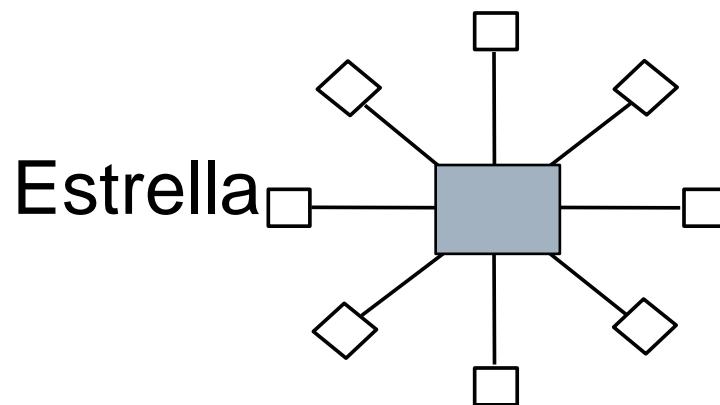
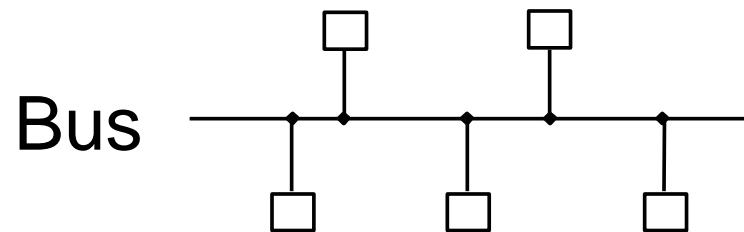
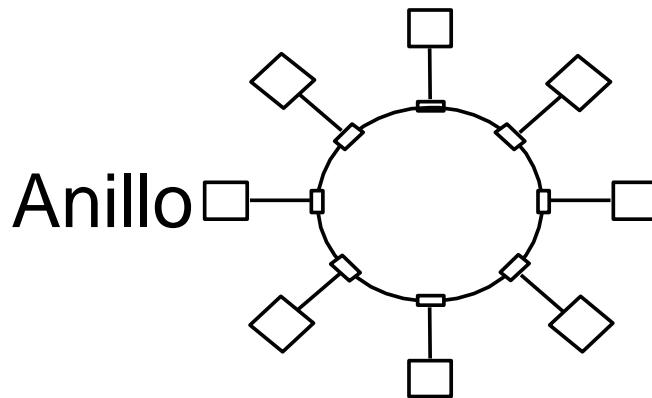


Tema 4

Redes LAN

Principales topologías de las redes LAN



	VENTAJAS	INCONVENIENTES
ANILLO	<ul style="list-style-type: none">- El acceso a la red está asegurado en un tiempo máximo definido (determinista).- Simplificación de la confirmación de tramas.- Buen comportamiento ante situaciones de alto tráfico.- Permite políticas de priorización de tramas.	<ul style="list-style-type: none">- El fallo en uno de los nodos supone el colapso de la red.- La incorporación de nuevos nodos no es sencilla, precisa de un diseño de conexión adecuado.
BUS	<ul style="list-style-type: none">- Fallo de la interfaz no afecta a otros nodos.- Sencilla inserción de nuevas estaciones.	<ul style="list-style-type: none">- El mecanismo de control de acceso al medio (MAC) resulta complejo para garantizar un tiempo de acceso determinado.- La rotura del bus puede bloquear el tráfico incomunicando los nodos.- Bajo rendimiento cuando el tráfico es intenso.
ESTRELLA	<ul style="list-style-type: none">- Fácil inserción de nuevos elementos.- Alta seguridad.- Fácil detección de nodos con fallos. <i>Y si el nodo central es activo...</i>- Posibilidad de múltiples protocolos.- Posibilidad de priorizar de tramas.	<ul style="list-style-type: none">- Un fallo en el nodo central bloquea las comunicaciones.- <i>Si el nodo es activo se retrasa el tráfico.</i>- Las ampliaciones están sujetas a la capacidad del nodo central, si la exceden aumentan mucho los costes.

Asignación estática del canal:

- Usando FDM o TDM (división por anchos de banda o por intervalos de tiempo).
- Ineficiente e inflexible.

Asignación dinámica del canal:

Se basan en un modelo que cumple:

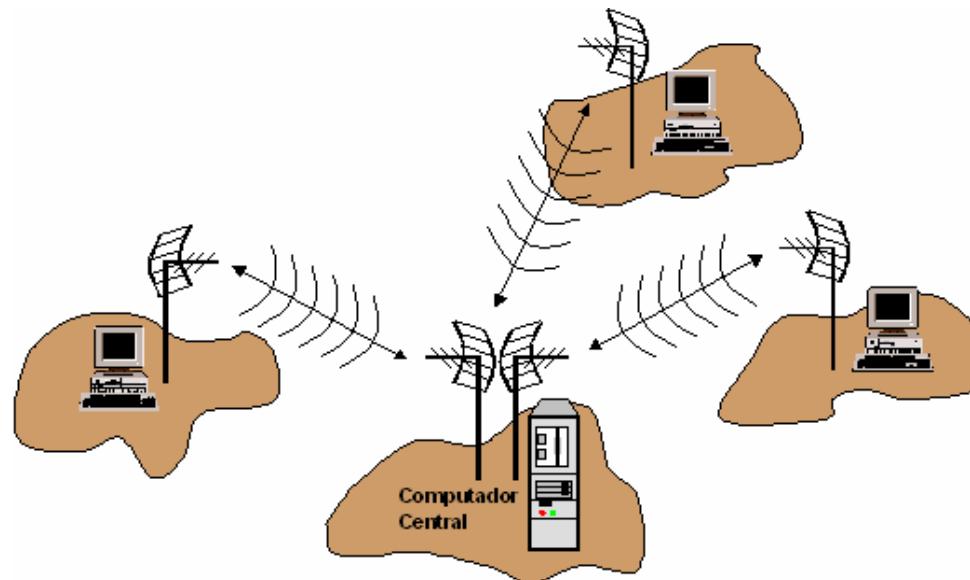
- Los nodos con estaciones que emiten sus tramas a un ritmo dado con independencia las unas de las otras.
- Existe un único canal compartido por todas las estaciones.
- Si dos nodos intentan transmitir el mismo tiempo se produce una “colisión”, es decir, una señal en el canal de trama errónea, detectable por todas las estaciones, y que implica la necesidad de retransmitir las tramas.

Los hay de contienda, sin colisión y de contienda limitada.

La red ALOHA:

Desarrollado en la Universidad de Hawái en la década de los 70

Objetivo: permitir las comunicaciones entre las estaciones y el computador central



Protocolo MAC de la red ALOHA

- Las estaciones periféricas transmiten cuando **quieren**.
- Cuando el computador central recibe una trama correcta envía una **confirmación**.
- Si la estación emisora no recibe esta confirmación dentro de un intervalo de tiempo dado (vencimiento), se entiende que la trama ha sufrido una **colisión**.
- Cuando transcurre el **tiempo de vencimiento**, es necesario retransmitir la trama colisionada. En este caso, las estaciones que sufrieron la colisión deben dejar transcurrir un **intervalo aleatorio** de tiempo adicional antes de la retransmisión.

El problema de los retardos

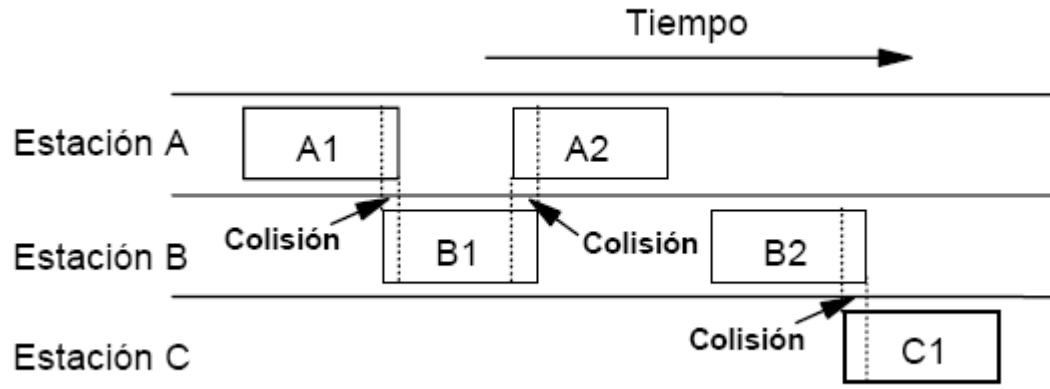
Debido a las distancias, los retardos de propagación pueden llegar a ser de varios milisegundos.

El tiempo que es necesario esperar para saber si una trama colisionó y así retransmitirla es considerable, reduciendo el rendimiento del protocolo

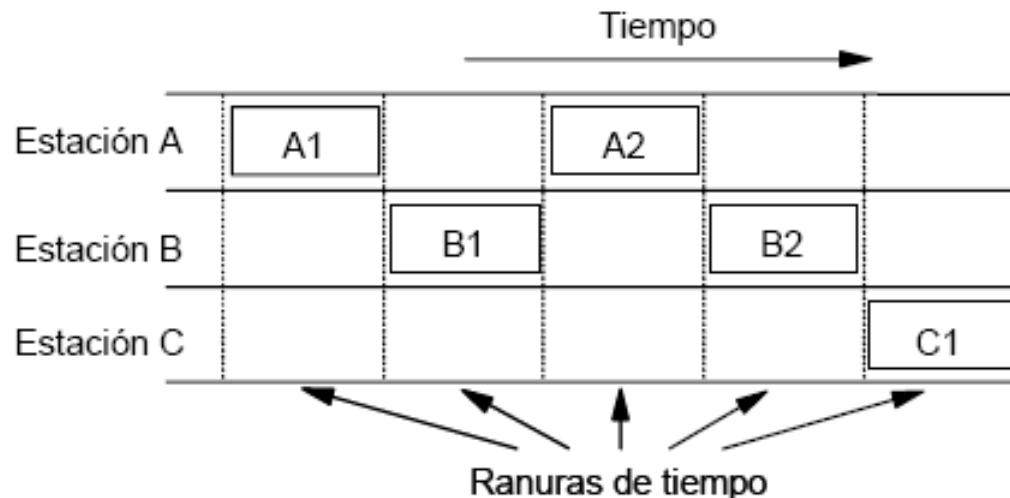
Versiónes del protocolo ALOHA

Versiones del protocolo ALOHA:

ALOHA puro (eficiencia del 18%)



ALOHA ranurado (eficiencia del 37%)



Protocolos con colisión: CSMA

Protocolo CSMA: Carrier Sense Multiple Access (acceso múltiple con detección de portadora)

Mejora con respecto al protocolo ALOHA: **detección de portadora**

Una estación de la red, antes de transmitir, escucha el canal:

1. Si el canal está **libre**, entonces **transmite**.

Si transcurrido un tiempo determinado el emisor no recibe confirmación, entonces se supone que la trama ha sufrido una colisión.

En caso de colisión hay que esperar un tiempo aleatorio para reintentar transmitir la trama.

2. Si el canal está **ocupado**, entonces se **espera** a que quede libre. En cuanto quede libre...

...En cuanto quede libre...

No persistente : Espera un tiempo aleatorio antes de intentar la transmisión.

1-persistente : La estación trasmite en cuanto se puede, sin esperar.

Si hay dos o más estaciones a la espera de que el canal quede libre para empezar a transmitir, éstas sufrirán una colisión con toda seguridad

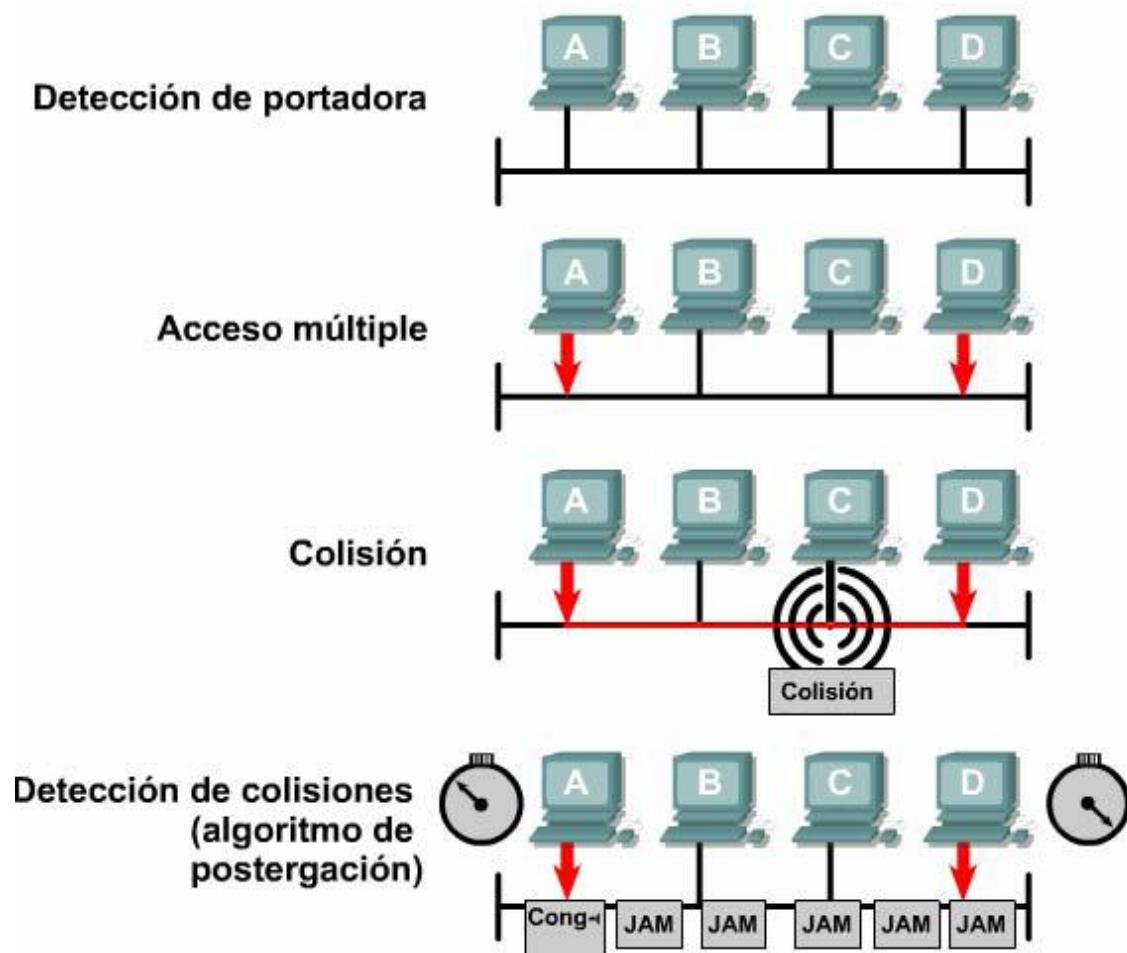
P-persistente: Con probabilidad $(1-p)$ espera un tiempo aleatorio antes de transmitir.

