

## T.2

### INDICE:

#### 1. Caracterización y Servicios del Nivel de Enlace

#### 2. Redes de Acceso Múltiple

2.1 Redes de Acceso Múltiple con Detección de Portadora

2.2 Redes de Paso de Testigo

2.3 Redes Inalámbricas

#### 3. Protocolo de Control de Enlace de Alto Nivel (PPP)

3.1 Unidades de Datos PPP

3.2 Funcionamiento del Protocolo PPP

## 1. CARACTERIZACIÓN Y SERVICIOS DEL NIVEL DE ENLACE

### 1.1. 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 Acceso al medio.

Control de flujo.

Control de errores (detección y corrección)

Comunicación half/full duplex.

#### Control de acceso al medio

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. Protocolos MAC: Medium Access Control

#### 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, time-out, ...

Protocolos:

-Parada y espera

-Repetición selectiva

-Go back-N

#### Control de errores

Debe ser capaz de detectar tramas incorrectas. Debe ser capaz de corregir esas tramas o definir estrategias a seguir cuando se detecten errores.

Técnicas detectoras: Bits de paridad, CRC, checksums, ...

Técnicas de corrección/control de errores: Códigos de hamming, confirmaciones positivas/negativas, retransmisiones, temporizadores, ...

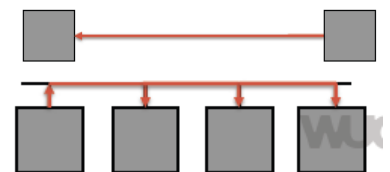
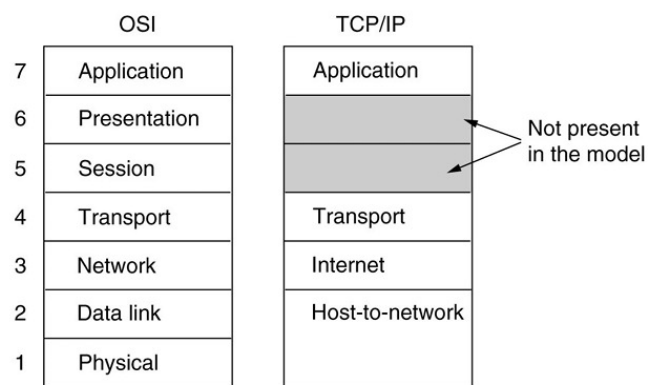
### 1.2. Protocolos básicos

Tres protocolos básicos:

Protocolo de parada y espera (stop-and-wait)

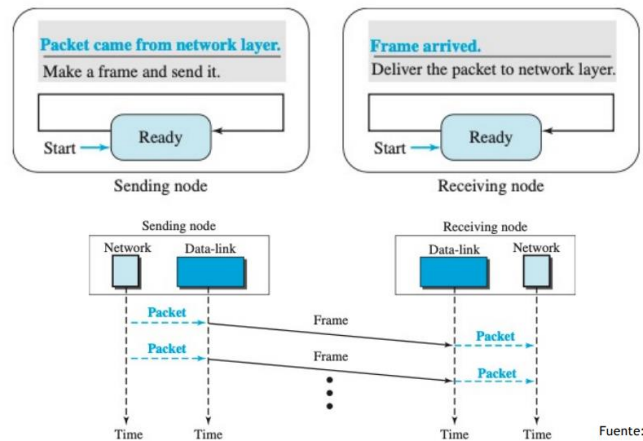
Protocolo de repetición selectiva

Protocolo Go-Back-N



Estos protocolos se pueden usar: A nivel de transporte (alto nivel). A nivel de enlace (bajo nivel).

### 1.2.1. Un protocolo básico

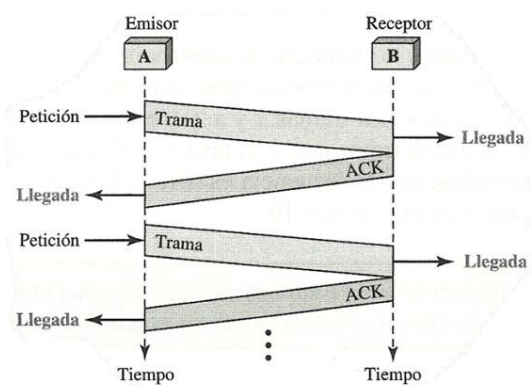


### 1.2.2. Protocolo de parada y espera Funcionamiento básico (control de flujo)

1. Se transmite un segmento
2. El receptor envía una confirmación
3. El emisor no envía el siguiente segmento hasta que recibe la confirmación (ACK)

#### Eficiencia

Medida que indica la proporción de tiempo necesario para enviar información útil respecto al total requerido. Lo ideal es una eficiencia del 1



#### Principales problemas en las comunicaciones:

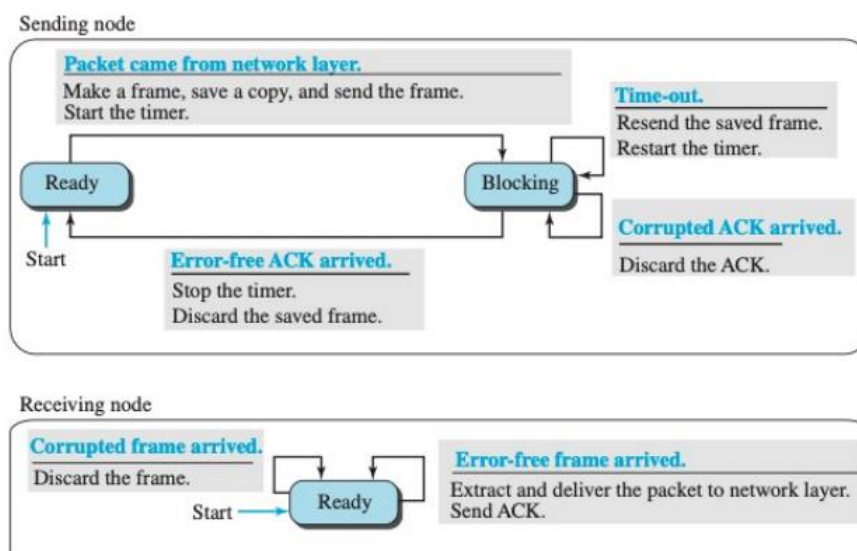
- Pérdida de la trama enviada
- Pérdida de la confirmación (ACK)

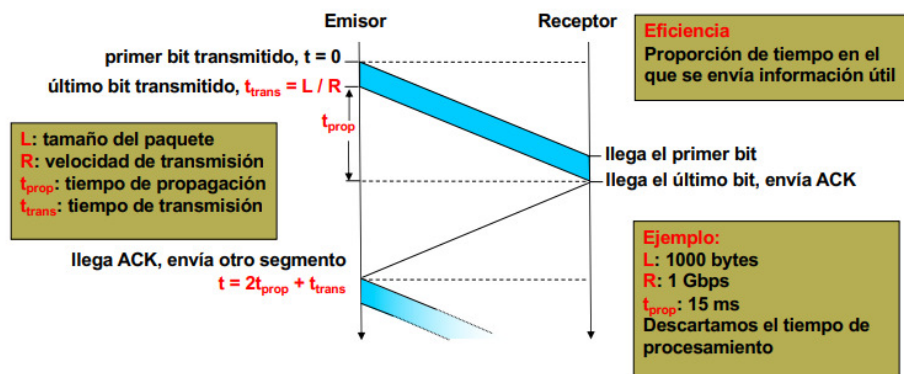
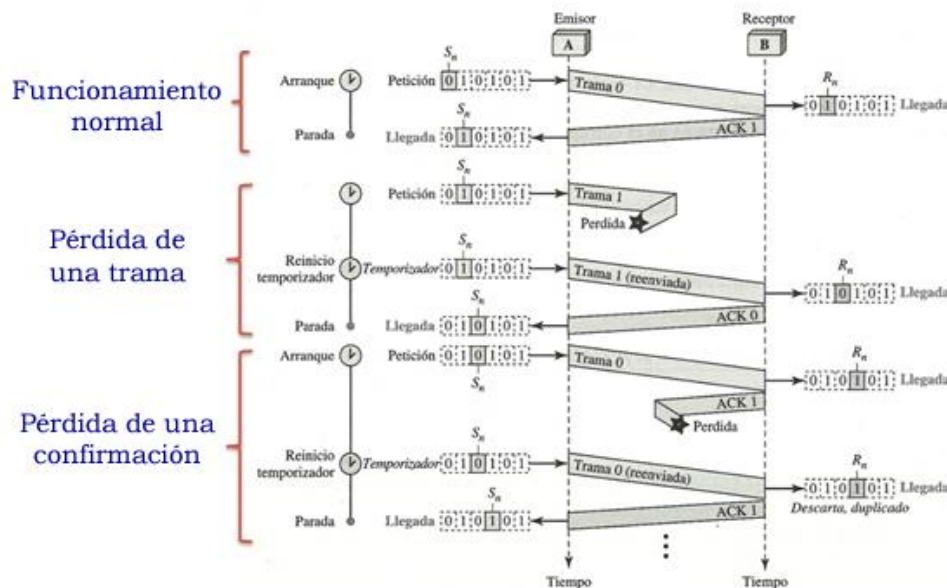
#### Temporizadores (timeout):

