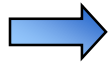

REDES

LAN

RESUMEN



1

Conceptos de Redes

2

Conmutación de Circuitos, Mensajes y Paquetes

3

Modelo de Referencia OSI

4

Redes LAN: Generalidades

5

Redes LAN: IEEE 802.3 – ETHERNET

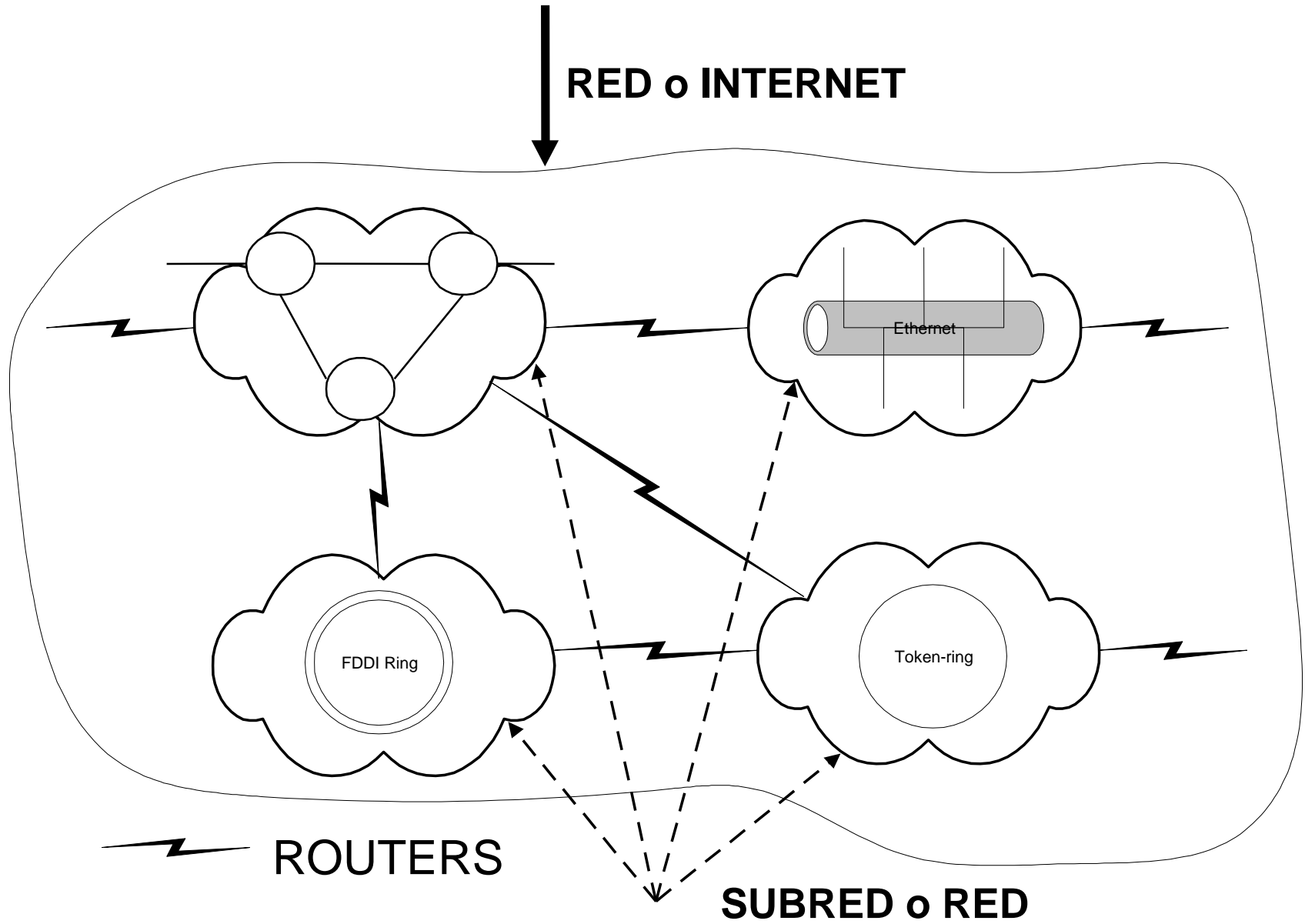
Subred: es una red *homogénea* en cuanto a su tecnología, por ejemplo una red **ETHERNET**, **TOKEN RING**, **FDDI**, etc. El modelo **OSI** hace mención a este concepto cuando se refiere a una red.

Red: Conjunto de Nodos, enlaces y Subredes *heterógeneas*, es decir de *distinta tecnología*. Se enlazan con unos dispositivos denominados **ROUTERS**.

Otra Terminología:

Red: a lo que definimos anteriormente como *Subred*.

Internet: a lo que definimos anteriormente como *Red*



Los parámetros más típicos que podemos citar son :

1. Velocidad Efectiva o **Throughput**, se mide en **bits/segundo**.
2. Retardo de Tránsito, se mide en segundos o milisegundos
3. Tasa de fallos (**BER**)

1. Throughput:

Es la cantidad de **bps** (bits por segundo) que se pueden introducir a la red en el punto de terminación de red (**PTR**), es decir, el ritmo al cual la red *acepta información*.

Además es necesario señalar que la capacidad nominal del enlace **C** y la velocidad efectiva o **Throughput** efectivo *no son lo mismo*. **C** es toda la capacidad física que brinda el enlace y como hay recursos compartidos en la red (enlaces, canales y nodos), ocurre que $C_{ef} < C$.

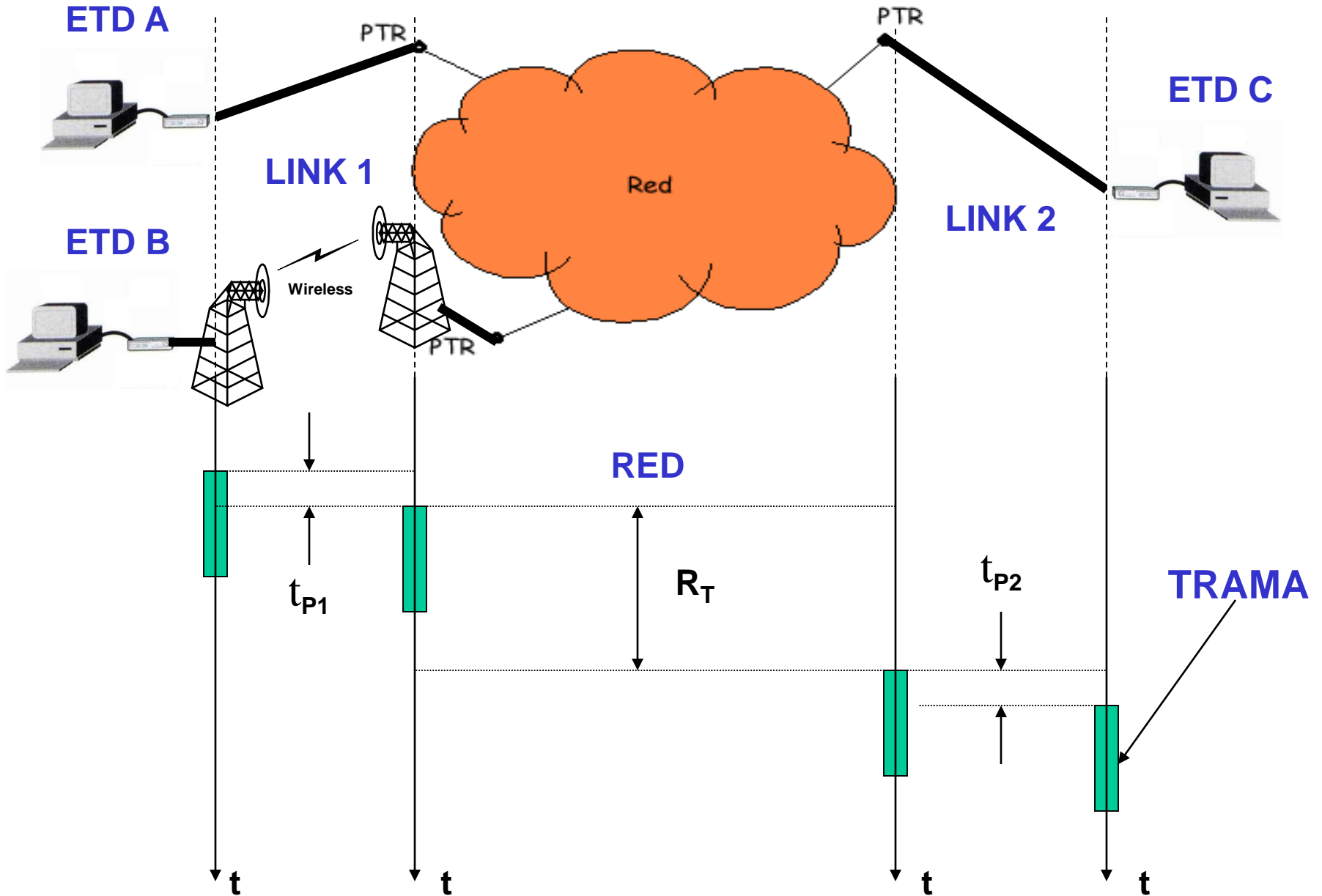
2. Retardo de Tránsito (R_T):

Es el tiempo que transcurre desde que la red recoge un bit en el punto de terminación de red origen hasta que se recibe en el **PTR** destino. Este tiempo R_T siempre será mayor que el tiempo de propagación de la señal t_p en un dado medio físico.

3. Tasa de fallos:

Se caracteriza por medio de la probabilidad de error en bit (**Pe**), esto es la probabilidad que un bit no llegue correctamente a su destino. Los fallos pueden ser debidos a *pérdidas*, *corrupción*, *duplicación* y *desórdenes* en *bits* o *paquetes*. El uso de códigos de redundancia reduce la tasa de fallos, pero no puede hacer nada si ***el sistema está indisponible***, por ejemplo, si se caen los enlaces que conectan un nodo con el resto, dicho nodo está incomunicado.

Conceptos de Redes



Existen Tres aspectos fundamentales a destacar en redes:

 **Retardo**

 **Ancho de Banda**

 **Confiabilidad** (Calidad de Servicio)

RESUMEN

1

Conceptos de Redes



2

Conmutación de Circuitos, Mensajes y Paquetes

3

Modelo de Referencia OSI

4

Redes LAN: Generalidades

5

Redes LAN: IEEE 802.3 – ETHERNET

Caracterización de Tráficos

	Longitud	Retardo
Tiempo Real (Voz, Fax, Telemetría, Video)	$10^5 - 10^7$ bits	< 200 ms, cte.
Interactivo / Transaccional (Teleproceso, Consulta Bases de Datos)	600 – 6000 bits	< 1 S
Diferible (Transferencia de archivos, Correo Electrónico, Transmisión de Imágenes)	$10^5 - 10^8$ bits	Horas / Minutos

- **DE CIRCUITOS**

- **DE MENSAJES**

- **DE PAQUETES**

- 1. CIRCUITO VIRTUAL**

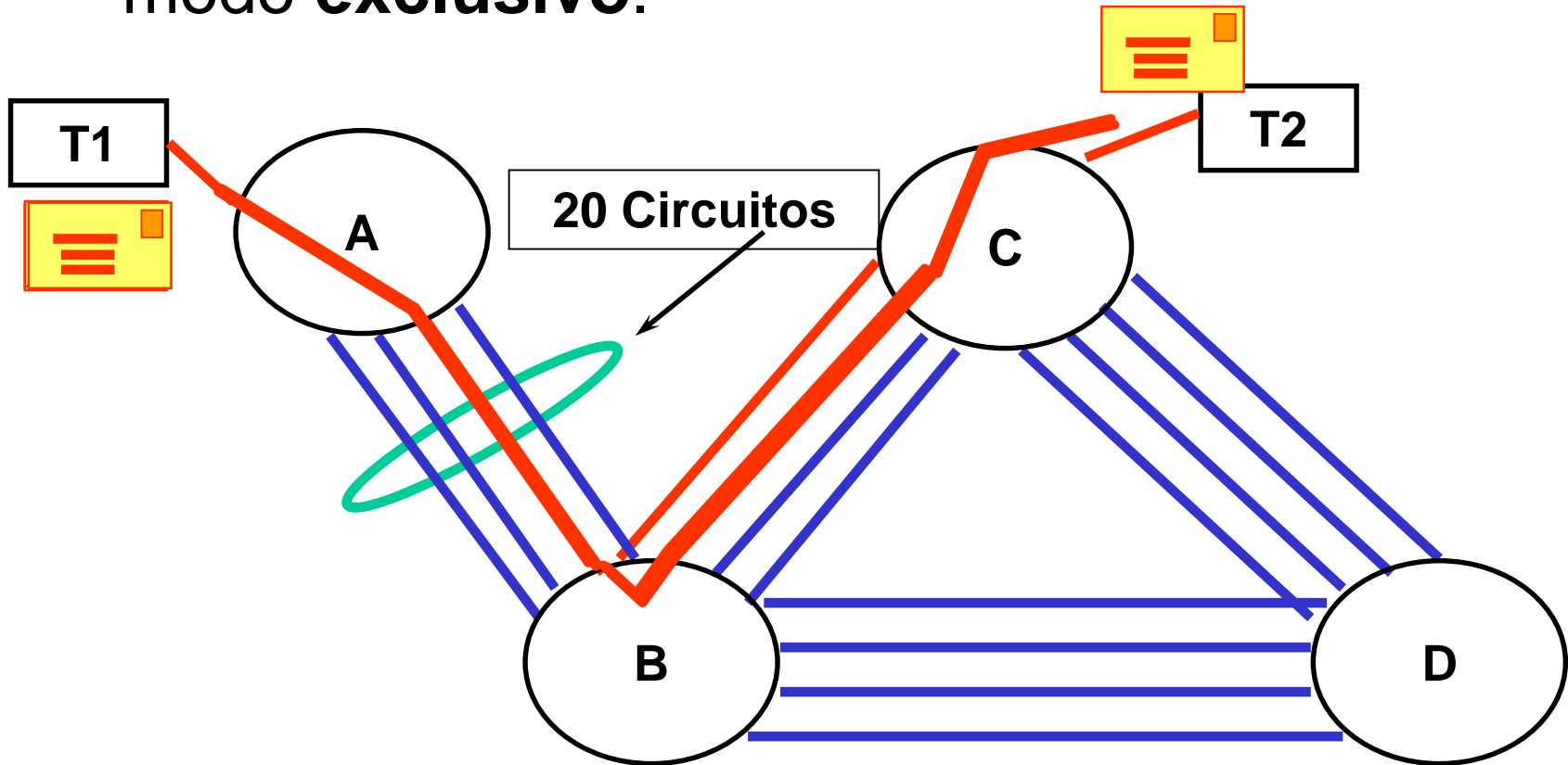
-  PERMANENTE

-  CONMUTADO

- 2. DATAGRAMA**

Conmutación de Circuitos

- Se asigna a la comunicación recursos físicos de modo **exclusivo**.



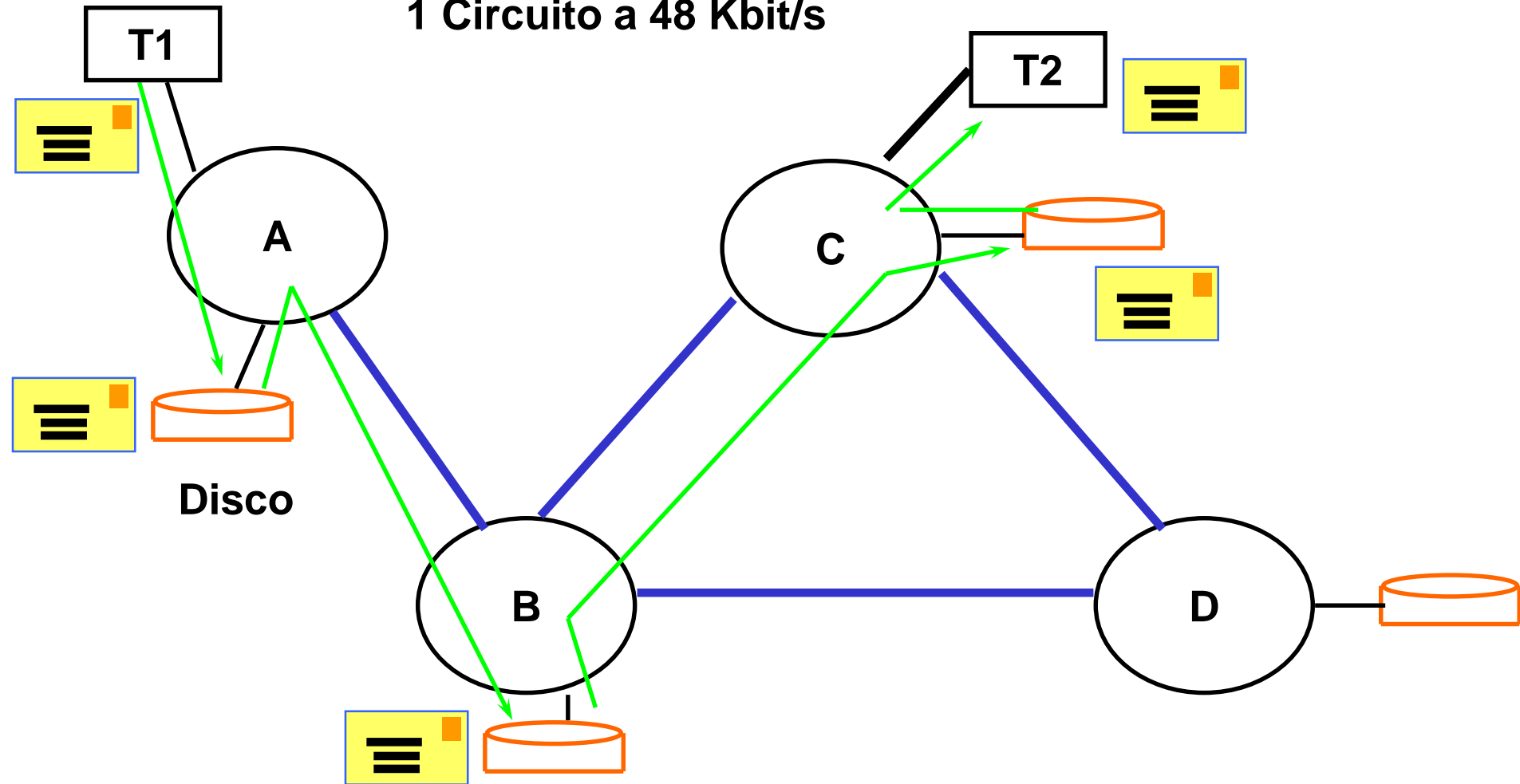
$$C_r = 20 \times 2.400 \text{ bit/s}$$

➤ **DESVENTAJAS DE LA CONMUTACIÓN DE CIRCUITOS**

- Uso ineficiente durante períodos de inactividad
- Si todos los circuitos están ocupados la comunicación no puede efectuarse
- Requiere la misma velocidad en terminales y circuitos internodales de la red

Conmutación de Mensajes

1 Circuito a 48 Kbit/s



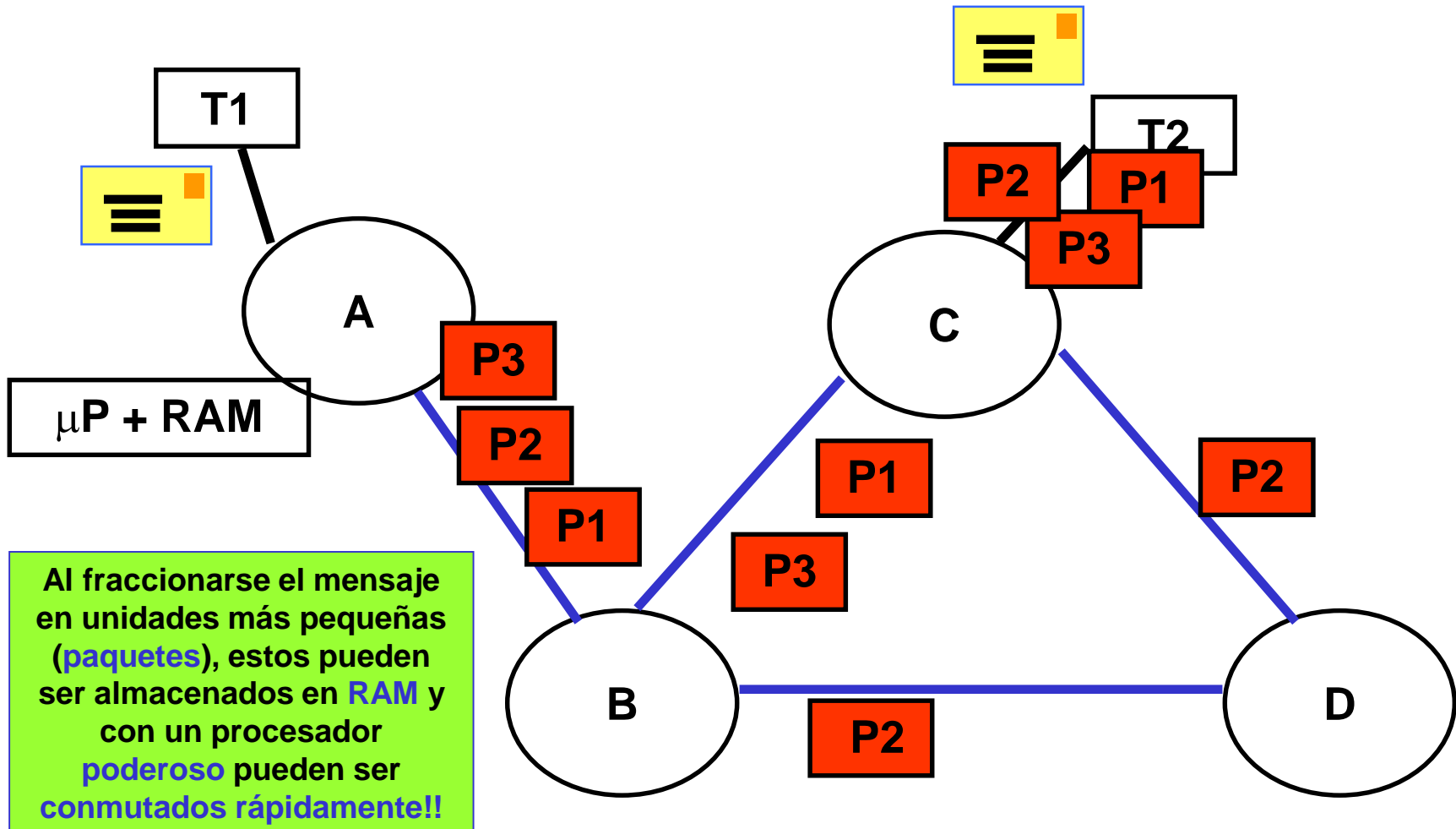
➤ CONMUTACIÓN DE MENSAJES

- Asignación dinámica del circuito cuando la troncal está libre.
- Almacenamiento del mensaje en la red si el circuito está ocupado (*sistemas de almacenamiento y reenvío – **Store and Forward***).