Con probabilidad p transmite en cuando se puede.

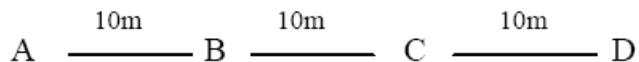
En caso de **colisión, en todos los tipos (1-persistente, p-persistente, y no persistente)**, se **espera un tiempo aleatorio** antes de intentar retransmitir la trama

CSMA/CD : Añade detección temprana de colisión, esperando un tiempo aleatorio para la retransmisión.

CSMA/CA : Se centra en evitar colisiones cuando el alcance de las estaciones depende de la distancia.



Supongamos cuatro ordenadores A, B, C y D situados en línea y separados 10 metros cada uno del siguiente:



Supongamos también que el alcance máximo de cada uno de ellos es de 12 metros.

Ahora imaginemos que implementamos un protocolo CSMA para su comunicación; la secuencia de sucesos para transmitir una trama podría ser la siguiente:

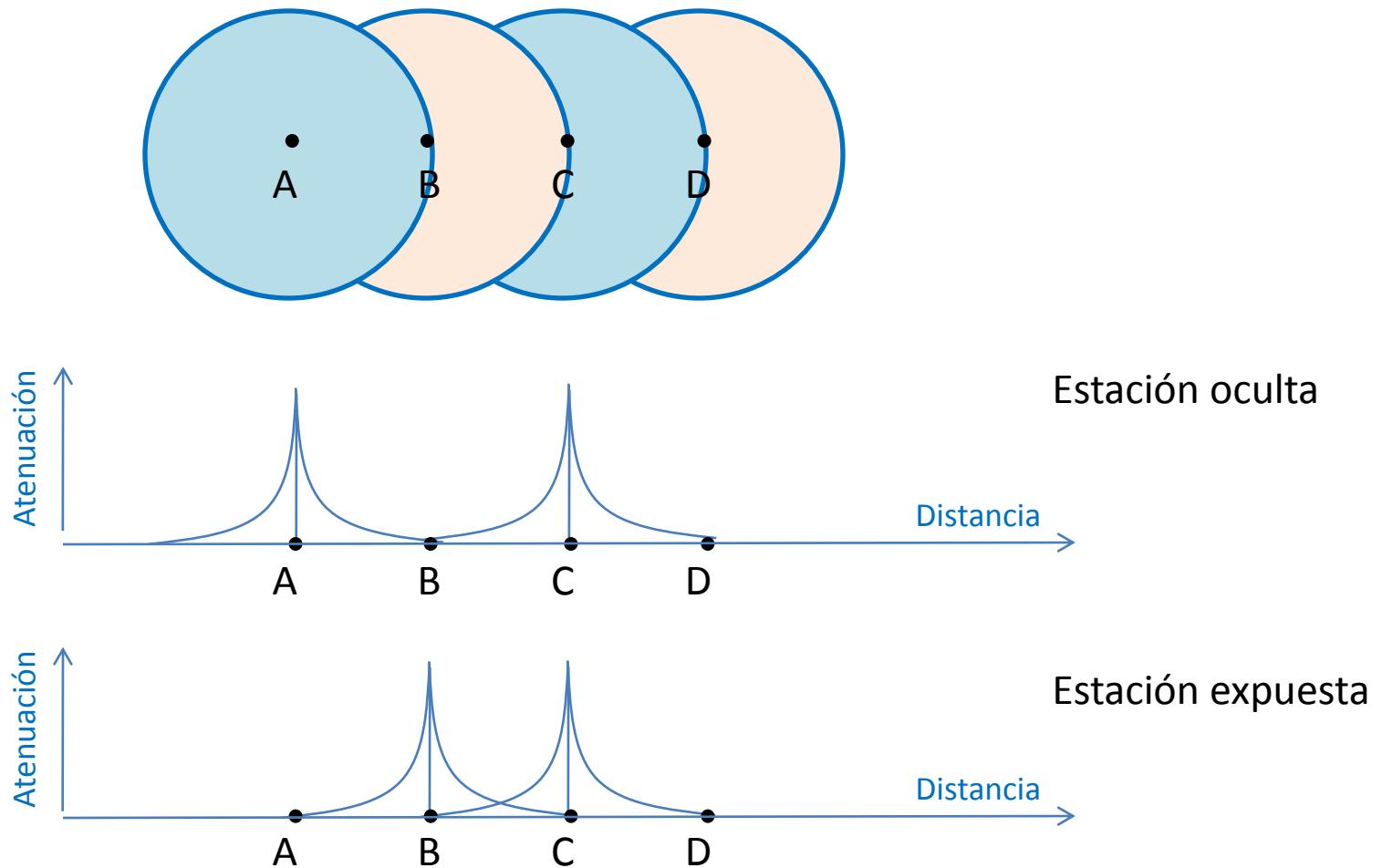
1. A desea transmitir datos a B; al detectar el medio lo encuentra libre y empieza la transmisión.
2. Con A transmitiendo C desea transmitir datos hacia B; detecta el medio y lo encuentra libre (C no escucha a A pues esta a 20m de distancia), por tanto C empieza a transmitir.

El resultado es una colisión en el receptor (B) que no es detectada ni por A ni por C. Esto se conoce como *el problema de la estación oculta*.

Imaginemos ahora la misma distribución de estaciones y otra secuencia de sucesos:

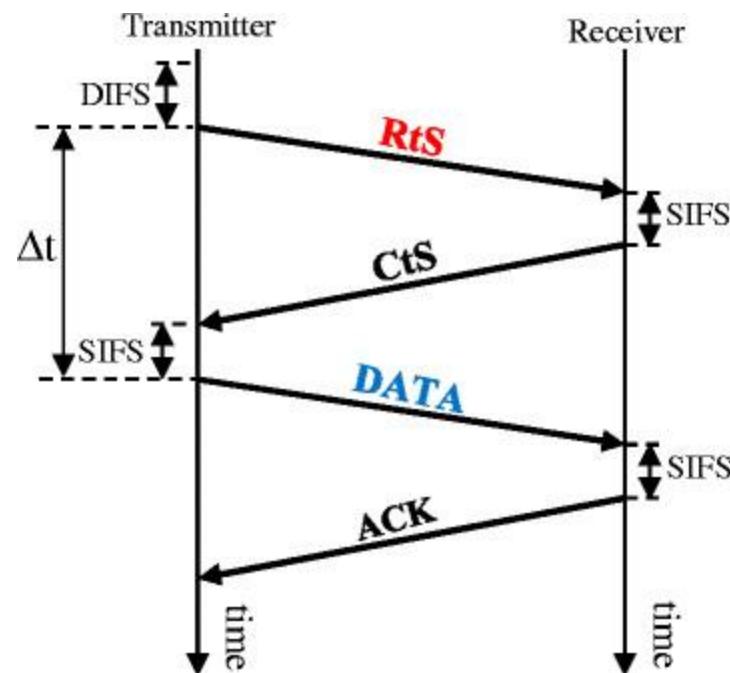
1. B desea transmitir datos hacia A, detecta el medio libre e inicia la transmisión.
2. A continuación C desea transmitir datos hacia D; como detecta que B está transmitiendo se espera a que termine para evitar una colisión.

El resultado es que una transmisión que en principio podría haberse hecho sin interferencias (ya que A no puede escuchar a C y D no puede escuchar a B) no se lleva a cabo, reduciendo así la eficiencia del sistema. Esto se conoce como *el problema de la estación expuesta*.



MACA (Multiple Access with Collision Avoidance) es el protocolo MAC que ha servido de base para el estándar IEEE 802.11 que es el que especifica el funcionamiento de LANs inalámbricas. MACA resuelve los dos problemas antes mencionados de la siguiente forma:

1. Cuando una estación tiene una trama que transmitir antes de enviarla envía una trama pequeña de aviso (de 30 bytes) denominada RTS (Request To Send). La trama RTS contiene información sobre la longitud de la trama que se pretende transmitir y la estación de destino.
2. Al recibir la trama RTS la estación de destino, si está en condiciones de recibir la transmisión, responde con otra trama denominada CTS (Clear To Send). La trama CTS también indica la longitud de la trama que se va a recibir.



Ahora apliquemos este protocolo al caso de la estación oculta para ver que ocurre:

1. A transmite una trama RTS a B indicando la longitud de trama que desea enviarle.
2. B responde con una trama CTS que también especifica la longitud de la trama. En este momento C capta la respuesta de B, por lo que se percata de que va a tener lugar una transmisión en la que B actuará de receptor y sabe que deberá permanecer en silencio durante el tiempo que dure la transmisión (C sabe lo que durará pues conoce la longitud de la trama y la velocidad de la red).
3. A envía a B la trama correspondiente.

En el caso de la estación expuesta ocurriría lo siguiente:

1. B transmite a A una trama RTS indicando que quiere enviarle datos. En ese momento C se entera de las intenciones de B.
2. A devuelve a B una trama CTS. Entretanto C, que ha captado el RTS pero no el correspondiente CTS, comprende que aunque detecta que B está transmitiendo el destinatario está fuera de su alcance, por lo que puede comunicar con D cuando quiera, sin esperar a que B termine.

Protocolos de paso de testigo

Se utiliza una trama con un formato especial, llamada **testigo**,

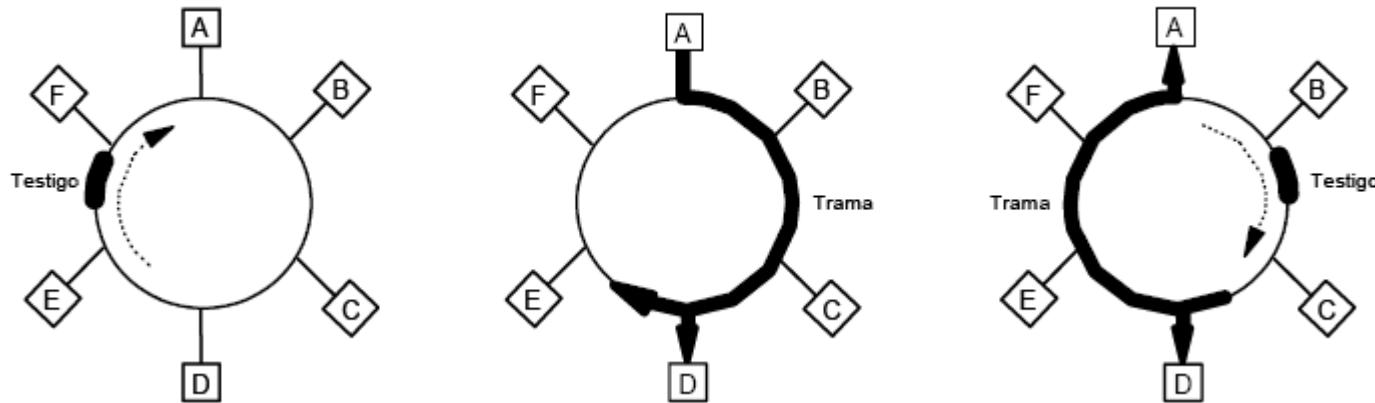
Esta trama va pasando de una estación a otra de forma **rotatoria**.

Cuando una estación desea transmitir debe esperar a recibir el testigo

Cuando lo tiene, puede transmitir, y sólo puede ella (sin colisiones).

El tiempo de posesión del testigo está limitado → **DETERMINISMO**

Ejemplo: **token ring** (paso de testigo en anillo) o **token bus**.



Suelen utilizarse cuando se trabaja con tiempo **ranurado**.

Cuando una estación quiere trasmisir, debe reservar una ranura temporal.

Ejemplos: BRAP, cuenta atrás binaria, y mapa de bits.