Se activa cuando el emisor envía una trama. Si se cumple el tiempo sin recibir confirmación -> Reenvía

#### Numeración de tramas y confirmaciones:

Usa 1 bit (0 ó 1) para evitar la aceptación de la misma trama varias veces. La confirmación se numera indicando la siguiente trama que espera recibir





$$E_{sender} = \frac{t_{trans}}{2 t_{prop} + t_{trans}} = \frac{.008 \text{ ms}}{30.008 \text{ ms}} = 0.00027$$

La ecuación completa de eficiencia incluye más términos

$$E = \frac{t_{trans,data}}{t_{trans,data} + t_{prop,data} + t_{proc,rec} + t_{trans,ack} + t_{prop,ack} + t_{proc,send}}$$

donde

$t_{trans,data}$ : tiempo de transmisión de datos

$t_{prop,data}$ : tiempo de propagación de datos

$t_{proc,rec}$ : tiempo de procesamiento en receptor

$t_{trans,ack}$ : tiempo de transmisión del ACK

$t_{prop,ack}$ : tiempo de propagación del ACK

$t_{proc,send}$ : tiempo de procesamiento en el emisor

Es razonable en la mayoría de los casos despreciar el tiempo de transmisión del ACK porque:

La confirmación puede ir en una trama de transmisión de datos en el otro sentido (esto se conoce como piggybacking).

La trama de ACK puede ser muy corta

También es razonable despreciar los tiempos de procesamiento porque son pequeños en comparación con el de transmisión.

En ocasiones asumimos que el tiempo de propagación es simétrico (igual en ambos sentidos).

**Ventajas:** Simple de implementar. Eficiente si los mensajes son de gran tamaño

**Inconvenientes:** Ineficiencia si usan mensajes pequeños. No siempre los mensajes pueden ser de gran tamaño

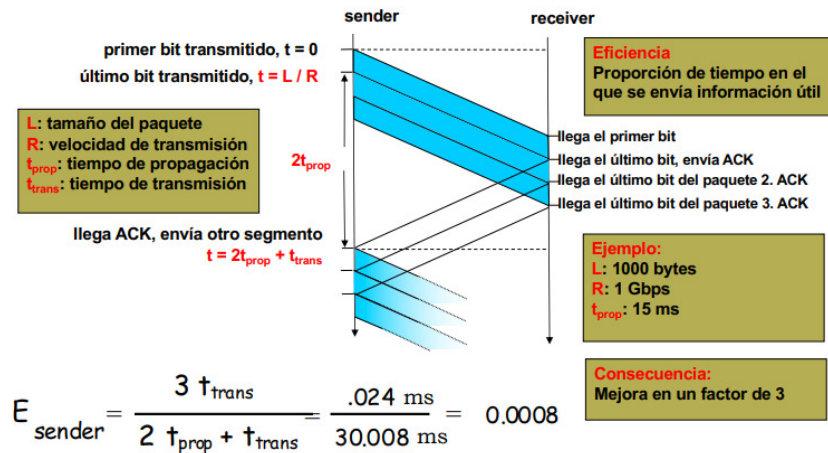
**Motivos para romper mensajes grandes:** Tamaño limitado de la memoria del receptor. Si hay errores hay que retransmitir mucha información. En medios de acceso múltiple la red no puede estar ocupada durante mucho tiempo.

**Alternativa de mejora: pipelining:** Enviar mensajes 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



### 1.2.3. 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

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:

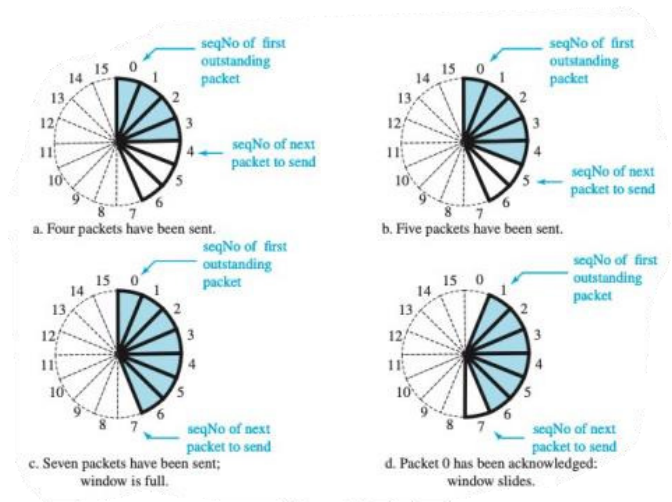
Mensajes numerados de  $[0, 2^m - 1]$

Máximo tamaño de ventana:  $2^m$

**Ejemplo:**

–  $m = 4$  (bits) -> Numeración:  $[0, 15]$

– Tamaños de ventana posible:  $[1, 16]$  -> Tamaño de ventana elegido = 7



**Ejemplo:**

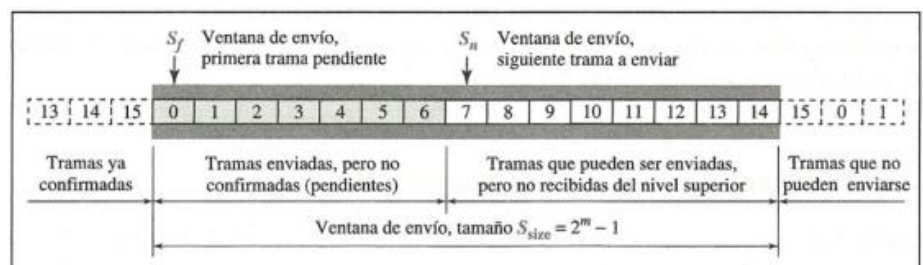
–  $m = 4$

– Numeración:  $[0, 15]$

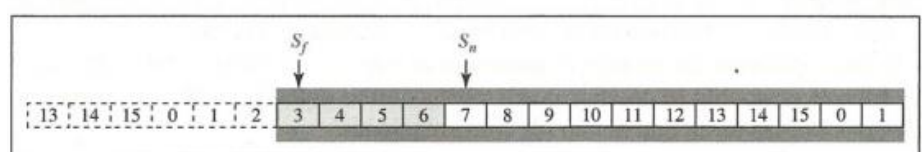
– Tamaños de ventana posible:  $[1, 16]$

