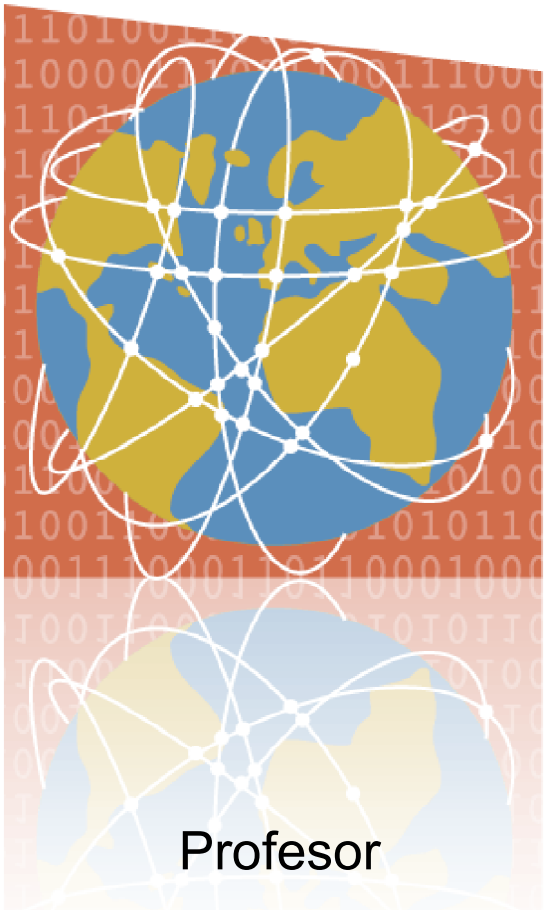
Protocolos de Interconexión de Redes

Tema 0.

Fundamentos de la Redes de Comunicación



Profesor

Alberto E. García Gutiérrez

Este Tema se publica bajo licencia:

Creative Commons 3.0 BY-NC-SA

Tema 0.

FUNDAMENTOS DE LAS REDES DE COMUNICACIÓN

1 TIPO DE REDES DE COMUNICACIÓN
- 1.1 REDES WAN
- 1.2 REDES LAN

2 TOPOLOGÍA
- 2.1 TOPOLOGÍA EN ESTRELLA
- 2.2 TOPOLOGÍA EN BUS
- 2.3 TOPOLOGÍA EN ÁRBOL
- 2.4 TOPOLOGÍA EN ANILLO
- 2.5 TOPOLOGÍAS MIXTAS

3 MEDIOS DE TRANSMISIÓN
- 3.1 CABLE COAXIAL
- 3.2 CABLE DE PAR TRENZADO
- 3.3 FIBRA ÓPTICA
- 3.4 WIRELESS
- 3.5 APLICACIONES

4 NORMALIZACIÓN
- 4.1 ORGANISMOS DE NORMALIZACIÓN

5 MODELOS DE REFERENCIA: ARQUITECTURAS
- 5.1 ESTRUCTURA FUNDAMENTAL

6 EL MODELO ISA OSI
- 6.1 CONCEPTOS BÁSICOS
- 6.2 LA COMUNICACIÓN OSI
- 6.3 NIVELES OSI

7 TIPOS DE ARQUITECTURAS
8. NORMALIZACIÓN DEL NIVEL DE ENLACE: IEEE 802
9. TECNICAS DE TRANSMISION
10. CONTROL DE ACCESO AL MEDIO
- 10.1 CONTROLADOS
- 10.2 CONTIENDA
- 10.3 RESERVA

11. CONTROL DE ACCESO AL MEDIO EN REDES DE ALTA VELOCIDAD
12. REDES X25
13. FRAME RELAY

1. TIPOS DE REDES DE COMUNICACIÓN

La estructuración del concepto de Red de Ordenadores primero pasa por el análisis de los siguientes aspectos fundamentales:

- La **arquitectura**, es decir la definición abstracta de los servicios soportados por la red y los protocolos implicados en las comunicaciones establecidas en la misma.

- El **modelado** de la red, es decir el establecimiento y diseño de los modelos matemáticos que mejor describan el comportamiento de la red, con el fin de permitir el análisis y evaluación de los parámetros de calidad tanto de los servicios como de la red en sí.

- Las características **físicas** y **lógicas**, es decir, la realidad física de la red de comunicación de ordenadores.

Estas últimas son quizá las más importantes, de las cuales destacan tanto la topología y los medios de transmisión (la estructura y elementos del nivel físico de la red) como los sistemas de transmisión, acceso y conmutación.

Según las directivas de la **UIT-T** (**Unión Internacional de Telecomunicaciones sección Transmisión**), en su **Libro Verde de las Telecomunicaciones**, o según se recoge en el ámbito nacional en la **Ley de Ordenación de las Telecomunicaciones** (**LOT**) las Redes de Comunicación pueden ser fundamentalmente (dependiendo de quién sea el Operador de la Red):

- **Redes Públicas**, es decir, redes gestionadas, controladas y explotadas comercialmente por un operador dependiente de la Administración Pública. Proporcionan servicios de transmisión de voz y datos en igualdad de condiciones a la totalidad de los usuarios, posibilitando el establecimiento de comunicación entre distintos puntos de terminación de red.

- **Redes Privadas**, es decir, redes cuyos equipos y programas de control son de propiedad y explotación exclusiva de una única entidad. Permiten a los usuarios de un grupo cerrado proveerse de los servicios de telecomunicación que precisen y disponer en todo momento de la totalidad de los recursos de la red con la fiabilidad y calidad de servicios requeridos. Su principal diferencia con las redes públicas estriba en que solo dan servicio a un grupo cerrado de usuarios, lo que significa que nadie que no pertenezca a dicho grupo tiene acceso a los recursos de red.

- **Redes Privadas Virtuales**: son redes privadas pero ofertadas por un operador de la red pública. Este establece de forma personalizada a cada cliente una red dedicada para su servicio exclusivo con los requerimientos que este establezca y contrate. Esto significa un conjunto de grupos cerrados de usuarios dentro de la misma red, pero que solo pueden tener comunicación entre usuarios del mismo grupo y no con los de otros grupos, de forma que desde el punto de vista del usuario, solo existe su grupo en la red.

- **Redes Corporativas**: son redes de telecomunicación que ofrecen servicios a un conjunto limitado de entidades relacionadas entre sí. Su principal objetivo es crear entornos de servicio y transporte unificado a la medida de las empresas de la corporación y la explotación óptima de la infraestructura de telecomunicación compartida.

- **Redes Móviles**: son redes de telecomunicación en las que los terminales no están en una posición fija, sino que pueden encontrarse en movimiento estableciendo conexiones con otros terminales a través de estaciones base que componen la red intermedia. La tecnología utilizada suele ser radio, ya sea a nivel terreno o vía satélite.

Sin embargo, esta clasificación no resulta nada intuitiva. Si atendiéramos a la **cobertura** de servicio de las mismas, podríamos dividir las redes de telecomunicación en:

- **Redes de Área Local (LAN - Local Area Network)**: son todas aquellas redes de ordenadores limitadas exclusivamente a una extensión máxima de un kilómetro y un límite teórico de 8000 puestos de trabajo.

- **Redes de Área Metropolitana (MAN - Metropolitan Area Network)**: Son redes de dimensiones a nivel regional. Suelen interconectar tanto a sistemas individuales como a otras LAN, y cuando su dimensión se limita a edificios también se las conoce como **Redes de Campus**.

- **Redes de Área Extensa (WAN - Wide Area Network)**: Superan en extensión a las MAN (también podrían considerarse WAN a nivel regional), aunque no necesariamente en número de puestos. Suelen ser utilizadas para la interconexión de oficinas o sucursales en distintos puntos geográficos, siendo el ejemplo más actual y de mayor dimensión la red **INTERNET**.

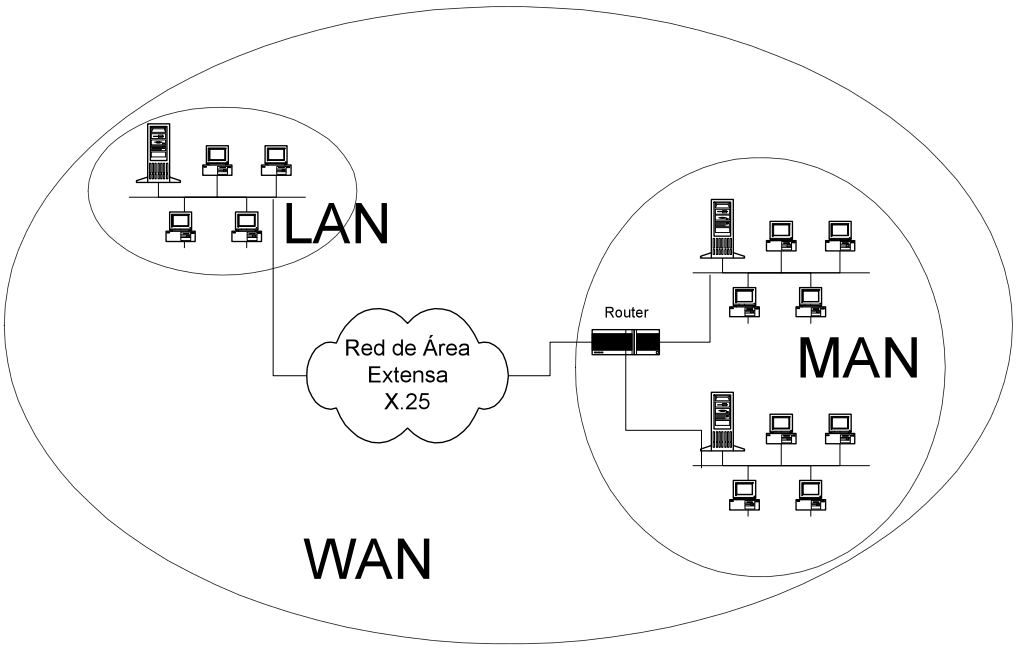


Fig. I.1: *Los conceptos de LAN, MAN y WAN.*

1.1 REDES WAN

Una Red de Área Extensa es aquella que tiene las siguientes características:

- Cubre una amplia superficie o área geográfica.
- Utiliza, en general, medios de telecomunicación suministrados por operadores externos.

Atendiendo al modo de transferencia (La UIT-T define transferencia como el conjunto de transmisión, multiplexación y conmutación) podemos definir los siguientes tipos de WAN:

- **Redes dedicadas**: utilizan circuitos dedicados para cada transmisión sin realizar funciones de conmutación. Los circuitos dedicados pueden ser tanto analógicos, como digitales. Las velocidades de transmisión son fijas, contratadas al operador, normalmente hasta 2 Mbps.

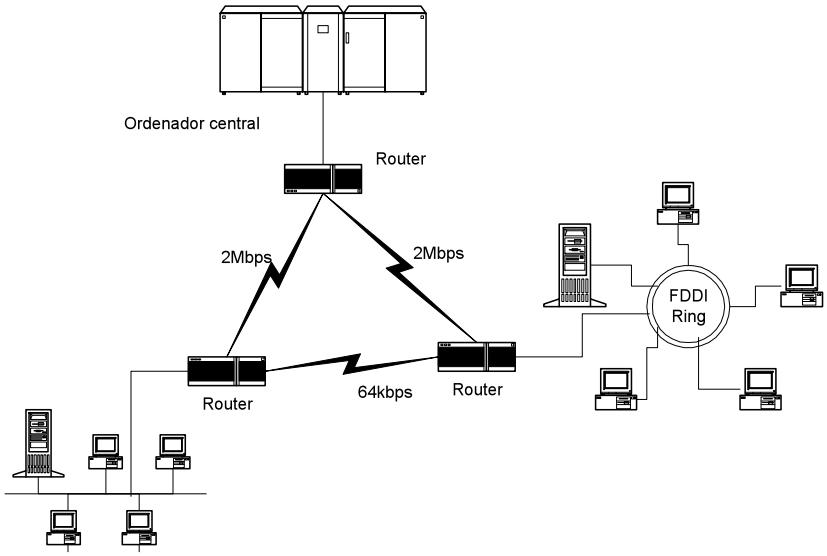


Fig. I.2: *Red de interconexión de LAN's a un ordenador central remoto mediante líneas dedicadas a Telefónica.*

- **Redes de conmutación de paquetes**, como la red **Iberpac**, basada en la Recomendación **X.25**.

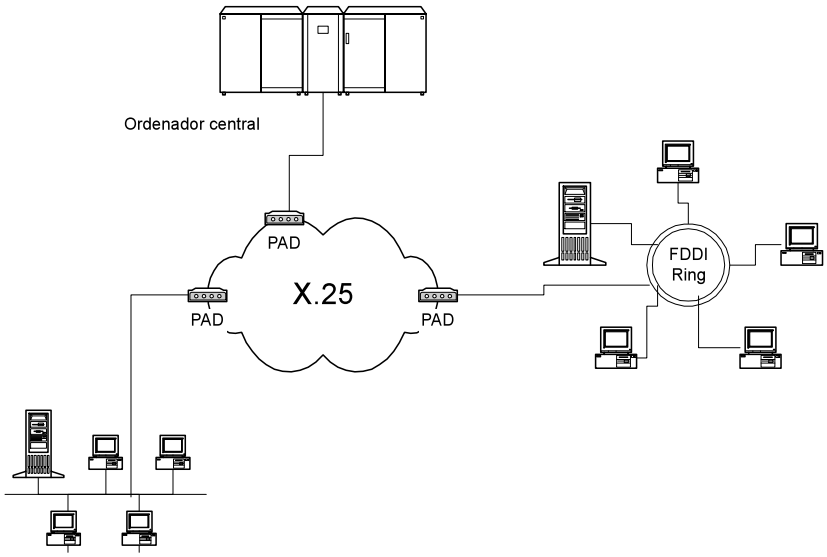


Fig. I.3: *Red de interconexión de LAN's a un ordenador central remoto mediante la red de conmutación de paquetes Iberpac (X.25).*

- **Redes de conmutación analógica de circuitos**, como la **Red Telefónica Conmutada** (RTC). Las velocidades siguen las recomendaciones **V.xx,** desde los 640 hasta los 28800 bps.

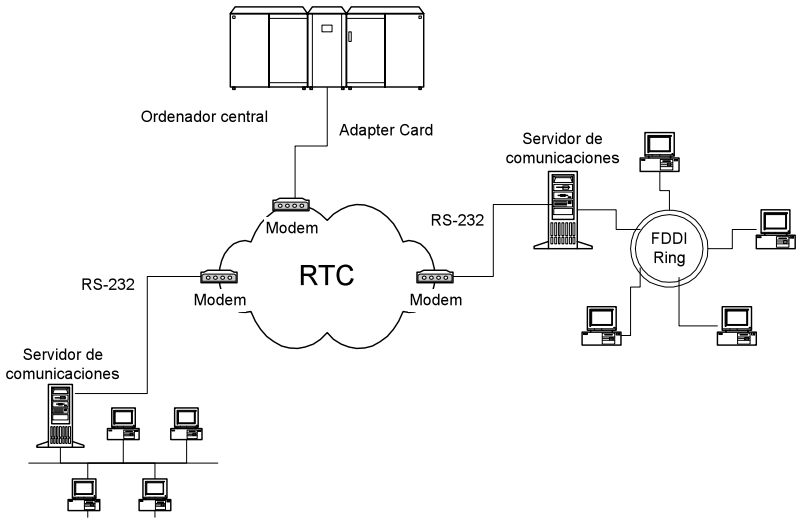


Fig. I.4: *Red de interconexión de LAN's a un ordenador central remoto mediante la red telefónica conmutada.*

- **Redes Digitales de Servicios Integrados** (**RDSI**), basadas en conmutación digital de circuitos. Hace uso de canales de 64 kbps (canal básico), pero pueden contratarse hasta 30 canales (canal Primario), obteniendo una velocidad máxima de 2 Mbps.

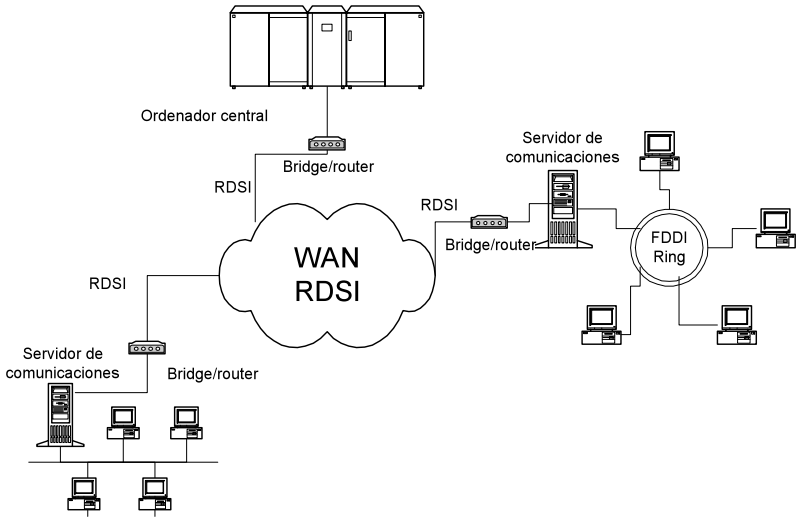


Fig. I.5: *Red de interconexión de LAN's a un ordenador central remoto mediante la Red Digital de Servicios Integrados (RDSI).*

- **Redes de conmutación rápida de paquetes**, o retransmisión de tramas, como **Frame Relay**. Las velocidades típicas llegan hasta los 2 Mbps.

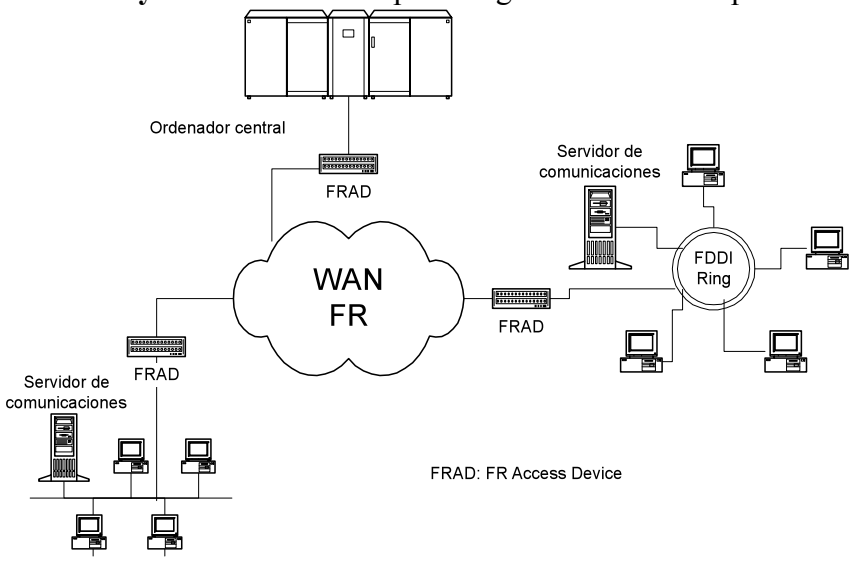


Fig. I.6: *Red de interconexión de LAN's a un ordenador central remoto mediante la Red Frame Relay(propia o de telefónica).*

- **Redes de transmisión de células**, mediante el **Modo de Transferencia Asíncrono** (**ATM**), como base de las Redes Digitales de Servicios Integrados de Banda Ancha (**RDSI-BA**). Aunque todavía en pleno desarrollo las velocidades máximas van desde los 115 Mbps hasta los 655 Mbps, e incluso se habla del orden de Gbps.

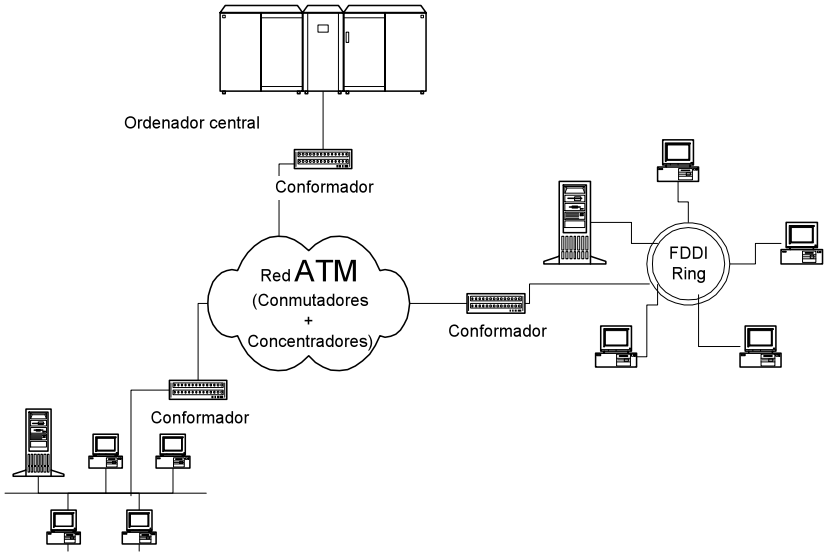


Fig. I.7: *Red de interconexión de LAN's a un ordenador central remoto mediante la Red Frame Relay(propia o de telefónica).*

1.2 REDES LAN

Una Red de Área Local puede definirse como un sistema de comunicaciones que proporciona interconexión a una variedad de dispositivos en un área restringida y que no utiliza medios de telecomunicación externos.

A destacar cuatro elementos fundamentales:

- **Sistemas de comunicaciones**, es decir, el conjunto de elementos cuyo objetivo es el intercambio de información entre dispositivos.
- **Dispositivos**, es decir, cualquier nodo de la red, desde un gran ordenador hasta un PC, pasando por clúster de terminales, impresoras, etc.
- El **ámbito geográfico** de la red, que generalmente se restringe a un único edificio o a un conjunto de ellos.
- La **propiedad** de los medios de comunicación es privada, lo que permite una gran flexibilidad a la hora de compartir el medio y definir los métodos de comunicación.

Las velocidades de transmisión son elevadas, cubriendo rangos muy amplios incluso en un mismo tipo de filosofía tecnológica. Así por ejemplo, la filosofía **Ethernet** va desde 10 Mbps de la Ethernet tradicional, los 100 Mbps de la **Fast-Ethernet**, hasta 1 Gbps de la **Giga-Ethernet**.

Una de las principales características de una LAN son su alto grado de **conectividad**, la cual permite la comunicación *peer-to-peer* independientemente del tipo de los equipos conectados, e **interconexión**, posibilitando la conexión con otras redes de incluso distinta arquitectura y tecnología mediante elementos pasarela (**gateways**).

2. TOPOLOGÍA DE REDES

La topología de una red de área local define la situación de cada equipo con relación al resto de equipos y de la propia red, condicionando fuertemente las prestaciones de la misma.

Los criterios a considerar en la elección de su topología difieren de los aplicables a las redes WAN. Así, la topología de una red LAN dependerá de:

- La **complejidad** de la instalación y el **mantenimiento** del cableado.
- La **vulnerabilidad** a fallos o averías.
- La **gestión** del medio y la localización de averías.
- La capacidad de **expansión** y **reconfiguración**.
- El **coste**.

2.1 TOPOLOGÍA EN ESTRELLA

En la topología en estrella todas las estaciones están conectadas mediante enlaces bidireccionales a un nodo central, que asume las funciones de gestión y control de las comunicaciones, proporcionando un camino entre dos dispositivos que deseen comunicarse.

Sus ventajas son:

- El acceso está en todo momento bajo el control de la central.
- La configuración de la red y la localización de fallos son fáciles, ya que pueden estar gestionadas por el nodo central.

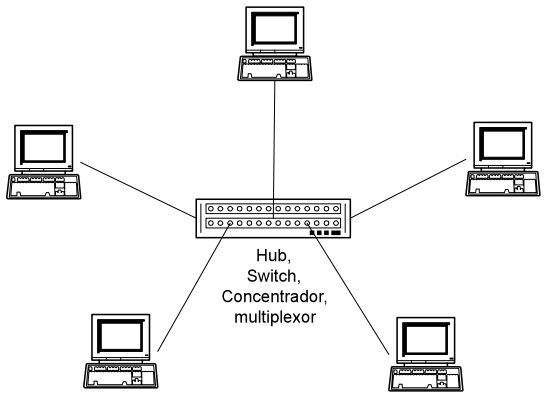


Fig. I.8: *Configuración en estrella a través de un elemento intermedio.*

Por otra parte sus inconvenientes son:

- En caso de fallo del nodo central se produce el bloqueo de toda la red.
- La longitud de cableado es elevada.

Ejemplos de esta topología se encuentran constantemente en la RTC, mientras que en las LAN no suele darse con mucha frecuencia, dado que precisamente se aleja de la filosofía

de distribución de inteligencia.

2.2 TOPOLOGÍA BUS

En la topología Bus todas las estaciones se conectan a un único medio bidireccional o bus con puntos de terminación bien definidos. Cuando una estación transmite, su señal se transmite a ambos lados del emisor hacia todas las estaciones que se encuentren conectadas al bus, por lo que también reciben el nombre de "canal de difusión".

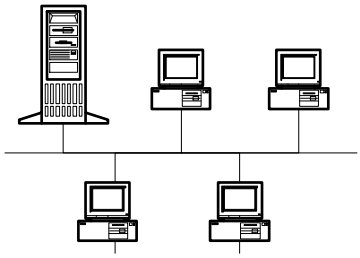


Fig. I.8: *Configuración en bus (Ethernet de cable fino o grueso).*

Sus ventajas son:

- Están constituidas fundamentalmente por elementos pasivos, solo encontrándose elementos activos en las estaciones.
- Por tanto una avería solo afectaría a la estación implicada.
- Presentan una alta modularidad, por lo que es facilísimo añadir o retirar estaciones de la red.
- Su adaptación a la distribución geográfica se realiza con un coste reducido.

Como desventaja destacar el que una avería en el bus provoca en el mejor de los casos la incomunicación entre los segmentos de red que se generan.

Un ejemplo de topología bus es la utilizada por las redes Ethernet, especialmente sobre cable coaxial. En el caso de las redes Ethernet sobre par trenzado se da un caso curioso: pese a ser una red de acceso sobre bus común, su topología es en estrella, de tal forma que las estaciones se conectan a un elemento denominado HUB, que implementa electrónicamente el bus de coaxial anterior.

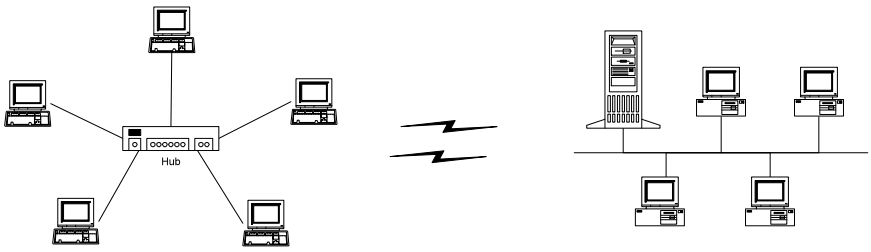


Fig. I.9: *Ethernet de par trenzado: el elemento intermedio (HUB) implementa electrónicamente el bus de las Ethernet de coaxial.*

2.3 TOPOLOGÍA DE ÁRBOL

La topología en árbol es una generalización de la topología en bus en la que el cable se desdobla en varios ramales mediante el empleo de dispositivos de derivación. Dependiendo del elemento utilizado podemos encontrarnos situaciones muy diferentes:

- Si utilizamos un Repetidor estaríamos realmente prolongando el bus, con lo que nos veríamos limitados por el número de estaciones conectadas (un máximo de 30 estaciones en segmentos de 185 metros en la red Ethernet), ya que todas accederían al bus.

- Si utilizamos un Bridge (puente) evitamos dicho problema, ya que este elemento solamente deja pasar aquella información del bus que realmente vaya dirigida a alguna estación del otro segmento (en el ejemplo, ahora con un bridge duplicaríamos el número máximo de estaciones a conectar).

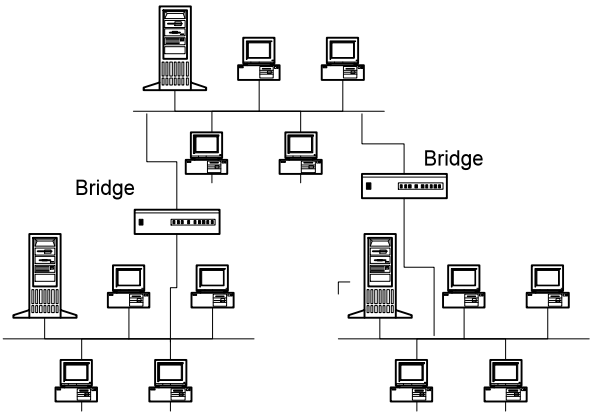


Fig. I.10: Árbol mediante Bridges: se establecen tres dominios diferentes (cada LAN por separado).

Ejemplos de esta topología podemos verlos en edificios cableados conectando las distintas plantas, e incluso en las instalaciones de antenas colectivas.

2.4 TOPOLOGÍA EN ANILLO

El anillo consiste en una serie de repetidores conectados entre sí mediante un único enlace de transmisión unidireccional formando un camino cerrado.

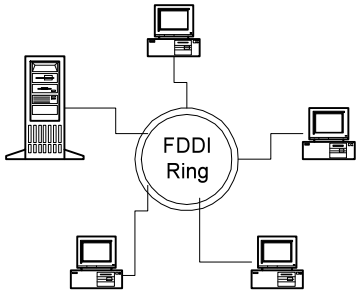


Fig. I.11: Anillo: cada equipo lleva una tarjeta repetidora.

La información se transfiere secuencialmente de un repetidor al siguiente a lo largo del anillo. Cada repetidor regenera y retransmite cada bit. Cuando una estación recibe información destinada a ella la recibe y procesa, en caso contrario se encargará de hacerla pasar hacia la próxima estación.

Los repetidores constituyen un elemento activo, pudiendo estar integrados en las propias estaciones, y realizan la recepción, autenticación y emisión de la información, así como el acceso a la red.

Sus ventajas son:

- El tiempo de respuesta está controlado.
- Facilita la gestión de averías.

En cuanto a las desventajas:

- Al estar todas las estaciones involucradas en la transferencia de datos, el fallo de un repetidor inutiliza por completo la red.
- Requiere de mecanismos de control sofisticados para detectar informaciones corruptas y evitar un ciclo sin-fin de retransmisiones (en

algunos casos de hace uso de una estación monitora).

Ejemplo de esta topología son las Redes Token Ring por paso de Testigo. Una variante consiste en duplicar los repetidores de cada estación, con lo que se establecen dos anillos (uno para cada sentido), uno de los cuales hace de respaldo en caso de fallo del otro. La tecnología por fibra óptica FDDI sigue esta misma filosofía.

2.5 TOPOLOGÍAS MIXTAS

Aquí se incluyen topologías en las que se hace una mezcla de las topologías anteriores. Caben destacar las configuraciones en estrella-estrella y anillo-estrella.

La topología estrella-estrella es básicamente una topología bus mediante el uso de equipos concentradores (HUBS). La estructura lógica es idéntica al bus, ya que todos los equipos acceden al mismo cable pero a través de los concentradores. Con esta topología se puede reducir el riesgo de bloquear toda la red por fallo o avería de un segmento de la misma.

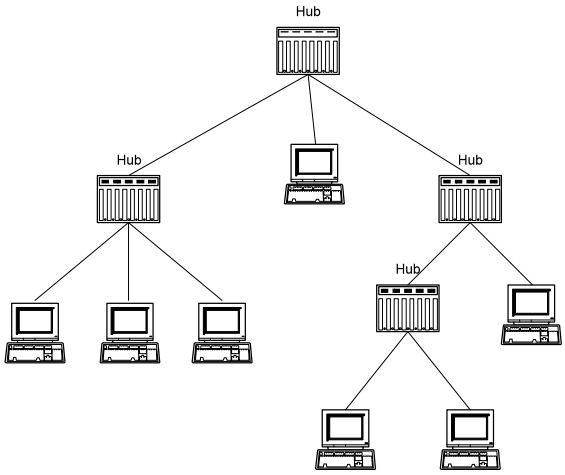


Fig. I.12: *Topología estrella-estrella*.

Por su parte, la topología anillo-estrella es la alternativa a la configuración en anillo. De la misma forma que mediante los HUB, ahora se hace uso de una unidad de acceso, denominada MAU, que si bien permite configurar físicamente una estrella, desde el punto de vista lógico, sigue siendo un anillo.

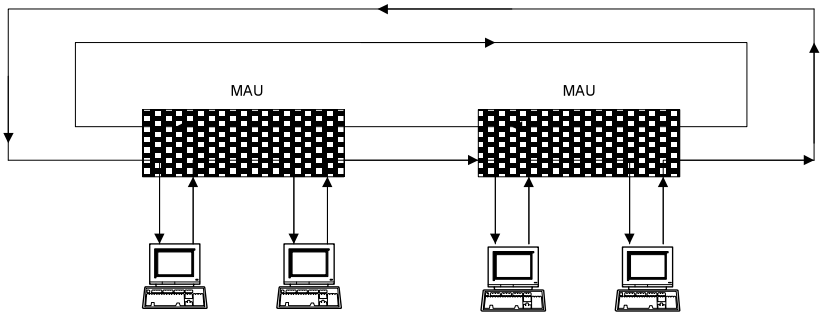


Fig. I.13: *Topología anillo-estrella.*

En caso de que se averíe una estación o un segmento de cable, la unidad de acceso puede cortocircuitar automáticamente esa estación o segmento de cable, de tal manera que el resto del anillo lógico puede permanecer activo. Si la avería se produce en un equipo, la MAU cortocircuita dicho equipo, mientras que si la avería se produce en la conexión entre MAU's, el anillo se reconfigura, restableciendo el anillo.

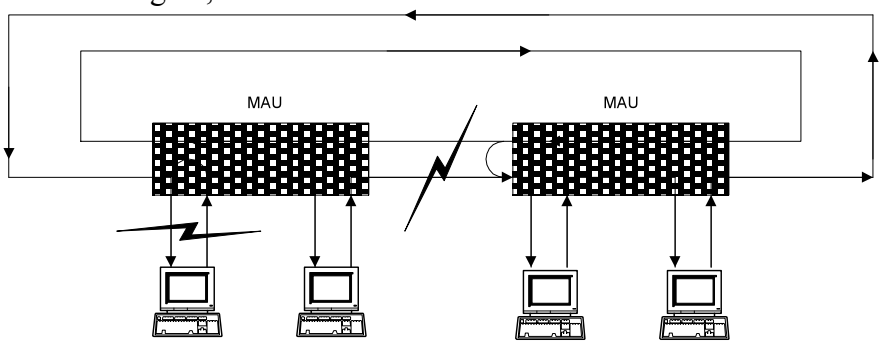


Fig. I.14: *Reconfiguración del anillo.*

3. MEDIOS DE TRANSMISIÓN

El elemento clave a la hora de interconectar equipos, y en definitiva de diseñar e implementar una red no es otro sino el **medio físico** que es el que transporta la información y establece el nexo de unión entre los distintos equipos y sistemas conectados a la red. La razón por la cual resulta fundamental no reside solamente en la necesidad de establecer el nexo físico, sino a que dependiendo de cómo deseemos establecer el mismo, el medio físico se erigirá en limitador ya sea por distancias, velocidades de transferencia, topología e incluso métodos de acceso. Los principales medios de transmisión utilizados tanto en las redes LAN como en las WAN son los cables de cobre y la fibra óptica, y además, por supuesto, el medio natural de transmisión, el aire.

La selección del tipo de medio a utilizar va a venir determinada por el análisis de un conjunto de parámetros fundamentales:

- **Ancho de Banda**: "*Espectro de frecuencias que el medio puede transmitir*". Está directamente relacionado con la velocidad de transmisión: *a mayor ancho de banda, mayor velocidad de transmisión*. Sin embargo, los parámetros limitativos los constituyen tanto las mismas características físicas del cable, como de su longitud. Por esta razón, muchas veces se tiene en cuenta la relación *distancia / velocidad*, y así por ejemplo, una conexión realizada vía una interfaz RS-232 tiene definida dentro de sus características una velocidad de 9600 bps para una distancia máxima de 25 m.

- La **longitud** del segmento de cable, limitada según el tipo de cable, la arquitectura o la topología de la red, especificándose para cada una las distancias máximas utilizables.

- La **fiabilidad** de la transferencia, normalmente medida según *tasas de error* (relación bits erróneos / bits totales) que determinan la calidad de la transmisión. Va a estar directamente relacionada con la *atenuación* del cable, así como por las *interferencias* externas.

- La **seguridad**, es decir, la posibilidad de que las señales transmitidas puedan ser interceptadas e incluso eliminadas.

- La "**instalabilidad**", es decir, lo fácil que resulte realizar una instalación basada en ese tipo de medio, directamente relacionada con las características mecánicas del cable: ligereza, flexibilidad, dimensiones, etc.

- El **coste**, determinante a la hora de seleccionar el tipo de medio a utilizar, y que no tiene por que venir impuesto exclusivamente por la instalación del mismo, sino también por todos los elementos asociados a dicha configuración.

3.1 CABLE COAXIAL

El cable coaxial consta fundamentalmente de **un par de conductores de cobre o aluminio**. Uno de ellos está dispuesto como **núcleo central** recubierto por material aislante y dieléctrico de *teflón o plástico*, sobre el que se dispone el segundo conductor en forma de malla de *hilos trenzados* o *lámina metálica cilíndrica*. Todo el cable suele estar cubierto por *aislamientos de protección*, para reducir tanto las interferencias externas, como las emisiones procedentes del interior. Su ancho de banda suele ser mayor que el del cable de pares, siendo utilizado tanto para transmisión de datos, como para voz, audio y vídeo.

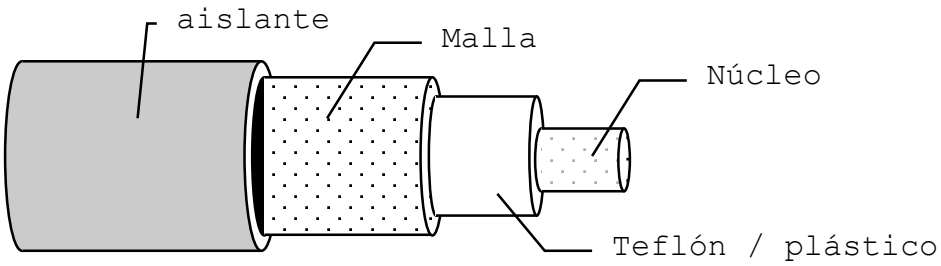


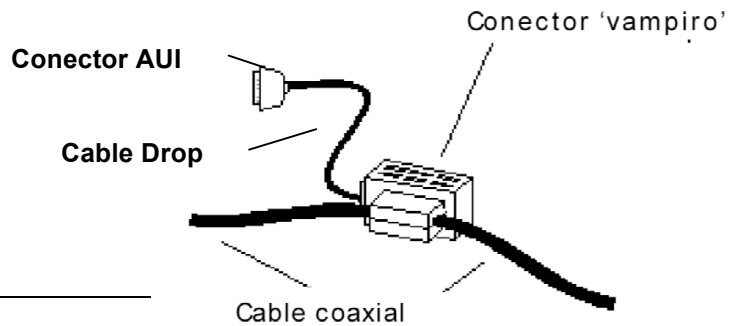
Fig. I.15.: *Cable coaxial*.

En el caso concreto de las LAN se emplea tanto en la transmisión *banda base* como en la transmisión *banda ancha*, y ha sido desde su introducción, la base de la red *Ethernet*. En la actualidad, a pesar de que ha sido prácticamente eliminada de casi todos los diseños de red *Ethernet*, ha vuelto a resurgir con fuerza gracias a las nuevas tecnologías de redes de acceso para *servicios multimedia de alta velocidad*, en las que se vienen denominando redes híbridas **HFC** (*Hybrid Fibber Coax*).