Protocolo de mapa de bits

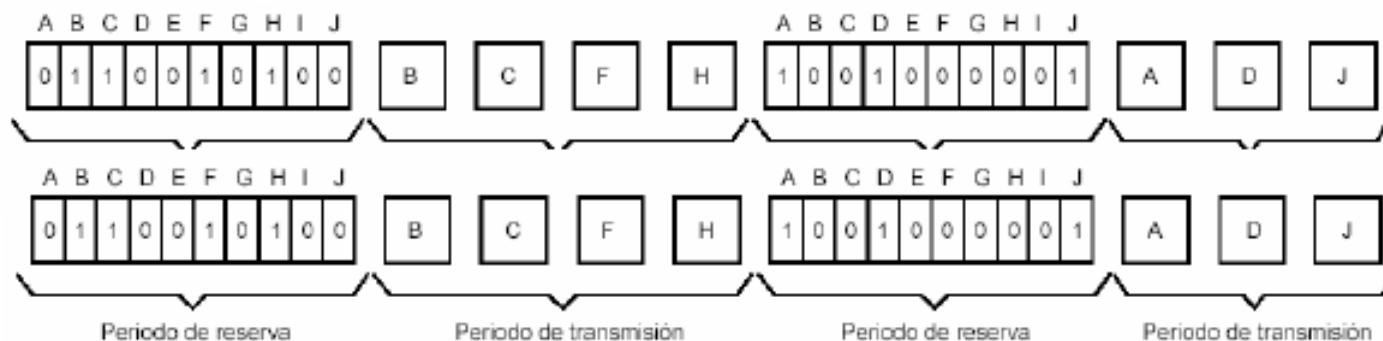
Periodo de reserva

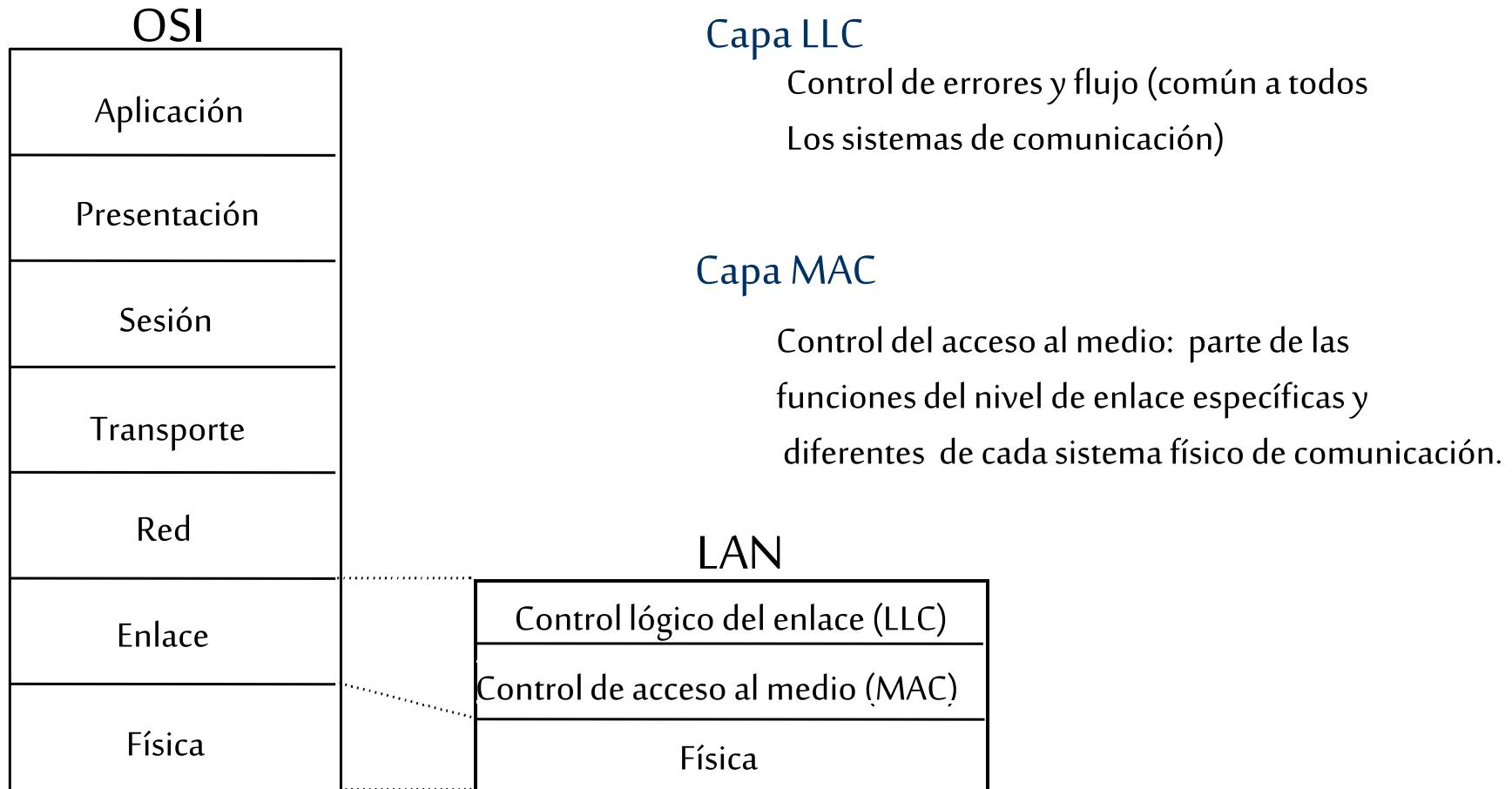
Está formado por una serie de bits de reserva, uno por cada estación conectada a la red.

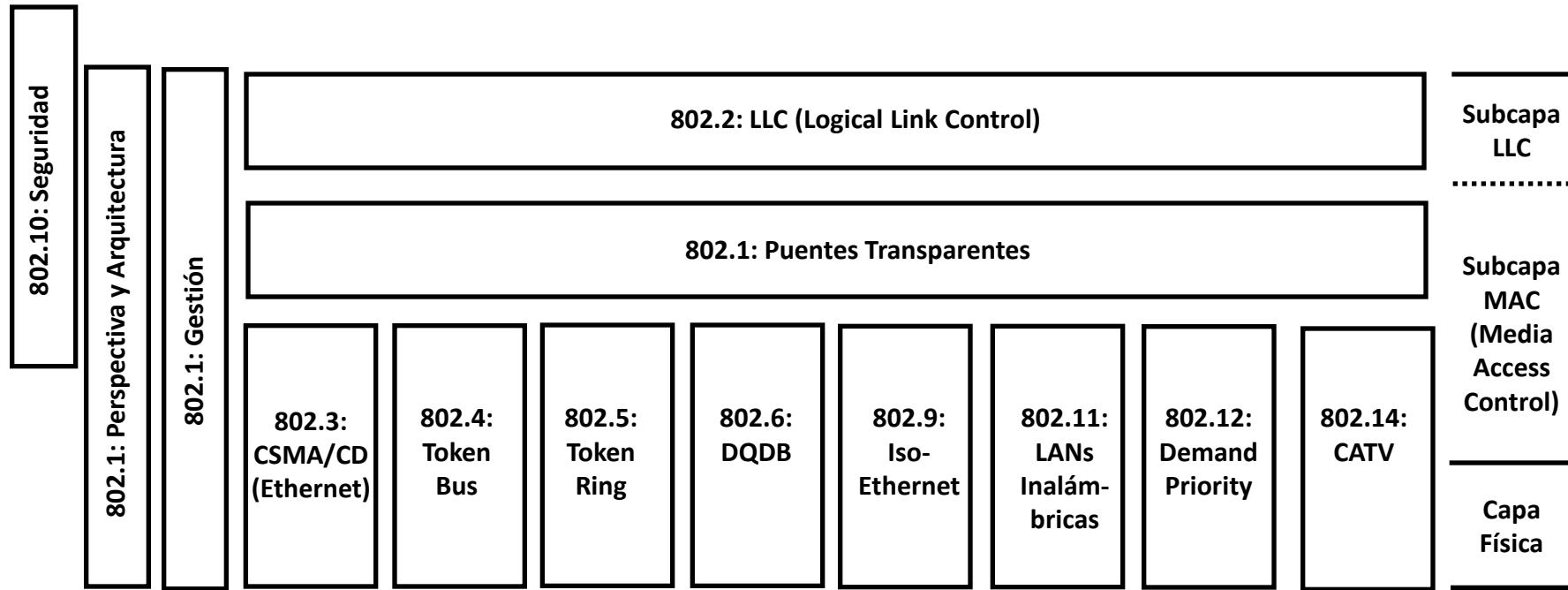
Cuando una estación desea transmitir debe poner un “1” en su bit correspondiente.

Periodo de transmisión

En este período, las estaciones que pusieron un 1 en su bit de reserva correspondiente pueden transmitir una trama de datos







Características:

-Desarrollado originalmente por Digital, Intel y Xerox (**DIX**)

-**Ethernet** define las características de cableado y señalización de nivel físico y las tramas del nivel de enlace del modelo OSI.

-Base para el **Estándar IEEE 802.3** que es **distinto**

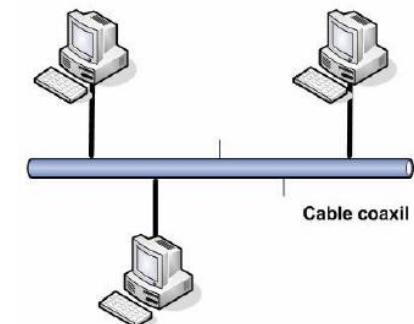
Ambos se diferencian en uno de los campos de la trama de datos.

Las tramas Ethernet y IEEE 802.3 pueden coexistir en la misma red.

-Método de acceso al medio: **CSMA/CD**

Distintas Topologías

Bus



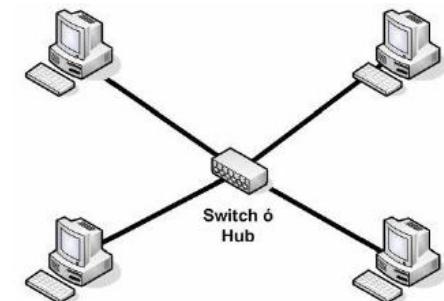
Estrella (HUB o SWITCH)

Distintos medios físicos

Cable Coaxial
Par Trenzado
Fibra óptica

Evolución de redes Ethernet

Ethernet 10 Mbps
Fast Ethernet 100 Mbps
Gigabit Ethernet 1Gbps
10Gigabit Ethernet 10Gbps



Cuando una estación quiere transmitir, debe realizar las siguientes acciones:

1. La estación escucha el canal
2. Si el canal está libre transmite inmediatamente
3. Si el canal está ocupado

Se queda escuchando a la espera de que quede libre

Cuando queda libre transmite inmediatamente (**1-persistente**).

4. Durante la transmisión

Sigue escuchando el canal.

Si información escuchada ≠ información transmitida: **Colisión**

5. En caso de colisión

Interrumpir inmediatamente transmisión

Enviar **señal de invalidación** a todas las estaciones

Iniciar mecanismo de contienda para retransmitir, esperando un tiempo aleatorio que aumenta progresivamente con cada intento hasta **16 intentos**.

Comparación entre DIX Ethernet y IEEE 802.3

Trama DIX Ethernet	Preámbulo	Destino	Origen	Tipo	Datos	Relleno	FCS	
	8 bytes	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	2 ó 4 bytes	
Trama IEEE 802.3	Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
	7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 a 1500 bytes	0 a 46 bytes	4 bytes

Preámbulo (7 bytes)

Patrón de bits 10101010 repetido 7 veces

Se utiliza para permitir que el receptor se sincronice con el emisor

Delimitador de inicio, SOF (1 byte)

Patrón 10101011 en IEEE 802.3 (en Ethernet era 10101010)

Dirección MAC destino (6 bytes)

Dirección física, MAC o Ethernet del destinatario de la trama.

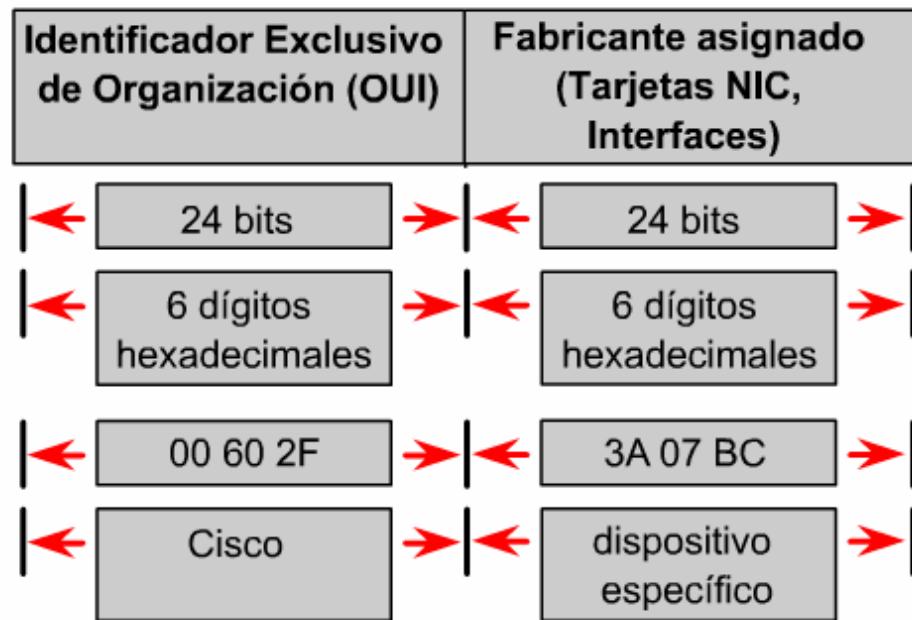
Puede ser individual (unicast), de grupo (multicast) o de difusión (broadcast)

Dirección MAC origen (6 bytes)

Dirección física (MAC o Ethernet) de la estación emisora de la trama

Tiene un formato similar al de la dirección destino.

Las direcciones MAC tienen 48 bits. Suelen representarse así a1:0c:d5:69:71:fe.
Vienen grabadas en las NICs.



Cada fabricante compra un rango (prefijo de 3 octetos) por 1000\$. Esta información es pública. Algunas aplicaciones la tienen y sustituyen el prefijo por el nombre del fabricante

Cada rango (prefijo de 3 octetos) permite fabricar $2^{24} = 16,777.216$ tarjetas de red.

Longitud / Tipo de Protocolo.

En IEEE 802.3

Indica la **longitud** del campo de datos. Es siempre **menor o igual a 1500 bytes**

En Ethernet

Indica el **tipo** de protocolo de la capa superior al que van dirigidos los datos.

Los valores de tipo siempre son **mayores que 1500**

Ejemplos:

IP = 2048 (0800 HEX);

ARP = 2054 (0806 HEX)

Datos (máximo 1500 bytes)

Contiene los datos transmitidos. Como máximo pueden ocupar 1500 bytes.

Relacionado con la **MTU** (Maximum Transfer Unit) de la red.

Relleno (máximo 46 bytes)

Bytes de relleno para el caso de tramas menores de 64 bytes

Código de redundancia (4 bytes)

Código para detección errores de transmisión.

Nomenclatura estándares: Se habla de Ethernet 10BaseT, 1000BaseLX,...