❖ DESVENTAJA

- Los retardos de tránsito pueden ser grandes

Conmutación de Paquetes



➤ CONMUTACIÓN DE PAQUETES: PRINCIPIO DE FUNCIONAMIENTO

o Los mensajes de usuario se fragmentan en paquetes, de longitud variable, no superior a una máxima.

o Los paquetes llevan información de origen y destino, que la red utiliza para encaminar (*cuando exista un canal libre*). **Una vez enviado cada paquete, es destruido en el nodo, liberando así memoria.**

❖ Técnica diseñada para cursar tráfico de datos

- Interactivo
- Diferible

o No adecuada para tráfico **isócrono (voz y video)**

o **Objetivo:** sacar el máximo rendimiento de los recursos de la red, asignándolos sólo cuando haya tráfico y pudiendo utilizar encaminamiento alternativo.

o Eventual desorden de paquetes

✚ En conmutación de paquetes se requiere un **control de congestión**, el mismo consiste en lo siguiente:

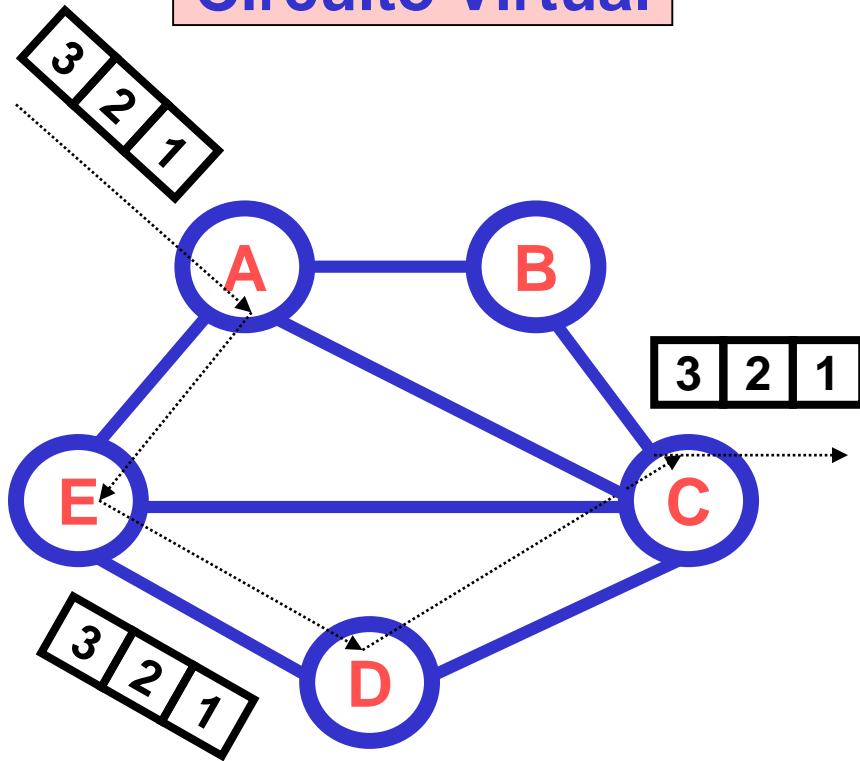
- ▶ Cuando a un nodo le llega más información de la que puede albergar en su memoria, éste avisa hacia atrás a los otros nodos que **bajen la velocidad de envío de información**. Esta información se va propagando hasta llegar a las fuentes generadoras de tráfico avisándoles que cesen de inyectar tráfico a la red, es decir que paren la transmisión.
- ▶ Otra manera de realizar control de congestión consiste directamente en el descarte de las tramas.
- ▶ Cuando la red está muy cargada, los paquetes tendrían diferentes retardos, por ende mediante esta técnica no puede transportarse tráfico isócrono (que requiere como máximo **200 ms de retardo** y además debe ser **constante**).

Conclusión:

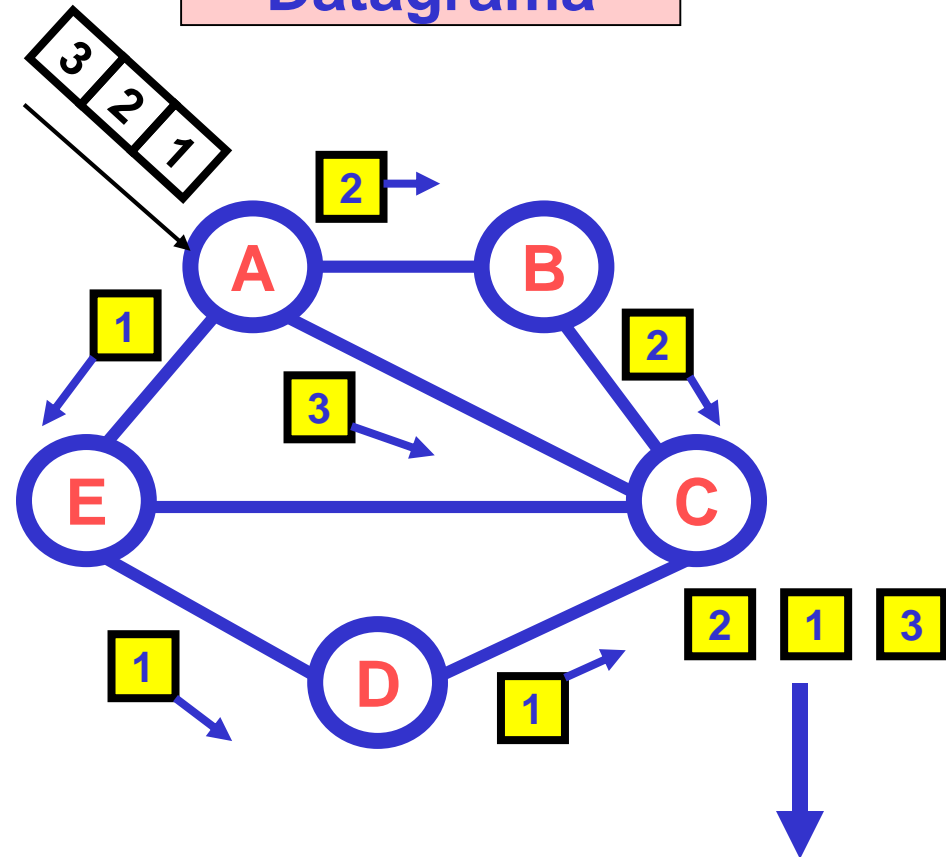
Se tiende al concepto de lo que se llama **Redes Integradas**, cuya característica es la de **reserva de recursos** (*en función del tipo de tráfico*), de manera tal que estas redes puedan transmitir cualquier tipo de servicio.

CIRCUITO VIRTUAL Y DATAGRAMA

Circuito Virtual



Datagrama



Ejemplo de desorden

Circuito Virtual vs. Datagrama

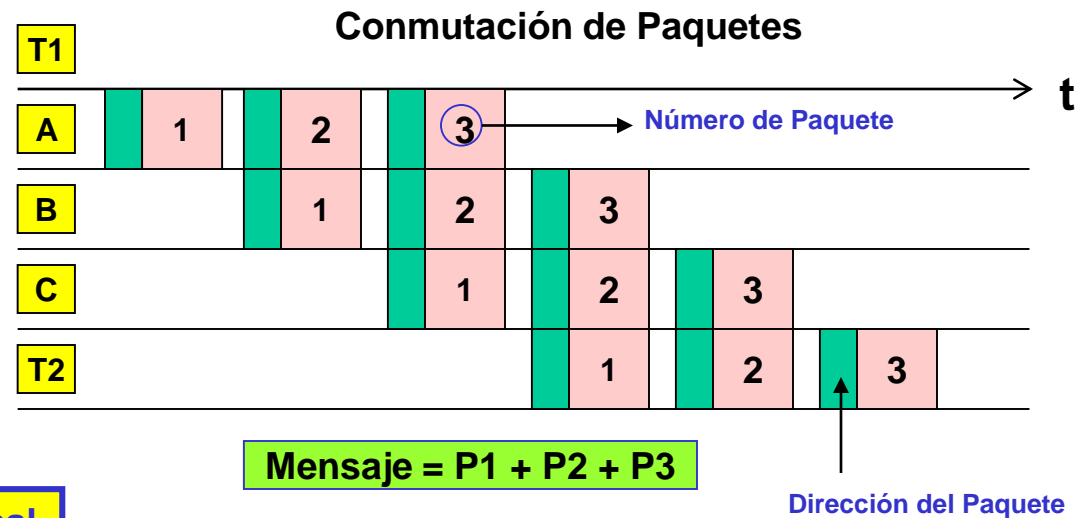
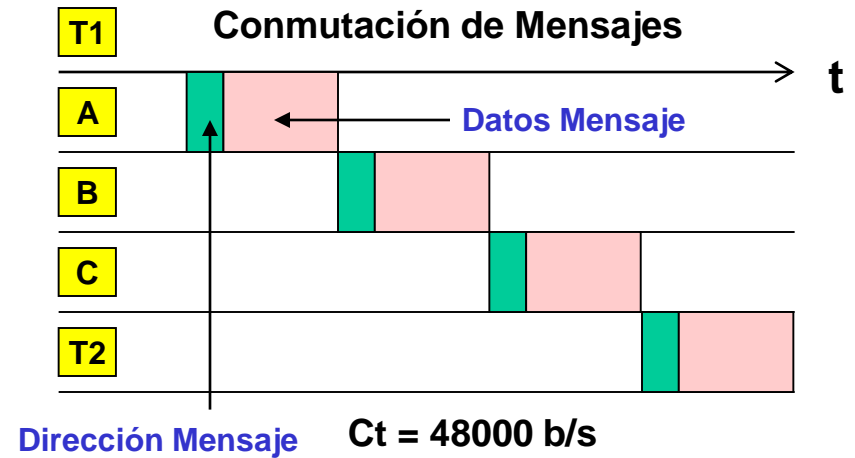
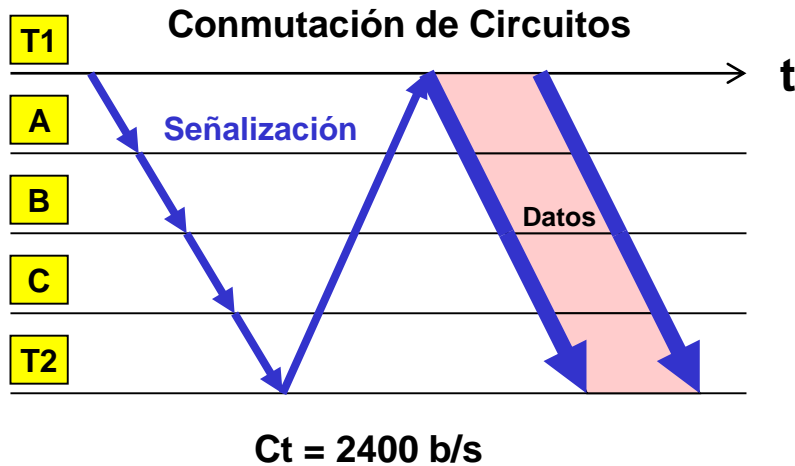
	Datagrama	Circuito Virtual
Direcciones	Siempre	Establecimiento
Encaminamiento o Ruteo	Por paquetes	Por sesión
Efecto de fallos	Paquetes (se pierden)	Sesión
Control de Congestión	Control de flujo: más difícil	Control de flujo
Servicio	CO y CL	CO

✚ **Control de flujo:** El **RX** mantiene un diálogo (handshake) con el **TX**, indicándole por ejemplo, que no le envíe información cuando está procesando información, está asociado al concepto de tráfico. Es un control **extremo a extremo**.

✚ **Control de congestión:** Se da entre los nodos del sistema. Puntualmente cuando se da congestión en un nodo se desvía el tráfico, si existe ruta alternativa. Aparte deberán ponerse en funcionamiento los mecanismos de **control de flujo**.

Conmutación de Circuitos, Mensajes y Paquetes

RETARDO DE TRÁNSITO



Ct: Capacidad de la troncal

Mensaje = P1 + P2 + P3

Análisis Comparativo

	RCC	RCM	RCP
Overhead o Encabezamiento	Establecimiento del circuito	Dirección del mensaje	Dirección y número de Paquete
Capacidad de circuitos	$C_i = \frac{C_T}{N^{\circ} \text{ de circuitos}}$	$C_i = C_T$	$C_i = C_T$
Número de Transmisiones	1	N+1	N+1
Transmisión simultánea en varios tramos	Un solo tramo	NO	Posible
Colas de espera	Establecimiento	En cada nodo	En cada nodo

RESUMEN

1

Conceptos de Redes

2

Conmutación de Circuitos, Mensajes y Paquetes



3

Modelo de Referencia OSI

4

Redes LAN: Generalidades

5

Redes LAN: IEEE 802.3 – ETHERNET

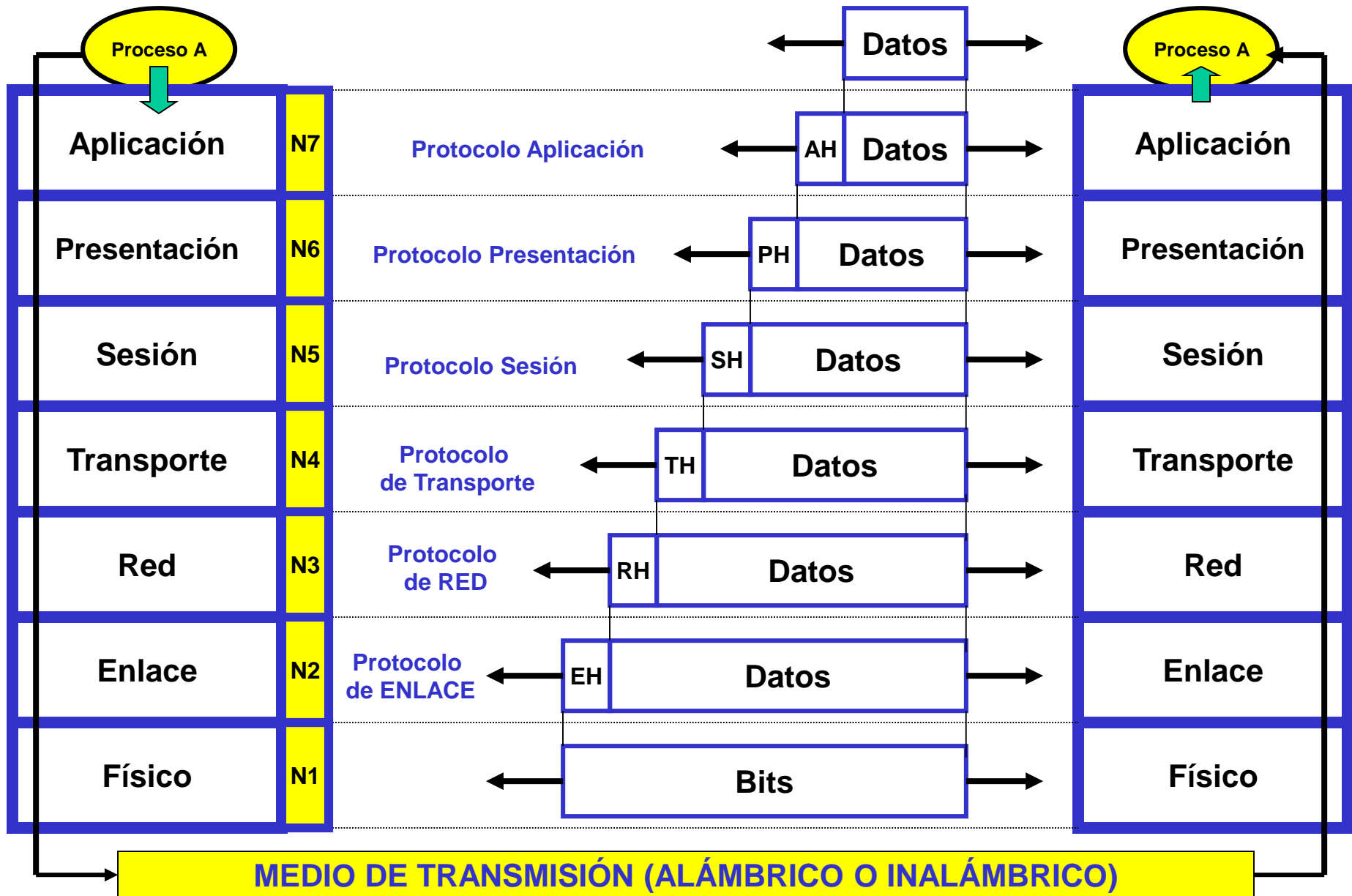
Durante las últimas dos décadas ha habido un enorme crecimiento en la cantidad y tamaño de las redes. Muchas de ellas sin embargo, se desarrollaron utilizando **implementaciones de hardware y software diferentes**. Como resultado, muchas de las redes eran **incompatibles** y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder **comunicarse entre sí**. Para solucionar este problema, la Organización Internacional para la Normalización (**ISO**) realizó varias investigaciones acerca de los esquemas de red. La **ISO** reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (**interoperabilidad**) y por lo tanto, elaboraron el modelo de referencia **OSI** en **1984**.



Ventajas de emplear el modelo OSI

- ♦ Reduce la complejidad
- ♦ Estandariza las interfaces
- ♦ Facilita la técnica modular
- ♦ Asegura la interoperabilidad de la tecnología
- ♦ Acelera la evolución
- ♦ Simplifica la enseñanza y el aprendizaje

Modelo de Referencia OSI



Host o Sistema Final



En un **sistema intermedio**, que es aquel que no procesa información sino que retransmite lo que los **sistemas finales** o **hosts** generan, sólo están presentes los niveles **1 y 2**, y en algunas ocasiones el **3**.

Nivel 0 o Medio Físico: su finalidad es transportar la señal. **Ejemplos: cable coaxil, UTP y Fibra óptica**

Nivel 1 o Nivel Físico: su objetivo es garantizar el *envío de bits*. Debe resolver problemas como decidir qué tensión es un “1” y qué tensión es un “0” o determinar cuántos μs dura un bit. Forman parte de este nivel los conectores y su **PIN OUT**.
Ejemplos: V24, V35 y G703

Medio Físico

Nivel 2 o de enlace:

Su objetivo es establecer una conexión **fiable** entre **dos o más** hosts *directamente conectados a través del enlace físico*. Para ello, implementará **control de errores, control de acceso al medio, establecimiento de conexiones**, etc. En este nivel cada host deberá poseer una dirección para diferenciarse (direcciones **MAC**).

Ejemplos: 802.3 / 802.2 / 802.5 – HDLC – FRAME RELAY

Nivel 3 o de Red:

Dicha capa se encarga del transporte de los paquetes de datos y se compone de la información del usuario que proviene de las capas superiores, más el agregado de información adicional, para el establecimiento y control de la transmisión. Esta capa permite el encaminamiento de la información a través de los nodos de la red, tratando de encontrar el camino idóneo para unir las redes. Se basa en dos elementos imprescindibles para lograr lo anteriormente citado:

- Direcciones lógicas asociadas con los hosts origen y destino
- Rutas a través de la red para alcanzar los destinos identificados con estas direcciones.

Nivel 4 o de Transporte:

Trata de **garantizar** una comunicación fiable o no extremo a extremo entre dos hosts sin preocuparse de la **red que los une**. **Ejemplo: TCP, UDP**

La **capa de transporte** permite establecer comunicaciones **punto a punto entre dos hosts**, por medio de una interfaz con la capa de aplicación denominada **puerto**. Por ejemplo el **Telnet** es una aplicación que me permite conectarme a un host en forma remota por medio de su **dirección IP**, y el número de puerto asociado es el **23**. Otro ejemplo consiste en la transmisión de un archivo, esta operación debe ser **fiable** (es decir sin errores de transmisión) y el protocolo de capa **4** que permite su implementación se denomina **TCP**. El transporte confiable utiliza el concepto de red orientada a la conexión (**CO**), que se basa en las siguientes características:

1. Asegurar que los segmentos enviados sean confirmados al emisor
2. Provee la retransmisión de cualquier segmento que no haya sido confirmado
3. Restablecer los segmentos en su secuencia correcta en el destino.

Se ocupa también del **control de congestión**, si los datagramas llegan muy rápido y no pueden ser procesados, éstos son alojados en una **memoria buffer temporal**. Si los datagramas son parte de una pequeña ráfaga, el **buffering** resuelve el problema. Si el tráfico intenso continúa, el host de destino **agota su memoria** y deberá **descartar** eventualmente los datagramas siguientes. Esto puede evitarse, ya que a nivel de transporte, el host destino puede emitir una señal de **“not ready”** al emisor, actuando como una señal de freno. Este mensaje le indicará al emisor que cese la transmisión de segmentos. Cuando el receptor se recupera y puede volver a recibir nuevos segmentos, le emite al emisor la señal de **“ready”** para que el emisor comience a enviar nuevamente tráfico. Para la transmisión de **tráfico isócrono** no se realiza este proceso, sino que se emplea un protocolo **no fiable** como lo es el **UDP**.