Podemos encontrar los siguientes tipos de cable coaxial:

- **Cable Coaxial Grueso** (*THICK*): Como su propio nombre indica el diámetro de este tipo de cable es el mayor de los de su gama. Presenta *una impedancia característica* de **50 Ohms**, y utiliza *conectores* de tipo "**N**". La especificación de la red *Ethernet* le asigna la denominación **10BASE5** (*10 Mbps, Transmisión Banda Base, 500 m*), lo cual significa que permite una velocidad de operación de **10** MBps, haciendo uso de un modo de transmisión en *Banda Base* con distancias de hasta **500** m por segmento de cable. Además, la especificación *Ethernet* indica que la dimensión máxima de una red *Ethernet* no debe superar los **2500** m, lo cual se consigue mediante la interconexión de varios segmentos a través de repetidores (5 segmentos como máximo)

Impedancia 50 Ohm
Conector "N", transceivers (vampire)
Velocidad de Transmisión max. 10 Mbps.
Transmisión en Banda Base
Distancia max. por segmento 500 m.
Distancia mín. Entre equipos 2.5 m
30 equipos / 185 m.



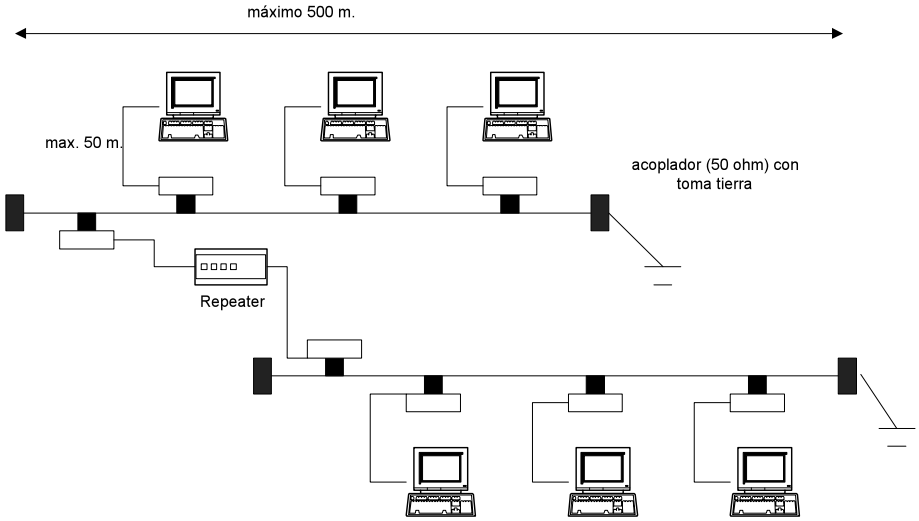


Fig. I.16.: *Red de cable grueso 10BASE5*.

Para la conexión de los equipos al conector, se hace uso de cables **AUI** ó **DROP** de *15 hilos*, permitiendo distancias máximas de **50 m**.

- **Cable Coaxial Fino** (*THIN*): Recibe la denominación **10BASE2**, o **RG58**. Físicamente es un cable de menor diámetro y por tanto más flexible, siendo actualmente el tipo de cable más utilizado en las *Ethernet en topología bus*.

Impedancia 50 Ohm
Conector "BNC"
Velocidad de Transmisión max. 10 Mbps.
Transmisión en Banda Base
Distancia max. por segmento 200 m (185 m).

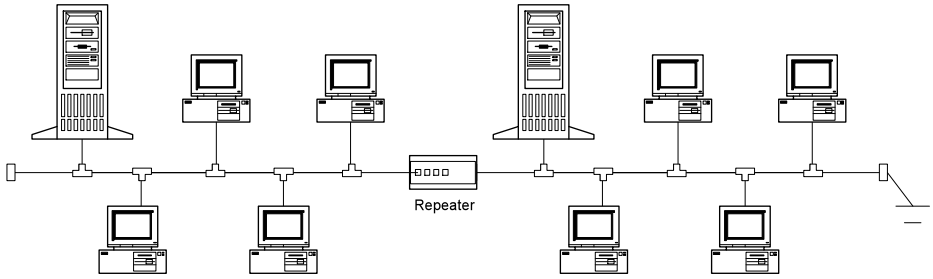


Fig. I.17.: *Red de cable fino 10BASE2*.

- **Cable coaxial de Banda Ancha**: Recibe la denominación 1**0BROAD36**. Es un cable utilizado en aplicaciones muy concretas. Una de las últimas tecnologías desarrolladas es la denominada **HFC**, híbridas Fibra-Coaxial. El coaxial en estos casos puede llegar a soportar velocidades muy superiores a los **10 Mbps**. Sin

embargo, de momento, las especificaciones de este tipo de coaxial serían:

Impedancia 75 Ohm
Velocidad de Transmisión ¿max?. 10 Mbps.
Transmisión en Banda Ancha
Distancia max. por segmento 3600 m.
Distancia real de cobertura 1800 m.

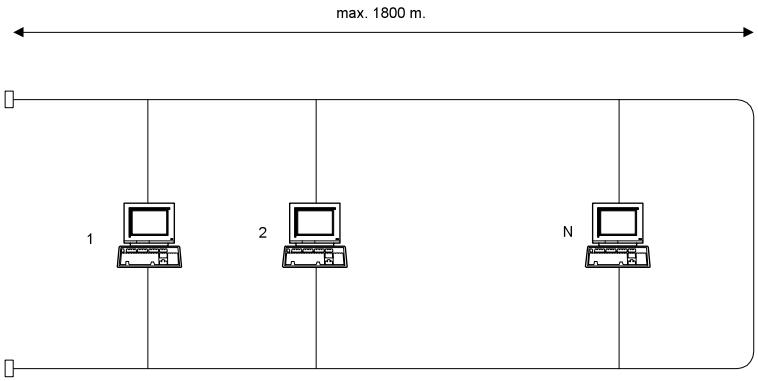


Fig. I.18.: *Red de cable de banda ancha*.

Como tipo especial de cable coaxial existe el denominado **twin-axial**. Sus características son similares a las de los coaxiales normales, salvo por la diferencia que ahora no lleva un conductor, sino *dos núcleos*. Por ello suele ser utilizado en situaciones en las que el nodo requiera de canales independientes para transmisión y recepción, o bien para asegurar líneas de respaldo. Ejemplos de sistemas que hacen uso de este tipo de cable son casi todos los terminales **AS/400**.

3.2 CABLE DE PAR TRENZADO

Este tipo de cable es el más utilizado actualmente en entornos de LAN Ethernet, es la base del "**cableado estructurado**", y hemos de tener en cuenta que toda la red telefónica, analógica y digital utiliza cables de este tipo. Las razones de su amplia utilización vienen dadas por su bajo coste y su sencillez de instalación. Básicamente el par trenzado consiste en agrupar una serie de conductores trenzándolos en forma de *hélice*. Físicamente este trenzado helicoidal reduce la influencia de las interferencias, no solo externas, sino también las que pueden introducir el resto de pares incluidos (Ej. *diafonía*).

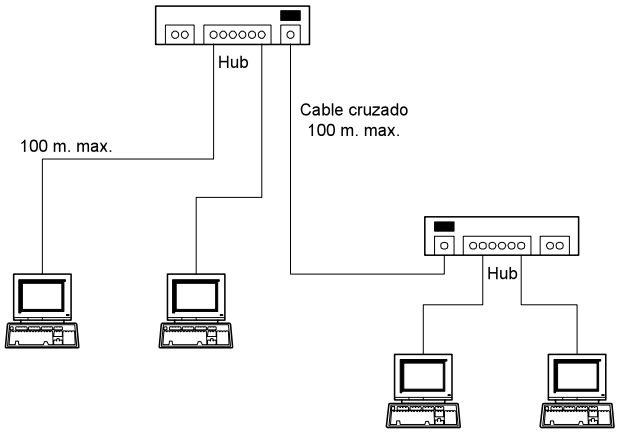


Fig. I.19.: *Red de par trenzado*.

Adicionalmente los pares trenzados pueden estar además protegidos contra las interferencias externas, mediante el uso de "**apantallamiento**", que no es sino añadir una cubierta conductora exterior a los pares, que absorbe la influencia electromagnética tanto externa, como interna. Dependiendo se si se utiliza *apantallamiento* o no, encontramos dos tipos fundamentales de cables de par trenzado:

STP (*Shielded Twisted Pair*): Par trenzado *apantallado*. Presenta una muy baja sensibilidad a las interferencias y reducida atenuación, por lo que resulta la opción más adecuada en entornos de larga distancia, altas velocidades de transmisión o fuertes interferencias electromagnéticas.

Impedancia 120-150 Ohm
Conector RJ11
Velocidad máxima de transmisión 150 Mbps (100 m)
Atenuación 30 dB / 300 m a 10 MHz.
2 pares trenzados por cable.

UTP (*Unshielded Twisted Pair*): Es el cable más utilizado dado su bajo coste y fácil instalación. Sus características son muy similares a las del **STP**, salvo que son más vulnerables ante las interferencias. También recibe la denominación **10BASET**.

Impedancia 100 Ohm
Conector RJ45
Vel. Max. transmisión 150 Mbps (100 m)
Atenuación 30 dB / 300 m a 10 MHz.
4 pares trenzados por cable.

A su vez el cable **UTP** puede ser dividido en diversas categorías, desde la **categoría 2**, **hasta la 5**, estando completamente normalizadas por la **EIA** (*Electronics Industries*

Association) desde 1991:

- **Categoría 2**: son los más sencillos, siendo utilizados para transmisión de datos a bajas velocidades (menor de **4 Mbps**), y concretamente, para telefonía.

- **Categoría 3**: fueron los primeros en utilizarse en las Ethernet a 10 Mbps, pero en distancias inferiores a 100 m y segmentos de 500 m. Han sido también utilizados en token ring por paso de testigo a 4 Mbps y 16 Mbps, e incluso en redes de alta velocidad a 100 Mbps (se requieren normalmente 4 pares).

- **Categoría 4**: son los menos utilizados.

- **Categoría 5**: son los que se están imponiendo actualmente, dado al abaratamiento de los costes, y a que pueden ser utilizados a 100 y 150 Mbps con solamente 2 pares.

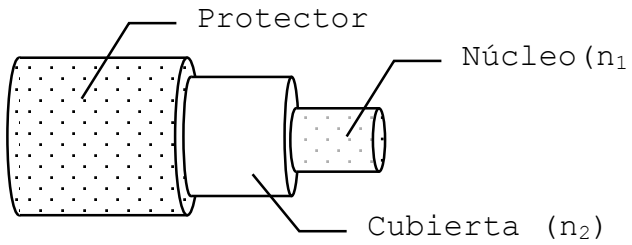
A continuación se muestra como ejemplo una tabla con las principales tecnologías de cable utilizadas en redes Ethernet, incluidas sus variantes de alta velocidad, FastEthernet y GigaEthernet:

Denominación	Cable	Pares	Full dúplex	Conectores	Distancia
10BASE5	Coaxial grueso	1	No	'N'	500 m
10BASE2	RG 58 (Coaxial fino)	1	No	BNC	185 m
10BASE-T	UTP cat. 3	2	Sí	RJ-45	100 m
10BASE-T	UTP cat. 5	2	Sí	RJ-45	150 m*
100BASE-TX	UTP cat. 5	2	Sí	RJ-45	100 m
100BASE-TX	STP	2	Sí	9 pin D sub.	100 m
100BASE-T4	UTP cat. 3	4	No	RJ-45	100 m
100BASE-T2	UTP cat. 3	2	Sí	RJ-45	100 m
1000BASE-CX	STP	2	Sí	8 pin HSSDC o 9 pin D sub.	25 m
1000BASE-T	UTP cat. 5	4	Sí	RJ-45	100 m

*La longitud máxima del cable UTP-5 según las normativas de cableado estructurado es 100 m, pero la norma 802.3 permite un alcance de 150 m cuando se utiliza 10BASE-T con cable categoría 5.

3.3 CABLE DE FIBRA ÓPTICA

Constituye el medio de transmisión más reciente y con mayor proyección hacia las redes de alta velocidad. Básicamente, una fibra óptica está constituida por un **núcleo** circular muy fino de **fibra de vidrio** (*silicio*) transparente, que suele estar rodeado por otro revestimiento de otro tipo de vidrio con diferente **índice de refracción**, y todo ello, envuelto



con una cubierta opaca.

Fig. I.20.: Fibra óptica.

Los tres componentes principales de un sistema de transmisión por fibra óptica podrían ser:

- **Transmisor**: transforma la *señal eléctrica (electrones*) en una *señal óptica (fotones*), que es modulada a la frecuencia adecuada y transmitida a través de la fibra óptica. La fuente de fotones suele ser un elemento *semiconductor*, denominado **LED**, o un sistema **LASER**, dependiendo de la potencia y frecuencias de emisión requeridas.

- La **fibra óptica**: se conecta al emisor de fotones por un extremo, y al detector por el extremo contrario. La *homogeneidad* de la línea depende en gran medida del número y la calidad de las conexiones. Estas deben ser realizadas con una relativa gran precisión.

- **Receptor**: Normalmente suele ser un *fotodiodo*, con tecnología similar a la del emisor. Realiza la posterior conversión de energía óptica a señal eléctrica. Normalmente suele estar asociado a **sistemas de amplificación**.

El principio de funcionamiento se basa en las *leyes de la óptica*, en los efectos de la **reflexión** y **refracción** de la luz al pasar de medios de transmisión con *diferentes índices de refracción*. El rayo luminoso entra a la fibra con un determinado ángulo. En un punto dado alcanza la frontera entre ambas cubiertas de Silicio, y al existir distintos índices, se produce la reflexión (*Ley de Snell*). De esta forma, el rayo atraviesa toda la extensión de la fibra, sin sufrir prácticamente atenuaciones. Para que el rayo no sea refractado a través del silicio

exterior, el índice de refracción del núcleo debe ser **mayor** que el del revestimiento. Así por ejemplo, valores típicos de índice de refracción pueden ser 1.5 para el núcleo y 1.48 para el revestimiento (el índice de refracción del aire es 1).

La luz, puede recorrer diferentes caminos dependiendo del ángulo de incidencia del rayo, lo cual permite la adición de varios rayos con diferentes fases, posibilitando la transmisión múltiple, siendo denominadas **fibras multimodo**. Las velocidades permitidas por este tipo de fibras dependen de cómo se distribuye el índice de refracción del núcleo: para **fibras con índice escalonado** (el núcleo presenta un índice de valor constante) las velocidades van desde *los 10 Mbps / 3 Km*, hasta los *100 Mbps / 300 m* (El producto *Vel_Mbps * Distancia_Km* no puede ser mayor de **30**). Por su parte, para las **fibras multimodo de índice gradual** (el índice del núcleo aumenta gradualmente desde el valor del de la cubierta, para alcanzar un valor máximo en el eje) alcanzan hasta *100 Mbps / 4 Km (Vel_Mbps * Distancia_Km ≅ 400*).

Sin embargo, hay situaciones en las que se desea que la atenuación sea mínima y la velocidad máxima, por lo que deben mejorarse los ángulos de incidencia de los rayos. Para ello, es necesario utilizar **fuentes de luz coherente**, y reducir los diámetros de la fibra hasta dimensiones cercanas a las *10 micras*. Son las llamadas **fibras monomodo**, que permiten velocidades del orden de *10 Gbps / 1 Km.*

Entre sus ventajas cabe destacar su alto ancho de banda, su pequeño tamaño y ligereza, su baja atenuación y su total aislamiento electromagnético. Sin embargo, hemos de tener en cuenta que sigue siendo una tecnología cara, especialmente a la hora de realizar las conexiones, y sobre todo, en los elementos de emisión y detección.

A continuación se presentan lo medios basados en fibra óptica utilizados actualmente en redes de la familia Ethernet:

Medio	Ventana	Luz	Fibra	Conector	Distancia
10BASE-FL	1ª	Normal	62,5/125	ST	2 Km
100BASE-FX	2ª	Normal	62,5/125	SC	2 Km
100BASE-SX (propuesto)	1ª	Láser	62,5/125 50/125	SC o ST	500 m 500 m
1000BASE-SX	1ª	Láser	62,5/125 50/125	SC	275 m 550 m
1000BASE-LX	2ª	Láser	62,5/125 50/125 9/125	SC	550 m 550 m 5 Km

3.4 WIRELESS

Aunque no es una tecnología demasiado extendida en el ámbito de las redes locales, la amplia difusión, y sobre todo el rápido desarrollo de los equipos *inalámbricos*, hace que este tipo de sistemas tenga una altísima proyección de futuro. Su principal aplicación ya no solo estaría restringida a aquellas zonas donde el tendido de cables resulta prácticamente imposible, sino que abarcaría una de las áreas más en boga de los últimos tiempos: el **teletrabajo**.

Básicamente, una red inalámbrica tiene su base en la utilización de **canales de radio**, principalmente en las bandas de **UHF** (*Ultra High Frequency*, de 300 MHz a 3 GHz), **microondas** (banda *SHD*, *Supe High Frequency*, de 3 GHz a 30 GHz) o **infrarrojos**.

La mayoría de las redes de este tipo trabajan sobre **UHF** de *902 a 928 MHz*, idéntica banda a la utilizada por los *teléfonos móviles e inalámbricos*. Operan con una cobertura de unos pocos cientos de metros y velocidades hasta 2 Mbps, siendo sus limitaciones consecuencia de la necesidad de un gran ancho de banda, y por la utilización de un código especial, denominado de **expansión**, que solamente es conocido por cada receptor.

Las redes que operan en *microondas* utilizan normalmente la Banda de 18 GHz, alcanzando velocidades de 10 a 15 Mbps y distancias del orden de 100 m.

Por su parte, las redes de *infrarrojos* imponen la necesidad de que emisor y receptor sean visibles el uno del otro, por lo que su cobertura se restringe a unas decenas de metros (velocidades de 4 a 10 Mbps).

3.5 APLICACIONES

A la hora de establecer el diseño de una red, una de las decisiones más importantes es la de seleccionar el medio físico, y en concreto el tipo de cable a utilizar (muchas veces impuesto por la tecnología e incluso por las distancias entre equipos).

Como hemos visto, el *cable coaxial* es el medio más utilizado tradicionalmente, sin embargo aunque está desplazado en la actualidad por el *par trenzado* (*UTP*) y la *fibra óptica*, no dejan de aparecer movimientos que defiendan su utilización (*redes HFC*).

Por su parte, el *par trenzado* es el más utilizado actualmente dado su bajo coste y su facilidad de manejo e instalación. Su eficacia está comprobada hasta velocidades de 150 Mbps (100 m), pero sin embargo, hay que tener muy en cuenta sus limitaciones en cuanto a distancia, sobre todo dependiendo de la topología utilizada.

	UTP / STP	Coaxial	F.O.
Ancho de Banda	Moderado	Grande	Muy grande
Longitud	Baja	Alta	Muy alta
Fiabilidad	Moderada	Alta	Muy alta
Seguridad	Baja	Moderada	Alta
Instalación	Sencilla	Moderada	Compleja
Coste	Bajo	Moderado	Alto

Tabla I.- *Comparativa de los tres tipos básicos de cables.*

	UTP categoría 5	STP categoría 5	Fibra
Costo material	118 Pts/m	226 Pts/m	251 Pts/m
Mano de obra	94 Pts/m	104 Pts/m	105 Pts/m
Total cableado	212 Pts/m	330 Pts/m	356 Pts/m
Interfaz (1)	102000 Pts	102000 Pts	134000 Pts multimodo 561000 Pts monomodo

(1)Representa el costo típico de una interfaz de ese tipo en un conmutador ATM.

Tabla II.- *Estimación de costes para los distintos medios estudiados.*

Por último, la *fibra óptica* es el que mayor penetración está teniendo en el mercado. La evolución y el rápido desarrollo de los dispositivos ópticos, así como las características mecánicas del medio lo hacen ideal para la transmisión e *interconexión* entre edificios, como red de *extensión de cobertura* e incluso como *red dorsal*. Su único límite actualmente reside en lo limitado de su aplicación en puestos individuales de trabajo.

4. NORMALIZACIÓN

Las comunicaciones entre equipos informáticos es un campo tan complejo que parece obvio el que se estén realizando constantemente arduos esfuerzos para la racionalización de las mismas. Para ello, en la informática, como en el resto de las ciencias y tecnologías se procede al establecimiento de **normalizaciones**, es decir, el consenso de todos o la mayoría de los participantes implicados en una determinada área sobre las especificaciones y criterios a aplicar de manera consistente en la elección y clasificación de los dispositivos, procesos y servicios.

La **normalización** permite el que diferentes fabricantes puedan producir equipos y sistemas compatibles y complementarios entre sí. Este hecho se traduce directamente cara al usuario, puesto que dicha liberalización obliga a los fabricantes a mejorar la calidad y los precios de sus productos para así asegurar una cuota de mercado razonable.

Las ventajas que introduce una determinada normalización podrían ser:

- Mejor relación **calidad precio**.
- **Compatibilidad** e **interoperabilidad** entre equipos y servicios.
- Simplificación del **uso**.
- Reducción del número de **modelos**.
- Reducción de los **costes**.
- Facilidad de **mantenimiento**.

Por su parte, podemos también encontrar ciertas desventajas, entre las que cabe destacar su tendencia a ralentizar el avance de las tecnologías, puesto que llegar a una determinada normalización puede suponer en la mayoría de los casos una actividad lenta y compleja, principalmente debido a la necesidad de contemplar cuatro etapas claramente diferenciadas:

* **Definición**
* **Desarrollo**
* **Revisión**

* **Promulgación**

Durante todo este proceso, las investigaciones avanzan, y posibilitan la aparición de nuevas técnicas que no son contempladas dentro de dicha normalización.

El resultado del proceso de normalización aparece reflejado en los denominados **Estándares**, que genéricamente podríamos definir como: "*acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para su utilización como normas, guías o definición de características con el objetivo de asegurar que los materiales, productos, procesos y servicios se ajusten a su propósito*".

Podemos encontrar diferentes tipos de estándares, que según su ámbito de aplicación pueden ser:

- **Estándares de organizaciones profesionales** representativas de la industria: *IEEE* (*Institute if Electrical and Electronics Engineers*)
- **Estándares de gobierno**: *MAP* (*Ministerio de Administración Publica*), *NIST* (*National Institute of Standards and Technology*)
- **Estándares de multifabricantes**: *ECMA* (*European Computer Manufacturing Association*)
- **Estándares nacionales**: *AENOR* (*Asociación Española de Normalización y Certificación*), *ANSI* (*American National Standard Institute*).
- **Estándares multinacionales**: *CEN* (*Comité Europeo de Normalización*).
- **Estándares internacionales**: *ISO* (*International Organization for Standarization*).

Cabe dar especial mención a las **Recomendaciones** de la **UIT-T**, como caso concreto de especificaciones de normalización en el área de las Telecomunicaciones.

Otra clasificación de los estándares habla de:

- **Estándares no vinculantes**: no existe obligación de adherirse a ellos.
- **Estándares obligatorios**.
- **Estándares de uso obligatorio sectorial**: obligatorios para ciertos sectores, y no vinculantes para el resto.

Además podemos también definir:

- **Estándares "de iure"** (*de derecho*): promulgados por asociaciones reconocidas oficialmente (como *ISO* o *AENOR*).

- **Estándares "de facto"** (*de hecho*): consecuencia de la aceptación generalizada por parte de los usuarios aunque haya sido definido por un único fabricante, o que hayan sido aceptados por un significativo número de fabricantes y grupos de usuarios (ejm. *TCP/IP*).

4.1. ORGANISMOS DE NORMALIZACIÓN

El **proceso de normalización** es llevado a cabo por organismos denominados "***entidades o grupos de normalización***". En la tabla se puede observar los principales **organismos** de **normalización**, de los cuales la mayoría no se dedica exclusivamente al área de las telecomunicaciones (solo la **UIT-T**, formada por los operadores de telecomunicaciones).

ANSI	*American National Standards Institute*
COSE	*Common Open Software Environment*
CCITT (UIT)	*Consultative Committee for International Telegraph and Telephone*
COS	*Corporation for Open Systems*
EIA	*Electronic Industries Association*
IEEE	*Institute of Electrical and Electronic Engineers*
ISO	*International Organization for Standardization*
OMG	*Object Management Group*
OSF	*Open Software Foundation*
SAG	*SQL Access Group*

La **Unión Internacional de Telecomunicaciones** es una organización mundial, dependiente de las **Naciones Unidas** en la cual tanto los gobiernos como el sector privado coordinan el establecimiento y operación de los *servicios* y *redes de telecomunicaciones*. Sus responsabilidades abarcan desde la **regularización** hasta la **harmonización** de las políticas

nacionales, pasando por la **normalización**, **coordinación** y **desarrollo** de las Telecomunicaciones internacionales.

Su principal objetivo es el de *facilitar el desarrollo de las telecomunicaciones para el beneficio universal de la humanidad mediante la definición de recomendaciones y la cooperación mutua*.

Sus orígenes se remontan a **1865**, como **Unión Internacional de Telégrafos**. Posteriormente, en **1924**, **1925** y **1927**, se fundaron respectivamente el **Comité Consultivo Internacional de Telefonía** (*CCIF*), el **Comité Consultivo Internacional de Telegrafía** (*CCIT*) y el **Comité Consultivo Internacional de Radio** (*CCIR*). En **1956**, el *CCIT* y el *CCIF* se unificaron en lo que se denominó **Comité Consultivo Internacional de Telefonía y Telegrafía** (*CCITT*), nombre que mantuvo hasta **1993**, año en el que desapareció para dar paso a la **UIT-T** y **UIT-R**.

La **UIT-T** se compone básicamente de **Grupos de Estudio**:

1. *Definición de servicios*
2. *Operación de red*
3. *Tarificación*
4. *Mantenimiento de red*
5. *Protección en entornos de interferencia electromagnética*
6. *Planta exterior*
7. *Redes de datos y comunicaciones de sistemas abiertos*
8. *Terminales para servicios telemáticos*
9. *Transmisión de audio y TV*
10. *Lenguajes para aplicaciones de telecomunicación.*
11. *Conmutación y señalización*
12. *Comportamiento de redes y terminales en transmisión extremo a extremo*
13. *Aspectos generales de red.*
14. *Modems y técnicas de transmisión para datos, telegrafía y servicios telemáticos.*
15. *Sistemas y equipos de transmisión*

Los **Grupos de Estudio** están formados por expertos y en los que participan las administraciones y entidades públicas y privadas del sector. Los **estándares**, denominados **Recomendaciones**, son adoptados formalmente en las **sesiones plenarias**, y publicados en un conjunto de libros conocidos por el color de sus cubiertas (*Blancos 1992 y 1993, Rojo Azules 1988, Rojos 1984, Amarillos 1980, Naranjas 1976*).

Por su parte, las recomendaciones del **UIT-T** son identificadas por una **letra**, que

indica el **tema** de la **serie de recomendaciones**, seguida por un número:

E *- Redes telefónicas y RDSI*
V *- Comunicación digital sobre red telefónica*
X *- Redes públicas de comunicación de datos*
I *- RDSI*
Q *- Operación y mantenimiento*

Dentro de la **UIT-T** se diferencian cinco clases de **miembros**:

* *Representantes de administraciones de telecomunicación nacionales.*
* *Agencias privadas de operadores reconocidas (ejm. AT&T).*
* *Organizaciones industriales y científicas (ejm. IBM y DEC).*
* *Otras organizaciones internacionales (ejm. ISO).*
* *Agencias especializadas en otros temas relacionados (ejm. OMS).*

Dentro del ámbito europeo, la organización más importante dentro de la UIT-T es el **Instituto Europeo de Normalización de Telecomunicaciones** (*ETSI European Telecommunication Standards Institute*), que surgió en **1988** al amparo del **Acta Única** de la **CE** con el principal objetivo de producir los estándares necesarios para lograr un mercado de telecomunicaciones europeo unificado. Sus miembros pueden ser:

* *Administraciones y organizaciones de normalización nacionales.*
* *Operadores de redes públicas.*
* *Usuarios.*
* *Fabricantes.*
* *Proveedores de servicios.*

Las normas producidas por los organismos dependientes del ETSI son voluntarias, sin embargo existen excepciones en las que se especifica la aplicación obligatoria de un estándar. En estos casos cada país miembro de la **Unión Europea** debe incorporar estos estándares a la **legislación nacional**. En el ámbito de las telecomunicaciones los principales estándares obligatorios cubren las siguientes áreas:

- **Public Procurement**: desde 1990 se exige a las organizaciones que deseen licitar contratos públicos hagan referencia a las Normas Europeas.

- **Open Network Provision**: la derregulación en el sector de las telecomunicaciones requiere la definición de interfaces abiertos para el acceso a la red, los cuales deben hacer referencia a las **Normas Europeas**.

5. MODELOS DE REFERENCIA: ARQUITECTURAS

Existen cuatro tendencias fundamentales presentes en el mundo del procesamiento y la comunicación de datos:

- La necesidad de **protocolos de comunicación** de datos que trasciendan los límites de los anteriores protocolos.
- La capacidad de **trasladar** inteligencia a dispositivos cada vez más **pequeños**.
- El desarrollo de las comunicaciones entre clases más **nuevas** de dispositivos.
- La necesidad de **interconectarse** con medios más nuevos de **transportadoras** comunes.

Una **arquitectura de comunicaciones** debe ser el vínculo de unión para todos los productos de comunicación de datos, tanto existentes, como futuros de un vendedor. La arquitectura logra esto especificando rigurosamente:

* Los conceptos y estructuras lógicas involucrados.
* Una serie de reglas y pautas referentes a la interconexión.
* Una serie de configuraciones de red posibles.

Estos tres aspectos de la arquitectura al combinarse de diferentes maneras especifican un producto en particular. De este modo, la arquitectura asegura que todos los productos de comunicación relacionados, trabajen juntos en una forma consistente y compatible. Los productos de la red que resultan, tanto aquellos proporcionados por el vendedor como aquellos desarrollados por el usuario, pueden evolucionar para aprovechar las nuevas técnicas y servicios con un mínimo impacto sobre el medio de operaciones.

Dentro de la aspiración total de cohesión del producto, hay una serie de objetivos claves que una arquitectura debe satisfacer:

- Hacer la red **transparente** para el usuario final y programador de aplicaciones.
- Mejorar la **manipulación** de los cambios en cualquiera de los elementos de la red.

- Permitir que sistemas centrales múltiples u otros dispositivos inteligentes sean **conectados** a la misma red.
- Habilitar terminales funcionalmente **diferentes**.
- **Independizar** las aplicaciones de los procesos de comunicación.
- Establecer y proteger el diálogo **extremo a extremo**.
- **Conectar** físicamente a los medios de transmisión.

Por su parte, el mecanismo de conexión entre extremos debe:

* *Maximizar la cantidad de datos que se transmiten.*
* " *la seguridad de los datos ante perturbaciones.*
* " *la disponibilidad de las rutas.*
* *Minimizar el tiempo de transmisión.*
* " *los costes.*
* " *la congestión de tráfico.*

Una arquitectura debe brindar una filosofía de **control de red** que integre completamente al control dentro de la red, de manera que una porción de red del sistema de comunicaciones no dependa de otros componentes para mantenerse en operación.

La arquitectura debe facilitar la distribución de la capacidad de procesamiento a través de todo el sistema de comunicación. Esto se logra por medio de una **división lógica** del sistema de comunicación en una serie de **funciones de red** y en una serie de dos o más **funciones de procesamiento** que se comunican a través de las funciones de red. Estas funciones de procesamiento se tratan de forma idéntica, independientemente de su diferencia de tamaño.

5.1 ESTRUCTURA FUNDAMENTAL

Toda arquitectura va a estar basada en una serie de **modelos de referencia**. Un modelo es una representación o simplificación que hace a un concepto más comprensible. Para comprender modelos de sistemas complejos, es importante dividir las estructuras en partes fácilmente comprensibles. Los sistemas de comunicación se consideran a menudo estratificados en **capas** de funciones.

El sistema se estructura en **capas** que sirven para proporcionar una ejecución apropiada de funciones que asegurarán:

- **Independencia** de actividades entre capas (un cambio en una capa solamente afectará a esa capa).

- El **ocultamiento** de una implementación específica de cada capa, según lo ven los usuarios de esa capa.

- La **utilización** de servicios comunes compartidos por diferentes aplicaciones.

- El **secuenciamiento** de los sucesos en el tiempo, de capa a capa.

La técnica estructural básica para construir la arquitectura del modelo de referencia, consiste en un conjunto jerárquico de capas. Se puede definir formalmente del modo siguiente:

1. *La **capa (n)** de la estructura hace uso de los **servicios** de tipo **(n-1)** proporcionados por las capas más bajas, a través del **acceso** de tipo **(n-1**).*

2. *La **capa (n)** se compone de **entidades** de tipo **(n)** que cooperan de acuerdo a un **protocolo** de tipo **(n**).*

3. *Las **entidades** de tipo **(n)** realizan **funciones** de tipo **(n)** que utilizan los **servicios** de tipo **(n-1)** para proporcionar **servicios** de tipo **(n)** a la **capa (n+1**).*

Gráficamente podemos representar estas tres definiciones fundamentales como se indica en la figura 21:

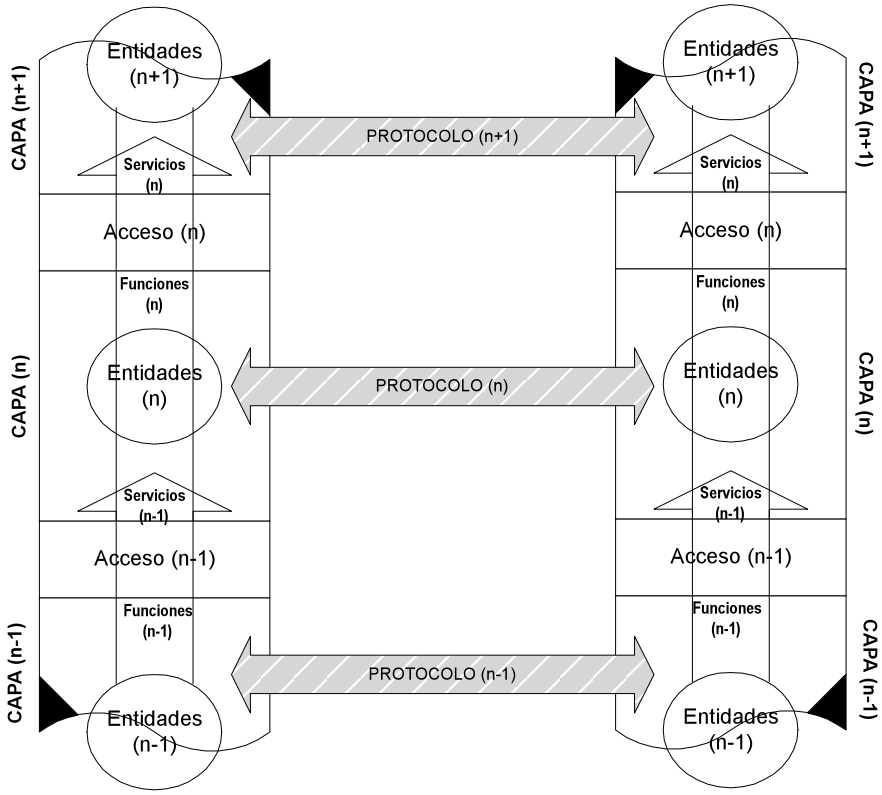


Fig. I.21*: Arquitectura = Estructuras estratificadas.*

La especificación de una capa de la arquitectura debe referirse en cierto modo a la serie de servicios proporcionados por las capas más bajas. Esto se hará mediante el uso **de funciones de acceso**. La serie de funciones de acceso a un servicio, debe ser considerada simplemente como un medio de describir la **estructura lógica** de la red. No implica, necesariamente, la existencia de la interconexión correspondiente en cualquier implementación de una parte de la red.

Una característica común a las arquitecturas, es la de una estructura en capas en cada nodo de la red. Aunque el número exacto de capas de funciones apropiadas todavía no está respaldado por la demostración rigurosa, ha surgido de la experiencia un cierto **consenso**. Las capas básicas de protocolo consisten de **transmisión**, **administración de servicios** y **funciones de aplicación**:

- **Funciones de transmisión**: La capa de transmisión se ocupa del **enrutamiento** y **movimiento** de datos entre el origen y el destino. Esta capa maneja el **camino** y las **conexiones** a **nivel de enlace**. El que los datos sean transportados a través de *cables*, *microondas*, o *satélites* es intranscendente,

mientras sean entregados sin alteración en el destino apropiado. Determinadas **técnicas de transmisión**, tales como la *conmutación de paquetes*, requieren algún formato específico de los datos (realizado por el correspondiente protocolo de transmisión). Esta capa debe incluir también el **control de errores** para asegurar que los datos se entreguen correctamente, y si no es así, para corregirlos o retransmitirlos. Por su parte, la función de enrutamiento recibe la petición de transporte de otras capas y hace el mejor uso posible de los servicios de transmisión disponibles.

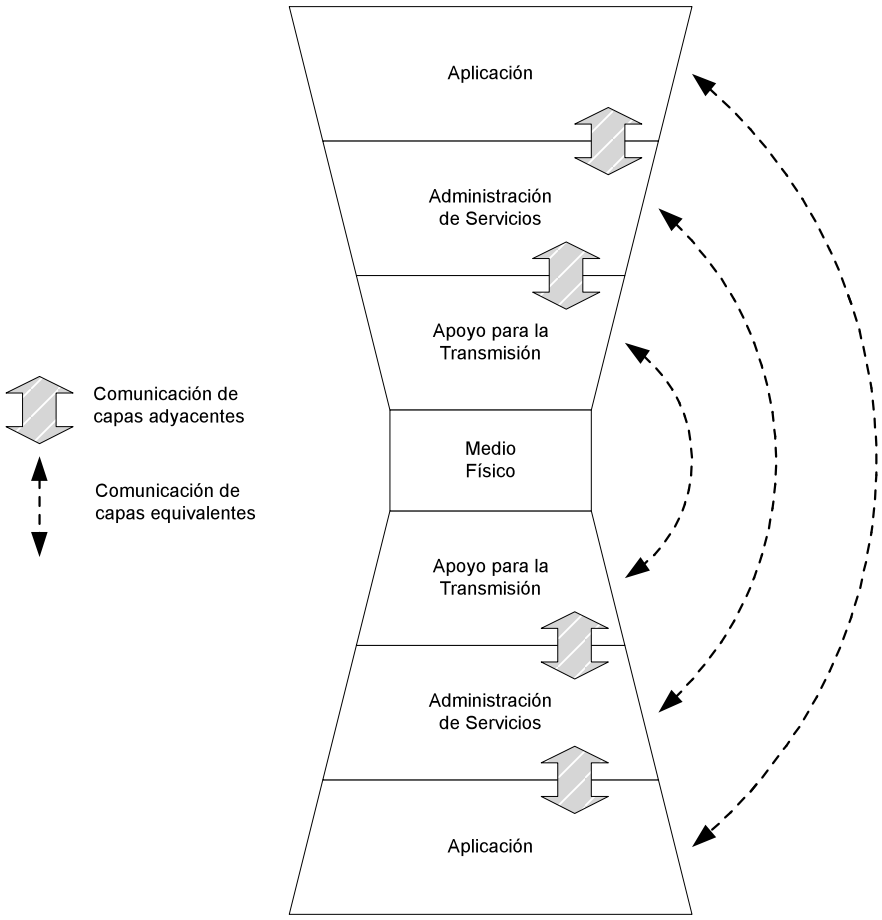


Fig. I.22: *Capas básicas o fundamentales de una arquitectura*.

- **Servicios**: la segunda capa o capa de "*administración de servicios*" proporciona transformaciones específicas según el dispositivo: de las características del emisor a las necesidades del receptor. Esta capa es clave para la confección de redes, ya que proporciona las *funciones de traducción*

entre las características de terminales físicas y programas de aplicación. La capa de administración de servicios tiene también otros dos papeles fundamentales: **control de la red** y **control de sesión**. El control de sesión vigila el estado de la sesión, coordinando la activación / desactivación de una sección y brindando apoyo para comenzar, borrar y resincronizar los flujos de datos relacionados con la sesión.

- **Aplicaciones**: La capa de aplicación se ocupa de las funciones del usuario final y puede ser un programa de aplicación o un dispositivo de E/S, tal como un terminal. Los servicios de la capa de administración de servicios se invocan por peticiones, desde la capa de aplicación. En el ordenador, la capa de aplicación consiste en programas de aplicación, de los cuales el usuario solicita información a través del procesamiento de los datos. En el terminal la capa de aplicación está representada por el operador del mismo, o un programa de aplicación en la unidad de control.