– Tamaño de ventana elegido = 15

– Recibe confirmación de 0, 1 y 2



a. Ventana de envío antes de deslizar



b. Ventana de envío después del deslizamiento

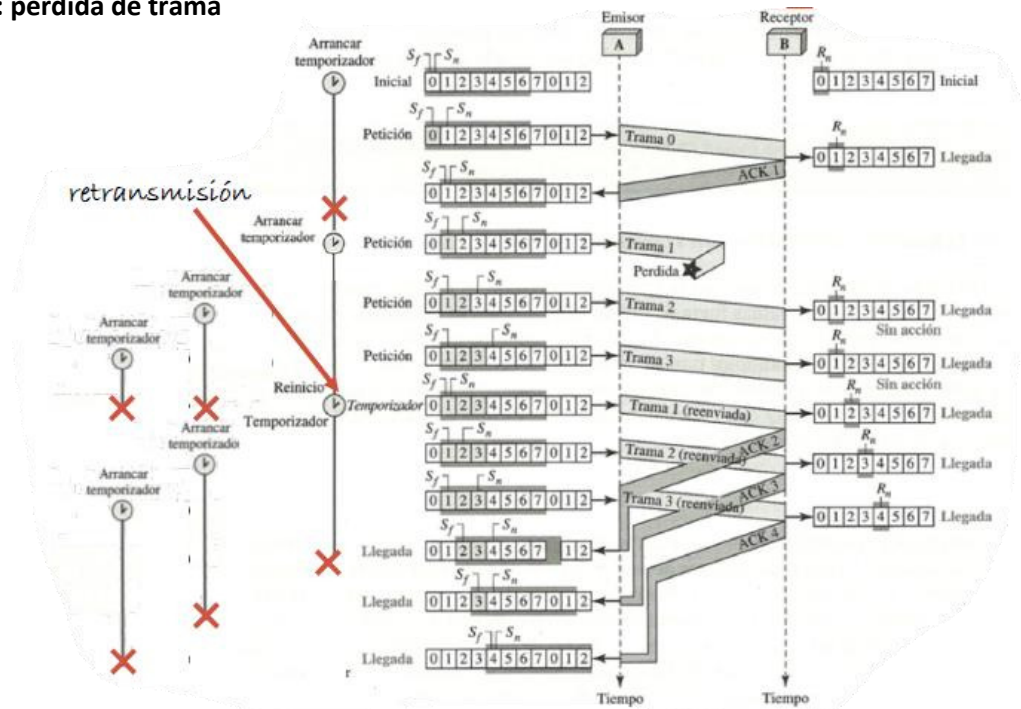


### 1.2.4. Protocolo Go-Back-N

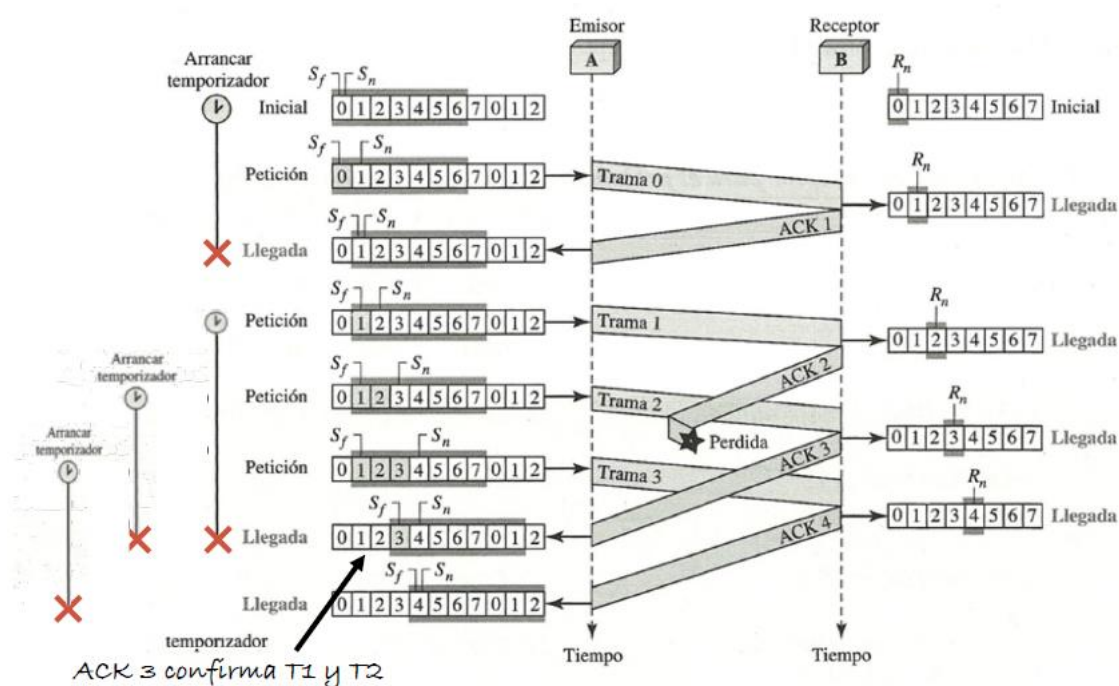
#### Características:

- Permite al emisor tener múltiples paquetes sin confirmar, sin que el receptor tenga que almacenar los paquetes en un buffer (Tamaño de la ventana de envío < 2m)
- El receptor sólo almacena el paquete que espera recibir (Tamaño de la ventana de recepción: 1)
- El receptor sólo contesta (ACK con el número de trama que espera recibir a continuación) si recibe la trama indicada en su ventana. En otro caso, no responde nada – La recepción de un ACK con numeración X permite al receptor confirmar todas las tramas pendientes < X (confirmación acumulada)
- Uso de temporizadores en el emisor. Cuando se cumple se reenvían todas las pendientes de confirmación
- Más eficiente que parada y espera
- Menos eficiente que repetición selectiva

#### Ejemplo: pérdida de trama



#### Ejemplo: pérdida de confirmación



### 1.2.5. Protocolo de repetición selectiva. SRP (Selective Repeat Protocol)

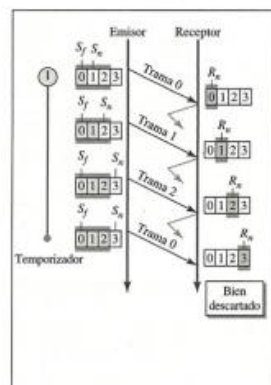
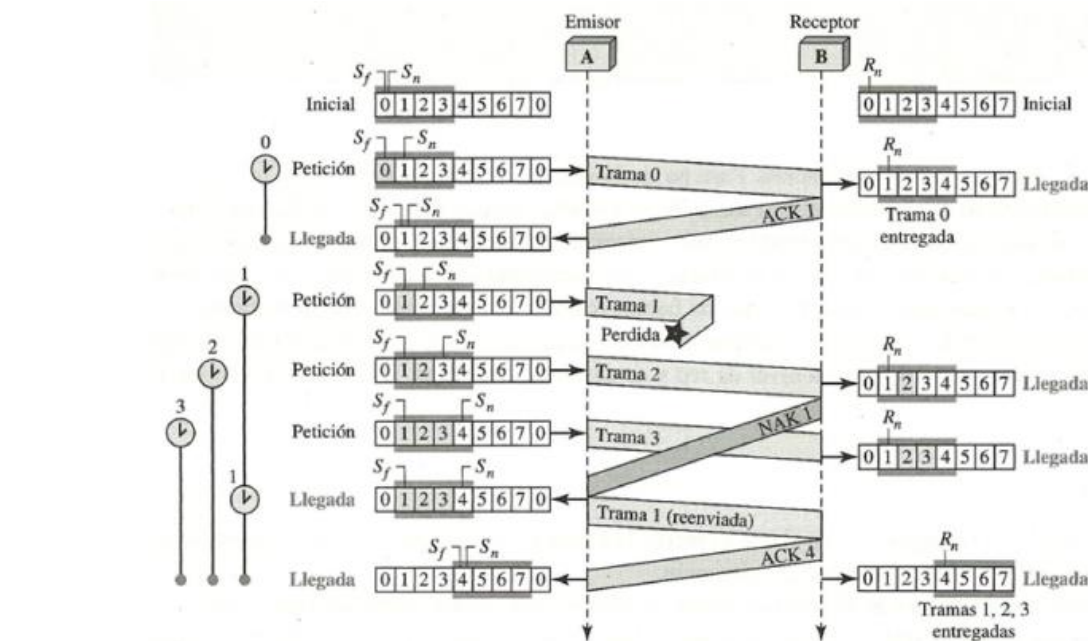
Más eficiente que parada y espera y Go-Back-N. Solo se retransmiten aquellas tramas no confirmadas. Pero las tramas pueden llegar fuera de orden

En el emisor: Es necesario un buffer para almacenar las tramas no confirmados (Tamaño máximo ventana de envío:  $2^{m-1}$ )

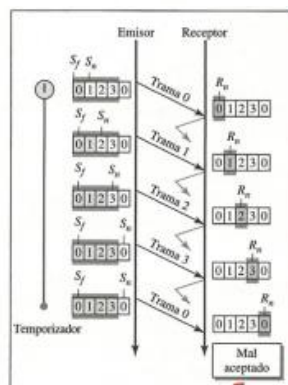
Reenvía tramas a petición del receptor o por temporizador (uno por trama)

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. El emisor envía un número de frames sin necesidad de esperar ACK individuales del receptor. El receptor puede rechazar de forma selectiva frames individuales, que serán retransmitidos. El receptor acepta frames fuera de orden y los almacena en el buffer. El emisor retransmite frames para los que ha expirado el timeout.