Velocidad	Método de señalización	Medio
10	BASE	2
100	BROAD	5
1000		-T
10G		-TX
100G		-SX
400G		-LX

Velocidad de transmisión
en Mbps.
 $10G = 10^6$ bps

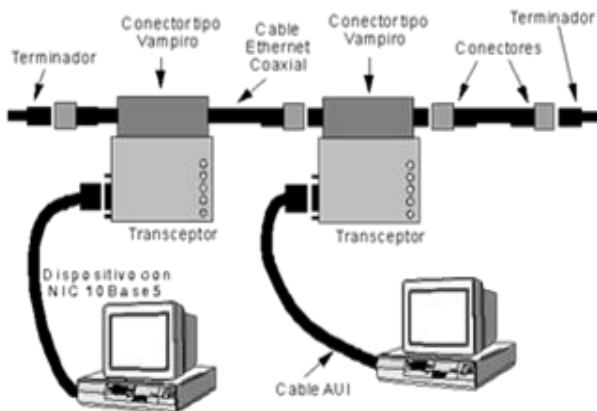
BROAD=banda ancha
(modulando)
BASE=banda base

2- cable coaxial (200 m aprox.)
5- cable coaxial (500 m aprox.)
T- Twisted (Par trenzado)
S- F.O corto alcance
L- F.O. largo alcance

X=Codificación y nº de canales

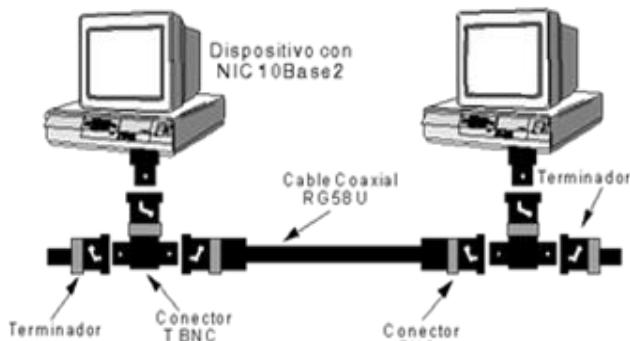
Tecnología	Cable	Distancia	Pares	Costo
10BASE5 10BASE2 10BASE-T 10BASE-F	Coaxial grueso 50 Ω	500 m	1	Bajo
	Coaxial fino 50 Ω	185 m	1	Bajo
	UTP-3/5	100/150 m	2	Bajo
	F.O. 1 ^a ventana	2 Km	1	Medio
100BASE-TX 100BASE-FX	UTP-5	100 m	2	Bajo
	F.O. 2 ^a ventana	2 Km	1	Alto
1000BASE-T 1000BASE-SX 1000BASE-LX	UTP-5e	100 m	4	Medio
	F.O. 1 ^a ventana	500 m	1	Medio
	F.O. 2 ^a ventana	5 Km	1	Alto
10GBASE-EX4	F.O. 3 ^a ventana	50 Km	1 (4λ)	Alto

10Base5 IEEE 802.3

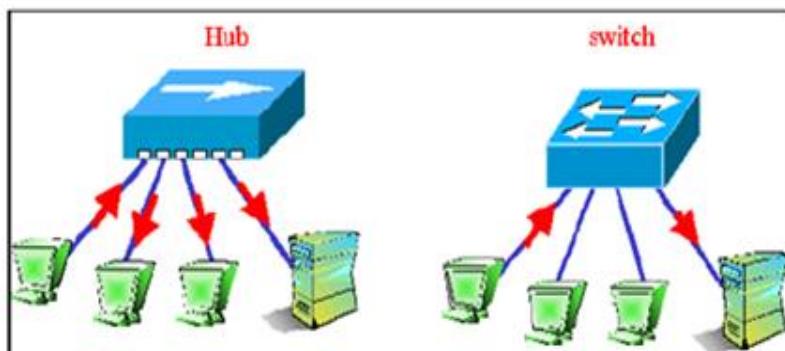


- Fue la primera implementación de ethernet (1980)
- Cable coaxial grueso de longitud máxima 500m.
- Precisa el uso de terminadores (50ohmios)

10Base2 IEEE 802.3a



- (1985) Red más barata sobre cable coaxial fino de 185 m. de longitud máxima
- Conectorización más fiable y sencilla (BNC)
- Precisa los mismos terminadores.



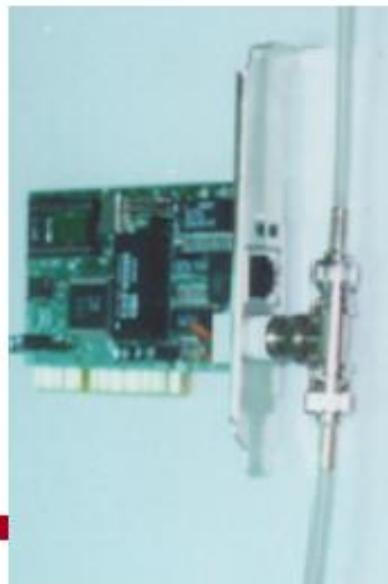
10BaseT IEEE 802.3i

- (1990) Definida sobre UTP cat-3
- Long. Máxima de 100m.
- Los equipos se conectan a hubs formando estrellas o estrellas extendidas.
- El uso de los switchs agrega el full-duplex.

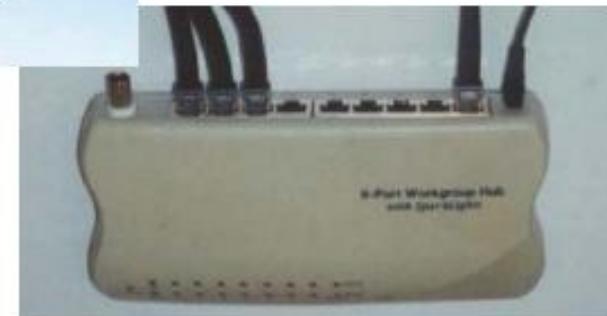
Ethernet

	10BASE5	10BASE2	10BASE-T
Medio Transm.	Coaxial grueso	Coaxial delgado	UTP cat. 3
Topología	Bus	Bus	Estrella con HUB
Modo de transmisión	Half-duplex	Half-duplex	Half-duplex
Velocidad	10 Mbps	10 Mbps	10 Mbps
Longitud máx.	500	185	100

Conexiones BNC para bus 10BASE2



Conexiones RJ-45 para hub 10BASE-T



Fast Ethernet

	100BASE-TX	100BASE-FX	100BASE-T4
Medio Transm.	2 pares UTP Cat 5	2 Fibras ópticas multimodo	4 pares UTP Cat 3
Topología	Estrella (HUB o Switch)	Estrella (HUB o Switch)	Estrella (HUB)
Modo de transmisión	HUB Half-duplex SWITCH Full-duplex	HUB Half-duplex SWITCH Full-duplex	Half-duplex
Velocidad	100 Mbps	100 Mbps	100 Mbps
Longitud máx.	100 m	Hasta 2000 m	100 m

Gigabit Ethernet

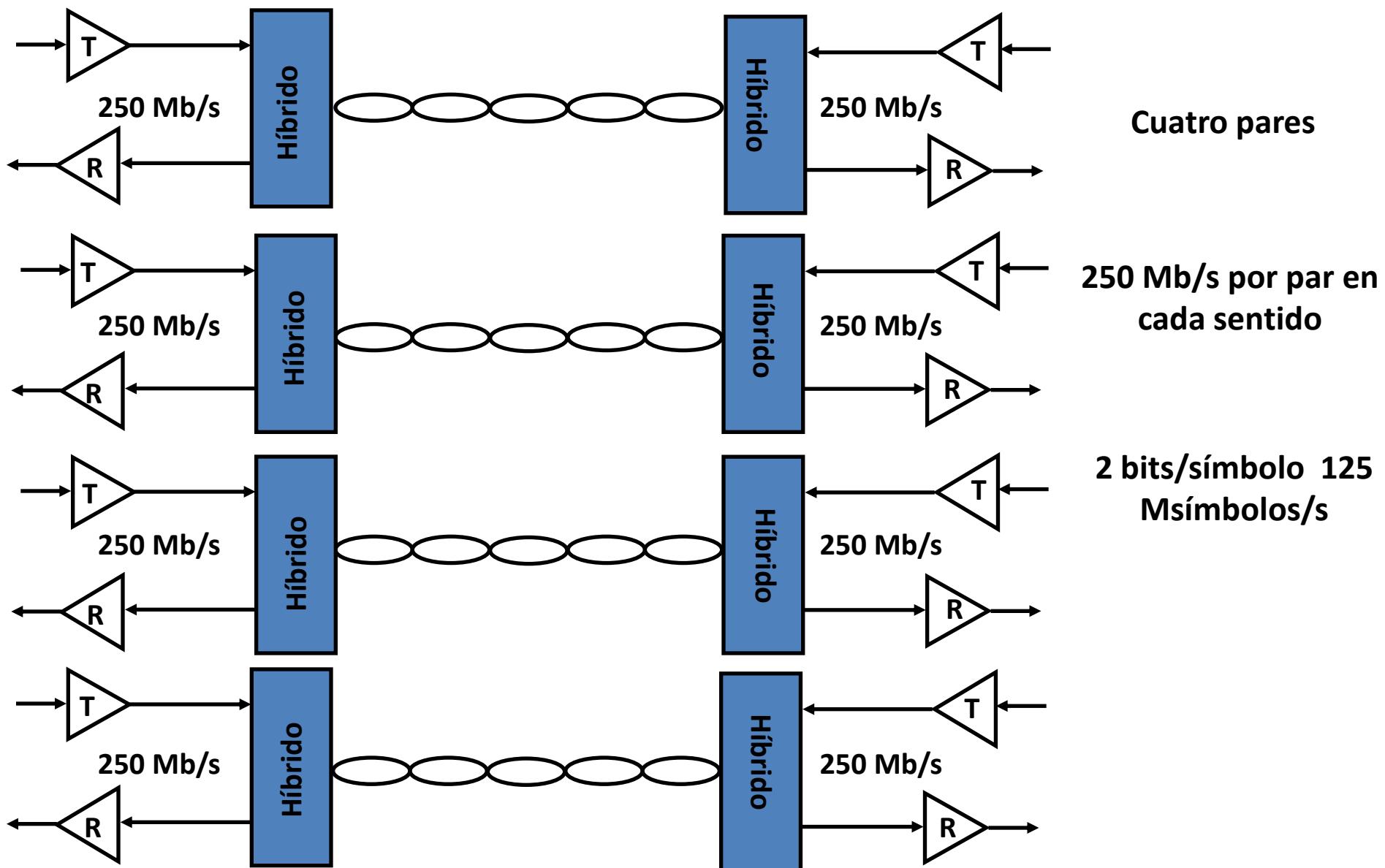
	1000BASE-SX	1000BASE-LX	1000BASE-CX	1000BASE-X
Medio Transm.	2 fibras óptica corto alcance	2 fibras óptica Largo alcance	2 pares STP	4 pares UTP Cat 5 o superior
Topología	Estrella (Switch)	Estrella (Switch)	Estrella (Switch)	Estrella (Switch)
Modo de transmisión	Full-duplex	Full-duplex	Full-duplex	Full-duplex
Velocidad	1 Gbps	1 Gbps	1 Gbps	1 Gbps
Longitud máx.	220-550 m	550-5000 m	25 m	100 m

10 Gigabit Ethernet (IEEE 802.3ae):

- Abandona CSMA/CD para ser punto a punto (**incompatible** con las anteriores).
- Hasta 40 Km en F.O. monomodo
- Compatible con un OC-192 de SDH

Tienen capacidad de autonegociación pudiendo coexistir con 10BaseT en la misma red

Medio	Veloc. (Mb/s)	Codific.	Pare s	Frec.M baud	Categ. Min.
Token Ring	4	Manch. Dif.	1	8	3
10BASE-T	10	Manchester	1	20	3
100BASE-X	100	4B/5B	1	125	5
100BASE-T2	100	PAM 5x5	2	25	3
1000BASE-TX	1000	PAM 5x5	4	125	5E
1000BASE-SX	1000	8B/10B	1	1250	F.O.
ATM	155,52	NRZ	1	155,52	5
10GBASE-EX4	10000	8B/10B	4	3125	F.O.
10GBASE-ER	10000	64B/66B	1	10300	F.O.

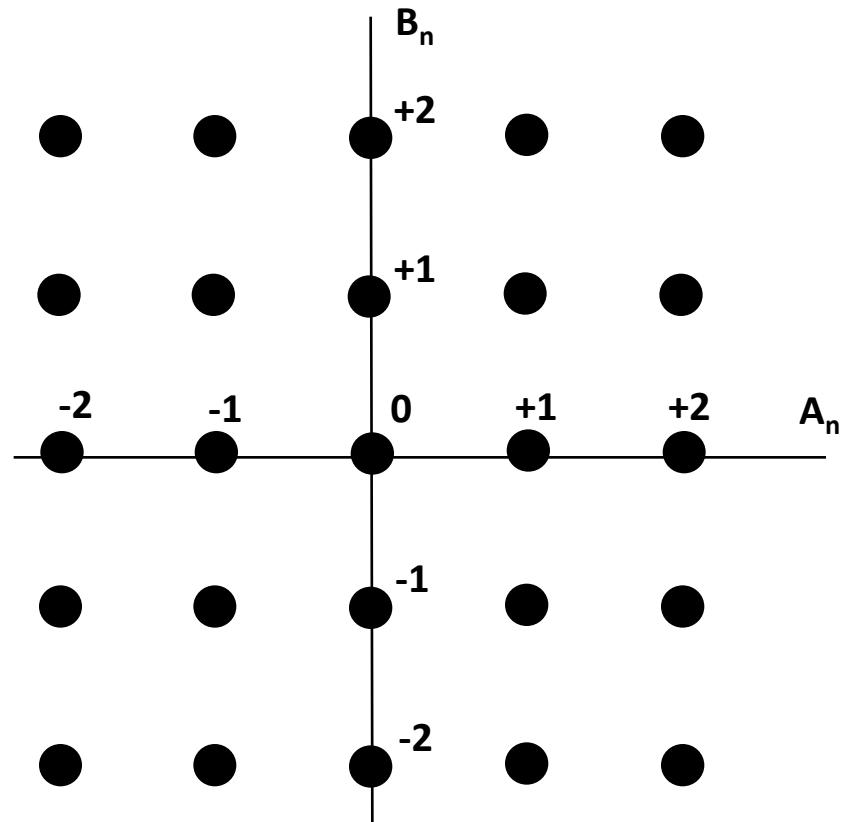


Codificación en Gigabit Ethernet

Codificación 4B/5B

Bits	Símbolo	Bits	Símbolo
0000	11110	IDLE	11111
0001	01001	J	11000
0010	10100	K	10001
0011	10101	T	01101
0100	01010	R	00111
0101	01011	S	11001
0110	01110	QUIET	00000
0111	01111	HALT	00100
1000	10010	No usado	00110
1001	10011	No usado	01000
1010	10110	No usado	01100
1011	10111	No usado	10000
1100	11010	No usado	00001
1101	11011	No usado	00010
1110	11100	No usado	00011
1111	11101	No usado	00101

