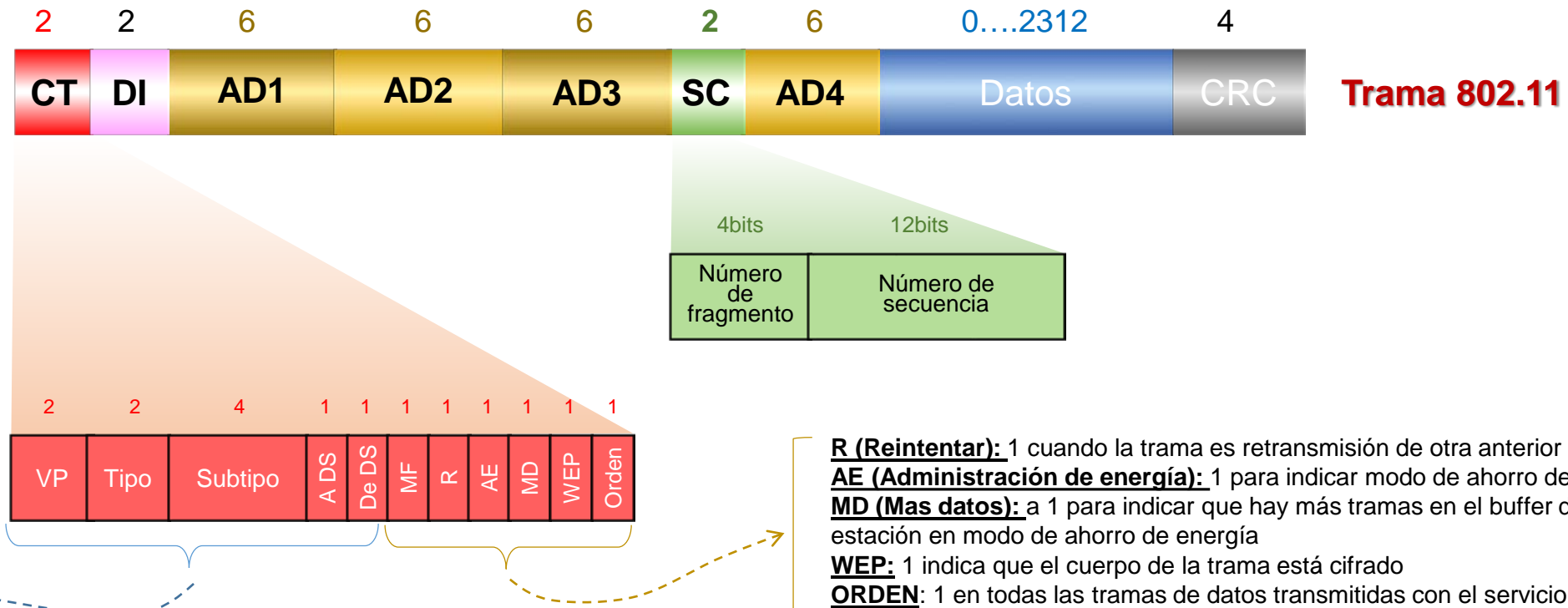
# La trama MAC IEEE 802.11 vs. trama IEEE 802.3



- **CT:** Control Trama.
- **AD1 – AD4:** Direcciones 1 a 4
  - Se utilizan para indicar el **Basic Service Set Identifier** (BSSID), el **Destination Address** (DA), el **Source Address** (SA), el **Receiver Address** (RA) y el **Transmitter Address** (TA). Si no hay DS (desde STA a STA): **AD1= DA, AD2 = SA, AD3 = BSSID, AD4 = NA**. El BSSID es un nombre de identificación único de todos los paquetes de una red inalámbrica pertenecientes a un determinado BSS.
  - Las asignación anterior cambia si el envío es de AP a STA, de STA a AP o de AP a AP
- **DI:** *Duration/ Identifier*. (Duración/ Identificador)
  - Indica durante cuantos microsegundos estará ocupado el canal por la transmisión de esta trama. El identificador se refiere a una etiqueta de la asociación de la STA
- **SC:** *Sequence Control* (Control de Secuencia)
- **Datos:** PDU, trama del nivel superior (LLC)