Nivel 5 o de Sesión:

Proporciona el control de la comunicación entre las aplicaciones; establece, gestiona y cierra las conexiones (**sesiones**) entre las aplicaciones. Es la capa responsable de diálogos entre los hosts.

Nivel 6 o de Presentación:

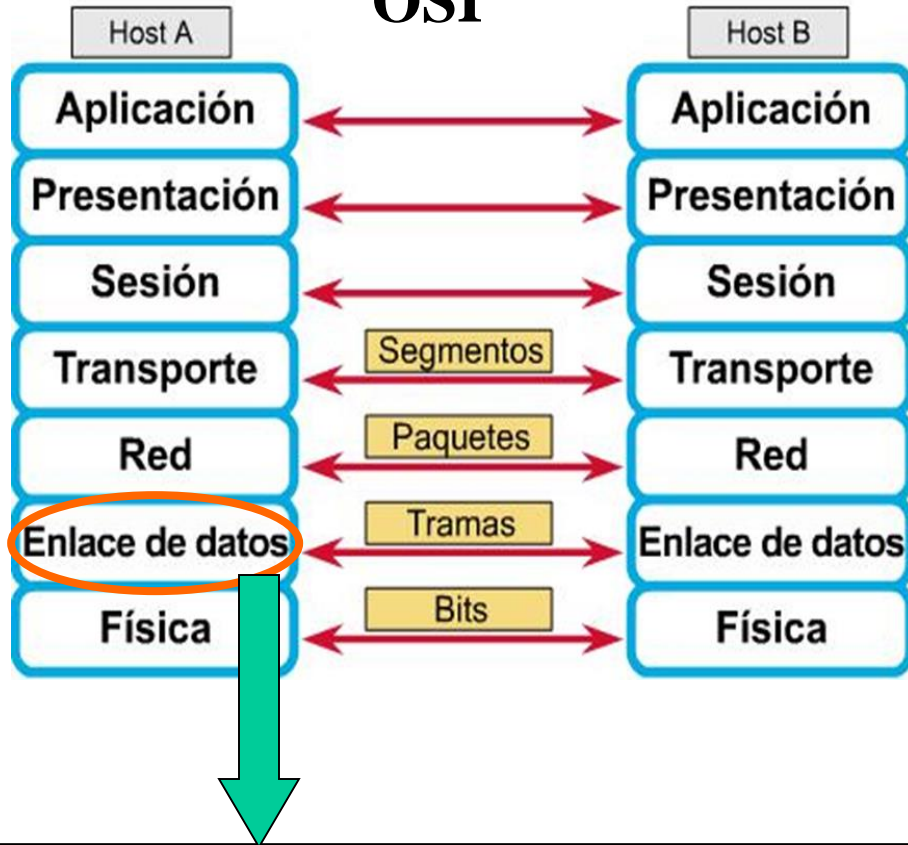
Proporciona a los procesos de la aplicación independencia respecto a las diferencias en la presentación de los datos (**sintaxis**). En concreto indica cómo deben ser preparados los datos a transmitir. **Ejemplos: ASCII, JPEG, MP3.** Otro ejemplo de codificación sería la **encriptación** de datos recibidos desde el nivel de aplicación y la **desencriptación** en el host de destino antes que sea enviada a la capa de aplicación correspondiente.

Nivel 7 o de Aplicación:

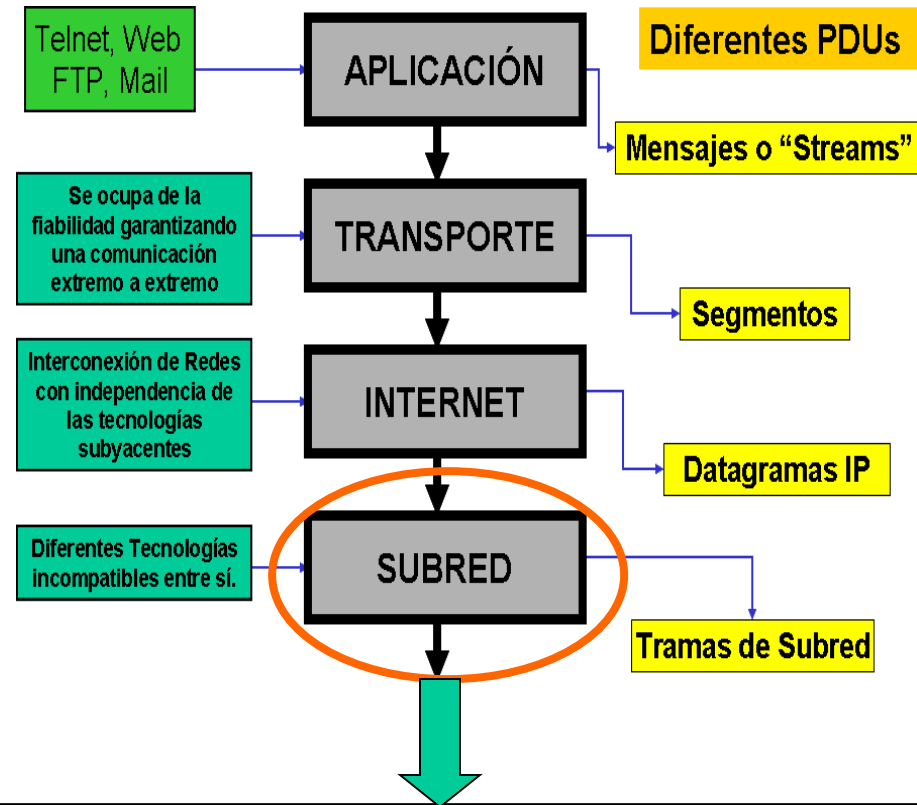
Es donde el usuario interactúa con la computadora. Proporciona el acceso al entorno **OSI** para los usuarios y también proporciona servicios de información distribuida.
Ejemplos: Telnet, Ftp, http

Los niveles situados por encima de la capa 4 están siendo muy cuestionados, hasta el punto que algunos opinan que estos niveles deberían formar parte de las aplicaciones y no del sistema de comunicaciones. El modelo **TCP/IP** concatena los tres niveles superiores del modelo OSI en uno solo denominado nivel de **aplicación**.

MODELO OSI

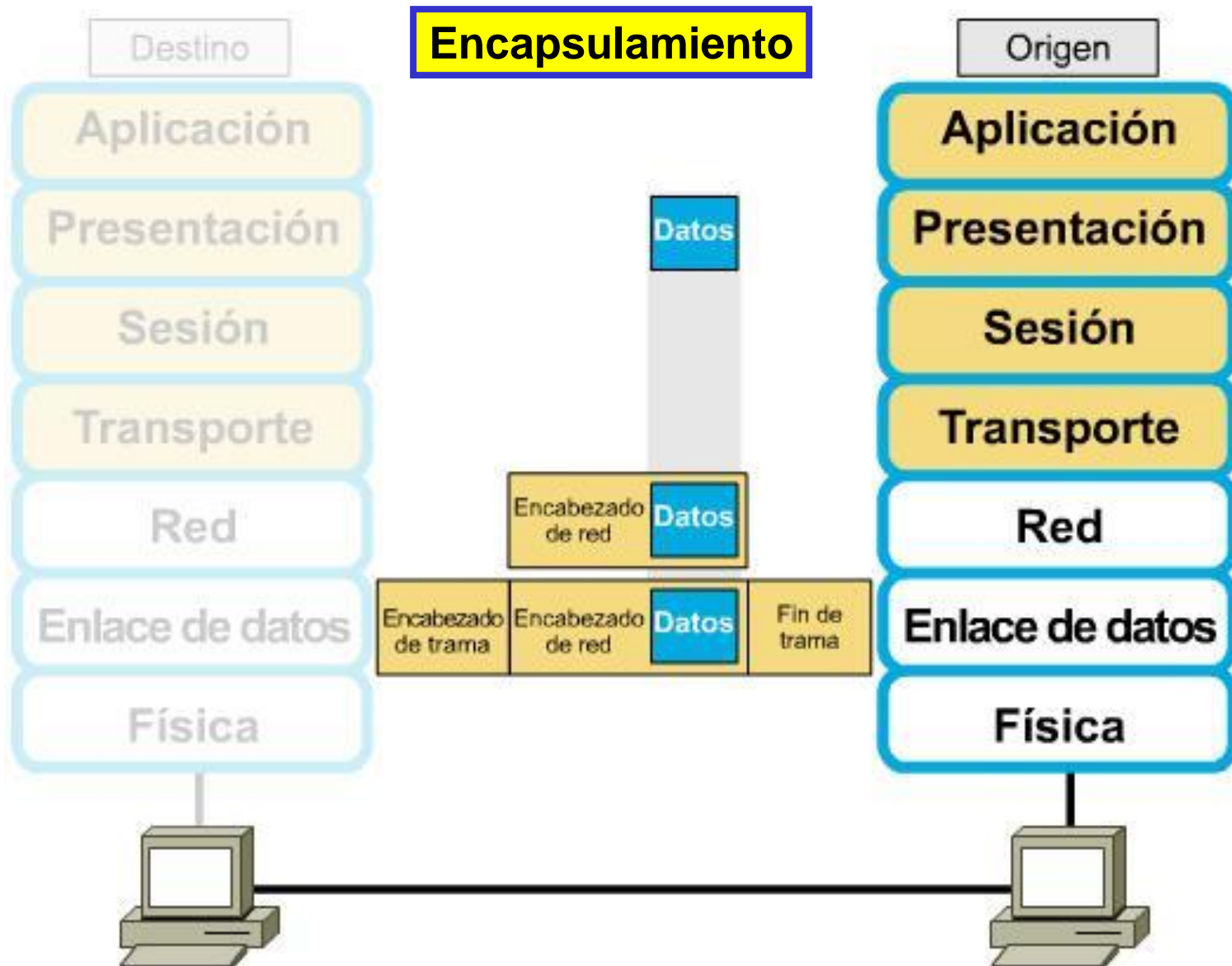


MODELO TCP/IP

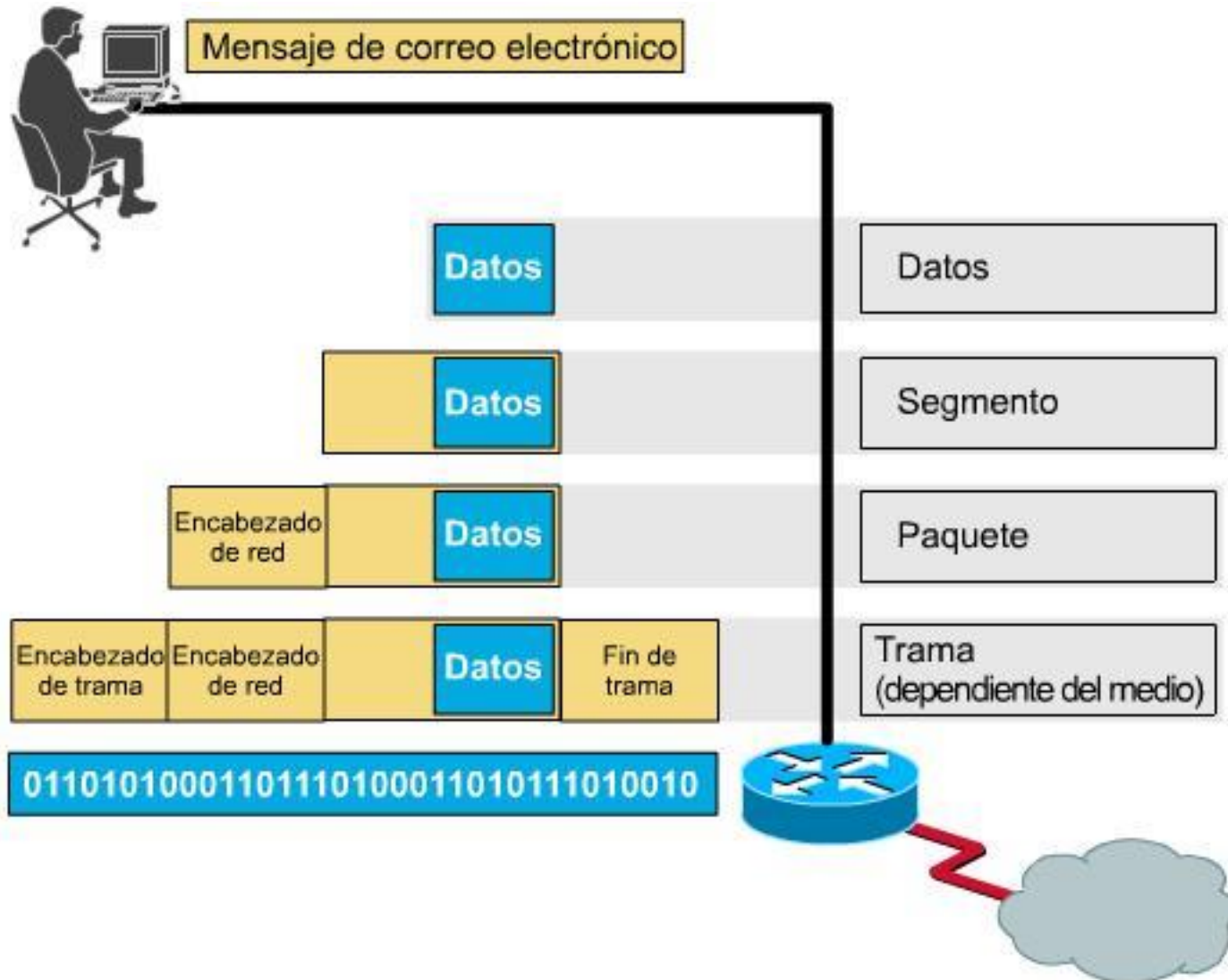


Permite a la capa de RED el acceso a los medios físicos a través de *tramas*. Controla el acceso hacia y desde los diferentes medios físicos. Se ocupa de la detección de errores (pero no de su corrección), esto será responsabilidad de la capa de transporte.