#### Ejemplo de uso de repetición selectiva



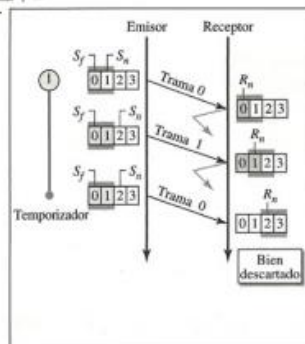
a. Tamaño de ventana  $< 2^m$



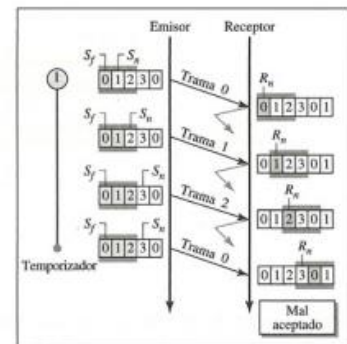
b. Tamaño de ventana  $= 2^m$

Go-Back-N  
( $< 2^m$ )

Repetición selectiva  
( $\leq 2^{m-1}$ )



a. Tamaño de ventana  $= 2^{m-1}$



b. Tamaño de ventana  $> 2^{m-1}$

### 1.3. Detección y corrección de errores

#### Detección de errores

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

Existen dos tipos de códigos:

Códigos detectores: bits de paridad, checksums, CRCs, etc.

Códigos correctores: códigos de Hamming

#### 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

#### 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

#### Sumas de comprobación (checksum)

Técnica general de detección de errores. Se suele aplicar cuando se reciben bloques de caracteres, en lugar de caracteres aislados.

En la emisión y recepción: Se suma cada carácter al checksum

Al final de la emisión: El emisor envía el checksum al receptor, y éste lo comprueba con el suyo

Se suele usar más en la capa de transporte: Es un esquema simple. 16 bits en TCP y UDP.

#### Códigos redundantes cíclicos

Se conocen como CRC (Cyclic Redundancy Check). Fundamento:

-Se envían k bits de información + r bits redundantes

-La trama de k+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

## 2. REDES DE ACCESO MÚLTIPLE

### Protocolos de acceso múltiple 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. Descentralizado/Distribuido

### 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)

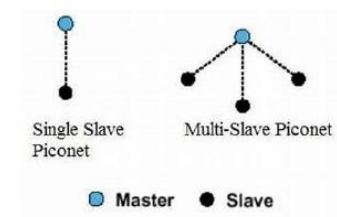
### Asignación del enlace

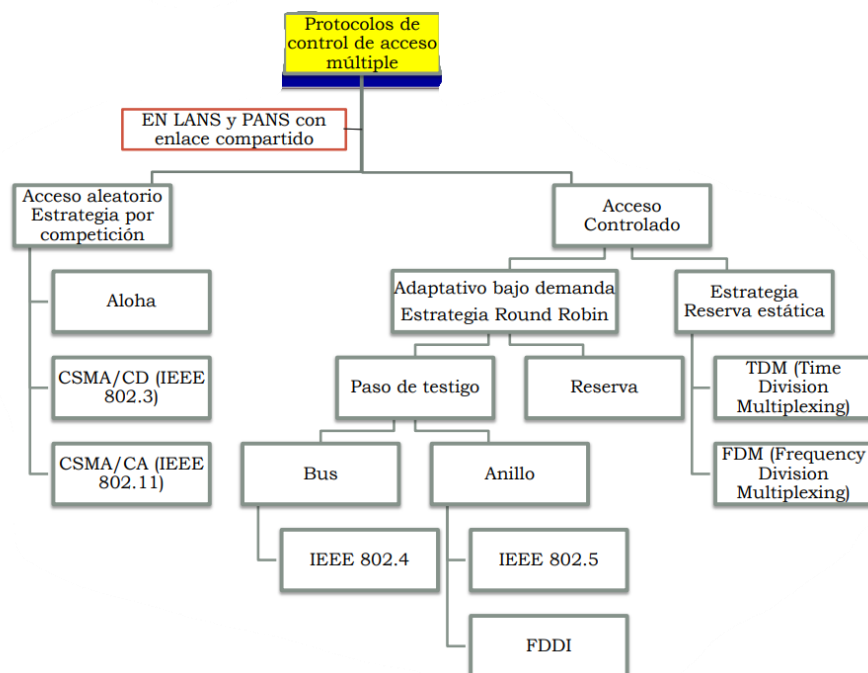
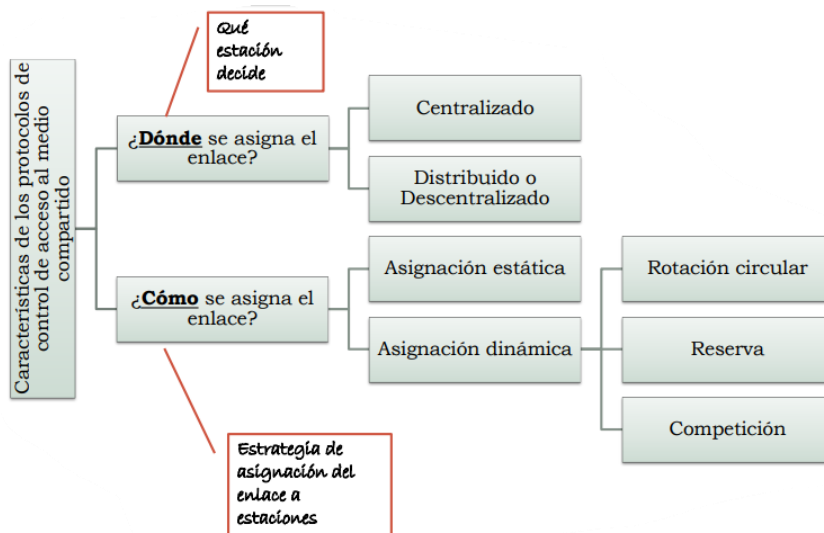
Dos formas de asignar el enlace:

Estática: Se dedica una capacidad dada a cada conexión. Válido en conmutación de circuitos (TDM y FDM). No óptimo en LANs (comunicación impredecible).

Dinámica: Para responder a solicitudes inmediatas

Tres categorías de asignación dinámica: Round robin (rotación circular), reserva y competición.





### 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.

### 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

### 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.



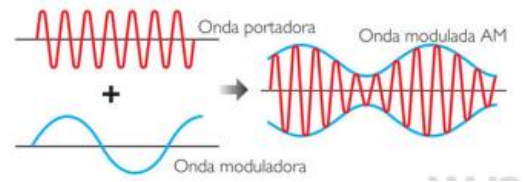
## 2.1. Redes de acceso múltiple con detección de portadora (ethernet)

### 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

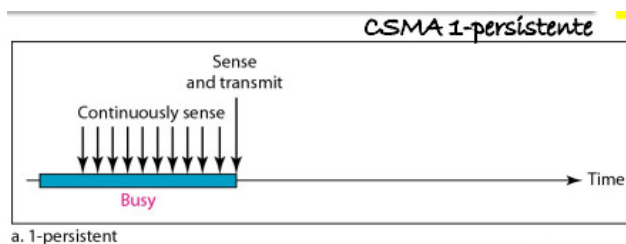
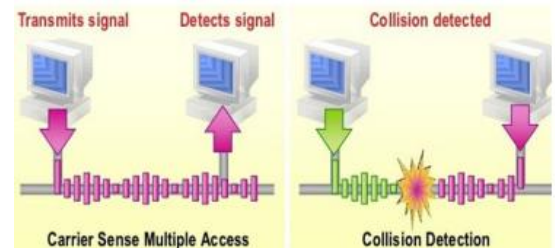


### Técnica se denomina CSMA: Carrier Sense Multiple Access.

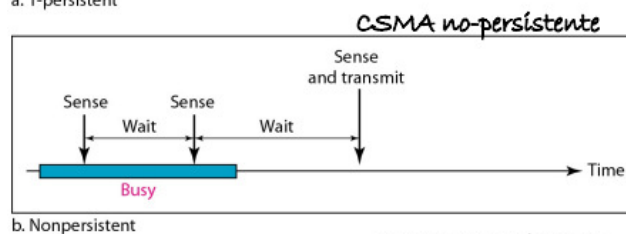
- (1) Detecta si alguien está transmitiendo en ese momento. Esta transmisión se detecta por la presencia de una señal portadora
- (2) Si el canal está inactivo, la estación puede transmitir
- (3) Si el canal está activo, la estación no puede transmitir. Podemos distinguir 3 tipos de algoritmos para determinar el comportamiento de una estación cuando ésta encuentra el canal ocupado.