Constelación de símbolos
en la codificación PAM 5x5



En 1000BaseX (fibra) se usa 8B/10B

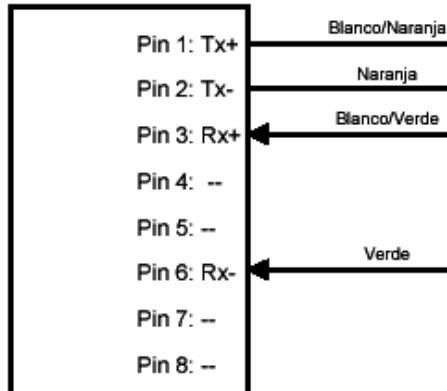
En 1000BaseT se usa PAM 5x5

Ethernet y Fast-Ethernet, cable directo y cruzado

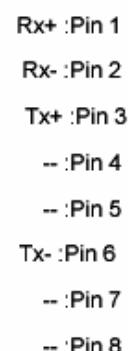
■ Cableado Ethernet (10BaseT y 100BaseTX)

■ Conexión Computador – Hub/Swicth

Estación con Adaptador
10BASE-T o 100BASE-TX



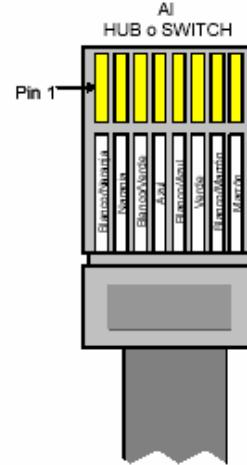
HUB o SWITCH
10BASE-T o 100BASE-TX



Al adaptador
10BASE-T
100BASE-TX

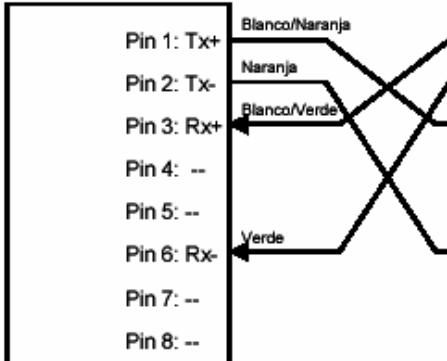


CABLE DIRECTO

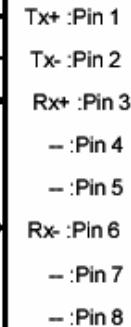


■ Conexión Computador-Computador

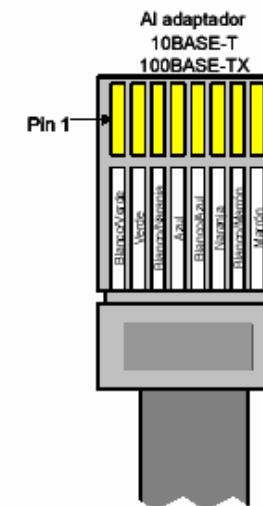
Estación con Adaptador
10BASE-T o 100BASE-TX



Estación con Adaptador
10BASE-T o 100BASE-TX



Al adaptador
10BASE-T
100BASE-TX

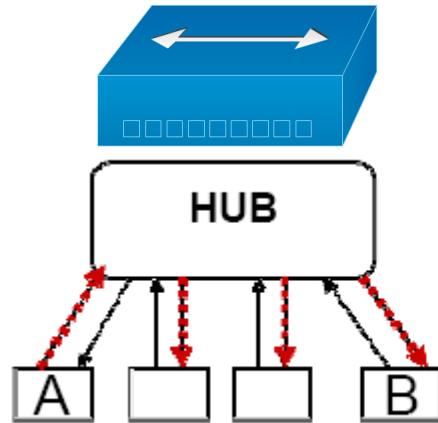


CABLE CRUZADO

Elementos de conexión en Ethernet

Hubs / Bridges / Switches

Concentradores o Repetidores / Puentes / Comutadores



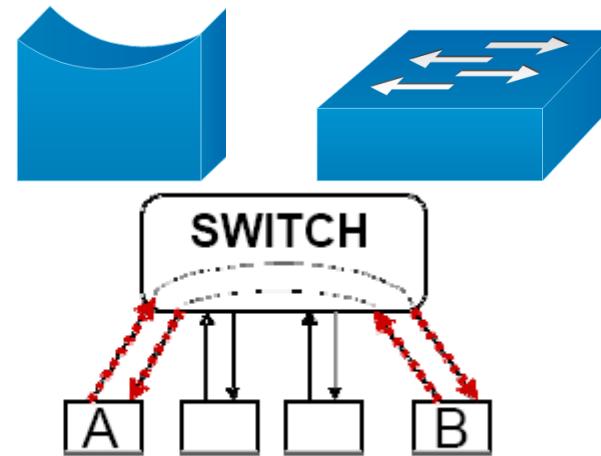
Repetidor (concentrador o hub)

Retransmite la información por todas las salidas.

Existencia de colisiones (necesario CSMA/CD)

Transmisión half-duplex

Privacidad baja



Comutador (switch, bridge si sólo tiene 2 bocas)

Retransmite la información únicamente por la salida adecuada

Libre de colisiones (no es necesario CSMA/CD)

Transmisión Full-duplex

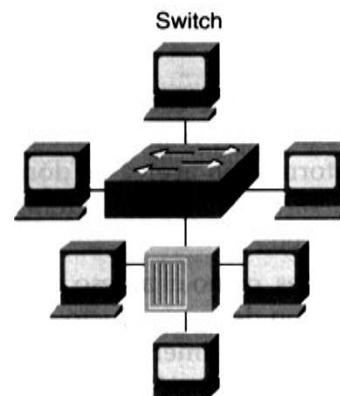
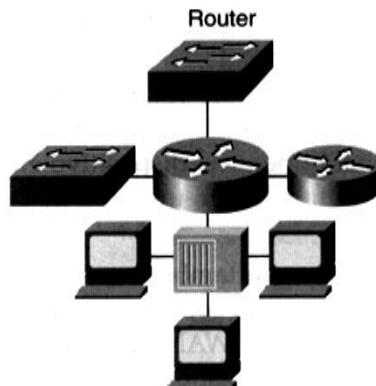
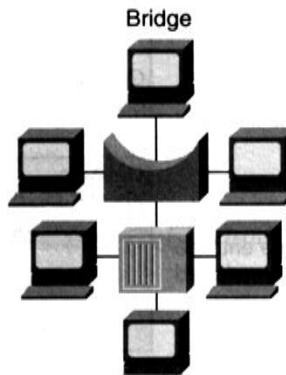
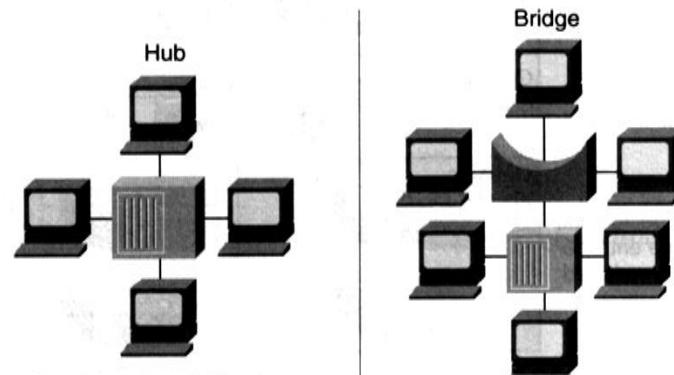
Privacidad elevada

Dominio de colisión y de difusión

Dominio de colisión:

Conjunto de equipos conectados a un medio donde se pueden producir colisiones de tramas.

Sólo los mantienen los hubs.



Dominio de difusión:

Conjunto de equipos susceptibles de recibir un mensaje dirigido a toda su red/subred.

Sólo los dividen los routers

Figura 1.25. Funciones de los dispositivos de red.

Preguntas:

1. ¿Qué campos debe comprobar un PC para saber que el paquete es IP cuando viene en formato IEEE 802.3?
2. ¿Qué protocolo usarías para controlar dispositivos de humedad y riego en una parcela de 200mx200m?
3. ¿Por qué Bluetooth es el protocolo más usado en dispositivos usualmente próximos?
4. ¿Por qué una compañía no puede usar wifi para dar servicio 5G?
5. ¿Qué alcance tiene Z-Wave?
6. ¿Cuál es la velocidad real cuando conecto con LTE en España?
7. ¿Cuál es la forma de pasar ficheros entre dos PCs con wifi más eficiente?
8. ¿Cómo se denomina la configuración topológica que usa Zig-Bee?
9. ¿Por qué es raro ver WiFis usando el canal 7?
10. ¿Qué debo usar para gestionar la seguridad en wifi de forma centralizada?
11. Si soy un hacker ¿con qué tipo de wifi me frotaría las manos?
12. ¿Cuál es la configuración wifi más eficiente y más segura?
13. ¿De cuántos equipos máximo es el dominio de colisión de una VLAN configurada en dos switches de 24 puertos?
14. ¿Por cuántos equipos como mínimo ha de pasar una trama que va de una VLAN a otra?

Protocolo LLC

LLC = control del enlace lógico (Logic Link Control)

Es el protocolo de enlace de las redes de área local y metropolitana
Estandarizado por la norma IEEE 802.2

LLC está basado en HDLC

Formato de trama similar

Incluye algunos campos adicionales

Mismos tipos de tramas

Información (I)

Supervisoras (RR, REJ, RNR)

Sin numerar (SABM, SABME, DISC, UA, ...)

Ofrece dos tipos de servicios

Orientados a conexión

Sin conexión

Formato LLC

Formato de tramas LLC

1 byte	1 byte	1 ó 2 bytes	1 byte	2 bytes	Tamaño variable
DSAP	SSAP	Control	ORG	Tipo	Datos

DSAP: Destination Service Access Point (protocolo de origen)

SSAP: Source Service Access Point (protocolo de destino)

DSAP y SSAP:

Puntos de acceso al servicio destino y fuente (como los puertos TCP pero para la entidad de nivel de red). Si los dos valen “AA” entonces se espera la extensión SNAP.

Control: Igual que en HDLC: identifica el tipo de trama, nº de secuencia, de confirmación, bit P/F, etc.

EXTENSION SNAP:

-**ORG:** Código de organización. En IP sería 00h.

-**Tipo:** Protocolo de red encapsulado. En IP 0800h (2048) en ARP 0806h(2054)

Tipos de tramas LLC

Tramas de información (I)  Campo Control =

1	2	3	4	5	6	7	8
0	N(S)	P/F	N(R)				

Se utilizan para transmitir datos en servicios orientados a conexión

Incluyen nº de secuencia, N(S), y nº de confirmación, N(R)

1	2	3	4	5	6	7	8
1	0	S	P/F	N(R)			

Tramas supervisoras  Campo Control =

1	2	3	4	5	6	7	8
1	0	S	P/F	N(R)			

En LLC se usan sólo tres tipos de tramas supervisoras

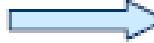
RR (Receptor Ready) trama de confirmación positiva (ACK)

REJ (Reject) trama de confirmación negativa (NAK) para RQ continuo con retroceso-N

RNR (Receptor Not Ready) trama de confirmación para suspender el envío de tramas

No se usan tramas SREJ

1	2	3	4	5	6	7	8
1	1	M	F/F	M			

Tramas sin numerar  Campo Control =

1	2	3	4	5	6	7	8
1	1	M	F/F	M			

Las tramas más sin numerar comunes son las siguientes:

SABM/SABME Establecimiento de conexión en modo ABM

DISC Desconexión

UA Confirmación sin numerar

UI Información sin numerar

FRMR Rechazo de trama (formato inválido)

RSET Reinicio de conexión

El protocolo LLC

Servicios orientados a conexión

Establecimiento de conexión

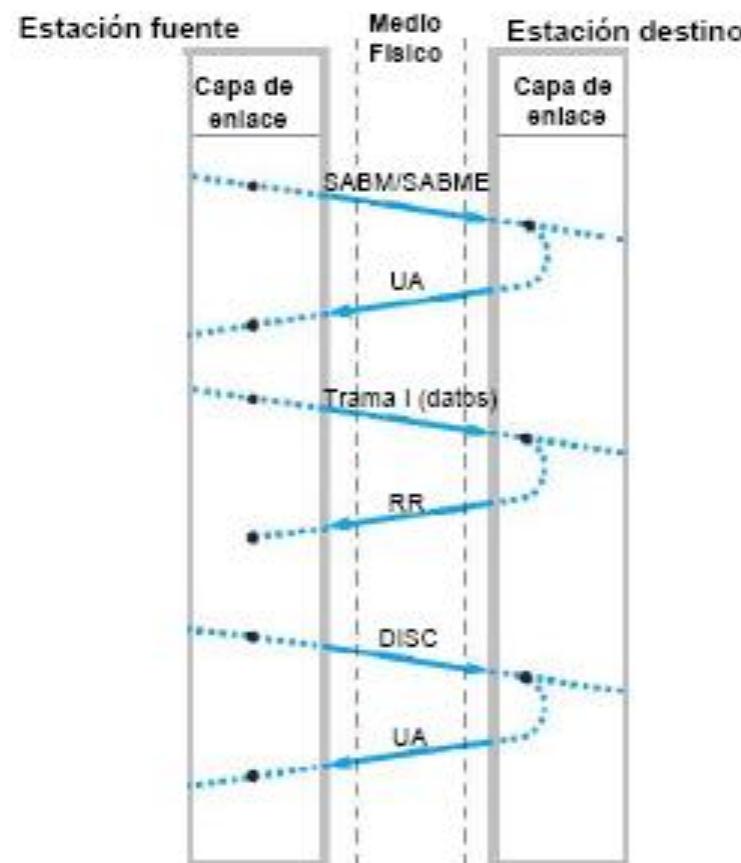
Tramas: SABM/SABME, UA (sólo se usan conexiones en modo ABM)

