

Tema 2

Técnicas de acceso y control de enlace

Profesores:

Mercedes Amor

Alberto Salguero

Inmaculada Ayala

Daniel Muñoz

Lidia Fuentes

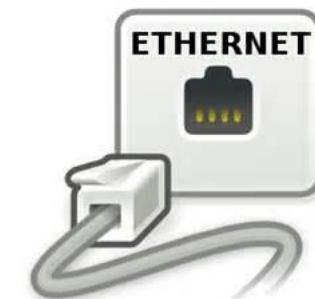
Francisco Servant

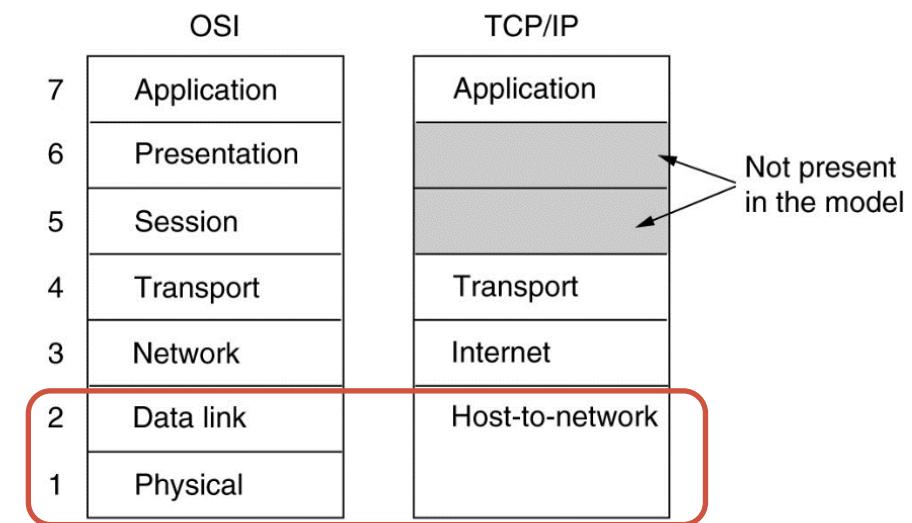
Gabriel Luque

Francisco Rus

Contenido del tema

- Caracterización y Servicios del Nivel de Enlace
- Redes de Acceso Múltiple
 - Redes de Acceso Múltiple con Detección de Portadora
 - CSMA/CD (Ethernet)
 - Redes Inalámbricas
 - Wifi
 - Bluetooth
- Protocolo de Control de Enlace de Alto Nivel (PPP)





CARACTERIZACIÓN Y SERVICIOS DEL NIVEL DE ENLACE

La capa de enlace

Objetivo básico:

Transferir los datos de la capa de red de un equipo a la capa de red de otro equipo con el que tiene **conexión directa**

Servicios que ofrece

Control de errores

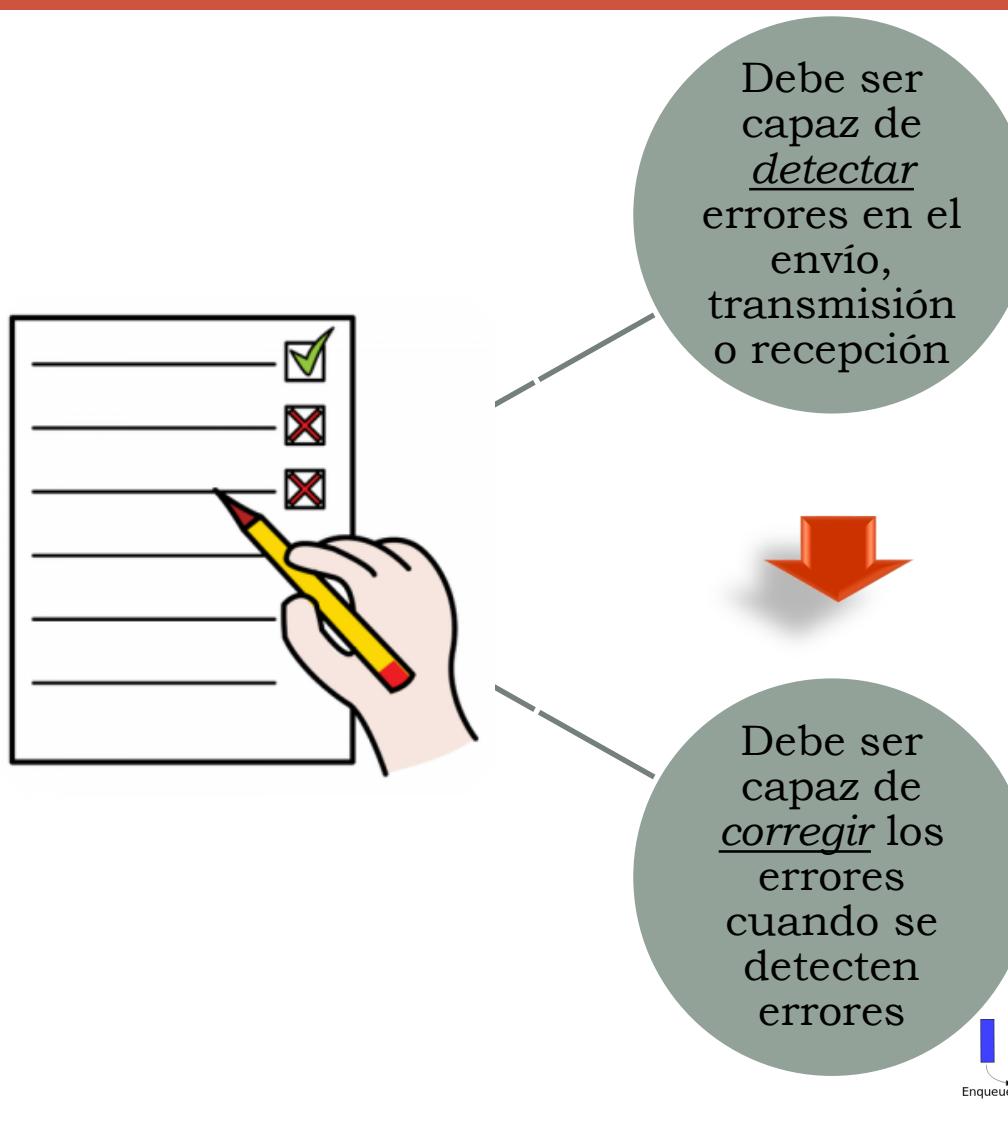
- Detección y Corrección

Control de acceso al medio

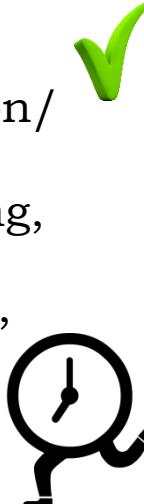
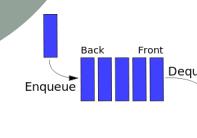
Control de flujo

Comunicación half/full duplex

La capa de enlace: control de errores



- Mensajes que se pierden, que llegan duplicados o con errores
- Técnicas detectoras de mensajes con errores:
 - Bits de paridad, CRC, checksums, ...
- Técnicas de corrección/ control de errores:
 - Códigos de hamming, confirmaciones positivas/negativas, retransmisiones, temporizadores, ...



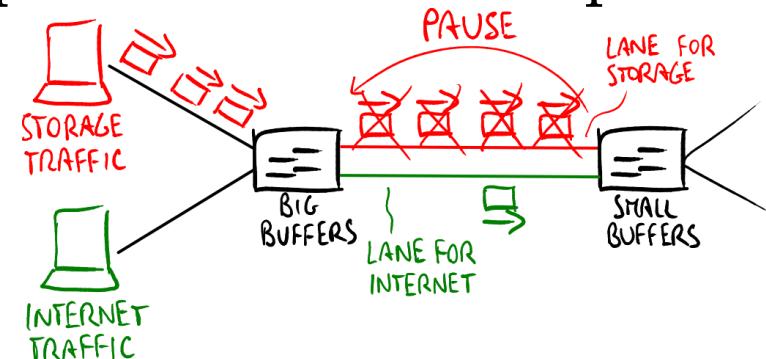
La capa de enlace: control de acceso al medio

- Transferir los datos de la capa de red de un equipo a la capa de red de otro equipo con el que tiene **conexión directa**:
 - Conectados a un mismo enlace
 - Tipos de enlace (tema 1)
 - Enlaces punto a punto
 - Enlaces de difusión o multipunto
- En enlaces punto a punto
 - Se debe garantizar el envío de bits de un extremo a otro
- En enlaces de difusión
 - Además, hay que controlar el acceso al medio compartido
 - Que estación puede transmitir
 - Función de los Protocolos MAC: *Medium Access Control*

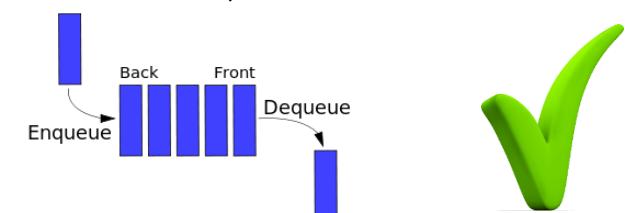


La capa de enlace: control de flujo

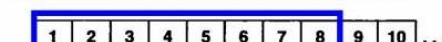
- Se usa para evitar que el emisor envíe más datos al receptor de los que éste es capaz de almacenar para su posterior tratamiento



- Técnicas: buffers, confirmaciones positivas, ...
- Protocolos
 - Parada y espera
 - Repetición selectiva
 - Ventana Deslizante (*sliding window*)

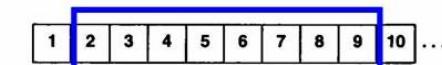


ESTADO INICIAL DE LA VENTANA DESLIZANTE



(a)

ESTADO DE LA VENTANA UNA VEZ DESLIZADA



(b)



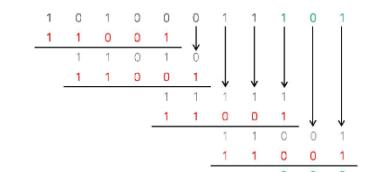
Detección y corrección de errores

- Se usan técnicas de redundancia
 - Bits adicionales que se añaden a las tramas para detectar errores



Bits de paridad,
Checksums,
CRCs, etc.

Detectan si hay error,
pero no dónde (que
bit(s) son erróneos)



Tipos
de
códigos

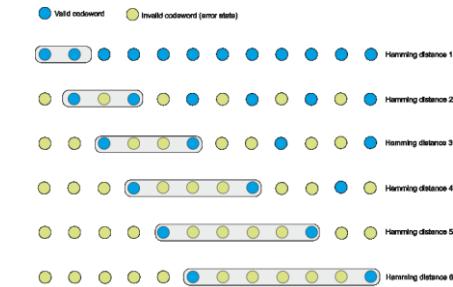
**Códigos
detectores**

Códigos de
Hamming

Corrección compleja

**Códigos
correctores**

3 bits extra para 4
para corregir un
único error



Detección de errores

- Bits de paridad
 - Se añade un bit de paridad al final del bloque de datos
 - Dos tipos de paridad
 - Paridad par: el número total de unos ha de ser par
 - Paridad impar: el número total de unos ha de ser impar

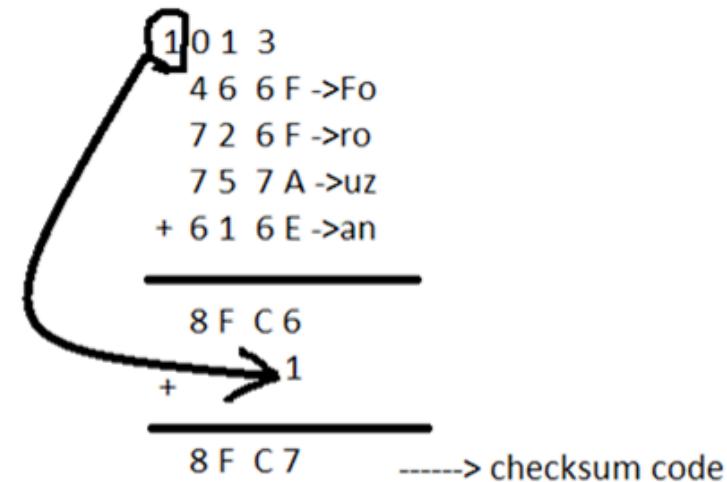
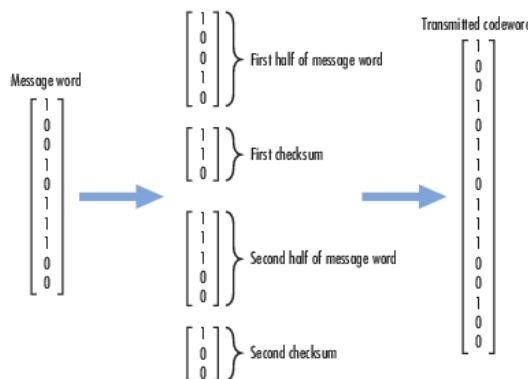
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
|---|---|---|---|---|---|---|---|

Paridad
(par)

- Comprobación de paridad
 - Detecta errores de un bit (o un número impar de bits)
 - No detecta errores de pares de bits
 - Ejemplo de aplicación: código ASCII
 - 7 bits + 1 bit de paridad

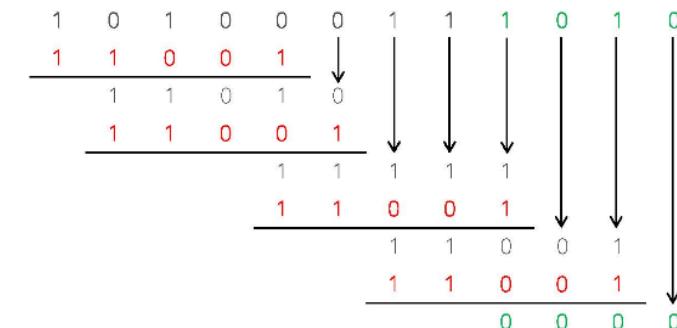
Detección de errores

- Sumas de comprobación (*checksum*)
 - Técnica general de detección de errores
 - Se suele aplicar a bloques de caracteres, en lugar de caracteres aislados (igual tamaño del checksum)
 - En la emisión y recepción
 - Se suma cada carácter al *checksum* (en complemento a 2) y el resultado debe de ser 0.
 - Se suele usar más en las capas de red y de transporte
 - Es un esquema simple
 - 16 bits en IP, TCP y UDP



Detección de errores

- Códigos redundantes cíclicos
 - Se conocen como CRC (*Cyclic Redundancy Check*)
 - Se envían d bits de información + r bits redundantes
 - La trama de $d+r$ bits ha de ser divisible por un número predeterminado
 - Si en el receptor la división tiene resto 0, se asume que no se ha producido ningún error
 - Los códigos CRC son particularmente interesantes porque su computación se puede realizar en hardware fácilmente:
 - Suele emplearse en protocolos implementados en HW
 - Capa de enlace/física
 - 16/32 bits en PPP
 - 32 bits en Ethernet y Token Ring
(*Magic number* = 0xC704DD7B)

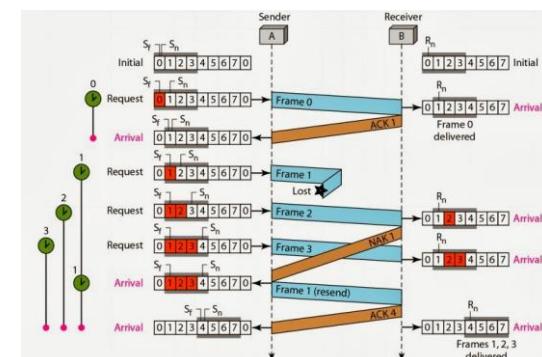


Control de errores



Cuando se DETECTA un error los datos (la trama) se DESCARTA en su totalidad y se debe de retransmitir

- ¿Cómo se entera el otro extremo de la pérdida para retransmitir?
- Técnicas de control de errores:
 - Asignación de números de secuencia
 - Confirmaciones positivas/negativas, retransmisiones, temporizadores, ...

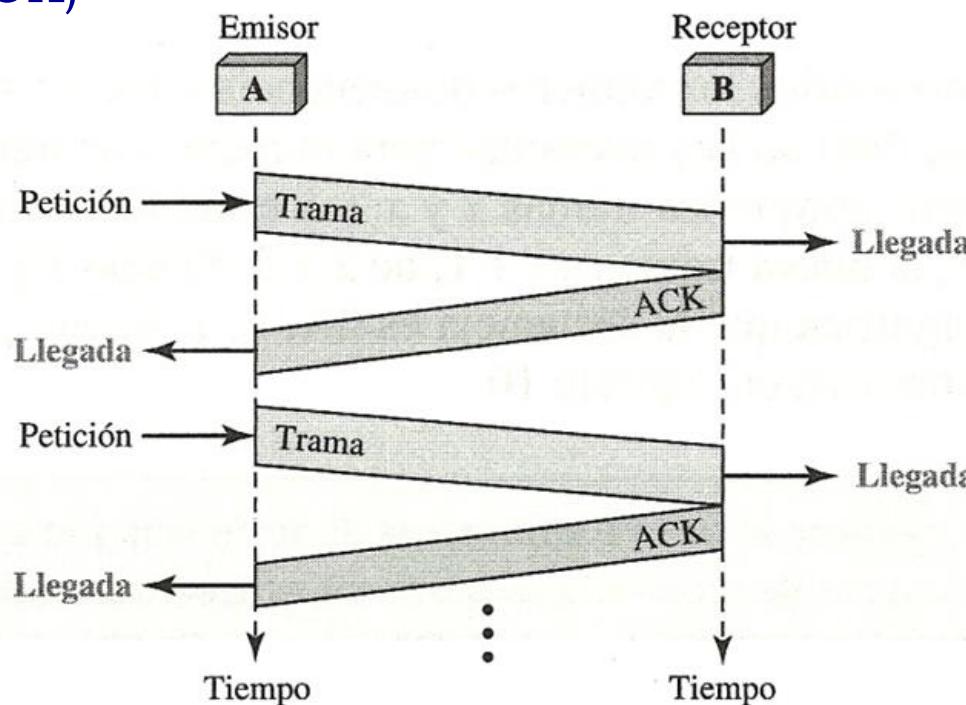


Protocolos básicos de control de errores/flujo

- Dos protocolos básicos
 - Protocolo de **parada y espera** (*stop-and-wait*)
 - Protocolo de **repetición selectiva** (*selective repeat*)
- Estos protocolos se pueden usar:
 - A nivel de transporte (alto nivel)
 - A nivel de enlace (bajo nivel)
- Se diferencian en la **Eficiencia**
 - Medida que indica la proporción de tiempo necesario para enviar información útil ($T_{envío\ útil}$) respecto al total requerido (T_{total})
 - Lo ideal es una eficiencia del 1 (o del 100%)
- $$Efectividad = \frac{T_{envío\ útil}}{T_{total}}$$

Protocolo de parada y espera (*Stop & Wait*)

- Funcionamiento básico:
 1. Se transmite una trama
 2. El receptor envía una confirmación
 3. El emisor no envía la siguiente trama hasta que recibe la confirmación (ACK)