# IEEE 802.11

## Formato de las tramas MAC de datos



**VP** (versión de protocolo): versión actual del protocolo 802.11 utilizado

**Tipo** (datos, control o gestión)

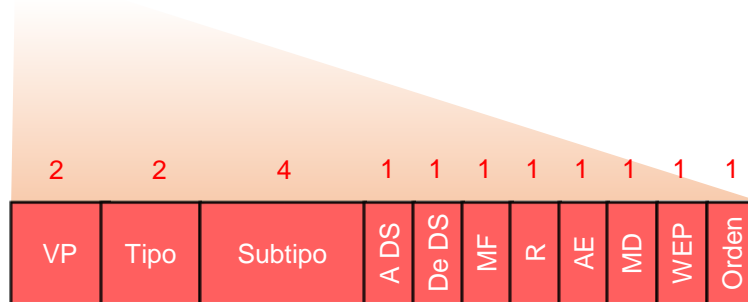
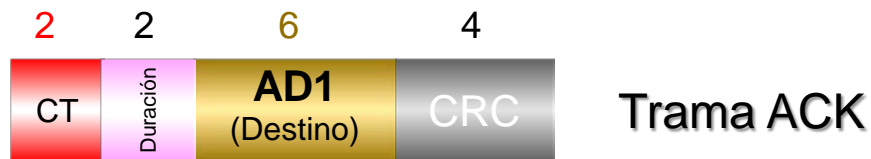
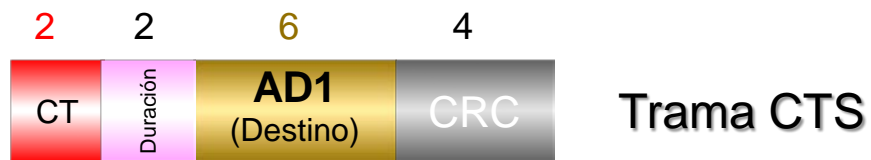
**Subtipos** (por ejemplo, RTS o CTS)