Transmisión de datos

Tramas: I, RR, REJ, RNR

Desconexión

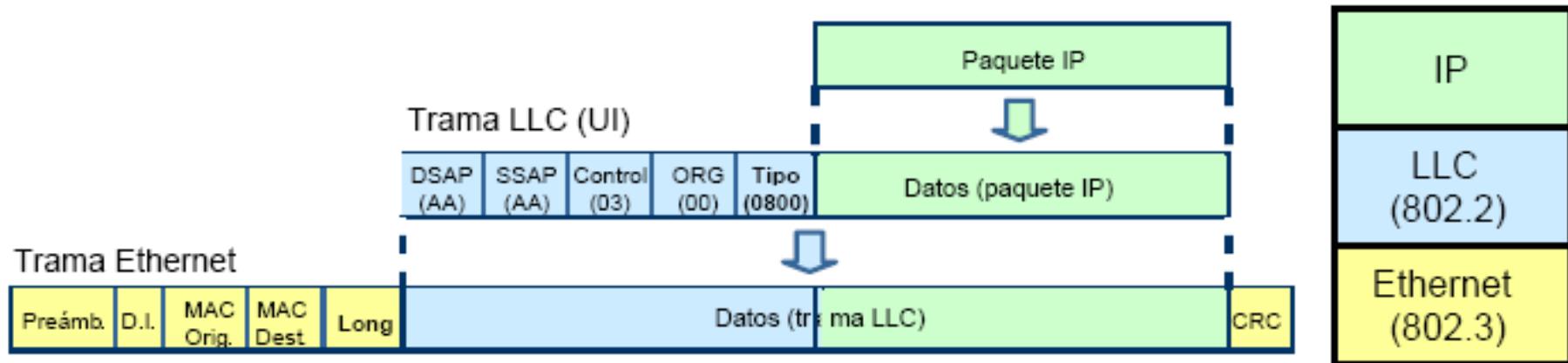
Tramas: DISC, UA



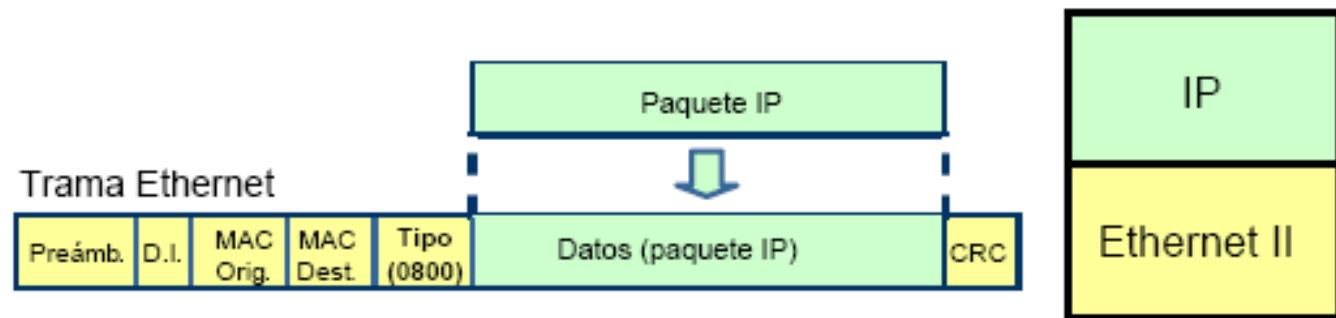
LLC para Ethernet

Ethernet II vs. IEEE 802.3 (2)

Encapsulado de IP sobre LLC (802.2) y Ethernet (802.3)



Encapsulado de IP sobre Ethernet II



D.I. Es el Delimitador de Inicio (SOF)

Token Bus

Desarrollado por General Motors para entornos industriales, es la base de la **pila MAP**. (Protocolos de Automatización de Procesos)

El medio de transmisión es el **cable coaxial** de banda ancha a **10Mbps**.

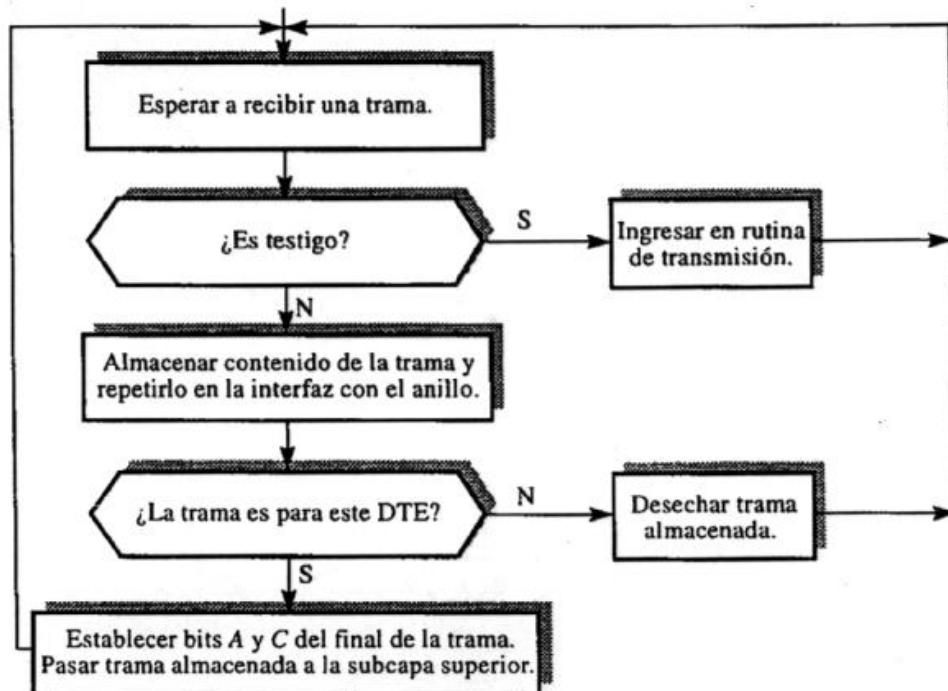
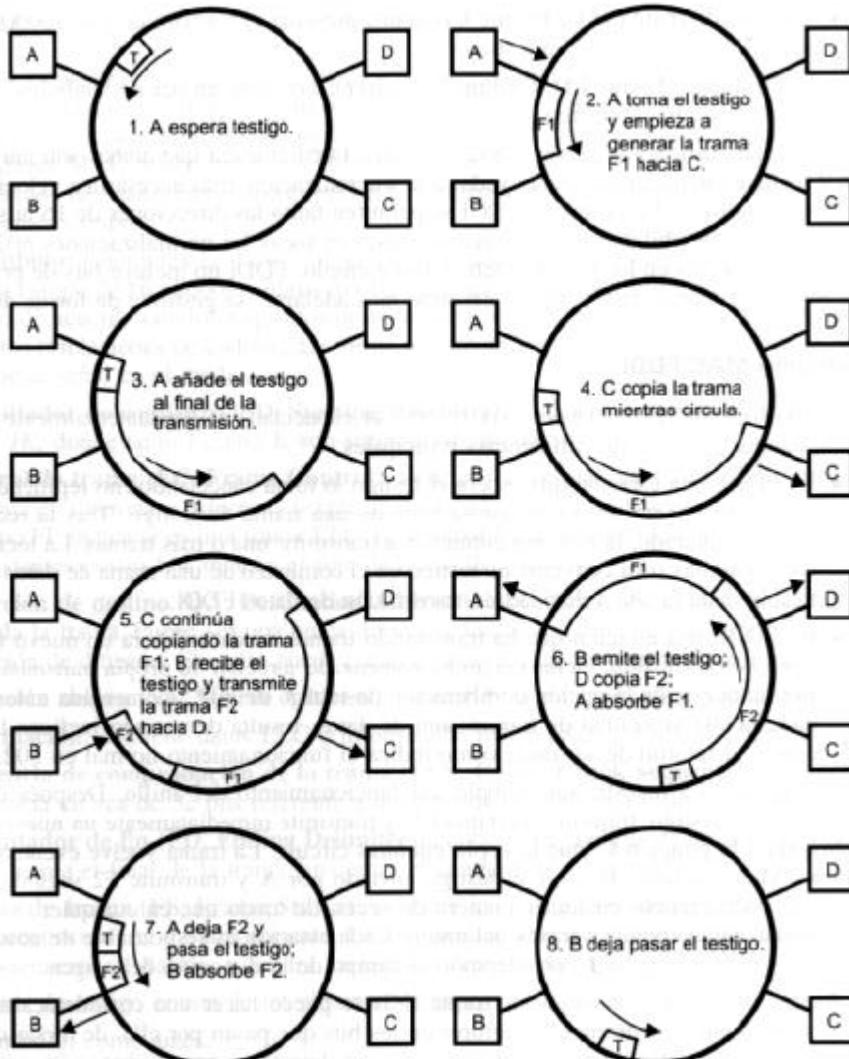
Es **determinista** y admite priorización de tramas.

Un **testigo circula por el bus** siguiendo el orden de las direcciones MAC de los nodos, otorgando permiso de transmisión por un tiempo máximo (10ms).

Utiliza el servicio **LLC tipo 1** (sin conexión ni control de secuencia).

La gestión del testigo incluye las eventualidades de **inicio de la secuencia, incorporación y desaparición de nuevos nodos**.

Token Ring



- Desarrollada por IBM en paralelo a Ethernet
- 4 o 16 Mb/s. Recientemente 100 Mb/s.
- Manchester Diferencial (mas robusto)
- Cable STP, UTP-3, UTP-5 y F. O.
- Topología lógica de anillo.
- Protocolo sin contención (sin colisiones)

FDDI

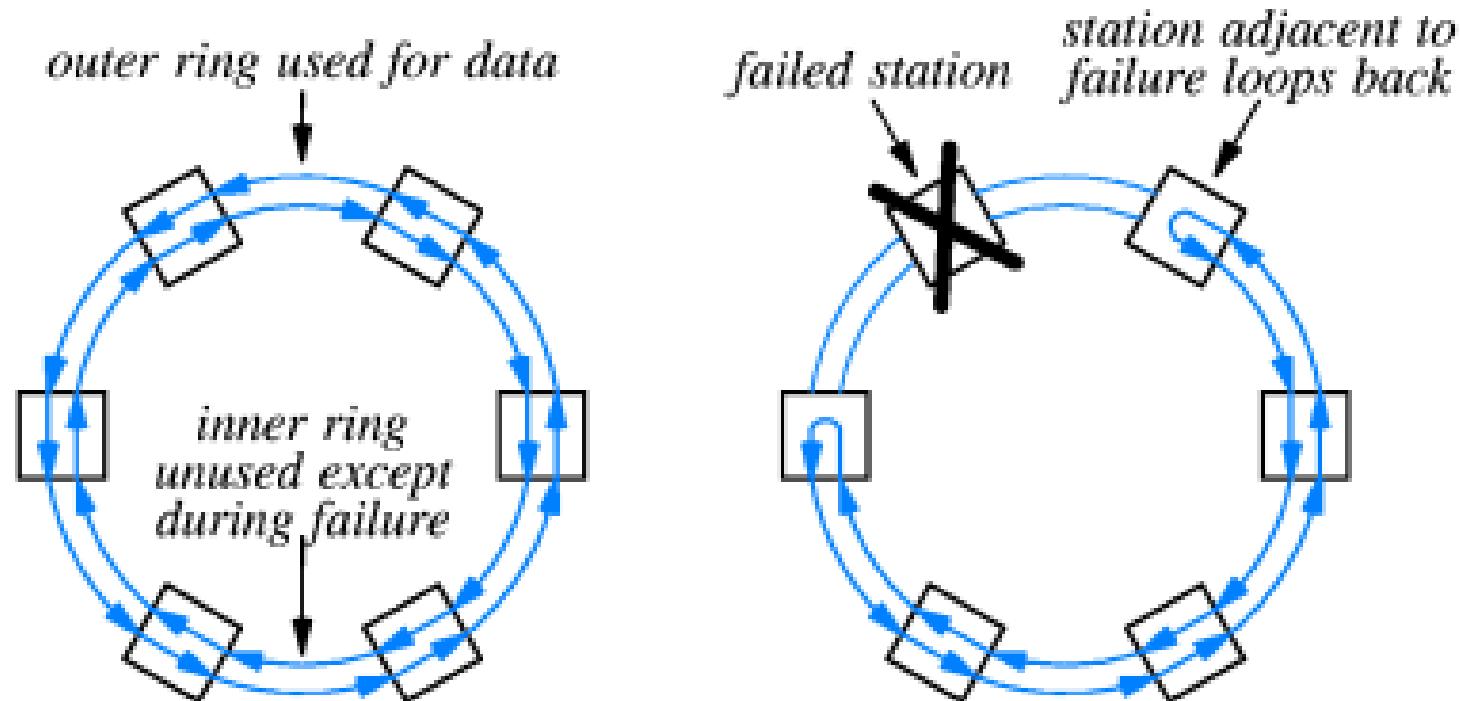
Es una red de **fibra óptica** de alto rendimiento muy parecida a token ring.