Otra característica común a las arquitecturas de redes de conmutadores es la de tener tres niveles de conexión dentro de la red. Ver figura 23.

Fig. I.23: *Niveles de Interconexión* **.**

- El **primero** o nivel más básico, es el del **enlace** entre dos nodos. Este enlace podría ser una única línea de comunicación que interconecta dos equipos, o una línea que une un dispositivo con varios, administrada por un *procesador de comunicaciones*, un *concentrador remoto* o un *controlador inteligente*. En cualquier caso es la interconexión eléctrica entre dos o más entidades físicas de la red. La conexión en este nivel de enlace se implementa usualmente por medio de uno de los controles de enlace de datos de alto nivel tal como el *HDLC*, funciones que se encuentran en la *capa de transmisión*.

- El **segundo** nivel de conexión dentro de la red es el que se encuentra entre el nodo de origen y el nodo de destino, y se le llama **canal extremo a extremo**. Esta es una *conexión lógica* o grupo de reglas de enrutamiento para el traslado de datos desde el nodo de entrada hasta el nodo de destino. La vía física puede ser constante durante la comunicación o puede variar dinámicamente, dependiendo de la arquitectura. Como referencia, en el *estándar X.25*, el procedimiento para interconectar redes públicas de paquetes, se aplica al nivel de caminos de conexión de la red.

- El **tercer** nivel de conexión es el que existe entre **usuarios finales**. Estos no siempre son personas.

Generalmente se considera que el usuario final está **fuera de la arquitectura de la red**. Así, la red no pone restricciones a las funciones dentro del usuario ni al formato de la interconexión con el usuario final. Por lo tanto, el concepto clave debe ser una definición estructurada sólo de los protocolos y formatos para flujos de mensajes en conexiones lógicas. El usuario final y su interconexión no están estructurados y son dependientes del producto.

6. EL MODELO ISA OSI

El modelo de referencia **ISA** se establece en el documento **CCITT X.200** y en el **ISO 7498** como un marco de trabajo para el desarrollo de los protocolos y la estructuración de las capas. Desde su primera promulgación en **1977**, hasta su definitiva estandarización en **1983**, los diferentes grupos de trabajo acordaron los siguientes principios maestros:

1. Una **estructura sencilla**: la estructura no debe constar de demasiadas capas.

2. **Enlaces sencillos** entre módulos: las interacciones entre capas en la frontera deben ser mínimas.

3. **Funciones distintas** en capas distintas: funciones de distinta naturaleza podrían entrar en conflicto dentro de la misma capa..

4. **Funciones semejantes** en la misma capa: sobre todo si están altamente

relacionadas.

5. **Fronteras** entre capas concretas: en función de las experiencias anteriores válidas.

6. Cada capa debe presentar un **funcionamiento interno** totalmente independiente de su funcionalidad.

7. Toda **frontera física** debe ser frontera entre capas: como por ejemplo, en cualquier punto que existiera un controlador de comunicaciones.

8. **Niveles de abstracción** de datos distintos determinan capas distintas.

9. **Modificaciones** internas a una capa deben ser transparentes para el resto de las capas.

10. Cada capa solo presenta **dos fronteras**: una con la capa superior y otra con la capa inferior.

La **ISA** solamente tiene que ver con la transmisión de la información entre los procesos de aplicación y se desentiende del sistema real en si, esto es, qué maquinaria es, qué microprograma dispone, qué lenguajes de programación utiliza y en definitiva, qué fabricante es.

Un aspecto importante de la *ISA* es que pretende alcanzar el concepto de sistemas distribuidos en lo relativo al procesamiento distribuido, bancos de datos distribuidos, etc. En suma, todo lo concerniente a la conexión de sistemas corporativos. En la *X.200* se citan textualmente las siguientes actividades:

a) **Comunicación entre procesos**, que concierne al intercambio de información y a la sincronización de la actividad entre procesos *ISA*.

b) **Representación de datos**, que concierne a todos los aspectos de la creación y mantenimiento de descripciones de datos y de transformaciones de datos para la modificación del formato de los datos intercambiados.

c) **Almacenamiento de los datos**, que concierne a los medios de almacenamiento y a los sistemas de ficheros y de bases de datos.

d) **Gestión de procesos y recursos**, que concierne a los medios por los cuales los procesos de aplicación ISA son declarados, iniciados y controlados.

e) **Integridad y seguridad**, que concierne a las restricciones en materia de procesamiento de información que deben observarse o garantizarse durante el

funcionamiento de los sistemas abiertos.

f) **Soporte de programas**, que concierne a la definición, compilación, almacenamiento, transferencia y acceso de los programas ejecutados por procesos de aplicación *ISA*.

6.1 CONCEPTOS BÁSICOS

En el **apartado 3** de este capítulo, se ha hecho una presentación de la estructura fundamental de casi todas las *arquitecturas de red* existentes. En el caso de la **ISA** podemos volver a hacer referencia a todo lo que se dijo allí.

Una cualquiera de las 7 capas del *OSI*, llamémosla **N**, está precedida por la **N-1** y seguida por la **N+1**. Cada capa recibe servicios de la **N-1** y presta los que necesite la **N+1**. Cada capa contiene una agrupación de **funciones lógicas** que constituyen un **servicio** para facilitar la comunicación: formalmente un servicio es, según la **UIT**, "*la capacidad de la capa N y de las capas por debajo de ella que se ofrece a las entidades N+1 en la frontera entre la N y la N+1*". Una **función** o un **grupo** de ellas conforma lo que se llama una **entidad** o **elemento activo**. Una *entidad* acepta unos datos de entrada (*argumentos*) y produce otros de salida (*valores*) que son lógicamente producto de las funciones que han intervenido. En cualquier momento dentro de una capa puede haber más de una *entidad* en activo.

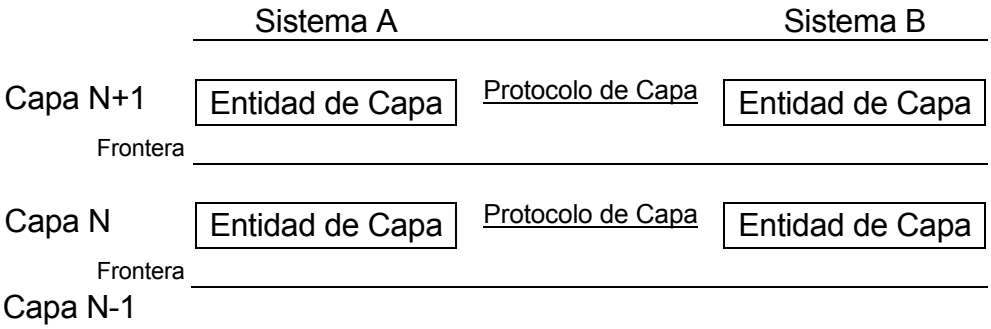


Fig. I.24: *Relación peer to peer entre capas.*

Un **protocolo** de capa **N** es (**UIT**) "*el conjunto de reglas y formatos (sintácticos y semánticos) que determinan el comportamiento de comunicación de las entidades N en la realización de funciones*".

6.2 LA COMUNICACIÓN OSI

Las relaciones entre las entidades de capas adyacentes se efectúan por medio de **peticiones**, **indicaciones**, **respuestas**, y **confirmaciones**. Tales secuencias de eventos se las

llama **primitivas de servicio**. Cada primitiva de servicio se define de manera similar a una *subrutina* de un programa de computador, esto es, tiene un nombre propio, unos argumentos y se la desencadena por una llamada.

Dos entidades de la capa **N** y en los sistemas **A** y **B** se comunican mediante su **protocolo** de capa (xxxxx) o protocolo entre pares (*peer protocol*). Las comunicaciones entre entidades pares establecen conexiones en transmisiones **duplex**, **semiduplex** o en **simplex**.

El intercambio de información y las relaciones entre capas adyacentes se efectúan a través de los **puntos de acceso a los servicios** (*Service Access Points* - **PAS**). En una capa **N** los **PAS** están situados en la frontera. Se dice que un **PAS N** identifica una entidad de capa **N+1**. A cada **PAS** se le asocia una dirección. Cada entidad **N+1** tiene su **PAS** en la frontera de **N**. Esto quiere decir que solamente se permite que resida una entidad por encima de un particular **PAS** y de este modo la dirección de ese **PAS** puede ser usada para identificar la entidad.

Entre dos sistemas alejados **A** y **B** y en la capa **N** las entidades **N(A)** y **N(B)**, usuarios de servicios se comunican por medio de los servicios prestados por la capa **N-1** que es el camino lógico y a su vez cada capa utiliza los servicios de las capas inferiores.

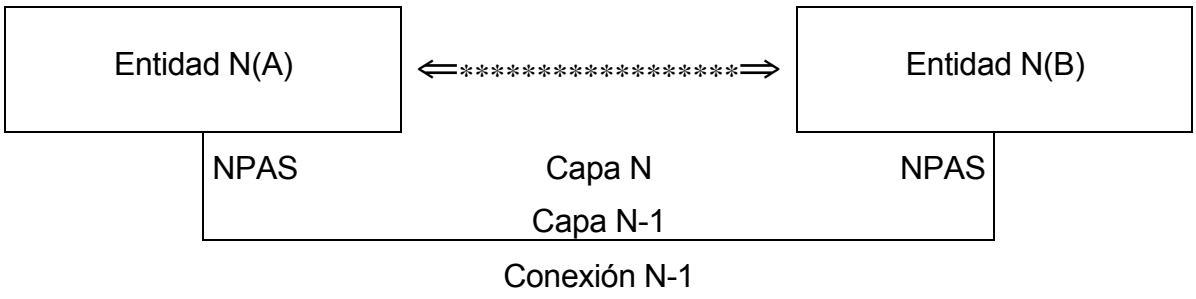


Fig. I.25: *Comunicación OSI.*

En el modelo de referencia los servicios operan en el **modo conexión** entre dos usuarios. Esto quiere decir que la información se intercambia cumpliendo las tres fases típicas: **conexión**, **transferencia** y **desconexión** (igual que en los circuitos conmutados de voz). En definitiva, una capa **N** hace una *conexión*, una *transferencia* y una *desconexión* con la capa **N+1**. Cada una de estas operaciones viene regida por un comando denominado **primitiva**.

Las primitivas en el **modo de conexión** son las siguientes:

- **PETICIÓN** (*request*): la inicia la capa **N+1** para solicitar o activar un *servicio* nominado a la capa **N**. Por ejemplo, la *capa de transporte* solicita con una *Petición* una conexión a la *capa de Red*.

- **INDICACIÓN** (*indication*): la emite la capa **N** para "*aconsejar*" la activación de un *servicio* de la **N+1**. Para continuar con el ejemplo anterior, un sistema que reciba una *Petición* para una conexión de *Red*, emitiría una *indicación* a la capa de *Transporte* quien tiene que decidir si acepta o rechaza.

- **RESPUESTA** (*response*): es dada por la capa *N+1* en contestación a la primitiva de *Indicación*. En el ejemplo anterior, la capa de *Transporte* daría una *respuesta* a la *Red* si ha aceptado.

- **CONFIRMACIÓN** (*confirm*): al término del proceso de *Petición* de *servicios* la capa *N* entrega al que puso la *Petición* la *Confirmación* de que el servicio ha sido completado. En el ejemplo la capa de *Red* informaría a la de *Transporte* que la conexión ha sido hecha con éxito.

Cada primitiva puede tener un determinado número de parámetros que acarrean información para los servicios respectivos.

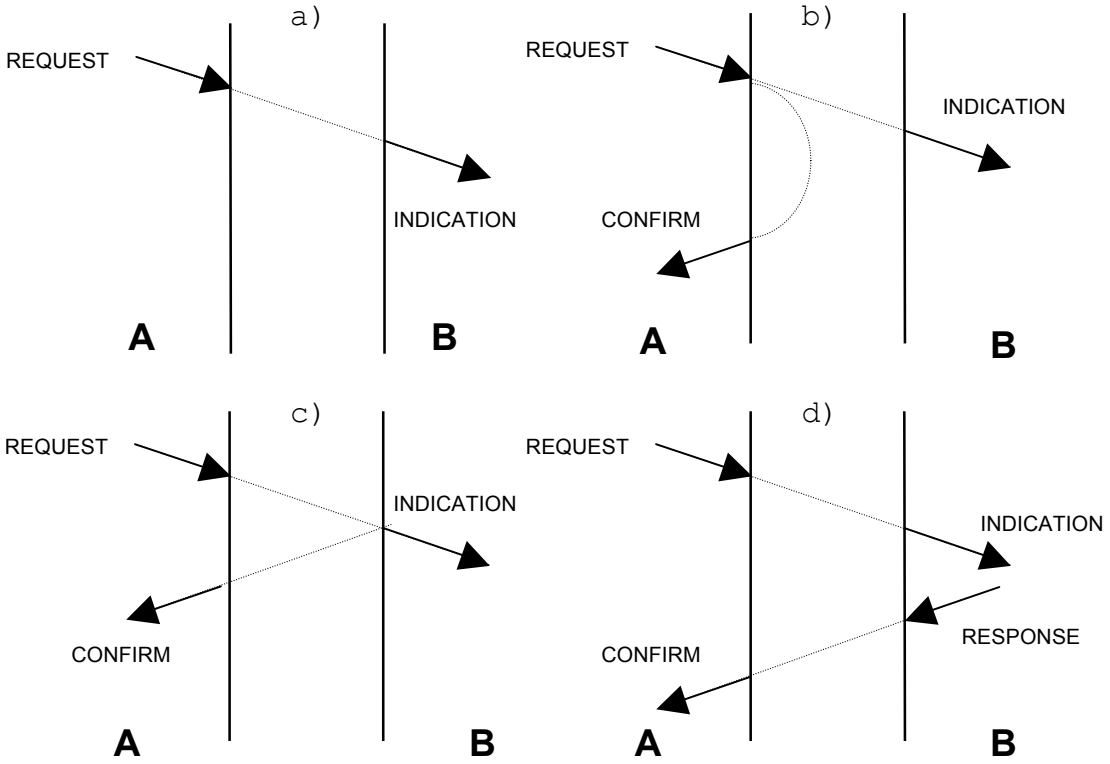


Fig. I.26: *Relaciones entre primitivas. A y B representan a los usuarios de los servicios, unidos ambos a través del interfaz del suministrador del servicio.*

Los diagramas anteriores son temporales, esto es, la primitiva de **INDICACIÓN**

sucede al cabo de un tiempo a la ocurrencia de **PETICIÓN**. De igual modo, la **CONFIRMACIÓN** de la **Conexión** sucederá un poco más tarde a la **RESPUESTA**. En el caso **d)** estamos en el caso de una **conexión** típica entre usuarios de servicios con **confirmación total**. El proceso de **desconexión** solicitado por uno cualquiera de los dos contiene la misma secuencia **temporal PETICIÓN-INDICACIÓN-RESPUESTA-CONFIRMACIÓN**. En aquellas situaciones en las que prive la urgencia se puede efectuar por parte de uno la **desconexión** sin que haya necesidad de **confirmación** por el otro (casos **b)** y **c)**).

En los enlaces entre usuarios que no necesitan conexión, **modo de operación sin conexión**, solamente se emplean dos primitivas de servicio: **PETICIÓN** e **INDICACIÓN,** como en el caso **b)**. Incluso, en los circuitos virtuales permanentes de la capa de **RED**, algo así como circuitos punto a punto, el usuario de la capa de **Transporte** no precisa de **CONFIRMACIÓN** por la de Red, como en el caso **a)**.

6.3 NIVELES OSI

Sea el caso de dos sistemas informáticos distintos, **A** y **B**, que desean intercambiar información de unas aplicaciones de venta comercial de productos y que se interconectan por medio de la red **IBERPAC**.

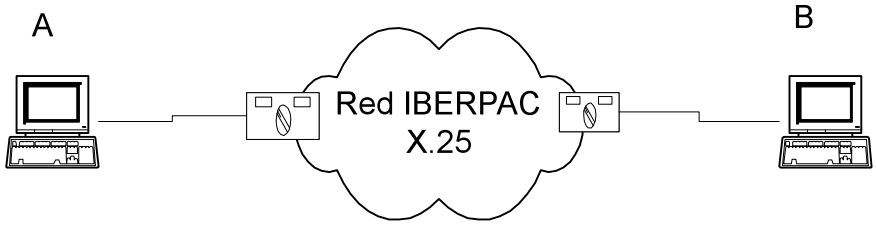


Fig. I.27: *Configuración de referencia a través de IBERPAC.*

El programa de **aplicación** establece conexión que va concatenándose capa a capa mediante sus correspondientes *primitivas*, en modo descendente por el sistema **A** hasta llegar al **físico** y en modo ascendente por los tres niveles de **IBERPAC**, vuelta a descender por los tres de la *red nacional de paquetes* para ascender por todas las capas del sistema **B** hasta llegar a la de su aplicación: en este momento todas las capas de A y B han establecido sus conexiones de entidades pares (*peer to peer*) con sus correspondientes protocolos de capa. En cada una de ellas la **ICP** (*Información de Control de Protocolo*) se añade a la **UDS** (*Unidad de Datos de Servicio*) como **cabecera de control**.

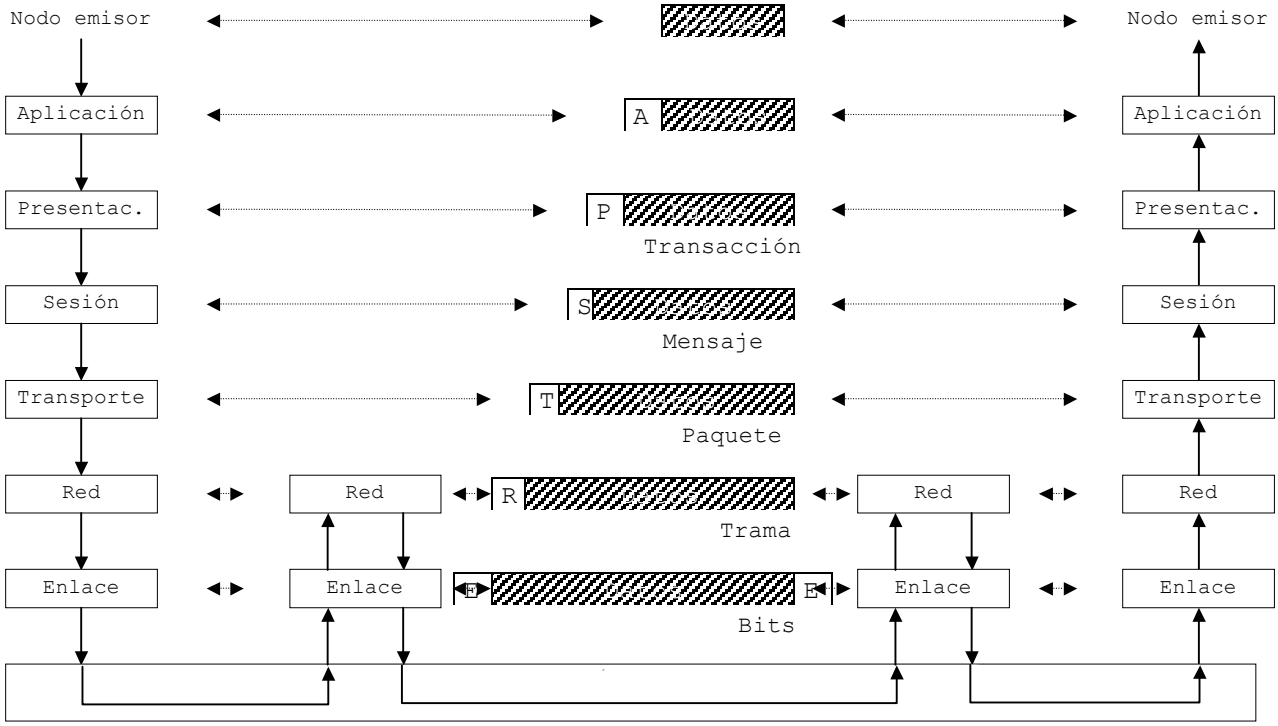


Fig. I.28: *Transmisión de datos en el modelo OSI.*

Con el fin de familiarizarnos con los niveles 2 y 3, sus **UDP** han sido nombradas como ***tramas*** y ***paquetes*** respectivamente. En la *trama* se indican *5* campos, cuatro de un octeto y uno de dos:

S	D	C	Paquete (UDP nivel 3)	SVT	S
Cabecera				Cola	

S : Octeto irrepetible de sincronismo de trama (01111110)
D: Octeto de dirección de la entidad de red
C: Octeto de control del enlace
SVT: Dos octetos de Secuencia de Verificación de trama (CRC)

Fig. I.29: *Formato de una UDP de nivel dos (Trama)*

En la figura 29 se ha esquematizado cómo las **ICP** se añaden a las **UDS** para formar las **UDP** (*Unidades de Datos de Protocolo*) a medida que la información va descendiendo por las capas del sistema **A**. Cuando la información sube por las del sistema **B** cada capa comprueba su cabecera y si cumple las reglas de protocolo *peer to peer*, la retira y solamente entrega a su capa inmediatamente superior la correspondiente *UDS* cumpliendo lo que le indique la *cabecera* o *ICP*.

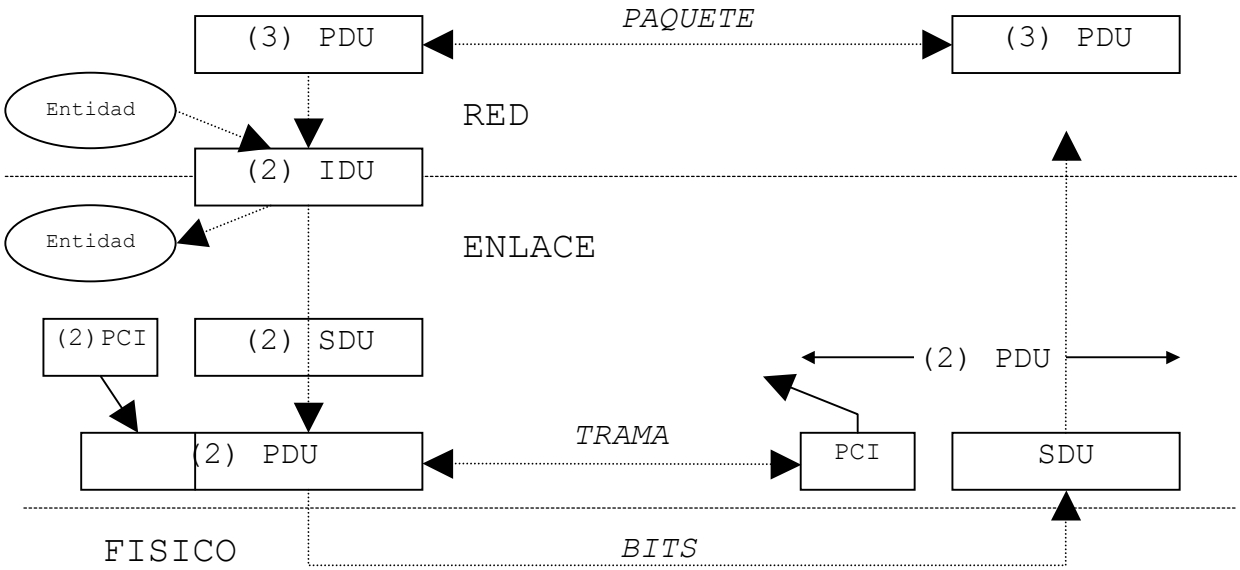


Fig. I. 30: *Ensamblado y desensamblado de las PDU de las tres primeras capas OSI.*

- *Ensamblado de las PDU* (*Unidades de Datos de Protocolo*): Una *PDU* de nivel 3 accede a través de la *SAP* y mediante los servicios y funciones aportados por la entidad de red en forma de *IDU* de nivel 2 (*Unidad de Datos de Interfaz*), pasando a ser una *UDS* (*Unidad de Datos de Servicio*). La entidad de enlace añade una *PCI* (*Información de Control de Protocolo*), pasando a constituir una *PDU* de nivel 2, que a su vez es pasada a la capa física.

- *Desensamblado de las PDU*: Una vez en el nodo destino, de dicha *PDU* la entidad de capa 2 extrae las correspondientes *PCI* y *SDU*, para pasar esta última a la capa 3 como *PDU* de Red.

6.4. Las capas del modelo OSI (Resumen)

El modelo OSI define siete capas:

1.Física
2.Enlace
3.Red
4.Transporte
5.Sesión
6.Presentación
7.Aplicación

La ISO ha especificado protocolos para todas las capas, aunque algunos son poco utilizados. En función del tipo de necesidades del usuario no siempre se utilizan todas ellas.

Pasaremos a describir brevemente las funciones desarrolladas por cada una de las capas.

6.1.1. La Capa Física

Esta capa transmite los bits entre dos entidades (nodos) directamente conectadas. Puede tratarse de un enlace punto a punto o de una conexión multipunto (una red broadcast, por ejemplo Ethernet). La comunicación puede ser dúplex, semi-dúplex o simplex. Si la información se transmite por señales eléctricas se especifican los voltajes permitidos y su significado (1 ó 0) y análogamente para el caso de fibra óptica. Se especifican las características mecánicas del conector, la señalización básica, etc.

Como ejemplos de la capa física podemos mencionar las norma EIA RS-232-C, utilizada por las puertas COM de los ordenadores personales, la EIA-RS-449, CCITT X.21/X.21bis, CCITT V.35. Las normas de redes locales incluyen en sus especificaciones la capa física (IEEE 802.3 o Ethernet, IEEE 802.5 o Token Ring, ISO 9314 o FDDI, etc.)

Muchas de las normas que existen en la capa física se refieren a la interfaz utilizada para conectar un ordenador con un módem o dispositivo equivalente, que a través de una línea telefónica conecta con otro módem y ordenador en el extremo opuesto. Este es el caso por ejemplo de las normas EIA RS-232-C, EIA-RS-449, CCITT X.21/X.21bis y CCITT V.35 antes mencionadas. En estos el conector del ordenador y el módem son de diferente 'sexo' (macho o hembra). En este contexto se suele utilizar la denominación DTE (Data Terminal Equipment) para referirse al ordenador y DCE (Data Circuit-Terminating Equipment) para referirse al módem. El 'módem' en ocasiones no es más que un adaptador, ya que por ejemplo la norma X.21 se utiliza para líneas digitales. En sentido general al equipo que actúa como adaptador entre el ordenador y el medio de transmisión se le denomina CSU/DSU (Channel Service Unit/ Data Service Unit).

6.1.2. La capa de enlace (data link)

La principal función de la capa de enlace es ofrecer un servicio de comunicación fiable a partir de los servicios que recibe de la capa física, también entre dos entidades contiguas de la red. Esto supone que se realice detección y posiblemente corrección de errores. A diferencia de la capa física, que transmitía los bits de manera continua, la capa de enlace transmite los bits en grupos denominados tramas (frames en inglés) cuyo tamaño es típicamente de unos pocos cientos a unos pocos miles de bytes. Si el paquete recibido de la capa superior es mayor que el tamaño máximo de trama la capa física debe encargarse de fragmentarlo, enviarlo y recomponerlo en el lado opuesto. En caso de que una trama no haya sido transmitida correctamente se deberá enviar de nuevo; también debe haber

mecanismos para reconocer cuando una trama se recibe duplicada. Generalmente se utiliza algún mecanismo de control de flujo, para evitar que un transmisor rápido pueda 'abrumar' a un receptor lento.

Las redes broadcast utilizan funciones especiales de la capa de enlace para controlar el acceso al medio de transmisión, ya que éste es compartido por todos los nodos de la red. Esto añade una complejidad a la capa de enlace que no está presente en las redes basadas en líneas punto a punto, razón por la cual en las redes broadcast la capa de enlace se subdivide en dos subcapas: la inferior, denominada subcapa MAC (Media Access Control) se ocupa de resolver el problema de acceso al medio, y la superior, subcapa LLC (Logical Link Control) cumple una función equivalente a la capa de enlace en las líneas punto a punto.

Ejemplos de protocolos de la capa de enlace incluyen ISO 7776, la capa de enlace de CCITT X.25, RDSI, LAP-D, ISO HDLC. Como ejemplos de protocolos de la subcapa MAC podemos citar los de IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), ISO 9314 (FDDI). El protocolo de subcapa LLC de todas las redes broadcast es el IEEE 802.2.

6.1.3. La capa de red

La capa de red se ocupa del control de la subred. Esta es la capa que tiene 'conciencia' de la topología de la red, y se ocupa de decidir por que ruta va a ser enviada la información; la decisión de la ruta a seguir puede hacerse de forma estática, o de forma dinámica sobre la base de información obtenida de otros nodos sobre el estado de la red.

De forma análoga a la capa de enlace la capa de red maneja los bits en grupos discretos que aquí reciben el nombre de paquetes; motivo por el cual a veces se la llama la capa de paquete. Los paquetes tienen tamaños variables, pudiendo llegar a ser muy elevados, sobre todo en protocolos recientes, para poder aprovechar eficientemente la elevada velocidad de los nuevos medios de transmisión (fibra óptica, ATM, etc.). Por ejemplo en TCP/IP el tamaño máximo de paquete es de 64 KBytes, pero en el nuevo estándar, llamado IPv6, el tamaño máximo puede llegar a ser de 4 Gbytes (4.294.967.296 Bytes).

Entre las funciones de la capa de red cabe destacar, aparte de la ya mencionada de elegir la ruta a seguir, el control del tráfico para evitar situaciones de congestión o 'atascos'. En el caso de ofrecer servicios con QoS el nivel de red debe ocuparse de reservar los recursos necesarios para poder ofrecer el servicio prometido con garantías. También debe ser capaz de efectuar labores de contabilidad del tráfico en caso necesario (por ejemplo si el servicio se factura en base a la cantidad de datos transmitidos).

En la capa de red es donde con mas intensidad se observa la distinción entre servicios orientados y no orientados a conexión (CONS vs CLNS). Las redes ATM, en el

nivel de red, dan un servicio de tipo CONS, y las redes TCP/IP un servicio de tipo CLNS.

La capa de red es la mas importante en redes de conmutación de paquetes (tales como X.25 o TCP/IP). Algunos ejemplos de protocolos utilizados en la capa de red son los protocolos de nivel de paquete y nivel de pasarela CCITT X.25 y X.75, el IP (Internet Protocol), CCITT/ITU-T Q.931, Q.933, Q.2931, y el OSI CLNP (ConnectionLess Network Protocol).

En las redes de tipo broadcast el nivel de red es casi inexistente, ya que desde un punto de vista topológico podemos considerar que en una red broadcast los nodos están interconectados todos con todos, por lo que no se toman decisiones de encaminamiento. Sin embargo veremos que la unión de redes broadcast mediante puentes suscita en algunos casos la necesidad de efectuar tareas propias del nivel de red en el nivel de enlace.

6.1.4. La capa de transporte

La capa de transporte es la primera que se ocupa de comunicar directamente nodos terminales, utilizando la subred como un medio de transporte transparente gracias a los servicios obtenidos de la capa de red. Por esta razón se la ha llamado históricamente la capa host-host. También se suele decir que es la primera capa extremo a extremo.

La principal función de la capa de transporte es fragmentar de forma adecuada los datos recibidos de la capa superior (sesión) para transferirlos a la capa de red, y asegurar que los fragmentos llegan y son recompuestos correctamente en su destino.

En condiciones normales la capa de transporte solicita a la capa de red una conexión diferente por cada solicitud recibida de la capa de sesión, pero puede haber razones de costo que aconsejen multiplexar diferentes conexiones en la capa de sesión sobre una sola conexión en la capa de red o, inversamente, razones de rendimiento pueden requerir que una conexión solicitada por la capa de sesión sea atendida por varias conexiones en la capa de red; en ambos casos la capa de transporte se ocupará de hacer la multiplexación mas adecuada de forma transparente a la capa de sesión.

La capa de transporte establece el tipo de servicio que recibe la capa de sesión, y en último extremo los usuarios. Éste podría ser por ejemplo un servicio libre de errores que entrega los mensajes en el mismo orden en que se envían; también podría ser un servicio de datagramas, es decir, mensajes independientes sin garantía en cuanto al orden de entrega ni confirmación de la misma, o un servicio broadcast o multicast en que los paquetes se distribuyen a múltiples destinos simultáneamente.

El control de flujo, que ha aparecido en capas anteriores, es necesario también en la capa de transporte para asegurar que un host rápido no satura a uno lento. La capa de

transporte realiza también su propio control de errores, que resulta ahora esencial pues algunos protocolos modernos como Frame Relay o ATM han reducido o suprimido totalmente el control de errores de las capas inferiores, ya que con las mejoras en la tecnología de transmisión de datos éstos son menos frecuentes y se considera mas adecuado realizar esta tarea en el nivel de transporte.

Salvo el caso de transmisiones multicast o broadcast el nivel de transporte se ocupa siempre de una comunicación entre dos entidades, lo cual le asemeja en cierto sentido al nivel de enlace. Por esto existen grandes similitudes entre ambas capas en cuestiones tales como el control de errores o control de flujo.

Ejemplos de protocolos de transporte incluyen el CCITT X.224, también llamado protocolo de transporte OSI TP4 (Transport Protocol 4). En Internet existen dos protocolos de transporte: TCP y UDP.

6.1.5. La capa de sesión

La capa de sesión es la primera que es accesible al usuario, y es su interfaz más básica con la red. Por ejemplo, mediante los servicios de la capa de sesión un usuario podría establecer una conexión como terminal remoto de otro ordenador. En un sistema multiusuario la capa de sesión se ocupa de ofrecer un SAP a cada usuario para acceder al nivel de transporte.

6.1.6. La capa de presentación

Hasta aquí nos hemos preocupado únicamente de intercambiar bits (o bytes) entre dos usuarios ubicados en dos ordenadores diferentes. Lo hemos hecho de manera fiable y entregando los datos a la sesión, es decir al usuario, pero sin tomar en cuenta el significado de los bits transportados. La capa de presentación se ocupa de realizar las conversiones necesarias para asegurar que dichos bits se presentan al usuario de la forma esperada.

Por ejemplo, si se envía información alfanumérica de un ordenador ASCII a uno EBCDIC será preciso efectuar una conversión, o de lo contrario los datos no serán interpretados correctamente. Lo mismo podríamos decir de la transferencia de datos enteros, flotantes, etc. cuando la representación de los datos difiere en los ordenadores utilizados.

6.1.7. La capa de aplicación

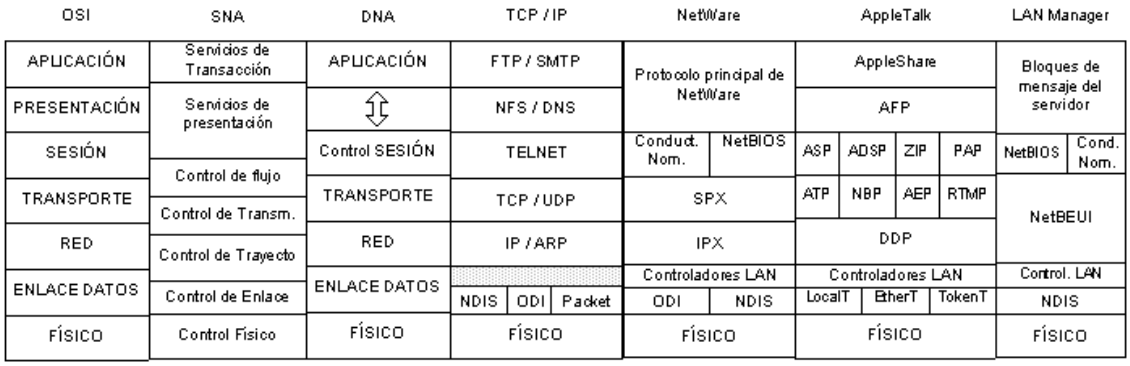
La capa de aplicación comprende los servicios que el usuario final está

acostumbrado a utilizar en una red telemática, por lo que a menudo los protocolos de la capa de aplicación se denominan servicios. Dado que se crean continuamente nuevos servicios, existen muchos protocolos para la capa de aplicación, uno o más por cada tipo de servicio.

Ejemplos de protocolos estándar de la capa de aplicación son el CCITT X.400, X.420, X.500, FTAM. SMTP, FTP, HTTP, etc.

7. TIPOS DE ARQUITECTURAS

En la siguiente figura se hace mención de las siete **arquitecturas propietario** más importantes del mercado:



FTP= File Transfer Protocol
SMTP= Simple Mail Transfer Protocol
NFS= Network File System
DNS= Domain Name Server
TCP= Transport Control Protocol
UDP= User Datagram Protocol
IP= Internet Protocol
ARP= Address Resolution Protocol

Fig. I.31: *Conjunto de protocolos y arquitecturas populares.*

En la siguiente tabla se puede observar la relación **Protocolo / arquitectura** desde el punto de vista de los distintos fabricantes:

OSI		UNIX	XNS	IBM		NOVELL
NIVELES SUPERIORES		PROD. ADICIONALES TCP/IP	APLICACIONES XNS	LAN SERVER APPC	PC LAN	SHELL
TRANSPORTE		TCP	SPP		NETBIOS	SPX
RED		IP	IPP	SNA		IPX
ENLACE		802.2 / LLC				
		MAC	MAC		MAC	
FISICO		802.3 / ETHERNET PHY / PMD	802.5 / TOKEN-RING PHY / PMD		FDDI / CDDI PHY / PMD	
MEDIOS FÍSICOS DE COMUNICACIONES UTP, STP, COAX, F.O., WIRELESS						

Fig. I.32: *Sistemas de red local.*

7.1 ARQUITECTURA SNA

SNA (*System Network Architecture*) es el estándar de **IBM** para la interconexión de sus ordenadores en forma de red. Nació en *1974* con un concepto totalmente centralista y *monoprocesador (Ver fig. 3.8)*, para pronto pasar a admitir la necesidad de más de un ordenador central. Fue la tecnología pionera en la estructuración de protocolos mediante capas o niveles:

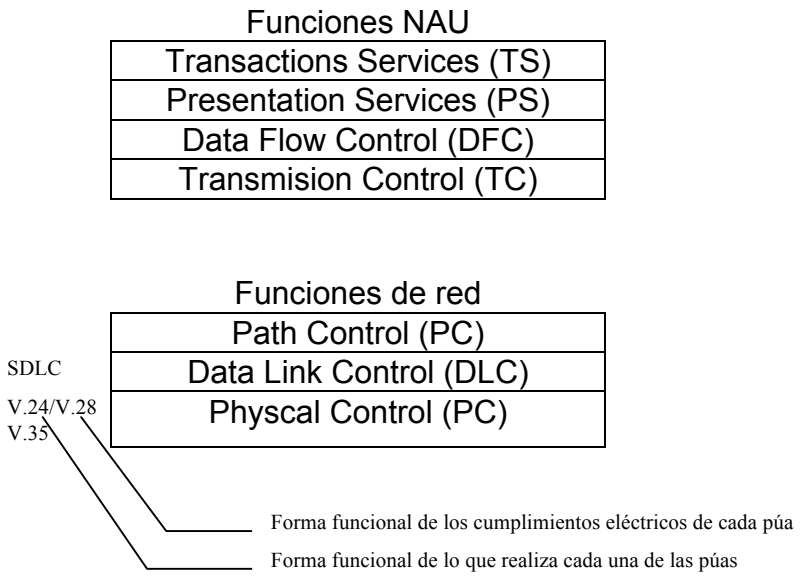


Fig. I.33: *Pila de protocolos SNA.*

Como se puede observar en la figura siguiente, consta de ocho niveles, uno más que el OSI, aunque las dos capas de gestión suelen considerarse una sola. Al igual que el OSI es una arquitectura **abstracta** en el sentido de que los niveles son independientes de los productos. Cada nivel es autónomo, y la modificación de un nivel superior o inferior no implica la reforma del nivel intermedio.