Protocolo de parada y espera

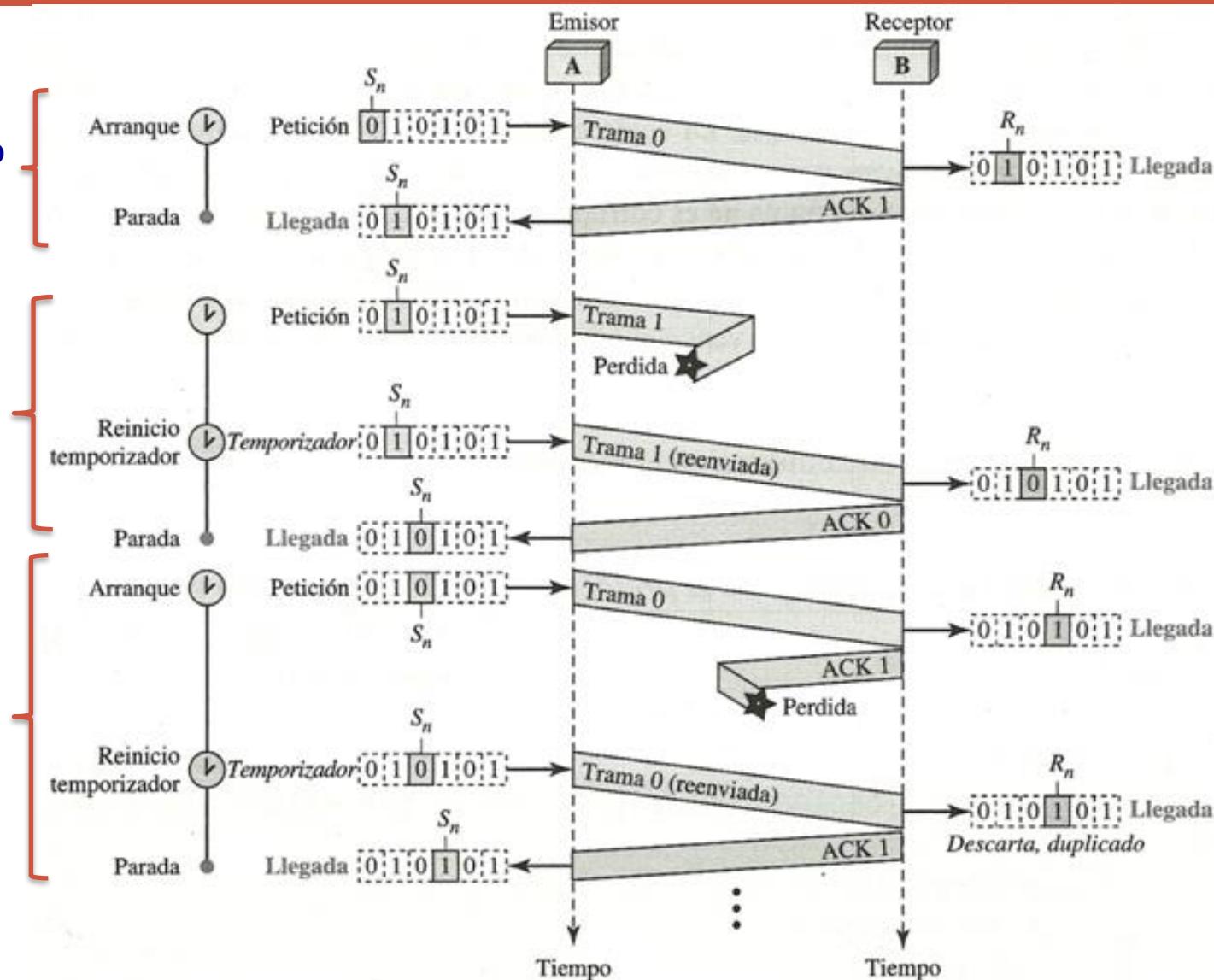
- Principales problemas en las comunicaciones:
 1. Pérdida de la trama enviada
 2. Pérdida de la confirmación (ACK)
- Detección y Soluciones
 1. **Temporizadores (timeout):**
 - Se activa cuando el emisor envía una trama.
 - Si se cumple el tiempo sin recibir confirmación -> Reenvía (**retransmisión**)
 2. **Numeración de tramas y confirmaciones positivas:**
 - Usa 1 bit (0 ó 1) para evitar la aceptación de la misma trama varias veces
 - ABP (Alternating Bit Protocol): Las tramas van numeradas (en secuencia: 0, 1, 0, 1, ...)
 - La confirmación positiva (**ACK – acknowledge**) también se numera indicando la siguiente trama que espera recibir

Protocolo de parada y espera

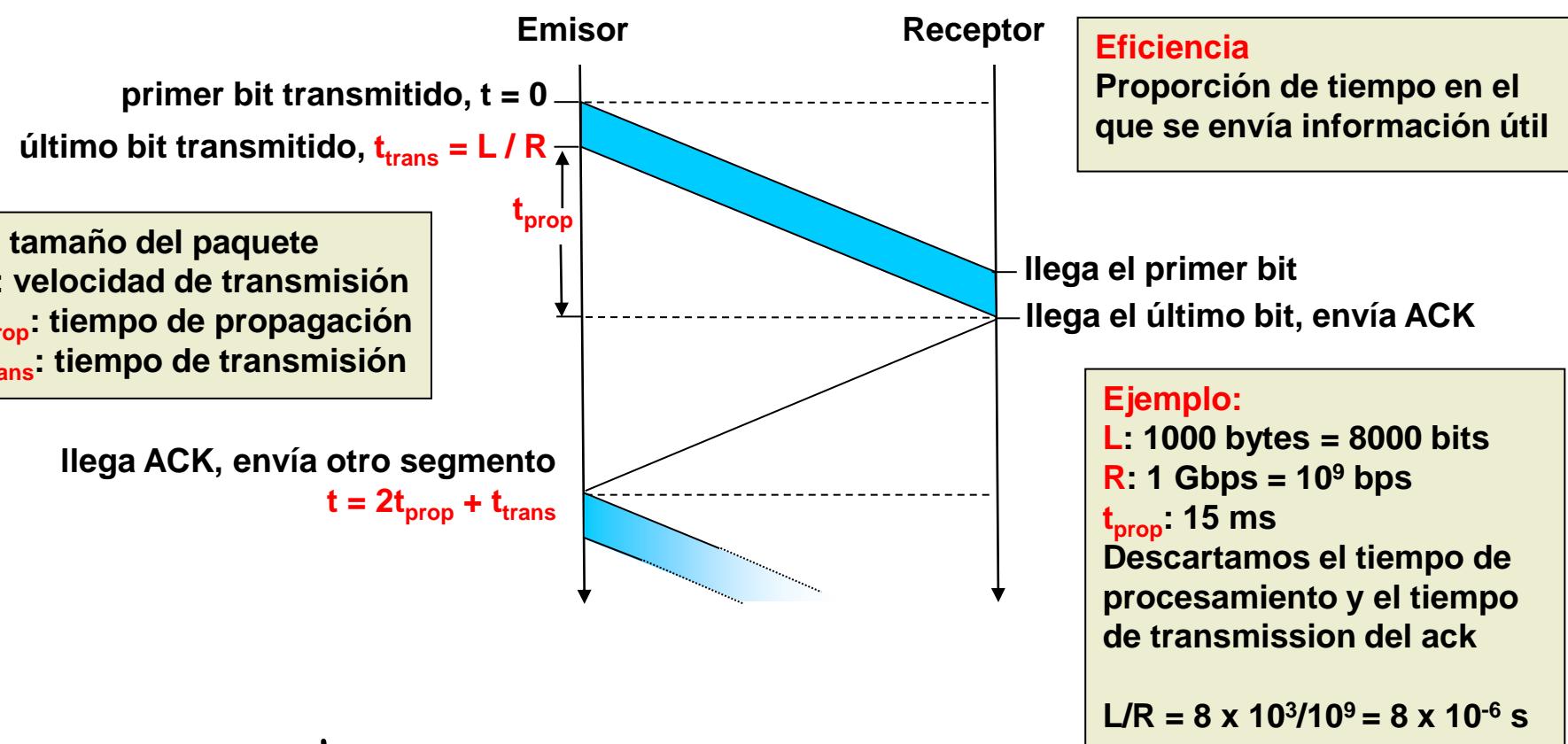
Funcionamiento normal

Pérdida de una trama

Pérdida de una confirmación



Protocolo de parada y espera: Eficiencia



$$E_{\text{sender}} = \frac{t_{trans}}{2 t_{prop} + t_{trans}} = \frac{0.008 \text{ ms}}{30.008 \text{ ms}} = 0.00027$$



Protocolo de parada y espera



Ventajas

- Simple de implementar
- Eficiente si los mensajes son de gran tamaño (L grande)

Inconvenientes

- Ineficiencia si usan mensajes pequeños
- No siempre los mensajes pueden ser de gran tamaño

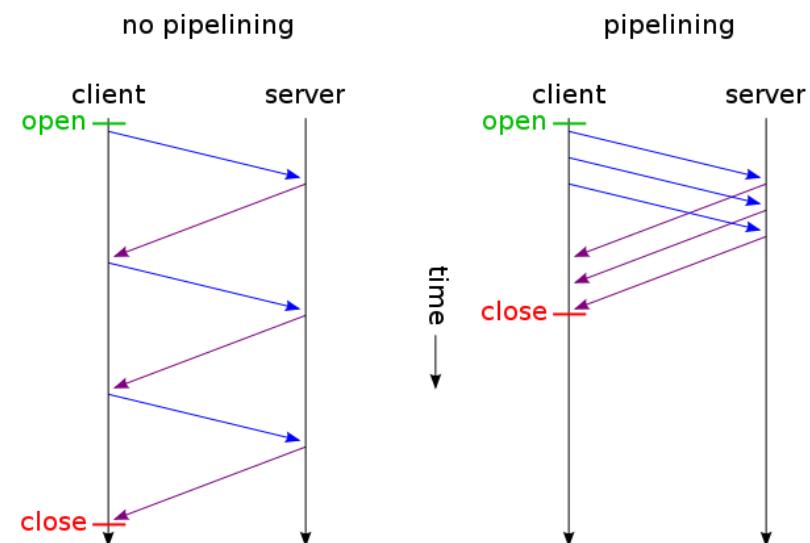


¿Por qué no se envían mensajes grandes?

- Tamaño limitado de la memoria del receptor
- Si hay errores hay que retransmitir mucha información
- En medios de acceso múltiple la red no puede estar ocupada durante mucho tiempo

Pipelining

- Alternativa de mejora: *pipelining*
 - Enviar más de un mensaje consecutivamente, sin esperar confirmaciones de los anteriores
- Consecuencias
 - El rango de los números de secuencia ha de ser ampliado
 - El receptor y/o el emisor han de usar buffers
- Dos técnicas básicas
 - Go-Back-N
 - SRP (*Selective Repeat Protocol*) – (variante Rechazo selectivo)
- Se basan en el concepto de **ventana deslizante**

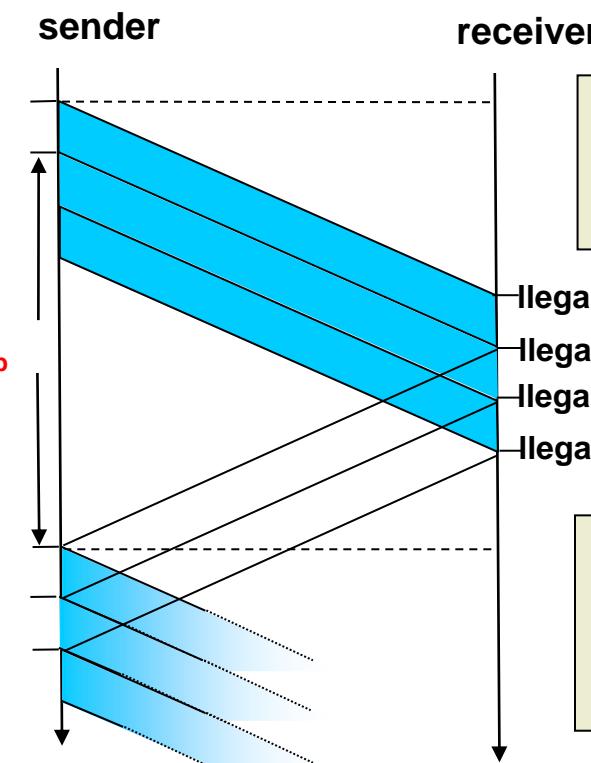


Eficiencia del Pipelining

primer bit transmitido, $t = 0$
último bit transmitido, $t = L / R$

L: tamaño del paquete
R: velocidad de transmisión
 t_{prop} : tiempo de propagación
 t_{trans} : tiempo de transmisión

Ilega ACK, envía otro segmento
 $t = 2t_{prop} + 3t_{trans}$



Eficiencia
Proporción de tiempo en el que se envía información útil

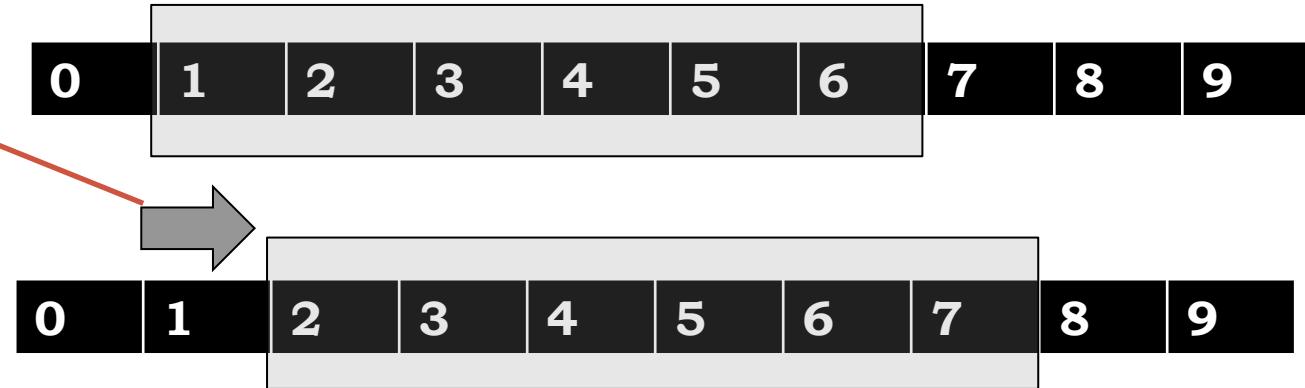
Ilega el primer bit
Ilega el último bit, envía ACK
Ilega el último bit del paquete 2. ACK
Ilega el último bit del paquete 3. ACK

Ejemplo:
L: 1000 bytes
R: 1 Gbps
 t_{prop} : 15 ms

$$E_{sender} = \frac{3 * T_{trans}}{2 * T_{prop} + 3 * T_{trans}} = \frac{0,024ms}{30 + 0,024} = 0,0008$$

Consecuencia:
Mejora en un factor de 3
(0,00027 en stop&wait)

Control de flujo por Ventana deslizante

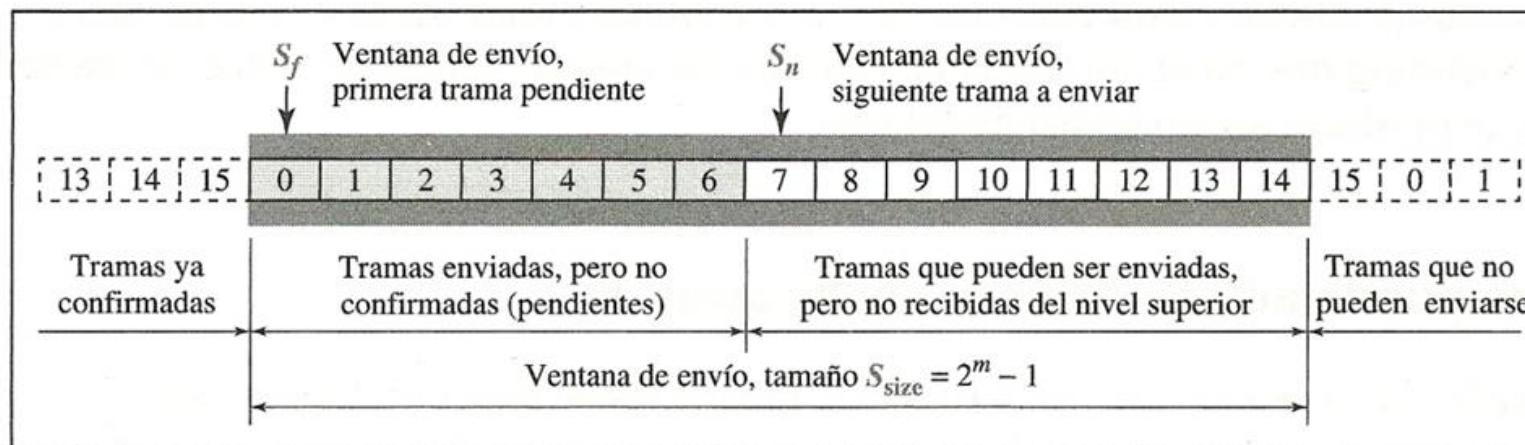
- Concepto de ventana:
 - Para el emisor
 - Una ventana (de emisión) es el conjunto de paquetes que se pueden enviar sin esperar confirmación

La ventana se desplaza al recibir las confirmaciones
 - Para el receptor
 - Una ventana (de recepción) es el conjunto de paquetes que debe estar preparado para recibir en cualquier momento
- Los mensajes usan m bits para numerar los paquetes:
 - Mensajes numerados de $[0, 2^m - 1]$
 - Máximo tamaño de ventana: 2^m

Nº de secuencia incluido en el mensaje

Concepto de ventana deslizante

- Ejemplo:
 - $m = 4$ (bits) → Numeración: [0,15]
 - Tamaños de ventana posible: [1,16] → Tamaño de ventana elegido = 15

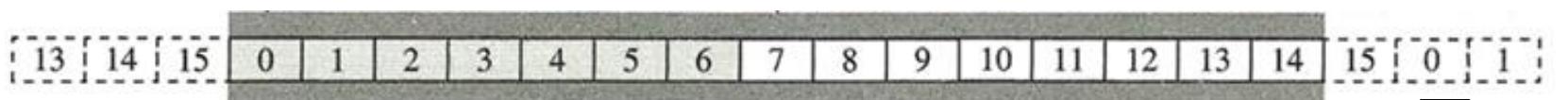


a. Ventana de envío antes de deslizar

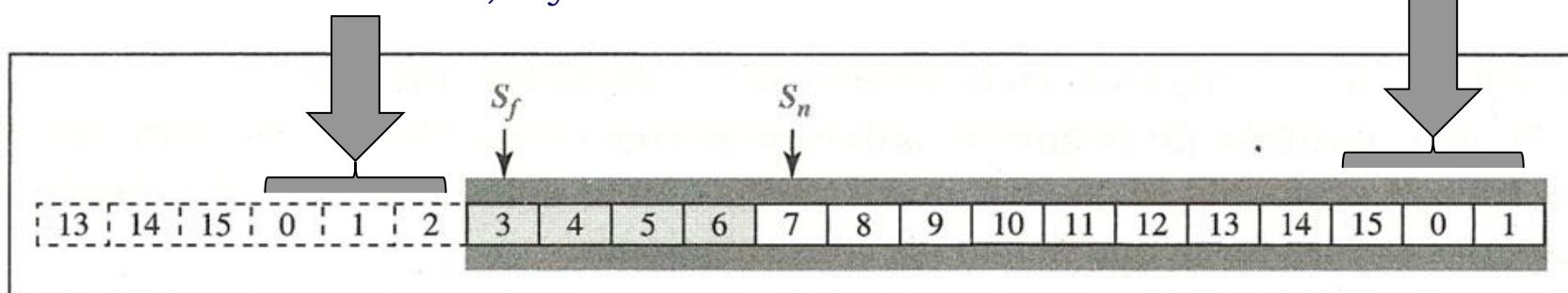
- **Dentro** de la ventana de emisión puede haber:
 - Tramas enviadas no confirmadas
 - Tramas sin enviar
- A la izquierda de la ventana están las tramas enviadas y confirmadas
- A la derecha tramas que no se pueden enviar

Concepto de ventana deslizante

- Ejemplo:
 - $m = 4$ (bits) \rightarrow Numeración: [0,15]
 - Tamaños de ventana posible: [1,16] \rightarrow Tamaño de ventana elegido = 15



Recibe confirmación de 0, 1 y 2



b. Ventana de envío después del desplazamiento

Cuando se reciben confirmaciones la ventana se desplaza:

Las tramas 0, 1 y 2 salen de la ventana (enviadas y confirmadas), y las tramas 15, 0 y 1 entran en la ventana de emisión.