Transmisiones a **100Mbps** en anillos de hasta 200Km con hasta 1000 nodos

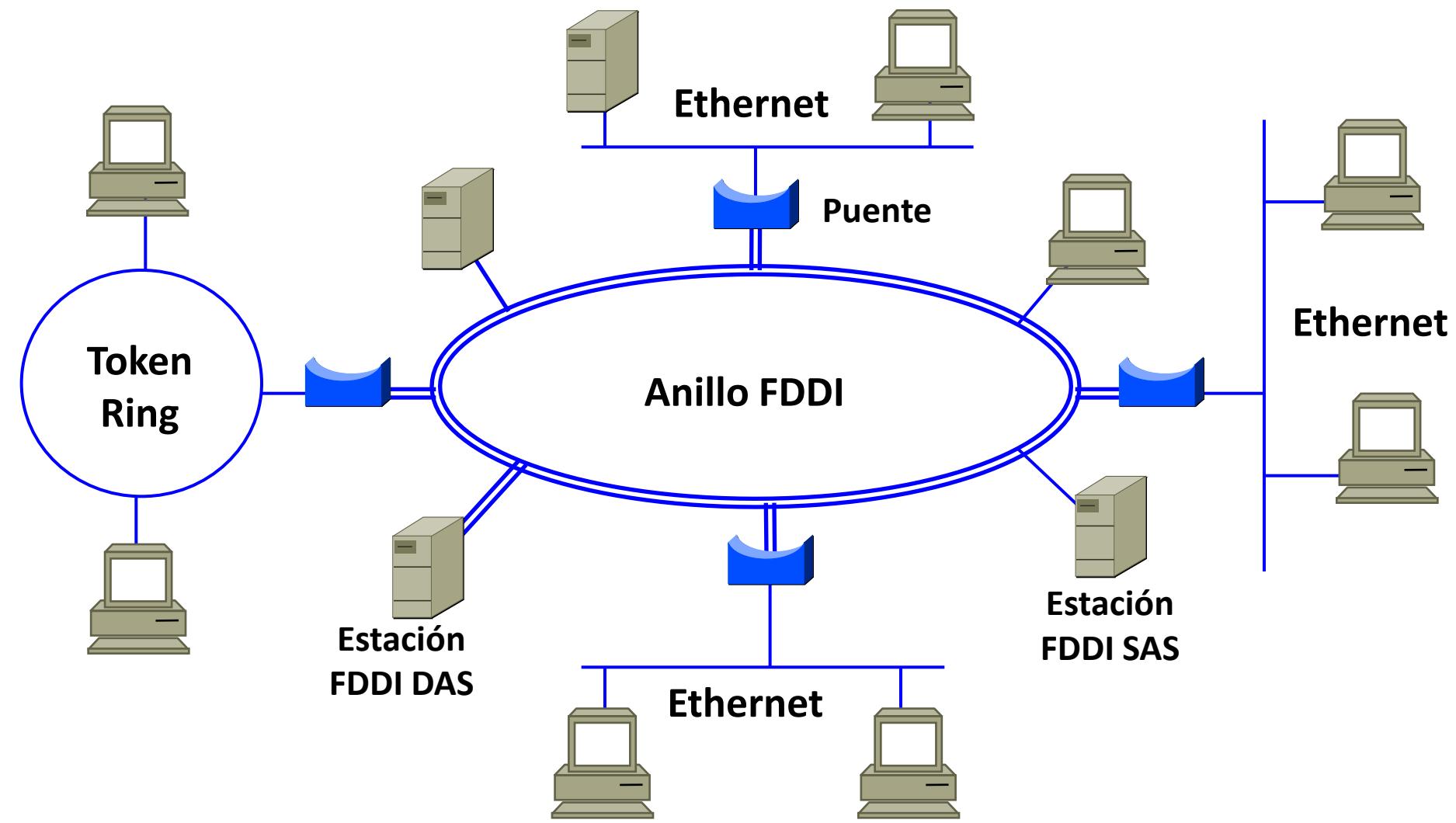
Se usa codificación **4B5B** a 125 Mhz.

No hay señal de **sincronismo**: los relojes de las estaciones deben ser muy precisos y es necesario dotar a las tramas de un preámbulo más largo.

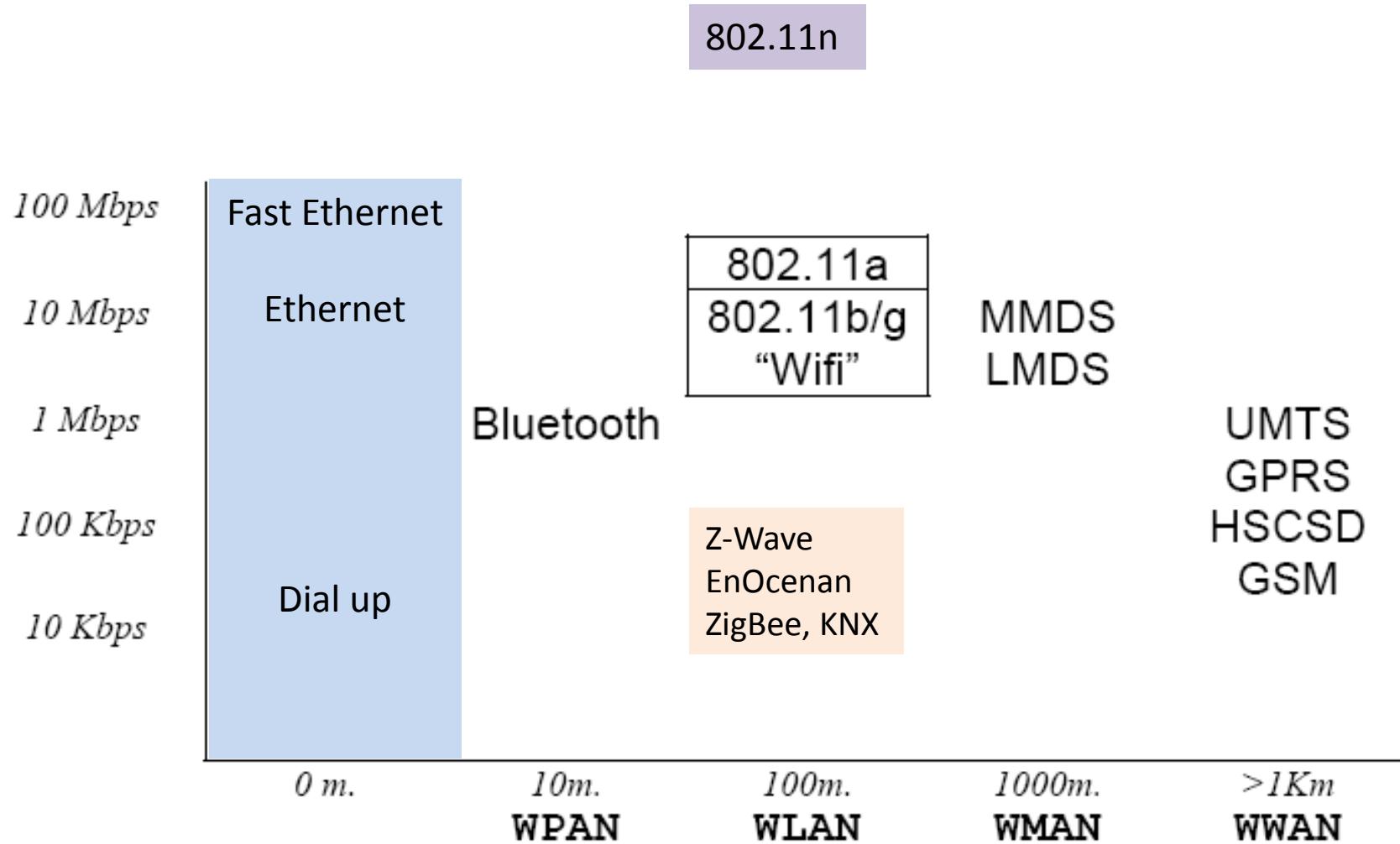
Su uso es más apropiado para interconectar redes (“**backbone**”) que para LANs



Uso de FDDI como ‘backbone’ entre LANs

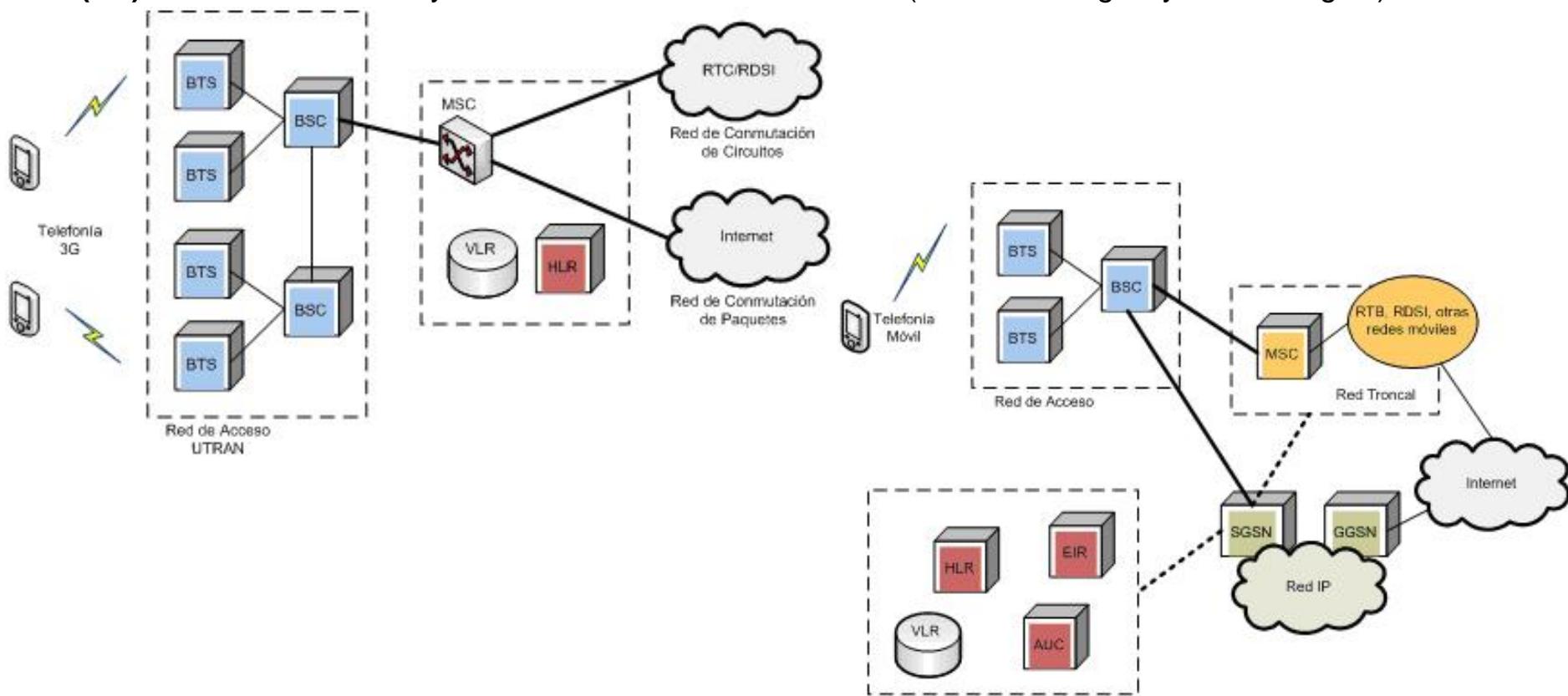


LAN inalámbricas



GSM, GPRS, UMTS

GSM (2G): 800-1900MHz. voz y SMS. Conmutación de circuitos. (1G era analógica y ésta es digital)



GPRS comutación de paquetes (navegación web). velocidades de 60 Kbps. Se aplica sobre la red GSM ya desplegada incorporando dos nuevos elementos como se muestra en la figura anterior:

SGSN. Conmuta paquetes, funciones de movilidad, autenticación y facturación.

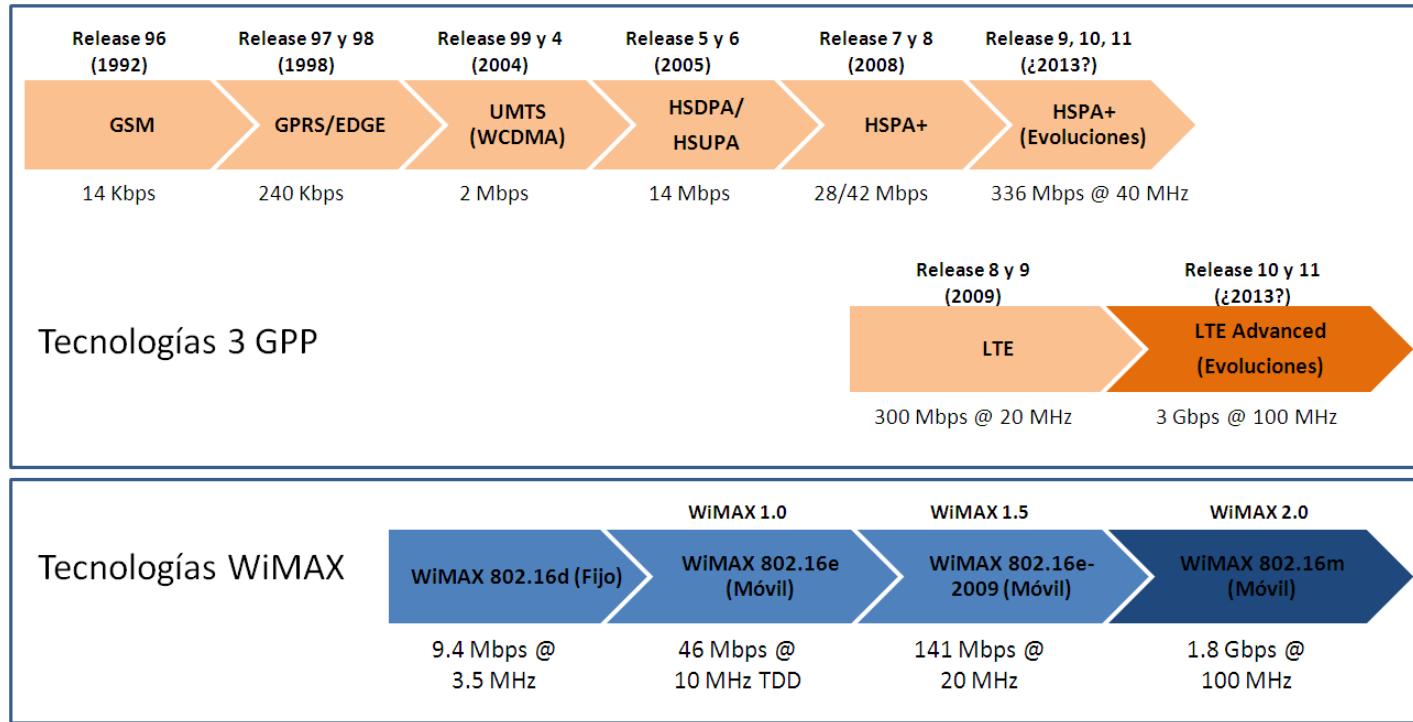
GGSN. Responsable de la interconexión con redes de paquetes externas y redirecciónamientos

GSM, GPRS, UMTS

2G(digital)

3G(1Mps)

4G(1Gpbs) 5G(2Gbps)



EDGE: 470 kbps. Formalmente 3G, práctica: 2,9G

UMTS:2 Mbps (3G)

HSPA: 14 Mbps

WIMAX: 134Mbps en celdas de 5km.

LTE: 300Mbps (50 en la práctica) (4G?)