Existen diversas variantes

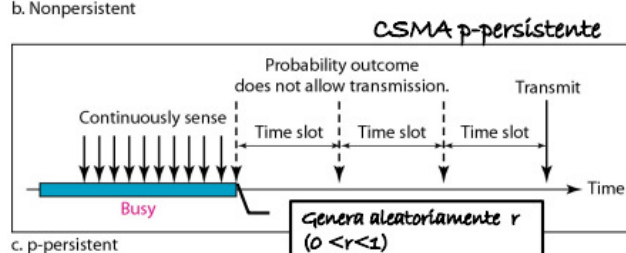
- CSMA 1-persistente
- CSMA no persistente
- CSMA p-persistente



Espera hasta que esté libre comprobando continuamente si esta libre



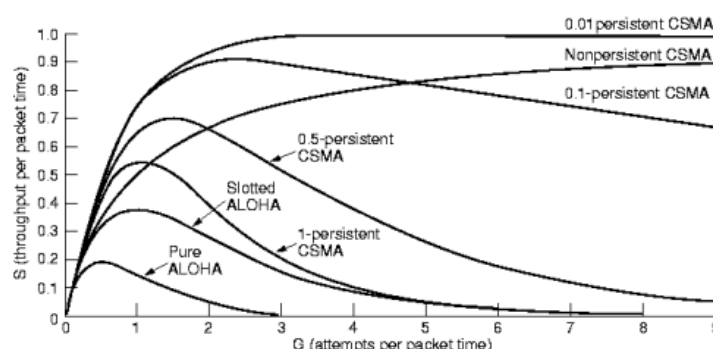
Espera un tiempo aleatorio antes de volver a detectar si está libre  
Intenta evitar que dos o más que estaban a la espera, empiecen a transmitir justo a la vez



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  $r \leq p$  transmite.
3. En otro caso se espera al siguiente intervalo y vuelta a 1

### Gráfico de eficiencia



**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. Si ambas señales son las mismas no ha habido colisión. Si otra estación también envía las señales se mezclarán y detectará la colisión.

### 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  $\{0, 1, 2, 3, \dots, 2^m - 1\}$ , donde  $m := \min[10, n]$

-El nodo espera  $512 \cdot k$  tiempos de bit (a 10 Mbps, 1 tiempo de bit es  $10^{-7}$  segundos)

Si  $n = 16$ , se abandona la transmisión

Análisis:

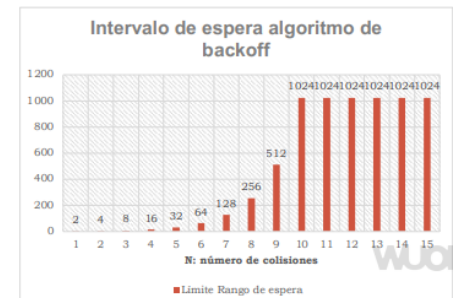
Si hay pocas colisiones, la espera es pequeña

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

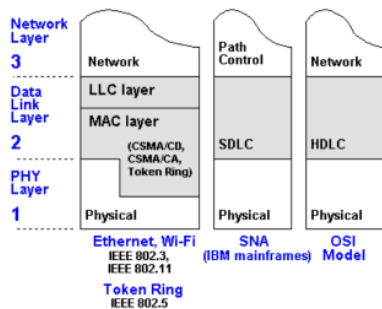
Si el tiempo de espera fuera fijo y pequeño. Muchas colisiones

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.



## 2.2.Redes de área local IEEE 802

El estándar IEEE 802



### IEEE 802.x

### OSI

IEEE 802.x							OSI	
802.2 Control del Enlace Lógico							2	
802.3	802.4	802.5	802.6	802.7	802.8	802.9	MAC	
csma-cd	token-bus	token-ring	dqdb	b. ancha	fibra ópt.	rdsi	Física	1

MAC (Medium Access Control): Control de Acceso al Medio

LLC (Logical Link Control): Control del Enlace Lógico

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.

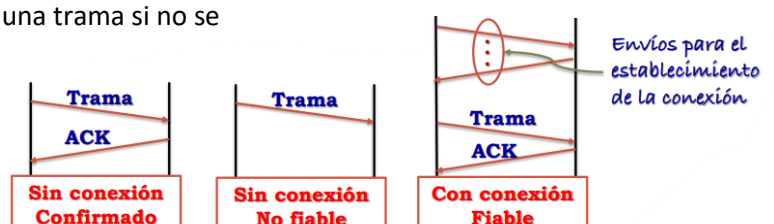
Se diferencian en la capa física (características del equipo de transmisión) y en el protocolo MAC.

### 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

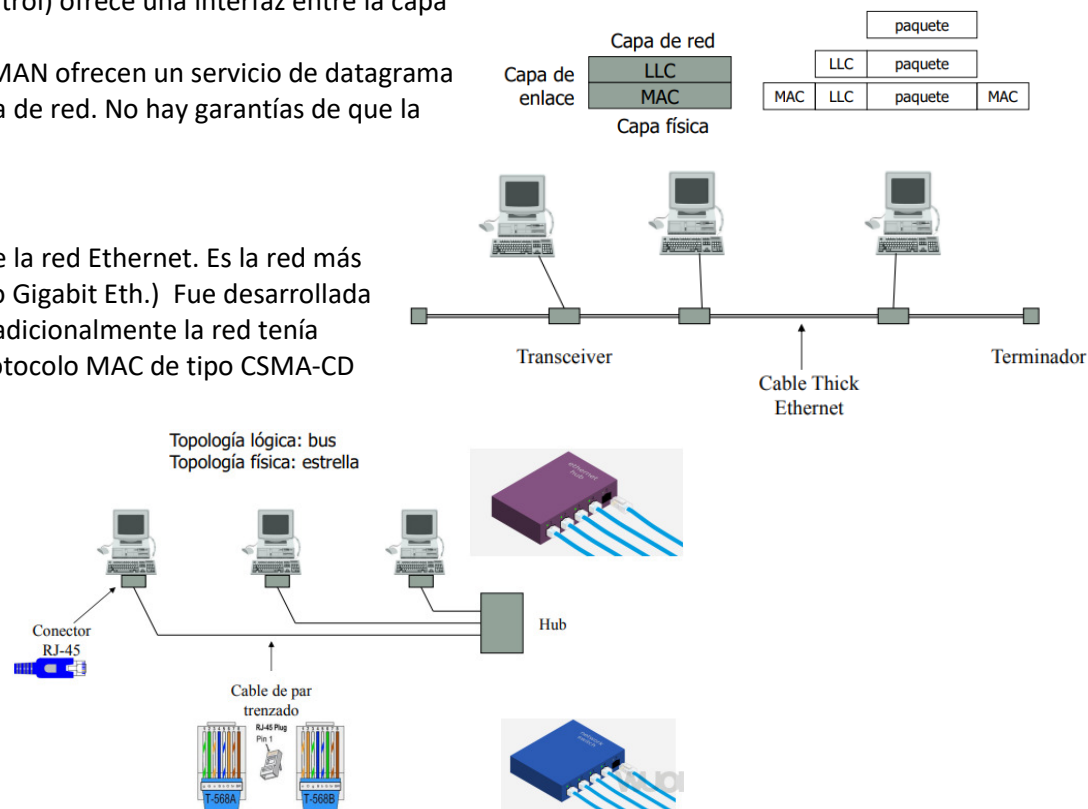


La capa LLC (Logical Link Control) ofrece una interfaz entre la capa de red y la capa MAC.

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 Ethernet con par trenzado



### Distinción entre transmisión unicast, multicast, y broadcast

Ethernet standard utiliza cable coaxial (bus) o par trenzado (estrella)

Transmisión es siempre a todas las estaciones (broadcast)

La distinción está en qué estaciones se quedan con la trama y cuáles la descartan.

-En la transmisión a una sola estación (unicast), solo el destinatario se la queda, y el resto la descarta

-En la transmisión de grupo (multicast), las estaciones que son miembros del grupo se la quedan, el resto la descarta

-En la transmisión a todas las estaciones (broadcast), todas las estaciones (excepto el emisor) reciben la trama y se la quedan

### 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

7 primeros bytes (valor 10101010): Sirven para “despertar” al receptor y sincronizar su reloj con el emisor.

8º byte (valor 10101011): Los dos últimos bits 11 señalizan el comienzo de la trama

– Direcciones MAC origen y destino: 6 bytes en Hexadecimal (formato AA:AA:AA:AA:AA:AA).

– Tipo de trama: Contiene identificador del protocolo de nivel superior (red): IP, ARP, AppleTalk, Novell IPX. Se puede utilizar para multiplexación (múltiples protocolos a nivel de red).