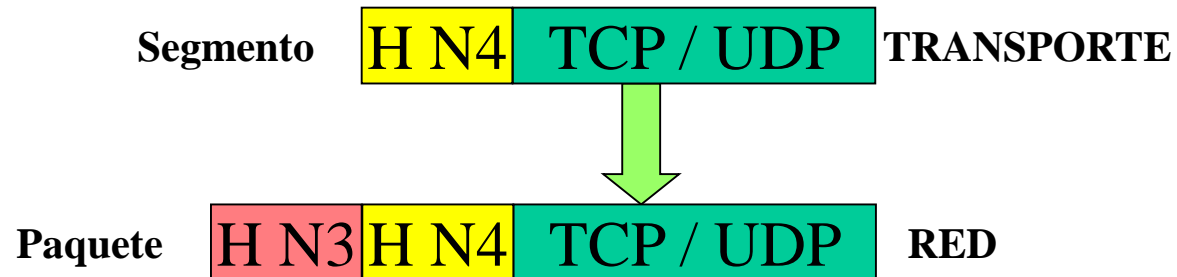
Modelo de Referencia OSI



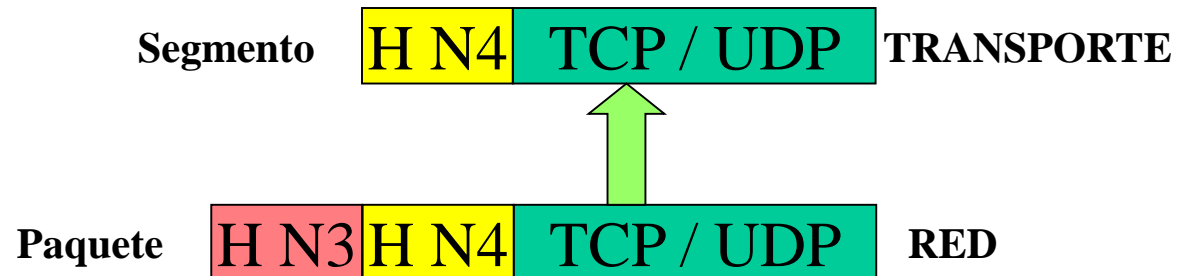
Ejemplo de Encapsulamiento



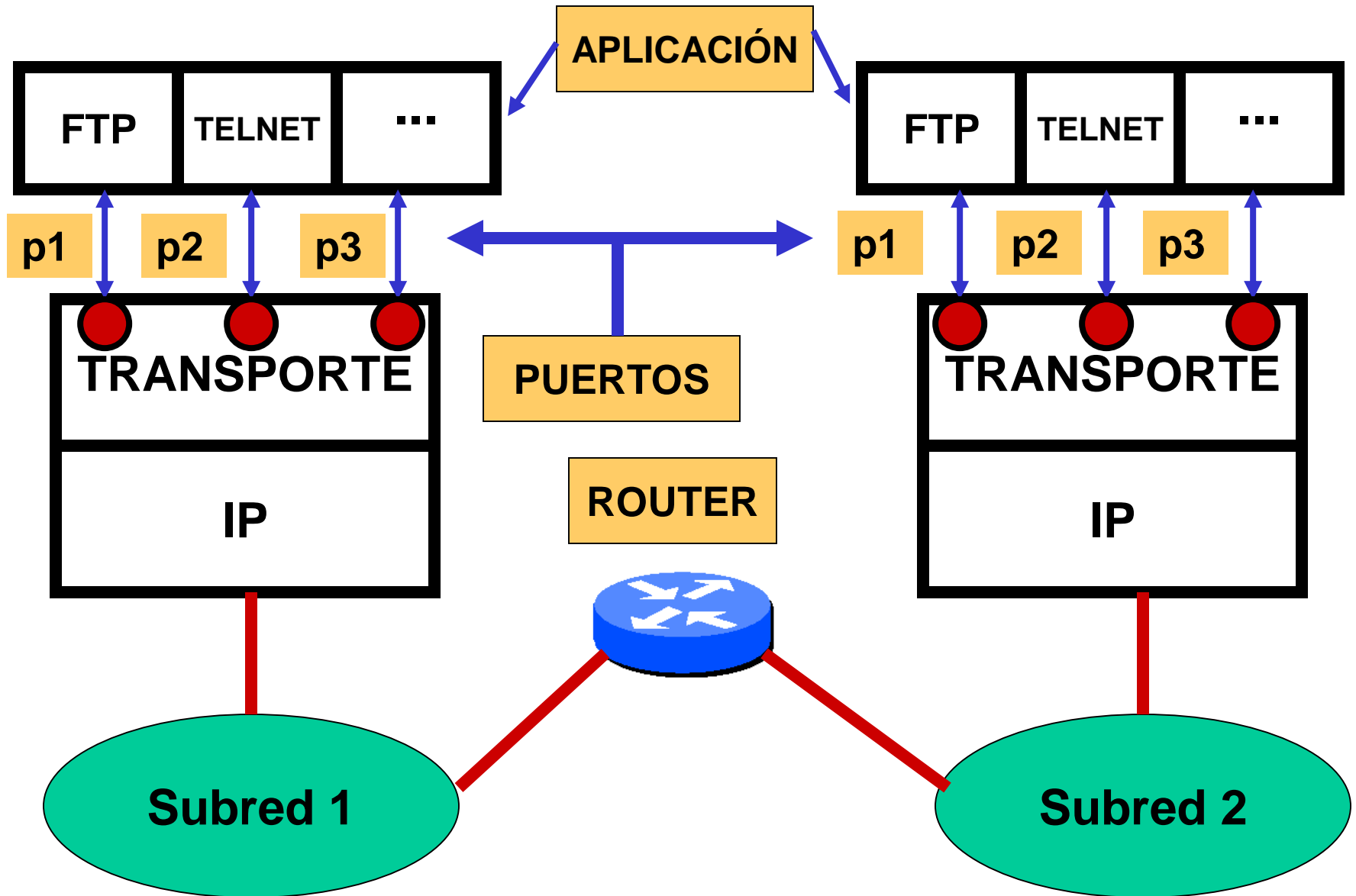
PROCESO DE ENCAPSULAMIENTO



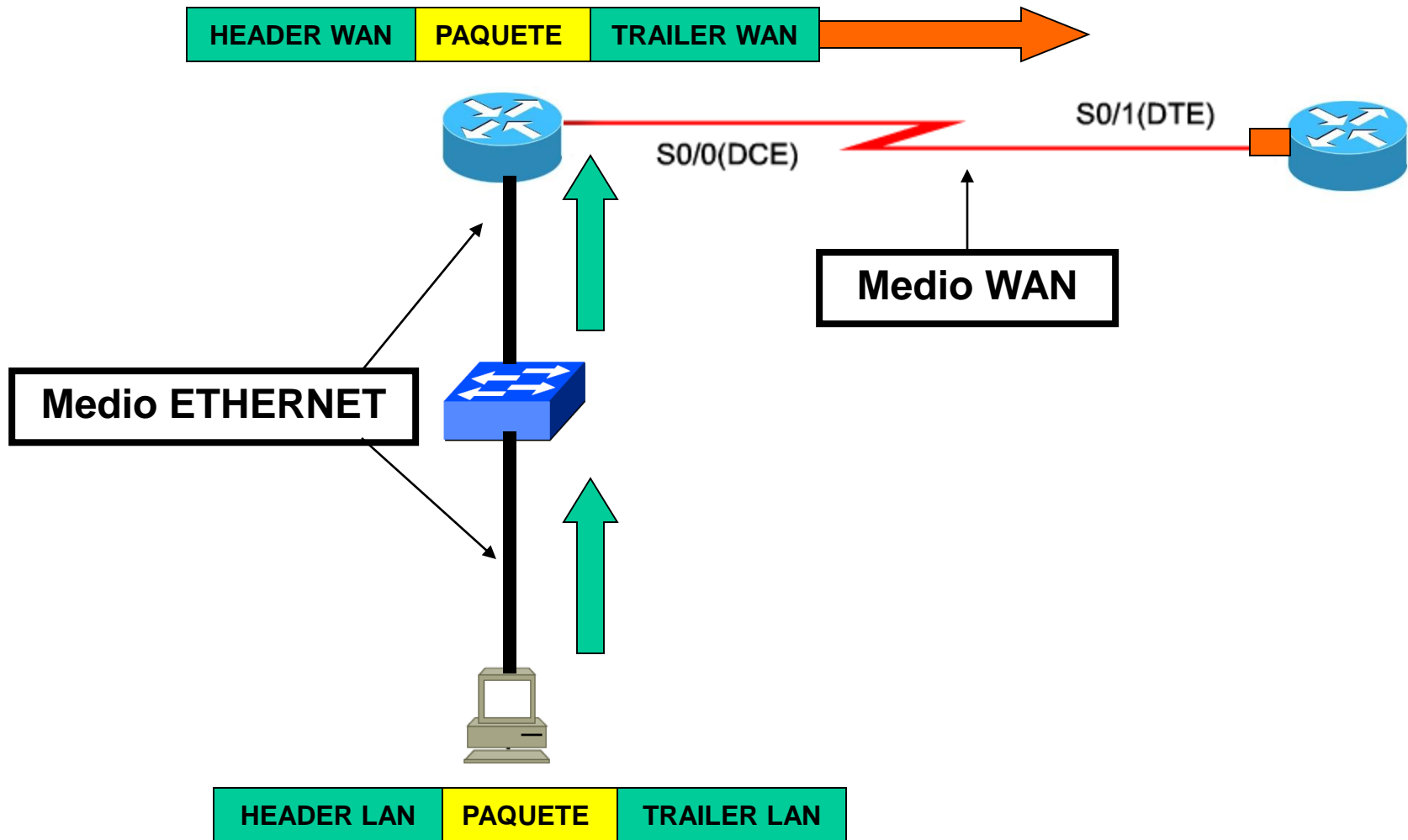
PROCESO DE DESENCAPSULAMIENTO



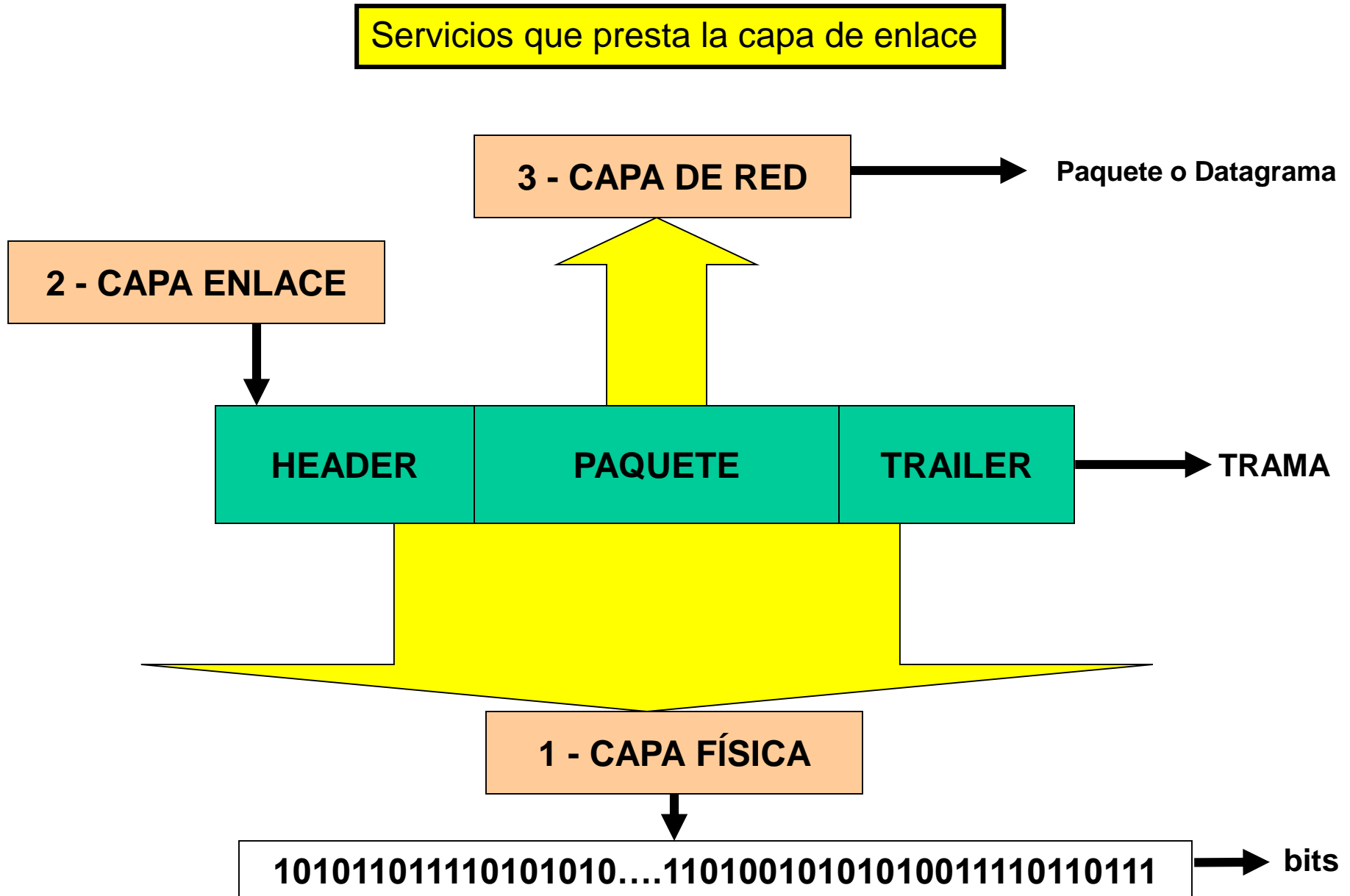
Modelo de Referencia OSI – Capa de Transporte



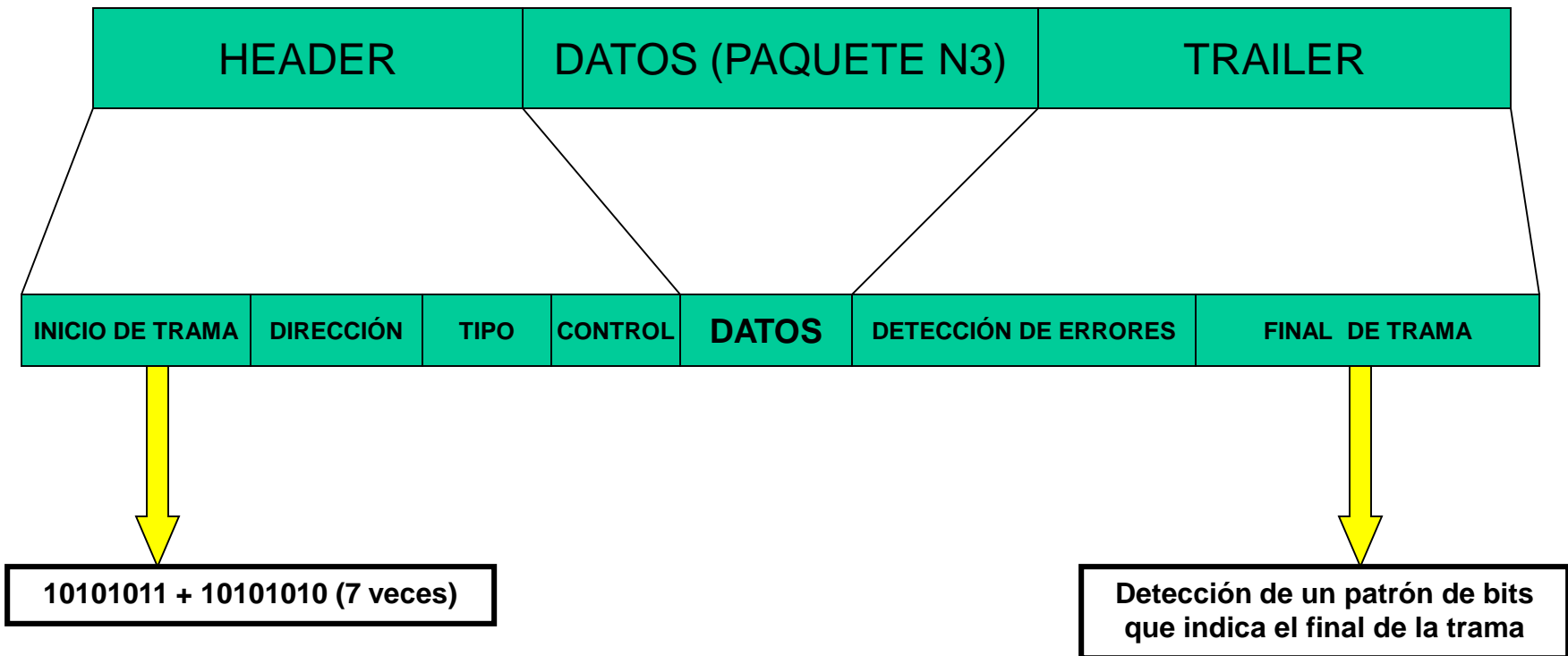
Modelo de Referencia OSI – Capa de RED



Modelo de Referencia OSI – Capa de Enlace – Generación de Tramas I



Configuración del Paquete para su transmisión en el medio físico

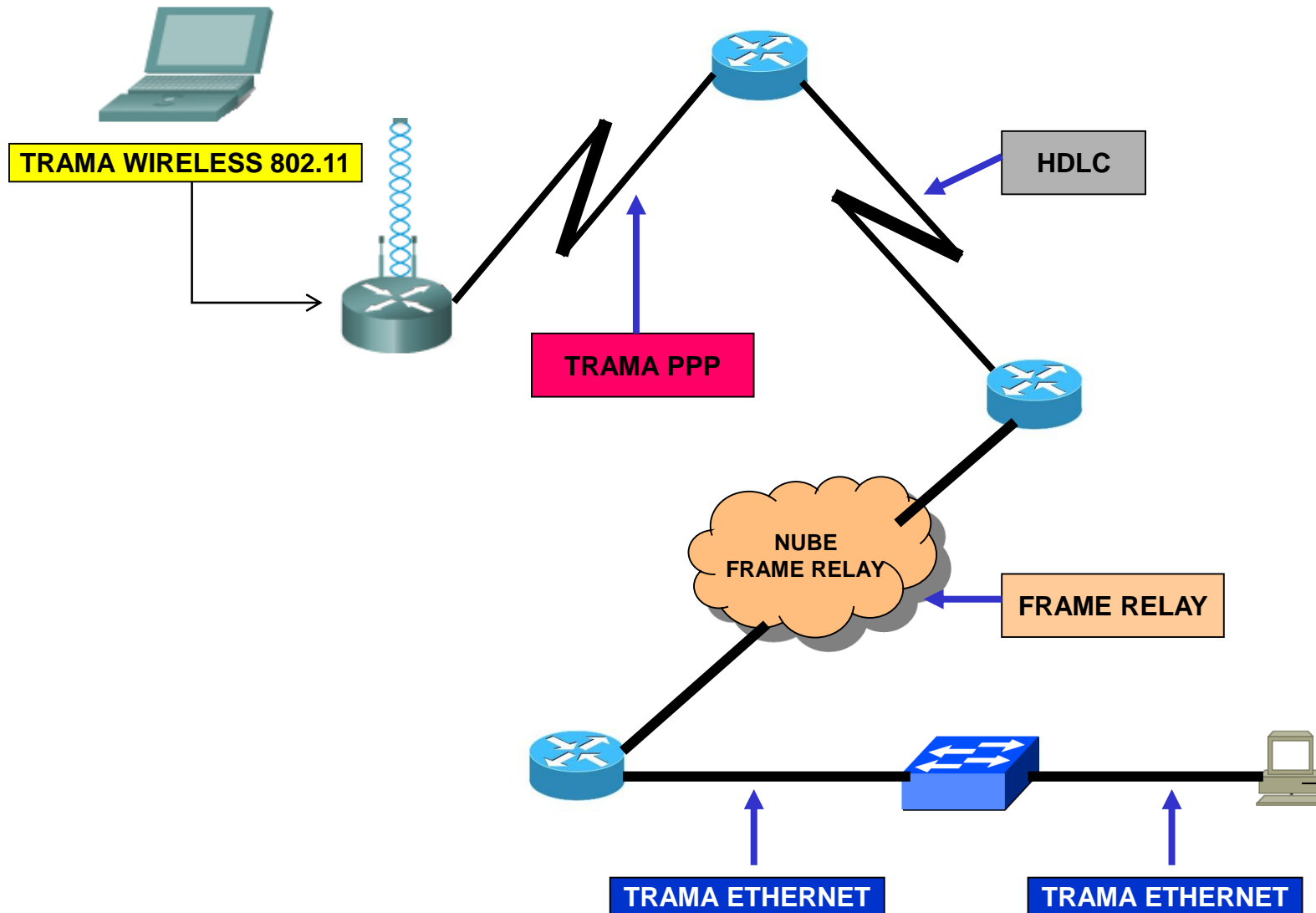


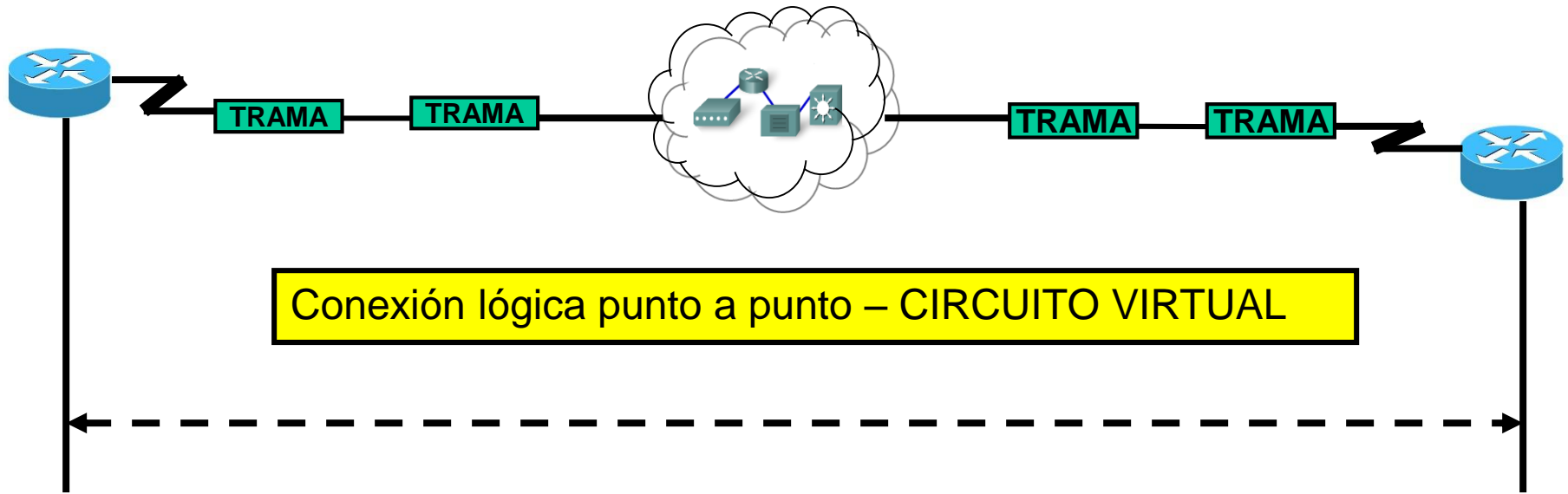
HEADER

- **TIPO**: tipo de datos que transporta la trama
- **CONTROL**: servicios de control de flujo

Subcapas del nivel de enlace

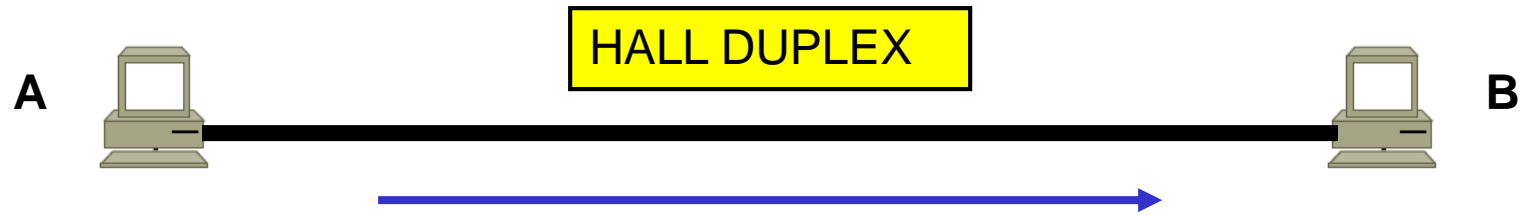
Ejemplo de cambio de tramas en función del medio físico o del tipo de red atravesado



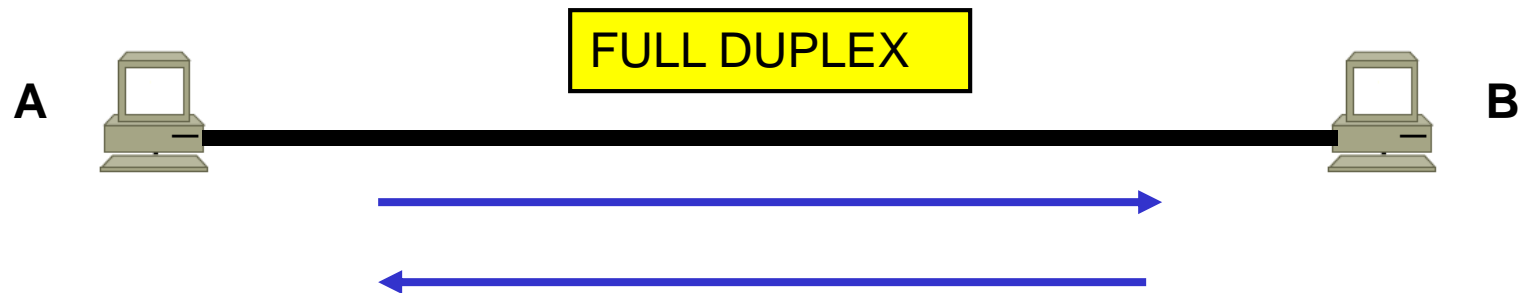


No se requieren direcciones en una trama punto a punto, ya que en esta conexión hay un sólo destino posible.

Comunicaciones HALF DUPLEX y FULL DUPLEX



La comunicación se realiza sólo en un sentido (de A hacia B o viceversa). Cuando un host transmite, el otro sólo puede recibir.



La comunicación se realiza simultáneamente en ambos sentidos, tanto de A hacia B como de B hacia A.