Protocolo de repetición selectiva

- SRP (*Selective Repeat Protocol*)
 - Más eficiente que parada y espera
 - **Solo** se retransmiten aquellas tramas no confirmados:
 - Las tramas pueden llegar fuera de orden
 - En el emisor:
 - Es necesario un buffer para almacenar las tramas no confirmados (Tamaño máximo ventana de envío: 2^{m-1})
 - $m = 2 \rightarrow$ ventana máx. $2^{2-1} = 2$
 - $m = 3 \rightarrow$ ventana máx. $2^{3-1} = 4$
 - $m = 4 \rightarrow$ ventana máx. $2^{4-1} = 8$
 - Reenvía tramas **a petición del receptor** o por temporizador (uno por trama)

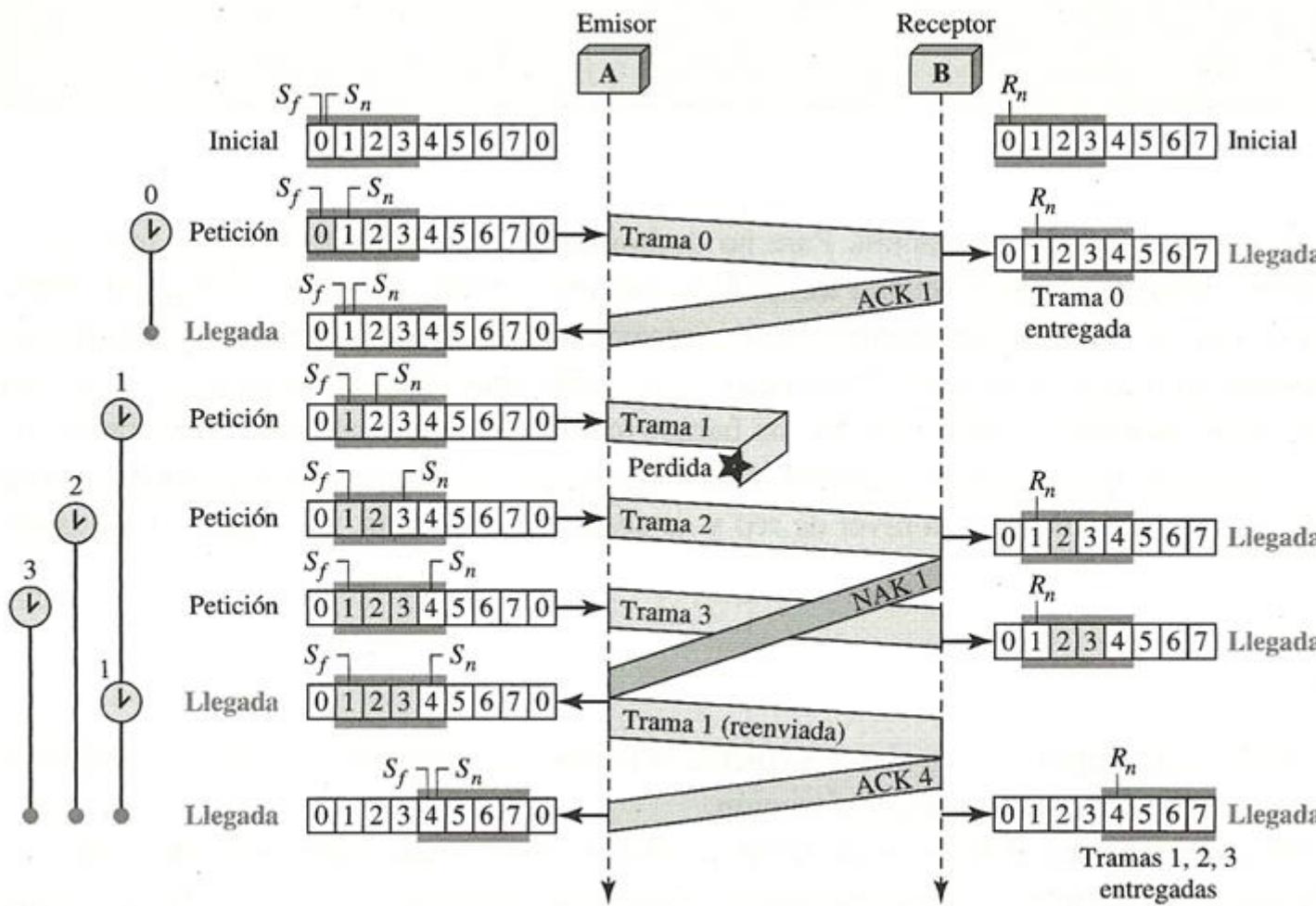
Protocolo de repetición selectiva

- SRP (*Selective Repeat Protocol*)
 - En el receptor
 - Es necesario un buffer para almacenar las tramas que llegan fuera de orden (Tamaño máximo ventana de recepción: 2^{m-1})
 - Si recibe una trama fuera de orden, envía una petición de repetición (NAK, **confirmación negativa**) con la que esperaba recibir
 - **Confirmación (POSITIVA) acumulativa:** La recepción de un ACK con número de secuencia X permite al receptor confirmar todas las tramas pendientes con número de secuencia < X



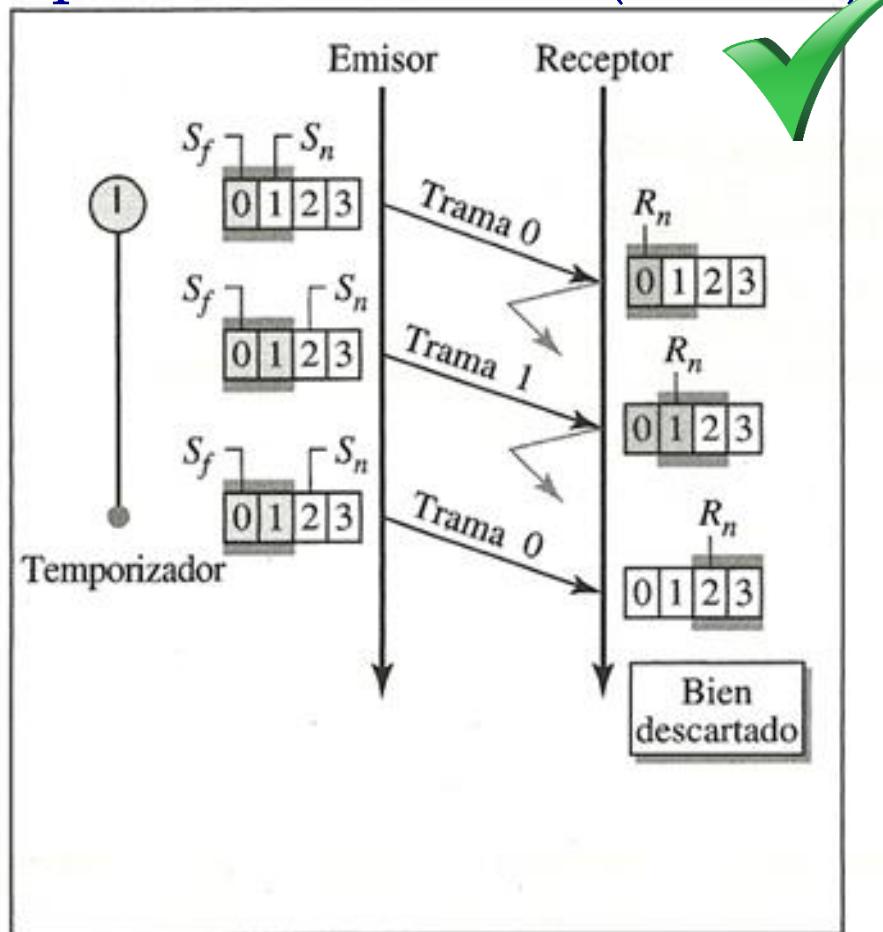
Protocolo de repetición selectiva

- Ejemplo de uso de repetición selectiva

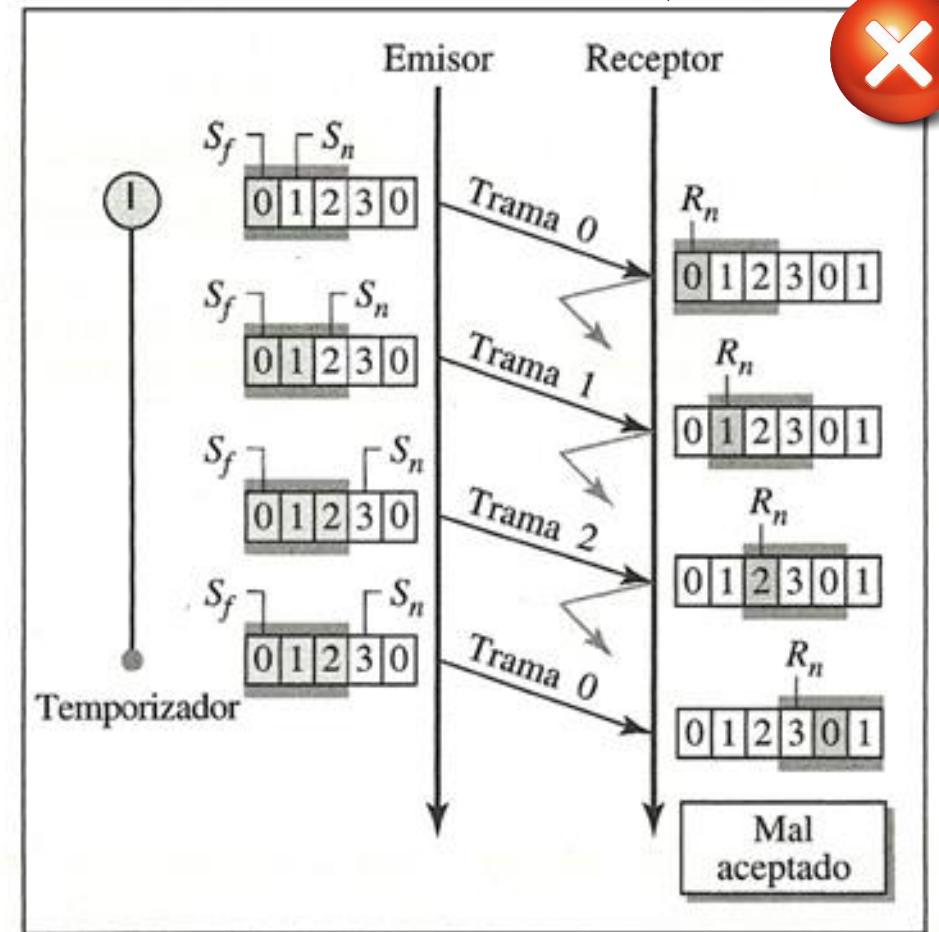


Numeración y tamaño de las ventanas

Repetición selectiva ($\leq 2^{m-1}$)

a. $\text{Tamaño de ventana} = 2^{m-1}$

Repetición selectiva ($> 2^{m-1}$)

b. $\text{Tamaño de ventana} > 2^{m-1}$

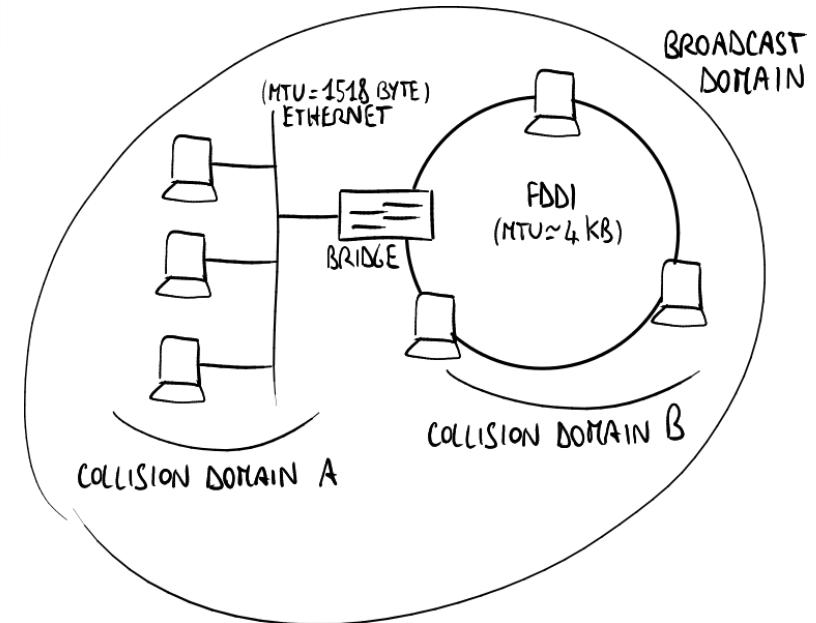
Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

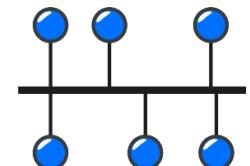
Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet



- Redes de Acceso Múltiple con Detección de Portadora (Ethernet)
- Redes Inalámbricas (WiFi y Bluetooth)

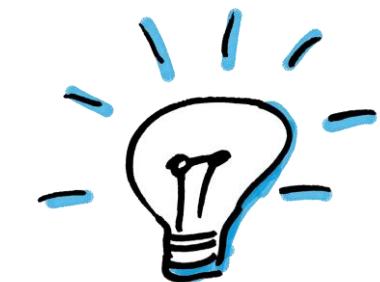
REDES DE ACCESO MÚLTIPLE



Protocolos de acceso multiple para control de acceso al medio

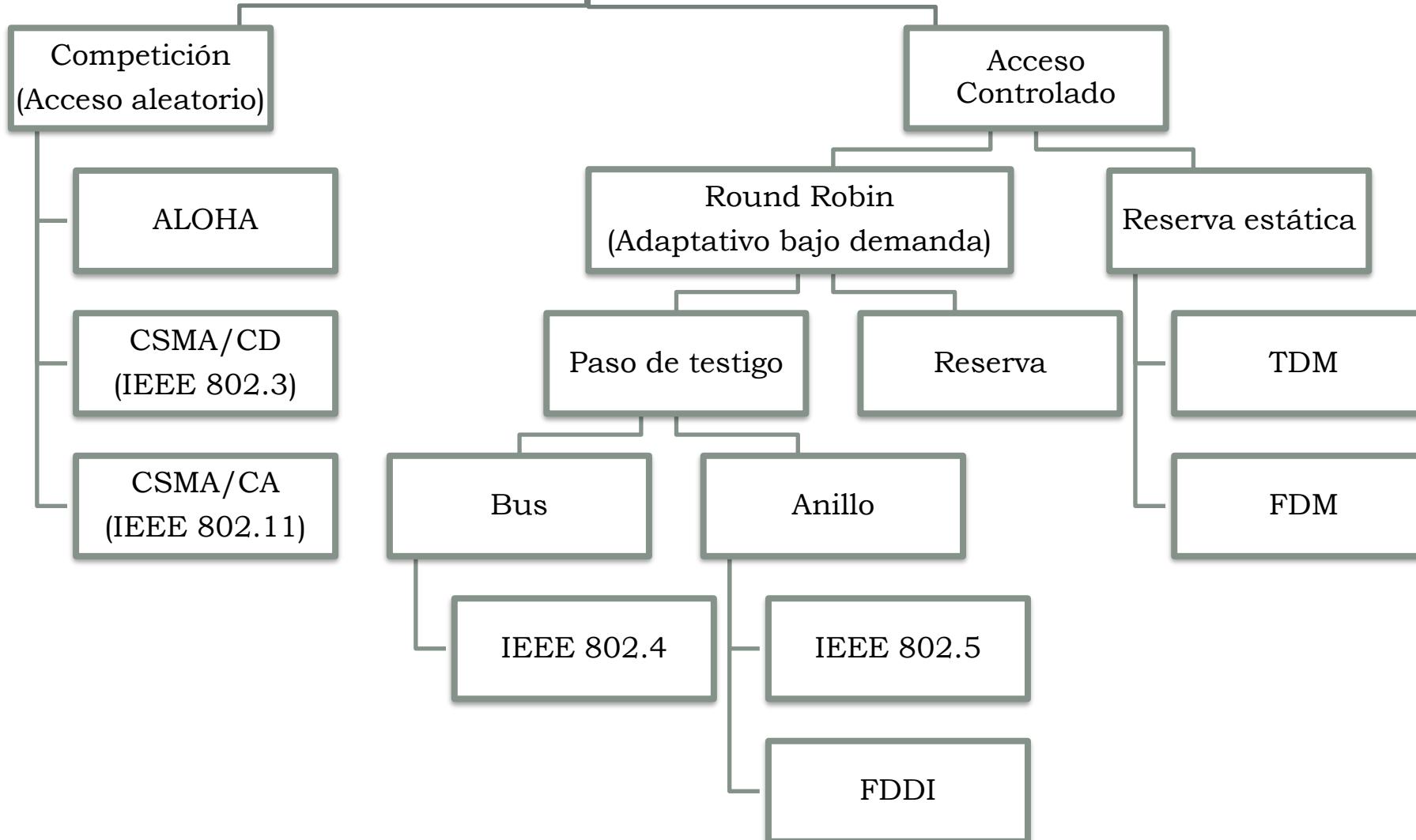
- En las redes de área local
 - No se suelen usar enlaces punto a punto, sino enlaces multipunto, acceso múltiple o de difusión
 - Es necesario un protocolo que controle el acceso de las estaciones conectadas a ese enlace compartido
- El control de los accesos a un medio compartido lo lleva a cabo un protocolo MAC (*Medium Access Control*)
- Dos tipos de control de acceso:
 - Una de las estaciones se encarga de controlar el acceso, siempre la misma
 - Centralizado
 - Todas las estaciones se encargan de controlar el acceso
 - Distribuido y/o descentralizado

Características de los protocolos de control de acceso al medio compartido



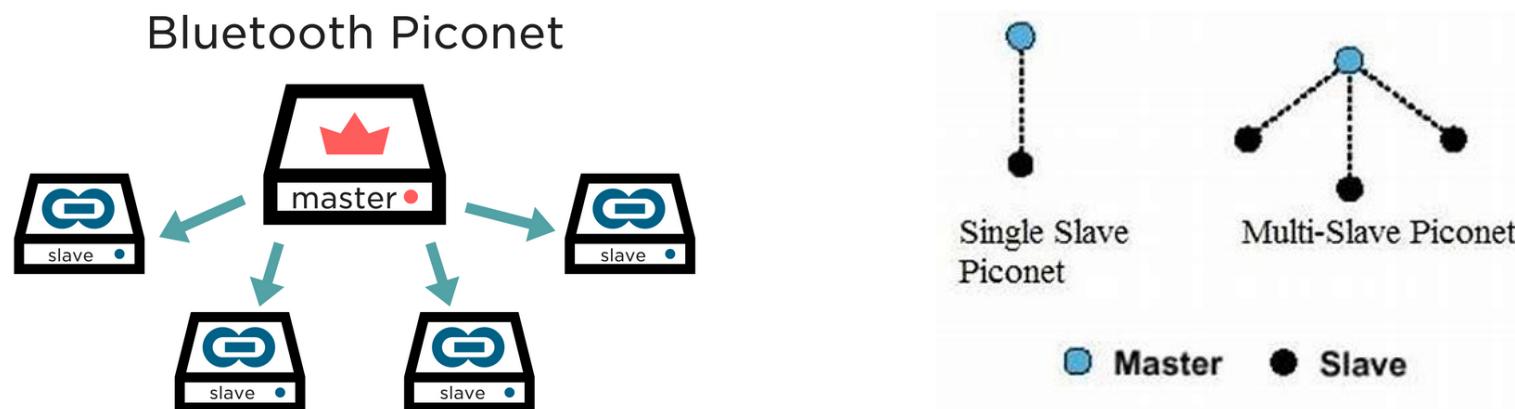
Protocolos de control de acceso múltiple

EN LANS y PANS con enlace compartido



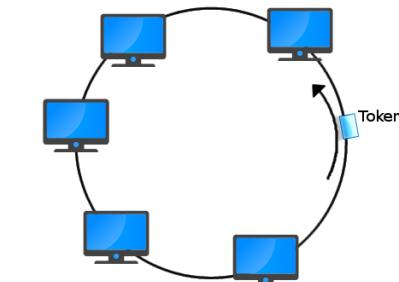
Protocolos de acceso al medio centralizados

- Ventajas de un control centralizado
 - Mayor control de los accesos
 - Lógica de acceso relativamente sencilla
 - Evita problemas de coordinación distribuidos
- Inconvenientes: poca tolerancia a fallos, cuellos de botella
- Ejemplo: Acceso en Redes Bluetooth (**IEEE 802.15**)



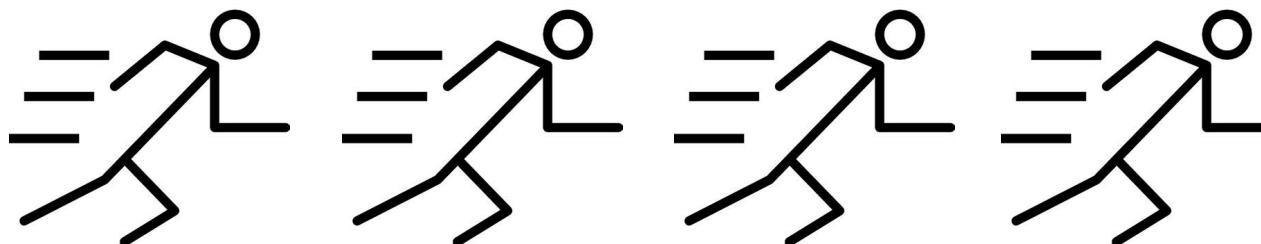
Asignación del enlace

- Estrategia *Rotación Circular (Round robin)*
 - Cada estación tiene un turno u oportunidad para transmitir, que puede ser utilizada o no
 - En cualquier caso, el turno pasará a la siguiente estación
 - El control puede ser centralizado o distribuido
 - Un método centralizado es el sondeo (*polling*)
 - Un método distribuido es el paso de testigo (*token passing*)
 - Es un método adecuado cuando varias estaciones tienen que transmitir datos durante largos períodos de tiempo



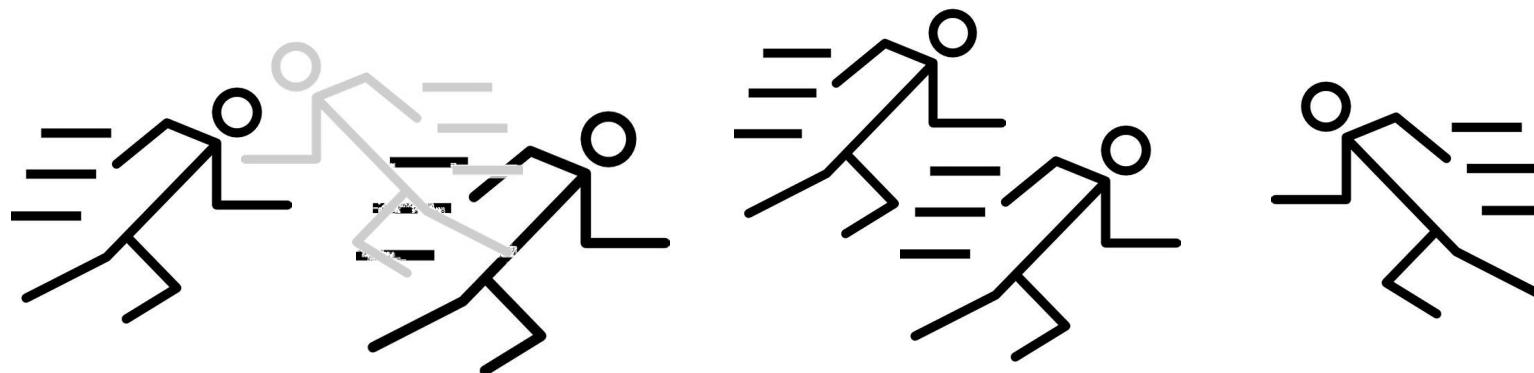
Asignación del enlace

- Estrategia de reserva
 - El tiempo se divide en intervalos de tiempo discretos
 - Como en TDM
 - Cuando una estación quiere transmitir
 - Reserva intervalos de tiempo para un largo período
 - Técnica válida para tráfico continuo