**A DS:** se establece en 1 para las tramas de datos destinadas al sistema de distribución

**Desde DS:** se establece en 1 para las tramas de datos que salen del sistema de distribución

# IEEE 802.11

## Formato de las tramas MAC de control



### Tipo/Subtipo

00/0000 = Association Request

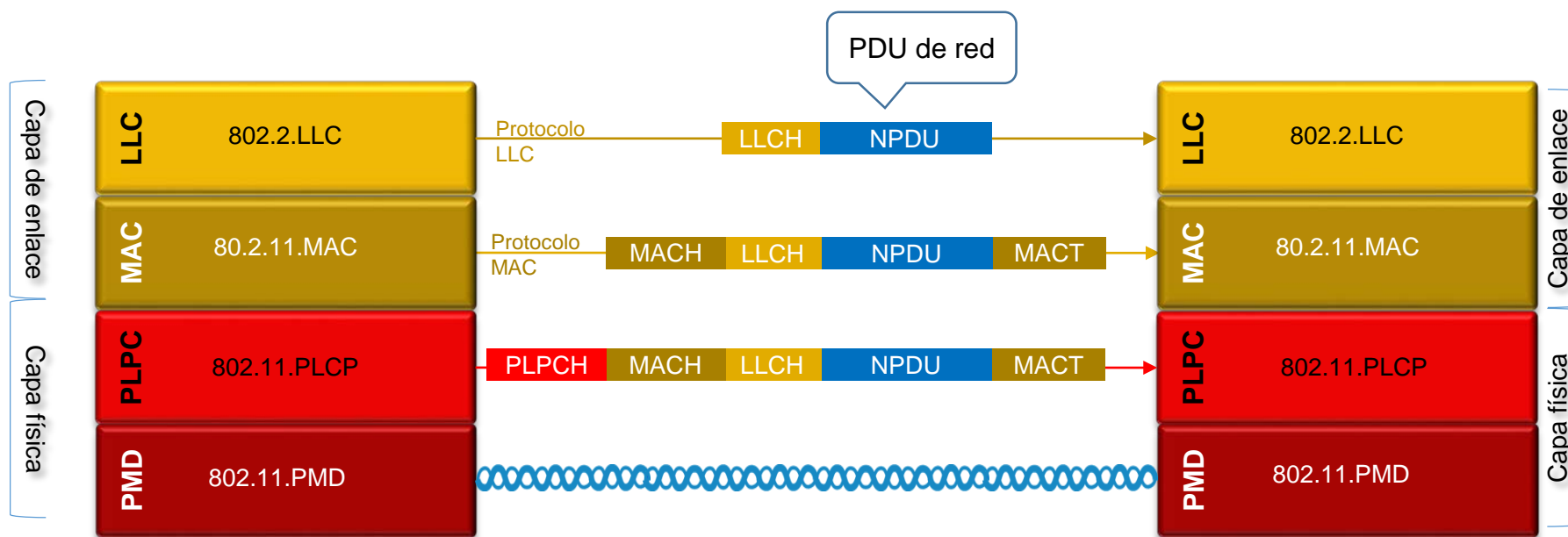
01/1011 = Control/RTS

10/0000 = Dato



# IEEE 802.11

## Encapsulación



MACT (*MAC trail*)  
MACH (*MAC header*)  
PLCPH (*PLCP header*)

PLCP (*Physical Layer Convergence Procedure*)  
PMD (*Physical Medium Dependent Layer*)



## 4. La capa física

Formato de la trama física (PLCP)

Distribución de canales

Formato de la capa física

Antenas habituales

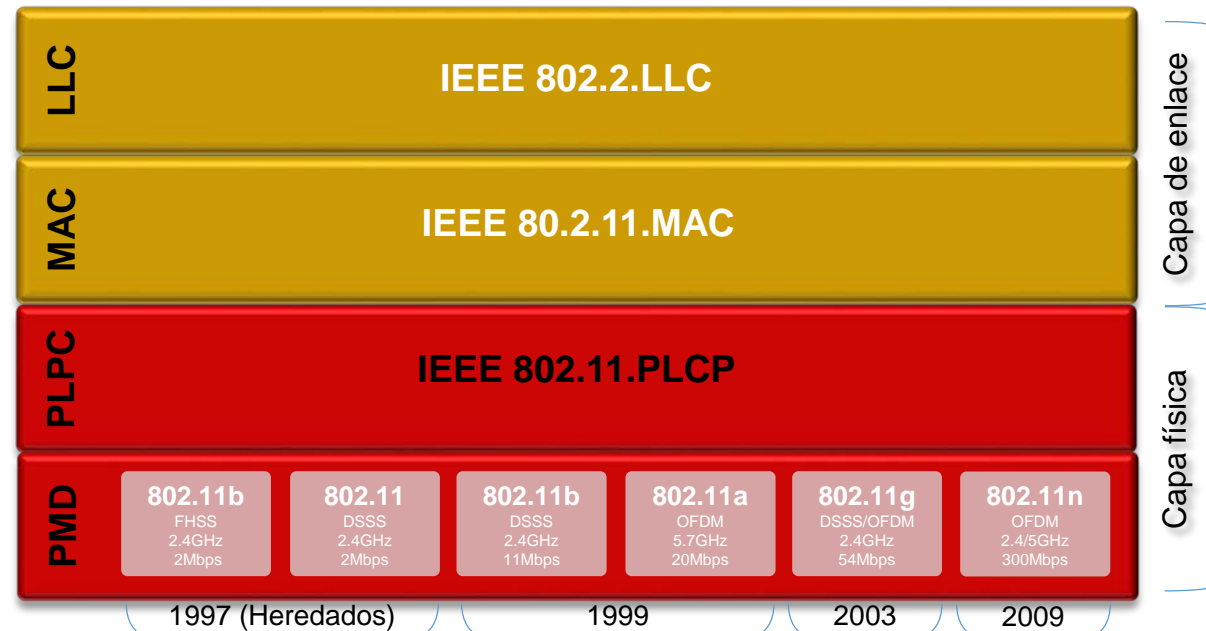
# IEEE 802.11

## Capa física



■ El modelo 802.11 divide la capa física en dos:

- **PLCP** (*Physical Layer Convergence Procedure*): tiene la función de convergencia con el sistema físico
- **PMD** (*Physical Medium Dependent Layer*): interacciona con el medio según una técnica de modulación y codificación determinadas.

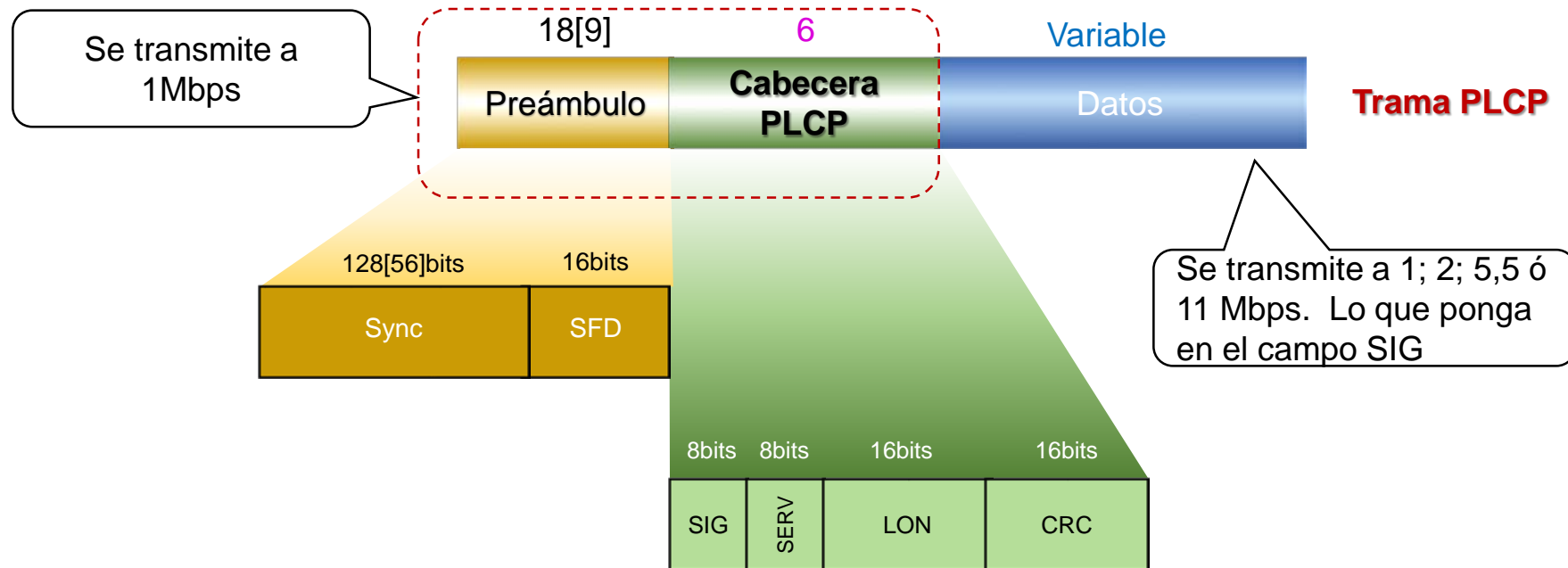


# IEEE 802.11

## Formato de la trama física (PLCP)



- Las principales funciones que desempeña la cabecera PLCP son:
  - 1) Establecer la sincronización entre emisor y receptores a fin de que interpreten correctamente el principio de cada bit y de la trama misma.
  - 2) Indicar la velocidad de transmisión utilizada