RESUMEN

1

Conceptos de Redes

2

Conmutación de Circuitos, Mensajes y Paquetes

3

Modelo de Referencia OSI

4

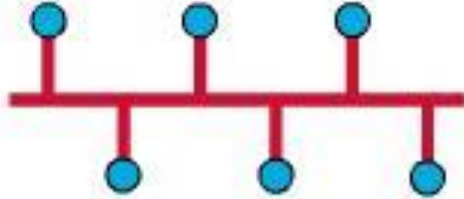
Redes LAN: Generalidades

5

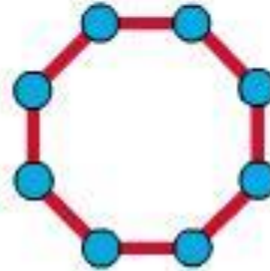
Redes LAN: IEEE 802.3 – ETHERNET



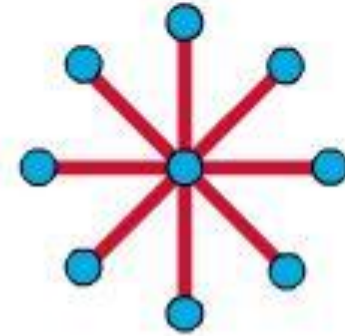
TOPOLOGÍAS



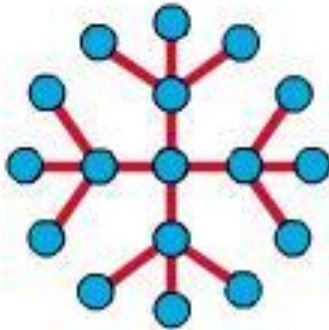
Topología de bus



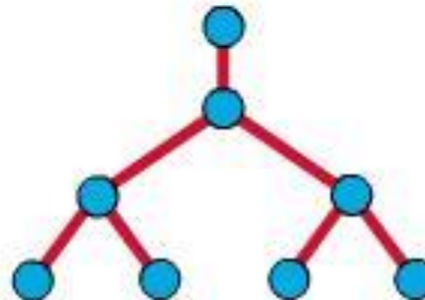
Topología de anillo



Topología en estrella



Topología en estrella extendida



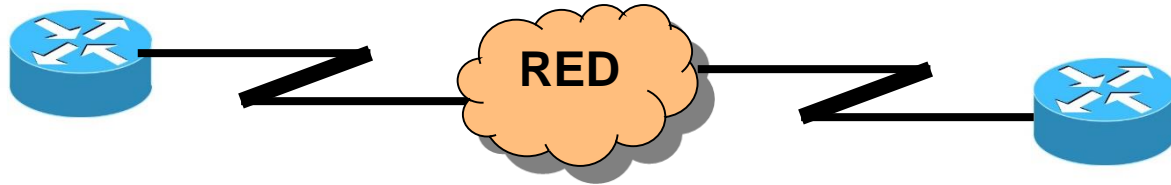
Topología jerárquica



Topología en malla

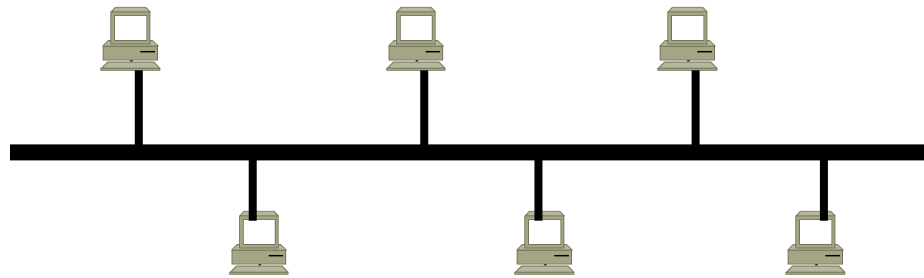
Redes LAN: Generalidades

Topología lógica y Física

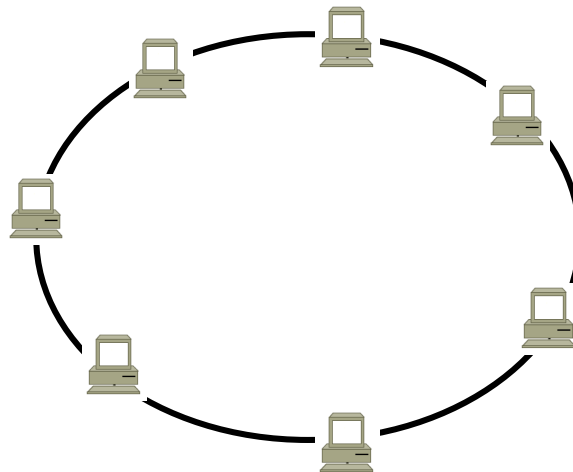


Punto a punto

Acceso múltiple



Bus



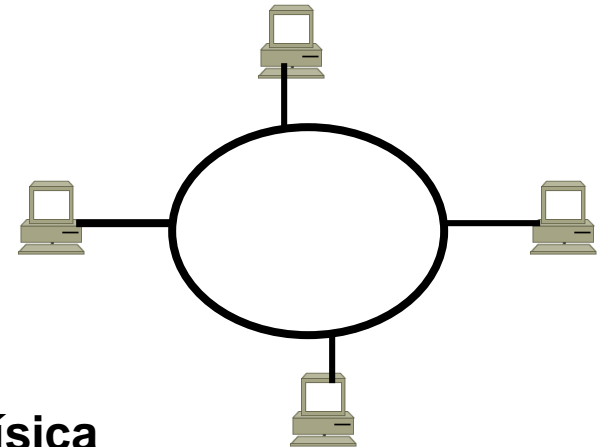
Anillo

Redes LAN: Generalidades

Topología Lógica: **BUS**

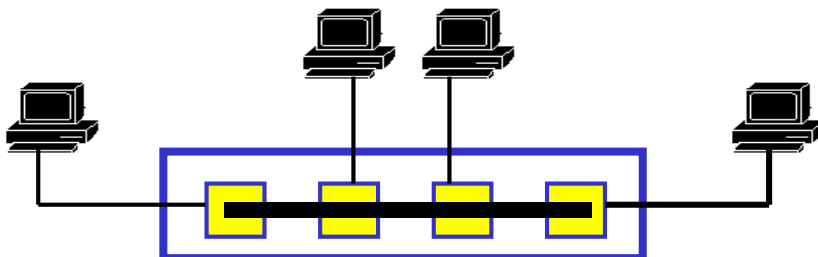


Topología Lógica: **ANILLO**

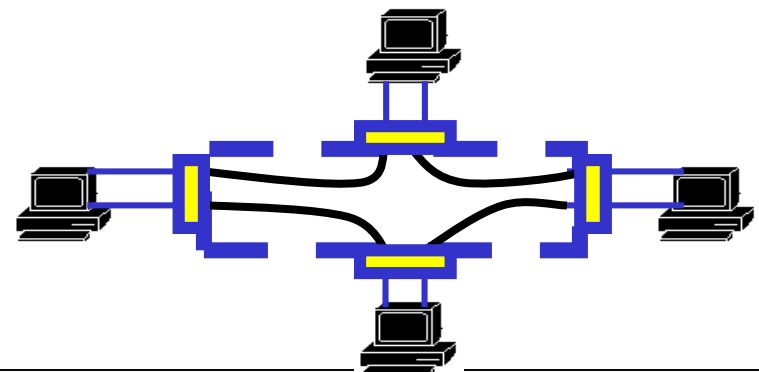


Topología lógica y Física

Topología Física: Estrella (HUB ETHERNET)



Topología Física: Estrella (HUB TR)



Norma IEEE 802 para Redes LAN

En los años **80**, el **IEEE** se encontró ante la tarea de establecer un **estándar** para las redes de área local **LAN**, de forma que los usuarios pudieran elegir a qué fabricante comprar la red sin encontrarse con una incompatibilidad total entre equipos. Este propósito se vio frustrado por la falta de acuerdo entre los integrantes del comité. Al final, el **IEEE** se tuvo que conformar con una serie de estándares que cubrían la parte baja de la arquitectura **OSI**, **hasta el nivel de enlace**, y que compartían el interfaz con el nivel de red (nivel 3 de OSI). De este modo se conseguía que las aplicaciones de niveles superiores fueran independientes del modelo concreto de red que hubiera debajo, es decir se consiguió que la red **fuera transparente para el usuario**.

El **IEEE** ha generado varios estándares para **LANs**. Dichos estándares se agrupan colectivamente bajo una única norma conocida como **IEEE802**, la cual incluye **CSMA/CD**, **Token Bus** y **Token Ring**. El **IEEE 802** ha sido adoptado por **ANSI** e **ISO** (**ISO 8802**). Los estándares están divididos en partes, cada una publicada **como un tomo separado**.

El **802.1** da una introducción al conjunto de estándares. El estándar **802.2** define la parte alta del nivel de enlace que utiliza el protocolo llamado **LLC** (Logical Link Control). Las partes **802.3** a **802.5** describen los **tres estándares LAN**, que son respectivamente **CSMA/CD**, **Token Bus** y **Token Ring**. Cada estándar cubre los aspectos del nivel físico y la capa **MAC** (nivel de enlace).

Métodos de acceso a la capa MAC

Básicamente existen dos mecanismos: contienda y por selección

Contienda: es un mecanismo en donde los hosts se pelean por el recurso, que es un medio compartido. Las redes basadas en este método emplean una topología lógica tipo **BUS**. Puede suceder que dos hosts intenten transmitir simultáneamente, en cuyo caso se genera lo que se denomina una **colisión**. Un clásico de este tipo de sistemas es **ETHERNET**. Se emplea un proceso identificado como CSMA / CD (Carrier Sense Medium Access collision detect).



Selección: en este caso cada host tiene un turno para transmitir. Aquí el medio compartido suele ser una estructura en anillo. Normalmente circula por el anillo una trama denominada **token**. Cuando un host recibe el token puede transmitir. Si lo hace quita el token y envía por el anillo la trama de datos. Si no tiene nada para transmitir devuelve el token al siguiente host dentro del anillo. Este método se caracteriza por no tener **colisiones**. Un clásico ejemplo lo constituían las redes **TOKEN RING** (propiedad de IBM, ya en desuso).

Para lograr el **objetivo de transparencia de la red para el usuario** era necesario normalizar la arquitectura de protocolos de todos los **modelos de red**. Al enfrentarse al **nivel de enlace** se dieron cuenta de la complejidad que implicaba dicha hazaña. La decisión que tomaron fue la de dividir el **nivel 2** en **dos subniveles**:

MAC (Medium Access Control):

Controla el acceso al medio de transmisión, que es compartido. **Es diferente para cada tipo de red**, de acuerdo con la técnica que se emplee.

LLC (Logical Link Control):

Cubre el resto de las funciones del nivel de enlace de **OSI**. **Es igual para todas las redes**, y por lo tanto es aquí donde se realiza la **convergencia** entre todos los modelos.

El servicio que el nivel **MAC** ofrece al **subnivel LLC** está definido como **no fiable y no orientado a conexión**. Sin embargo, el servicio ofrecido por el subnivel **LLC** al nivel de red no se establece de forma **unívoca**, sino que hay tres opciones, dependiendo del uso que se vaya a hacer de la red.

LLC1	No fiable No orientado a conexión De los tres es la más utilizada en la práctica
LLC2	Fiable Orientado a conexión
LLC3	Datagramas con asentimiento

Otra característica del **LLC** es que permite el acceso a la red de varias entidades de nivel superior, a través de diferentes puntos de acceso al servicio, conocidos como **LSAPs** (Link Service Access Point). Cada **LSAP** es una especie de **dirección de acceso al LLC**, que las entidades superiores utilizan para *identificarse como origen y destino de información dentro de la máquina*. Las entidades de nivel superior son, generalmente, **procesos en ejecución** en un PC.

FUNCIONES DE LOS NIVELES

❖ Nivel Físico:

- ✚ Topología y cableado, interfaces eléctricas y mecánicas, señales, tiempo de duración de los bits, niveles de corriente, etc.

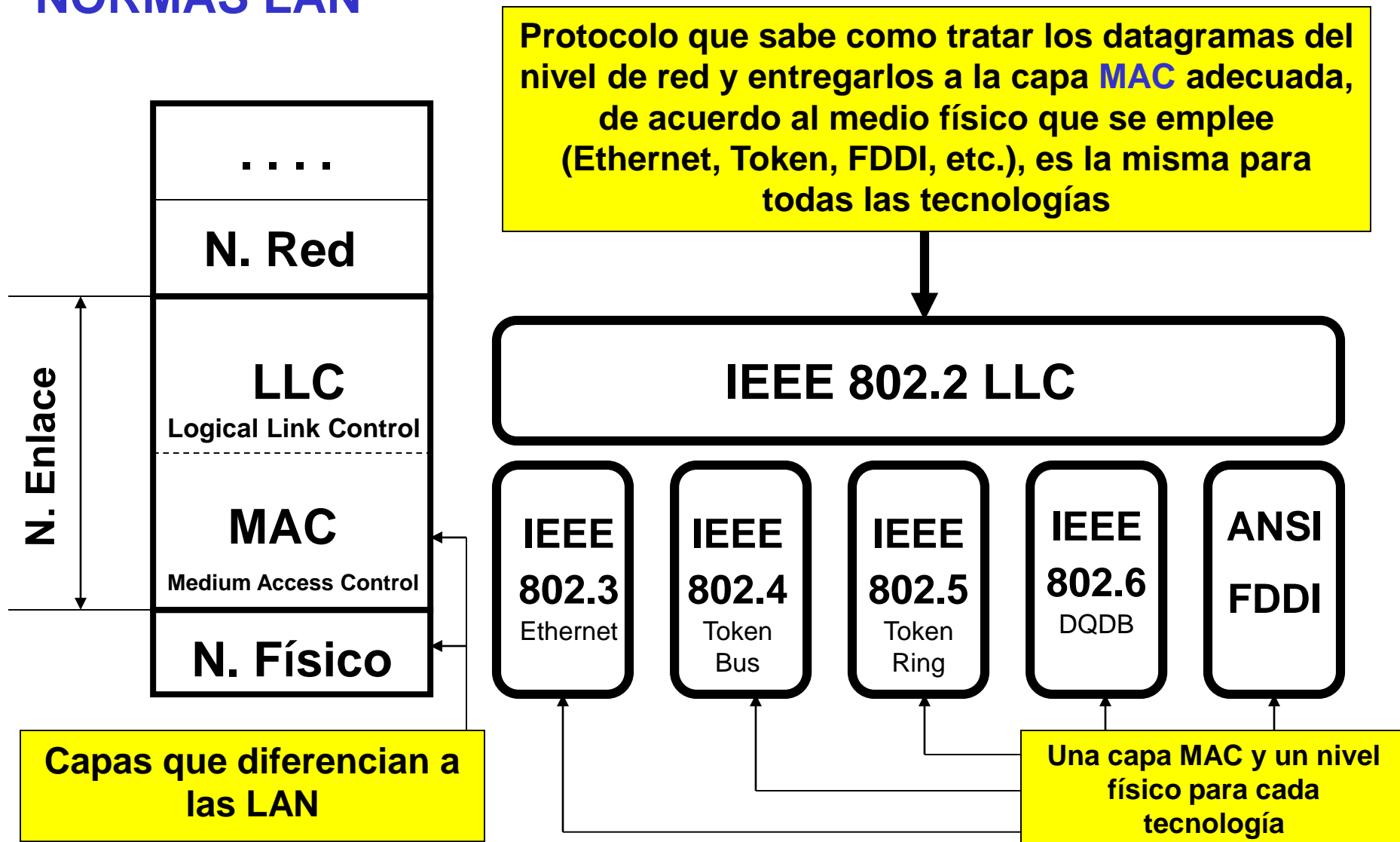
❖ Subnivel MAC:

- ✚ Gestión del acceso al medio compartido
- ✚ **Direccionamiento** (comunicación punto a punto o **UNICAST**, multipunto o de **GRUPO** o **MULTICAST** y difusión o **BROADCAST**)

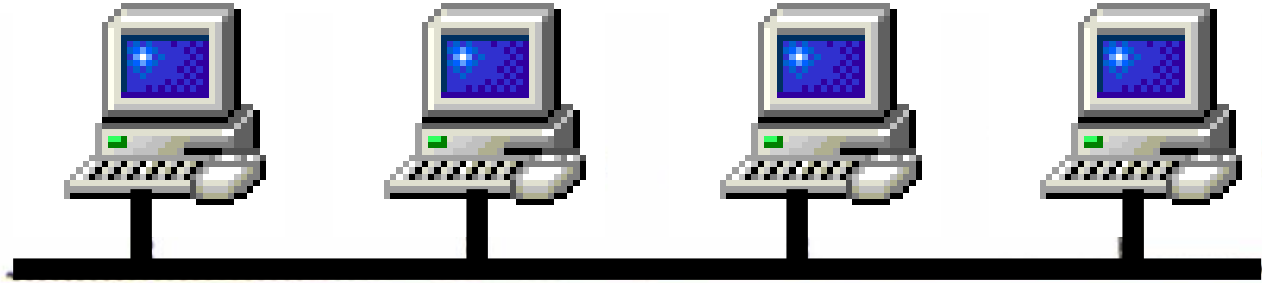
❖ Subnivel LLC:

- ✚ Multiplexación

NORMAS LAN



DIRECCIONES



- ⊕ Todas los hosts escuchan todas las transmisiones
 - ▶ Se necesitan direcciones para los hosts
 - ▶ Existen también direcciones de grupo (**multicast**), que engloban a varios hosts
- ⊕ Cada trama lleva:
 - ▶ Una dirección de destino (individual o de grupo)
 - ▶ Una dirección fuente (individual)

DIRECCIONES IEEE

❖ Formato:

- **6 bytes** (2^{48} direcciones)
- Primer bit de transmisión indica si la dirección es **UNICAST** o de **grupo (multicast)**.
- Cada estación tiene una dirección **Unicast**
- Las direcciones únicas son administradas por el **IEEE**
 - El **IEEE** asigna los **3** primeros bytes a cada fabricante
 - El fabricante asigna los otros **tres** bytes a sus productos

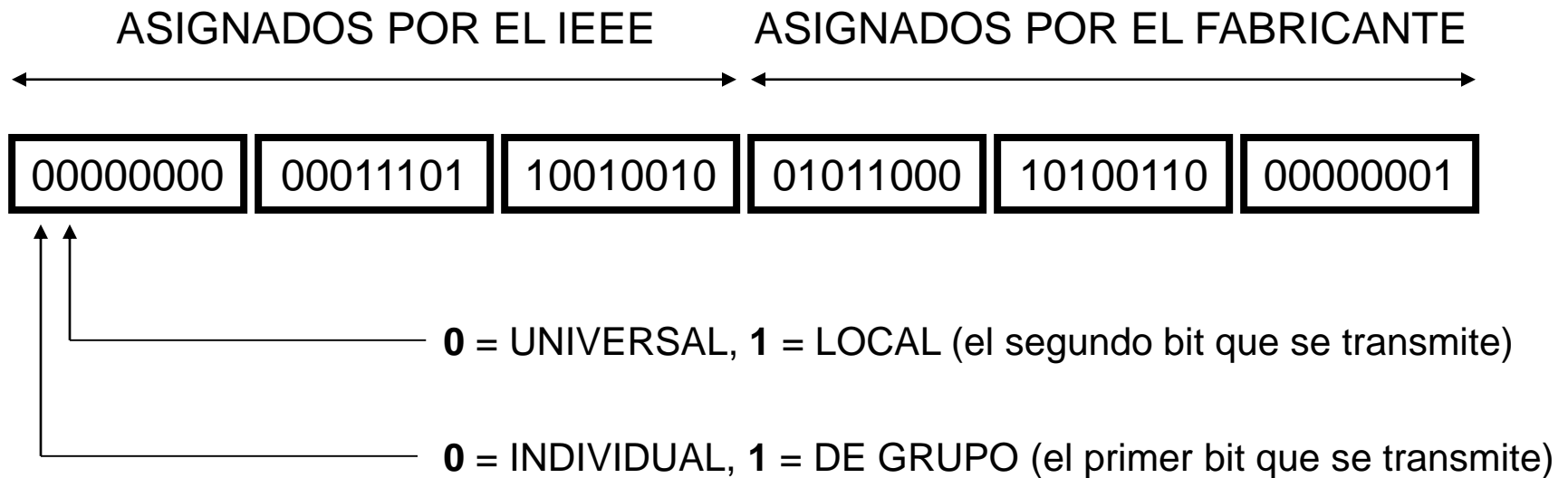
❖ No son jerárquicas

- No guardan ninguna relación con la localización, tal como veremos luego las direcciones IP.

EJEMPLO

❑ dirección

00:1D:92:58:A6:01




Unicast / Multicast

Permite enviar en 3 modos:

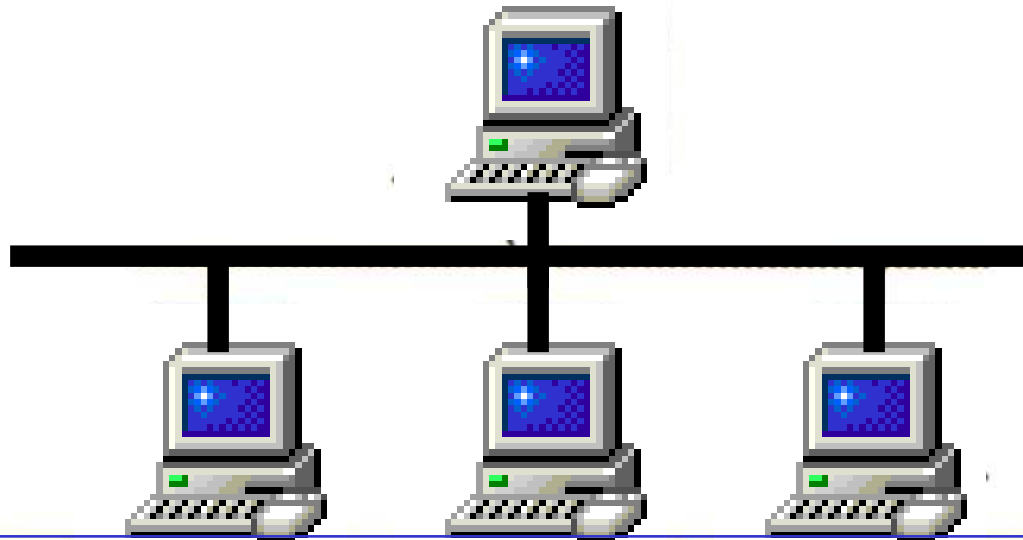
- **Unicast** (bit = 0): destino único; es el uso general
- **Multicast** (bit = 1): el destino es un grupo de usuarios determinado, configurado como tal desde el software por el administrador del sistema.
- **Broadcast** (**FF:FF:FF:FF:FF:FF**) o de difusión, el mensaje llega a todos los usuarios. La difusión de mensajes (**broadcast**) en una red es un tema delicado, ya que puede acarrear problemas de tráfico. En algunas situaciones es muy útil, como cuando un terminal se incorpora a la red y desea localizar a un servidor determinado, por lo que debe permitirse entonces su uso, siempre que sea racional.