Asignación del enlace

- Estrategia de competición
 - Todas las estaciones compiten por acceder al medio
 - Puede haber colisiones
 - Son técnicas de naturaleza descentralizada
 - Técnica válida para tráfico a ráfagas
 - Tienden a deteriorar las prestaciones en condiciones de alta carga



Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet



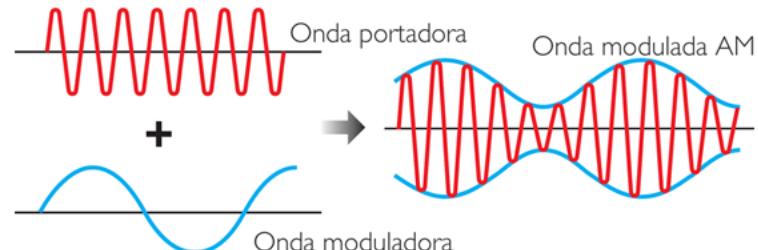
REDES DE ACCESO MÚLTIPLE CON DETECCIÓN DE PORTADORA (ETHERNET)



Detección de portadora

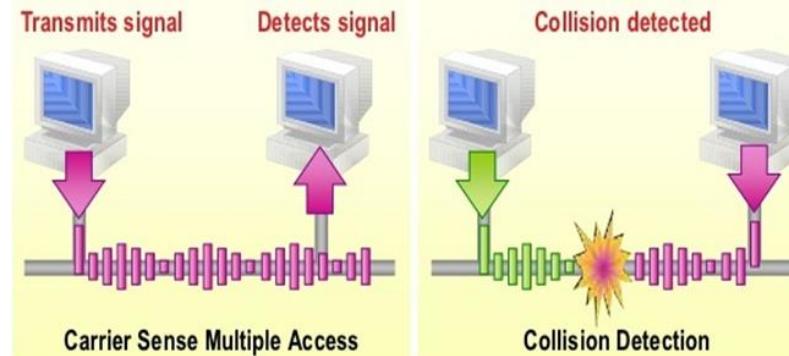
- En las redes cuya estrategia es el acceso por competición pueden existir colisiones
 - Una colisión se produce cuando dos tramas se transmiten simultáneamente por el mismo enlace (las señales se superponen)
 - Las colisiones son detectables (directa o indirectamente)
 - Una trama que colisiona debe ser retransmitida
- **Detección de portadora (carrier sense)**
 - Consiste en detectar la señal portadora, antes de transmitir para determinar si el enlace está en uso o no antes de enviar

Sin detección de portadora las estaciones transmiten libremente y después comprueban si la transmisión tuvo éxito



Protocolos de Acceso Múltiple basados en Detección de Portadora

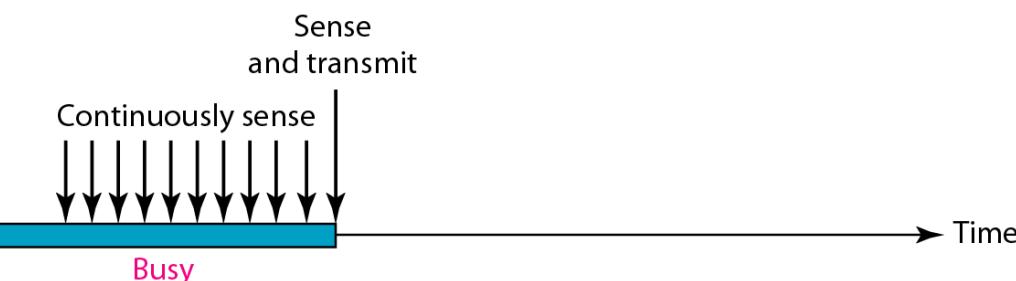
- Técnica CSMA (*Carrier Sense Multiple Access*)
 - (1) Detecta si alguien está transmitiendo en ese momento. Esta transmisión se detecta por la presencia de una señal portadora
 - (2) Si el canal está inactivo, la estación puede transmitir
 - (3) Si el canal está activo, la estación no puede transmitir. Podemos distinguir 3 tipos de algoritmos para determinar el comportamiento de una estación cuando ésta encuentra el canal ocupado
- Existen diversas variantes
 - CSMA 1-persistente
 - CSMA no persistente
 - CSMA p-persistente



Sí se detecta colisión: Se espera un tiempo aleatorio y repite su esquema

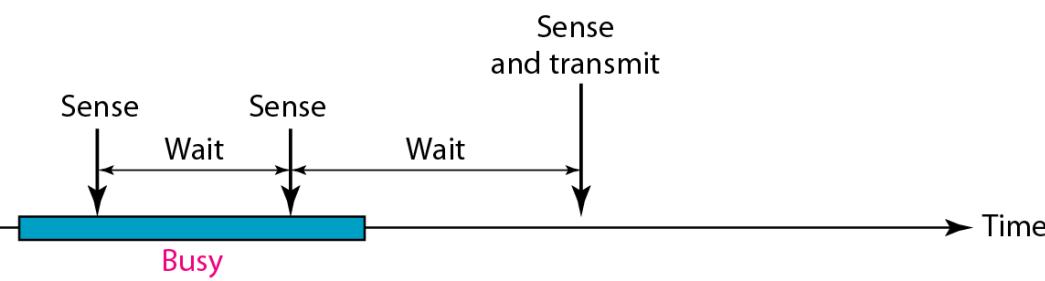
¿Qué hacer si el canal está ocupado?

CSMA 1-persistent



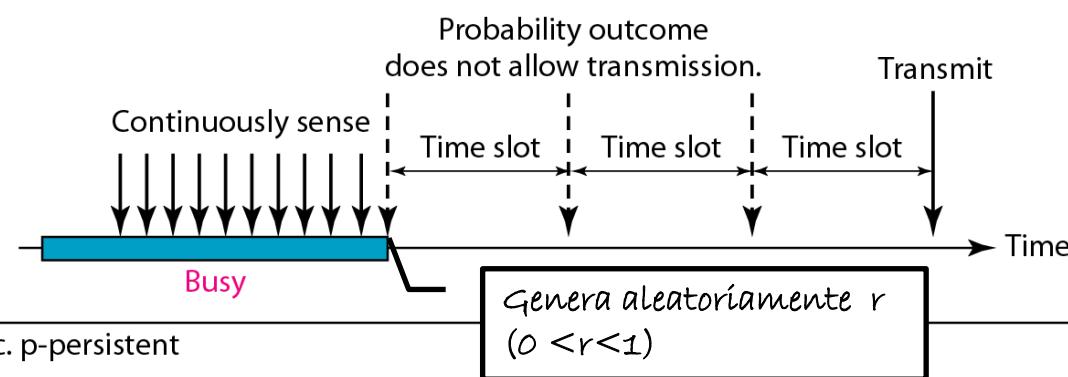
a. 1-persistent

CSMA no-persistent



b. Nonpersistent

CSMA p-persistent



c. p-persistent

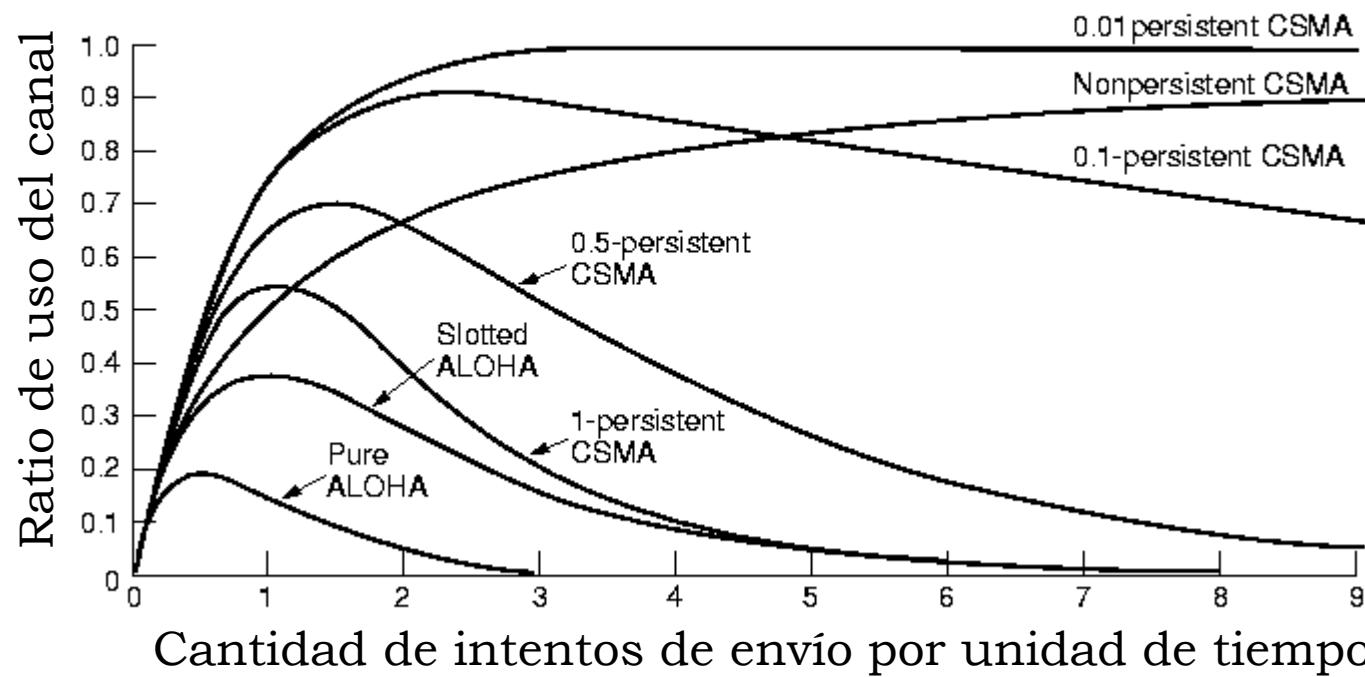
Espera hasta que esté libre comprobando continuamente si esta libre

Espera un tiempo aleatorio antes de volver a detectar si está libre
Intenta evitar que dos o más que estaban a la espera, empiecen a transmitir justo a la vez

El tiempo se divide en intervalos
Se espera hasta que esté libre
Al liberarse el canal se transmite con una probabilidad **p**:
 1. Se genera una **r**.
 2. Si **r ≤ p** transmite.
 3. En otro caso se espera al siguiente intervalo y vuelta a 1

Protocolos basados en CSMA

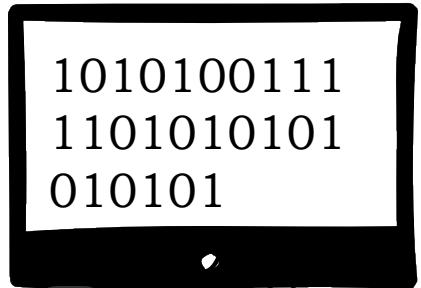
- Gráfico de eficiencia



Protocolos basados en CSMA

- CSMA-CD
 - *Carrier Sense Multiple Access with Collision Detection*
 - Se basa en que las estaciones abortan la transmisión tan pronto como detectan una colisión
 - En los protocolos anteriores las tramas se transmiten enteras
- Funcionamiento
 - Cuando se quiere transmitir
 - Si el canal está libre, se transmite
 - Si el canal está ocupado, se espera hasta que esté libre (1-persistencia)
 - Si se detecta colisión
 - Se transmite una señal corta de interferencia para informar al resto de estaciones (señal de **jamming**)
 - Y se espera un tiempo aleatorio antes de empezar de nuevo

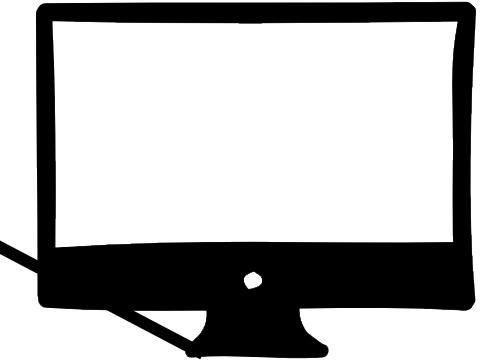
¿Cómo se detecta una Colisión?



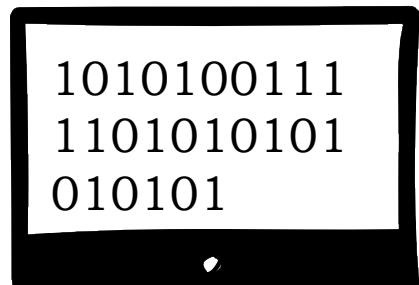
Mientras
envía,
compara ...

10011110101010101010101

... si ambas señales
son las mismas no
ha habido colisión

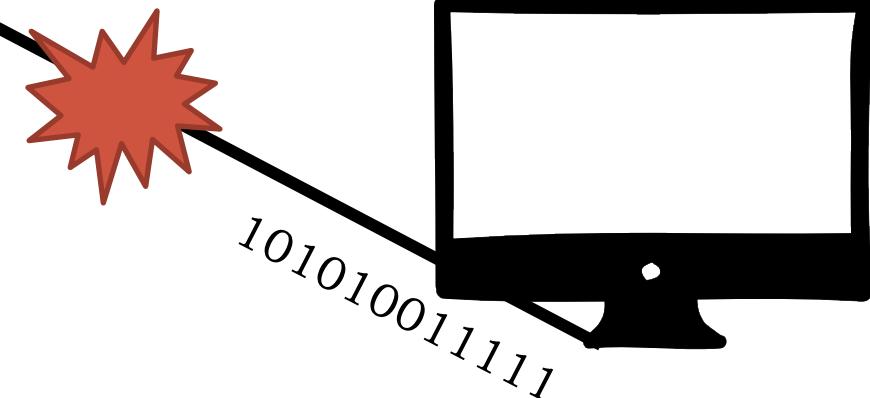


¿Cómo se detecta una Colisión?



Pero si otra
estación también
envía ...

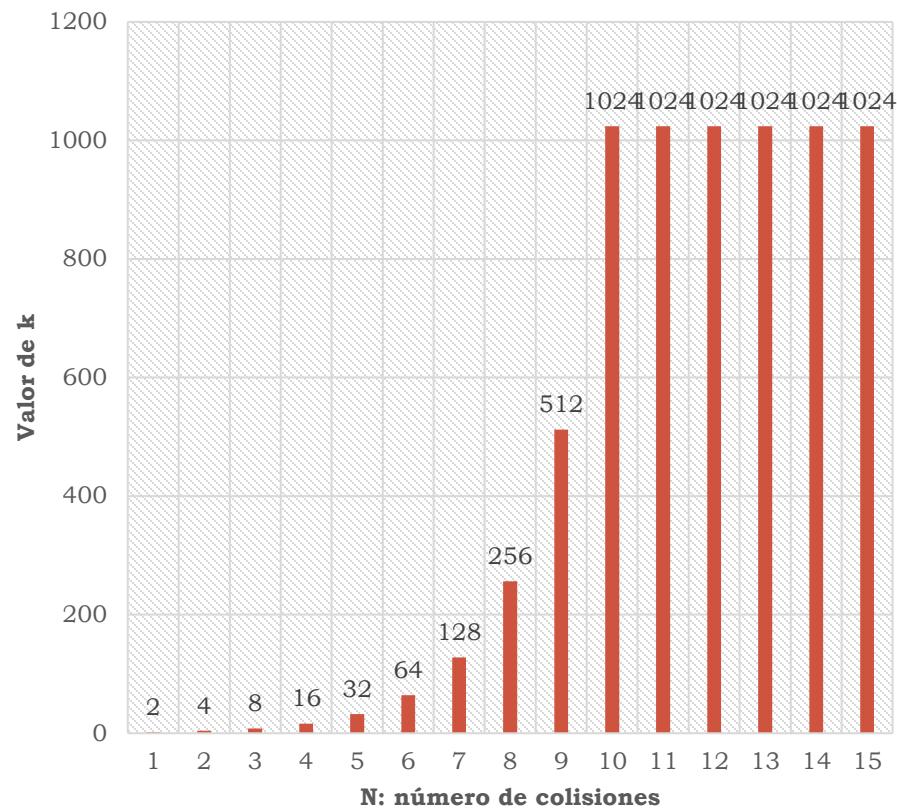
... las señales se
mezclarán, y
detectará la
colisión



Protocolos basados en CSMA

- CSMA-CD: Algoritmo de retroceso exponencial binario (Backoff)
 - Se utiliza para definir las esperas en caso de colisión
 - Si el paquete ha colisionado $n < 16$ veces seguidas
 - El nodo selecciona un número aleatorio k con igual probabilidad del conjunto $\{0, 1, 2, 3, \dots, 2^m\}$, donde $m := \min[10, n]$
 - El nodo espera $512 * k$ tiempos de bit (a 10 Mbps, 1 tiempo de bit es 10^{-7} segundos)
 - Si $n = 16$, se abandona la transmisión

Intervalo de espera algoritmo de backoff



Protocolos basados en CSMA

- CSMA-CD: Algoritmo de retroceso exponencial binario
- Análisis
 - Si hay pocas colisiones, la espera es pequeña
 - Si hay muchas colisiones, espera razonable que crece poco a poco
 - Si el tiempo de espera fuera fijo y muy grande
 - Pocas colisiones, pero las que hay introducen mucho retraso
 - Si el tiempo de espera fuera fijo y pequeño
 - Muchas colisiones
- Consecuencia
 - Las tramas deben ser lo suficientemente largas para que se detecte una colisión antes de que finalice la transmisión
 - En caso contrario, las prestaciones son las mismas que CSMA

Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet



IEEE 802 STANDARDS

802.1 Covers network management, etc.

802.2 Specifies the data link layer for the following access methods...

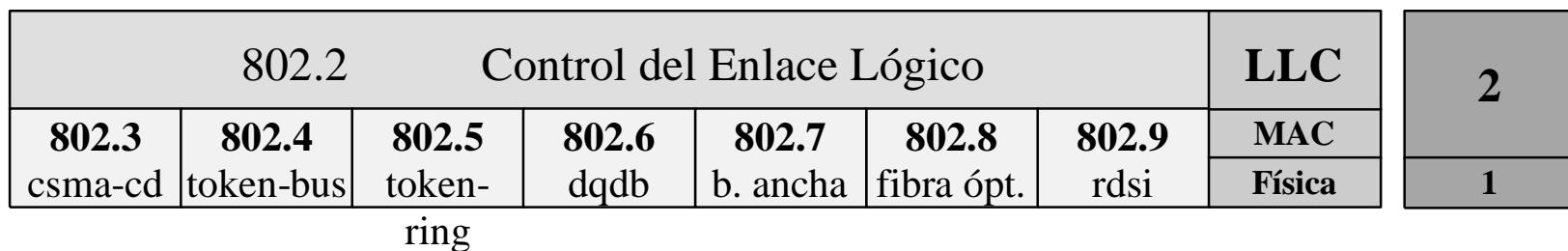
| | | | |
|--|--|----------------------------|--------------------------|
| 802.3 CSMA/CD Ethernet | 802.4 token bus | 802.5 token ring | 802.6 DQDB MAN |
| 802.3u CSMA/CD Fast Ethernet | | | |
| 802.3z CSMA/CD Gigabit Ethernet | | | |
| 802.3ae 10 Gigabit Ethernet | 802.12 Demand priority 100VG - AnyLAN | | |

REDES DE ÁREA LOCAL IEEE 802

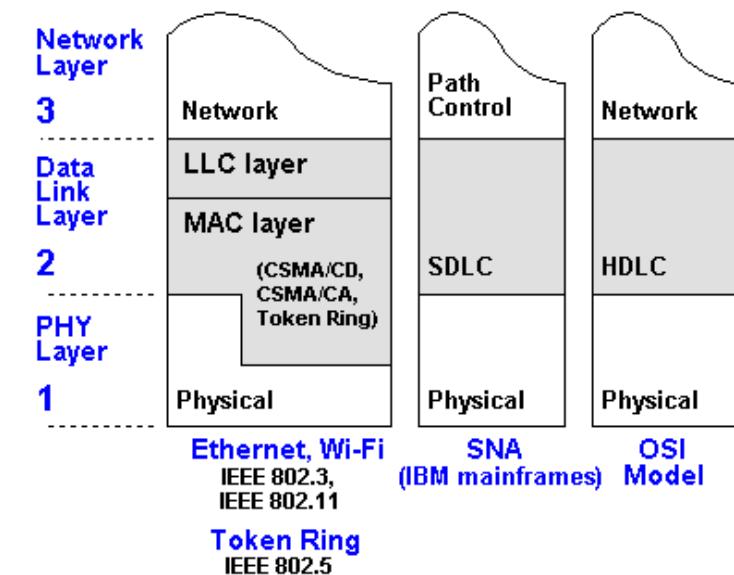
Redes de área local IEEE 802

- El estándar IEEE 802

IEEE 802.x



- **MAC (*Medium Access Control*)**
 - Control de Acceso al Medio
- **LLC (*Logical Link Control*)**
 - Control del Enlace Lógico