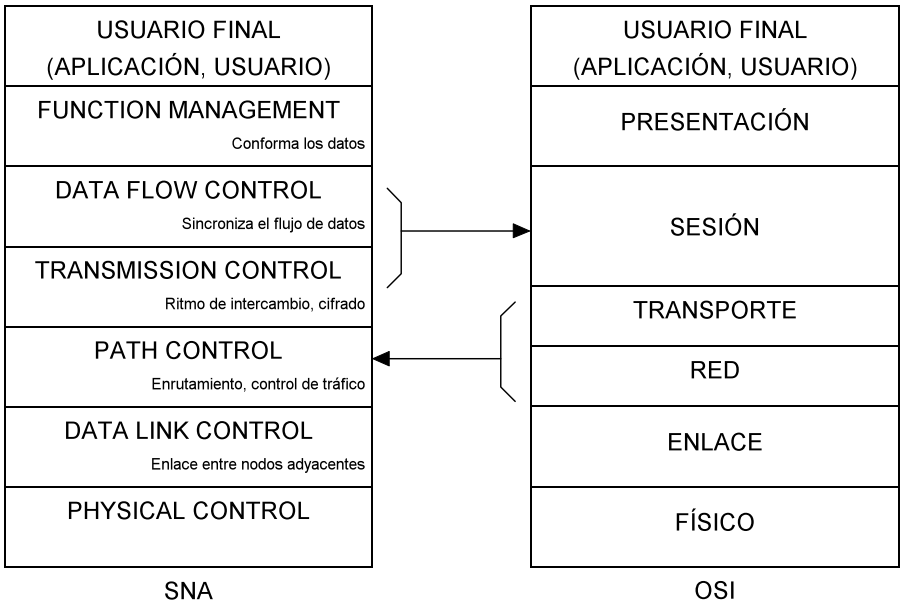


Fig. I.34: *SNA frente a OSI.*

En una red SNA una **UCP** (*Unidad Central de Proceso*) se conecta a la red mediante una **UCT** (*Unidad de Control de Transmisión*), que puede estar integrada en la **UCP**. A los usuarios se les denomina **Usuarios Finales** (**UF**), y sin tener por que ser humanos, deben situarse en los extremos de la red.

Además, la red va a presentar tres tipos básicos de componentes:

- **Nodos**: conjunto de hardware y software que implementan los niveles de la arquitectura SNA.
- **Enlaces**: que conectan nodos adyacentes.
- **Unidades Direccionables de la Red** (**NAU**).

Los **UF** ven la red a través de las **NAU** (*Network Addressable Unit*), que presentan una dirección de red y un nombre simbólico exclusivos. Su principal función es la de sincronizar la comunicación entre usuarios finales, pero además lleva a cabo la gestión de los recursos de cada nodo y ayudan a controlar y gestionar la red en sí.

Una conexión SNA recibe el nombre de **Sesión**, que se define como "*asociación lógica entre dos UF a través de sus NAU*".

SNA define los siguientes tipos de **NAU**:

- **Unidades lógicas** (**LU**) : el elemento básico de una *Sesión* entre dos *UF*.

- **Unidades Físicas** (**PU**): realizan la gestión de los enlaces, tanto por hardware como por software. Podemos distinguir:

  PU 5: Nodo *UCP*. Contiene un **SSCP**, una *PU* y varias *LU* asociadas al programa de aplicación. Da servicios de sesión y ruta.

  PU 4: Nodo *Controlador de Comunicaciones* (**UCT**). Es una *PU 5* sin *SSCP*.

  PU 2: Nodo *Periférico*. Son controladores de terminales (*Cluster Controllers*). Contienen una *PU* y una *LU* para cada usuario.

  PU 2.1: Nodo *Periférico*. Reside en nodos distribuidos, poseyendo un subconjunto de funciones *SSCP*.

  PU 1: Nodo *Periférico*. Soporta un controlador no inteligente mediante una *PU* y una sola *LU* de terminal no inteligente.

- **Puestos de Control de los Servicios del Sistema** (**SSCP** - *System Services Control Point*): Sus funciones pueden ser las de controlar los recursos del Sistema de Comunicaciones, supervisando el **Dominio** al que pertenece, gestionar el establecimiento de las sesiones, recibir mandatos del operador, enviar mensajes al operador.

La **SSCP** reside en una *UCP*, y gestiona un *dominio* de la red. Si la red cuenta con más de un *SSCP* se tiene una red de *múltiples dominios*, los cuales deben ser distintos. Todos los nodos y enlaces han de formar parte de un único dominio, el cual se define como el conjunto de nodos y enlaces controlados por un *SSCP* (Nodo tipo 5).

SNA permaneció prácticamente hasta 1985 como una estructura centralizada, aunque con cierta evolución (Ver figuras 35, 36 y 37.), que impedía el diálogo entre dos usuarios de red conectados a *PU 1*. Solamente era posible que un usuario pudiera hacer transacciones o trabajos con las aplicaciones de los ordenadores principales (*Host PU 5*). A partir de entonces, con la introducción del protocolo **APPN** (*Application Program To Program*) y de la unidad lógica *LU 6.2*, se hizo posible el intercambio directo de información entre terminales de cualquier punto de red, con lo que se posibilitaba la conexión de Redes de Área Local de topología en anillo con paso de testigo (*Token Passing Ring IEEE 802.5*), y el desarrollo de los sistemas de supervisión de red (***NETVIEW***), como se indica en la figura 38.

Desde 1987 *IBM* realizó importantes trabajos para conseguir la correcta adaptación de la arquitectura *SNA* a la arquitectura *OSI*.

Fig. I.35: *Red SNA Monodominio: Sistema centralizado.*

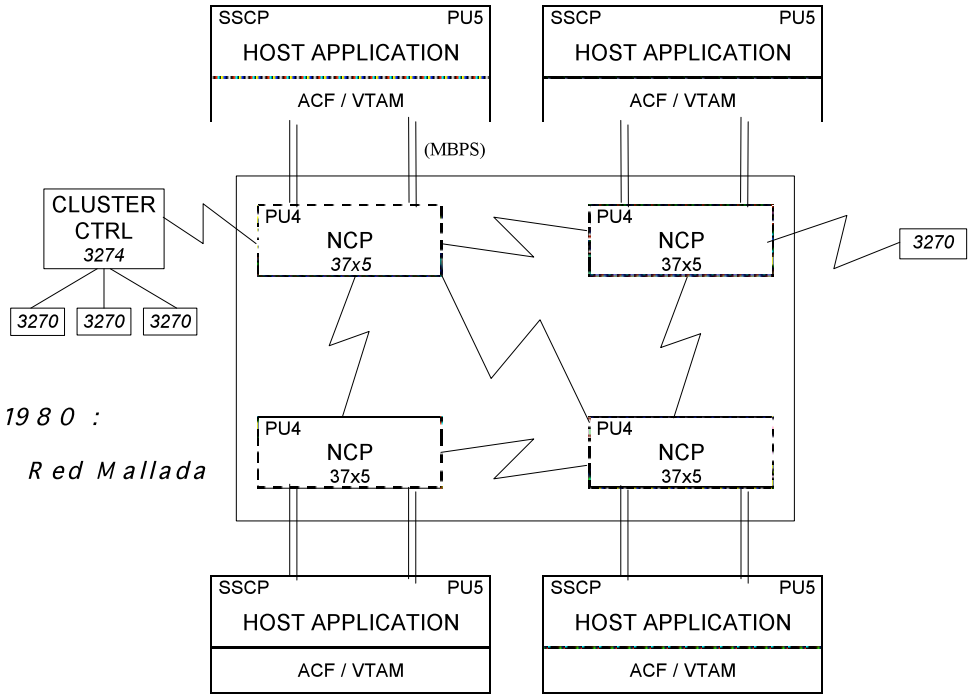


Fig. I.36: *SNA en sus comienzos: Redes totalmente malladas.*

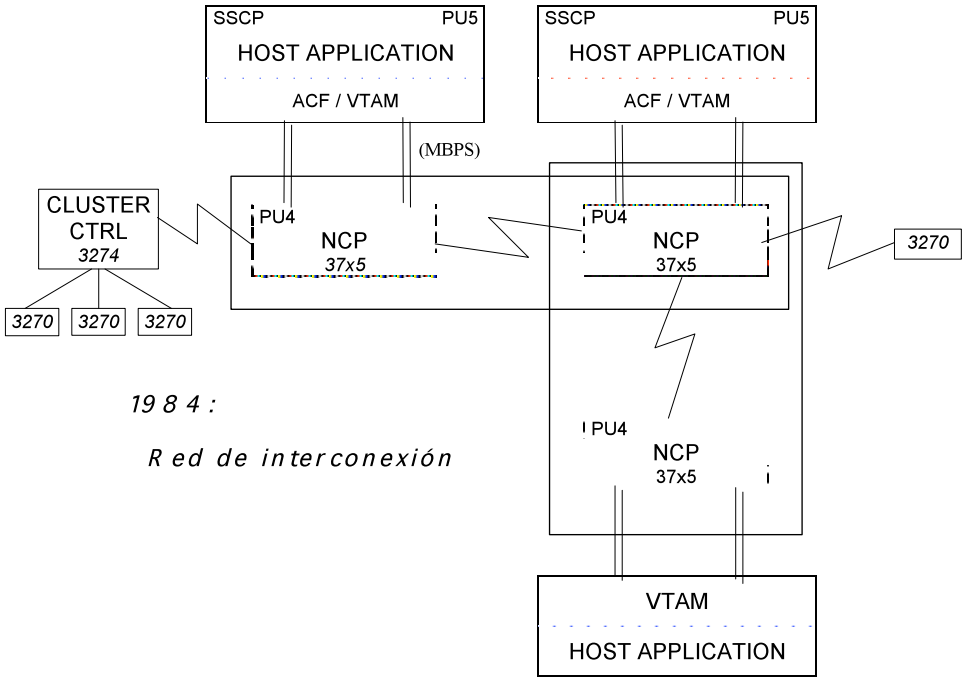


Fig. I.37: *Primera evolución: Interconexión de redes.*

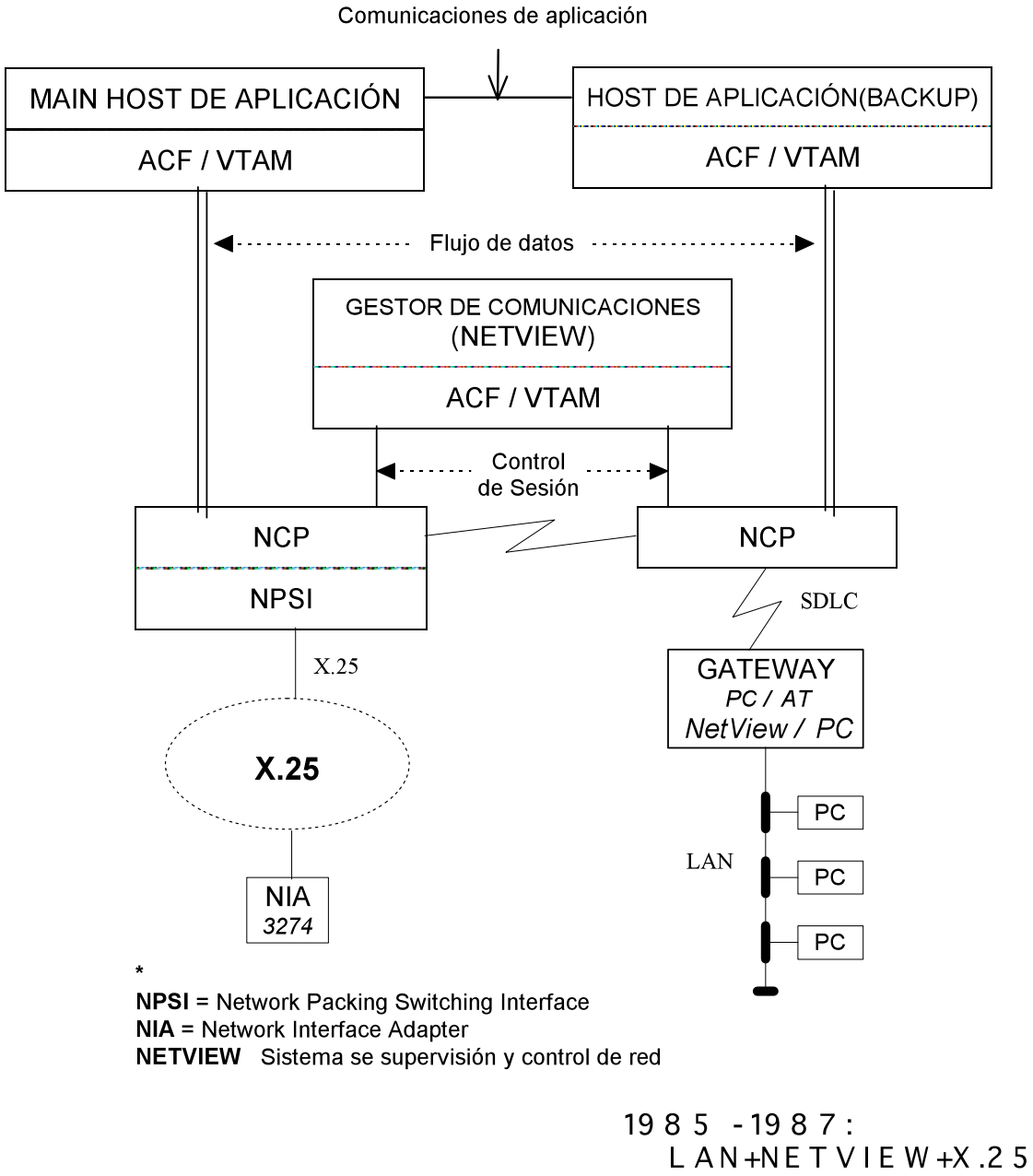


Fig. I.38: *Sistema final: Sistemas supervisados.*

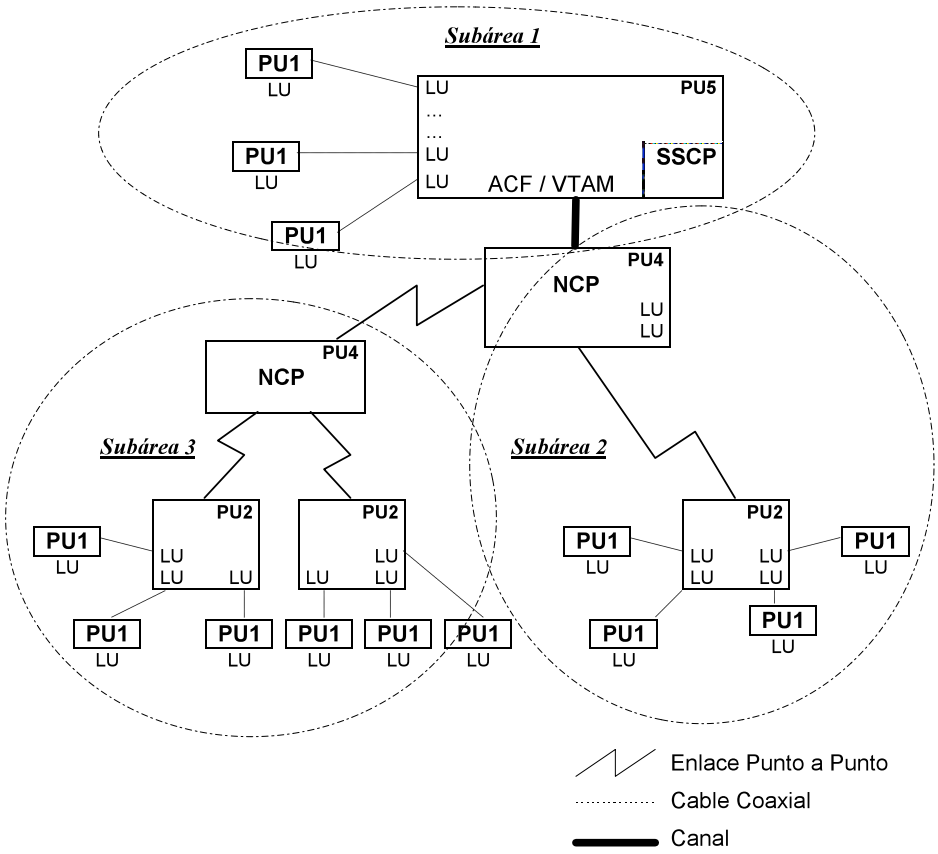


Fig. I.39: *SNA: Sistema de un único dominio y múltiples subáreas.*

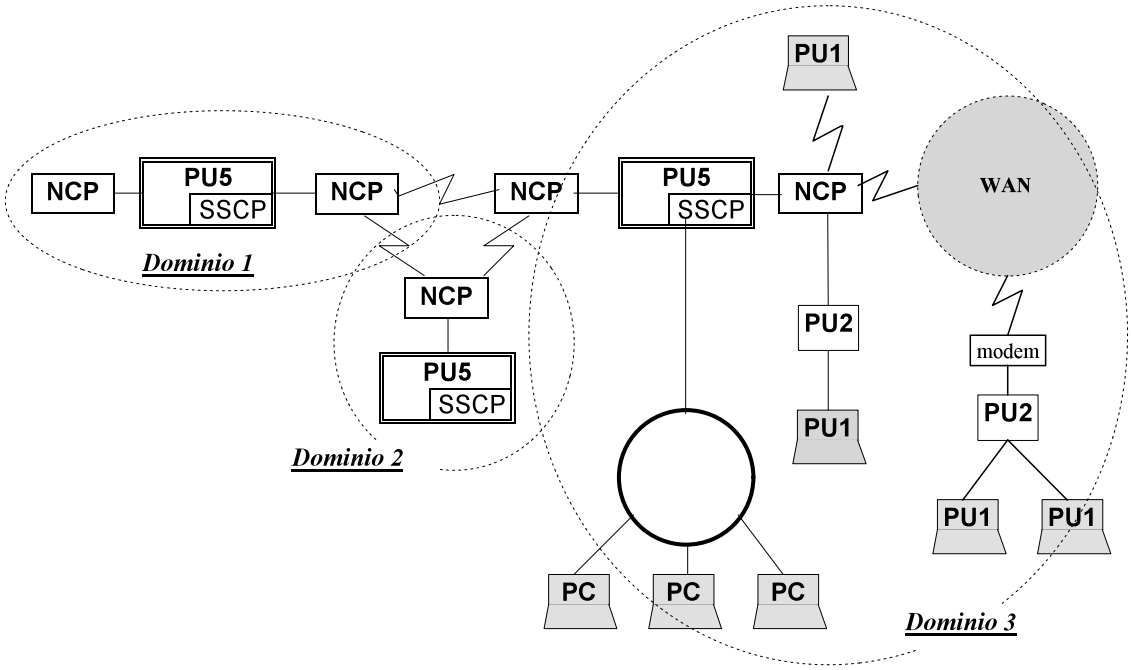


Fig. I.40: *SNA: Red de múltiples dominios.*

7.2 ARQUITECTURA DNA

La compañía **Digital Equipment Corporation** (**DEC**) introdujo en el año 1975 su arquitectura para sistemas en redes de comunicaciones de datos, denominada **DNA** (*Digital Network Architecture*). En principio, *DNA* especifica el marco de trabajo para el desarrollo de los productos de **DECnet**.

DNA se caracteriza por una topología sin sistema central, es decir, con control totalmente distribuido. Para alcanzar esta independencia topológica, las funciones de mantenimiento y control se ejecutan al nivel de las aplicaciones del usuario. Todos los nodos *DECnet* se direccionan de forma uniforme, de acuerdo a las características específicas de la aplicación del usuario que se ejecute. Los nodos que soportan aplicaciones centrales del usuario se denomina **HOST**, los que soportan terminales **CONCENTRADORES**, y los nodos que soportan funciones de ruteo y conmutación de mensajes, **NODO DE COMUNICACIONES**.

La arquitectura está representada en seis niveles principales:

APLICACIÓN
CONTROL DE SESIÓN
TRANSPORTE
CONTROL EXTREMO A EXTREMO (RED)
ENLACE DE DATOS DDCMP (DEC) LAP-B (HDLC / X.25) 802.3 / 802.2 (ETHERNET)
ENLACE FÍSICO V.24 / V.28 / v.35 V.10 / V.11 X.21

Fig. I.41: *Pila de protocolos DNA.*

- Capa de **aplicaciones de la red**: aquí se ejecuta el acceso a recursos, la transferencia de archivos y el cargador remoto del sistema. Utiliza el protocolo **DAP**: *Data Access Protocol.*

- Capa de **control de sesiones** (transporte y servicios)Utiliza los protocolos **NSP**

(*Network Services Protocol*) que implementa tanto el **Control de Sesión**, como el **Control Extremo a Extremo**.

- Capa de **Transporte**, que realiza las funciones de conmutación a partir del protocolo **TP** (*Transport Protocol*).
- Capa de **Red**, el *Control Extremo a Extremo* propiamente dicho.
- Capa de **enlace de datos**, que mantiene el camino de comunicación entre nodos adyacentes mediante el **DDCMP** (*Digital Data Communication Message Protocol*).
- Capa de **enlace físico**, donde se lleva el control de la transmisión de las señales eléctricas.

Para poder compatibilizar esta estructura de capas tan particular, *DNA* incorpora módulos que proveen compatibilidad a los equipos *DEC* con otras marcas, principalmente con *IBM*, en redes *SNA*. Para otro tipo de interconexiones *DNA* adopta el modelo **X.25** de la *UIT*.

7.3. OTRAS IMPLEMENTACIONES

Podemos encontrar otra serie de *modelos de referencia* que aunque no determinan arquitecturas de red en si, se han ido imponiendo dado el peso de sus *desarrolladores*. Así caben destacar los modelos impuestos por empresas tales como **Novell** o **Apple**, e incluso el estándar de facto **TCP/IP** (Tratado ampliamente en **capítulos posteriores**).

A) EL MODELO NOVELL

El modelo de red de **Novell IPX/SPX** es una implementación del protocolo **IDP** (*Internetwork Datagram Packet*) de **Xerox**. *IPX* permite que las aplicaciones que se ejecuten sobre estaciones de trabajo **DOS**, **Windows** u **OS/2** accedan a los *manejadores* de red de **Netware** y se comuniquen con otras estaciones de trabajo, servidores, u otros dispositivos de la red.

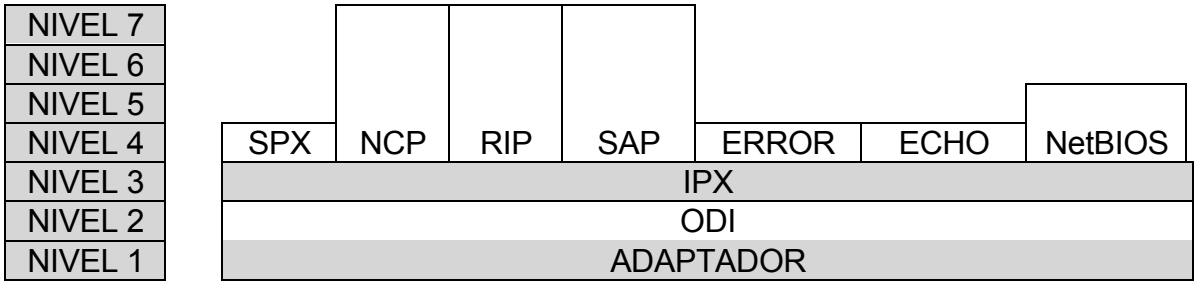


Fig. I.42: *Pila de protocolos NetWare.*

El conjunto de protocolos denominados **IPX/SPX** consiste en una variedad de protocolos iguales (**peer**):

IPX: *Internetwork Packet Exchange.*
SPX: *Sequential Packet Exchange.*
NCP: *Netware Core Protocol.*
SAP: *Service Advertising Protocol.*
RIP: *Router Information Protocol.*
Echo y **Error**: protocolos de mantenimiento interno.

Novell incluso ha implementado un emulador **NetBios** para que las aplicaciones que utilicen *NetBios* puedan usar *IPX* como protocolo de red.

Todos estos protocolos configuran la torre de protocolos **NETWARE** (ver fig. 3.15), no existiendo correlación directa con la de protocolos OSI.

El nivel **ODI** (*Open Data-Link Interface*) proporciona una función análoga a la del nivel de **enlace** de datos de *OSI*. El objetivo de *ODI* es permitir que uno o varios *manejadores* de protocolos de red utilicen uno o varios *manejadores* de **adaptadores**.

El *IPX* es un protocolo de **datagramas**, que lleva a cabo el mejor intento para enviar paquetes de datos, pero que no garantiza la entrega de los datos. El término "*datagrama*" significa que cada paquete se trata como una entidad individual, sin considerar ninguna relación lógica o secuencial con cualquier otro paquete.

El IPX es un protocolo **no orientado a la conexión**, por tanto poco fiable, transmite los datos a un nodo remoto pero no espera respuesta o una confirmación indicando si los datos han sido recibidos con éxito. Se deja a los protocolos de nivel superior que proporcionen esta transmisión de datos fiable; lo que en el entorno *NetWare* se implementa dentro de la **shell**. Debido a que el protocolo *IPX* es sin conexión y no espera una confirmación, es capaz de proporcionar mayor rendimiento que una conexión o sesión basada en protocolos como **SPX** o **NetBIOS**. Si observamos la estructura de un **paquete** *IPX* encontraremos:

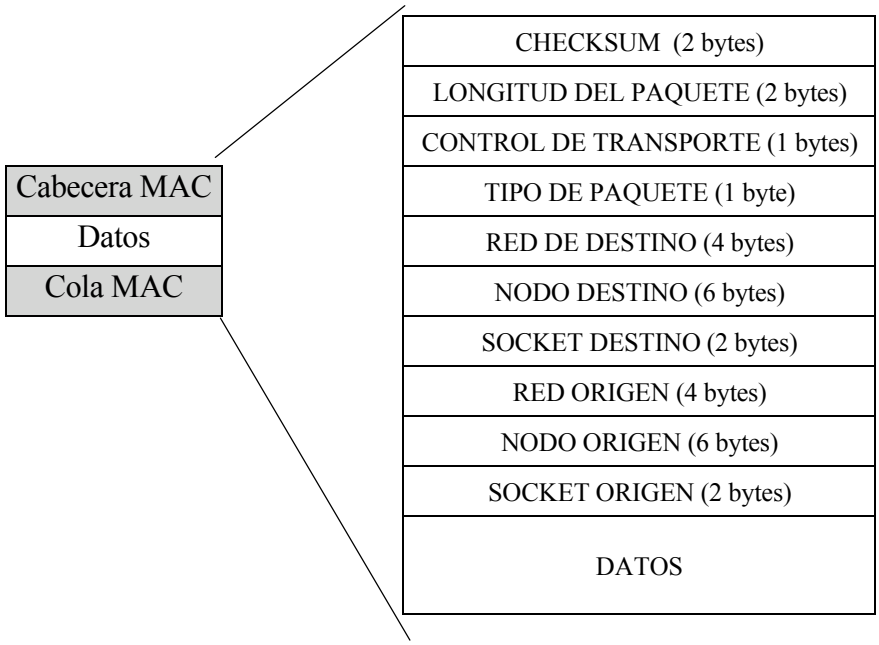


Fig. I.43: *Estructura del paquete IPX.*

Checksum: verifica los errores a nivel de paquete.
Longitud: suma de la longitud de la cabecera más la de la sección de datos (*longitud mínima de 30 bytes*).
Control de Transporte para los manipuladores de red *NetWare*.
Tipo de paquete: indica el tipo de servicio ofrecido o requerido por el paquete:

0: tipo de paquete desconocido
1: paquete de información de encaminamiento
2: paquete de eco
3: paquete de error
4: paquete de intercambio de paquetes (IPX)
5: paquete de protocolo de paquetes secuenciados (SPX)
16-31: protocolos experimentales
17: NCP

IPX utiliza un esquema de *direccionamiento* de *12 bytes* para transmitir sus paquetes de datos, y dicha dirección se divide en tres secciones:

Redes origen y destino, utilizada para direccionar grupos de trabajo. Cada dirección de red tiene que ser única en la red (*IPX/SPX*).

Nodos origen y destino, direcciona nodos de red dentro de los grupos de trabajo (análogamente a las direcciones de los adaptadores *token-ring*).

Sockets origen y destino, se pueden utilizar para **multiplexar** funciones dentro de un nodo de red.

Los **sockets IPX** permiten que varios protocolos de alto nivel utilicen los *servicios IPX* de forma concurrente. Un *socket* es una dirección utilizada por el nivel *IPX* para identificar el protocolo de alto nivel al que se le debería pasar el paquete.

A fin de que un protocolo cliente *IPX* se comunique con su homólogo correspondiente, necesita conocer el número de *socket* de su aplicación homóloga remota. Para asegurar que el paquete *IPX* viaja a través de la red al sistema correcto, el programa cliente también debe conocer la dirección de nodo y de red de su homólogo.

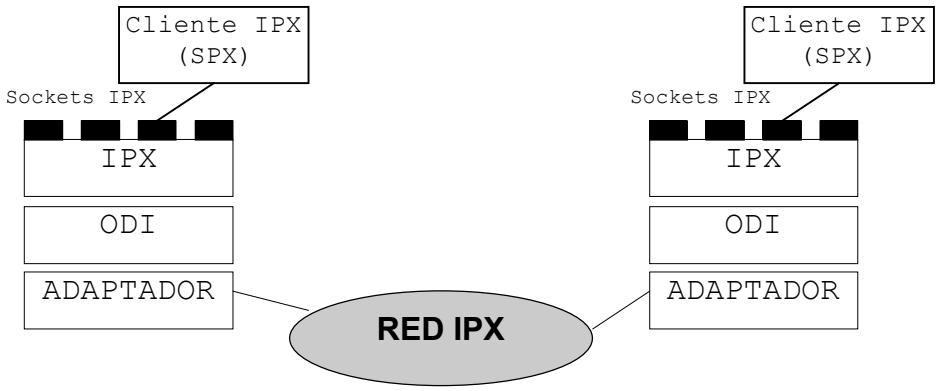


Fig. I.44: *Representación de los sockets IPX.*

B) EL MODELO DE APPLE

Los ordenadores **Macintosh** de **Apple** son conectados en redes locales a través del protocolo propietario **AppleTalk**, y cuya torre de protocolos sería:

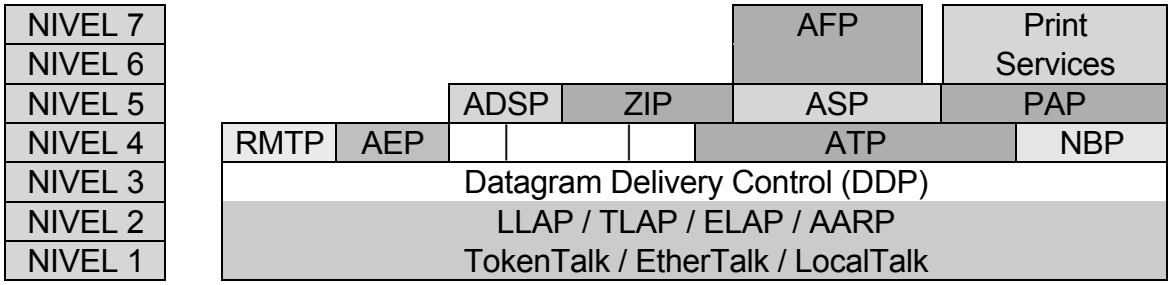


Fig. I.45: *Torre de protocolos AppleTalk.*

LocalTalk es un sistema de *cableado* fácilmente configurable que permite conectar estaciones de trabajo y otros dispositivos, como impresoras o "*escáneres*", a un entorno de red **AppleTalk**. *LocalTalk* se estructura en una topología de *bus* y su operación la gestiona el **LLAP** (*LocalTalk Link Access Protocol*).

LLAP proporciona los servicios básicos de transmisión de paquetes entre nodos de una red *LocalTalk*, y gestiona el acceso al enlace compartido utilizando el método **CSMA/CD**. El protocolo **LLAP** utiliza un mecanismo de direccionamiento de nodos que permite asignar dinámicamente la identificación de los nodos, que consiste en un número de *8 bits*.

Las redes *AppleTalk* también pueden establecer enlaces de datos con redes *Ethernet* y pase de *testigo en anillo*, aunque en estos casos no se utiliza el *LLAP*, ya que los mecanismos de direccionamiento son diferentes (la identificación de nodos en *Ethernet* y *Token* se lleva a cabo por medio de 48 bits). La traducción de la identificación de los nodos de *AppleTalk* a los de una red Ethernet o de pase de testigo se lleva a cabo mediante un protocolo especial denominado **AARP** (*AppleTalk Address Resolution Protocol*).

TokenTalk y **EtherTalk** proporcionan acceso a redes de *pase de testigo* y *Ethernet* utilizando, respectivamente, los protocolos **TLAP** (*TokenTalk Link Access Protocol*) y **ELAP** (*EtherTalk Link Access Protocol*).

El **DDP** (*Datagram Delivery Protocol*) es responsable del encaminamiento, entrega y empaquetado de datos básicos en *datagramas*.

El **RTMP** (*Routing Table Maintenance Protocol*) se utiliza para establecer y mantener las *tablas de encaminamiento*, que son fundamentales para el envío de *datagramas* de cualquier **socket** fuente a cualquier **socket** destino de la red. El *RTMP* permite que los **encaminadores** intercambien información de las tablas de encaminamiento de forma periódica, lo que permite actualizar el cálculo de los caminos más cortos a cada red de destino.

El **AEP** (*AppleTalk Echo Protocol*) es un protocolo especial de pruebas que permite determinar si un nodo está accesible. También se utiliza para estimar el tiempo que emplea un paquete en alcanzar un nodo de la red.

El **NBP** (*Name Binding Protocol*) se utiliza para convertir los "**alias**" (*nicknames*) de la red en direcciones.

El **ATP** (*AppleTalk Transaction Protocol*) es un protocolo orientado a la conexión cuyo propósito principal es garantizar la entrega de paquetes de datos.

El **ZIP** (*Zone Information Protocol*) permite hacer corresponder la red *AppleTalk* con la zona apropiada, siendo implementado por los encaminadores.

El **ADSP** (*AppleTalk Data Stream Protocol*) es un protocolo *orientado a conexión* que proporciona una interfaz a las redes *AppleTalk*. Establece el mantenimiento de flujos **full-duplex** de datos entre dos *sockets* de la red.

El **PAP** (*Printer Access Protocol*) es un protocolo *orientado a conexión* que permite múltiples sesiones entre una estación cliente y un servidor, gestionando el arranque, mantenimiento y liberación de la sesión, así como la transferencia de datos en la misma.

Por último, el **AFP** (*AppleTalk Filing Protocol*) permite al usuario acceder a los recursos de memoria de un sistema remoto empleando los mismos mandatos que los utilizados para manipular los recursos locales.

C) LA ALTERNATIVA DE IBM : NETBIOS

Cuando empezaron a desplegarse las redes de ordenadores personales, **IBM** introdujo los protocolos **NETBIOS**, debido a que no existían estándares para los niveles superiores.

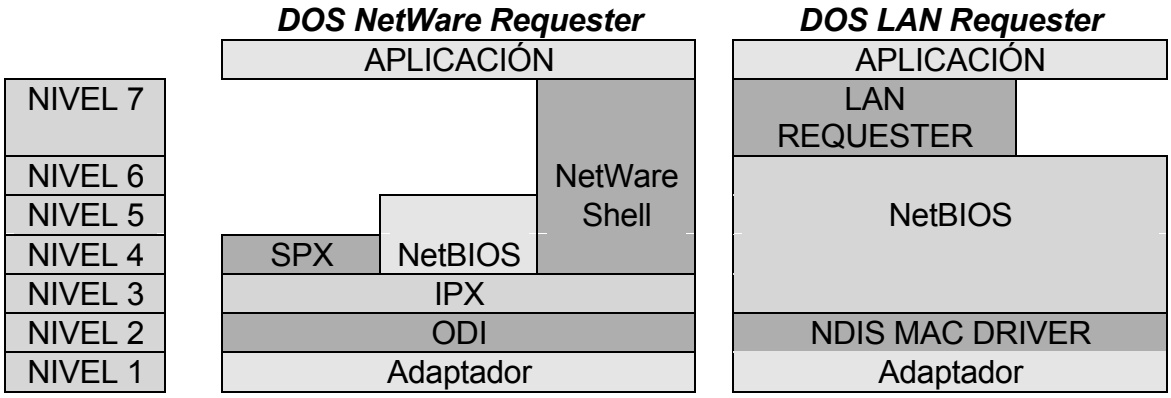


Fig. I.46: *Torre de Protocolos: NetWare y LAN Server de NetBIOS.*

En la figura se muestran dos implementaciones de **NetBIOS** en un entorno **DOS**: la de **IBM** y la de **NetWare**. Como puede observarse, el emulador de **Novell** implementa *NetBIOS* sobre **IPX** de forma análoga a **SPX**, pero no genera tramas compatibles con el *NetBIOS* de **IBM**:

IBM utiliza *NetBIOS* para proporcionar servicios de sesión entre el **LAN Requester** y el **LAN Server**. La **Shell** de *NetWare*, sin embargo, no utiliza *NetBIOS* para proporcionar servicios de sesión entre la *shell* cliente y el servidor, ya que la *shell* cliente de *NetWare* es

independiente de *NetBIOS*.

Es importante destacar que una aplicación que utiliza el entorno *NetBIOS* de *IBM* no puede comunicarse con otra que utiliza el entorno *NetWare*, ya que las aplicaciones que empleen la interfaz *NetBIOS* se ejecutarían exclusivamente sobre la torre de protocolos de *Netware* o sobre la de *IBM*.

NetBIOS mantiene la sesión enviando periódicamente una trama al nodo remoto para informarle de que todavía se encuentra disponible y que puede recibir datos, por lo que utiliza ciclos de memoria de manera continua aunque la aplicación del usuario no realice peticiones. *IPX*, por el contrario, sólo transmite tramas a través de la red cuando tiene datos que transmitir, por lo que *NetBIOS* tiene un impacto mayor sobre los recursos disponibles.

8. NORMAS IEEE 802 PARA LAN

Los **comités 802 del IEEE** se concentran principalmente en la interfaz física relacionada con los niveles físicos y de enlace de datos del modelo de referencia **OSI** de la **ISO**. Los productos que siguen las normas 802 incluyen **tarjetas** de la interfaz de red, **bridges**, **routers** y otros componentes utilizados para crear LANs de **par trenzado** y **cable coaxial**.

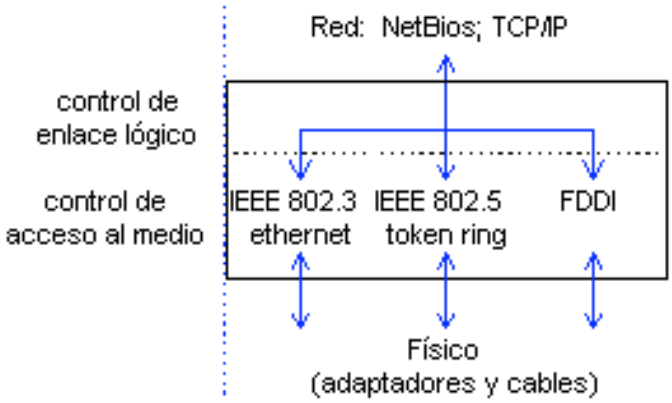


Fig. I.47: *Capa de enlace IEEE 802.*

El nivel de enlace se divide en 2 subniveles **MAC** y **LLC**. Son diferentes en la capa física en la subcapa MAC, pero son compatibles en la subcapa de enlace. El MAC es un módulo de software incorporado a la estación de trabajo o al servidor que proporciona una interfaz entre una tarjeta de interfaz de red **NIC** y el software redirector que se ejecuta en el computador.

802.1 da una introducción al conjunto de normas y define las primitivas de interfaz, para interconexión de redes.

802.2 describe la parte superior de la capa de enlace que utiliza el protocolo LLC.
802.3 describe la norma CSMA/CD.
802.4 describe la norma token bus.
802.5 describe la norma token ring.
802.6 red de área metropolitana MAN
802.7 grupo asesor para técnicas de banda ancha
802.8 grupo asesor para técnicas de fibra óptica.
802.9 redes integradas para voz y datos.
802.10 seguridad de red.
802.11 redes inalámbricas.
802.12 LAN de acceso de prioridad bajo demanda (100VG-Any LAN).

8.1 DEFINICIÓN DE INTERCONEXIÓN DE RED 802.1

Define la relación entre las normas 802 del IEEE y el modelo de referencia de la OSI. Este comité define que las direcciones de las estaciones de la LAN sean de 48 bits para todas las normas 802, y así cada adaptador puede tener una única dirección.