RESUMEN

- 1** Conceptos de Redes
- 2** Conmutación de Circuitos, Mensajes y Paquetes
- 3** Modelo de Referencia OSI
- 4** Redes LAN: Generalidades
-  **5** Redes LAN: IEEE 802.3 – ETHERNET

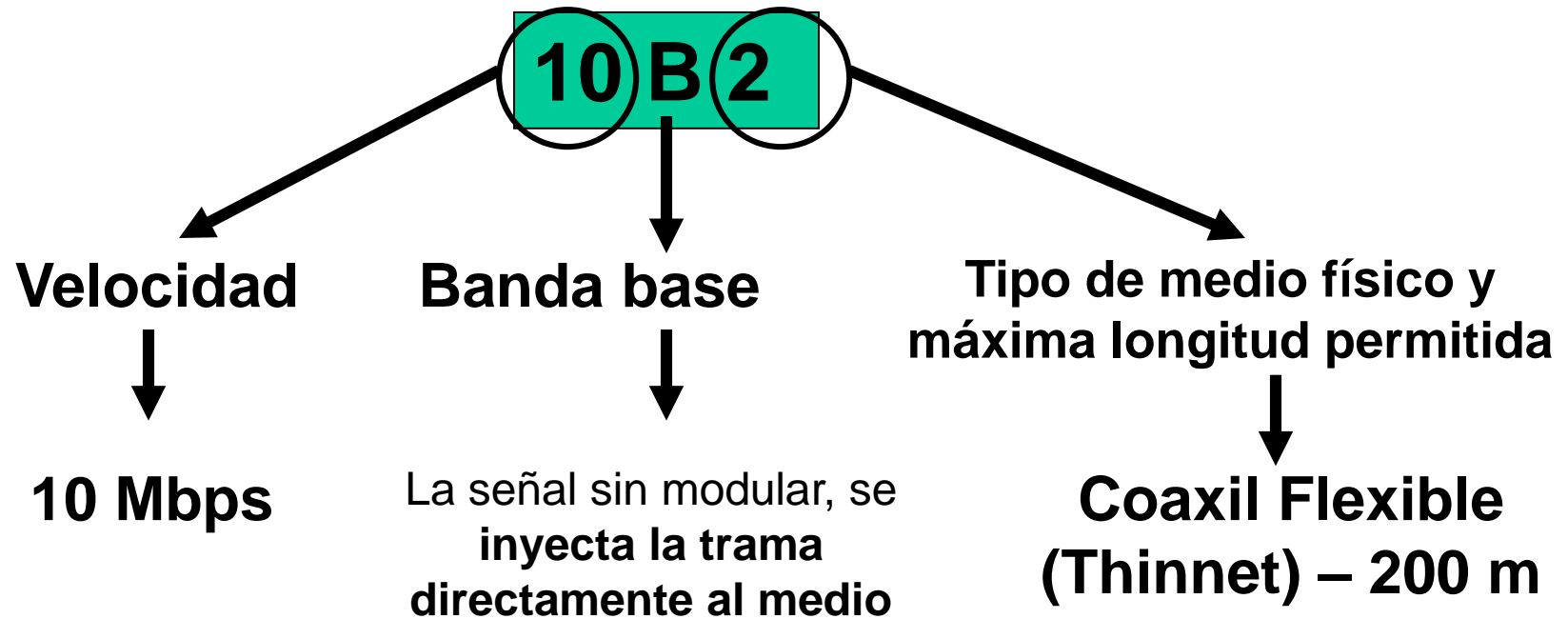
✚ Se caracteriza por:

▶ Topología en bus (física / lógica)



✚ Técnica de acceso **CSMA/CD**:

- ▶ Método de acceso múltiple (Multiple Access)
- ▶ Escucha de portadora (Carrier Sense)
- ▶ Detección de colisiones (Collision Detect)



Ejemplos:

10B2 10 Mbps Banda Base Coaxil flexible (BNC T) – 200 m

10B5 10 Mbps Banda Base Coaxil grueso (TRANCEIVER) – 500 m

10BT 10 Mbps Banda Base Cable UTP sin apantallar – Fichas RJ45 (Par Trenzado – Twister Pair) – 100 m

10BF 10 Mbps Banda Base (Fibra óptica)



Cable coaxil 10B2

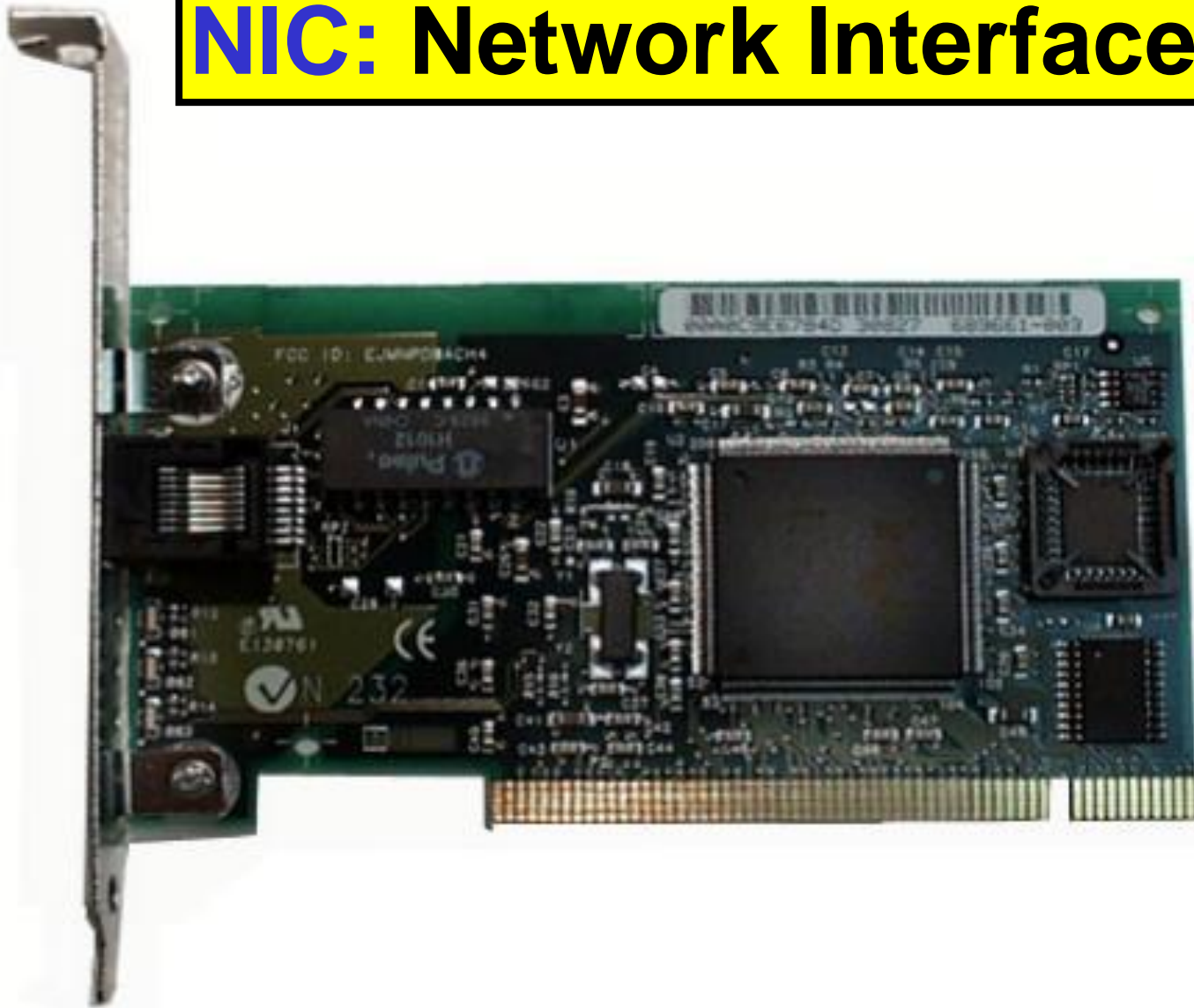


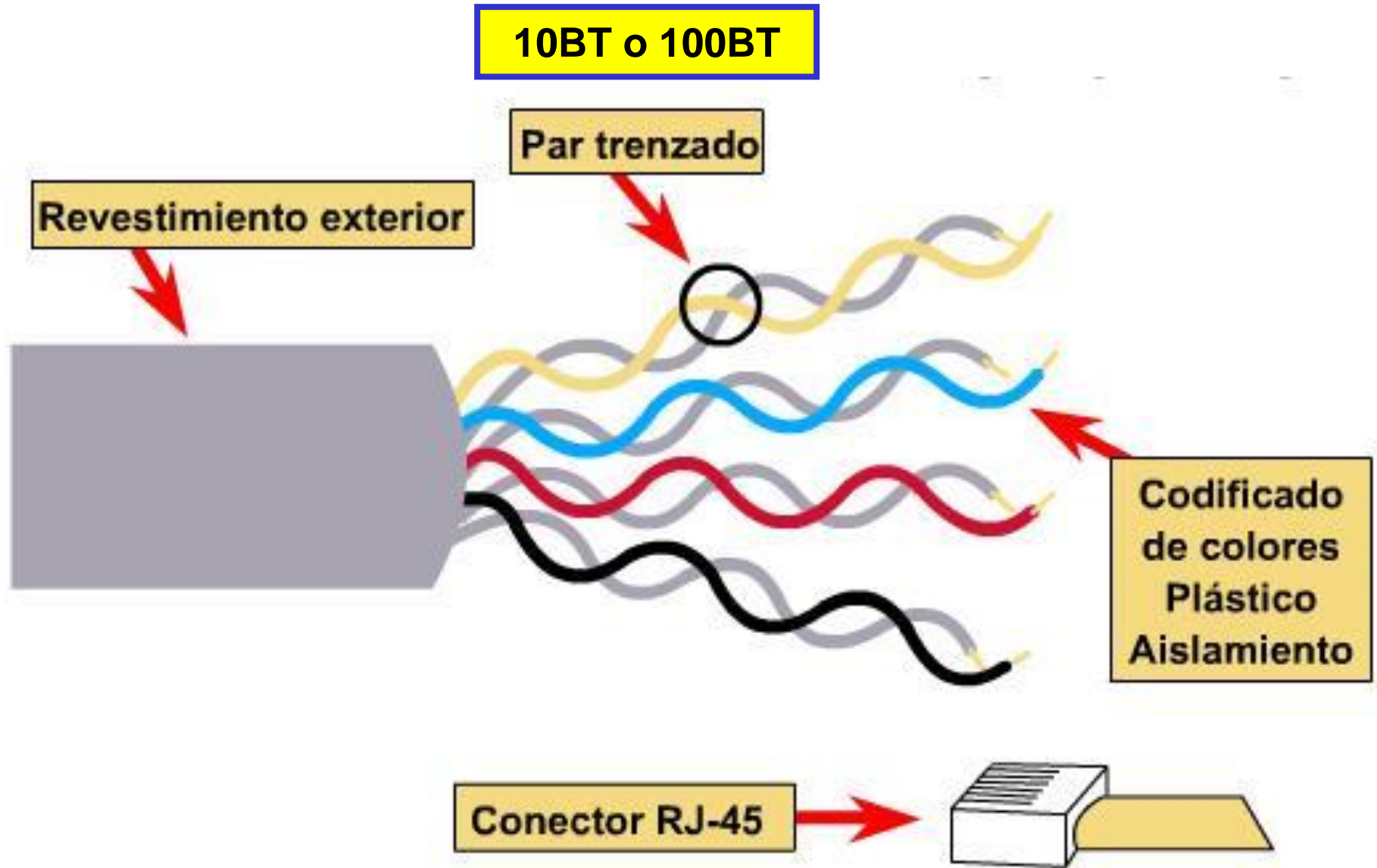
Conector BNC



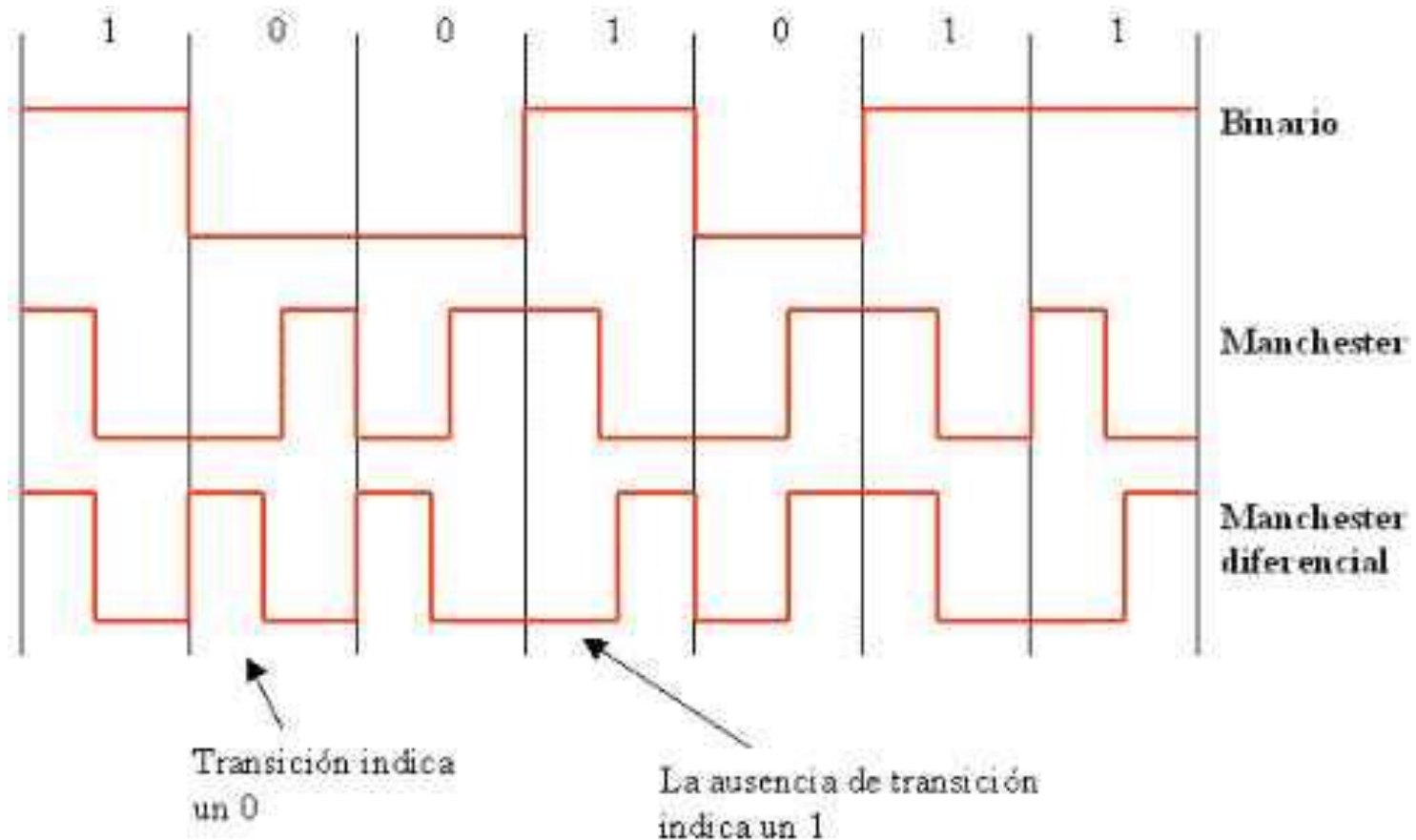
Cable coaxil 10B5

NIC: Network Interface Card

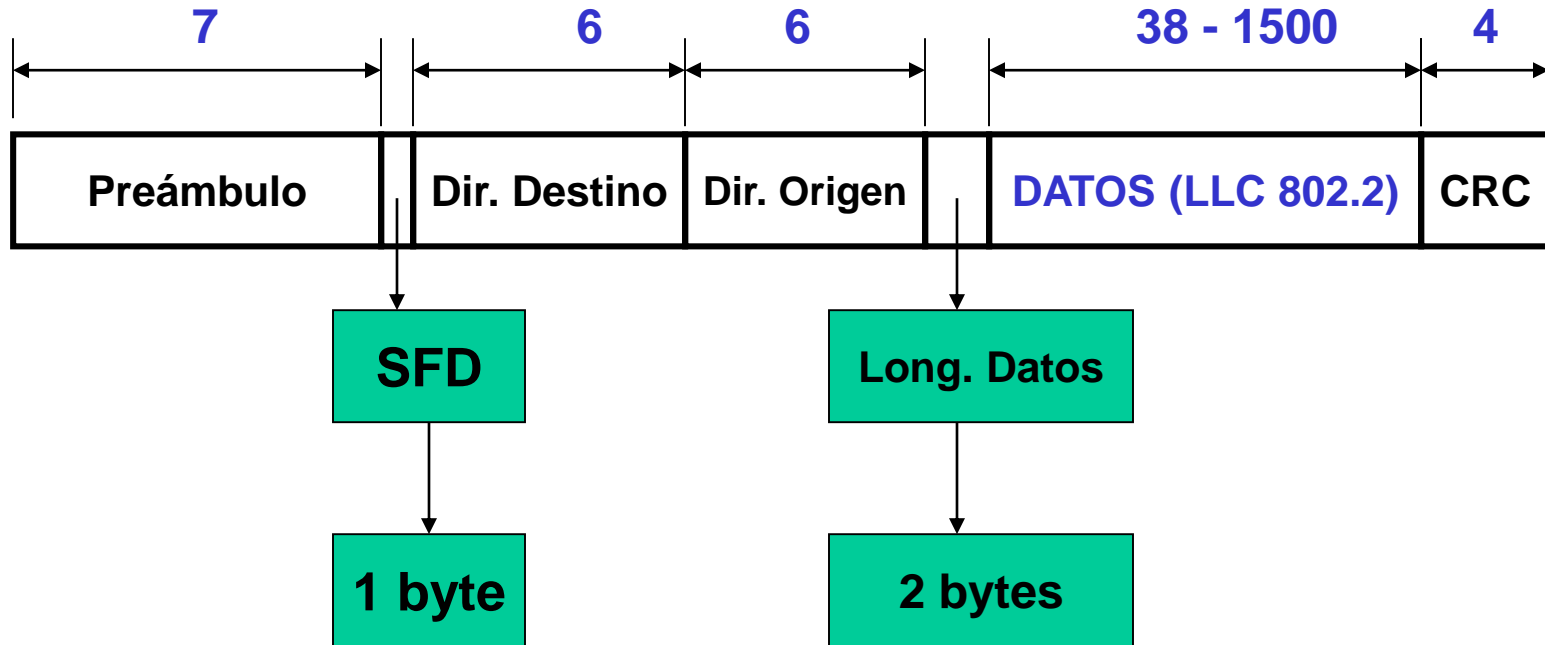




Para la detección de las colisiones no es adecuado el uso de un código binario, ya que no es sencillo detectar bien las mismas y porque además es **vulnerable al ruido**. Por todo lo antedicho se usa la codificación **Manchester** (Ethernet) y **Manchester diferencial** (Token ring).

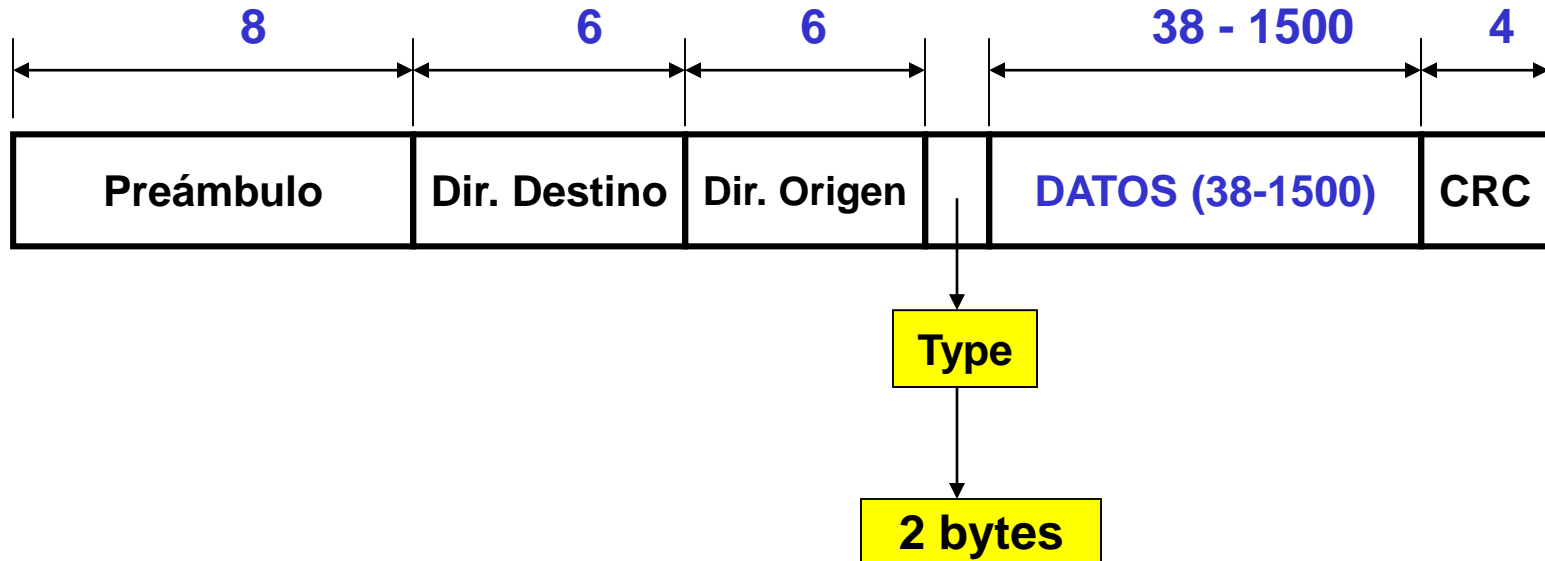


FORMATO DE LA TRAMA IEEE 802.3



- **Preámbulo** (7 bytes) : 1010.....10 para sincronizar los relojes
- Delimitador de principio de trama (**SFD** – 1 byte)
- Dirección de origen y destino (6 bytes)
- Longitud de datos (2 bytes): en número de bits
- **Datos (LLC)** (38-1500 bytes). La limitación es para que una estación no acapare el medio.

FORMATO DE LA TRAMA – Ethernet II



- Ethernet II emplea el campo **Type** en lugar de **Lenght**. El campo **Type** indica el tipo de protocolo que transporta la trama en su campo de datos. Por ejemplo **0806h** indica ARP, **0800h** IP, etc.
- Además Ethernet II no emplea LLC, o sea el IEEE 802.2
- Ethernet II es el formato de trama que más se emplea en la actualidad.

EL MÉTODO DE ACCESO CSMA/CD

❖ Escucha de portadora (*Carrier Sense*)

- si el medio está libre: se transmite
- si el medio está ocupado: se espera

❖ Detección de colisiones (*Collision Detection*)

- Durante la transmisión, se analiza la señal
- Si se detecta colisión:
 - ▶ Se **refuerza** la colisión (**32 bit noise burst**)
 - ▶ Se deja de transmitir
 - ▶ Se entra en una espera de duración aleatoria

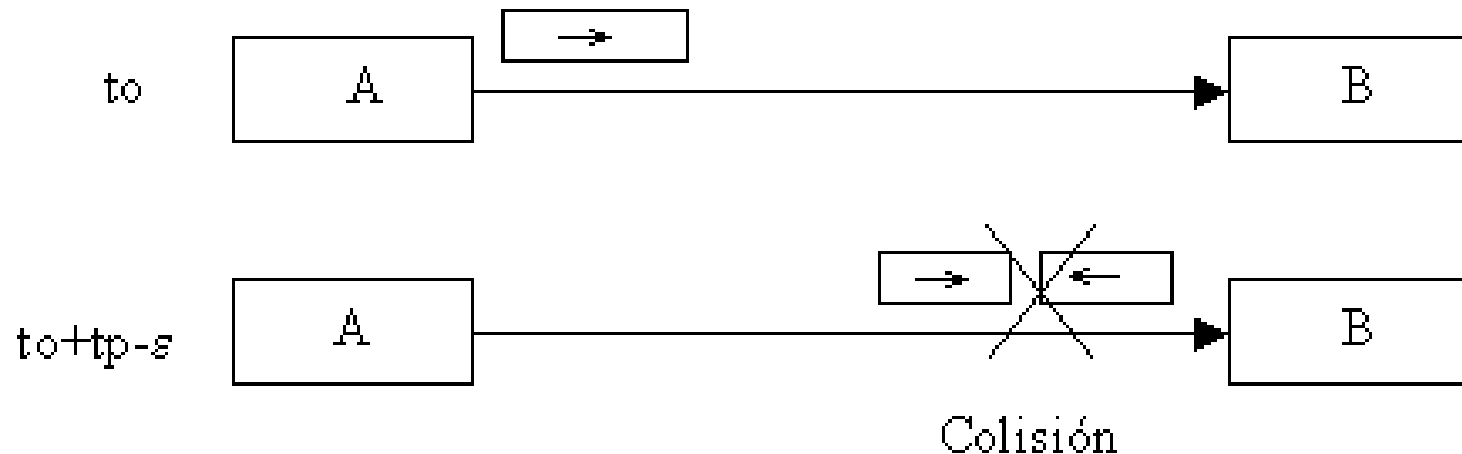
❖ No hay prioridades (Cualquier estación puede transmitir en cualquier momento)

❖ No se garantiza un tiempo máximo de acceso a la red.