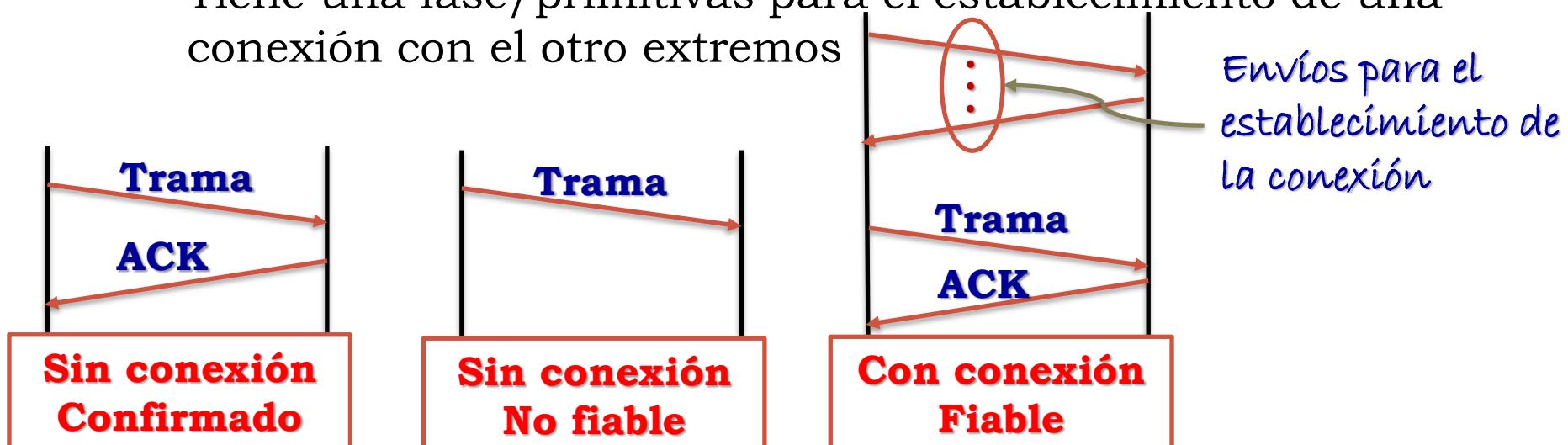


Redes de área local IEEE 802

- En el estándar IEEE 802
 - El protocolo MAC regula el acceso al canal dando a cada nodo la posibilidad de transmitir sus paquetes
 - El protocolo LLC proporciona los servicios de transmisión de paquetes entre nodos
 - Un mismo LLC puede residir sobre distintos protocolos MAC
 - Las LANs especificadas por el estándar IEEE 802 son compatibles en los niveles superiores a LLC
 - Se diferencian en la capa física (características del equipo de transmisión) y en el protocolo MAC

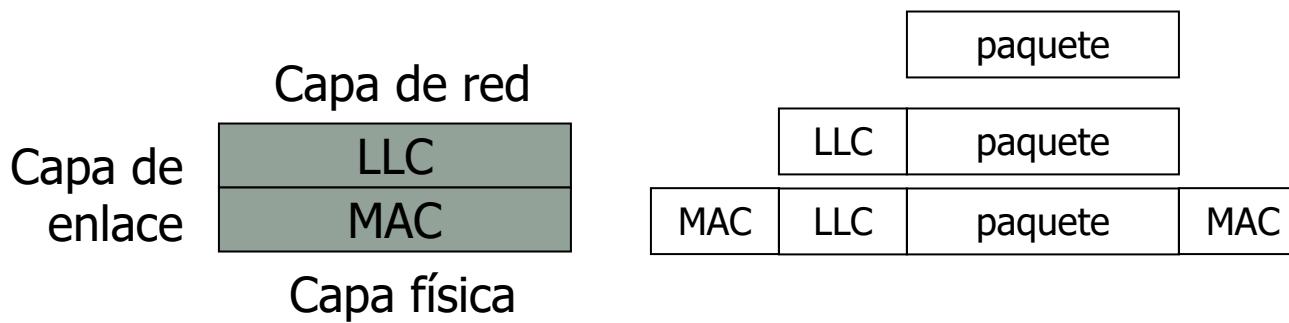
Redes de área local IEEE 802

- 802.2 : Servicios que ofrece LLC (tres)
 - Servicio sin conexión confirmado
 - No se puede enviar una trama si no se ha confirmado la anterior
 - Servicio sin conexión no fiable
 - No se garantiza que el paquete llegue bien a su destino
 - Servicio orientado a la conexión fiable
 - Tiene una fase/primitivas para el establecimiento de una conexión con el otro extremo



Redes de área local IEEE 802

- La capa LLC (*Logical Link Control*) ofrece una interfaz entre la capa de red y la capa MAC

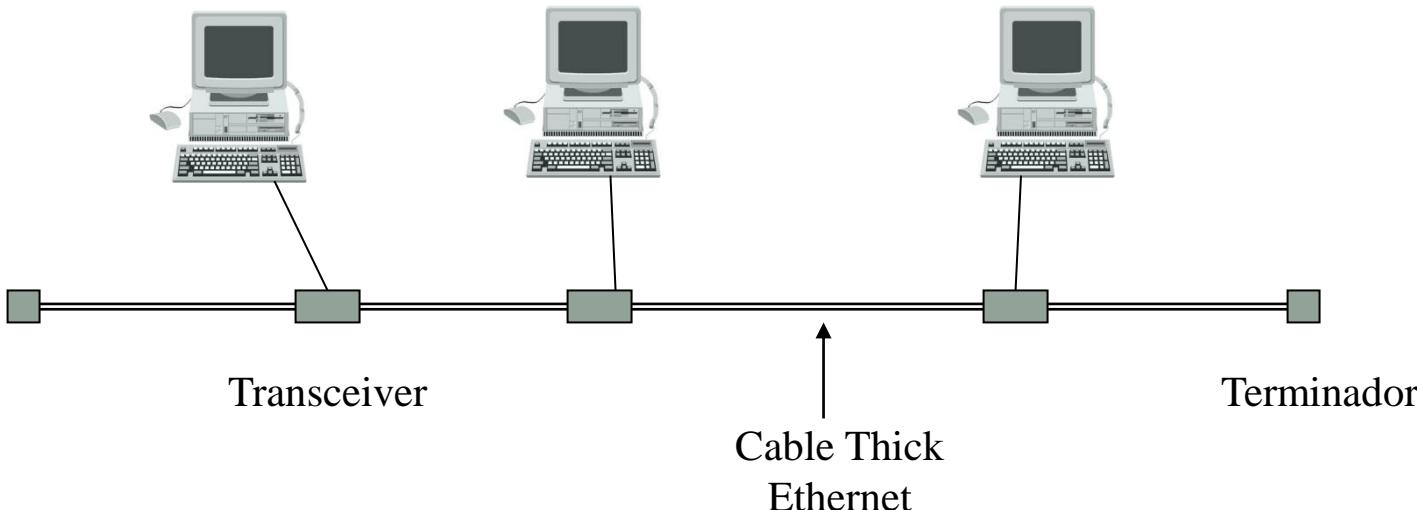


- En general, las redes LAN y MAN ofrecen un servicio de datagrama de tipo *best-effort en la capa de red*
 - No hay garantías de que la comunicación sea fiable



Red IEEE 802.3 (Ethernet)

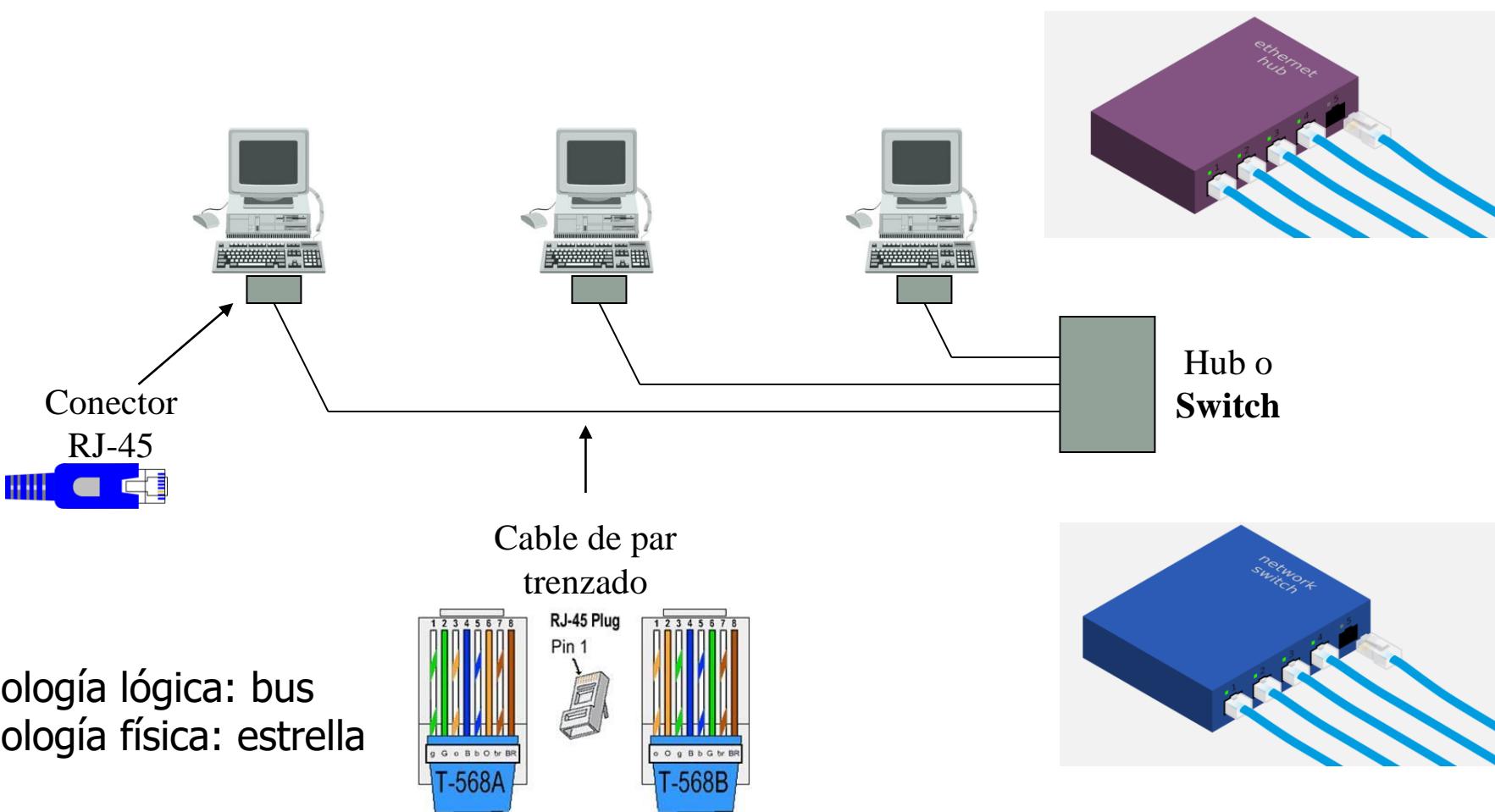
- El estándar IEEE 802.3 define la red Ethernet
 - Es la red más usada hoy día (versión Fast o Gigabit Eth.)
 - Fue desarrollada por Xerox en los años 70
 - Tradicionalmente la red tenía topología de bus
 - Usa un protocolo MAC de tipo CSMA-CD





Red IEEE 802.3 (Ethernet)

- Ethernet con par trenzado



Red IEEE 802.3 (Ethernet)

- Formato de la trama Ethernet II

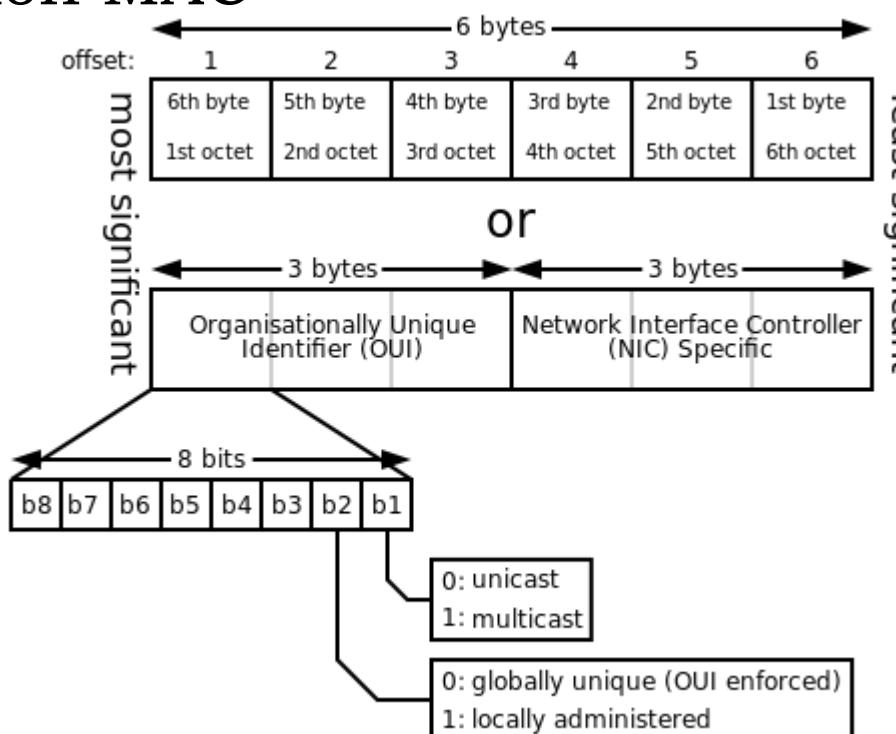
Formato de trama Ethernet II

| Preámbulo | Dirección de destino | Dirección de origen | Tipo de trama | Datos | FCS |
|-----------|----------------------|---------------------|---------------|------------------|-----------|
| 8 octetos | 6 octetos | 6 octetos | 2 octetos | 46- 1500 octetos | 4 octetos |

- Preámbulo:** 7 bytes para sincronizar + 1 inicio de trama
- Direcciones MAC origen y destino**
- Tipo de trama:** Protocolo de nivel superior que encapsula la trama. En algunas implementaciones es la longitud.
- Datos** del protocolo encapsulado (puede ser necesario “relleno/padding”)
- Control de errores:** CRC

Red IEEE 802.3 (Ethernet)

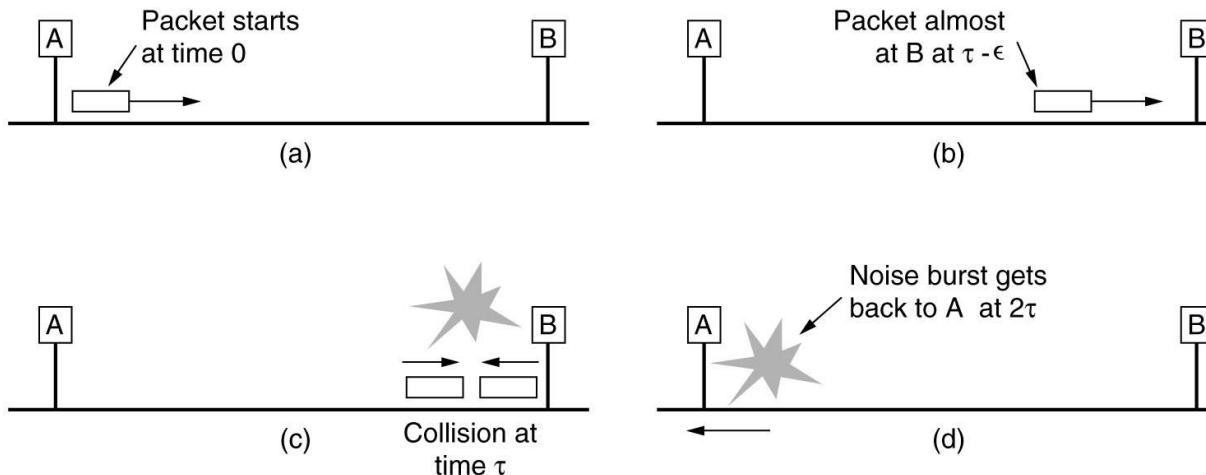
- Dirección MAC



- 3 primeros bytes: fabricante:
 - Menos significativo: Un equipo (0) o muchos (1)
 - Segundo menos significativo: Global (0) o local (1)
- 3 últimos: identificador de la tarjeta

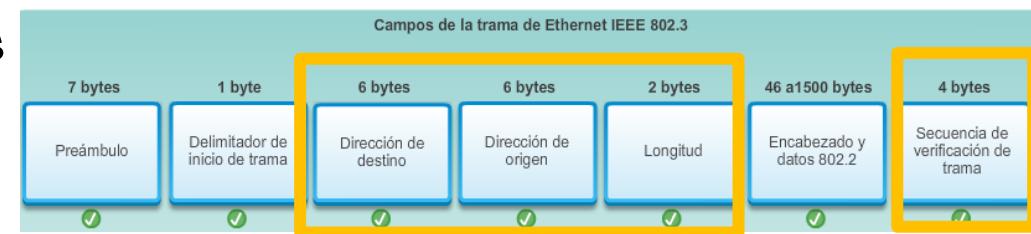
Red IEEE 802.3 (Ethernet)

- ¿Porqué hay un campo de relleno?
 - En CSMA/CD hay que detectar las colisiones:
 - El emisor es el encargado de detectarlas, escuchando y comparando mientras transmite
 - las tramas tienen que ser lo suficiente largas como para detectar colisiones



Red IEEE 802.3 (Ethernet)

- Análisis:
 - En la red Ethernet:
 - Velocidad de transmisión: 10Mbps
 - Longitud máxima del cable: 2500 m (5 secciones de 500 m con 4 repetidores)
 - Round-trip time: 50 microsegundos en el peor caso (estaciones en ambos extremos)
 - La trama tiene que transmitirse al menos durante 50 microsegundos
 - A 10 Mbps, un bit se trasmite en 100nseg
 - La trama tiene que al menos tener 500 bits
 - → Se redondea a 512 bits (**64 bytes**)
 - Longitud CABECERA: $6 + 6 + 2 + 4 = 18$
 - Pad: $64 - 18 = 46$ bytes



Red IEEE 802.3 (Ethernet)

- Se debe cumplir que $T_{trans} > 2 * T_{prop} + T_{trans-jamming}$
 - El emisor envía un paquete y el receptor al final del enlace es el que detecta la colisión
 - El receptor tiene en transmitir la señal de *jamming* y esta tiene que llegar al emisor antes de termine de enviar la trama
 - Ese tiempo de transmisión mínimo se conoce como tiempo de rodaja

Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet

REDES INALÁMBRICAS (WIFI Y BLUETOOTH)

Protocolos para redes inalámbricas

- Las redes locales inalámbricas son cada vez más habituales
- Todas comparten el medio: ondas de radio
- Al más alto nivel, podemos clasificar las redes inalámbricas de acuerdo a dos criterios:
 - Si un paquete cruza la red inalámbrica exactamente en un salto (inalámbrico) (single hop) o en múltiples saltos (inalámbricos) (multiple hop)
 - Si hay una infraestructura, como una estación base, en la red

| | Single hop | Multiple hops |
|---------------------|--------------------------|---|
| Infraestructura | WIFI, WIMAX, 3G | ZIGBEE red MESH (de malla) de sensores |
| Sin Infraestructura | Bluetooth WIFI ad hoc | Redes MANET y VANET |

Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet

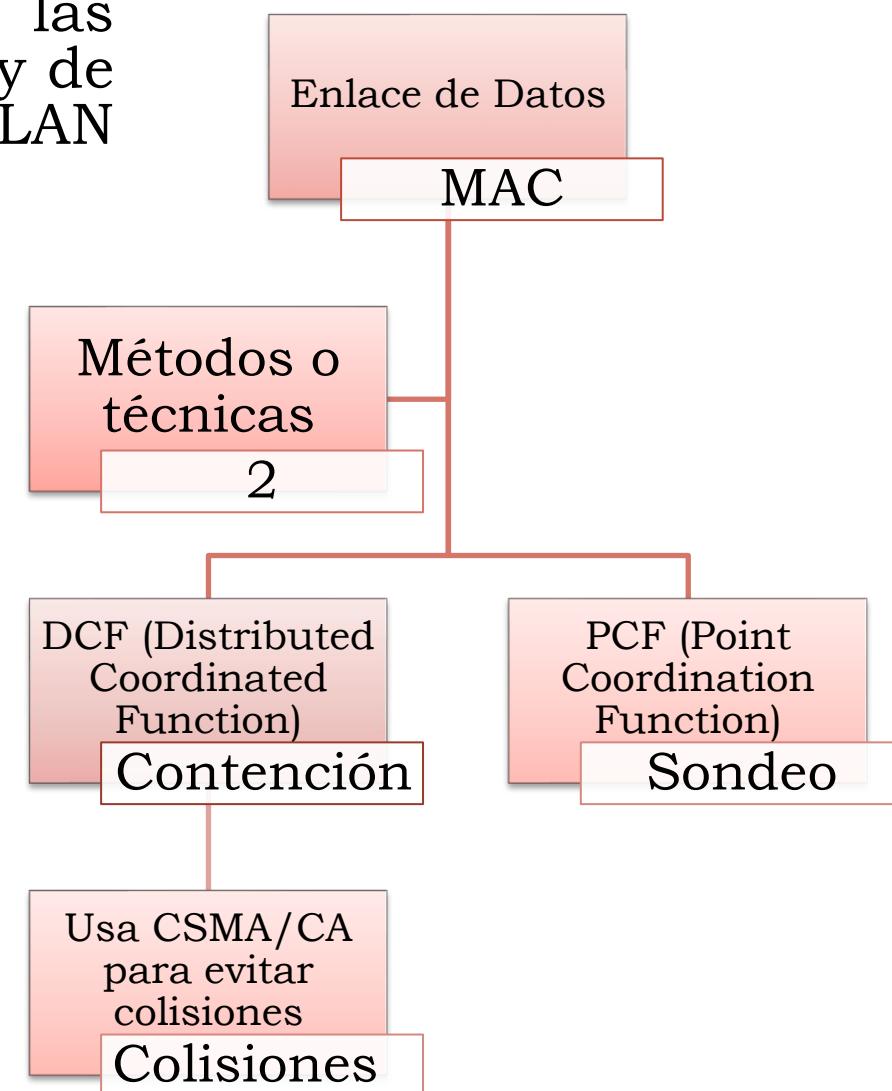
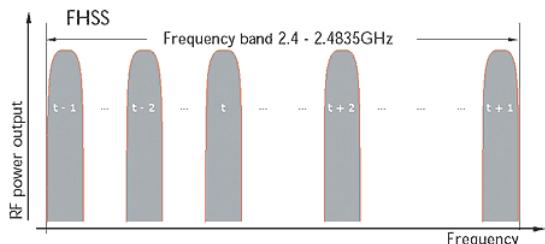
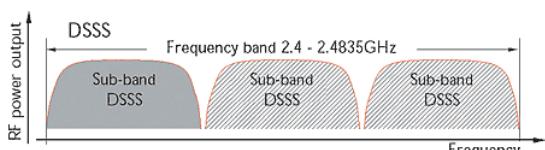
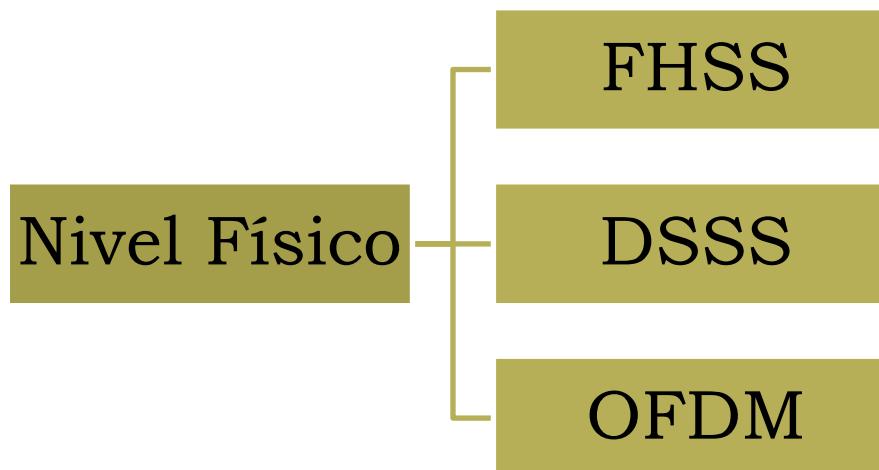


**802.11
(WIFI)**



LAN Inalámbricas: WIFI

- IEEE 802.11 → Define las especificaciones del nivel físico y de enlace de datos para una LAN inalámbrica:



LAN Inalámbricas: WIFI: Frecuencias y Canales

- La tecnología WiFi utiliza dos bandas de frecuencia (2.4 GHz y 5 GHz), con 11 y 40 canales cada una respectivamente
- Al utilizar una frecuencia de 2.4 GHz, todos los dispositivos se agolpan esperando su turno
 - Las interferencias llegan a un punto en el que afectan la velocidad

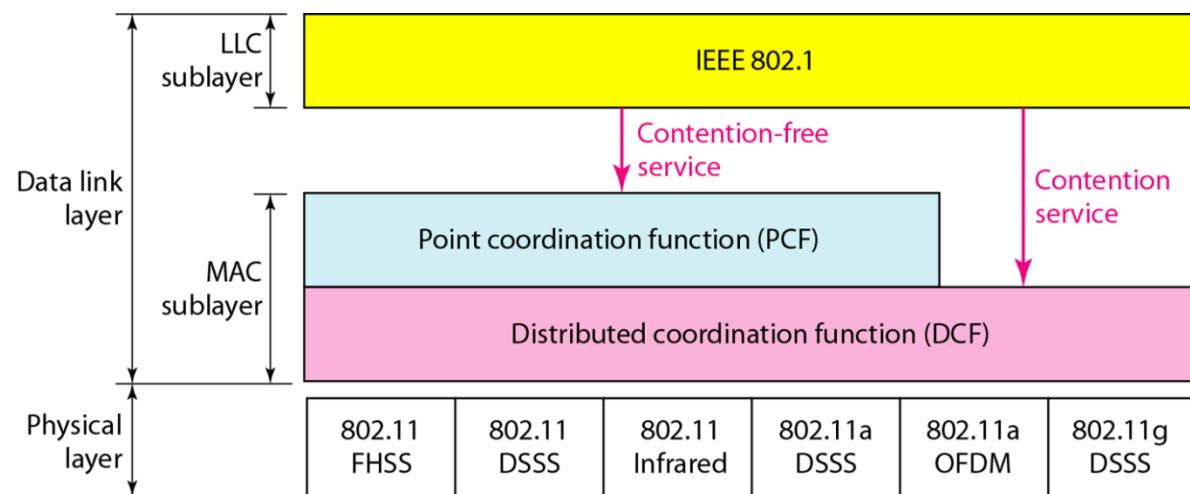


LAN Inalámbricas: WIFI: Frecuencias y Canales

| | Ventajas | Desventajas |
|---------|--|---|
| 2.4 GHz | <ul style="list-style-type: none">✓ Accesible desde mayores distancias✓ Compatible con una gran cantidad de dispositivos | <ul style="list-style-type: none">✓ Frecuencia muy usada por todos los dispositivos que admite |
| 5 GHz | <ul style="list-style-type: none">✓ Mucho más ancho de banda✓ Generalmente menos interferencias en 5 GHz porque la frecuencia no está tan demandada | <ul style="list-style-type: none">✓ Disponible para distancias más cortas✓ No admite tantos dispositivos |

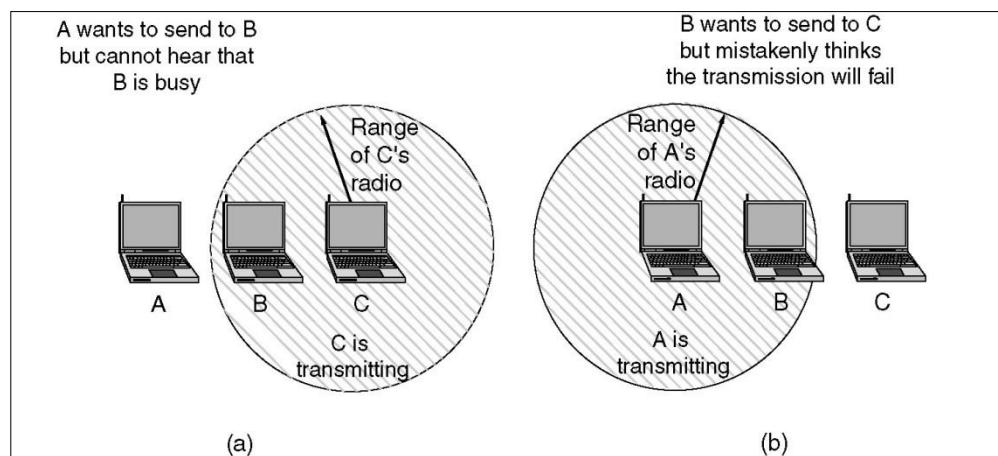
Redes IEEE 802.11: Subnivel MAC

- Se definen dos subniveles MAC
 - La función de coordinación distribuida (DCF)
 - Por contención con detección de portadora
 - Utiliza CSMA como método de acceso
 - Dos modos de detección de la ocupación canal : Físico (Physical Channel Sensing) o Virtual (Virtual Channel Sensing)
 - La función de coordinación puntual (PFC) (*OPCIONAL*)
 - Mecanismo de acceso centralizado por sondeo (punto de acceso)



Redes IEEE 802.11: Dificultades

- En la función de coordinación distribuida (DCF) CSMA-CD (IEEE 802.3) no es aplicable directamente:
 - Dificultades para implementar detección de colisiones
 - Para poder detectar la colisión es necesario poder enviar y recibir a la vez → Es costoso de implementar en las tarjetas inalámbricas
 - La señal que se envía tiene mucha más energía que la que se recibe
 - Problemas por la cobertura, no existen en las redes cableadas
 - Problema de la estación oculta



Redes IEEE 802.11: Protocolo MAC DCF

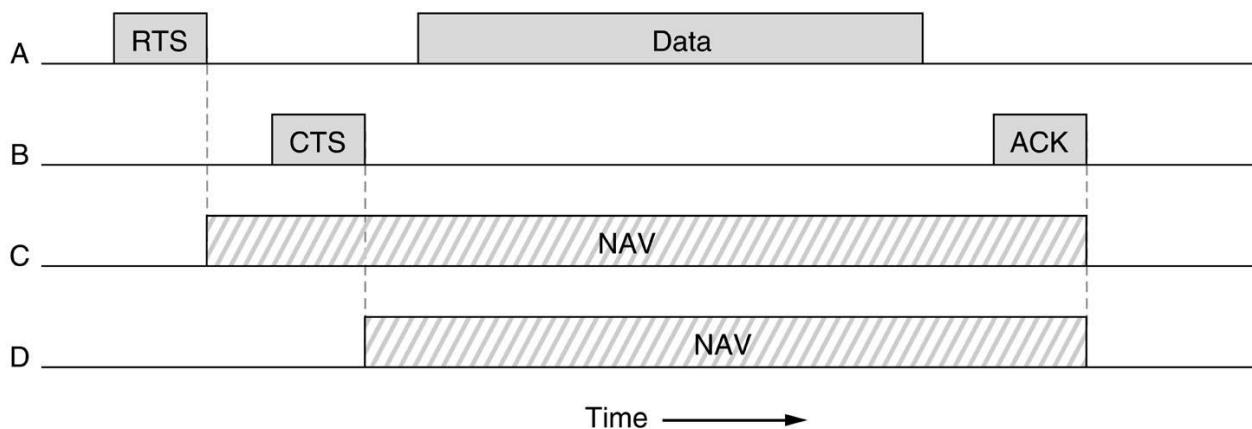
- Modo: *physical channel sensing*
 - Si una estación quiere transmitir escucha el medio
- Modo: *virtual channel sensing*
 - Uso de VECTOR DE ASIGNACIÓN DE RED
 - NAV → Network Access Vector
 - Las estaciones al enviar incluyen el tiempo que necesita ocupar el canal
 - Las estaciones que quieren transmitir crean un temporizador denominado NAV que determina cuando tiempo debe de pasar antes de poder comprobar si el canal está libre
 - Por tanto, antes de comprobar si el medio está libre, comprueba su NAV para ver si ha expirado (ahorro de energía)

Redes IEEE 802.11: Protocolo MAC DCF

- Si una estación quiere transmitir escucha el medio/mira su NAV
 - Si está libre transmite
 - Si no está libre espera a que finalice la transmisión en curso
 - Si hay colisión: retroceso exponencial binario
- ¿Cómo sabe si hay colisión?
 - Introduce mensajes de confirmación (ACK) en la capa de enlace
 - De otro modo, los mensajes perdidos se detectan en la capa de transporte, lo que introduce mucho retardo (se producen más errores que en redes cableadas)
 - Ajustes en el uso del algoritmo de retroceso exponencial binario

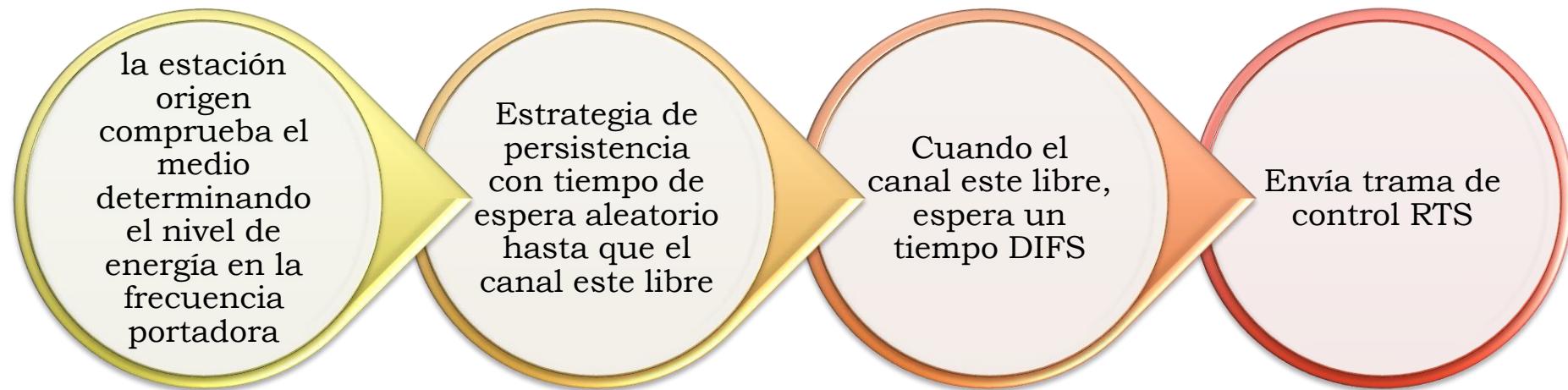
Redes IEEE 802.11: Protocolo MAC DCF

- Protocolo tipo MACAW (MACA for Wireless)
 - *Multiple Access with Collision Avoidance*
 - Idea básica: informar previamente con un pequeño paquete (RTS) indicando que se quiere enviar un paquete de datos por parte del emisor y confirmar (paquete CTS) por parte del receptor
 - CSMA/CA: Variante de MACAW



Redes IEEE 802.11: CSMA/CA

Cuando una estación quiere transmitir y antes de enviar la trama ...



DIFS → tiempo de espera de espacio entre tramas distribuido
(Distributed InterFrame Space)

RTS → trama de Petición de Envío (Request To Send)
(contiene la longitud de la trama de datos) necesario para calcular el NAV

Redes IEEE 802.11: CSMA/CA

Mientras la estación destino ...



SIFS → tiempo de espera espacio corto entre tramas
(Short InterFrame Space)

CTS → trama de Permiso para Enviar(Clear To Send)
(contiene la longitud de la trama de datos)

Redes IEEE 802.11: CSMA/CA

De nuevo, en la estación origen ...



Y en la estación destino ...



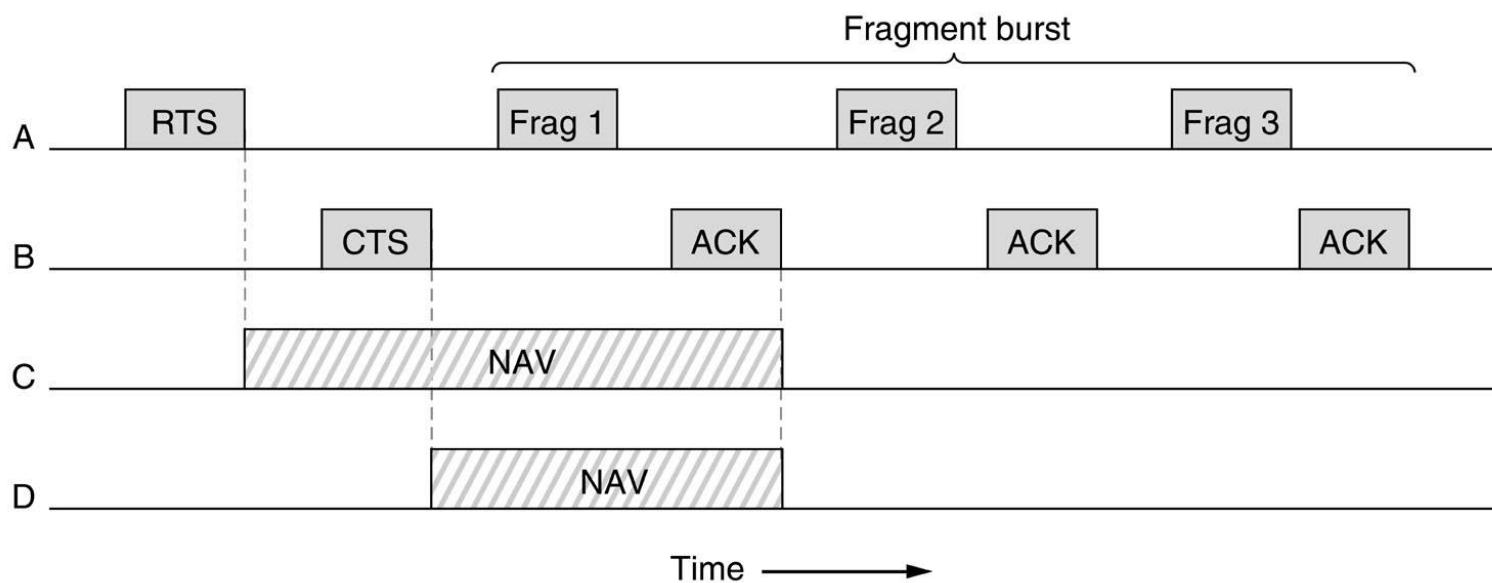
¿Cómo se evita la colisión? ... ¿y si hay colisión?

- ¿Cómo aplaza una estación el envío de datos si una estación adquiere el acceso?
 - Mediante el NAV y su activación al escuchar los RTS/CTS
- ¿Qué ocurre si hay colisión mientras la tramas RTS/CTS están en transición (periodo de acuerdo)?
 - Dos o más estaciones pueden enviar tramas RTS al mismo tiempo y pueden colisionar
 - Debido a que no hay forma de evitar la colisión, el EMISOR(es) asume que se ha producido si no recibe una trama CTS del RECEPTOR
 - Se espera un tiempo según la estrategia de espera aleatoria y se comienza de nuevo

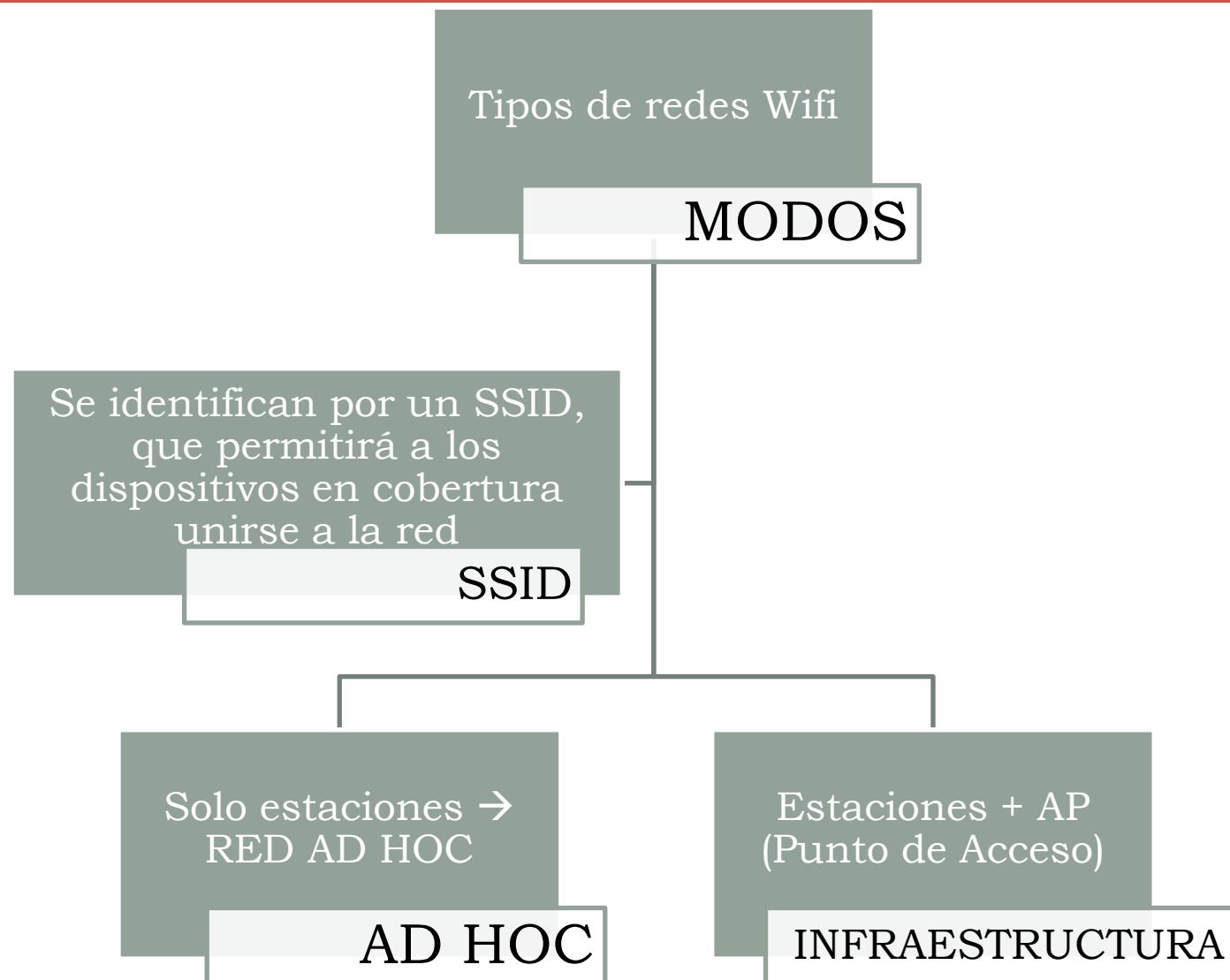


Redes IEEE 802.11

- Además, dado que el número de colisiones puede ser alto y para minimizar el impacto de la retransmisión
→ Los paquetes se pueden fragmentar
 - Se usa un protocolo de parada y espera



Arquitectura Wifi



Redes IEEE 802.11: Identificación de Wifi

SSID (Service Set Identifier) es el nombre que identifica una red inalámbrica Wifi

- Va incluido en las tramas de forma que pueda ser identificado como parte de ella.