8.2 CONTROL DE ENLACES LÓGICOS 802.2

Define el protocolo que asegura que los datos se transmiten de forma fiable a través del enlace de comunicaciones **LLC Logical Link Control**. En los bridges estos dos subniveles se utilizan como un mecanismo modular de conmutación a un frame que llega a una red ethernet y se destina a una red token ring , se le desmonta su header de frame ethernet y se empaqueta con un header de token ring.

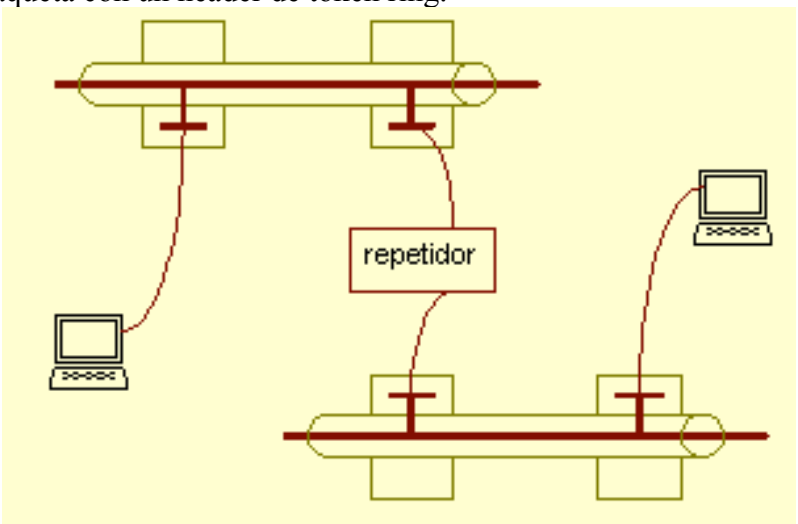


Fig. I.48: *Interconexión de segmentos mediante repetidor.*

El LLC suministra los siguientes servicios:

- **Servicio orientado a la conexión** en el cual se establece una sesión con un destino y se libera cuando se completa la transferencia de datos.
- **Servicios orientados a la conexión con reconocimiento** parecido al anterior, en el cual se confirma la recepción de los paquetes.
- **Servicio sin reconocimiento no orientado a la conexión** en el cual no se establece una conexión ni se confirma su recepción.

8.3 NORMA IEEE 802.3 Y ETHERNET

Se utilizan en redes LAN con protocolo CSMA/CD. Históricamente se inicia en el sistema ALOHA en Hawai, continuándose su desarrollo por la XEROX y posteriormente entre XEROX, DEC e Intel proponen una norma para la ethernet de 10 Mbps la cual fue la base de la norma 802.3.

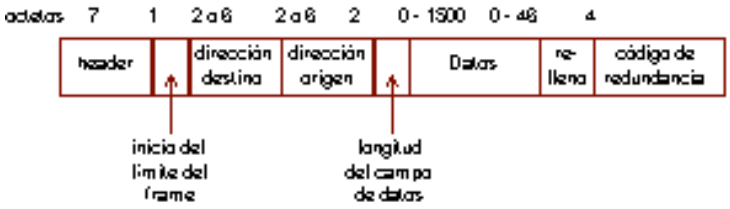


Fig. I.49: *Marco de la trama Ehternet.*

Se define el Protocolo de sub capa MAC para 802.3. La estructura del frame para un 802.3 es:

- El header de 7 octetos contiene el patrón 10101010 en cada octeto, generándose un pulso cuadrado de 10 MHz durante 5,6 ms, permitiendo que el reloj del receptor se sincronice con el del transmisor.

- El octeto de inicio del frame contiene el patrón 10101011 para denotar el inicio del mismo.

- En el campo de dirección de destino, el primer bit (el 47) es 0 a menos que indique que es dirección de grupo, en cuyo caso el bit es un 1. Las direcciones de grupo autorizan a múltiples estaciones a recibir el mensaje. Con todos los bits del destino en 1 se pretende una difusión completa, o transmisión promiscua, incluyendo los bridges.

- El bit 46 se emplea para distinguir las direcciones locales de las de naturaleza global. Las direcciones locales son asignadas por el administrador de red en cuanto las globales son asignadas por el IEEE para que no exista ningún duplicado en todo el mundo. Se espera que con 46 (48-2) bits, aproximadamente 7 x 1013 direcciones, no se produzcan duplicados, siendo problema de la capa de red el como encontrar la estación direccionada.

- El campo de datos puede tener entre 0 y 1.500 octetos. Se establece que un frame tiene como mínimo 64 octetos, por lo cual si un campo de datos es igual a cero, se utilizará el campo de relleno para mantener el mínimo de 64 octetos.

- Los 4 últimos octetos son para el código de redundancia cíclica o CRC de 32 bits calculado por el tx y verificado por el rx; aceptándose el frame si hay coincidencia entre el CRC recibido y el calculado.

El CSMA/CD no proporciona asentimiento, por lo que es necesario enviar un nuevo frame de confirmación desde el destino al origen.

8.4 NORMA IEEE 802.4: TOKEN BUS

Debido a problemas inherentes del CSMA/CD como la característica probabilística de su protocolo que podría hacer esperar mucho tiempo a un frame, o la falta de definición de prioridades que podrían requerirse para transmisiones en tiempo real, se ha especificado esta norma diferente. La idea es representar en forma lógica un anillo para transmisión por turno, aunque implementado en un bus, porque cualquier ruptura del anillo hace que la red completa quede desactivada. Por otra parte el anillo es inadecuado para una estructura lineal de casi todas las instalaciones.

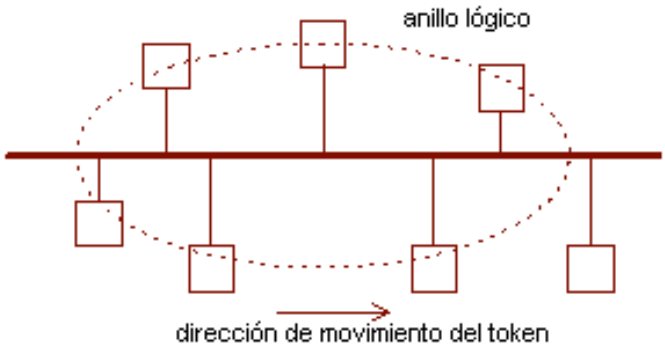


Fig. I.50: *Mecanismo de token bus.*

El token o testigo circula por el anillo lógico y sólo la estación que posee el testigo puede enviar información en el frame correspondiente. Además, cada estación conoce la

dirección de su vecino lógico para mantener el anillo.

El protocolo de subcapa MAC para 802.4 token bus se define de la manera siguiente:

Al iniciar el anillo, las estaciones se le introducen en forma ordenada, de acuerdo con la dirección de la estación, desde la más alta a la más baja. El testigo se pasa también desde la más alta a la más baja.

Para transmitir, la estación debe adquirir el testigo, el cual es usado durante un cierto tiempo, para después pasar el testigo en el orden adquirido. Si una estación no tiene información para transmitir, entregará el testigo inmediatamente después de recibirlo.

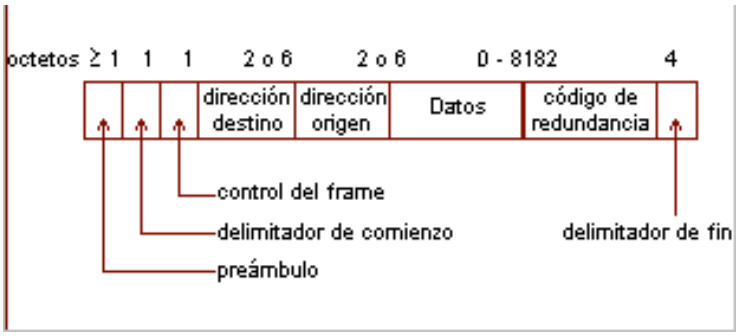


Fig. I.51: *Marco de la trama 802.4.*

La estructura del frame para un 802.4 es:

- El preambulo es utilizado para sincronizar el reloj del receptor.
- Los campos correspondientes a los delimitadores de comienzo y fin del frame contienen una codificación analógica de simbolos diferentes al 0 y 1, por lo que no pueden aparecer accidentalmente en el campo de datos.

8.5 NORMA IEEE 802.5, TOKEN RING

Una de sus características es que el anillo no representa un medio de difusión sino que una colección de enlaces punto a punto individuales. Fue seleccionada por la IBM como su anillo LAN.

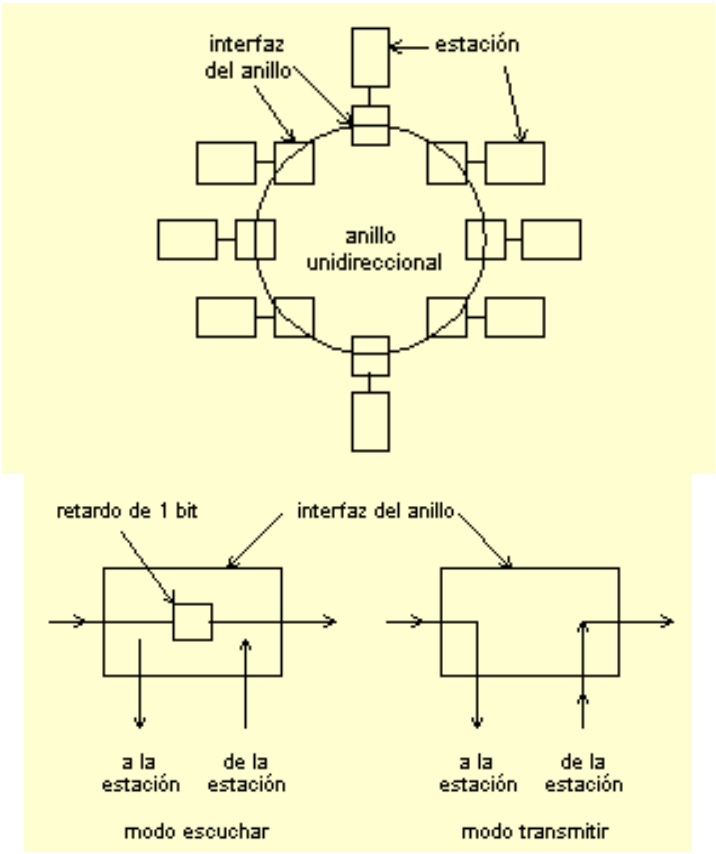


Fig. I.51: *Modo de operación de token ring.*

8.6 802.6 RED DE ÁREA METROPOLITANA MAN

Define un protocolo de alta velocidad en el cual las estaciones enlazadas comparten un bus doble de fibra óptica que utiliza un método de acceso llamado bus dual de cola distribuida o DQDB Distributed Queue Dual Bus.

DQDB es una red de transmisión de celdas que conmuta celdas con una longitud fija de 53 bytes, por lo tanto, es compatible con la ISDN de banda ancha ISDN-B y ATM. La conmutación de celdas tiene lugar en el nivel de control de enlaces lógicos 802.2.

8.7 802.7 GRUPO ASESOR PARA TÉCNICAS DE BANDA ANCHA.

Proporciona asesoría técnica a otros subcomités en técnicas de conexión de red de banda ancha.

8.8 802.8 GRUPO ASESOR PARA TÉCNICAS DE FIBRA ÓPTICA.

Proporciona asesoría técnica a otros subcomités en redes de fibra óptica como alternativa a las redes actuales basadas en cobre.

8.9 802.9 REDES INTEGRADAS PARA VOZ, DATOS Y VÍDEO.

Tanto para LANs 802 como para ISDNs. La especificación se denomina IVD Integrated Voice and Data, y el servicio proporciona un flujo multiplexado que puede llevar información de datos y voz por los canales que conectan las dos estaciones sobre cables de par trenzado de cobre.

8.10 802.10 SEGURIDAD DE RED.

Grupo que trabaja en la definición de un modelo normalizado de seguridad que interopere sobre distintas redes e incorpore métodos de autentificación y de cifrado.

8.11 802.11 REDES INALÁMBRICAS.

Comité que trabaja en la normalización de medios como la radio de amplio espectro, radio de banda angosta, infrarrojos y transmisiones sobre líneas de potencia.

8.12 802.12 LAN de acceso de prioridad bajo demanda (100VG-anylan).

Comité que define la norma ethernet a 100 Mbps con el método de acceso de prioridad bajo demanda propuesto por la Hewlett Packard y otros fabricantes. El cable especificado es un par trenzado de 4 hilos de cobre utilizándose un concentrador central para controlar el acceso al cable. Lass prioridades están disponibles para soportar la distribución en tiempo real de aplicaciones multimediales.

Los concentradores 100VG-AnyLAN controlan el acceso a la red con lo cual eliminan la necesidad de que las estaciones de trabajo detecten una señal portadora, como sucede en el CSMA/CD de la norma ethernet.

Cuando una estación necesita transmitir, envía una petición al concentrador, mientras que todas las transmisiones se dirigen a través del concentrador, que ofrece una

conmutación rápida hacia el nodo destino.

El emisor y receptor son los únicos involucrados en las transmisiones, a diferencia del CSMA/CD donde la transmisión es difundida por toda la red. Si múltiples peticiones de transmisión llegan al concentrador, primero se sirve la de mayor prioridad, y si dos estaciones de trabajo hacen la solicitud con la misma prioridad y al mismo tiempo, se van alternando para darles servicio. Este método de trabajo es mejor que CSMA/CD.

9. TÉCNICAS DE TRANSMISIÓN

En este apartado se va a analizar cómo se transmiten los datos de las estaciones de la red al medio físico. En las redes de área local se utilizan principalmente dos modalidades: **Transmisión en Banda Base** y **Transmisión en Banda Ancha**.

En **Banda Base**, la transmisión se realiza de forma *digital*, sin emplear técnicas de modulación. En **Banda Ancha**, la señal digital se *modula* y seguidamente se envía al medio.

La técnica de transmisión empleada implica diferencias en la forma de *multiplexar* el medio entre las diferentes estaciones y también en la forma de codificar la señal.

En la actualidad, la técnica dominante en las redes de área local es la de Banda Base.

9.1. REDES DE BANDA BASE

En las redes de banda base, la señal se transmite sin modulación. En consecuencia, cada vez que se realiza una transmisión se utiliza *todo el ancho de banda del medio*. Por ello, debe emplearse técnicas de *medio compartido* para que éste pueda ser utilizado por múltiples estaciones. La ventaja fundamental de la transmisión en banda base es su sencillez, puesto que no requiere moduladores/demoduladores. La contrapartida es que, debido a la distorsión de la señal digital con la distancia, se requiere el empleo de **repetidores** para regenerar la señal a partir de una cierta distancia, que depende del tipo de medio utilizado, del tipo de red y de la velocidad de transmisión.

La señal es transmitida secuencialmente al medio en forma de *trenes de bits "1"* y *"0"*. Si se hace corresponder un nivel de voltaje con un *"1"* y otro nivel con *"0*", existe el inconveniente de que no se producen transiciones en la red cuando se envían corrientes de *"1"* o corrientes de *"0"*. Ello dificulta la recuperación de la señal por parte del receptor, dado que no hay ninguna indicación de cuándo comienza y cuándo termina un bit, al no haber cambios de nivel en la señal. Esta circunstancia hace que se pueda perder la *sincronización* entre el emisor y el receptor, con lo que la información recibida es errónea. Para resolver el problema de la sincronización, es necesario establecer algún mecanismo que permita que se produzcan siempre transiciones independientemente de la secuencia de bits transmitidos. Uno de los sistemas más utilizados es el denominado **codificación Manchester**. En la figura se representan dos ejemplos de codificación *Manchester*. En la codificación de *Manchester básica*, un bit *"0"* se representa por una transición de nivel alto a nivel bajo en medio del intervalo, mientras que un *"1"* se representa por una transición de nivel bajo a nivel alto en medio del intervalo. En la codificación de *Manchester diferencial*, un *"0"* se identifica por la presencia de una transición al comienzo del intervalo, mientras que un *"1"* por ausencia de transición al comienzo del intervalo. Además, siempre debe haber una transición en medio

del intervalo.

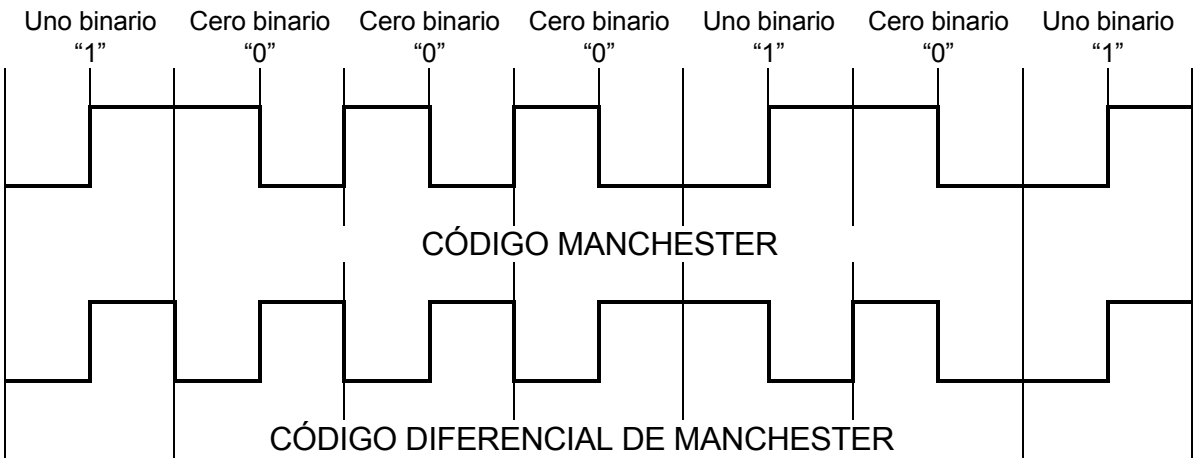


Fig. 1.: *Codificación Manchester.*

Como se ha visto, la codificación de Manchester resuelve el problema de la sincronización, generando transiciones con independencia de la corriente de bits emitida. Sin embargo, el número de transiciones que tiene lugar es el doble de la velocidad de transmisión expresada en bits. Por ello, este tipo de codificación se emplea hasta velocidades del orden de *16 Mbps* (es decir **32 Mbaudios**). Para velocidades de *100 Mbps* o superiores se emplean técnicas de codificación más eficientes.

9.2. REDES DE BANDA ANCHA

Las redes de banda ancha utilizan señales analógicas moduladas. Normalmente, el medio utilizado es un *cable coaxial* de *75 ohmios* de impedancia característica, similar al utilizado en la toma de antena de un televisor. Las frecuencias de transmisión suelen alcanzar los *300* ó *400 MHz*. El ancho de banda total del cable se puede dividir, mediante técnicas *de multiplexación por división de frecuencias* (**FDM**), en grupos de canales de banda más estrecha. Cada uno de estos canales puede ser utilizado independientemente para un determinado tipo de servicio. Así, un canal de TV tiene un ancho de banda del orden de 6 MHz y una red de datos que opere a 10 Mbps ocupa un ancho de banda del orden de 18 MHz. En la figura se representa un esquema de multiplexación por división de frecuencia. Cada canal es independiente de los otros canales de distinta frecuencia; pueden proporcionar distintos servicios, utilizar distintos métodos de acceso o transmitir a distinta velocidad. Cuando dos o más canales tienen el mismo tipo de operación, si bien a distinta frecuencia, pueden interconectarse mediante unos dispositivos denominados puentes de banda ancha. En el caso de una red de área local, cada canal, conceptualmente, puede ser considerado como

una red independiente.

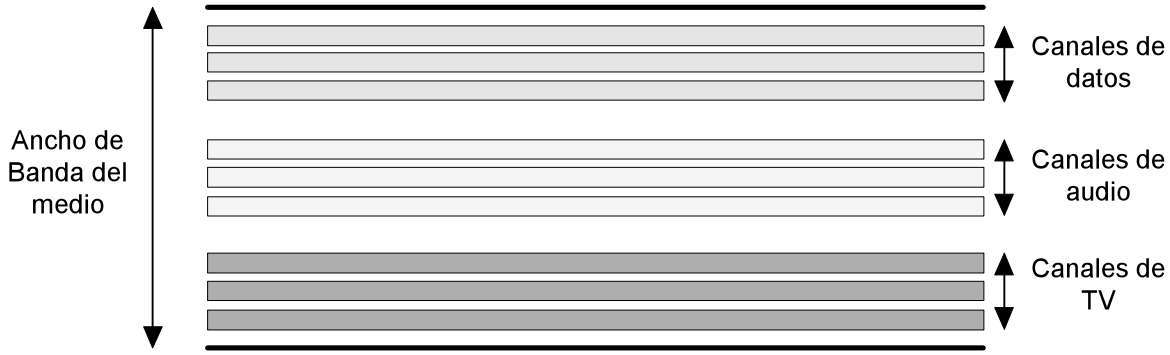


Fig. 2: *Multiplexación por división de frecuencia.*

En resumen, las ventajas principales de las redes de banda ancha son la posibilidad de integrar todo tipo de señales en un solo medio y la gama de distancias que pueden abarcar. Sin embargo, la utilización de modems entraña un coste superior y una planificación e instalación de la red más elaborados.

10. CONTROL DE ACCESO AL MEDIO

Las redes locales se componen de un conjunto de dispositivos que deben compartir la capacidad de transmisión de la red a la que se encuentran conectados. Por tal motivo, para evitar conflictos y errores, se hace necesario algún **método de control de acceso** al medio de transmisión.

El *protocolo de control de acceso al medio* es el factor que más caracteriza el funcionamiento de una red de área local. De él dependen parámetros básicos en la evaluación de una red como son el rendimiento, fiabilidad, disponibilidad y la gestión de la red:

- **Rendimiento:** depende del grado de aprovechamiento del medio, su capacidad para repartir el derecho de acceso y la resolución de los conflictos de acceso.

- **Fiabilidad**: el protocolo debe proporcionar los mecanismos necesarios para asegurar un servicio continuo sin errores y debe ser capaz de detectar y corregir situaciones anómalas.

- **Disponibilidad**: la oportunidad de acceso debe estar en todo momento bien repartida entre todas las estaciones conectadas a la red.

- **Gestión de red:** aspectos como la reconfiguración de la red, gestión de nodos

con prioridades, direccionamiento a todas las estaciones (broadcasting), etc, deberían estar incluidos en el método de acceso.

Las características básicas que permiten proporcionar una primera clasificación de las técnicas de acceso al medio son: el "*dónde*" y el "*cómo*". El "*dónde*" hace referencia al tipo de control, que puede realizarse de forma centralizada o descentralizada. En un esquema centralizado una estación garantiza el derecho de acceso a la red. La estación que desee transmitir debe esperar hasta que reciba permiso de la estación maestra. En una red de control distribuido el conjunto de estaciones realiza colectivamente la función de control de acceso al medio para determinar dinámicamente el orden de transmisión.

Las principales ventajas del esquema centralizado son:

- Permite mayor **control** sobre el acceso.
- Se facilita la **gestión** de la red (asignación de prioridades y resolución de conflictos).
- La **lógica** de las estaciones, excepto en la estación maestra, es lo más sencilla posible.

Entre sus inconvenientes destacan:

- Se trata de una red muy **vulnerable** (la funcionalidad de la red está muy localizada).
- La estación controladora puede actuar como cuello de botella, reduciendo la **eficiencia** de la red.

Los pros y los contras del *control centralizado* son, respectivamente, las desventajas y ventajas del *control distribuido*.

En relación al "*cómo*", los métodos de acceso pueden clasificarse en dos grandes grupos: **compartición** y **repartición** del medio.

Los *métodos de repartición del medio* son procedimientos **estáticos**. Se dedica una capacidad fija a una conexión. No son adecuados para redes de área local, debido a que la demanda de las estaciones es, por lo general, impredecible. Es preferible tener la posibilidad de asignar la capacidad de forma dinámica, en función del tráfico, como se hace en los *procedimientos de compartición.*

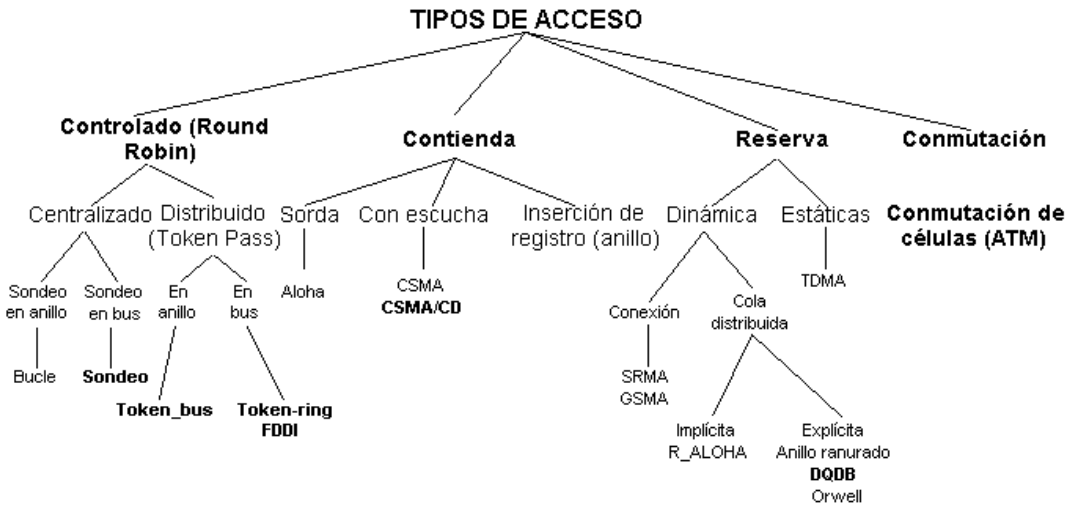


Fig. 3: *Tipos de métodos de acceso.*

Los *métodos de compartición* más utilizados en la actualidad son **CSMA/CD**, perteneciente a las técnicas de **contienda** y **paso de testigo en anillo**, en el grupo de las técnicas **controladas**. También se consideran los métodos de **reserva**, por una parte, para mantener la clasificación tradicional, y por otra para incluir el procedimiento denominado ***DQDB*** *(Distributed Queue Dual Bus*) utilizado en redes *MAN*.

10.1. CONTROLADO o ROUND ROBIN

Las técnicas de **Round Robin** son conceptualmente simples, basadas en la filosofía de conceder a cada uno su oportunidad. Cada estación, por turno, recibe el permiso de transmitir. Durante esta oportunidad la estación puede declinar transmitir, o bien transmitir sujeta a ciertos límites superiores, generalmente expresados en cantidad máxima de tiempo. En cualquier caso, la estación, cuando finaliza, debe ceder su turno, pasando el derecho de transmisión a la siguiente estación dentro de la secuencia lógica de estaciones.

El control de los turnos puede estar **centralizado** o **distribuido**. El **sondeo** o **polling** es un ejemplo de *técnica centralizada*. Las **técnicas de paso de testigo** pertenecen al grupo de *métodos distribuidos*.

10.1.1. CONTROL CENTRALIZADO: SONDEO

La técnica de sondeo es un método ampliamente utilizado en las tradicionales redes

WAN. Se fundamenta en la relación maestro esclavo entre el nodo central y las demás estaciones del anillo o bus.

En el caso de la topología en anillo (bucle), para que un nodo pueda transmitir debe recibir permiso del nodo central a través de un mensaje de "sondeo". Este permiso se va pasando secuencialmente de estación en estación a lo largo de toda la red. La estación puede transmitir cuando recibe permiso. Al finalizar su transmisión pasa el permiso a la estación siguiente. El inconveniente de esta técnica reside en la necesidad de que la comunicación entre dos nodos cualquiera pase por la estación central.

En el caso de la topología en bus (típica de las redes multipunto), la estación central pregunta, por turnos, a cada estación subordinada, si tiene algún mensaje para enviar; en caso afirmativo, la estación subordinada, recibe permiso para enviar la información a la estación central que, a su vez, la transmite hacia la estación destino. Durante esta transacción la estación subordinada también recibe los datos que pudieran estar destinados a ella. Este mismo nodo, para volver a transmitir, ha de esperar a ser interrogado de nuevo.

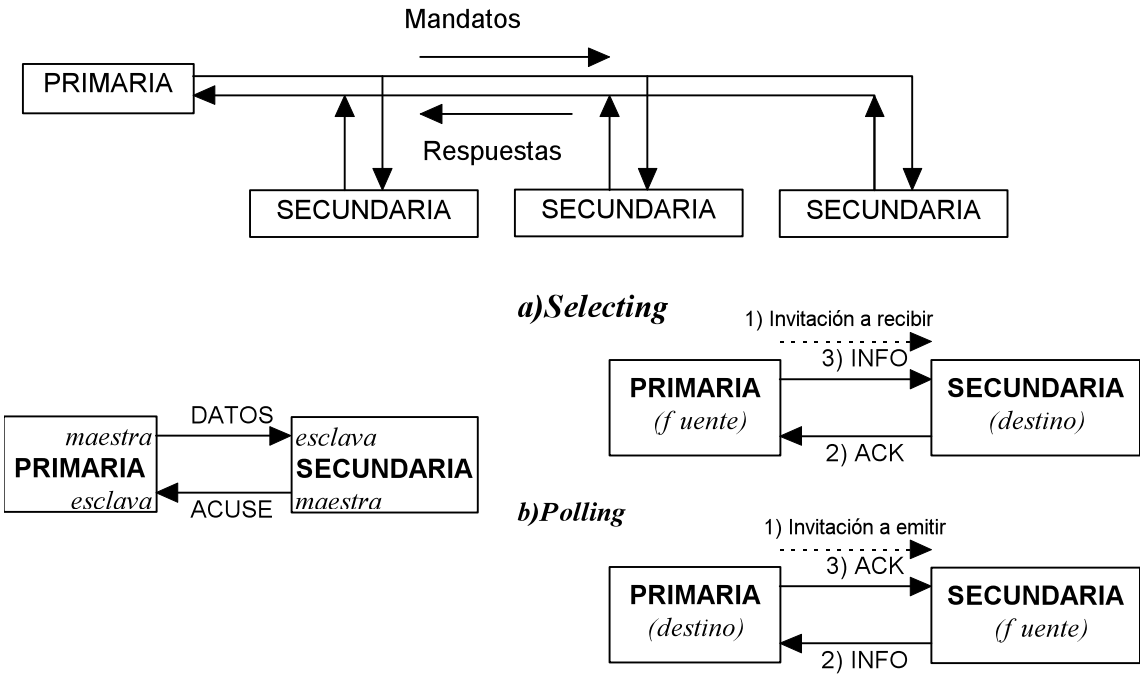


Fig. 4 : *Configuración típica de un Sondeo en topología bus, y modos de operación (comunes a las topologías bus y anillo): a) Selecting (selección) y b) Polling (sondeo).*

La diferencia con la técnica anterior estriba en que es necesario transmitir un mensaje para cada nodo, ya que si se realizase con un mensaje de "*sondeo*" para todas las estaciones podría causar colisiones en las respuestas. Se trata de un sistema sencillo de llevar a la práctica, no se producen conflictos entre estaciones que desean transmitir y es fácil establecer prioridades entre estaciones haciendo que las de mayor prioridad sean interrogadas con mayor

frecuencia. No obstante, como estructura centralizada que es, se halla expuesta a los inconvenientes que plantea el fallo de la estación central y la interrogación de un número elevado de estaciones puede hacer que la espera entre turnos para una estación sea excesivamente larga.

Este método de control solía emplearse en redes locales de corto alcance, con pocos puestos de trabajo y con una baja frecuencia de transacciones.

Estos dos métodos expuestos no responden realmente al planteamiento de las redes de área local. En realidad, son sistemas que se utilizaban como control de dispositivos. Su mención, sin embargo, merece interés y además servirá como punto de partida y de comparación con otras técnicas propias de las LAN.

10.1.2. CONTROL DISTRIBUIDO

Este método puede considerarse como una forma de interrogación distribuida en la que todas las estaciones de la red intervienen en la circulación de un paquete especial de información que recibe el nombre de **testigo** (*token*) y que indica, a la estación que lo recibe, que tiene a su disposición el medio para efectuar una transmisión. Este método de acceso es aplicable tanto a las *topologías en anillo* como a las *topologías en bus*.

10.1.2.A. PASO DE TESTIGO EN BUS (TOKEN BUS)

En esta técnica las estaciones del *bus* o *árbol* forman un **anillo lógico**, es decir, a las estaciones se les asigna una posición lógica en una secuencia ordenada y circular. Cada estación conoce la identidad de su estación antecesora y de su sucesora en el anillo lógico. La ordenación física de las estaciones en el bus es irrelevante e independiente de la ordenación lógica.

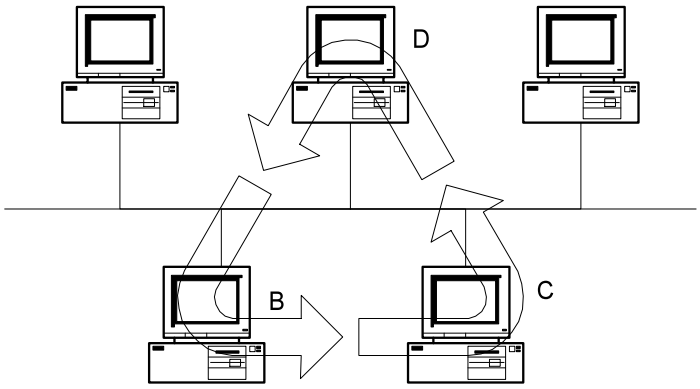


Fig. 5: *Ejemplo de paso de testigo en bus.*

En la figura se muestra un ejemplo de esta técnica. Las estaciones **B**, **C** y **D** están inscritas en un anillo lógico por donde circula el testigo; por tanto, pueden enviar y recibir información. Las estaciones **A** y **E** están excluidas y no pueden enviar información, sin embargo, pueden seguir recibiéndola gracias a las características de la topología bus.

Como se ha indicado anteriormente, una *trama de control*, *testigo* o *token*, regula el derecho de acceso. La estación que recibe el testigo tiene garantizado el derecho de acceso al medio para transmitir. Una vez que haya finalizado su transmisión o expire el tiempo asignado, pasa el testigo a las estación siguiente en la secuencia lógica.

Como puede observarse, el estado normal de operación es una alternancia de fases de *transferencia de información y transferencia de testigo*. Las estaciones que no necesitan transmitir información pueden seguir conectadas a la red captando todas las transmisiones, si bien quedan excluidas del anillo lógico. Esta técnica requiere un gran esfuerzo de mantenimiento. Una o más estaciones deben realizar, como mínimo, las siguientes funciones:

- **Iniciación del anillo**: cuando se arranca la red o se recupera de un fallo de funcionamiento, el anillo debe iniciarse. Se necesita, en consecuencia, un algoritmo descentralizado que decida el orden de iniciación.

- **Adición al anillo**: periódicamente debe concederse la oportunidad a las estaciones no participantes de insertarse en el anillo.

- **Eliminación del anillo**: una estación debe ser capaz de retirarse del anillo.

- **Recuperación de errores**: como direcciones duplicadas o rotura del anillo.

Su cualidad primordial es el rendimiento que se incrementa a medida que aumenta la tasa de datos hasta alcanzar un nivel de equilibrio, sin llegar a desestabilizarse con la

saturación del medio. Otra ventaja es la posibilidad de establecer prioridades en el acceso al medio, ya que es posible proporcionar tanto un esquema de acceso equitativo como un esquema de acceso con prioridades, el cual puede ser necesario en aplicaciones transaccionales o de tiempo real.

Por último, cabe destacar que se trata de un método de acceso determinativo, es decir, existe un límite superior para la cantidad de tiempo que una estación debe esperar antes de obtener el derecho de acceso. Este límite es conocido porque cada estación en el anillo lógico sólo puede poseer el testigo durante un tiempo máximo determinado. Esta característica, junto con su flexibilidad, hacen que este método se utilice para la automatización de procesos industriales (entornos **MAP**, *Manufacturing Automation Protocol*).

Entre sus desventajas cabe citar su complejidad y la infrautilización del ancho de banda con el paso de testigo en casos de baja carga del sistema.

10.1.2.B. PASO DE TESTIGO EN ANILLO (TOKEN RING)

Posiblemente constituya la técnica de control de acceso para topología en anillo más antigua, propuesta en su forma original en *1969* y conocida como **Newhall Ring**. Este método ha sido normalizado por el **Comité de Normalización para LAN IEEE 802** y ha saltado a un primer plano tras haber recibido el respaldo de **IBM**.

Esta técnica, al igual que la de *paso de testigo en bus*, se basa en una pequeña trama, testigo o *token* que circula a lo largo del anillo. Un *bit* indica su estado: **libre** u **ocupado**. Cuando ninguna estación transmite, el testigo simplemente circula por el anillo pasando de una estación a la siguiente. Una estación que desee transmitir debe esperar a recibir el testigo; entonces modifica el estado del mismo de *libre* a *ocupado,* e inserta a continuación la información a enviar junto con su propia dirección a la de destino. El paquete de datos así modificado prosigue su circulación por el anillo hasta llegar a la estación receptora, que copia su contenido y lo vuelve a poner en circulación. Cuando el paquete vuelve a llegar a la estación emisora, ésta lo retira de la red y genera un nuevo testigo libre.

En la figura se muestra un ejemplo de esta técnica. En un momento dado **(1)** el testigo pasa del nodo **A** al **B**. **B** desea enviar información al nodo **D**, **(2)**, para lo que modifica el testigo y hace circular la información por el anillo a través de **C**. Posteriormente **(3)**, **D** copia la información, le añade la marca de recepción y la reenvía a **B** a través de **A**. Por último **(4)**, **B** retira la información, genera un nuevo testigo y lo vuelve a poner en circulación.

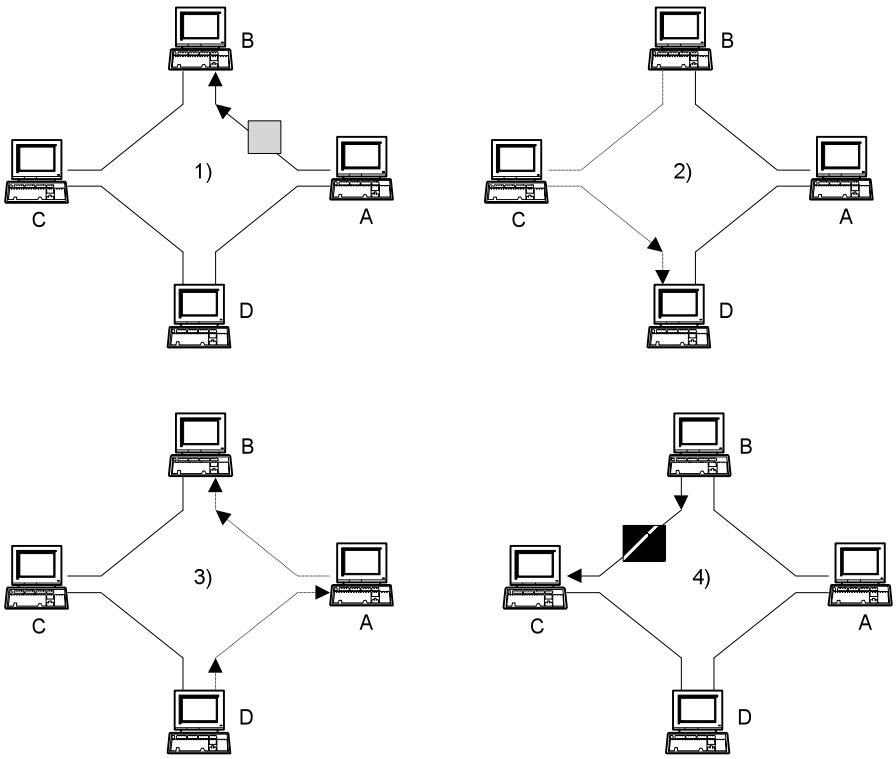


Fig. 6: *Ejemplo de paso de testigo en anillo.*

De manera análoga a la técnica de paso de testigo en bus son necesarias funciones de mantenimiento del anillo. Estas funciones, entre las que se incluyen las de **supervisión del testigo**, **determinación y recuperación de errores**, existen en todas las estaciones, pero sólo una actúa como *monitor activo*, mientras que las demás estaciones permanecen como monitores pasivos a la espera de posibles averías en el monitor activo.