– Datos del protocolo encapsulado: Máxima longitud 1500 bytes, mínima 46 bytes

Si longitud >1500, los datos se fragmentan y se hace más de una trama

Si longitud <46, se rellena hasta completar con 0's (padding). Se entrega a la capa superior con el padding incluido.

– Control de errores: CRC-32: Se calcula sobre los campos tipo de trama y datos. Si no es 0, se descarta la trama

### Dirección MAC

Se transmite de izquierda a derecha byte a byte. Cada byte se transmite de derecha a izquierda (Bit menos significativo se transmite antes)

3 primeros bytes: fabricante: Menos significativo: Un equipo/unicast (0) o muchos/multicast (1). Segundo menos significativo: Global (0) o local (1)

3 últimos: identificador de la tarjeta

### ¿De qué tipo son las siguientes direcciones?:

A. 4A:30:10:21:10:1A -> Dirección unicast porque A en binario es 1010 (par).

B. 47:20:1B:2E:08:EE -> Dirección multicast porque 7 en binario es 0111 (impar).

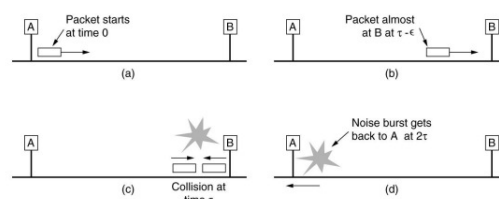
C. FF:FF:FF:FF:FF:FF -> Dirección broadcast porque todos los dígitos son F en hexadecimal (48 bits valor todos 1 en binario).

### ¿Por qué 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.



### Análisis

En la red Ethernet:

Velocidad de transmisión: 10Mbps.

Longitud máxima del cable: 2500 metros (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 transmite 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



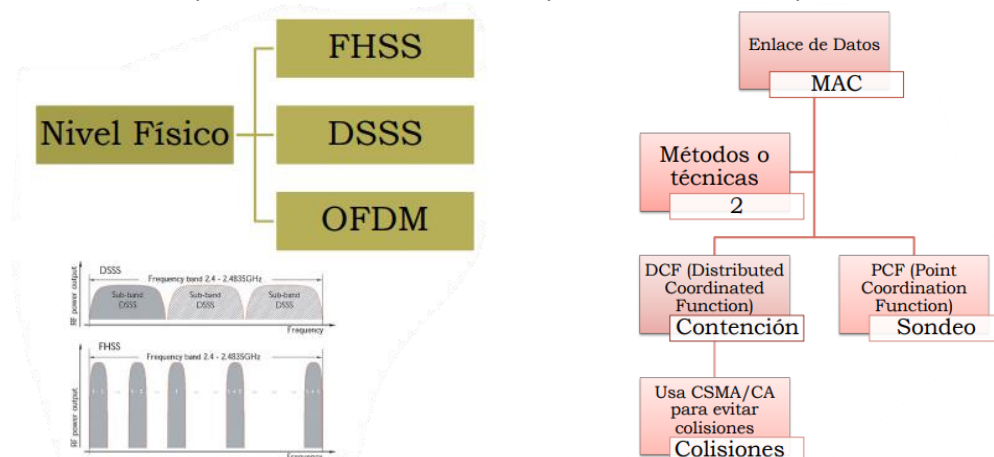
### 2.3.Redes inalámbricas (wifi y bluetooth)

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

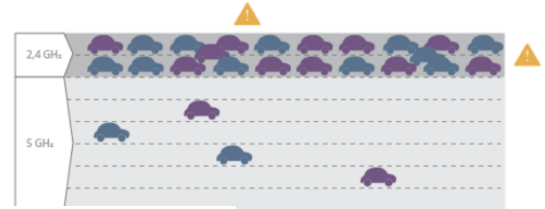
### 802.11. Redes de Área Local Inalámbricas – WIFI

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





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.

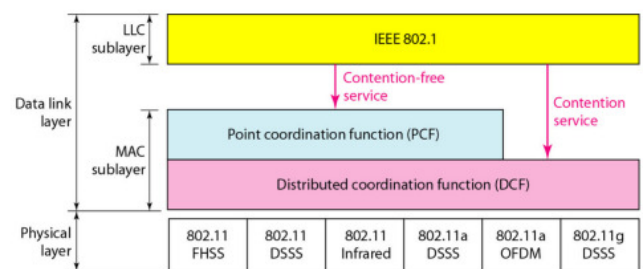


	Ventajas	Desventajas
2.4 GHz	<ul style="list-style-type: none"> <li>✓ Accesible desde mayores distancias</li> <li>✓ Compatible con una gran cantidad de dispositivos</li> </ul>	<ul style="list-style-type: none"> <li>✓ Frecuencia muy usada por todos los dispositivos que admite</li> </ul>
5 GHz	<ul style="list-style-type: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

### 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 (PCF) (\*OPCIONAL\*): Mecanismo de acceso centralizado por sondeo el punto de acceso



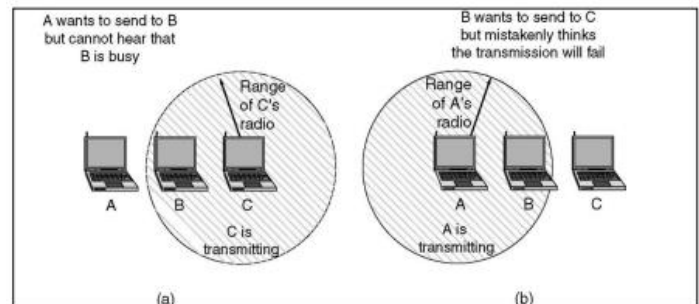
### Dificultades

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 y de la estación expuesta



### 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).

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

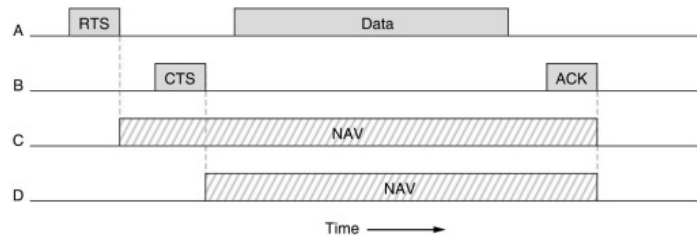
¿Cómo sabe si hay colisión?

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



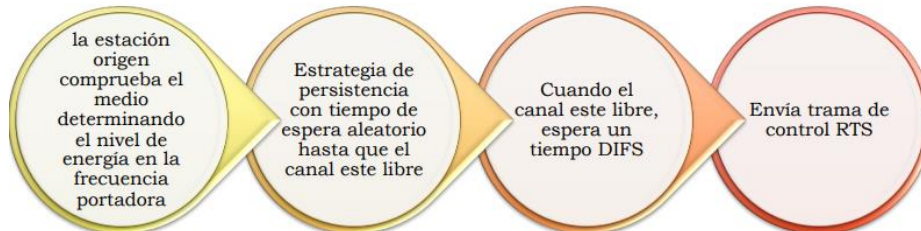
### Protocolo tipo MACAW (MACA for Wireless)

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



### 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.

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)

De nuevo, en la estación origen ...



Y en la estación destino ...



### ¿Cómo se evita la colisión?

¿Cómo aplaza una estación el envío de datos si una estación adquiere el acceso?

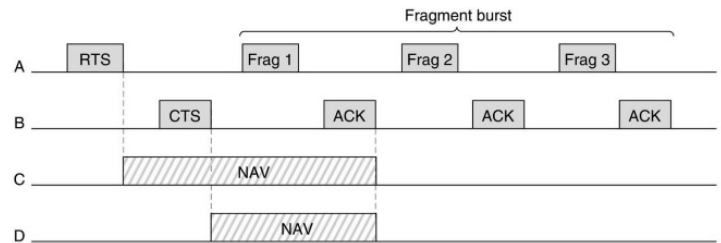
Mediante el NAV y su activación al escuchar los RTS/CTS

¿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

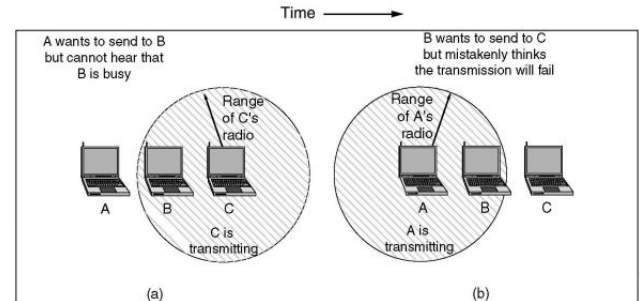
## Redes IEEE 802.11

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

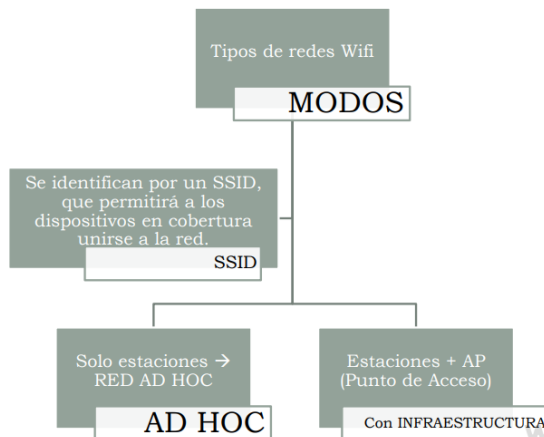


El problema de estación oculta (a): Se soluciona con RTS y CTS

El problema de la estación expuesta (b) ¿Solución?