Formado por un máximo de 32 caracteres ASCII

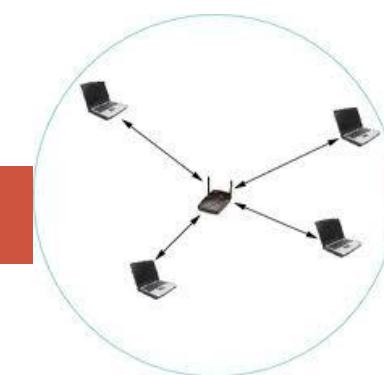
- de forma típica encontramos una combinación de letras y números.

Los dispositivos que quieren comunicarse entre sí deben tener el mismo SSID.

- El SSID puede ser o no visible según si está habilitada su difusión.



Redes IEEE 802.11: Modos de redes Wifi



- Modo Ad hoc
 - Es una red aislada y no puede enviar datos a otras redes
 - Las estaciones pueden formar una red, localizarse y acordar formar una red Ad hoc → Wifi Direct
- Modos Infraestructura
 - Estaciones + AP (punto de acceso)
 - Requerido para que todos los dispositivos se conecten y comuniquen





Redes IEEE 802.11: Concepto de BSS

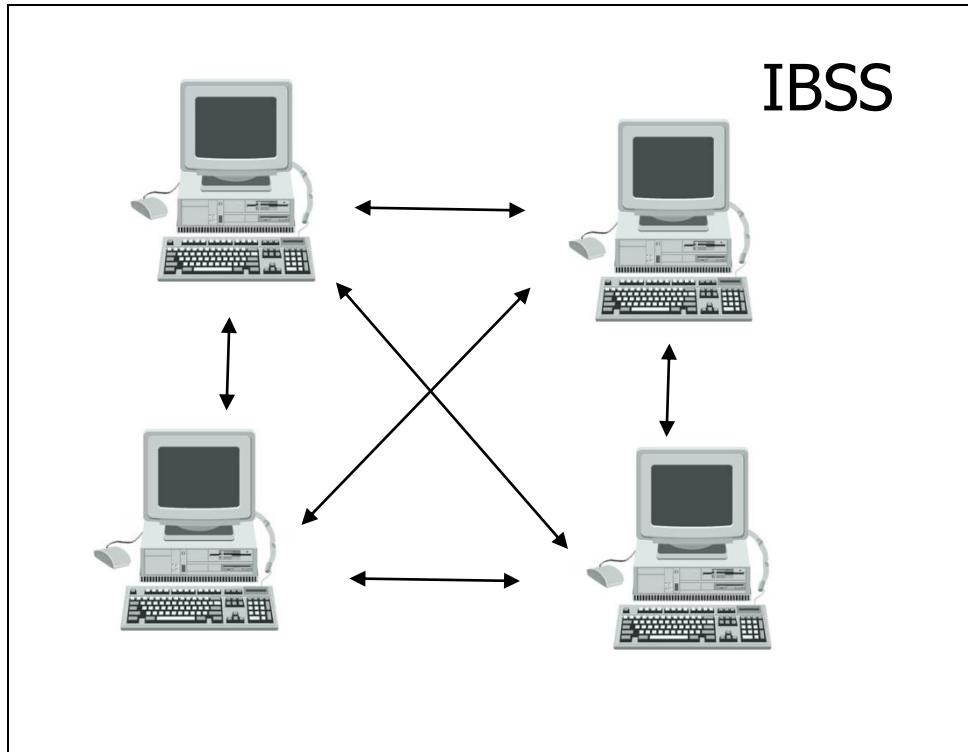
- Un Conjunto Básico de Servicios (BSS – Basic Service Set) es un grupo de estaciones que se comunican entre sí
- Un BSS se compone de
 - estaciones móviles o fijas
 - una estación base opcional → PUNTO DE ACCESO
- Arquitectura ad hoc
 - Un conjunto BSS sin AP
 - es una red aislada y no puede enviar datos a otros BSS
 - Las estaciones pueden formar una red, localizarse y acordar formar una BSS
- Red con Infraestructura
 - BSS con AP

BSS: Conjunto de servicios básico
AP: Punto de acceso



Redes IEEE 802.11

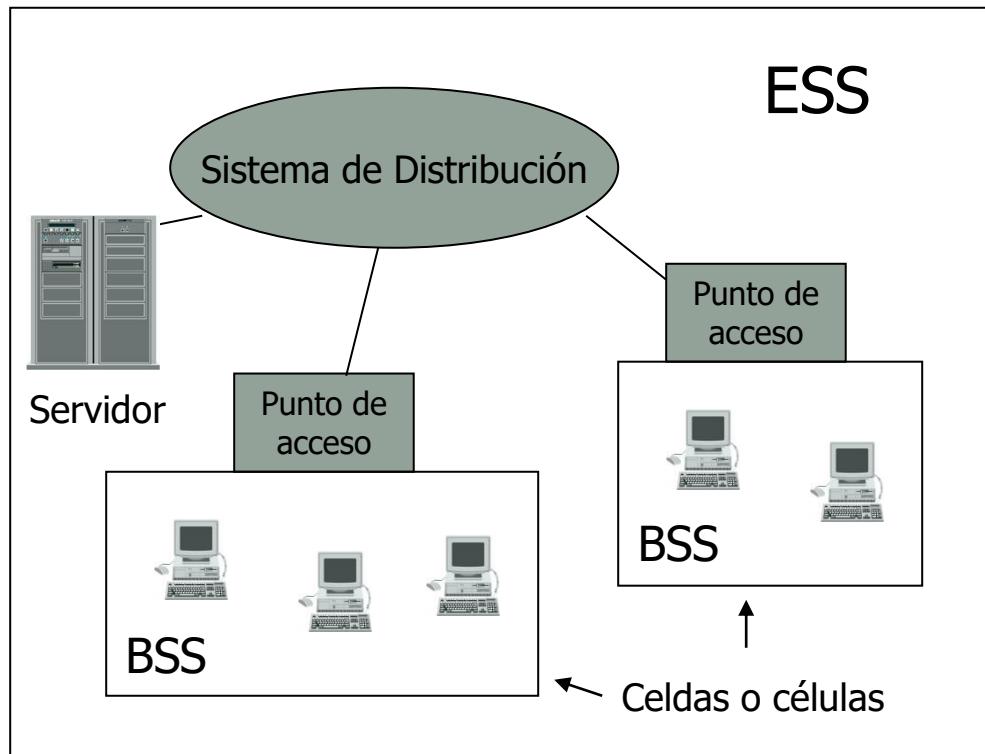
- Arquitectura: modo Ad hoc



IBSS:
Conjunto de Servicios
Básico Independiente

Redes IEEE 802.11

- Arquitectura: modo Infraestructura
- Dos o más BSS pueden unirse a través de un sistema de distribución para formar un ESS

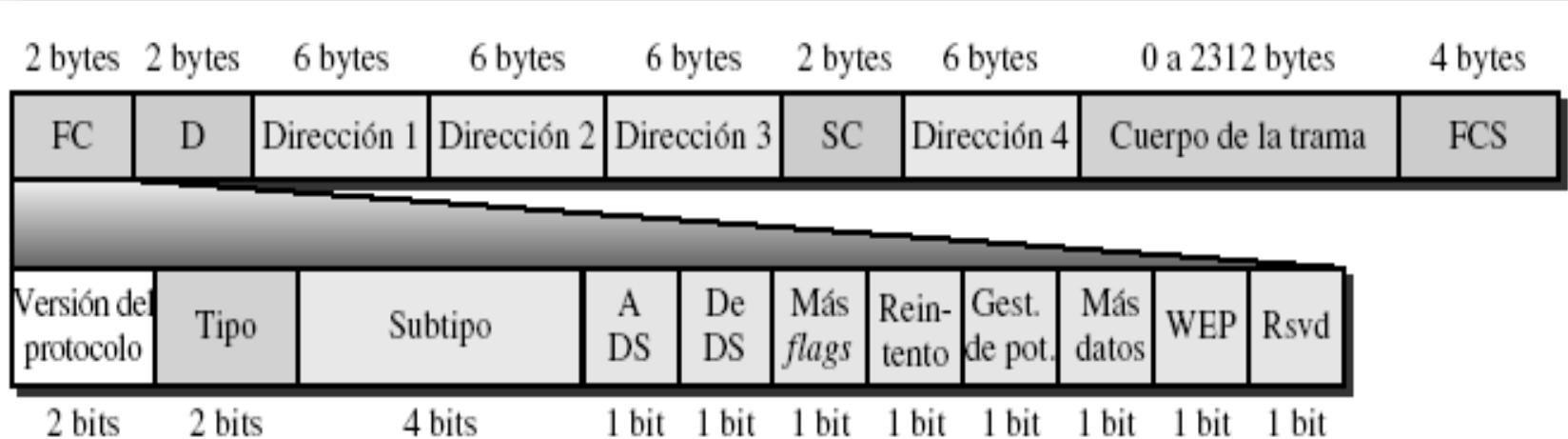


BSS:
Conjunto de servicios básico

ESS:
Conjunto de servicios extendido

Redes IEEE 802.11: Trama

- Más compleja que la de Ethernet (802.3)
 - Algunos campos son opcionales (dependen del tipo):
 - Tipo 0: Gestión: Authentication, Beacon, Probe...
 - Tipo 1: Control: RTS, CTS, ACK
 - Tipo 2: Datos
 - Versiones recientes reducen el cuerpo de la trama para añadir más campos



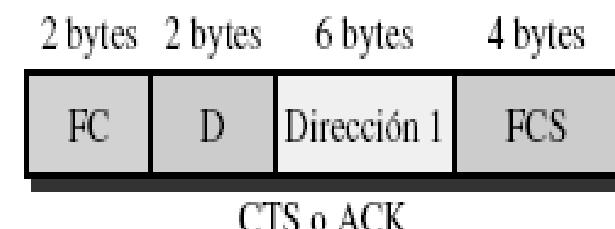
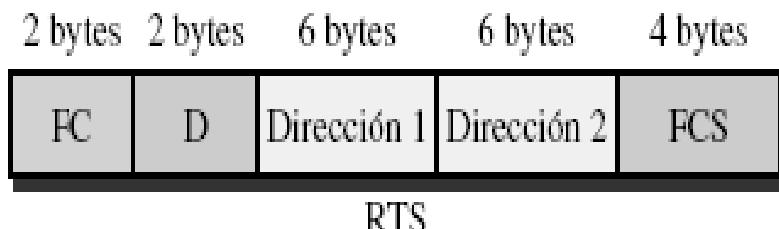
Redes IEEE 802.11: Trama

- FC (*frame control*): 2 Bytes – Tipo e información control

| Campo | Explicación |
|---------------------|--|
| Versión | La versión actual (802.11) es la 0 |
| Tipo | Tipo de Información: gestión (00), control (01) o datos (10) |
| Subtipo | Subtipo de los tipos anteriores |
| A DS | = {0, 1} |
| DE DS | = {0, 1} |
| Más flags | = 1, más fragmentos |
| Reintento | = 1, trama retransmitida |
| Gestión de Potencia | = 1, la estación está en modo gestión de potencia |
| Más Datos | = 1, la estación tiene datos que enviar |
| WEP | Intimidad equivalente a cable (cifrado implementado) |
| Rsvd | Reservado |

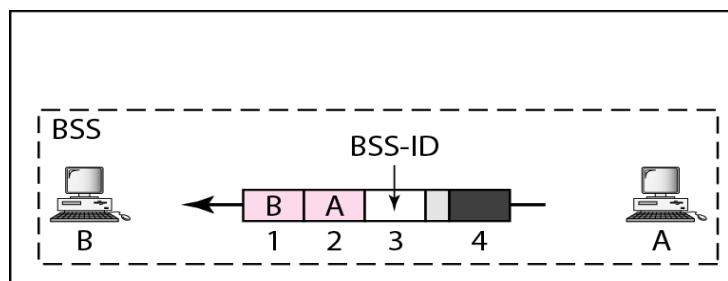
Redes IEEE 802.11: Trama

- D – 2 bytes
 - En las tramas de **datos, CTS y RTS** define la duración de la transmisión que se utiliza para fijar el NAV (en ms)
 - En la trama de **control** para el ahorro de energía, define el identificador de la estación.
- Direcciones – 4 campos de 6 bytes (6 x 4)
 - 4 campos de dirección cuyo significado depende de los campos A DS y De DS en el campo FC
- CS - Control de secuencia
 - Nº de secuencia del control de flujo
- Depende del tipo puede que algunas direcciones y el CS no aparezcan. Ej. (tramas de control):

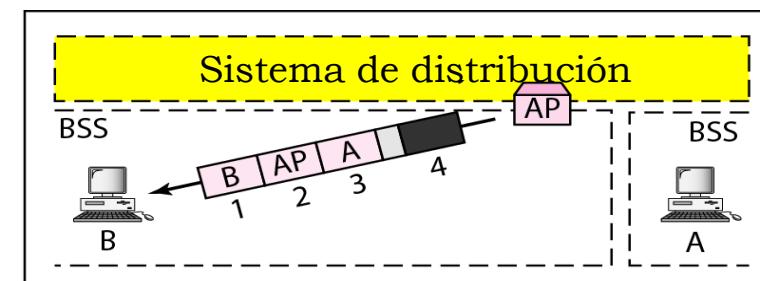


Redes IEEE 802.11: Trama - Direccionamiento

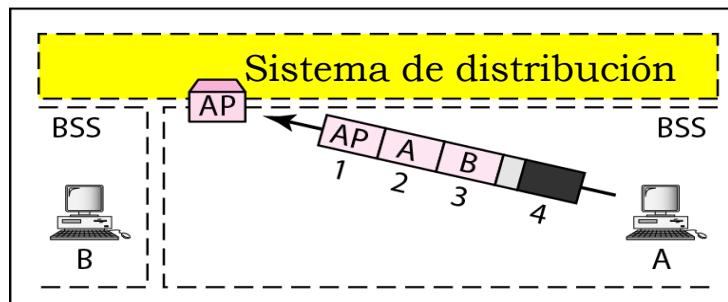
| A DS | DE DS | Dirección 1 | Dirección 2 | Dirección 3 | Dirección 4 |
|------|-------|-------------|-------------|-------------|-------------|
| 0 | 0 | Destino | Origen | ID de BSS | N/A |
| 0 | 1 | Destino | AP emisor | Origen | N/A |
| 1 | 0 | AP receptor | Origen | Destino | N/A |
| 1 | 1 | AP receptor | AP emisor | Destino | Origen |



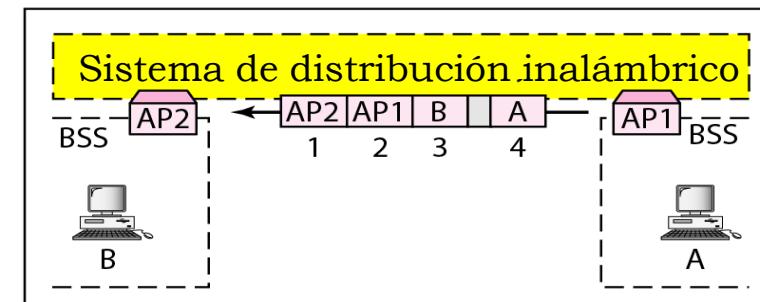
a. Caso 1



b. Caso 2



c. Caso 3



d. Caso 4

Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet

Red Inalámbrica de Área Personal **BLUETOOTH**



LANs inalámbricas de área personal (PAN): Bluetooth

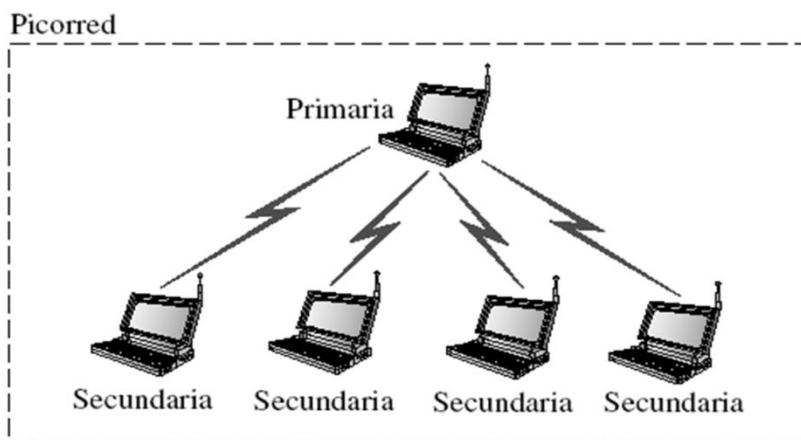
- Bluetooth:
 - Tecnología de LAN inalámbrica de área personal
 - Permite la conexión de dispositivos variados: teléfonos, portátiles, cámaras, impresoras, ...
 - Reemplazar cables en conexión de teclados, ratones o impresoras
 - Sensores conectados con dispositivo de monitorización para control de salud
 - Originalmente, proyecto de compañía Ericsson
 - Posteriormente se estandarizó como 802.15.1 (redes de área personal, PAN)
 - Red Ad hoc: se forma de manera espontánea
 - Dispositivos se encuentran unos a otros
 - Forman una picorred o red dispersa

LANs inalámbricas: Bluetooth

Piconet

Arquitectura picorred:

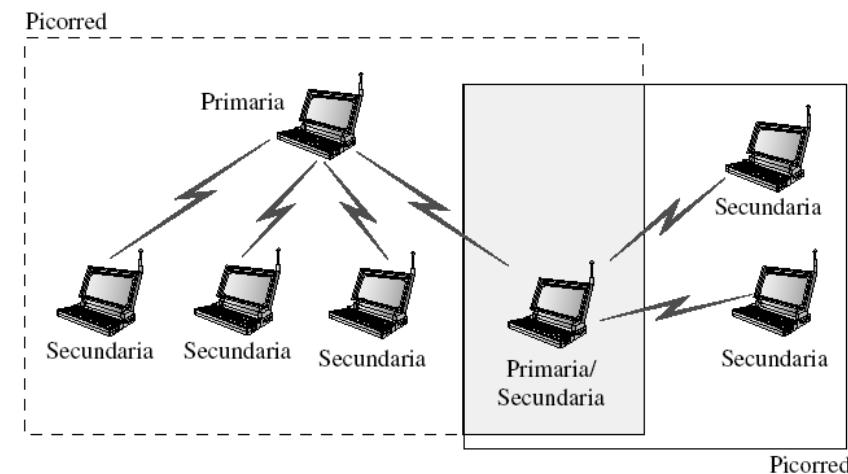
- Máximo 8 estaciones
- 1 estación actúa de primaria, el resto secundarias.