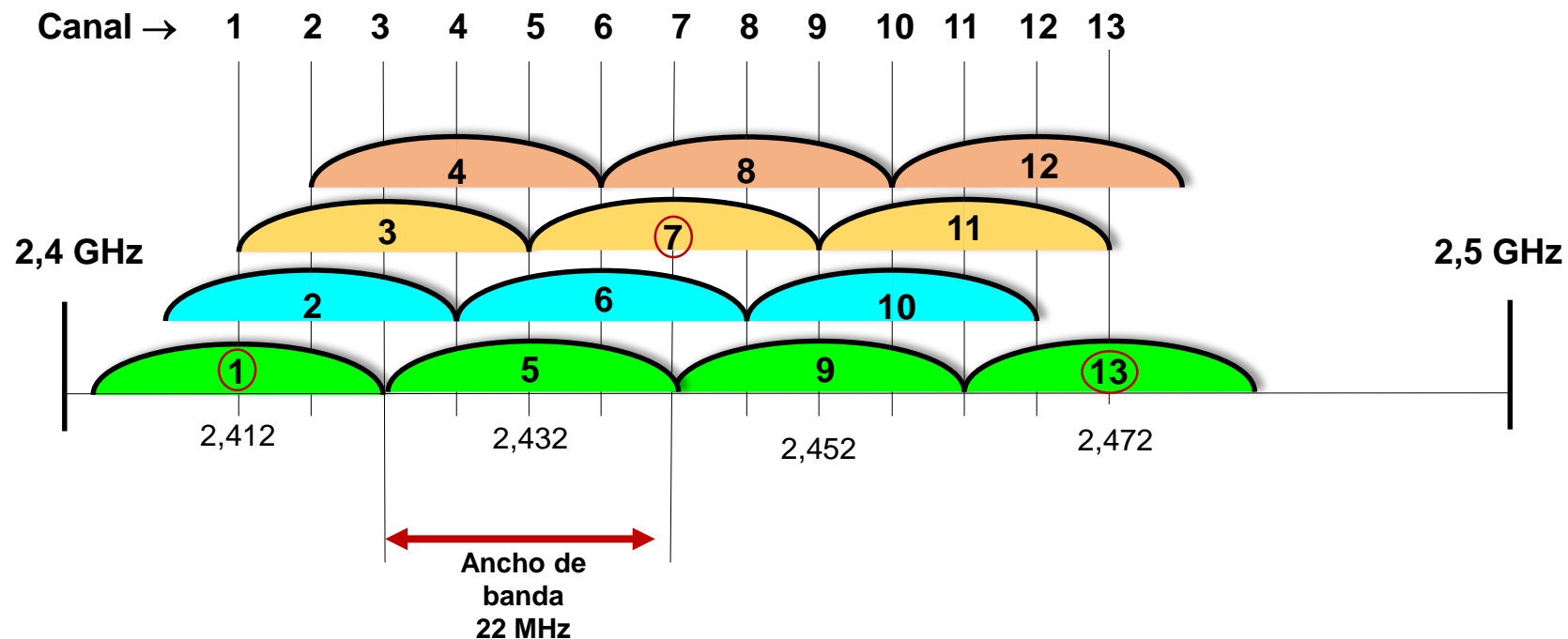


# IEEE 802.11

## Distribución de canales 802.11b/g (Europa)



- Como puede apreciarse en la figura, una parte muy importante de la señal de un canal se meterá sin remedio en los canales adyacentes creando interferencias.
- Podemos usar la combinación 1, 6 y 11, la 2, 7 y 12 o la 3, 8 y 13, pero sin duda alguna, lo más conveniente es separar un poco más los canales usados y que la diferencia entre ellos quede en 30 MHz. Por tanto:
  - En Europa, los canales más óptimos a usar en puntos de acceso cercanos o adyacentes para eliminar el solapamiento entre canales y minimizar las interferencias son tres: el 1, el 7 y el 13.