## Arquitectura WIFI



## Identificación de redes 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.

## Modos de redes Wifi

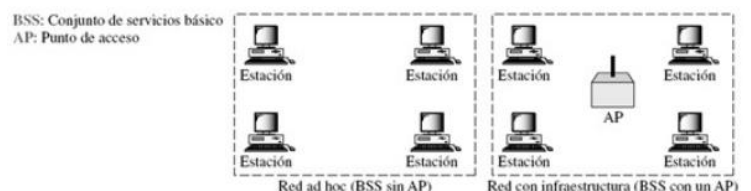
Modo ad hoc: Es una red aislada y no puede enviar datos a otras redes. Las estaciones pueden formar una red, localizarse y acordar formar una red ad hoc -> wifi direct.

Modos Infraestructura: Estaciones + AP (punto de acceso). Requerido para que todos los dispositivos se conecten y comuniquen.

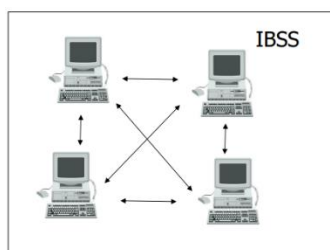
## Concepto de BSS

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 y una estación base opcional a 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

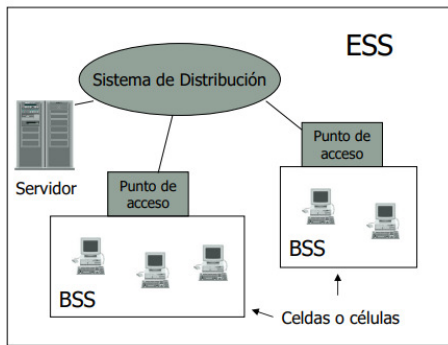


## Arquitectura: modo ad hoc



IBSS: Conjunto de Servicios Básico Independiente

## 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

## Trama

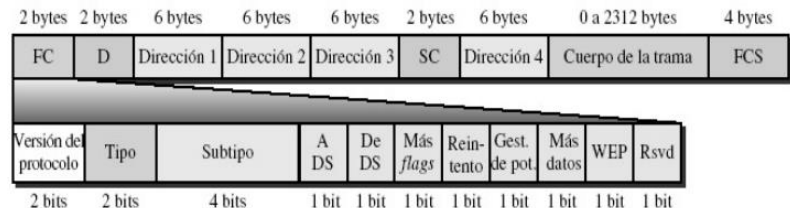
Más compleja que la de Ethernet (802.3). Algunos campos son opcionales (dependen del tipo):

– 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



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

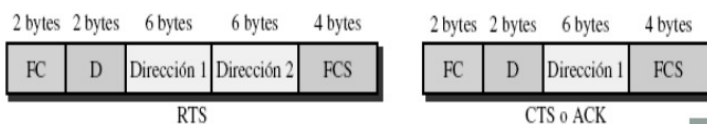
Campo	Explicación
Versión	La versión actual (802.11) es la 0
Tipo	Tipo de Información: gestión (00), control (01) o datos (10)
Subtipo	Subtipo de los tipos anteriores
A DS	= {0,1}
De DS	= {0,1}
Más flags	= 1, más fragmentos
Reintento	= 1, trama retransmitida
Gestión de Potencia	= 1, la estación está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

D – 2 bytes : En la trama de control, define el identificador de la trama. En el resto define la duración de la transmisión que se utiliza para fijar el NAV (en ms)

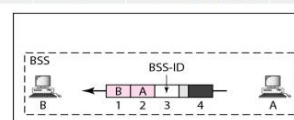
Direcciones – 4 campos de 6 bytes (6 x 4): 4 campos de dirección cuyo significado depende de los campos A DS y De DS en el campo FC

CS - Control de secuencia: N° de secuencia del control de flujo

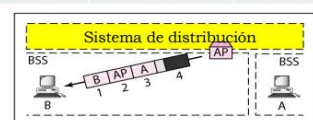
Depende del tipo puede que algunas direcciones y el CS no aparezcan. Ej. (tramas de control):



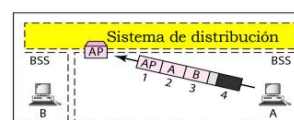
A DS	De DS	Dirección 1	Dirección 2	Dirección 3	Dirección 4
0	0	Destino	Origen	ID de BSS	N/A
0	1	Destino	AP emisor	Origen	N/A
1	0	AP receptor	Origen	Destino	N/A
1	1	AP receptor	AP emisor	Destino	Origen



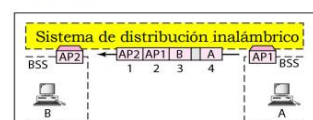
a. Caso 1



b. Caso 2



c. Caso 3



d. Caso 4

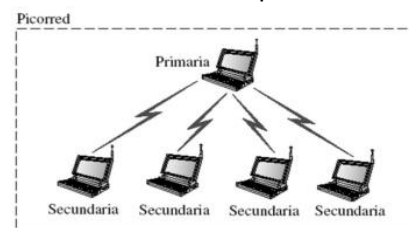
## BLUETOOTH

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.

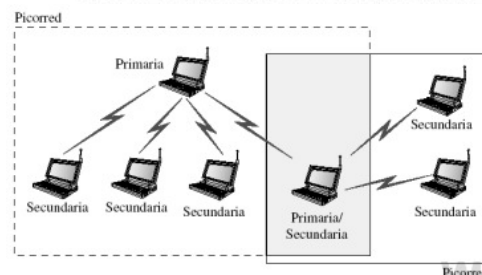
Originalmente, proyecto de compañía Ericsson. Posteriormente se estandarizó como 802.15.1 (redes de área personal, PAN)

Red ad hoc: se forma de manera espontánea. Dispositivos se encuentran unos a otros. Forman una picorred o red dispersa

**Arquitectura picorred:** Máximo 8 estaciones. 1 estación actúa de primaria, el resto secundarias.



**Arquitectura Red Dispersa (Scatternet):** Combinación de picorredes. Una estación secundaria en una picorred actúa de primaria en otra. Una estación puede ser miembro de dos picorredes



Bluetooth ofrece una arquitectura en capas:

-Protocolos básicos:

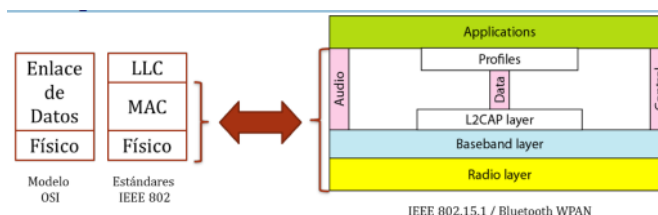
- Radio
- Banda Base
- Protocolo de Gestión del Enlace (LMP)
- Protocolo de adaptación y gestión del enlace lógico (L2CAP)
- Protocolo de Descubrimiento de Servicios (SDP)

-Protocolos de control de telefonía (y sustitución de cable): RFCOMM, AT, TCS BIN

-Protocolos adoptados

### 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 µs) antes de saltar a otra

Evita interferencias con otras redes

Requiere que todos los dispositivos de la picorred estén sincronizados

**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

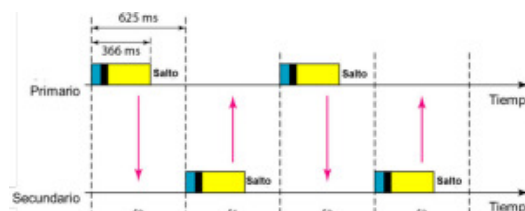
En 1 ranura, la estación primaria envía una trama a una secundaria o una secundaria a la primaria

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.