Scatternet

Arquitectura Red Dispersa

- Combinación de picorredes
- Una estación secundaria en una picorred actúa de primaria en otra
- Una estación puede ser miembro de dos picorredes



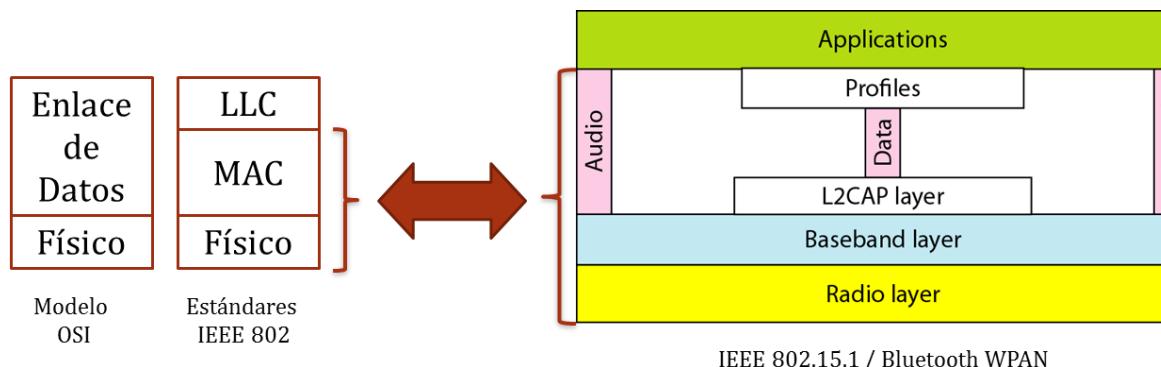
Picorred

Arquitectura de Protocolos

- Bluetooth ofrece una arquitectura en capas:
 - Protocolos básicos
 - Radio
 - Banda Base
 - Protocolo de Gestión del Enlace (LMP)
 - Protocolo de adaptación y gestión del enlace lógico (L2CAP)
 - Protocolo de Descubrimiento de Servicios (SDP)
 - Protocolos de control de telefonía y sustitución de cable
 - RFCOMM
 - AT
 - TCS BIN
 - Protocolos adoptados

LANs inalámbricas: Bluetooth

- Niveles en Bluetooth
 - No se corresponden exactamente con el modelo de Internet



- Nivel de radio
 - Aproximadamente equivalente a nivel físico
 - Emplea banda ISM de 2,4 GHZ, dividida en 79 canales de 1 MHz
 - Utiliza técnica de “espectro ensanchado por salto de frecuencias”
 - Los dispositivos cambian de frecuencia 1600 veces por segundo
 - Cada frecuencia es sólo utilizada durante $1/1600$ s ($625 \mu\text{s}$) antes de saltar a otra
 - Evita interferencias con otras redes
- **Requiere que todos los dispositivos de la piconred estén sincronizados**

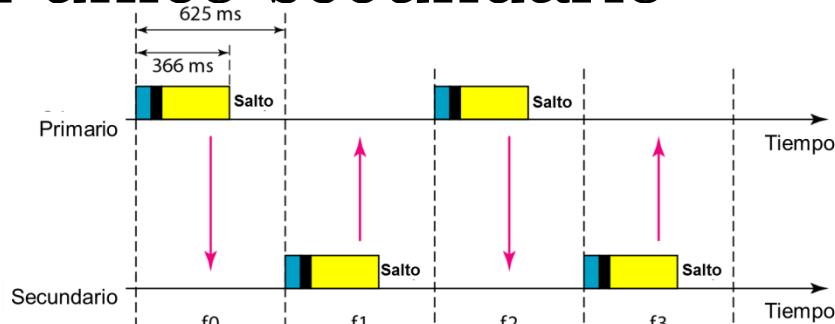
LANs inalámbricas: Bluetooth

- Nivel de banda base
 - Equivalente al subnivel MAC
 - establece conexión, direcciona, formato paquete, temporización y control de potencia
 - Las estaciones comparten en el tiempo el ancho de banda del canal
 - Método de acceso Síncrono → forma de TDMA (Acceso Múltiple por División en el Tiempo)
 - 1 ranura de tiempo = permanencia en una misma frecuencia
 - En 1 ranura, la estación primaria envía una trama a una secundaria o una secundaria a la primaria
 - Cada estación tiene asignada una ranura de tiempo durante el cual puede enviar datos
 - Las estaciones tienen que estar sincronizadas (conocer el comienzo y posición de su ranura)
 - El primario y el secundario se comunican usando ranuras.
 - La comunicación ocurre SÓLO entre el primario y el secundario
 - Los secundarios no pueden comunicarse directamente entre sí.

LANs inalámbricas: Bluetooth

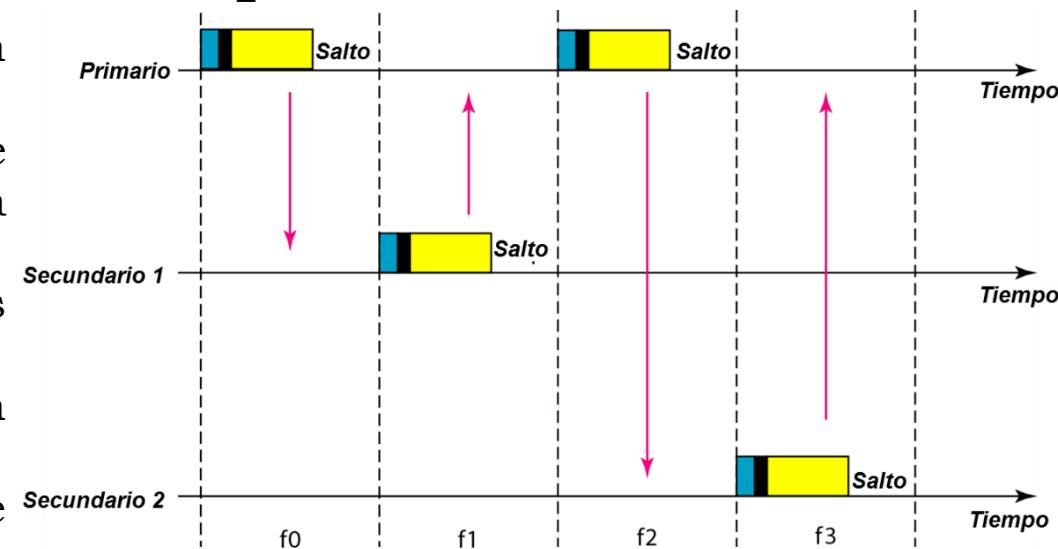
- Comunicación con un único secundario

- El primario utiliza ranuras con número par (0,2,4,...)
- y el secundario las impares (1,3,5,...)



- Comunicación con múltiples secundarios:

- El primario utiliza ranuras con número par
- El secundario envía en la siguiente ranura impar... sólo si la trama anterior llevaba su dirección
 - Todas las secundarias escuchan las ranuras pares
 - Sólo una secundaria envía en la siguiente ranura impar
- Método de muestreo con reserva de tiempo



LANs inalámbricas: Bluetooth

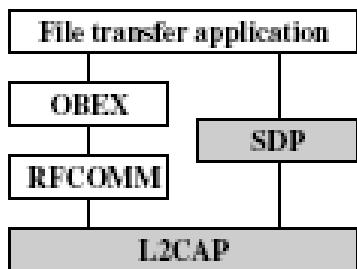
- Se pueden establecer dos tipos de enlace entre un dispositivo primario y otro secundario.
 - Enlace orientado a conexión síncrono (SCO)
 - Más importante evitar la latencia (retardo en entrega de datos) que integridad (entrega libre de errores)
 - Si se daña un paquete, nunca es retransmitido
 - Audio (tiempo real): llamada voz con Teléfono
 - Enlace no orientado a conexión asíncrono (ACL)
 - Integridad de datos más importante que latencia
 - Si la trama se corrompe, se retransmite
 - Datos

LANs inalámbricas: Bluetooth

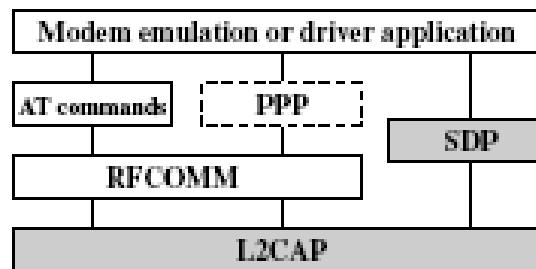
- L2CAP
 - Protocolo de control y adaptación del enlace lógico
 - Equivale a subnivel LLC en LAN
 - Responsabilidades: multiplexación, segmentación y reensamblado, calidad de servicio y gestión de grupos
- Niveles superiores: Bluetooth define protocolos específicos para cada propósito
 - RFCOMM
 - Perfiles Bluetooth
 - Describen un modelo de uso de los protocolos para un servicio determinado
 - Transferencia de ficheros entre dispositivos
 - Transferencia de audio (Auriculares)
 - Control de llamadas y transferencia de voz
 - Acceso a LAN (anclaje o tethering)



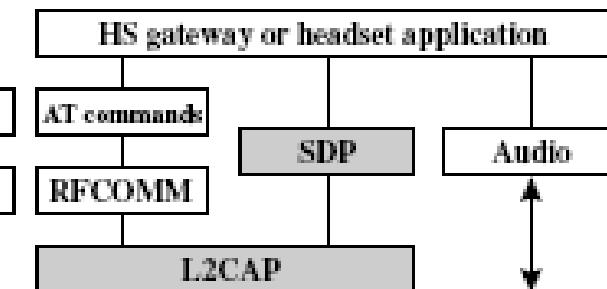
Perfiles Bluetooth - Modelos de Uso



(a) File transfer

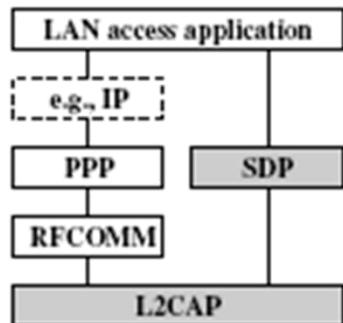


(b) Dial-up networking

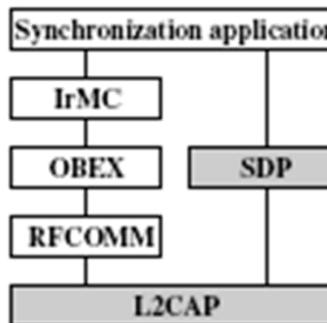


(f) Headset

(e) Cordless phone and intercom



(c) LAN access



(d) Synchronization

Bluetooth Low Energy

GAP (Generic Access Profile)

- Perfil que controla las conexiones y los anuncios en BLE.
- GAP es lo que permite que tu dispositivo sea público hacia el exterior y determina como dos dispositivos pueden (o no) interactuar entre ellos.
- Define 4 roles principales: dispositivos centrales y periféricos, dispositivos anunciadores y observadores.

GATT

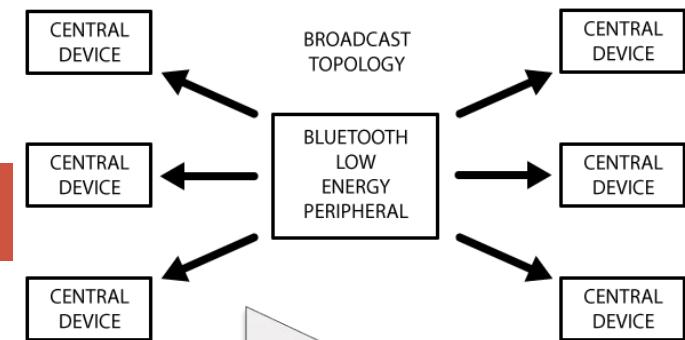
- Generic Attribute Profile,
- Define la manera en que dos dispositivos BLE pueden comunicarse usando Servicios y Características.
- Con un protocolo conocido como ATT, que se usa para almacenar los servicios, características y datos relacionados en una tabla usando identificadores de 16-bit para cada entrada en la tabla.

Los **periféricos** son dispositivos pequeños, de baja potencia, de bajos recursos, que pueden conectarse a dispositivos centrales mucho más potentes.

- Los dispositivos periféricos también suelen ser **anunciadores**
- Un ejemplo de periférico puede ser un glucómetro, un medidor de pulsaciones, un beacon, etc...

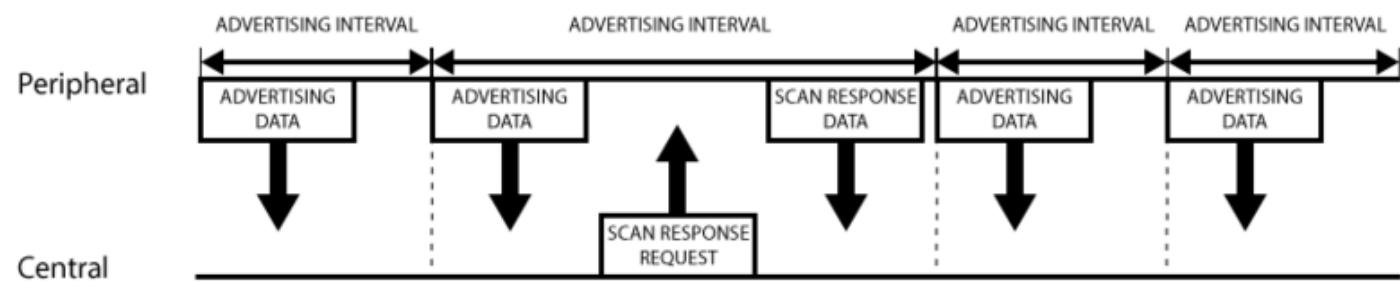
Un **dispositivo central** se corresponde normalmente con un teléfono móvil o una Tablet. Dispositivos con una capacidad de procesamiento mucho mayor que son recargados periodicamente.

- Los dispositivos centrales también suelen ser **observadores**

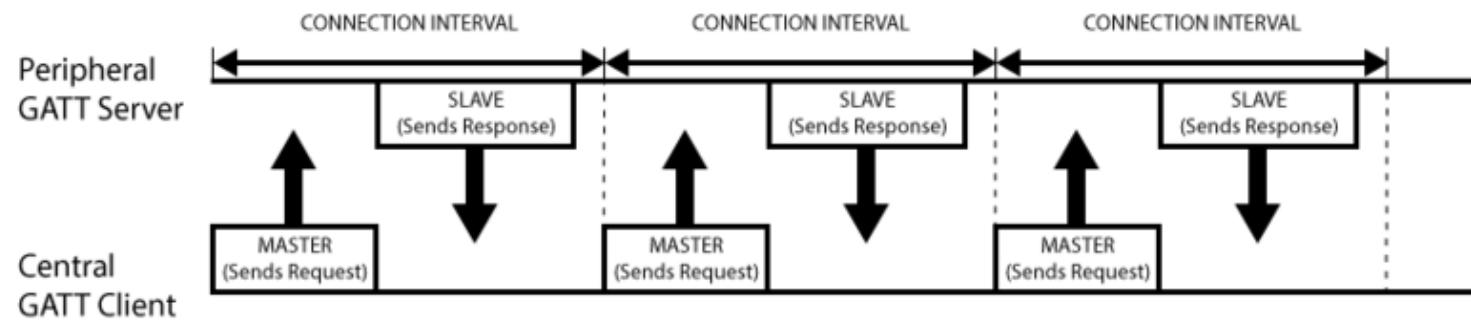


Bluetooth Low Energy: Comunicación

- Broadcast (advertising)
 - Los periféricos emiten mensajes de *advertising* a intervalos regulares



- **Todas las transacciones son iniciadas por el dispositivo maestro,**
 - el GATT Client (central), que recibe la respuesta del dispositivo secundario, el GATT Server (periférico)



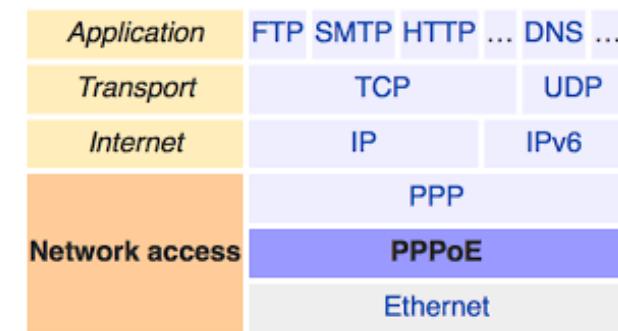
Tema 1. Introducción a las redes y sistemas distribuidos

Tema 2. Técnicas de acceso y control de enlace

Tema 3. Protocolos de Interconexión de Redes

Tema 4. Servicios básicos para el nivel de transporte en Internet

Tema 5. Aplicaciones distribuidas en Internet



- Unidades de Datos PPP
- Funcionamiento del Protocolo PPP

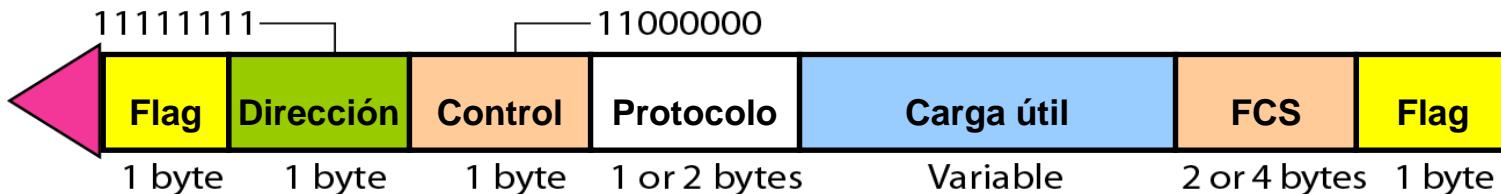
PROTOCOLO DE CONTROL DE ENLACE DE ALTO NIVEL (PPP)

PPP: Introducción

- Protocolo muy extendido para el acceso punto a punto
PPPoE : PPP over Ethernet
- Aspectos definidos por PPP:
 - Formato de la trama a intercambiar
 - Cómo negociar establecimiento del enlace e intercambio de datos
 - Cómo encapsular datos de nivel de red
 - Autenticación entre dispositivos
 - Soporte de múltiples protocolos y servicios a nivel de red
 - Configuración de direcciones de red
- Aspectos no definidos por PPP:
 - Control de flujo
 - Control de error mínimo: CRC para detección de error (en silencio). Sin numeración de secuencia

PPP: Unidad de datos

- Creación de tramas
 - Protocolo orientado a byte: transparencia a nivel de byte (escape: 01111101)
 - Campos:
 - Flag: Patrón 01111110
 - Dirección: Constante 11111111 (dirección de broadcast). Se puede negociar su omisión.
 - Control: Constante 11000000. Innecesario, omitible por negociación
 - Protocolo: Qué se transporta en campo datos (datos de usuario u otros)
 - Carga útil: datos de usuario u otra información. Máximo inicial 1500 bytes
 - Si la cantidad de datos reales es inferior al tamaño negociado -> padding
 - FCS: Secuencia de comprobación de trama (CRC estándar de dos o cuatro bytes)



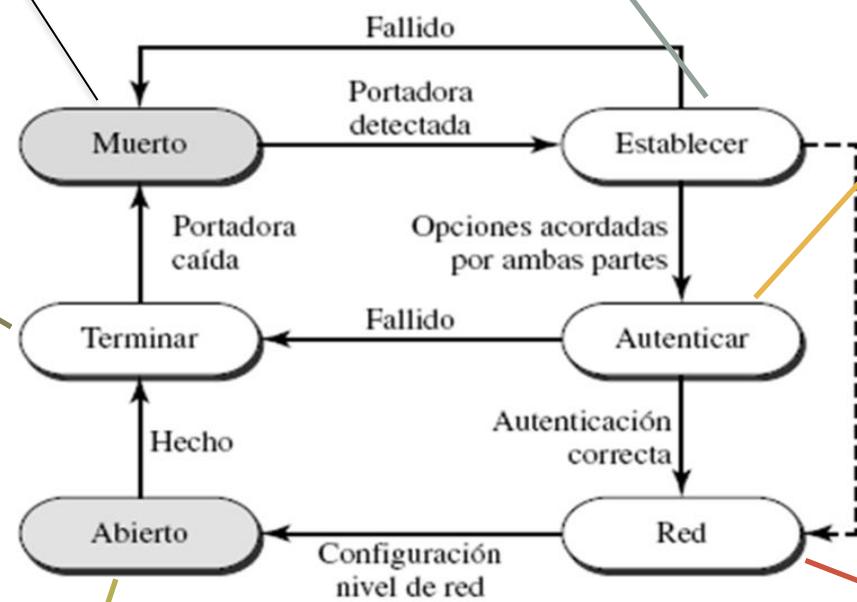
PPP: Funcionamiento básico

1. Línea en silencio, no hay portadora activa

2. Comienza comunicación. Negociación de opciones

3. Opcional. Si es acordada, debe superarse con éxito para pasar a fase de red

6. Se cierra el enlace y finaliza la conexión.



5 Comienza el intercambio de paquetes de datos. Transferencia de datos

4. Negociación de los protocolos a nivel de red. Necesaria dado que PPP soporta múltiples protocolos de red.

PPP: Principales protocolos

LCP (*Link Control Protocol*): Protocolo de control de enlace

- Establecer, mantener, configurar y terminar enlace
- Negociación de opciones entre ambos extremos

Protocolos de autenticación:

- Valida la identidad del usuario sobre el enlace de marcado
- Dos protocolos en PPP:
 - PAP (password authentication protocol)
 - CHAP (challenge handshake authentication protocol)

NCP (*Network Control Protocol*): Protocolos de control de red

- Protocolo de control de red específico para cada protocolo de red
 - IPCP configura enlace para transportar paquetes de datos IP
- Los paquetes NCP no llevan datos de nivel de red
 - Sólo configura el enlace al nivel de red para los datos que llegan