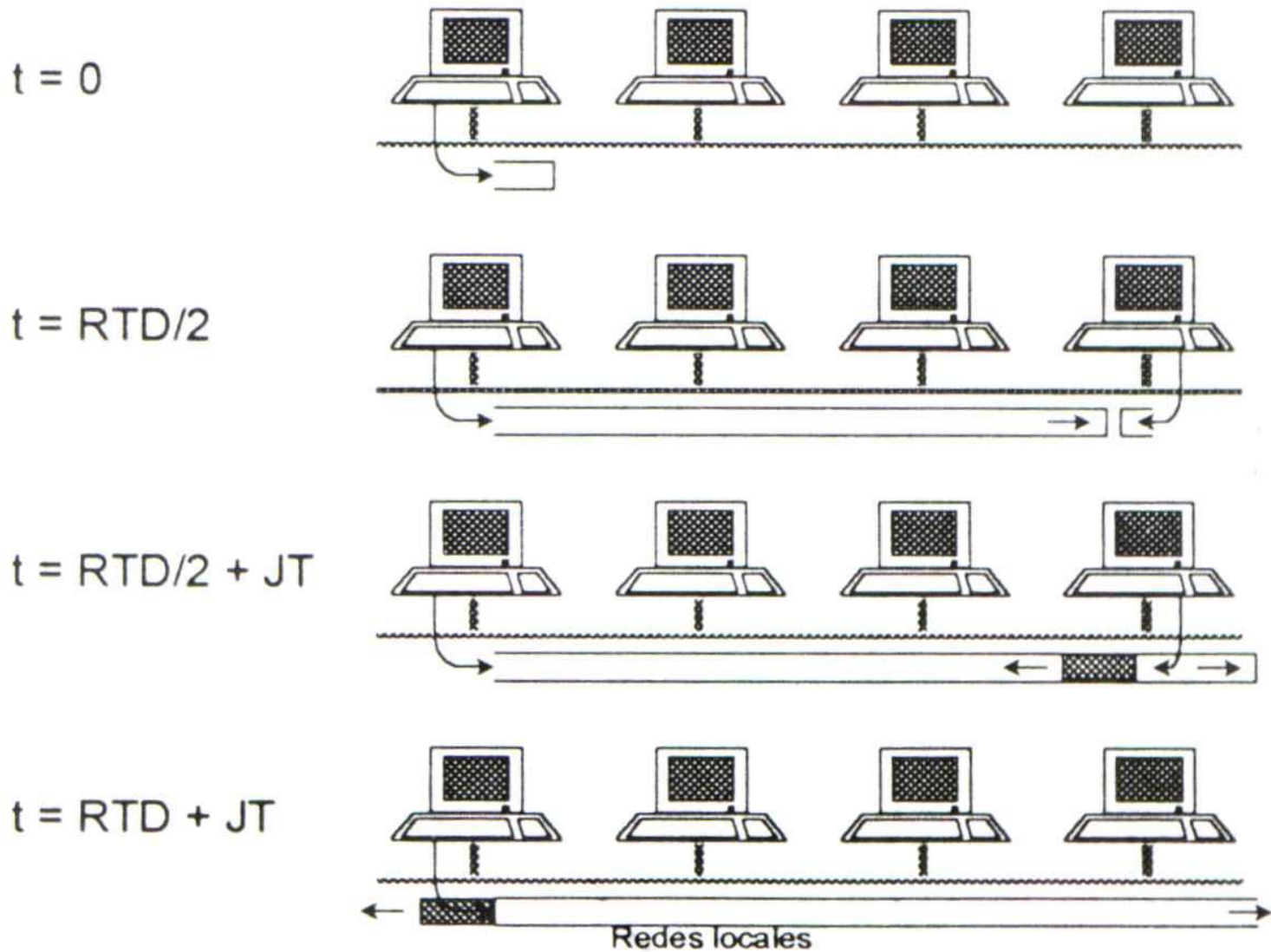
DEFINICIONES

◆ **JT** (Jam Time) = Tiempo de refuerzo de la colisión – **32 bits**

◆ **RTD** (Round Trip Delay) = Retardo de propagación de ida y vuelta, extremo a extremo.



VENTANA DE COLISIÓN = RTD + JAM TIME



VENTANA DE COLISIÓN

- Para detectar una colisión, se debe estar aún transmitiendo
- **Definición:**
 - Ventana de colisión (**Time Slot**) = **RTD + JAM TIME**
 - Duración de la ventana de colisión **512 bits**
- Hasta que no transcurre la ventana de colisión no estamos seguros de no tener colisión.
- ▶ Las tramas no pueden ser menores que el Time Slot, o sea **512 bits**.

REPETIDORES

+ Permiten alargar la longitud de la red

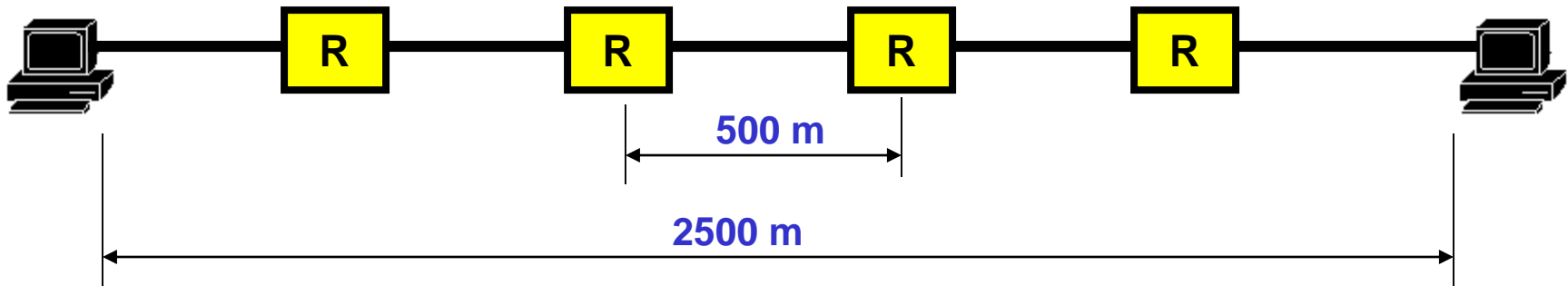


■ Unen segmentos de red

- Dos o más
- Pueden utilizar distinto medio físico
- Pero deben ser:
 - ▶ de la misma velocidad
 - ▶ usar el mismo protocolo **MAC** (por ejemplo no **ETHERNET** con **TOKEN RING (802.3 con 802.5)**)

Primera versión de la norma: 10BASE5

Usa como medio físico un coaxial de **50 Ω** (un cable rígido de buena calidad y caro). Permite segmentos de hasta 500 m, hasta un número máximo de **5** segmentos con repetidores. La distancia máxima es, por lo tanto, de **2,5 km**. **Cuánto vale RTD ?**



$$RTD = 2 \times (5 \times tp_{coaxil} + 4 \times tp_{repeater}) \quad v_{coaxil} = \frac{C}{\sqrt{\epsilon_{r \text{ POL}}}} = 1,98 \cdot 10^8 \text{ m/s} \quad \epsilon_{r \text{ POL}} = 2.3$$

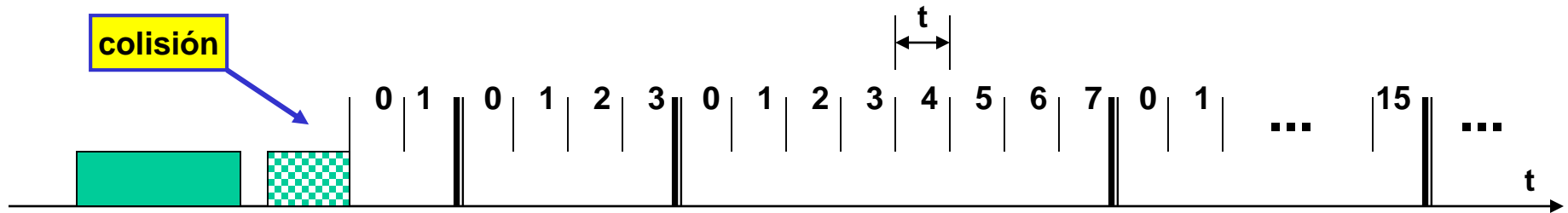
$$\therefore tp_{coaxil} = \frac{500 \text{ m}}{1,98 \cdot 10^8 \text{ m/s}} = 2,53 \mu \text{s}$$

Suponiendo un $tp_{repeater} \approx 2 \mu \text{s}$

$$RTD = 2 \times (5 \times 2,53 + 4 \times 2) \cong 42 \mu \text{s} \quad N^{\circ} \text{ bits} = \frac{42 \mu \text{s}}{0,1 \mu \text{s}} = 420 \text{ bits}$$

A estos 420 bits le sumamos los 32 bits de JT y estamos en 452 bits. De aquí surge que el tamaño mínimo de la trama sea de 512 bits (64 bytes) !!!

Una de las funciones del protocolo **MAC de ETHERNET 802.3** es que una vez detectada una colisión se pase a resolverla, para ello el protocolo aplica una técnica denominada **BEB** (Binary Exponential Backoff).



Consiste en dividir el tiempo posterior a una colisión en **slots de duración t** (intervalo de vulnerabilidad). Tras la colisión las estaciones involucradas vuelven a intentar transmitir en una de las dos ranuras de tiempo siguientes de forma **aleatoria**. Si se vuelve a producir una colisión, esas estaciones intentarán transmitir en una de las **4** ranuras siguientes. Ante nuevas colisiones, las estaciones verán multiplicado sucesivamente por **2** su margen de repetición, que será de **2^i** tras la colisión **i -ésima**. Esto se mantiene hasta la **10ª colisión**, a partir de la cual el intervalo se estabiliza en **1024 slots**. Finalmente si se alcanza la **16ª colisión**, la estación desiste del proceso e informa al nivel superior del error de transmisión.

181.28.113.152

72.163.4.154

Comunicación Peer to Peer (IV)

Encapsulamiento

Desencapsulamiento

Direccionamiento

SWITCH

ROUTER

ROUTER

SWITCH

HOST A

HOST B

Aplicación

Presentación

Sesión

TCP/UDP

IP

Eth

N1

Eth

N1

N1

Eth

FR

N1

N1

IP

IP

FR

Eth

N1

N1

Eth

N1

N1

Aplicación

Presentación

Sesión

TCP/UDP

IP

Eth

N1

101101101011

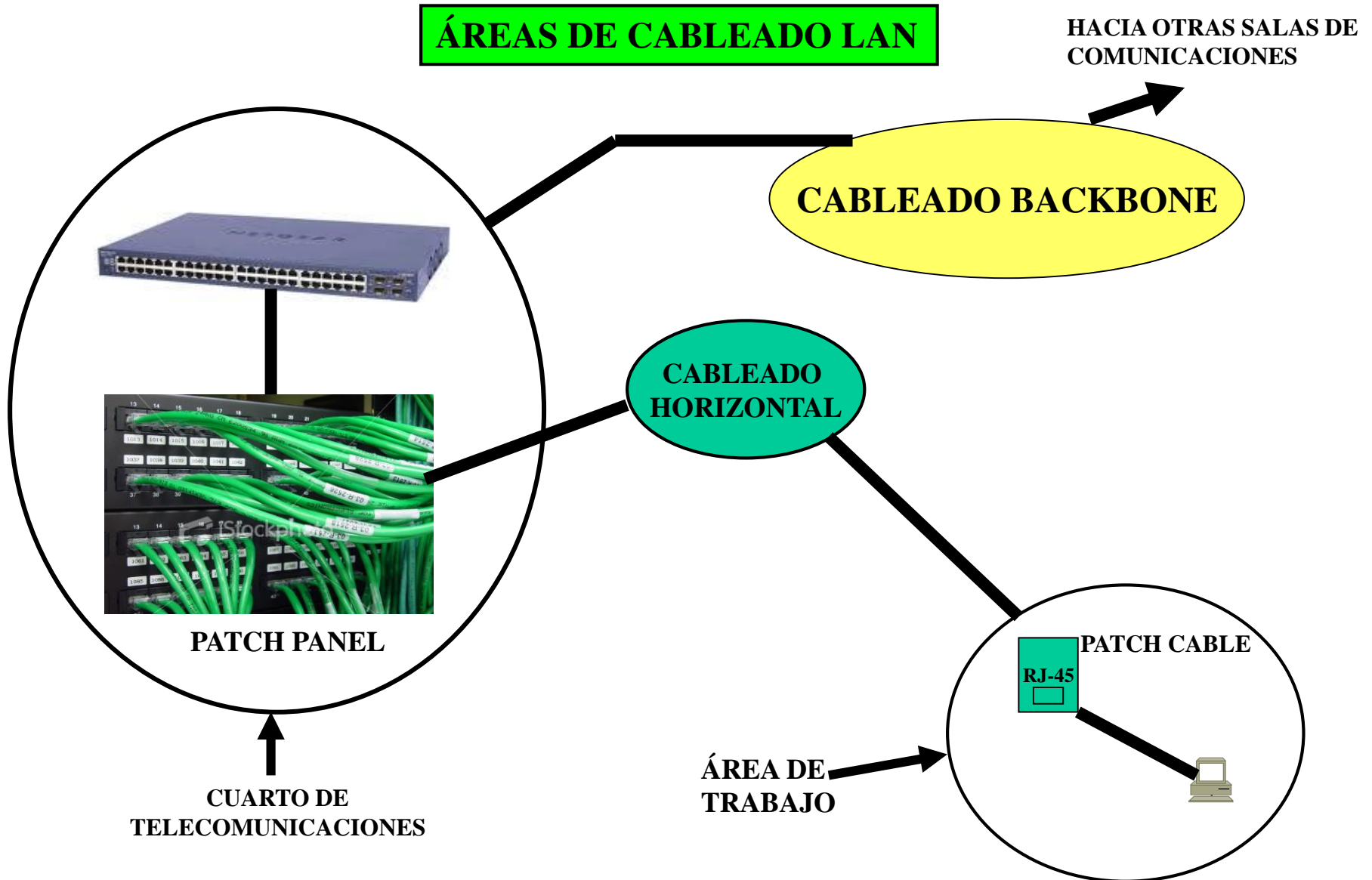
101101101011

bits

Enrutamiento

bits

Cableado en redes LAN y WAN



Cableado en redes LAN y WAN

Los tipos de medio pueden ser:

- UTP (categorías 5, 5e, 6 y 7)
- Fibra óptica multimodo o monomodo
- Wireless



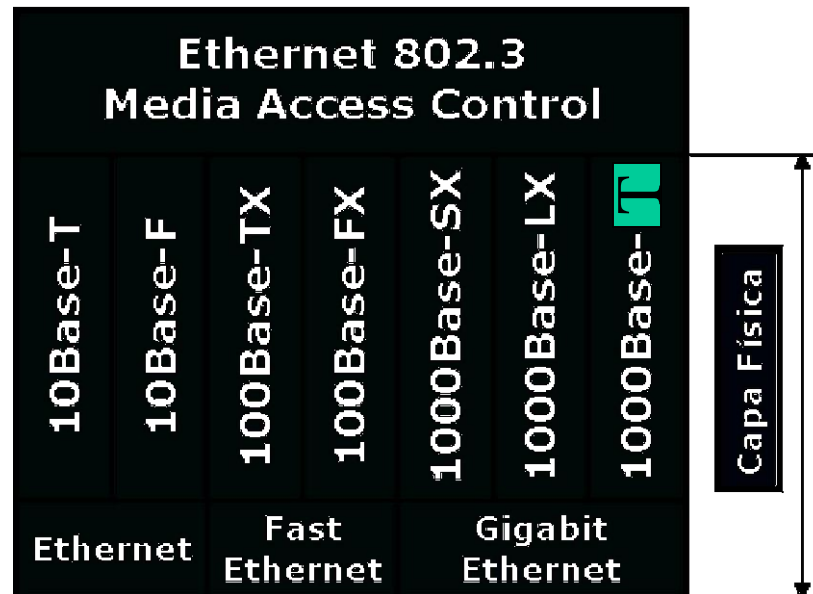
UTP



FIBRA

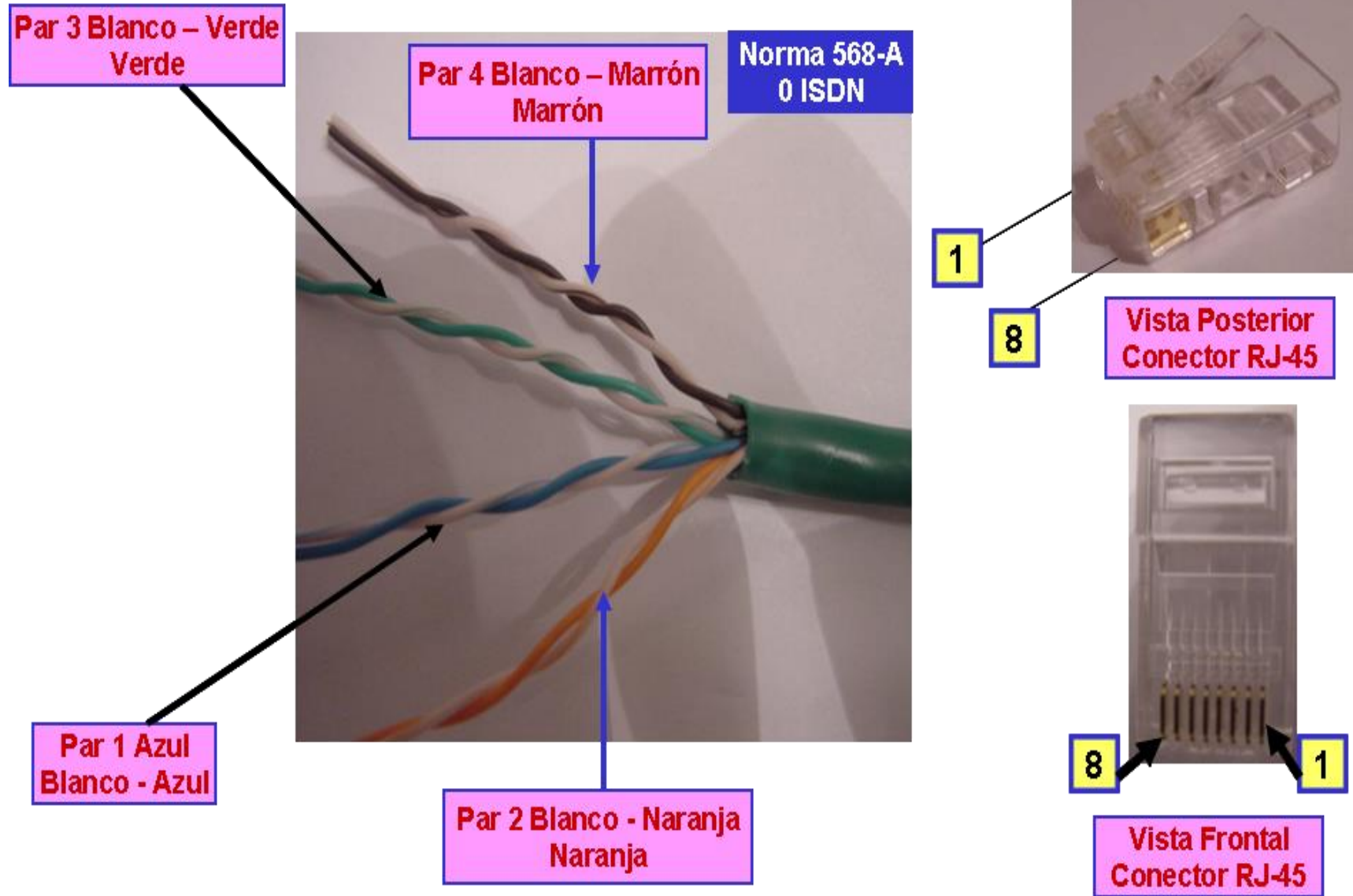


WIRELESS

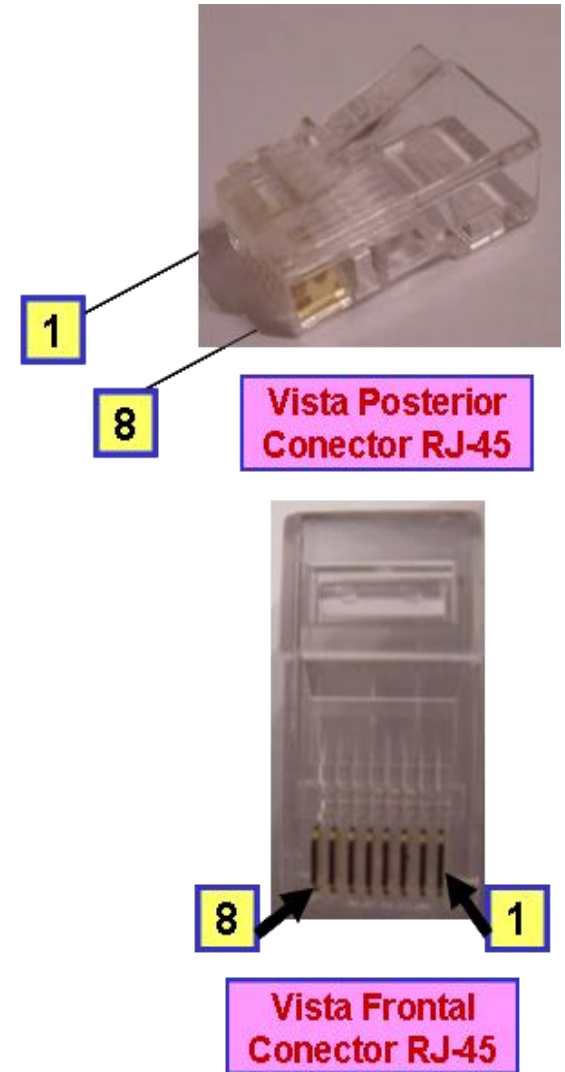
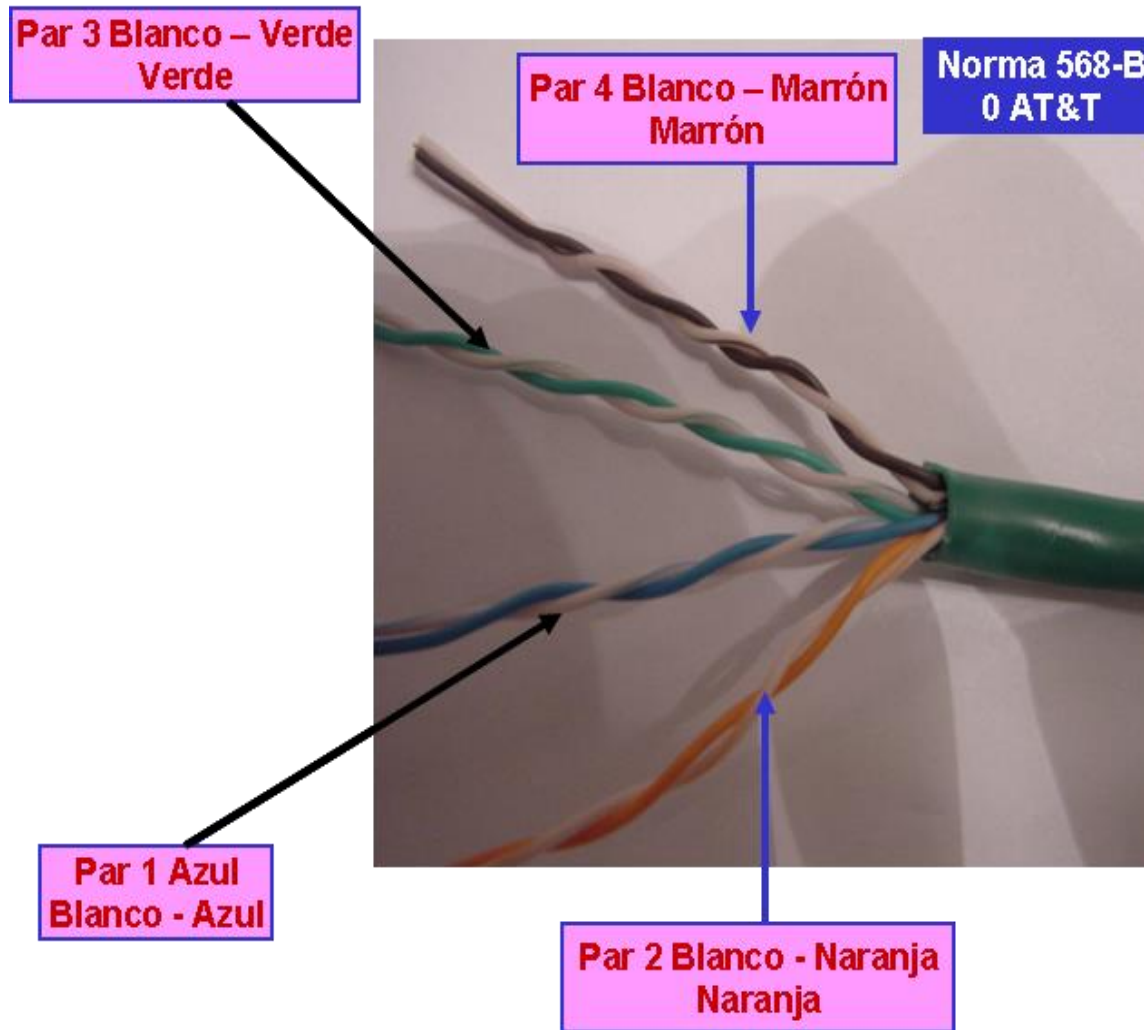


Interface	Medio	Velocidad	Distancia
10Base-T	UTP Categoría 5	10 Mbps	100 m
10Base-F	Fibra	10 Mbps	2 Km
100Base-TX	UTP Categoría 5	100 Mbps	100 m
100Base-FX	Fibra óptica Multimodo	100 Mbps	2 km
1000Base-T	UTP Categoría 5E	1000 Mbps	100 m
1000Base-SX	FO multimodo (62.5 µm)	1000 Mbps	220 m
1000Base-LX	FO monomodo (10 µm)	1000 Mbps	5 Km

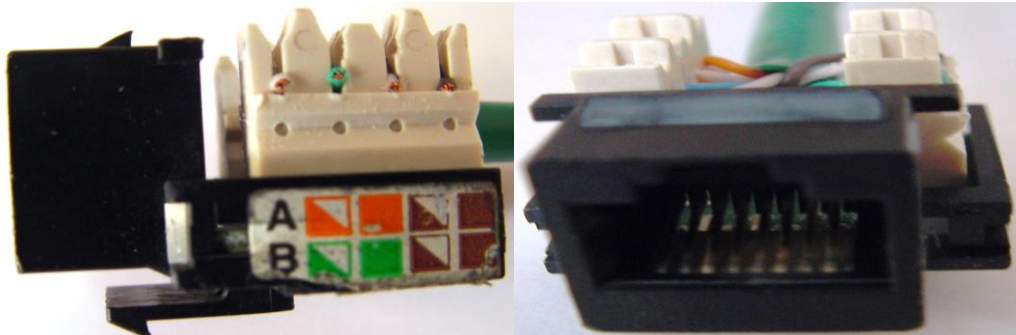
Cableado en redes LAN y WAN



Cableado en redes LAN y WAN



Diversas Herramientas empleadas en cableado de LAN



Cableado en redes LAN y WAN

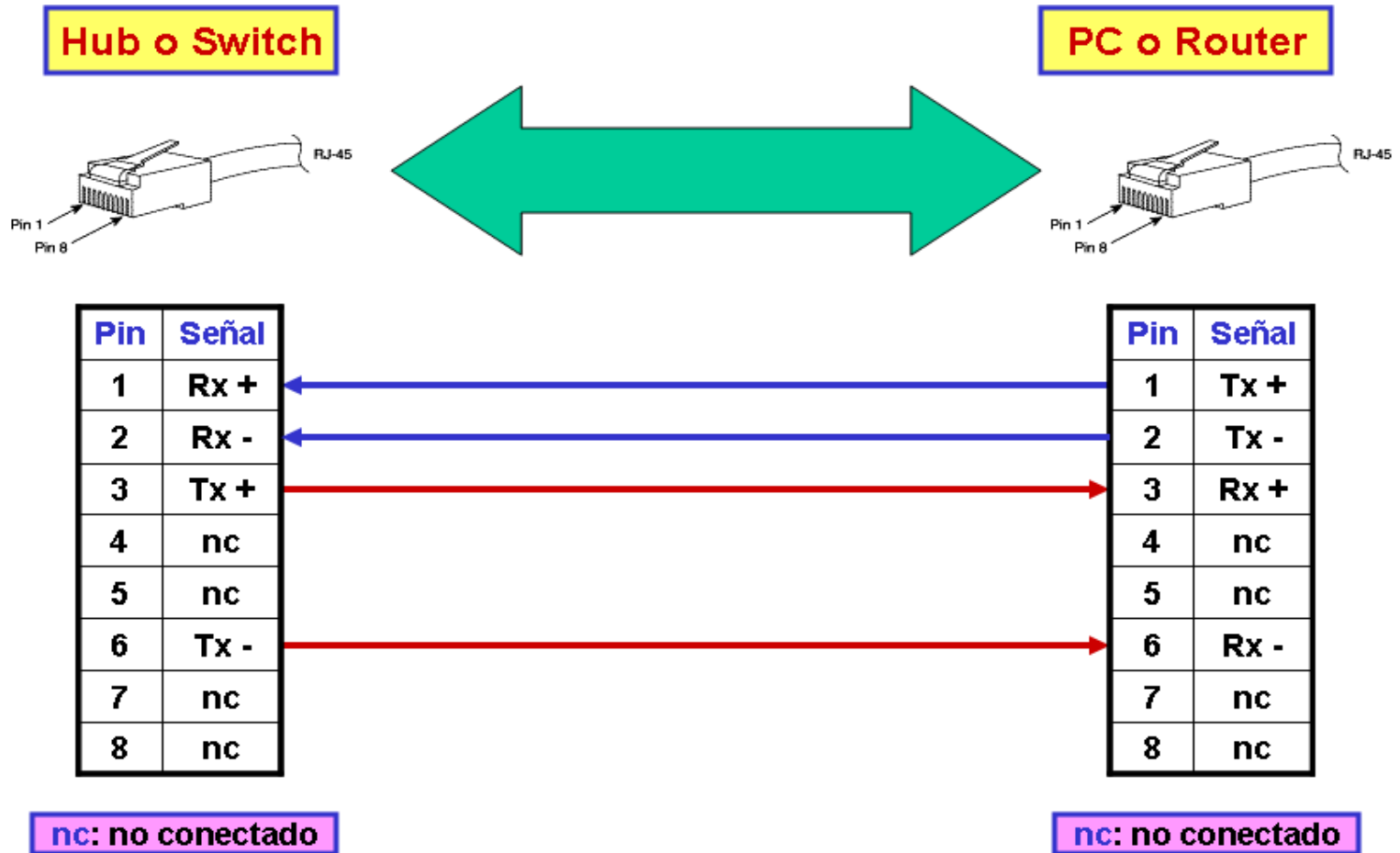
Norma 568-A 0 ISDN

PIN	PAR	Función	COLOR	10/100 BaseT Ethernet	100 BaseT4 y 1000BT Ethernet
1	3	TX	Blanco Verde	SI	SI
2	3	RX	Verde	SI	SI
3	2	TX	Blanco Naranja	SI	SI
4	1	Telefonía	Azul	NO	SI
5	1	Telefonía	Blanco Azul	NO	SI
6	2	RX	Naranja	SI	SI
7	4	Respaldo	Blanco Marrón	NO	SI
8	4	Respaldo	Marrón	NO	SI

Norma 568-B 0 AT&T

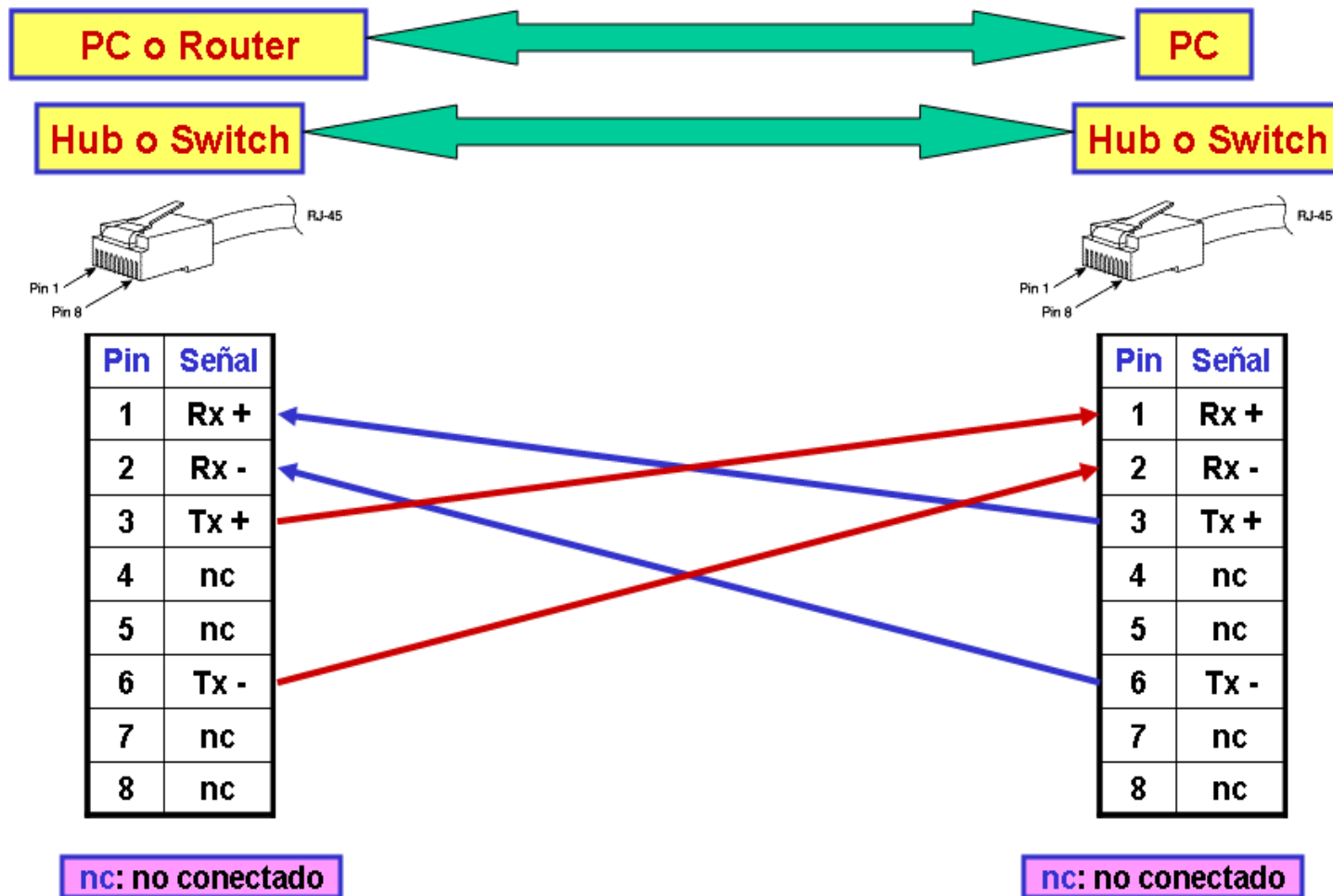
PIN	PAR	Función	COLOR	10/100 BaseT Ethernet	100 BaseT4 y 1000BT Ethernet
1	2	TX	Blanco Naranja	SI	SI
2	2	RX	Naranja	SI	SI
3	3	TX	Blanco Verde	SI	SI
4	1	Telefonía	Azul	NO	SI
5	1	Telefonía	Blanco Azul	NO	SI
6	3	RX	Verde	SI	SI
7	4	Respaldo	Blanco Marrón	NO	SI
8	4	Respaldo	Marrón	NO	SI

Cableado en redes LAN y WAN



CABLE DERECHO

Cableado en redes LAN y WAN



CABLE CRUZADO O CROSSOVER

✚ Cable derecho

■ Para conectar entre

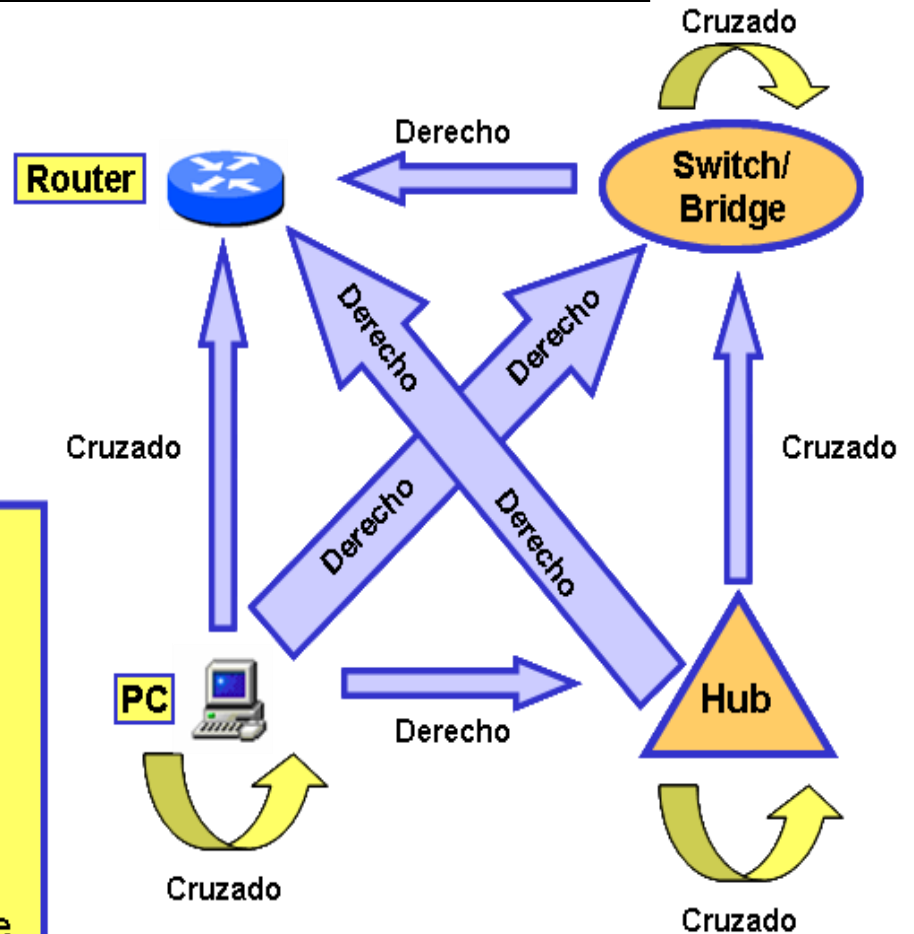
- ▶ PC y Hub
- ▶ PC y Switch / Bridge
- ▶ Hub y Router
- ▶ Switch /Bridge y Router

✚ Cable cruzado

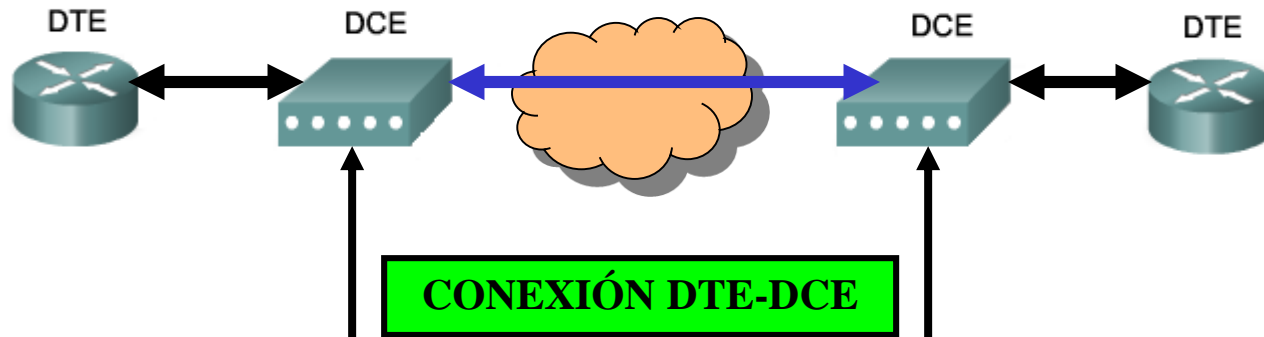
■ Para conectar entre

- ▶ PC a Router
- ▶ PC a PC
- ▶ Hub a Hub
- ▶ Switch /Bridge a Switch / Bridge
- ▶ Hub a Switch /Bridge

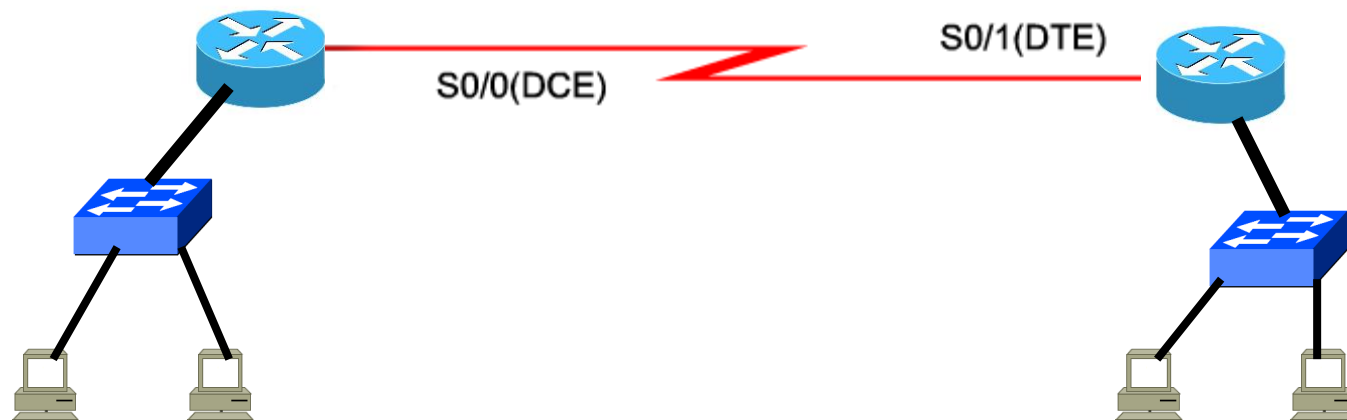
RESUMEN CABLEADO LAN



CABLEADO EN WAN



El dispositivo DCE es el encargado de proveer la señal de temporización



Conexión de laboratorio DTE-DCE Back to Back

CABLEADO EN WAN



DTE SERIAL



DTE SMART SERIAL

Conectores DB-60 a V.35



DCE SERIAL



DCE SMART SERIAL

Cableado en redes LAN y WAN