# IEEE 802.11

## Antenas habituales. Diagrama de radiación



- La antena mas habitual y barata es el **dipolo omnidireccional**
- Los equipos a menudo usan 2 antenas dipolo llamadas **antena diversidad**
  - Cuando el equipo recibe una trama de prueba, al utilizar dos antenas, obtiene dos señales de las cuales elige la que considera más conveniente.



Antena dipolo 10 cm - 2,5dBi

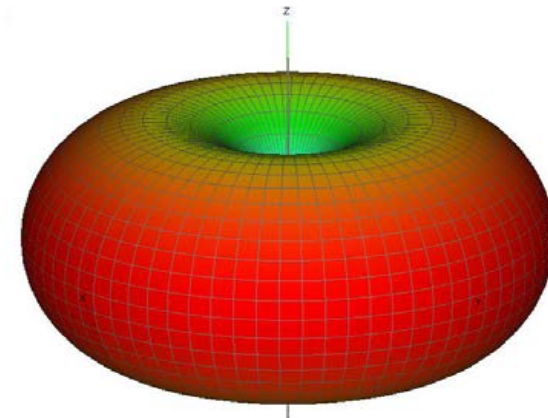


Diagrama de radiación 3D





# 5. Casos de estudio

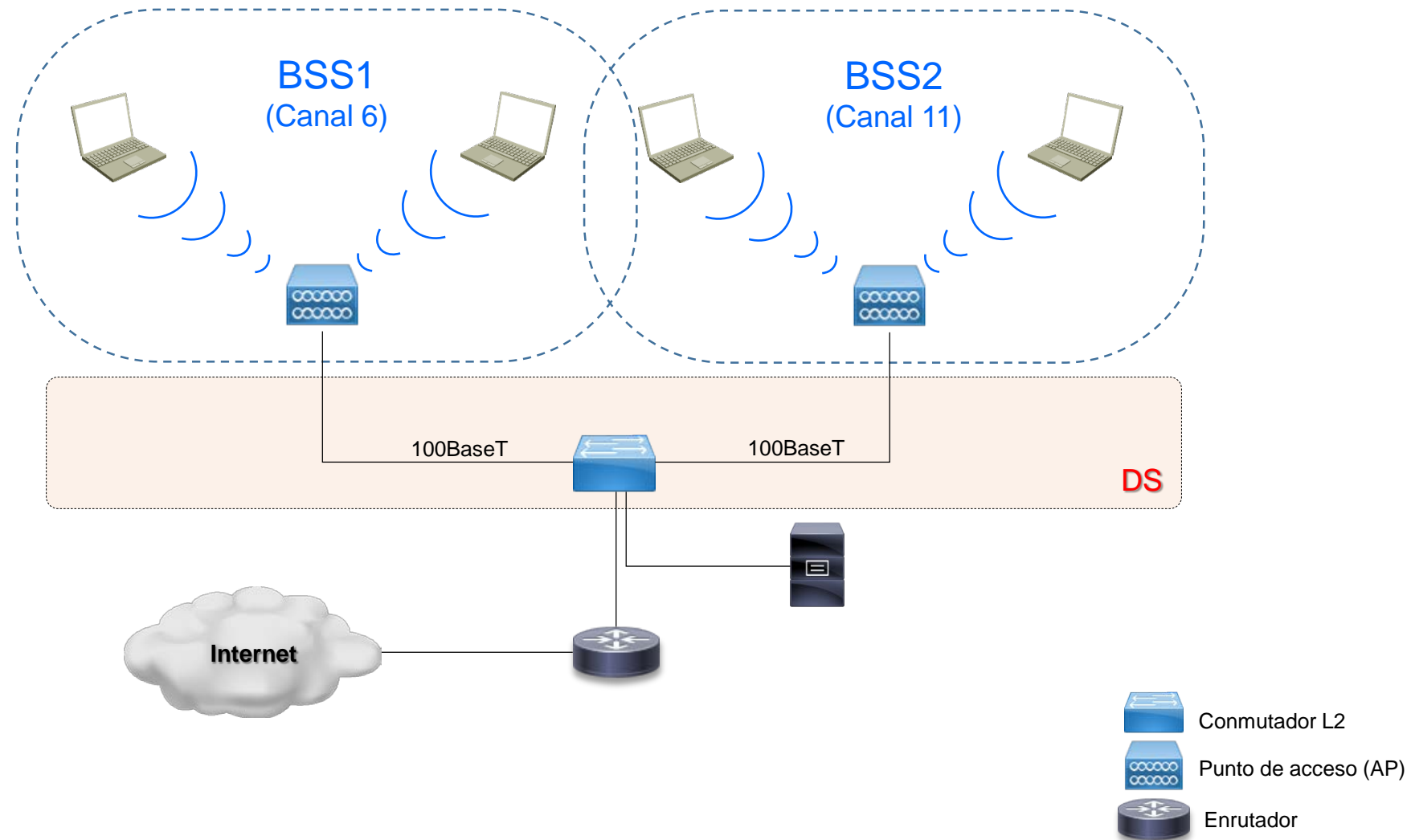
DS Ethernet 100Base-T  
Acceso WiFi desde el hogar