La principal ventaja del *paso de testigo en anillo* es el elevado rendimiento, superior incluso al de *paso de testigo en bus*. Su adaptación, de forma natural, a la topología en anillo por su característica de medio unidireccional, mejora sensiblemente su eficiencia en relación al método *token-bus*. Otro de los beneficios lo constituye la garantía de un reparto equitativo de la red entre todas las estaciones, asimismo es posible establecer mecanismos de prioridades.

Entre sus desventajas se encuentran la disminución de la eficiencia en caso de baja carga de sistema debido a la circulación del testigo y su relativa complejidad en relación con los procedimientos de contienda.

10.2 CONTIENDA

En este tipo de técnicas un nodo es libre de lanzar sus mensajes en cualquier momento, sin estar seguro de que ningún otro dispositivo está intentando transmitir simultáneamente. Cuando dos o más estaciones intentan ocupar el canal al mismo tiempo, se produce una **colisión** (interferencias provocadas por la transmisión simultánea) entre los mensajes que estaban siendo emitidos. Acto seguido se desencadena un proceso o *algoritmo de contienda* para resolver la posesión del medio.

Los métodos de contienda pueden clasificarse en **técnicas con o sin *escucha*** *(transmisión sorda*), según si poseen o no información del estado del canal (*libre* u *ocupado*). Normalmente esta escucha se efectúa por detección de la presencia de la señal, tomando el nombre de técnicas de **Acceso Múltiple por Detección de Portadora** (**CSMA**. *Carrier Sense Multiple Access*).

En un segundo nivel, las técnicas de contienda pueden clasificarse en **troceadas** y **no troceadas** (*slotted* - *unslotted*). Este troceado puede ser **de paquete** o **de retardo**, diferenciándose en el intervalo (*slot*) que toman como referencia para dividir el tiempo con vistas a la transmisión de los paquetes.

- **Troceado de paquete**. En las técnicas en las que se emplea el *troceado de paquete*, el tiempo se divide en intervalos iguales de un tamaño correspondiente a la duración de un paquete (cuya longitud ha de ser fija). Los dispositivos deben estar sincronizados con un *reloj maestro* que marca los intervalos. Cuando una estación tiene un paquete para transmitir, espera al principio del siguiente intervalo y si actúa sin escucha (*técnica sorda*) procede a la transmisión.

- **Troceado de retardo**. Los métodos que hacen uso de este troceado dividen el tiempo en intervalos, llamados *T-slots*, cuya duración es igual al retardo máximo de propagación extremo a extremo del canal. Los dispositivos se encuentran también sincronizados respecto a un *reloj maestro*. El troceado con retardo se utiliza en las técnicas con escucha donde dicho retardo incide en la decisión a tomar de si el canal está libre o no. A diferencia de lo que ocurre en el troceado de paquete, la longitud de éste puede ser variable.

10.2.1 ACCESO ALEATORIO

10.2.1.A. TRANSMISIÓN SIN ESCUCHA

El primero de los *métodos de acceso aleatorio,* denominado **ALOHA** o **ALOHA puro**, fue desarrollado para la comunicación de terminales dispersos con un ordenador central, vía satélite. Sin embargo, es aplicable a cualquier medio de transmisión compartido por un conjunto de usuarios no coordinados. El protocolo utilizado era simple: transmitir el mensaje en cuanto hubiera uno preparado para ello. A continuación, la estación escucha el

medio durante un período de tiempo igual al doble del tiempo de propagación entre las dos estaciones más separadas; si recibía reconocimiento de la transmisión, ésta había ido bien, de lo contrario reenviaba la trama. Después de repetidos intentos abandonaba. La trama puede considerarse inválida debido al ruido del canal o porque otra estación haya transmitido al mismo tiempo. En este último caso se produce una condición de error en la red denominada "*colisión*".

El método *ALOHA* es muy sencillo, y paga una penalización por ello. Dado que el número de colisiones aumenta muy rápidamente al incrementarse la carga del sistema, la utilización máxima del canal es solo del *18%.* Con el objeto de mejorar esta eficiencia se modificó el método *ALOHA* mediante el método *ALOHA ranurado*, dividiendo el tiempo de transmisión del canal en intervalos fijos de duración igual al tiempo de transmisión de la trama, y permitiendo transmitir únicamente al principio de uno de estos intervalos. De esta forma se alcanza un rendimiento del *36 %.* La técnica *Aloha ranurado* se suele denominar también *Aloha-S*. Es interesante comentar que ha vuelto a cobrar actualidad por su utilización en telefonía móvil en el ámbito de oficinas, campus o recintos.

10.2.1.B. TRANSMISIÓN CON ESCUCHA

Ambos métodos *ALOHA* y *ALOHA ranurado*, exhiben una pobre utilización. Ninguno de ellos se beneficia de una de las principales ventajas de las redes locales de velocidad inferior a *10 MBps*: el retardo de propagación entre estaciones es generalmente muy pequeño comparado con el tiempo de transmisión de la trama. Considérense las siguientes observaciones. Si el tiempo de propagación entre estaciones es grande comparado con el tiempo de transmisión de la trama, entonces, después de que una estación emita una trama, pasará un período de tiempo prolongado hasta que otra estación detecte tal transmisión. Durante este tiempo puede transmitir cualquier otra estación. Se tendrá, por lo tanto, una *colisión* en la red. Supongamos, sin embargo, que el tiempo de propagación es muy pequeño comparado con el tiempo de transmisión de la trama. En este caso, la emisión de una trama por parte de una estación es conocida casi instantáneamente por las demás estaciones. De esta manera, si las estaciones dispusieran de alguna forma de detectar el estado de la red, no intentarían transmitir hasta que la primera estación hubiera finalizado. Las colisiones serían menores y solo se darían en el caso de que dos estaciones comenzaran a transmitir casi simultáneamente.

Las anteriores observaciones llevaron al desarrollo de la técnica conocida como **acceso múltiple con detección de portadora** (**CSMA**, *Carrier Sense Multiple Access*) o **escuchar antes de hablar** (**LBT**, *Listen Before Talk*). Una estación que desee transmitir, escucha primero el medio para determinar si hay otra transmisión en progreso. Si es así, la estación tras un período de espera, lo vuelve a intentar, siguiendo uno de los algoritmos que se describen posteriormente. Si el medio está libre, la estación transmite; ahora bien, puede suceder que dos o más estaciones intenten transmitir casi al mismo tiempo. Se producirá en

este caso una colisión. Para tratar esta situación, tras transmitir, la estación espera la confirmación, durante un período de tiempo razonable, teniendo en cuenta el retardo máximo de propagación de la red y el hecho de que la estación que tiene que emitir la confirmación debe, también, competir por el canal para responder. Si no hay confirmación, la estación emisora asume que se ha producido una colisión y retransmite.

La utilización máxima usando *CSMA* excede con diferencia a la de *ALOHA* y *ALOHA ranurado*. Esta utilización depende de la longitud de la trama y del tiempo de propagación. Cuanto mayores son las tramas o menor es el tiempo de propagación, mayor es la utilización.

En la técnica *CSMA* se hace necesario un algoritmo que especifique lo que debe hacer una estación si encuentra el medio ocupado. Existen tres posibles alternativas. Una de éstas es el algoritmo *CSMA no-persistente*. La estación que desea transmitir escucha el medio y sigue las siguientes reglas:

1) Si el medio está libre transmite.

2) Si el medio está ocupado, espera durante un período de tiempo extraído de una distribución de probabilidad (retardo de transmisión) y vuelve al paso 1).

La utilización de tiempos de retransmisión aleatorios reduce la probabilidad de colisiones. La desventaja reside en que, aunque haya varias estaciones preparadas para transmitir, es probable que exista un período de tiempo durante el cual el medio permanece ocioso después de la transmisión.

Para evitar este período de inutilización se emplea el protocolo **1-persistente**. En este caso las estación que quiere transmitir escucha el medio y:

1) Si el medio está libre transmite.

2) Si el medio está ocupado continua escuchando hasta que esté disponible, entonces transmite inmediatamente.

3) Si se produce una colisión, reconocida por la inexistencia de confirmación, espera durante un período de tiempo aleatorio y vuelve al paso 1).

La tercera técnica, **CSMA p-persistente**, es un compromiso entre reducir las colisiones, como el *no-persistente*, y reducir el período de tiempo ocioso del medio, como *1-persistente*. Sus reglas son las siguientes:

1) Si el medio está libre transmitir con probabilidad **p** y con probabilidad **(1-p)** retrasar la transmisión una unidad de tiempo. Esta unidad, generalmente, es igual

al retardo máximo de propagación.

2) Si el medio está ocupado, continúa a la escucha hasta que el canal esté libre y vuelve al paso 1).

3) Si la transmisión se retrasa en un unidad de tiempo vuelve al paso 1).

La cuestión ahora es determinar el valor más efectivo de **p**. El problema básico es evitar la inestabilidad de la red en condiciones de alto tráfico. Consideremos el caso en que **n** estaciones tengan tramas para enviar mientras está teniendo lugar una transmisión. Al final de esta transmisión el número de estaciones que intentan transmitir es **np**. Si **np** es mayor que **1** serán varias las estaciones que transmitan y se producirá una colisión; y lo que es más, tan pronto como estas estaciones se den cuenta de que ha habido una colisión, lo intentarán de nuevo, provocando así más colisiones. Además, estos reintentos competirán con las nuevas transmisiones de las otras estaciones, incrementándose la probabilidad de colisión. Finalmente, todas las estaciones estarán intentando transmitir, provocando continuas colisiones y haciendo que el rendimiento descienda drásticamente. Para evitar esta catástrofe, el producto **np** debe ser **menor** que **1**, para el caso del pico de carga de **n**. A medida que **p** disminuye se reducen las colisiones, pero aumenta el tiempo de espera de las estaciones.

10.2.1.C. CSMA/CD (CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION)

La técnica **CSMA**, aunque más eficiente que *ALOHA* y *ALOHA ranurado*, presenta una manifiesta ineficiencia. Cuando dos tramas colisionan, el medio permanece sin usar mientras dura la transmisión de las tramas afectadas. En el caso de tramas largas en comparación con el tiempo de propagación, la cantidad de ancho de banda desperdiciado es considerable. Es posible reducir este tiempo de ociosidad del medio si la estación se mantiene escuchando el canal mientras transmite (**detección de colisión**). En este caso se añaden las siguientes reglas a las de CSMA:

1) Si se detecta una colisión durante la transmisión, esta cesa inmediatamente y se transmite una pequeña trama de **consenso de colisión** (trama de *jam*) para asegurarse de que todas las estaciones se han enterado de la existencia de la colisión.

2) Después de emitir la señal de *jam* se intenta transmitir, tras esperar un período de tiempo aleatorio, usando, de nuevo, *CSMA*.

En la figura se representa la operación de la técnica **CSMA/CD**:

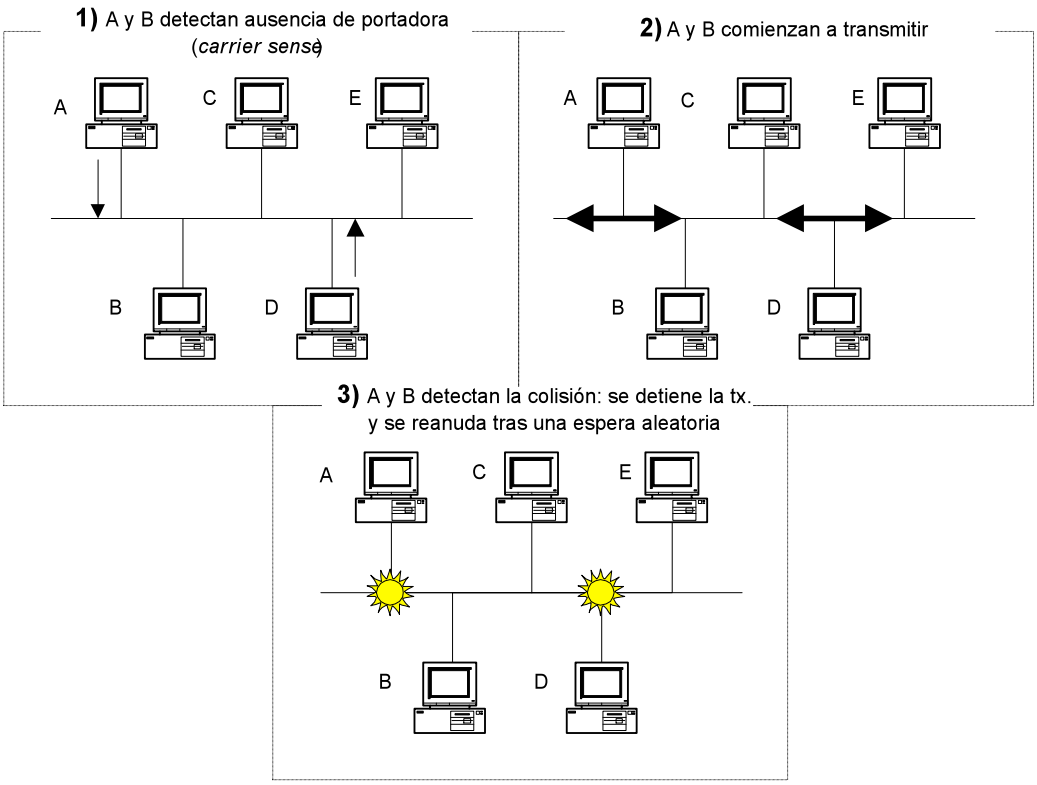


Fig. 7: *Acceso CSMA/CD*

Cuanto mayor sea la longitud de la red, mayor será el número de colisiones y menor el rendimiento, debido a que el tiempo requerido para detectar colisiones es mayor. La cuestión, ahora, es evaluar este tiempo. La figura siguiente ilustra la respuesta para el caso de sistemas banda base. Consideremos el caso peor: dos estaciones separadas a la mayor distancia posible. Como puede observarse, el tiempo en detectar una colisión es igual a dos veces el retardo de propagación. Se deduce, también, la necesidad de utilizar tramas lo suficientemente grandes como para permitir la detección de la colisión antes de que finalice la transmisión. En la mayoría de los sistemas que utilizan *CSMA/CD* se requiere que todas las tramas sean como mínimo de esa longitud.

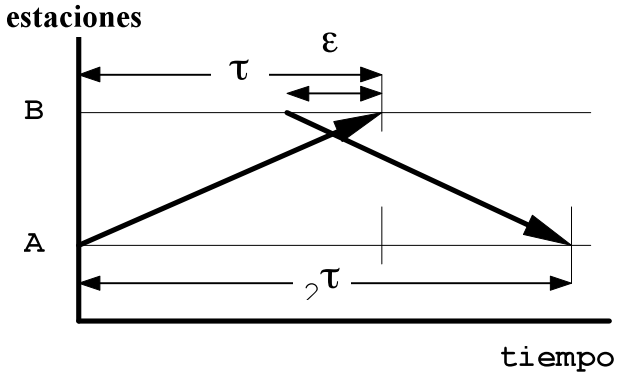


Fig. 8: *Detección de colisión.*

Es interesante analizar qué algoritmo de persistencia se emplea en el caso de *CSMA/CD*. Puede resultar sorprendente la elección de la técnica *1-persistente*. Tanto *Ethernet* como *IEEE 802* utilizan este algoritmo. Las técnicas *no-persistente* y *p-persistente* presentan problemas de rendimiento. En el caso del *no-persistente* la capacidad del medio se ve desperdiciada debido a que éste generalmente permanece ocioso tras una transmisión, aunque haya estaciones esperando transmitir. En el caso del *p-persistente*, *p* debe ser lo suficientemente bajo como para evitar la inestabilidad, lo que conlleva, en ocasiones, enormes retrasos en condiciones de poco tráfico.

El algoritmo *1-persistente*, que después de todo significa *p=1*, podría parecer incluso más inestable que el *p-persistente*, debido a la "codicia" de las estaciones por transmitir. Lo que le salva de caer en la inestabilidad es que el tiempo desperdiciado debido a una colisión es corto (si las tramas son grandes en relación con el tiempo de propagación) y que, con el algoritmo de resolución de colisiones denominado "*random backoff*", es improbable que dos tramas involucradas en una colisión vuelvan a colisionar en los próximos intentos. Para asegurarse de que el *backoff* mantiene la estabilidad, *IEEE 802.3* y *Ethernet* utilizan la técnica denominada "*binary exponential backoff*". Una estación intentará transmitir repetidamente en caso de colisión, pero después de cada colisión se dobla el valor medio del retraso aleatorio, y tras *16* intentos abandonará e informará del error.

El algoritmo *1-persistente* presenta una gran ventaja, el mantener su eficiencia en una amplia variedad de características de tráfico. En el caso de tráfico bajos garantiza que una estación pueda disponer del canal tan pronto como este quede libre, en contraste con las técnicas *no-persistente* y *p-persistente*. Con tráficos elevados es tan estable como las otras técnicas. Como desventaja, debida al algoritmo de *backoff*, indicar el efecto "*último en llegar, primero en salir*" (*last-in, first-out*): las estaciones sin colisiones o con muy pocas, dispondrán de la oportunidad de transmitir antes que estaciones que han esperado más tiempo.

Entre las ventajas merece la pena destacar la simplicidad del algoritmo. Esto supone una implementación sencilla, de bajo coste y alta fiabilidad, aspectos éstos sobre los que también redunda el hecho de tratarse de una técnica muy utilizada y suficientemente probada. Proporciona, además, un acceso equitativo a la red y exhibe, como se verá posteriormente, un

buen rendimiento hasta una determinada carga.

Presenta también inconvenientes: resulta difícil, para los equipos de diagnóstico distinguir entre errores esperados, por ejemplo, procedentes de colisiones, y aquellos inducidos por ruido o fallos. La detección de colisiones impone un tamaño mínimo de trama, lo que supone la infrautilización del ancho de banda en situaciones donde predominan los mensajes cortos, como pueden ser entornos altamente interactivos. La característica de acceso equilibrado representa un inconveniente en entornos que se pretendan gestionar en función de prioridades. En cuanto al rendimiento, *CSMA/CD* presenta un rendimiento pobre a medida que la carga del sistema y la longitud de las red se incrementan.

La técnica *CSMA/CD* es el método de acceso al medio más utilizado. La versión original para banda base fue desarrollada y patentada por **Digital**, **Intel** y **Xerox** (**DIX**) como parte de su red local *Ethernet*.

10.2.2. INSERCIÓN DE REGISTRO

Aunque el método de acceso a un anillo sea intrínsecamente controlado, también pueden establecerse *métodos controlados con estrategias de contienda*. Éste es el caso de la técnica de **inserción de registro**, que se ha clasificado dentro de los métodos de acceso *aleatorio* porque cumple la premisa básica de estos tipos de técnicas: el acceso al medio se realiza por decisión propia de la estación.

En cada estación se utilizan, como puede observarse en la figura, dos registros: un **registro de desplazamiento**, conectado en serie al anillo, de tamaño igual a la máxima longitud de la trama, utilizado para almacenar temporalmente las tramas que circulan por la red, y un **buffer** para almacenar las tramas generadas por la propia estación.

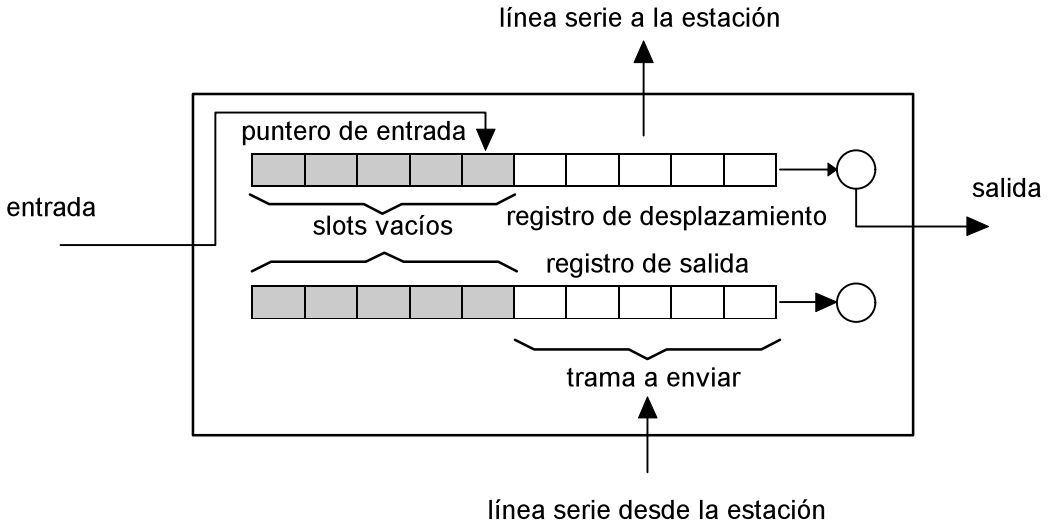


Fig. 9: **Ejemplo de inserción de registro.**

Considérese, en primer lugar, el caso en que la estación no tiene nada que transmitir; en esta situación trata únicamente la información procedente del anillo. Cuando el anillo está inactivo, el puntero de entrada señala la posición situada más a la derecha del registro de desplazamiento, indicando así que está vacío. Cuando llegan datos del anillo, éstos se insertan bit a bit en el registro de desplazamiento, desplazándose el puntero una posición a la izquierda por cada bit. La trama tiene como primer campo la dirección de destino. Tan pronto como este campo se encuentre totalmente en el registro de desplazamiento, la estación puede determinar si la trama está dirigida a ella; si no es así, la trama es retransmitida mediante el desplazamiento de un bit fuera del registro a medida que un nuevo bit llega por el extremo izquierdo, permaneciendo, por tanto, el puntero estacionario. Cuando se ha recibido el último bit de la trama, la estación continúa desplazando bits hacia la derecha hasta que toda la trama es transmitida. Si durante este tiempo llega alguna nueva trama, ésta comenzará a acumularse en el registro a medida que la primera se transmite; si no se recibe ninguna trama el puntero vuelve a la posición inicial.

Consideremos ahora el caso en que la estación tenga datos que transmitir. Para que pueda proceder a transmitir deben cumplirse las siguientes condiciones:

A) debe haber un mensaje preparado en el buffer de salida.

B) debe existir un hueco en el registro de desplazamiento al menos tan grande como el mensaje a enviar. Es decir, el puntero de entrada debe estar situado suficientemente a la derecha.

C) debe haberse detectado el final del mensaje que está pasando en ese momento por la estación (si está pasando alguno).

Si se cumplen estas tres condiciones, se transfiere en paralelo el área de salida al registro de desplazamiento, ocupando la zona a la izquierda del apuntador de entrada y éste se desplaza a la izquierda tantos lugares como bits tiene el mensaje a transmitir. Seguidamente, si no aparecen bits por el extremo izquierdo del registro de desplazamiento, es decir, si no se reciben mensajes, el apuntador se desplaza a la derecha a medida que se transmiten los bits.

Esta técnica permite tener mensajes de distintas estaciones circulando simultáneamente por el anillo. Como puede observarse existe un retraso en cada nodo, cuyo valor mínimo equivale a la longitud del campo de dirección y el valor máximo es la longitud del registro de desplazamiento.

La técnica de *inserción de registro en anillo* da lugar a un reparto equitativo del medio: cuanto más inactivo esté el anillo, la estación podrá transmitir trama tras trama utilizando todo el ancho de banda; por el contrario, si el anillo tiene una carga elevada, una

extracción se encontrará con que después de transmitir una trama el registro de desplazamiento no se ajustará adecuadamente a otra trama y deberá esperar, por tanto, a que los espacios o "*gaps*" entre los mensajes se acumulen para poder volver a transmitir.

La ventaja más destacable de la técnica de inserción de registro es que consigue la máxima utilización del anillo. Otras características son que permite tramas de longitud variable y la posibilidad de que existan varias tramas a la vez en el anillo.

La desventaja fundamental la constituye el mecanismo de *control de errores*. Permitir múltiples tramas exige el reconocimiento de la dirección destino para retirar la trama, ya sea ésta retirada por el emisor o por el receptor. Si esta dirección se daña y ninguna estación es capaz de reconocer la trama, esta circulará indefinidamente por el anillo. La exigencia de reconocer las direcciones impone además un retraso en cada nodo por trama igual a la longitud de ese campo. Otro problema surge de la sincronización de los registros de desplazamiento cuando se utilizan velocidades elevadas.

10.3. RESERVA

Esta técnica se caracteriza porque los nodos solicitan una **reserva** y no inician la transmisión de la información hasta que ésta se les concede. Son métodos libres de colisiones en cuanto a la transmisión se refiere, pudiendo darse el hecho en el proceso de *establecimiento* de la reserva.

Los métodos de reserva, pertenecientes al grupo de compartición del medio, se pueden subdividir en:

- **Sistemas centralizados** compuestos normalmente por dos canales, uno asignado a la transmisión de los mensajes y otro a resolver las demandas de reserva. Estos canales pueden estar *multiplexados en el tiempo o en la frecuencia*. La técnica **SRMA** (*Split Channel Reservation Multiple Access*) corresponde a este último caso. El problema de efectuar la reserva por el canal especial es idéntico al planteado en el acceso al medio de transmisión de los mensajes, y se resuelve generalmente utilizando una técnica de *contienda*. Si se recurre, por el contrario a un método de selección *multiplexado*, resulta un sistema *sin colisiones*. Este último caso se da en la técnica **GSMA** (*Global Scheduling Multiple Access*). Los *tipos de reserva* que pueden ser solicitados son **de conexión**, en el que se solicita al controlador la reserva del recurso por un determinado período de tiempo, o **de mensaje**, en el que se efectúa una nueva reserva para cada mensaje a transmitir.

- **Sistemas distribuidos** en los que la asignación de las reservas se realiza colectivamente por todos los nodos de la red. Puede distinguirse entre técnicas

implícitas y **explícitas**. En las primeras no existe propiamente un procedimiento de solicitud y resolución de reserva previa a la transmisión, por lo que una estación que pretende utilizar el canal intenta tomarlo directamente. Si lo consigue, todas las demás estaciones entienden que lo tiene reservado hasta que se señalice lo contrario. Durante la toma inicial del canal se pueden producir colisiones que se resolverán utilizando algunas de las técnicas de *contienda*. Un ejemplo de esta técnica es la **R_ALOHA**. En las técnicas de reserva *explícita*, previamente al proceso de transmisión se inicia un procedimiento de establecimiento de reservas, que hasta que no es resuelto no permite la emisión de los mensajes. Las reservas explícitas se realizan para un solo paquete (método "*subtramas*" de reserva) o para un lote o mensaje de información completo. Ejemplo clásico de *técnica de reserva explícita con control distribuido* es el **anillo ranurado** (*slotted ring*). El estándar *IEEE 802.6* conocido como **DQDB** (*Distributed Queue Dual Bus*) también puede encuadrarse entre las *técnicas explícitas*.

10.3.1. ANILLO RANURADO (SLOTTED RING)

Su funcionamiento se basa en la circulación de una determinada cantidad de paquetes vacíos (*ranuras o slots*) en el anillo. Cada uno de estos paquetes tiene un *bit de comienzo* que identifica el estado del paquete (*ocupado* o *libre*) y un *campo de dirección*.

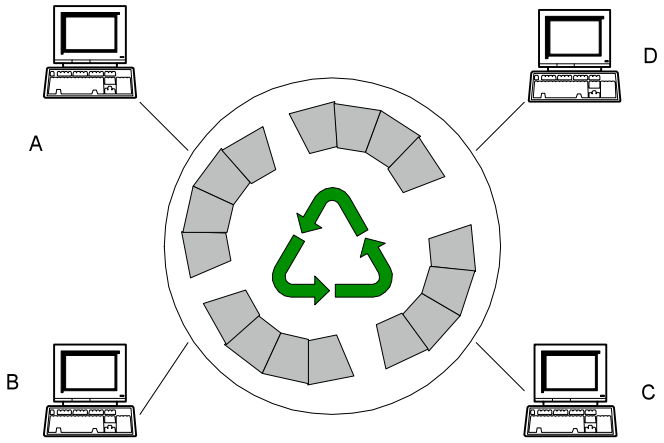


Fig. 10: *Esquema de funcionamiento del anillo ranurado.*

En el momento de activación de la red, todos los paquetes son iniciados como libres. Cuando una estación desea transmitir un mensaje espera hasta encontrar una ranura vacía, introduce en ella su información, cambia el estado del slot a ocupado y pone la dirección del nodo de destino. Mientras no reciba nuevamente la ranura que ha puesto en circulación, no podrá utilizar otra. Al volver el paquete a la estación emisora, ésta se encarga de restituir el estado de la ranura, dejándola libre. Además, el slot contendrá información sobre si la

estación destino aceptó o no el paquete. El número de paquetes en el anillo permanece invariable, y viene determinado por la longitud de la ranura, la longitud total del anillo y el procedimiento de puesta en marcha que se utilice.

En la red se suele asignar una estación monitora encargada de iniciar el funcionamiento, eliminar ranuras defectuosas y, en general, de las funciones de control de la red. La virtud básica de esta técnica se encuentra en su simplicidad, sin embargo, desperdicia una gran cantidad de paquetes vacíos en condiciones de poca carga, por otro lado, los paquetes deben transportar gran cantidad de información de control, aspecto éste que hace disminuir su rendimiento de manera considerable.

Este método se utilizó originalmente en el anillo de *Cambridge* y se ha propuesto para redes *MAN* con el nombre de **anillo de Orwell**.

11. MÉTODOS DE ACCESO PARA REDES DE ALTA VELOCIDAD

11.1. FDDI: FIBER DATA DISTRIBUTED INTERFACE

A comienzos de los años ochenta se identificó la necesidad de interconectar computadores a muy alta velocidad. este requerimiento no estaba cubierto por los procedimientos existentes. Surgió así el estándar **ANSI X3T9.5 FDDI** que opera a *100 Mbps*.

El método de control de acceso se definió para una topología en anillo, utilizando el principio de *paso de testigo*: solamente la estación que tiene el testigo puede transmitir. *FDDI* utiliza una topología con *doble anillo* tal como se indica en la figura 11.

Con este doble anillo se puede continuar la operación con todas las estaciones en caso de avería de un enlace.

La diferencia fundamental con la técnica de paso de testigo en anillo convencional utilizado en el estándar *IEEE 802.5* es que, en *FDDI*, cuando una estación ha terminado de transmitir sus tramas libera un testigo, con lo cual pueden existir simultáneamente múltiples tramas de distintas fuentes, si bien sólo puede haber un testigo libre. De esta manera se incrementa el rendimiento a alta velocidad.

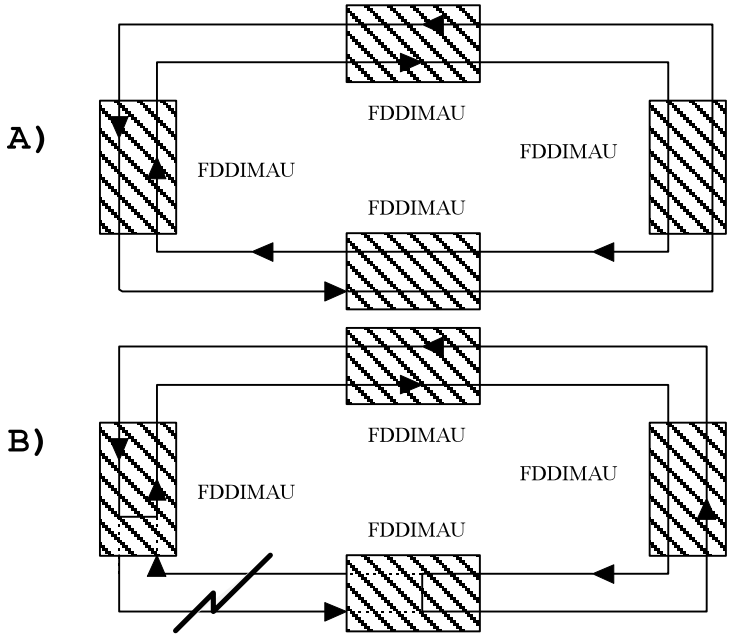


Fig. 11: *Reconfiguración en FDDI con doble anillo:*

A) operación normal, B) fallo del enlace.

11.2 DQDB: DISTRIBUTED QUEUE DUAL BUS

El procedimiento *DQDB* se generó como respuesta a la necesidad de redes *MAN* de alta velocidad, con características compatibles con la tecnología *ATM* emergente que comenzaba a ser considerada como respuesta universal para todo tipo de redes y servicios. La solución aceptada y normalizada por el subcomité del *IEEE 802.6* se basa en el principio de un bus dual físico con un procedimiento de acceso con cola distribuida y fue denominado **DQDB**, *Distributed Queue Dual Bus*. Se basó en una propuesta de la *Universidad de Western Australia* denominada originalmente **QPSX** (*Queued Packed and Synchronous Switch*).

La topología de las *MAN DQDB* se compone de dos buses unidireccionales a los que acceden los nodos conectados. Debe existir una estación que genere las tramas en cada bus (que en el caso de *DQDB* son células de tamaño fijo, de *48* octetos de información y *5* octetos de cabecera para conseguir la máxima compatibilidad con la tecnología *ATM*). Los dos buses operan en direcciones opuestas, tal como se indica en la figura 11. Los nodos se conectan a ambos buses utilizando conexiones de lectura y escritura. La operación de lectura no afecta a los datos entrantes, y la operación de escritura se realiza mediante un circuito *OR* lógico, entre la señal entrante y los datos del nodo. De esta forma se garantiza una fiabilidad muy alta, pues los datos no pasan por el nodo.

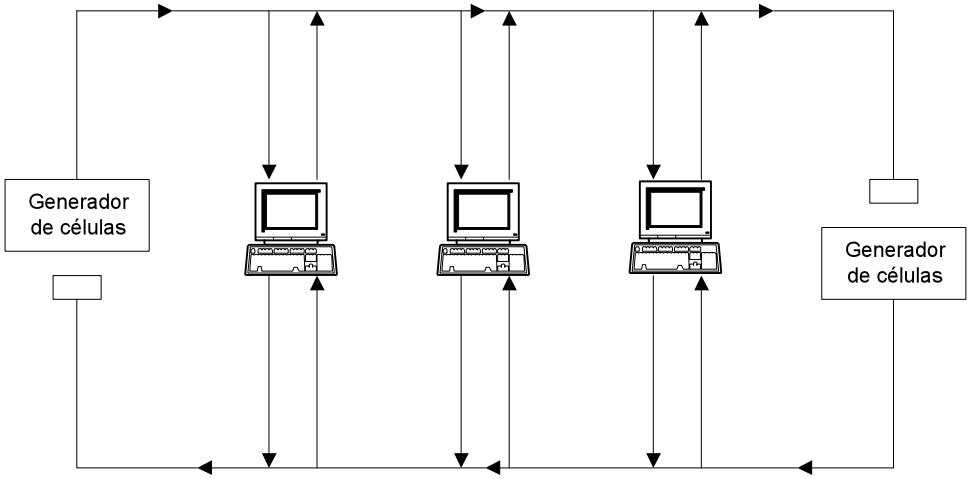


Fig. 12: *Esquema de configuración DQDB.*

En caso de fallo del bus se realiza un procedimiento de reconfiguración que permite mantener operativos a todos los nodos. Esto es posible porque el bus se instala inicialmente en bucle. de esta forma, cuando falla el bucle, los dos nodos adyacentes a la localización de la avería toman la función de generadores de trama y el nodo cabecera del bus pasa a ser un

nodo normal, manteniéndose operativo todo el bus.

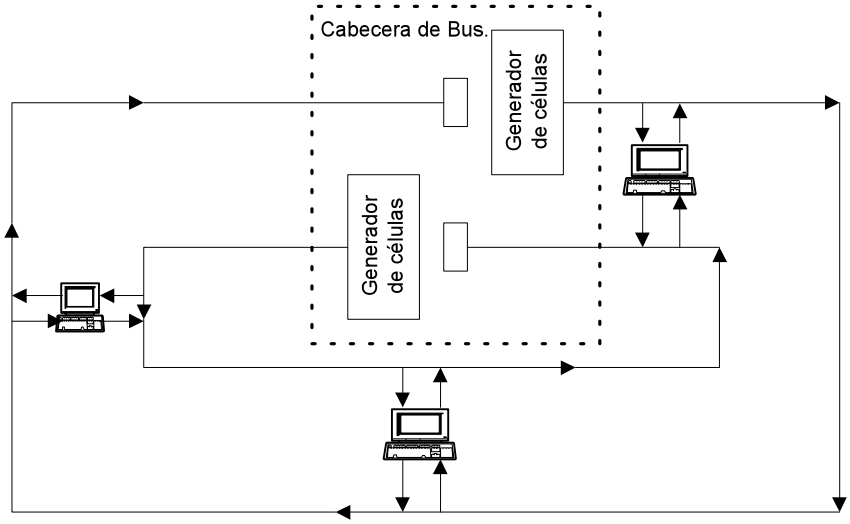


Fig. 13: *DQDB con bus en doble anillo.*

El control de acceso al medio se basa en el principio de **cola distribuida**, es decir, a nivel lógico, existe una cola de información por cada bus, si bien físicamente la cola está distribuida entre todos los nodos. Hay dos bits de control de la operación en cada célula: un *bit de ocupado* y un *bit de petición*. Si se representa el caso de transferencia de información por el bus **A**; en consecuencia, las peticiones de reserva se realizan por el bus **B**, para que las estaciones anteriores del bus **A** sepan cuántas peticiones previas hay para transferir datos. De forma simétrica tendría lugar la transferencia sobre el bus **B**. Las estaciones conocen, por la dirección de destino, el bus por el que tienen que transmitir las células. En cada nodo se proporciona un contador, denominado **Request Counter** (**RC**), que cuenta los bits de petición cuando pasan por el nodo. El contador *RC* se incrementa en una unidad cada vez que pasa un bit de petición. A su vez, el contador se decrementa en una unidad cada vez que pasa una célula vacía por el bus **A**; con ello, el nodo en cuestión deja libre la célula para que la pueda ocupar una estación posterior en el bus **A** que previamente lo hubiese solicitado. Cuando un nodo tiene una célula para transmitir, lo coloca en la cola distribuida, informando a los nodos anteriores mediante el bit de petición para asegurar que le dejen una célula vacía cuando le llegue el turno. Para que las células se transmitan en el momento oportuno, el valor del contador *RC* se copia en un contador de cuenta atrás, **CD** (*Countdown Counter*), en el momento de hacer la petición, mientras que el contador *RC* se inicia a cero. De esta forma, el contador *CD* conoce el número de células en cola de las estaciones anteriores del bus **A**. Cuando todas las células en la cola han sido transmitidas, el nodo puede poner la suya en el bus.

El ejemplo comentado corresponde al método denominado de **cola arbitrada** (*QA*). También existe un procedimiento para señales isócronas denominado **cola prearbitrada**

(*PQ*).

11.3 RDSI: RED DIGITAL DE SERVICIOS INTEGRADOS

La tecnología **RDSI** basada en **TDM** no se utiliza específicamente en entornos *LAN* o *MAN*, si bien sí se está utilizando en interconexiones entre *LAN* remotas, interconexión de un nodo remoto a una *LAN*, o para acceso de una *LAN* a los servicios de *Internet*, utilizando *WAN RDSI*.

La RDSI (Red Digital de Servicios Integrados) o ISDN (Integrated Services Digital Network) consiste en extender hasta el mismo bucle de abonado la red digital; esto es una evolución lógica de la sustitución de la red analógica entre centrales por una digital que muchas compañías telefónicas empezaron hace bastantes años, por razones más que evidentes. Con la aparición de una red de alta velocidad denominada RDSI de banda ancha (ATM) se sintió la necesidad de añadirle un adjetivo a la antigua RDSI, por lo que a veces se la denomina también RDSI de banda estrecha, narrowband-ISDN o N-ISDN.