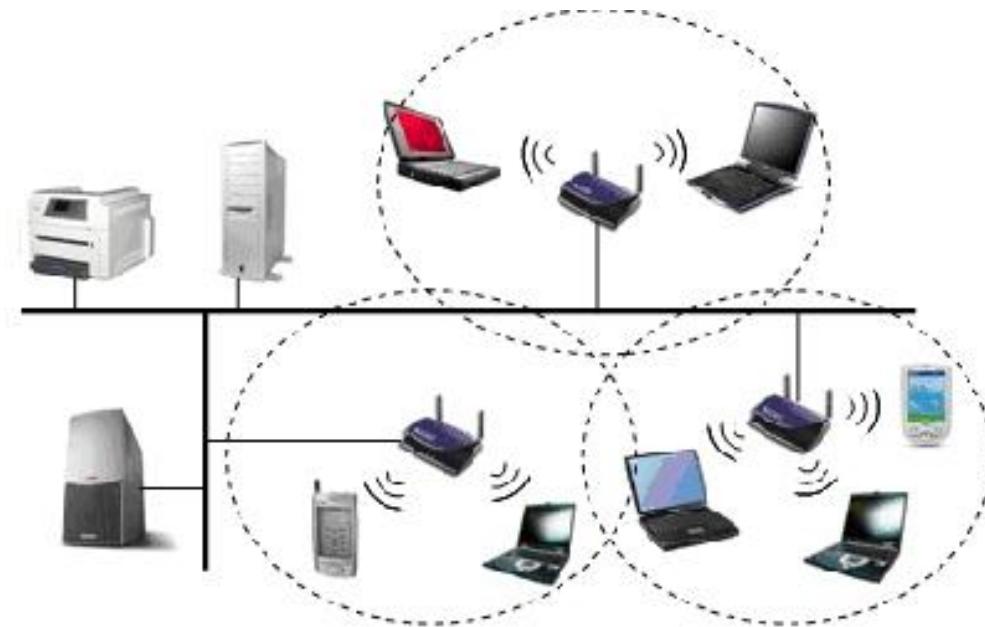
España: Yoigo da LTE 20-40 Mbps en la práctica. Vodafone da 5G en las principales ciudades
Wimax media de 15 Mbps.

IEEE 802.11.Definiciones

Las redes de área local inalámbricas (WLANs) se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación.

Las antenas pueden ser:

- Omnidireccionales. Menor alcance, independencia de la orientación.
- Direccionales



Constituidas por:

- TR (terminales de red)
- PA (Puntos de acceso)

La configuración puede ser:

-Ad-hoc: Cuando no existe punto de acceso. Modo “Master” en cada TR. Además existen las especificaciones wifi **Direct** y el enlace directo **TDLS**.

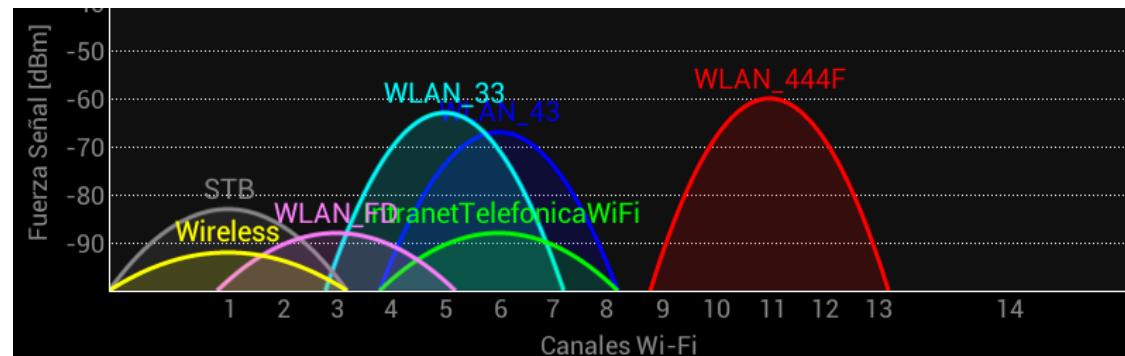
-Infraestructura: Todos los equipos hablan con el PA. Modo “Master” en el PA y “Managed” en todos los TR.

-Redes acopladas (redes “mesh”): Combinación de los anteriores

Estándares WLAN

Estándar	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n	Bluetooth IEEE 802.15.1	HiperLAN/2
QoS	No	No	No	No	Si	Sí
Finalización	2002	1999	2003	2009	2005	2000
Banda de frecuencias	5 GHz	2,4 GHz	2,4 GHz	2,4 - 5 GHz	2.4 GHz	5 GHz
Tasa máxima	54 Mbps	11 Mbps	54 Mbps	600 Mbps	3 Mbps	54 Mbps
Otras características	Incompatible con b y g	Compatible con g a 11Mbps	Compatible con b a 11 Mbps	Compatible con anteriores	No interfiere con wifi a partir de v1.2. Muy bajo consumo. Hasta 10m (PAN).	Desarrollado por el ETSI

Estándares WLAN - WIFI



CANALES:

En torno a los 2,5 GHz hay un ancho de banda (20MHz) dividido en canales (1-11 en USA, hasta el 13 en EU y hasta 14 en Japón). Para evitar interferencias se eligen canales simultáneos separados de 5 en 5 (ej:1-5-11).

En torno a los 5 GHz el W=40MHz, lo que da 23 canales NO SOLAPADOS.

MIMO:

Las antenas múltiples sirven para mejorar la SNR sin aumentar la potencia de emisión.

EXTENSORES O REPETIDORES:

Aumentan el alcance del PA. Al consumir el mismo ancho de banda suponen una merma en la capacidad de tráfico total de la red.

WPS (WiFi Protected Setup):

Es una utilidad para autoconfiguración de WPA. Se basa en un pin que el usuario introduce en cada uno de los equipos o en un botón. Es vulnerable a ataques de fuerza bruta.

Seguridad en redes inalámbricas

1- Ocultar el **SSID: Service Set Identifier**. Nombre que va a ser radiado por el PA WIFI.

2- Encriptación: WEP/WPA:

- WEP** (Wired Equivalent Privacy) , cifra los datos con una clave pre-compartida (64-128 bits) **fija**.
- WPA**: (Wi-Fi Protected Access) presenta mejoras:
 - Cambio dinámico de las claves de acceso (TKIP).
 - WPA2**: Compatible con IEEE 802.11i
 - Mejora el cifrado con CCMP que usa AES.

Enterprise: permite uso de servidores RADIUS para claves

EAP: alternativa a Enterprise para la autenticación: (EAP-TLS, EAP-OTP, EAP-MD5...).

3- **IPSEC** (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

4- Filtrado de **MAC**, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.

Figure 1: Encrypted WEP frame

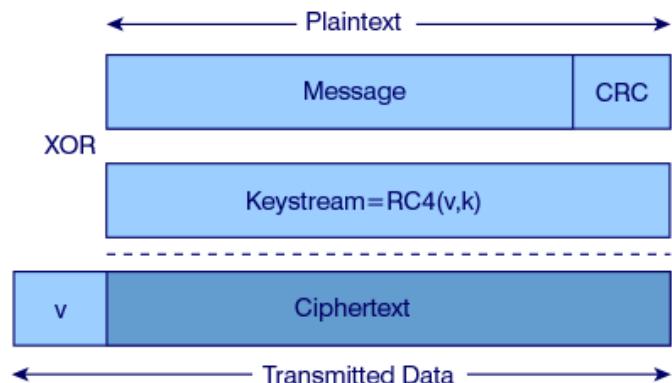


Figure 1: Encrypted WEP frame

Éstas son válidas
también para redes
Ethernet.

Bluetooth

Especificación para Redes Inalámbricas de Área Personal (**WPANs**) que posibilita la transmisión de voz y datos (2,4 GHz).

Diseñado para generar el **mínimo consumo** posible en los dispositivos.

El nivel físico utiliza **saltos de frecuencia** (frequency hopping) en un conjunto amplio portadoras para evitar interferencias. Se realiza una permutación aleatoria de 79 frecuencias en la banda ISM. Algunas de ellas pueden no utilizarse si presentan interferencias frecuentes (“compatibilidad” con wifi).

Se utiliza modulación en frecuencia y se alcanzan velocidades de transmisión de **1, 2 ó 3Mbps**.

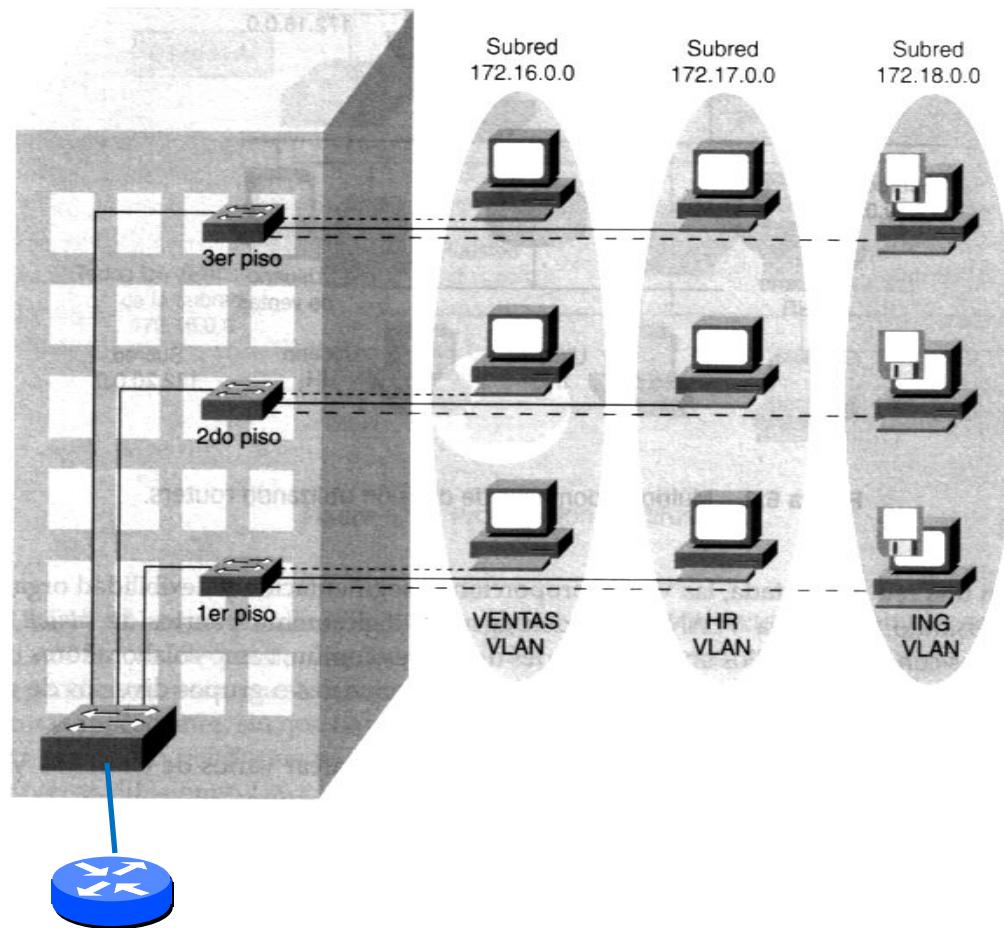
El canal físico se divide en **ranuras de tiempo** que se utilizan para enviar paquetes entre los dispositivos (time-division multiplexing), consiguiendo así el full-duplex.

Hay **varias especificaciones** de dispositivo (clase 1, 2 y 3) , cada cual con diferentes alcances (1-100m) y consumos máximos (1-100mW).

Hay **varias versiones**: desde 1.2 (1Mbps) hasta la 4.0 (**32Mbps**)

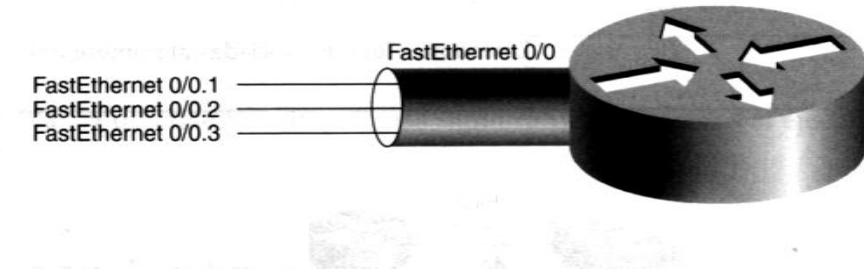
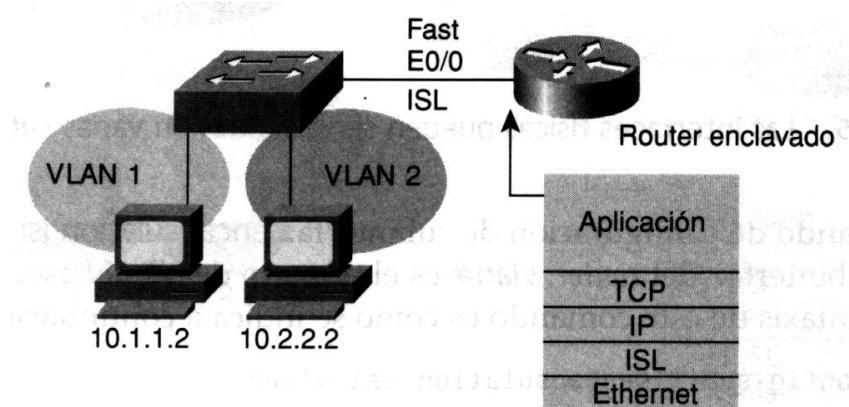
VLAN

- Redes **lógicas** (redes IP) independientes dentro de una misma red **física**.
- útiles para **reducir el dominio de difusión**
- Cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.
- Las VLANs funcionan en el **nivel 2** (Nivel de enlace).



Comutación VLAN

Para pasar de una VLAN a otra, es necesario usar el router, incluso cuando los PCs involucrados están en el mismo switch.



Es necesario que los dispositivos interconectados (otros switches y el router) comparten el protocolo de enlace (**Trunking protocol**) VLAN elegido (ISL o IEEE 802.1Q).

Aunque sea un único interfaz físico, se descompone en **varios interfaces lógicos** cada uno de los cuales actúa como si fuera una tarjeta de red independiente (incluso se enruta entre ellos)