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



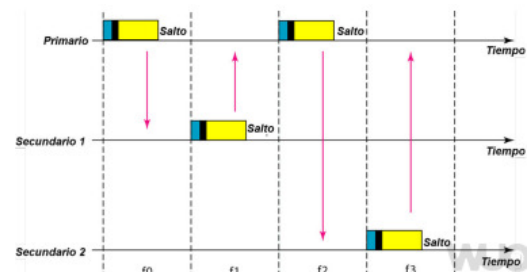
Comunicación con múltiples secundarios:

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

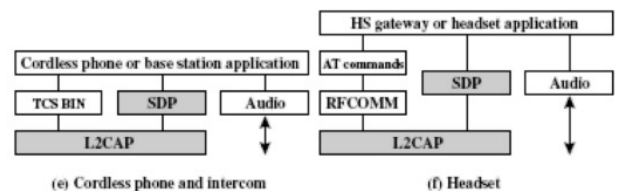
Método de muestreo con reserva de tiempo



En el nivel de Radio la comunicación se controla mediante el establecimiento de dos tipos de enlaces físicos

Enlace orientado a conexión síncrono (SCO): Audio (tiempo real): llamada voz con Teléfono

Enlace no orientado a conexión asíncrono (ACL): Datos



## 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 y Perfiles Bluetooth: Describen un modelo de uso de los protocolos para un servicio determinado.

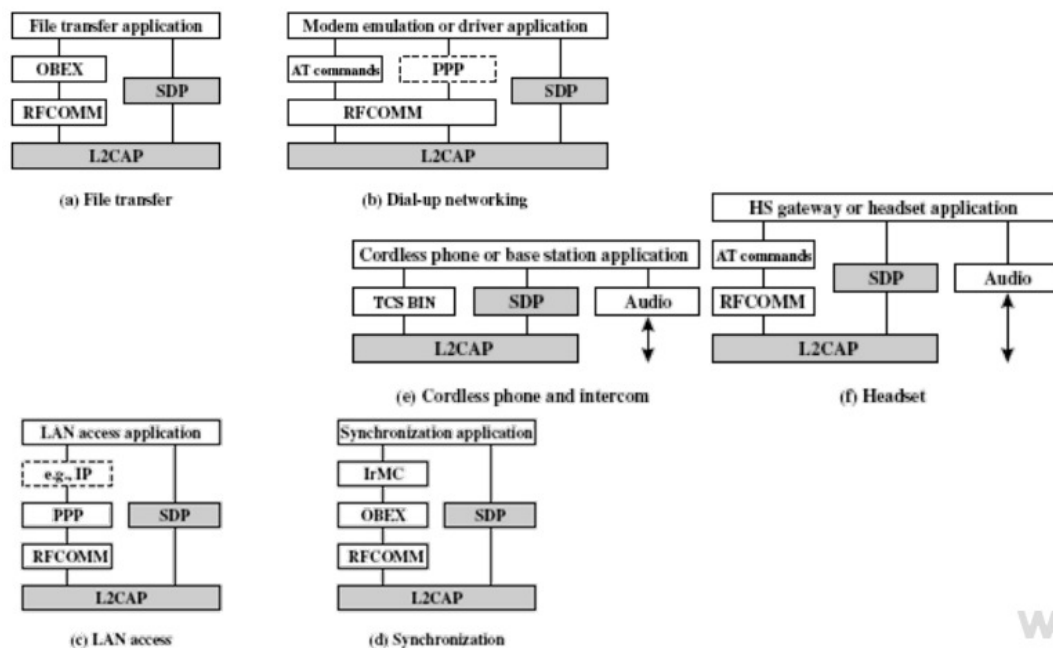
Transferencia de ficheros entre dispositivos

Transferencia de audio (Auriculares)

Control de llamadas y transferencia de voz

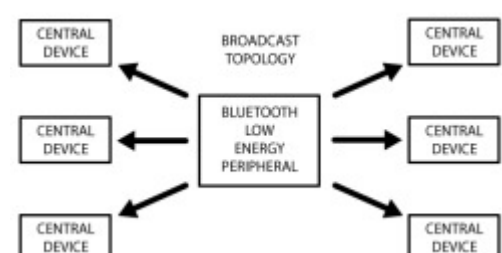
Acceso a LAN (anclaje o tethering)

## Perfiles Bluetooth - Modelos de Uso



## 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 dos roles principales: dispositivos centrales y los periféricos.





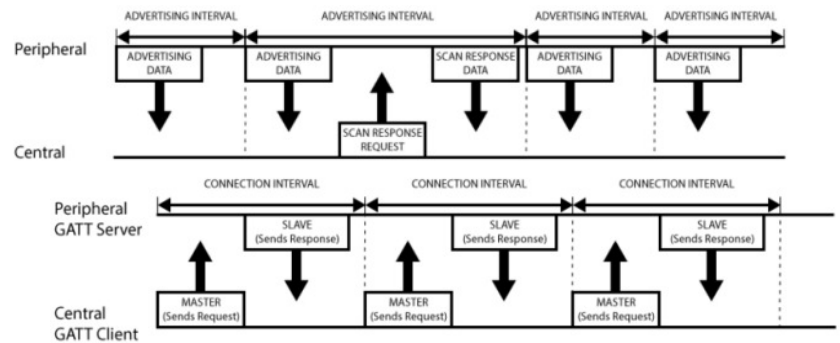
**GATT:** Generic Attribute Profile, Define la manera en que dos dispositivos BLE pueden comunicarse usando los Servicios y Características. Con un protocolo conocido como ATT, que se usa para almacenar los servicios, características y datos relacionados en una tabla usando identificadores de 16-bit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

### 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 esclavo, el GATT Server (periférico).



## 3.PROTOCOLO DE CONTROL DE ENLACE DE ALTO NIVEL (PPP)

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

### 3.1. Unidad de datos

#### Creación de tramas

Protocolo orientado a byte: transparencia a nivel de byte (escape: 01111101)

Campos:

Flag: Patrón 01111110

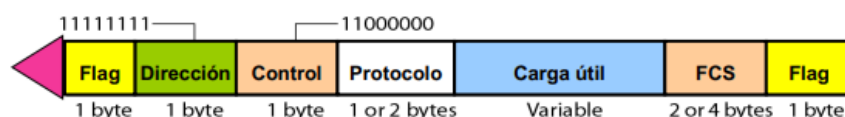
Dirección: Constante 11111111 (dirección de broadcast). Se puede negociar su omisión.

Control: Constante 11000000. Innecesario, omitible por negociación.

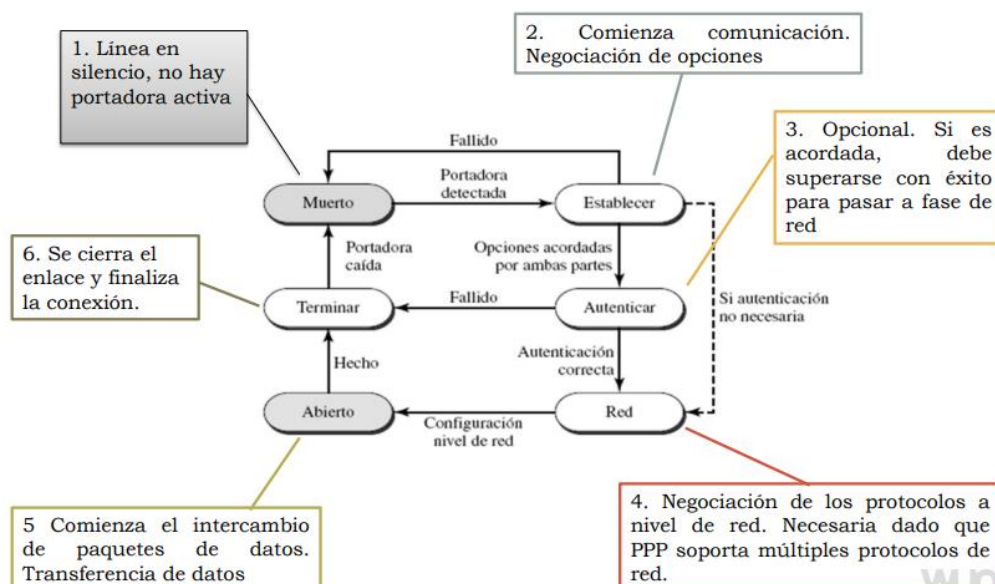
Protocolo: Qué se transporta en campo datos (datos de usuario u otros)

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)



## Funcionamiento básico



### 3.2.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