Dado que la transmisión de la señal se hace de forma digital en todo el trayecto, en RDSI el teléfono actúa de códec digitalizando la señal acústica del auricular con una frecuencia de muestreo de 8 KHz, enviando ocho bits por muestra. En el caso de conectar un ordenador a la línea no necesitamos utilizar módem (pero sí un adaptador) y podremos transmitir datos a una velocidad de 64 Kb/s. A diferencia de lo que ocurre con las conexiones analógicas, los 64 Kb/s están asegurados, sin ruidos ni interferencias, y no hay necesidad de negociar la velocidad en función de la calidad de la línea.

El estándar RDSI contempla dos tipos de acceso al servicio:

- El acceso **básico** también llamado **BRI (Basic Rate Interface)** o acceso 2B+D. Está formado por dos canales digitales de 64 Kb/s también llamados canales B (de Bearer, portador) mas un canal de 16 Kb/s de señalización también llamado canal D, posiblemente de Data). Está orientado a usuarios domésticos y pequeñas oficinas

- El acceso **primario** también denominado **PRI (Primary Rate Interface)** está formado en Europa por 30 canales B y uno D de señalización, todos de 64 Kb/s; también se le llama 30B + D. En Norteamérica y Japón es 23B + D (23 canales B y uno D, todos de 64 Kb/s). La diferencia se debe a que en Europa un PRI se transporta en una línea E1 mientras que en Norteamérica y Japón se utiliza una T1.

En algunos países existe un servicio denominado canal H con una capacidad de 384 Kb/s, es decir, equivalente a seis canales B.

Generalmente los equipos que comunican mediante RDSI establecen inicialmente la comunicación utilizando un solo canal B, y cuando el tráfico supera un determinado umbral durante un tiempo superior al establecido (por ejemplo tráfico superior a 48 Kb/s durante mas de 20 segundos) se efectúa la segunda llamada (se conecta otro canal B) para disponer así de 128 Kb/s. Este proceso de agregación puede seguir hasta agotar los canales libres en alguno de los dos puntos que se conectan (por ejemplo un BRI no podrá agregar mas de dos canales); tanto el número máximo de canales a utilizar como las condiciones en las que se establecerán canales adicionales son configurables por el usuario. El canal D normalmente no se utiliza, aunque a veces se emplea para tráfico X.25; también adaptadores que permiten agregar los tres canales de un BRI obteniendo así una conexión de 144 Kb/s.

El acceso primario está pensado para grandes oficinas o centros proveedores de servicios. Por ejemplo un proveedor de conectividad Internet puede ofrecer acceso RDSI a sus usuarios (que normalmente emplearán un BRI) y en vez de instalar múltiples accesos básicos instalar un acceso primario que le permitirá atender simultáneamente hasta 30 clientes (o quizá algunos menos si decide permitir que los clientes que lo deseen utilicen dos canales).

Las conexiones o llamadas RDSI se pagan de acuerdo con la misma tarifa de uso que la red analógica, y con los mismos ámbitos (metropolitano, provincial, nacional e internacional). El RDSI resulta una alternativa a veces más barata que las líneas dedicadas de 64 Kb/s incluso para conexiones permanentes, especialmente en ámbito metropolitano; en estos casos debe estudiarse y valorarse el costo de ambas alternativas.

La posibilidad de utilizar RDSI cuando hay picos de tráfico da una gran flexibilidad. También es interesante el uso de RDSI como servicio de desbordamiento; por ejemplo, una oficina que tiene un tráfico constante con su central podría tener una línea dedicada de 64 Kb/s y un acceso básico RDSI para disponer en horas punta de un ancho de banda de hasta 192 Kb/s (los 64 Kb/s de la líneadedicada mas los 128 Kb/s de los dos canales B); los equipos pueden configurarse para que la primera y segunda conexiones RDSI se establezcan cuando el caudal de tráfico supere unos valores preestablecidos. Otro uso de la RDSI es como servicio de emergencia: dos oficinas unidas normalmente por una línea dedicada pueden en caso de avería de ésta conectar por RDSI en cuestión de segundos, de forma automática y transparente a los usuarios; según el tráfico entre las oficinas la conexión RDSI de reserva deberá ser un acceso básico o primario; en el caso de un acceso primario la capacidad podrá llegar a los 1.920 Kb/s (30 canales B).

Una aplicación interesante de la RDSI es la videoconferencia. Existen en el mercado equipos que por un precio muy razonable permiten convertir un PC en una

estación de videoconferencia; la señal de vídeo es captada por una cámara, enviada al PC para su digitalización y compresión, y enviada después por dos canales B a la estación remota, donde sufre el proceso inverso. En el estado actual de las técnicas de compresión de audio y vídeo con 128 Kb/s es posible efectuar una videoconferencia de calidad aceptable. Los sistemas de videoconferencia de mayor calidad utilizan un canal H de RDSI (384 Kb/s) o incluso una línea E1 directamente; con 384 Kb/s es posible obtener una calidad comparable a la de una emisión de televisión.

Físicamente un acceso básico esta formado por un dispositivo denominado NT1 (Network Terminating device 1) que dispone de un conector RJ45 (similar al conector telefónico normal) donde el usuario conecta su terminal RDSI (teléfono, fax, alarma, ordenador, etc.) Es posible conectar a un mismo acceso básico hasta ocho dispositivos diferentes con selección en base a subdirecciones (utilización de un dígito adicional al efectuar la llamada) o al tipo de dispositivo llamante (un fax llama a otro fax, un ordenador a otro, etc.). Un acceso primario en Europa esta formado por una interfaz G.703 (dos cables coaxiales para transmisión y recepción de 75 ohmios con conectores BNC); se trata exactamente del mismo interfaz físico que se suministra para una línea E1.

Para poder llevar la señal digital por el bucle de abonado sin modificación es preciso que la distancia a cubrir no sea superior a unos 5-6 Km; por este motivo la cobertura de RDSI en áreas rurales es aún muy deficiente.

En España la RDSI empezó a funcionar en 1993, aunque con una cobertura muy restringida. Actualmente está bastante extendida (siempre limitada a áreas metropolitanas) y sus tarifas son muy atractivas.

Como ya hemos comentado el estándar RDSI se demoró más de lo conveniente, y como consecuencia de ello lo que hubiera sido un servicio realmente innovador en su momento se ha quedado en una modesta mejora en la velocidad respecto a lo que se obtiene utilizando un módem. Además, en los módems se utilizan de forma generalizada algoritmos de compresión, ya que existen estándares seguidos por muchos fabricantes. En RDSI no existe un estándar para la compresión de datos, por lo que cada fabricante tiene su sistema propio. La aparición de módems de 56 Kb/s puede ser otro factor que inhiba el desarrollo de la RDSI.

11.4 ATM: ASYNCHRONOUS TRANSFER MODE

Prácticamente cuando RDSI estaba apareciendo en el mercado la ITU-T empezó a trabajar en un nuevo estándar de red digital para servicios avanzados. Dado que se pretendía que la nueva red digital fuera de elevadas prestaciones, con posibilidad de transmitir vídeo en alta resolución y servicios similares, se la denominó RDSI de banda ancha (RDSI-BA, Broadband ISDN o B-ISDN). Para no repetir el 'fracaso' que supuso la

tardía aparición del estándar RDSI; la ITU-T decidió utilizar en este caso una tecnología realmente novedosa, en la que hacía tiempo pensaban algunos ingenieros de telecomunicaciones pero que suponía un cambio radical de filosofía; la nueva tecnología se denomina ATM (Asynchronous Transfer Mode). Los primeros estándares B-ISDN/ATM se publicaron en 1988; en ese mismo año la ITU-T adoptó un nuevo proceso mas ágil de creación de estándares. A pesar de estas innovaciones, la industria consideró que la ITU-T no era suficientemente ágil en relación con los estándares ATM y en 1991 se creó el ATM forum, que en 1994 reunía ya a más de 150 miembros principales (fabricantes de ordenadores y equipos de comunicaciones, así como compañías telefónicas).

Para satisfacer las crecientes necesidades de ancho de banda de las aplicaciones para todo tipo de servicios, voz, datos, imagen estática o vídeo, y tratar de encontrar una solución universal para todo tipo de entornos, *LAN*, *MAN* o *WAN*, la tecnología *ATM* se perfila como la opción más prometedora. Aunque existen varios aspectos que están en proceso de normalización, ya existen productos y soluciones, tanto para estaciones de trabajo como para interoperación de *LAN*, basados en tecnología *ATM*.

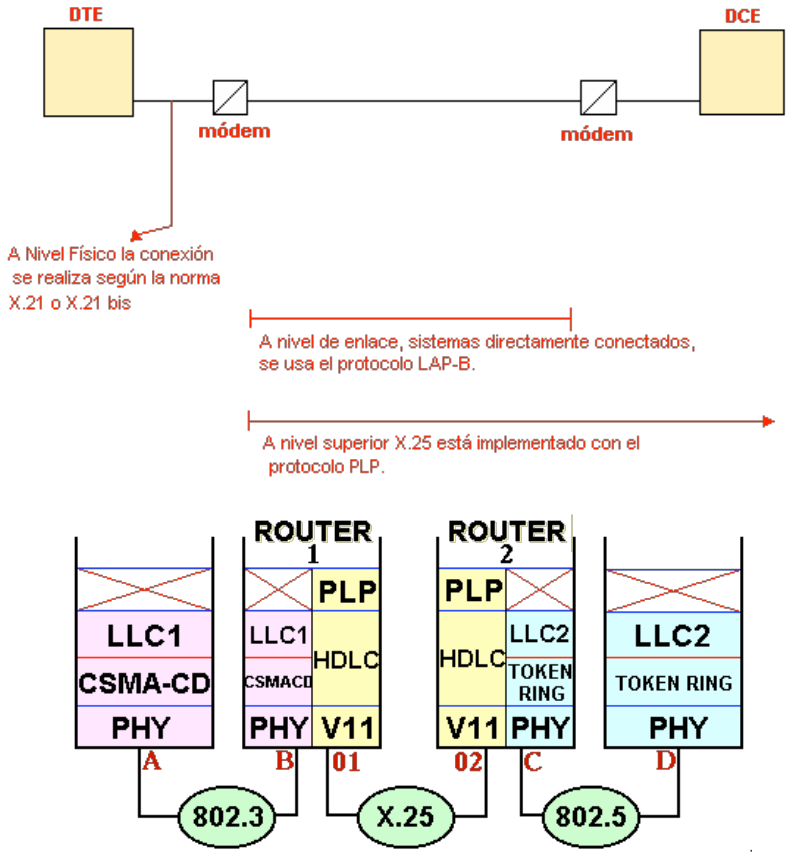
ATM es un procedimiento orientado a conexión. Las conexiones se pueden establecer de forma semipermanente o bien por duración de una llamada en el caso de circuitos conmutados. La transferencia de información puede considerarse como una transferencia de paquetes basada en *TDM asíncrono* y en el uso de células de tamaño constante: *48 octetos* de información y *5* octetos de cabecera. La cabecera de las células se utiliza fundamentalmente para identificar las células pertenecientes al mismo canal virtual en *la multiplexación por división en el tiempo asíncrona*, así como para funciones de encaminamiento. La integridad de las células se preserva por canal virtual. El campo de información de las células se transfiere transparentemente a través de la red. dentro de la red no se realizan procesos tales como control de errores, y todos los servicios (voz, datos, vídeo...) pueden ser transmitidos a través de la red *ATM*, incluyendo los servicios no orientados a la conexión propios de las redes locales.

12. REDES X.25.

12.1. INTRODUCCIÓN

X.25 es un estándar para el acceso a redes públicas de conmutación de paquetes. No especifica cómo está la red implementada interiormente aunque el protocolo interno suela ser parecido a X.25.

El servicio que ofrece es orientado a conexión, fiable, en el sentido de que no duplica, ni pierde ni desordena, y ofrece multiplexación, esto es, a través de un único interfaz se mantienen abiertas distintas comunicaciones. Vamos a estudiar todos los niveles de X.25, desde el Nivel Físico al Nivel de Red. En primer lugar veamos cuál es la forma más común de conexión y lo que abarca cada nivel :



Nomenclatura:

- DTE (Data Terminal Equipment): Es lo que utiliza el usuario final (PC con placa X.25 por ejemplo).
- DCE (Data Circuit Terminating Equipment): Podemos interpretarlo como un nodo local. A nivel de enlace (LAPB) las conexiones se establecen
- DTE-DCE. Ahora con el nivel de red, ampliamos las comunicaciones más allá del DCE, que hace de interconexión.

12.2 Nivel FÍSICO

Existen dos posibilidades:

- **X.21**: Se utiliza para el acceso a redes de conmutación digital. (Similares a las de telefonía digital.)
- **X.21bis**: Se emplea para el acceso a través de un enlace punto a punto. (Similar a RS-232 en modo síncrono.)

En cuanto las características mecánicas, se usan conectores *Canon* de *15 pines* o de *25 pines*. Las velocidades se mueven entre los **64kbps** y los **2Mbps**, velocidades que pueden parecer bajas y, de hecho, así son. X.25 presenta un problema de baja eficiencia por la exagerada protección contra errores que implementa y que con las redes de hoy en día no tienen sentido.

12.3 Nivel de ENLACE (LAP-B)

Ya sabemos que el objeto del Nivel de Enlace es garantizar la comunicación entre dos equipos directamente conectados. En X.25, este nivel queda implementado con el protocolo **LAP-B** (*Link Access Procedure - B*) que es un protocolo **HDLC 2,8**, es decir, con rechazo simple, indicado por el 2, y en el cual las tramas de información pueden ser utilizadas como tramas de control, indicado esto último por el 8. Veamos, en detalle, cuál es el formato de las tramas:

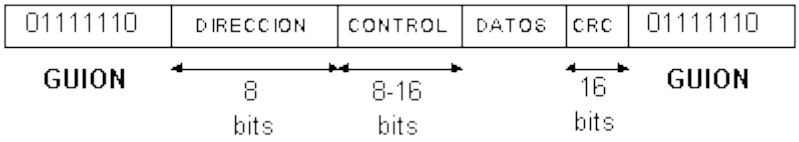


Fig. 14: *Trama de LAP-B.*

Analicémoslo más a fondo observando los tres tipos de tramas que se manejan:

a) **Tramas de información**: El campo de control es:

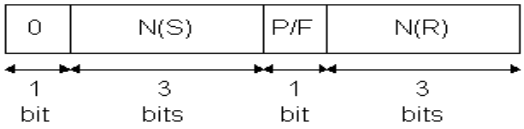


Fig. 15: *Campo de control de una trama de información.*

- El primer bit es obligatoriamente un *'0'*.
- En segundo lugar se coloca el número de secuencia de la trama de información que se envía.
- A continuación existe un bit denominado **P/F**. Es el bit *Poll/Final* de los protocolos *HDLC* que no entraremos a estudiar en profundidad.
- Por último, aparece un número de secuencia de asentimiento. Se utiliza

piggybacking, esto significa que se aprovechan las tramas de información para mandar asentimientos. Si un terminal recibe correctamente una trama y él quiere enviar otra, no genera un *ACK* y después manda su trama sino que incorpora el asentimiento en la propia trama. Por esto, representaremos las tramas de información con una *'I'* seguida de dos números. Con *I23*, por ejemplo, quien lo manda envía el equivalente a lo que antes representábamos con *I2* y *ACK3*, es decir, envía la trama 2 y advierte de que está esperando la trama 3 del otro interlocutor. En principio por defecto se utiliza numeración **modulo 7 (3 bits)**, así, las tramas irán con números desde el 0 hasta el 7 ambos incluidos. Si el retardo de asentimiento, tiempo que transcurre desde que se envía el último bit de una trama hasta que se recibe su asentimiento, es muy alto, puede interesar aumentar la numeración para poder mandar más tramas en dicho tiempo de asentimiento. Este es el motivo por el que se permite utilizar numeración extendida a **módulo 127 (7 bits)**.

b) **Tramas de supervisión**. El campo de control es:

Fig.16: *Campo de control de una trama de supervisión.*

y en el caso de numeración extendida:

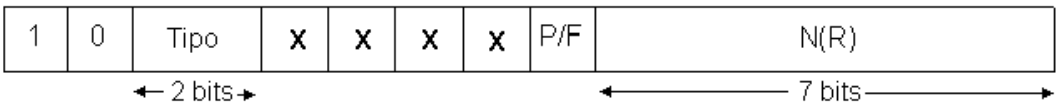


Fig.17: *Campo de control de una trama de supervisión con numeración extendida.*

Los tipos son:

BITS	TIPO	SIGNIFICADO
00	RR (Receiver Ready)	ACK
01	REJ (Reject)	Informa de que una trama llegó mal
10	RNR (Receiver Not Ready)	Se avisa al terminal origen que el receptor se desborda. Aún con esto se confirma la última trama recibida. El origen se queda parado hasta recibir un RR.
11	SREJ	Se utiliza en rechazo selectivo. Por tanto, no se usa en X.25.

c) **Tramas no numeradas**. El campo de control es:

Fig. 18: Campo de control de una trama no numerada.

Algunos tipos utilizados son:

- **SABM** (*Set Asyncronous Balance Mo*de): Sirve para configurar el receptor y el emisor.
- **UA** (*Unnumbered ACK*): Confirma tramas no numeradas que funcionan en modo parada y espera.
- **DISC**: Se utiliza para desconectar.
- **SABME**: Se configuran emisor y receptor acordando utilizar numeración extendida.
- **RESET**: Ante situaciones irrecuperables se pone todo a cero y se informa al nivel superior de que ha habido un fallo grave.

Analicemos un ejemplo completo para fijar todo lo explicado hasta ahora:

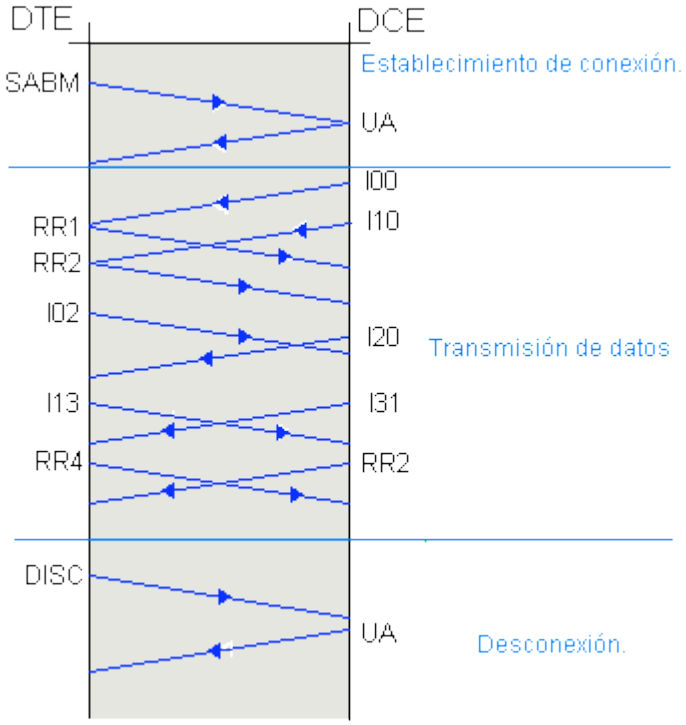


Fig.19: *Ejemplo de comunicación de LAP-B.*

Detengámonos en esta figura para entenderla a fondo. Diferenciamos en este tipo de comunicaciones tres fases:

Establecimiento de conexión:

En esta fase, un sistema final o *DTE* pide que se abra una comunicación con la trama *SABM*. En primer lugar, es importante señalar que el receptor será siempre un *DCE* puesto que trabajamos en el *Nivel de Enlace*, es decir, con comunicaciones entre entidades directamente conectadas. Con la trama citada, el *DTE* consigue

informar al *DCE* de qué características tendrá la comunicación que quiere establecer, en este caso por ejemplo, la numeración será la que exista por defecto y no será *numeración extendida*. Una vez recibida la trama correctamente en el *DCE*, éste contesta con *UA* para confirmar que la comunicación queda abierta. Hasta aquí, como podemos comprobar en la figura, se trabaja en *modo parada y espera.*

Fase de transmisión de datos:

Tras establecer la conexión y algunos de sus parámetros ya se puede pasar a mandar información. En el caso de la figura, es el *DCE* quien envía una trama, la trama *I00*. Como ya sabemos, esto quiere decir que la trama que se envía es la trama 0 y que el *DCE* está esperando recibir del *DTE* la trama 0. Tanto esta trama como la siguiente que manda el *DCE*, la *I01*, son confirmadas por el *DTE* con tramas *RR*. Como recordamos, no se asiente una trama con su número sino con el número de la trama que a partir de ese momento se espera, es decir, la siguiente a la que se confirma. Ésta es la razón por la que *I00* se confirma con *RR1*.

La primera trama que envía el *DTE* es *I02*, es decir, en este punto él manda la trama 0 y está esperando la 2. Una vez llega ésta al *DCE*, éste la confirma con *I31*, esto es, mandando su cuarta trama e indicando que queda a la espera de la trama 1 del *DTE*.

En el proceso ilustrado no figura ningún error pero, de haberlo, todo funcionaría como un *ARQ* con *rechazo simple*. Bien porque saltase un *TIMER* o por la recepción de una trama *REJ* se obligaría a la retransmisión a partir de la trama errónea.

El proceso así descrito continuará, si no surge ningún problema irrecuperable, hasta que uno de los interlocutores pida la desconexión.

Desconexión:

Una de las entidades envía la trama *DISC* que es confirmada con *UA*. Queda así la comunicación cerrada.

Por último, estudiemos algunos parámetros que intervienen en la comunicación y que son modificables y configurables en función de las condiciones de la red. Son:

- **T1** o **Plazo de Retransmisión**: Es el tiempo que se espera desde la transmisión de una trama hasta su retransmisión por falta de *ACK*. Es el objeto del *TIMER* del que hemos venido hablando hasta ahora.
- **T2** o **Retardo Máximo antes de Asentimiento**: Pueden no asentirse las tramas inmediatamente según llegan. Puede esperarse un tiempo menor que este *T2* por si llegan más tramas que puedan ser asentidas todas juntas.
- **T3** o **Plazo de Inactividad**: Si transcurre un tiempo sin que se transmita o reciba nada se emite un RR asintiendo la última trama que hubiese llegado. Es necesario testar el enlace para comprobar un posible fallo grave como la caída de un nodo...

- **N1** o **Longitud Máxima de la Trama**.
- **N2** o **Número Máximo de Retransmisiones de una Trama**: Si después de N2 retransmisiones de una trama, ésta no es asentida se resetea el enlace o se desconecta informando al nivel superior.
- **K** o **Tamaño de Ventana**.

12.4 Nivel 3 o nivel de RED

Este nivel está especificado por el **PLP** (*Packet Layer Protocol*) que es un protocolo de acceso a nivel de red y que proporciona un servicio al nivel superior:

- de *subred* (*SNACP*).
- modo *paquete*
- *orientado a conexión*.
- fiable.
- *multiplexación*: uso de una conexión para varias comunicaciones simultáneas. El DTE origen dialoga con su nodo, pero virtualmente lo hace con todos los *DTEs* multiplexados.

12.4.1 Circuitos virtuales (CV)

Podríamos definirlos como la asociación lógica entre usuarios para comunicarse entre ellos. En *X.25* hay 2 tipos de *CV*:

- **Conmutados** (*CVC*) : Hay que realizar un diálogo previo a la transmisión con el nodo local para establecerlos.
- **Permanentes** (*CVP*): Están establecidos de antemano (por contrato), así que no hace falta fase de establecimiento. Son muy útiles si se transmite mucho y con mucha frecuencia hacia un mismo destino.

Se identifican dentro de cada *DTE* por el número de **canal lógico** (*NCL*), que se negocia en la fase de establecimiento (sólo *CVCs*).

Podría además tener, por ejemplo, varios *CVs* establecidos con la misma máquina (cada uno con distinto *NCL* evidentemente).

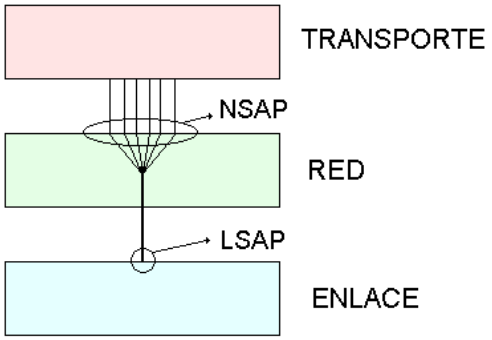


Fig. 20: *Los CVs y la multiplexación en teminología OSI.*

En la figura se muestra como la multiplexación que se ofrece al nivel de transporte, no es tal a nivel de enlace: en *LAPB* sólo hay una conexión.

La multiplexación se resuelve a nivel de red, aunando las diferentes conexiones (asimilables a *CVs*) que aparecen en el *NSAP* (*Punto de Acceso al Servicio a Nivel de Red*), en la que se ve desde el nivel de enlace en el *LSAP*.

12.4.2 Protocolo

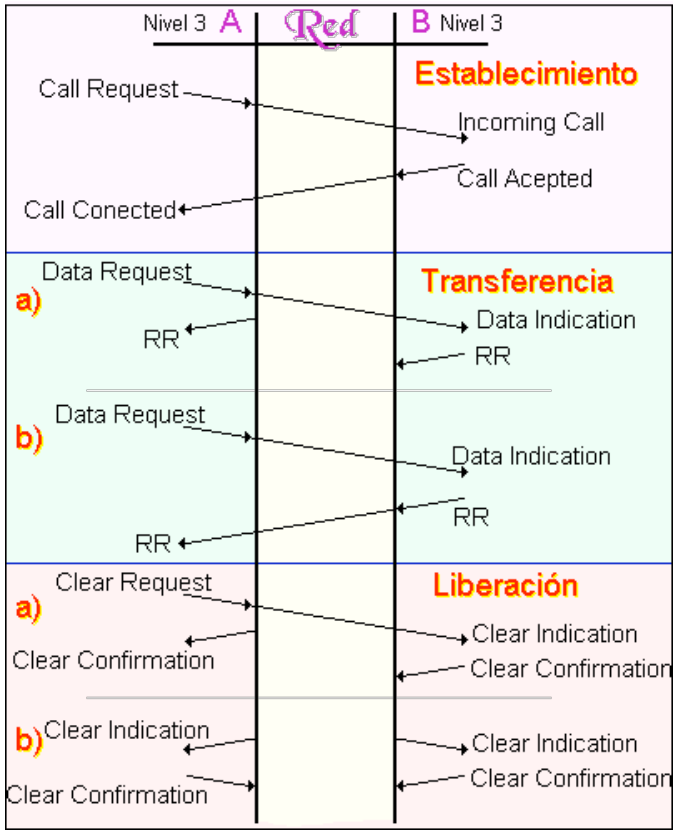


Fig.21: *Fases de la Transmisión.*

- **Fase de Establecimiento**: En la figura hemos supuesto que la llamada es aceptada, pero como veremos más adelante, podría ser rechazada. Esta fase sólo tiene lugar para *CVCs*. Llegados a este punto ambos lados estarán seguros de que la conexión se estableció bien.
- **Fase de Transferencia**: Como veremos, los datos pueden ser asentidos en el nodo local (caso 'a'), o en destino ('b').
- **Fase de Liberación**: La liberación a su vez puede ser solicitada por uno de los dos lados ('a') o por la propia red ('b').

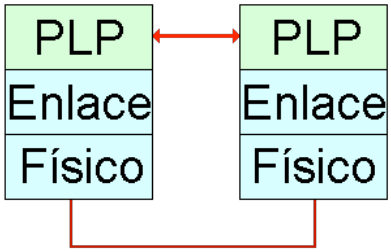


Fig.22: *Gráfica esquemática con los niveles OSI involucrados.*

- Los que dialogan son los dos *PLPs*. El nivel de enlace sólo sirve de mensajero
- Las direcciones a nivel de enlace son distintas de las de nivel de red.
- Con la dirección de enlace (que ya vimos que no se necesitaba realmente) llego al primer nodo. Allí se desencapsula y se usa la de red para llegar a los demás.

NOTA: A nivel de paquete no tenemos retransmisiones. Sí hay control (detección) de errores, pero no corrección.

12.4.3 Direcciones X.25

La recomendación **X.121** especifica el formato de las direcciones:

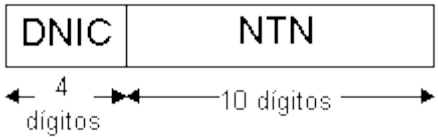


Fig.23: *Formato de las direcciones.*

- **DNIC** (*Data Network Identifier Code*): Identifica a cada red X.25 y distingue al operador público (**Iberpac** tiene uno, **Transpac** (Francia) otro, etc.). Es único a nivel mundial.
- **NTN** (*Network Terminal Number*): Número de abonado. En España está limitado a 9 dígitos.

Este tipo de dirección posibilita el encaminamiento jerárquico.

Codificación:

- La codificación se hace en **BCD**; concretamente se usa un octeto para cada 2 dígitos.
- En algunas ocasiones, el número de dígitos es impar (España p.ej.) lo cual da lugar a medio octeto sobrante y luego veremos que probablemente habrá que usar un relleno (pading).

Utilización:

- Usar siempre el *DNIC*, incluso si llamo a mi propia red. (es como si telefoneo Madrid-Madrid y siempre pongo el prefijo 91 delante).
- No usar el *DNIC* internamente y usar para llamadas externas *0+DNIC+NTN* (esto es lo que se utiliza en Iberpac).

12.4.4 Número de canal lógico (NCL)

Es un número que permite identificar al *CV* involucrado en una determinada transferencia y que es distinto a cada lado de la comunicación, aunque el *CV* sea el mismo.

El rango de *NCL* que pueden usarse, es algo a negociar con la empresa que ofrece el servicio (Telefónica, etc.). Más *NCL*, mayor número de *CVs* establecibles. Un *NCL* se especifica con 12bits, lo cual da lugar a que puedan usarse como máximo 4095 *NCLs* (el 0 tiene un significado especial).

Utilización:

Los *NCLs* se escogen por el *DTE* o por el DCE (la red en el fondo) cuando se necesitan, liberándolos cuando los acaban de usar. Ambos tienen una lista donde marcan los *NCLs* libres y ocupados (lo que se marca en una lista se refleja inmediatamente en la otra).

- El *DTE* empieza a escoger por los *NCLs* de mayor numeración.
- El *DCE* (la red) empieza por los de menor numeración.

Podría ocurrir que se juntasen en el centro (los *DTE* vienen de arriba y los *DCE* de abajo) y esto desemboca en varias posibilidades:

1. Que cuando *DTE* o *DCE* vayan a escoger un número, en sus listas figuren todos como ocupados. En este caso, no se aceptarían sus paquetes.
2. Que sólo quede un *NCL* por elegir y los dos lo cojan al mismo tiempo. En este caso la red (*DCE*) tendría prioridad. La conexión del *DTE* se contesta con un *clear* desde la red y se rechaza. (ver figura).

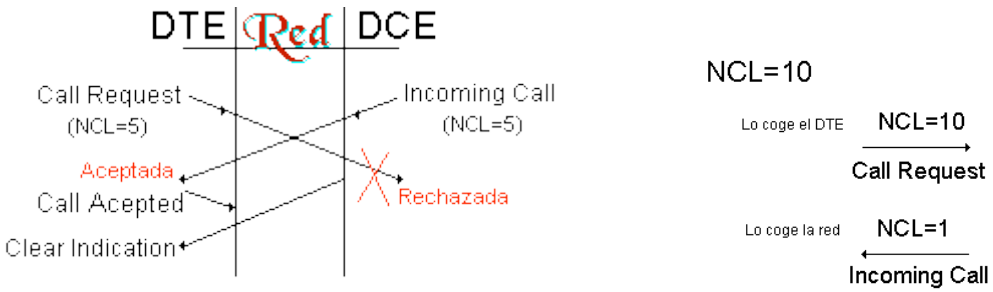


Fig.24: *Ejemplos del uso de NCLs.*

En respuesta a un *Call Request* anterior (que el *DTE* asignó sin problemas al *NCL* 6 por ejemplo), el *DCE* trata de asignar el *NCL* 5 pues lo ve libre. Así el *CV* de esa conexión tendría asociado el *NCL* 6 en el *DTE* y el 5 en el *DCE*. Al mismo tiempo el *DTE* ha visto libre el *NCL* 5 y trata de establecer un nuevo *CV* asignándoselo Como consecuencia de esto es la operación del *DCE* (de la red) la que se acepta, rechazándose el *Call Request* del *DTE*.

3. Una posible solución para evitar colisiones de este tipo, es dividir por rangos la oferta de *NCLs*. Por ejemplo asignar una cierta cantidad de números para *CVs* entrantes, otra para salientes y otros que fuesen bivalentes. Así solo habría colisión en los bivalentes, pues los entrantes y salientes sólo podrían ser elegidos por *DTE* y *DCE* respectivamente.

12.4.5 Formato general

Para el estudio del *PLP* vamos a ver el formato de sus *PDUs* (éstas se encuentran alineadas a octeto):

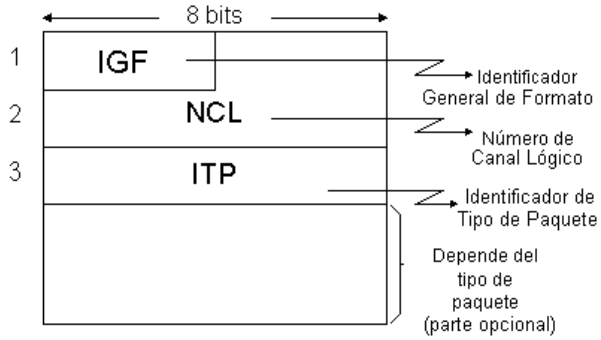


Fig.25: *Formato general de una PDU.*

La longitud del paquete no aparece escrita en ningún sitio, pues no es necesaria (va delimitado a nivel de enlace).

Para profundizar en el estudio de este nivel vamos a ver con más detalle. los siguientes paquetes:

- Paquete de Petición de Llamada y Paquete de Llamada Entrante.
- Paquete de Llamada Aceptada y Paquete de Comunicación Establecida.
- Paquete de Liberación de Conexión y Paquete de Indicación de Liberación.
- Paquete de Confirmación de Liberación.
- Paquetes de Asentimiento y Control de Flujo.
- Paquete de Datos.
- Paquete de Reinicio (RESET).
- Paquete de Rearranque (RESTART).
- Paquete de Interrupción.

Por último veremos como X.25 permite implementar un procedimiento multienlace.

A. Paquete de petición de llamada y de llamada entrante

Los paquetes de petición de llamada y llamada entrante tienen el mismo formato, diferenciándose únicamente en el sentido en que se transmite el paquete: *DTE-DCE* el primer caso y *DCE-DTE* en el segundo. Así pues tendremos:

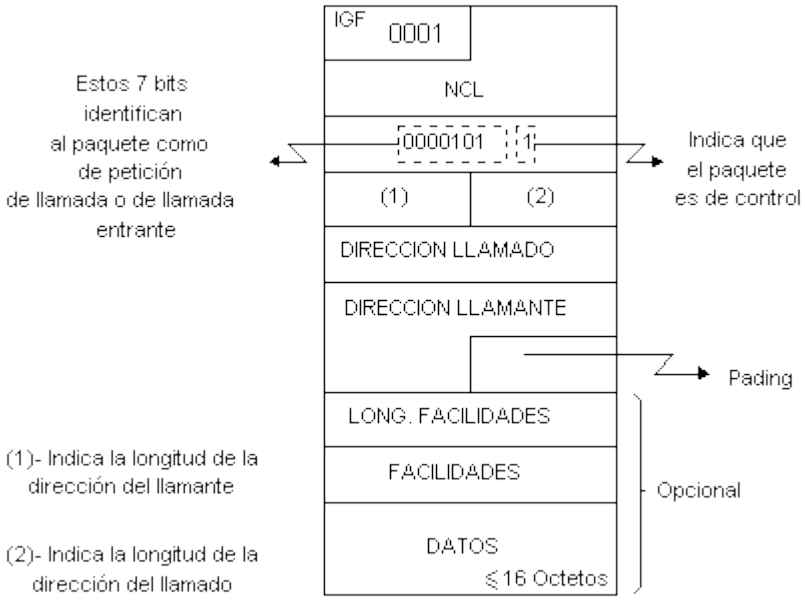


Fig.26: *Formato general de Petición de Llamada o Llamada Entrante.*

Las **longitudes** se codifican con cuatro bits que indican el número total de dígitos de las direcciones en X.25 Si las direcciones de llamante y llamado no tienen ambas un número impar de dígitos o un número par (de España a España por ejemplo, el semiocteto que sobra con una se cubre con el de la otra (9+9=18 par), puede sobrar algún semiocteto.

El **pading** se usa precisamente para solventar este problema de semi-octetos sobrantes. Es un relleno que se pone para que no sobre nada.

Campo de facilidades: Las facilidades son servicios suplementarios al servicio básico (Ej. especificación de uso de un tamaño de paquetes de datos superiores al tamaño por defecto (128 oct.), o de un tamaño de ventana diferente a 2, etc.). Su longitud está indicada por el campo longitud de facilidades.

Estos paquetes contienen **datos** de usuario del nivel superior, los cuales no llevan delante un campo de longitud ya que acaban donde acaba la trama. La longitud de este campo, como se ve en la figura anterior, es menor o igual que 16 octetos. Sin embargo, en la modalidad de selección rápida (*fast select*) pasa a ser menor o igual que 128 octetos. Estos datos generalmente se usan para:

1. Proporcionar un mecanismo de control de acceso, ya que con la dirección del

llamante sólo se identifica al ptr, no a los usuarios (autentificación).
2. Enviar la *PDU* de establecimiento de conexión del nivel superior.

B. Paquete de llamada aceptada y de comunicación establecida

El paquete de llamada aceptada va del *DTE* al *DCE* y el de comunicación establecida del *DCE* al *DTE*.

El formato es el mismo para los dos:

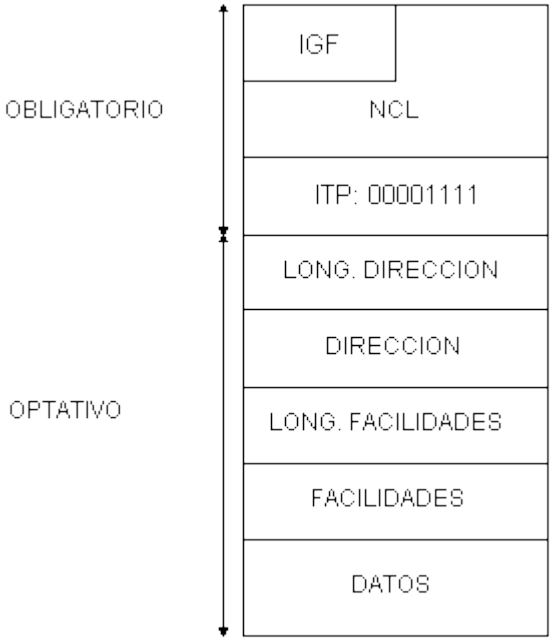


Fig.27: *Formato general de Llamada Aceptada o Comunicación Establecida.*

Si pongo los campos opcionales de facilidades o datos, tengo que poner también los de longitud y direcciones, aunque puedo dejarlos a cero.

Tanto estos paquetes como los de petición de llamada y los de llamada entrante, así como los de liberación de conexión y de indicación de liberación admiten la facilidad de selección rápida (fast select):

1. En estos paquetes se pueden introducir datos de hasta 128 octetos.
2. Si una estación nada más recibir una Petición de Llamada manda una *PDU* de desconexión, consigue una transferencia de datos sin haberse establecido la conexión.

X.25 facilita esta opción ya que hay aplicaciones que funcionan mejor en modo **datagrama** (servicio no orientado a conexión).

C. Paquete de liberación de conexión y de indicación de liberación

El paquete de liberación de conexión va del *DTE* al *DCE* y el de indicación de liberación del *DCE* al *DTE*.

Por lo demás ambos paquetes tienen el mismo formato:
Causa: Es un byte que indica por qué se ha liberado la comunicación (si ha sido el *DTE*, la red, etc.).
Diagnóstico: Es un byte que no hace sino refinar la causa.
La parte optativa se envía en base a las reglas del protocolo: no cuando el usuario lo desee, sino cuando lo exige el protocolo.