# Caso de estudio [1]

## DS Ethernet 100Base-T



- En este caso de estudio el ESS tiene dos BSS conectados.
- Cada BSS da servicio a una celda y estas se solapan con el fin de permitir la itinerancia (*roaming*)
  - Las celdas operan en canales distanciados (6,11) con el fin de que no se interfieran
- El DS es Ethernet 100Base-T y ofrece conectividad L2 entre los APs

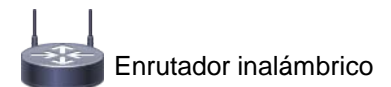
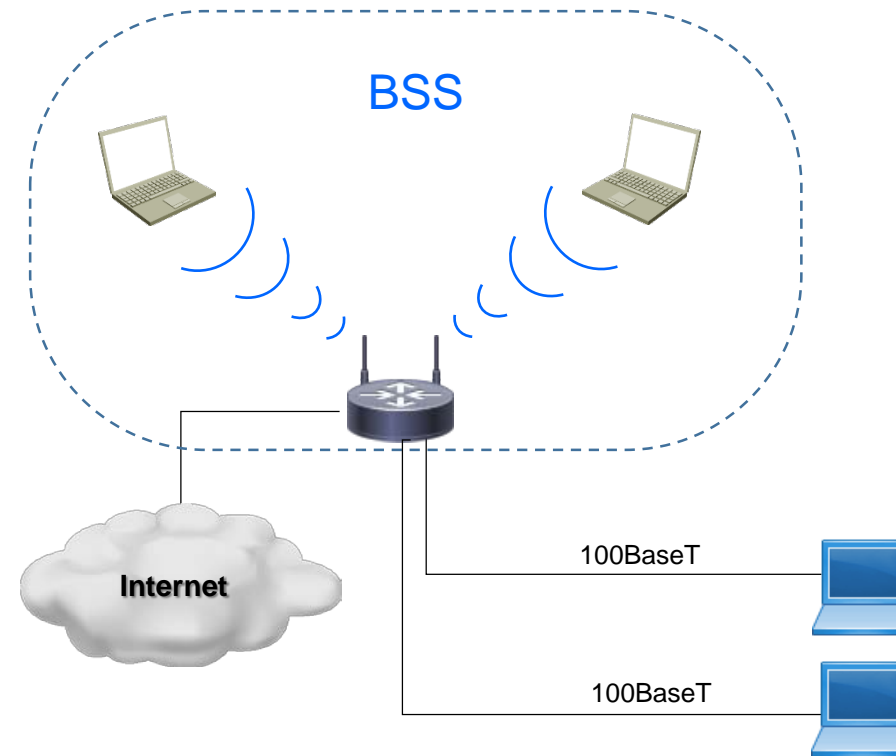


# Caso de estudio [2]

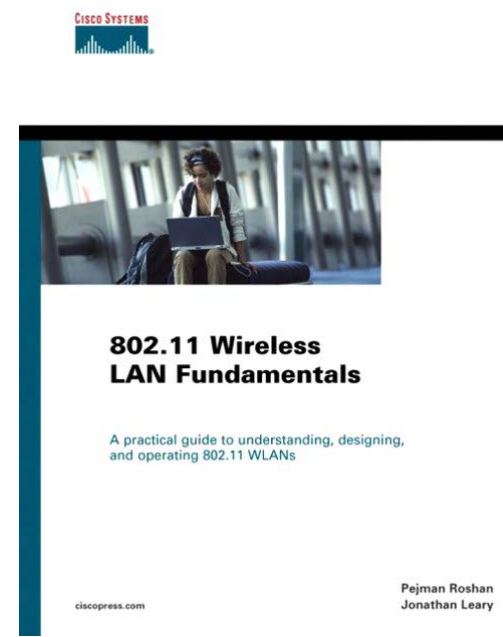
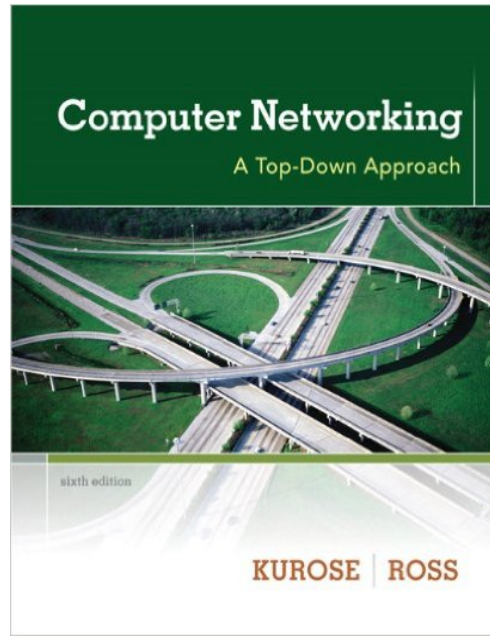
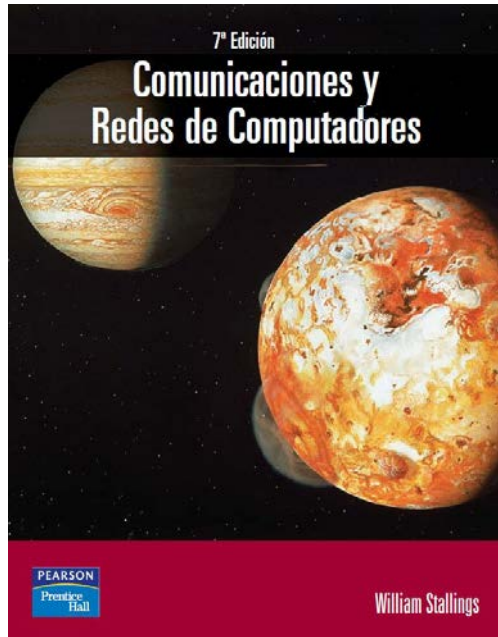
## Acceso WiFi desde el hogar



- Acceso inalámbrico desde el hogar
- El router tiene las siguientes capacidades:
  - un punto de acceso inalámbrico 802.11bg
  - conectividad Ethernet entre los host
  - Acceso Internet



# Referencias



- [1] William Stallings: *Comunicaciones y Redes de Computadores*. (7ª ed 2004). Prentice Hall
- [2] J Kurose & K Ross: *Computer Networking a Top Down Approach* (6ª ed 2013)
- [3] Pejman Roshan & Jonathan Leary: *802.11 Wireless LAN Fundamentals* (1ª ed 2003). Cisco Press