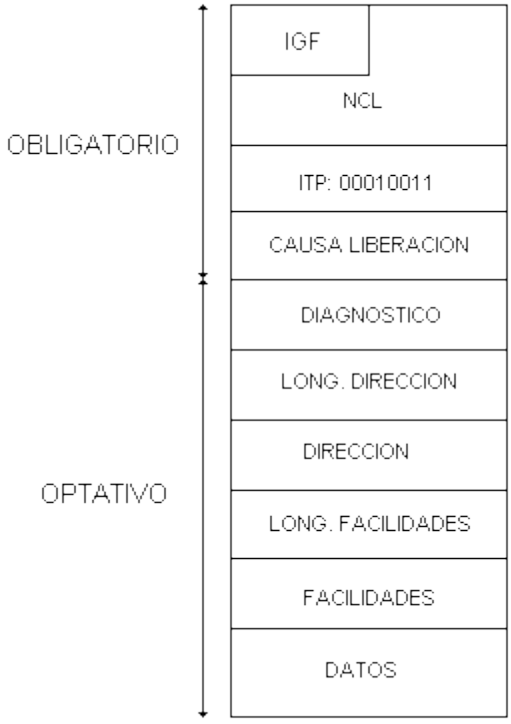


Fig.28: *Formato general de Liberación de Conexión e Indicación de Liberación.*

D. Paquete de confirmación de liberación

No hay campo de datos en este caso, ya que cuando se envía este paquete se cierra la conexión.

Su formato es el siguiente:

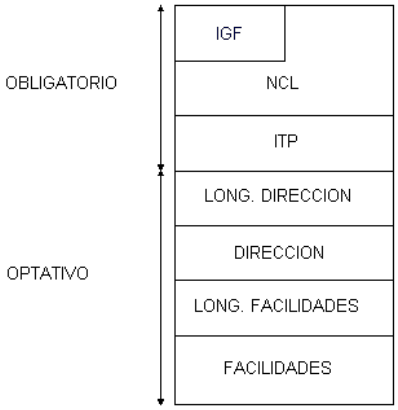


Fig.29: *Formato general de Confirmación de Liberación*

E. Paquetes de asentimiento y control de flujo

En X.25 no se utiliza *ARQ* pues no hay retransmisiones. Los números de secuencia y las ventanas se utilizan exclusivamente para hacer control de flujo de tipo *XON/XOFF* y para detección de errores. El nivel de enlace se supone fiable.

Hay dos tipos de paquetes: *RR* y *RNR*. Son paquetes explícitos de asentimiento y se utilizan como alternativa al *piggybacking*.

El formato de los paquetes *RR* y *RNR* es el mismo, diferenciándose entre ellos solamente en un bit:

Fig.30: *Formato general de Paquetes de asentimiento*

P(R) son 3 bits que indican el número de secuencia que se asiente (indica cuál es el siguiente que espera recibir)

Los paquetes *RR* y *RNR* varían ligeramente en el formato extendido:

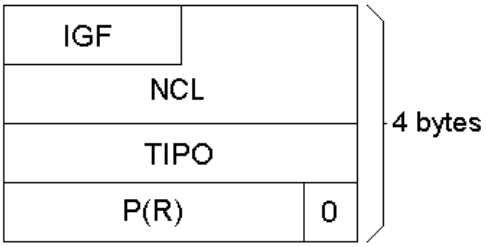


Fig.31: *Formato general extendido de RR y RNR.*

NOTA: Existe una opción adicional en X.25, que prácticamente no se usa y que incluye rechazos con retransmisiones (REJ se consigue con el campo de tipo a 01001)

F. Paquete de datos

El paquete de datos en la recomendación X.25 presenta el siguiente aspecto:

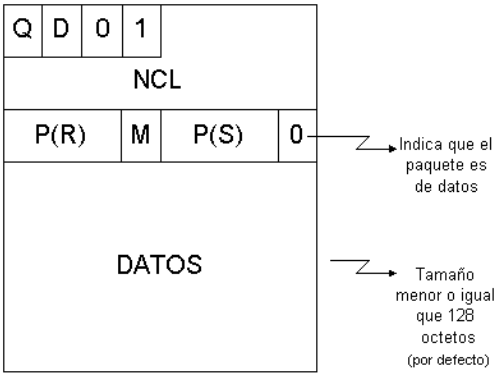


Fig.32: *Formato general de un Paquete de Datos.*

donde:

- bit **M**: se utiliza para segmentación y reensamblado.
  Si *M=1* faltan más paquetes por llegar de la *SDU* que se está transmitiendo.
  Si *M=0* no faltan más paquetes por llegar de la *SDU* que se está transmitiendo.
- **P(R):** Número de secuencia de recepción. Es también un asentimiento (*piggybacking*)
- **P(S):** Número de secuencia de transmisión.

Los números de secuencia (*P(R) y P(S)*) y la ventana se utilizan exclusivamente para control de flujo y detección de errores. El tamaño de la ventana por defecto en X.25 es 2 (se puede solicitar un aumento de ventana, pero será más caro, ya que se utilizan más recursos de la red).

- bit **D**: se utiliza para controlar el tipo de asentimiento (también llamado acuse de

recibo)

D=0 Asentimientos locales (sin acuse de recibo).
D=1 Asentimientos remotos (con acuse de recibo).

- bit **Q**: no afecta al comportamiento de X.25. La entidad de nivel de red simplemente informa al usuario del nivel superior de su estado a 0 o a 1. El bit Q se transporta de forma transparente. Se puede utilizar para que el nivel superior marque a sus paquetes de control (*Q=1*) o datos (*Q=0*).
- **DATOS**: es una secuencia de octetos (al menos uno, el paquete de datos no puede ir vacío). Hay un número máximo de octetos por paquete (p.ej. en Iberpac datos <=128 octetos). Al igual que la ventana, se puede solicitar un aumento del tamaño del paquete, pero esto también implica mayor ocupación de la red y mayor precio.

El paquete de datos varía ligeramente cuando se utiliza el formato extendido:

Fig.33: *Formato general extendido de un Paquete de Datos.*

G. Transferencia de datos

Longitud por defecto 128 octetos.

- Transparencia.
- Ventana deslizante (2 por defecto).
- Posibilidad de formato extendido.

No hay retransmisiones, pues se supone que la fiabilidad ya la proporciona el nivel de enlace. Se lleva una cuenta de los errores, pero no se corrigen (tiene una tasa de errores no detectados muy baja).

Los *RR* puedo retrasarlos tanto como quiera y usarlos para control de flujo o para asentir varias tramas a la vez, pues al no haber retransmisiones, no saltarán los timers (en *LAPB*, si trataba de hacer lo mismo, se retransmitía).

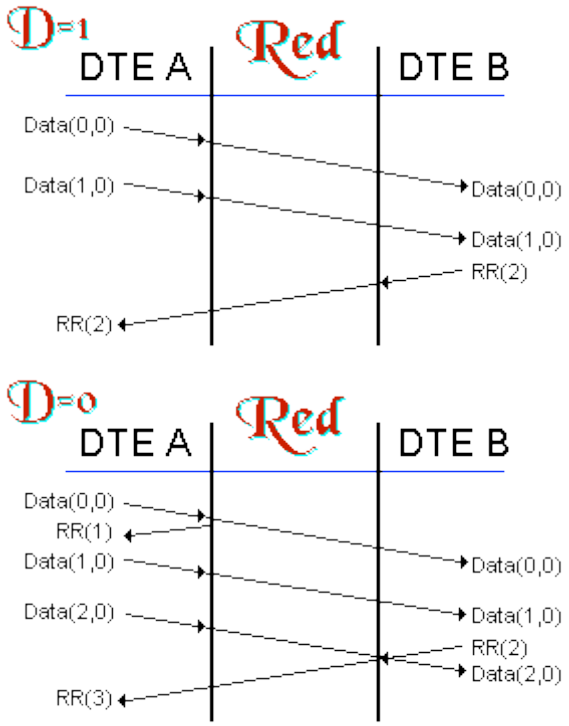


Fig.34: *A la izquierda ejemplo con asentimientos remotos. A la derecha locales.*

D=1; Asentimientos Remotos:

- Hasta que *RR(2)* no llegue al origen, no puedo seguir transmitiendo, pues se agotó la ventana (ineficacia).
- El asentimiento remoto me asegura que el mensaje llega al destino. Es muy útil en bases de datos por ejemplo.

D=0; Asentimientos Locales:

- Tras *RR(1)* el origen sabe que el mensaje ha llegado únicamente al primer nodo de la red.
- *RR(2)* es un asentimiento al *DCE* local de B. La red se encarga de llevarlo a A (en forma de *RR(3)* por un mecanismo llamado *back pres*sure, pero es totalmente distinto a un asentimiento remoto.
- *RR(3)* viene generado por la red, para que A pueda seguir transmitiendo. *D(2,0)* lo ha asentido la red, no B.
- Los números de secuencia también son distintos en los asentimientos, porque se hacen en local a cada nodo.
- Luego *RR(2)* hace que se genere *RR(3),* pero no es que *RR(2)* llegue a A.

NOTA: D(2,0) no se podría haber recibido en B, si no se hubiese generado antes RR(2), porque ya se había agotado la ventana.

- Es más lento en el control de flujo (aunque si no hay congestión no hay problema).
- Es más eficiente, pues puedo seguir transmitiendo.

H. Paquete de reinicio (RESET)

Los paquetes de petición e indicación de reinicio tienen la misma forma:

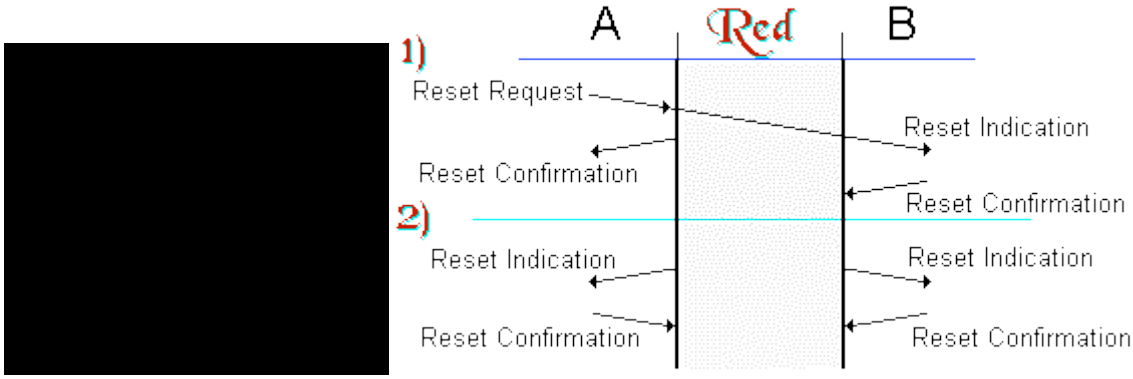


Fig.35: *Formato general de un Paquete de Petición de Reinicio y esquema del protocolo(RESET).*

Como se ve en la gráfica de la derecha, el *RESET* puede estar generado por uno de los dos lados (caso 1) o por la propia red (caso 2). El contenido de los campos causa y código viene especificado en la recomendación. Los paquetes de confirmación de reinicio por *ETD* y *ETCD* tienen el aspecto siguiente:

Fig.36: *Formato general de un Paquete de Confirmación de Reinicio.*

y la única diferencia entre ellos es el lugar donde se generan:

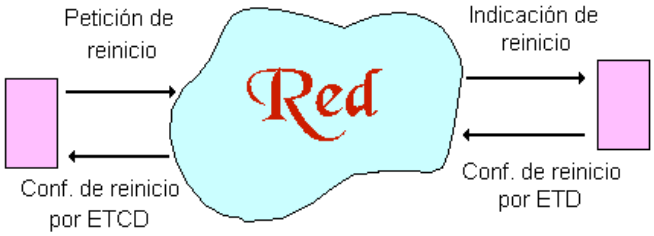


Fig.37: *Gráfico de la generación de paquetes de reinicio.*

Los efectos de un RESET son los siguientes:

- Pone los números de secuencia a 0.
- Descarte de paquetes.
- Informa al nivel superior.

I. Paquete de reinicialización (RESTART)

Es un procedimiento de recuperación frente a errores particularmente graves que afectan a toda la interfaz entre el usuario y la red (ej. se cae el equipo de usuario o el nodo local).

El formato de los paquetes es similar al de *RESET* (así como el intercambio de paquetes, sustituyendo *RESET* por *RESTART*):

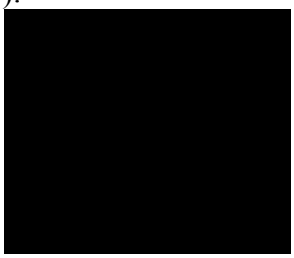


Fig.38: *Formato general del Paquete de Reinicialización.*

Se envía por el canal lógico 0, que es el que se reserva para señalización.

Los efectos de RESTART son:

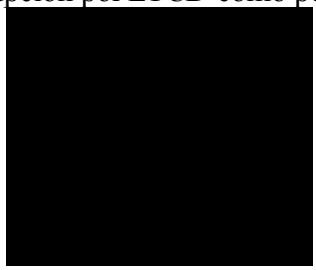
- Todos los CV permanentes se reinician.
- Todos los CV conmutados se desconectan.

Los paquetes de confirmación de rearranque por parte del *ETD* y *ETCD* son también iguales a los de confirmación de *RESET*:

Fig.39: *Formato general de Confirmación de Rearranque.*

J. Paquete de Interrupción

Tanto la interrupción por *ETCD* como por *ETD* presentan el siguiente aspecto:



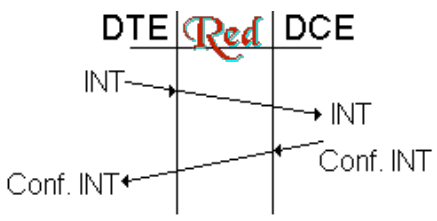


Fig.40: *Formato general del Paquete de Interrupción y protocolo de transmisión.*

Son paquetes también denominados fuera de banda, pues no están sometidos a control de flujo. El objetivo es que lleguen lo más rápidamente posible (son enviables incluso cuando la

transmisión está parada).

Funciona en **parada y espera**: hasta que no llega un *Conf.INT*, no puedo enviar otro *INT*.

El campo *DATOS* es variable. Históricamente el tamaño de los datos era de un octeto. Las versiones más modernas permiten hasta 32 octetos (en cualquier caso, es una cantidad pequeña, pues ya estaría enviando más de lo que se debe).

K. Transmisión de tramas de mayor longitud

A la hora de transmitir tramas de mayor longitud de la que admite X.25 en un paquete de datos (128 octetos por defecto), tenemos varias opciones:

- Negociar un *CV* que sea capaz de transmitir toda esa cantidad de datos de una vez (más sencillo, pero poco económico).
- Usar el bit *M*: Si el destino recibe un paquete con el bit *M=1*, almaceno y espero. Cuando reciba el de *M=0* (después de una serie con *M=1*), los reensamblo todos y los paso al nivel superior. (En IP no es tan sencillo porque pueden llegar desordenados y el *M=0* puede no ser el que corresponde al *M=1* anterior).

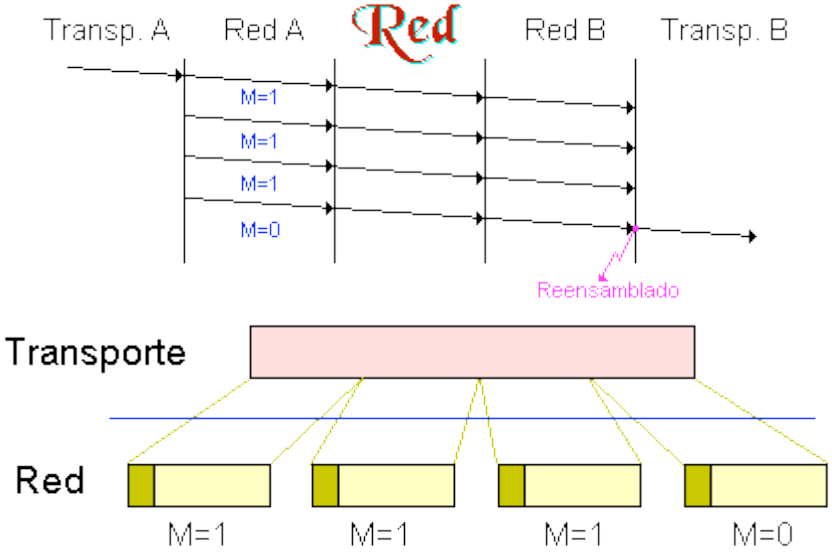


Fig.41: *Transmisión de paquetes de mayor longitud.*

Este tipo de transmisión es útil cuando:

- Si simplemente quiero enviar más de lo permitido
- El tamaño del paquete es mayor en el origen que en el destino.
- Incluso si el tamaño en el destino es mayor que en el origen, puedo almacenar varios mensajes antes de pasarlos todos juntos al nivel superior (aunque realmente no vayan juntos).

12.4.6 Facilidades

Este campo es común a varios tipos de paquetes y posibilita definir ciertos parámetros o modos de operación o "actuación" que de otra manera no se podrían establecer:

- Negociado de parámetros de control de flujo(longitud de paquete, ventana, módulo extendido, rango de CVs): hay dos opciones para el negociado: durante el establecimiento de la conexión, o por contrato con Telefónica.
- Grupos cerrados de usuarios.
- Cobro revertido.
- Grupo de captura: varios ordenadores que ofrecen el mismo servicio, con la misma dirección.

12.4.7 Procedimiento multienlace

En X.25 se puede hacer uso de la división de conexiones de la siguiente manera:

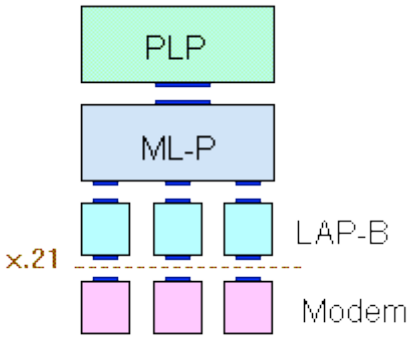


Fig.42: *Uso del ML-P.*

ML-P: *Multi-Link Protocol*. Es el encargado de hacer el multienlace.

Funcionamiento del ML-P:

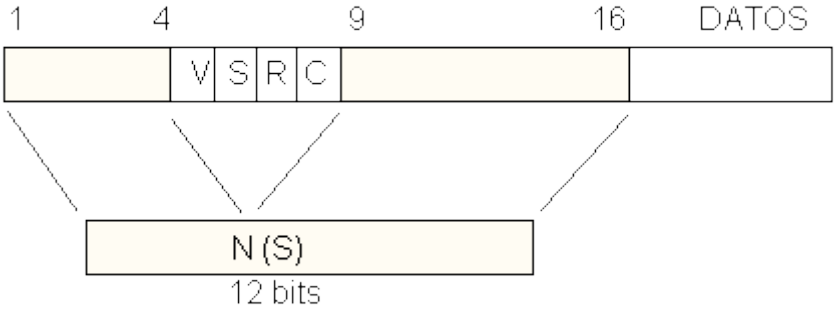


Fig.43: *Formato del ML-P.*

Los bits R y C se utilizan para indicar el tipo de PDU.

- *R=1* (*reset*): el que transmite la *PDU* solicita un establecimiento o reinicio de la conexión
- *C=1*: para confirmar (aceptar) el *reset* o el establecimiento de la conexión. Se utiliza para responder a un paquete con *R=1*. (*R=1* sería equivalente a lo que en *LAP-B* era *SABM* o *RST*) (*C=1* sería equivalente a lo que en *LAP-B* era *UA*)

Transmisión:

MLP debe repartir la carga entre las líneas que tiene por debajo. Reparte entre las que estén dispuestas a recibir. Además debe asignar números de secuencia (12bits).

Recepción:

MLP debe resecuenciar, ya que el retardo es variable entre las distintas líneas.

12.4.8 Tarificación

El coste de una red X.25 se reparte entre las siguientes contribuciones:

- **Coste de Instalación**.
- **Coste fijo**: pago mensual incluso si no hay ninguna transmisión.
- **Coste variable**:
  - **Coste por llamada**: fijo por cada circuito virtual establecido.
  - **Coste por tiempo**: suele cobrarse por segundo de conexión o fracción.
  - **Coste por tráfico**: Lo normal es cobrar por cada 64 bytes transmitidos o fracción.

NOTAS:

- Todas las contribuciones variables, dependen de la fecha y de la hora de la transmisión.
- No hay coste adicional por llamar a un sitio o a otro.
- El equivalente al paso telefónico es el UBT (Unidad Básica de Tarificación).

13. Frame Relay

Frame Relay surgió como un estándar de facto, producido por un grupo de varios fabricantes de equipos. Nació para cubrir necesidades del mercado no satisfechas hasta el momento en el sector de las comunicaciones. Se trataba de una solución transitoria, pero que ha logrado una gran aceptación, y su papel en la actualidad es importante. Las limitaciones que presenta *X.25* empezaban a ser evidentes:

X.25 es un estándar que impone una sobrecarga de procesamiento muy grande. Esta complejidad tan elevada impide operar a velocidades de línea altas. Un ejemplo es que, en la práctica, la ventana del nivel 3 impone limitaciones en velocidad.

El rango de caudales en acceso en que X.25 opera normalmente va desde *1.2Kb/s hasta 64 Kb/s*. Existen equipos que permitirían operar a una velocidad mucho mayor en la línea de acceso. Pero eso implicaría una congestión mayor en las líneas troncales (que conectan sistemas intermedios) de la red. Y precisamente lo que resultaría muy costoso económicamente es aumentar las velocidades a las que operan estos sistemas intermedios. De ahí que la solución haya sido adoptar otro estándar: *Frame Relay*.

Una aplicación muy importante de X.25 es el teleproceso o acceso a un *mainframe* desde terminales remotos. La velocidad de 64 Kbps sí puede resultar suficiente para cualquier terminal, pero es una cifra escasa para la línea que conecta al superordenador con la red.

Otras aplicaciones que no satisface X.25 son:

- Rápida y efectiva interconexión de *LANS*.
- Aplicaciones multimedia con audio y video en tiempo real.

Hay que tener en cuenta que una red de conmutación tiene recursos compartidos, y su funcionamiento depende de la carga de la red (a mayor carga el retardo se incrementa y el flujo disminuye). Como no resulta posible predecir el estado de la red, no sabemos cuanto tardará en transmitirse un paquete, ni podemos garantizar un caudal mínimo. Este problema se ha resuelto en *Frame Relay*, y existen garantías respecto al caudal.

Otra diferencia de *Frame Relay* respecto a X.25 es la separación entre el plano de usuario y el plano de control. Existen dos arquitecturas de protocolos diferentes para los datos de usuario y los datos de control. En X.25 los procedimientos de control y los datos de usuario utilizaban los mismos medios, y eso daba lugar a problemas en casos de congestión.

El estándar de facto evolucionó hacia varios estándares oficiales, como el propuesto por ANSI, o el creado por la ITU-T. Éste último presenta más diferencias respecto al estándar de facto.

13.1 Características

Para conseguir unas prestaciones mejores, en *Frame Relay* se ofrecen servicios más simples:

X.25 (Nivel 2)	Frame Relay (Nivel 2)
Generación de Flags	Generación de Flags
Transparencia	Transparencia
Código de Redundancia	Código de Redundancia
Descarte de Tramas (con CRC inválido)	Descarte de Tramas (con CRC inválido)
Almacenamiento de Tramas pendientes de ACK	---
Asentimiento de Tramas	---
Generación de Tramas REJ	---
Tratamiento de RR/RNR	---
(... y más funciones ...)	---

Así pues, los equipos que procesan las tramas deben realizar un procesamiento menor.

X.25 (Nivel 3)	Frame Relay (Nivel 3)
Multiplexación	---
Control de Flujo (RR/RNR)	---
Control de Interrupciones	---
Numeros de Secuencia	---
Establecimiento/ liberación de Llamadas	---
(... más funciones...)	---

En *Frame Relay* desaparece el Plano de Usuario al nivel 3. Pero como sabemos que *Frame Relay* ofrece un servicio orientado a conexión nos surge la siguiente pregunta: ¿Qué ocurre con el establecimiento y liberación de las llamadas? Pues que se lleva al plano de control del nivel 3. ¿Y con la función de multiplexación de conexiones? La función de multiplexación se pasa al nivel 2 en FR.

En *FR* se ofrece un servicio orientado a conexión y no fiable, con garantías de caudal mínimo. Resulta importante saber interpretar a qué nos referimos cuando decimos que es no fiable. Nos referimos a que tramas con errores en bits pueden ser detectatas y descartadas en los nodos de la red. Cuando una trama llega a un nodo se comprueba el *CRC*, y si no coincide, la trama se descarta, sin dar ningún aviso a los sistemas finales.

Pero por supuesto, para que ocurra esto, es necesario que antes se haya producido un error en tránsito en una trama; y la probabilidad de que esto ocurra suele ser suficientemente baja. Los protocolos de niveles superiores en los sistemas finales son los encargados de

detectar cuando se ha producido la pérdida de una trama.

Frame Relay ofrece dos tipos de conexiones:

- **Circuitos Virtuales Permanentes** (*PVC*). Están definidos en todos los estándares.
- **Circuitos Virtuales Conmutados** (*CVC*). Éstos sólo han sido definidos en el estándar propuesto por la ITU-T y no por el estándar de facto.

El servicio que suelen ofrecer los operadores de redes *FR* sólo incluye *PVC´*s, y es utilizado típicamente para dar servicios de comunicaciones dentro de una corporación.

13.2. Arquitectura de protocolos

En cada sistema final y sistema intermedio, tenemos dos arquitecturas distintas y separadas: la correspondiente al plano de usuario y la correspondiente al plano de control.

- **Plano de Usuario**:
  Nivel 2: (en la recomendación de ITU-T, el protocolo utilizado es LAP-F)
- **Plano de Control**:
  Nivel 2: *LAP-D*
  Nivel 3: *Q.933* (es una recomendación muy parecida a la *Q.931*, utilizada en *ISDN*)
- A **nivel físico**, hay también una separación de los flujos de información de usuario y de control.

13.3. Nivel de enlace en Frame Relay

Frame Relay utiliza a nivel de enlace el protocolo denominado *LAPF* (*Link Access Procedure for Frame-Mode Bearer Services*), que podemos traducir como 'procedimiento de acceso al enlace para servicios portadores en modo trama'). *LAPF* es una variante simplificada de *HDLC* que suprime la parte correspondiente al reenvío de tramas en caso de error; se construye un *CRC* que permite al destinatario comprobar que la trama ha llegado correctamente, pero si detecta algún error descarta silenciosamente la trama sin informar de ello al emisor (se confía en que los niveles superiores se ocuparán de ello); además *LAPF* requiere que la longitud de la trama a transmitir sea siempre un número entero de octetos. En general *LAPF* es bastante similar a *PPP*.

La longitud de una trama *LAPF* en bits siempre es múltiplo de ocho. Se practica el relleno de bits para conseguir la transparencia de los datos. Existen dos tipos de trama, la de control y la normal que es la que se utiliza para enviar datos. La estructura de una trama *LAPF* normal es la siguiente:

Campo	Tamaño (bytes)	Valor
Delimitador	1	01111110
Dirección	2	Variable
Datos	0-8188	Variable
Checksum	2	Variable
Delimitador	1	01111110

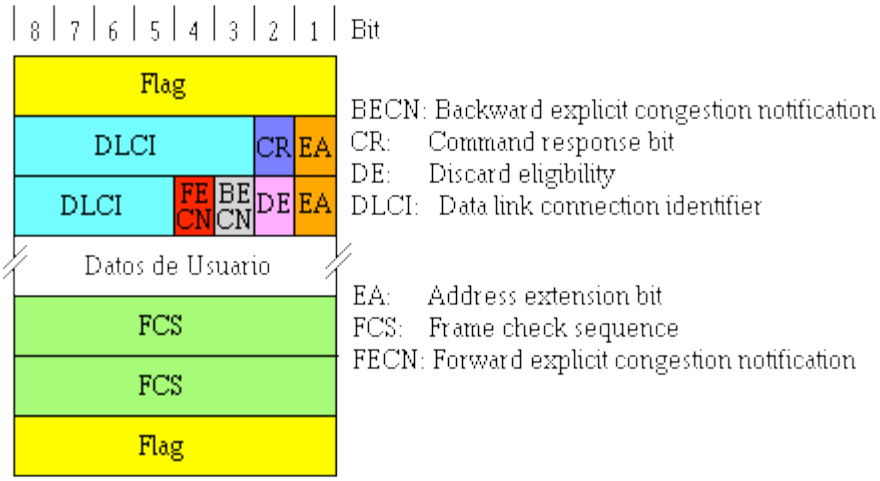


Fig. 44: *Formato de trama en FR.*

13.4. Formato del campo dirección en Frame Relay

Como ya sabemos *Frame Relay* es una red de conmutación de paquetes orientada a conexión; por tanto para que la comunicación sea posible es necesario antes que se establezca un circuito virtual entre dos hosts de la red. Los circuitos virtuales pueden ser permanentes o conmutados, y se identifican mediante los *DLCI* (*Data Link Connection Identifier*) que desempeñan en *Frame Relay* un papel similar a los *VPI/VCI* (*Virtual Path Identifier/Virtual Channel Identifier*) en *ATM* o a los *VCN* (*Virtual Circuit Number*) en *X.25*. Los *DLCI* tienen por defecto 10 bits de longitud, aunque se han definido extensiones que permiten utilizar con *DLCIs* de 16, 17 o 23 bits.

Estructura de una trama Frame Relay

La esencia del funcionamiento de *Frame Relay* se encuentra en el campo *Dirección*, que

tiene la siguiente estructura:

DLCI superior	C/R	0	DLCI inferior	FECN	BECN	DE	1

Fig. 45: *Estructura del campo dirección (por defecto) en una trama LAPF*

El significado de los diversos campos es el siguiente:

DLCI (Data Link Connection Identifier): este campo tiene una longitud total de 10 bits (aunque se encuentre dividido en dos partes). Especifica por que circuito virtual debe circular la trama correspondiente.

C/R (Command/Response): el significado de este bit es específico de la aplicación y no se utiliza en el protocolo *Frame Relay* estándar.

FECN (Forward Explicit Congestion Notification): como su nombre indica este campo de un bit se emplea en el control de congestión del que hablaremos mas tarde.

BECN (Backward Explicit Congestion Notification): lo veremos en el control de congestión.

DE (Discard Elegibility): este bit tiene una finalidad similar al CLP (Cell Loss Priority) de ATM, es decir, sirve para marcar las tramas de 'segunda clase', que son aquellas que el usuario ha metido en la red superando el caudal que tenía contratado.

El estándar prevé también el uso de campos dirección de 3 y 4 bytes con tamaños del DLCI de 16, 17 ó 23 bits; sin embargo el DLCI de 10 bits y la dirección de 2 bytes son los valores por defecto y los formatos extendidos no añaden nada realmente nuevo sobre el modo de funcionamiento de Frame Relay.

Para establecer un SVC en Frame Relay se utiliza el protocolo de señalización Q.933 de la ITU-T, que es un subconjunto del Q.931 utilizado en RDSI. De forma análoga a RDSI o ATM, Frame Relay utiliza señalización *fuera de banda* para establecer la conexión, es decir, se reserva un DLCI especial (el DLCI 0) para las funciones relativas al establecimiento y terminación del SVC. La siguiente tabla compara las funciones de señalización principales de Frame Relay, ATM y RDSI:

	Frame Relay	ATM	RDSI
Protocolo ITU-T de señalización	Q.933	Q.2931	Q.931
Canal de señalización	DLCI 0	VP 0 VC 5	Canal D

13.5. Control de tráfico en Frame Relay

El control de tráfico en Frame Relay se basa en la especificación de varios parámetros, sobre todo el denominado CIR (Committed Information Rate). El CIR se especifica en el momento de configurar los equipos en el caso de conexiones permanentes, o bien es solicitado por el usuario en el momento de efectuar una conexión temporal; en este último caso puede haber un proceso de negociación, es decir, la red puede no ser capaz de satisfacer la capacidad solicitada, en cuyo caso normalmente realiza una contraoferta; el usuario decide entonces si acepta dicha propuesta o si abandona para intentar en otro momento.

El control de tráfico en Frame Relay se realiza de la siguiente forma. El conmutador Frame Relay al que esta conectado el equipo del usuario realiza una monitorización permanente del tráfico que el usuario inyecta en la red por cada conexión virtual que tiene establecida. Si el usuario no supera en ningún momento el CIR sus tramas viajarán todas con el bit DE a cero; sin embargo, si el usuario excede dicha capacidad el conmutador Frame Relay pondrá a 1 el bit DE en aquellas tramas que hayan sido enviadas (en todo o en parte) por encima de la capacidad especificada en el CIR. Un segundo parámetro, conocido como EIR (Excess Information Rate), especifica un caudal que el usuario no deberá superar nunca, ya que las tramas recibidas por encima de este valor serán directamente descartadas por el conmutador.

La implementación práctica del algoritmo que acabamos de describir utiliza en realidad otros dos parámetros:

- B_c: Tamaño de ráfaga comprometida (Committed burst size). Indica la cantidad máxima de bits que la red se compromete a enviar, en condiciones normales, durante un intervalo de tiempo T. Estos datos pueden estar o no contiguos, es decir pueden formar parte de una o de varias tramas.

- B_e: Tamaño de ráfaga excedente (Excess burst size). Indica la máxima cantidad de bits que, además de B_c, podrá el usuario intentar enviar por la red, durante un intervalo de tiempo T. No hay compromiso en la transferencia de estos datos, o dicho con mas precisión, hay una menor probabilidad de que estos datos lleguen a su destino que los que son enviados dentro de B_c.

Entre los parametros B_c y CIR se cumple la relación:

$$B_c = CIR * T$$

Análogamente entre B_e y el EIR se cumple la relación:

$$B_e = EIR * T$$

Para comprender como funciona el control de tráfico en Frame Relay supongamos que un usuario contrata con Telefónica un acceso Frame Relay con una línea física E1, es decir con una capacidad máxima entre su ordenador y el conmutador Frame Relay de 2048 Kb/s. El usuario contrata además un PVC con un CIR de 1024 Kb/s; Telefónica configura el enlace con un EIR de 384 Kb/s y establece el valor de T en 1 segundo (con lo que automáticamente han quedado fijados los valores de B_c y B_e en 1024000 y 384000 bits). Obsérvese que aunque se han definido varios parámetros el único especificado en el contrato del usuario con Telefónica (y el único de cuyo valor el usuario tiene conocimiento oficial) es el CIR.

En esta situación nuestro usuario desea enviar un 'stream' de vídeo en tiempo real a un destino remoto, sin ningún tipo de control de flujo por parte del receptor y sin atender a ninguna notificación de congestión que pueda venir de la red. Supongamos que el usuario dispone de un parámetro en su ordenador mediante el cual puede fijar el caudal de tráfico que inyecta en la red. Supongamos también que el envío se hace utilizando siempre tramas de 50000 bits (6250 bytes). Si el usuario fija el flujo de datos a transmitir en 2000 Kb/s estará inyectando en el conmutador Frame Relay 40 tramas por segundo; en estas condiciones las primeras veinte tramas serán aceptadas sin más, las ocho siguientes serán aceptadas pero se les pondrá a uno el bit DE ya que superan el valor de B_c, y las doce restantes serán simplemente descartadas puesto que superan el valor de B_e.

Si el usuario reduce ahora el caudal a 1400 Kb/s enviará 28 tramas por segundo, 20 de las cuales tendrán el bit DE a cero y las ocho siguientes a uno; de esta forma el usuario está aprovechando casi al máximo la capacidad de la red, pero no tiene la seguridad de que todas las tramas lleguen a su destino.

Por último, si el usuario quiere tener máximas garantías de que todas las tramas llegarán a su destino deberá reducir el flujo a un valor no superior al CIR, por ejemplo a 1000 Kb/s, en cuyo caso emitirá 20 tramas por segundo y todas serán enviadas con el bit DE a cero.

Conviene destacar el hecho de que, independientemente del flujo que el usuario especifique en su aplicación, el enlace físico es en todos los casos de 2048 Kb/s con lo que una trama de 50000 bits siempre se transmitirá en 24,4 ms; así en el caso de transmitir un flujo de 2000 Kb/s el emisor está 24,4 ms enviado y 0,6 ms esperando; en caso de transmitir a 1000 Kb/s el emisor está 24,4 ms enviando y 25,6 ms esperando.

El bit DE también puede ser puesto de forma voluntaria por el usuario. Esto es interesante si el usuario (o la aplicación) puede identificar algunas tramas como mas importantes que otras. Por ejemplo en vídeo comprimido MPEG existen unos fotogramas que son de referencia, y otros que son interpolación de los anteriores y posteriores. Si se pierde un

fotograma de referencia la calidad se ve mucho mas afectada que si se trata de uno de interpolación. En nuestro ejemplo, en el caso de transmitir a 1400 Kb/s (28 tramas por segundo) la aplicación podría elegir en cada grupo de 28 tramas ocho que correspondan a fotogramas de interpolación y marcarlas, con lo que evitará que el conmutador Frame Relay asigne indiscriminadamente el bit DE a las últimas ocho tramas de cada intervalo, que podrían contener algún fotograma de referencia.

Podemos explicar el mecanismo de control de tráfico de Frame Relay mediante el modelo del pozal agujeread. En primer lugar tenemos un pozal agujereado, que denominamos pozal 'C', donde ρ = CIR y C = B_c; además tenemos el pozal 'E' con ρ = EIR y C = B_e que de alguna manera recoge todo el tráfico derramado por el primero (o el que el usuario voluntariamente quiere poner en él) y que envía tráfico de segunda clase, con menores garantías de llegar a su destino.

Si analizamos el ejemplo anterior con el modelo del pozal agujereado nos llevaremos alguna sorpresa. Supongamos el caso concreto en que nuestro usuario deseara enviar el stream de vídeo a 2000 Kb/s, pero únicamente desea hacerlo durante un segundo; antes habíamos llegado a la conclusión de que de las 40 tramas enviadas cada segundo 20 lo eran normalmente, 8 llevaban el bit DE puesto y 12 eran descartadas. En realidad esa conclusión solo es correcta en el caso de que se envíe el flujo de 2000 Kb/s de manera sostenida. Analicemos que ocurriría si se envía ese caudal únicamente durante un segundo; pasados 500 milisegundos el usuario ha introducido en el pozal C las 20 tramas que caben en él, por lo que la siguiente ya debería pasar al pozal E y consecuentemente llevar puesto el bit DE. Sin embargo, si pensamos un momento nos daremos cuenta de que en 500 milisegundos el pozal C ha tirado a la red una cantidad de tráfico igual a CIR * 0,5 = 512000 bits, o sea 10 tramas; cabrán pues 10 tramas más en el pozal C (estrictamente serán 9 ya que la primera trama no puede ser enviada hasta pasados 24,4 milisegundos); pasados 750 milisegundos han entrado en el pozal 30 tramas y han salido 15, con lo que el pozal aún no está lleno. Para este caso concreto podemos calcular el número de tramas enviadas por el pozal C en un tiempo t dado con la fórmula:

$$\text{Tramas enviadas} = (t-0{,}0244) * 1024000 / 50000 = (t - 0{,}0244) * 20{,}48$$

Por otro lado, las tramas recibidas en el pozal en un tiempo t serán:

$$\text{Tramas recibidas} = t * 2000000 / 50000 = t * 40$$

Suponiendo que antes estuviera vacío el pozal C se llenará cuando:

$$\text{Tramas recibidas} = \text{Tramas enviadas} + B_c/50000$$

O sea:

$$t * 40 = (t-0{,}0244) * 20{,}48 + 20{,}48$$

De aquí podemos calcular que t = 1,02 segundos, es decir, que con los parámetros que hemos puesto en este ejemplo las 40 primeras tramas se transmiten sin que ninguna sea descarta, ni siquiera marcada con el bit DE. Una vez llenado el pozal C empezaría a llenarse el pozal E de la misma forma, y finalmente una vez llenos ambos pozales se cumpliría el resultado que habíamos obtenido al principio.

Obsérvese como el mecanismo del pozal agujereado aumenta considerablemente la elasticidad de la red frente a tráfico a ráfagas.

En la figura siguiente se puede entender más claramente el significado de los parámetros antes mencionados.

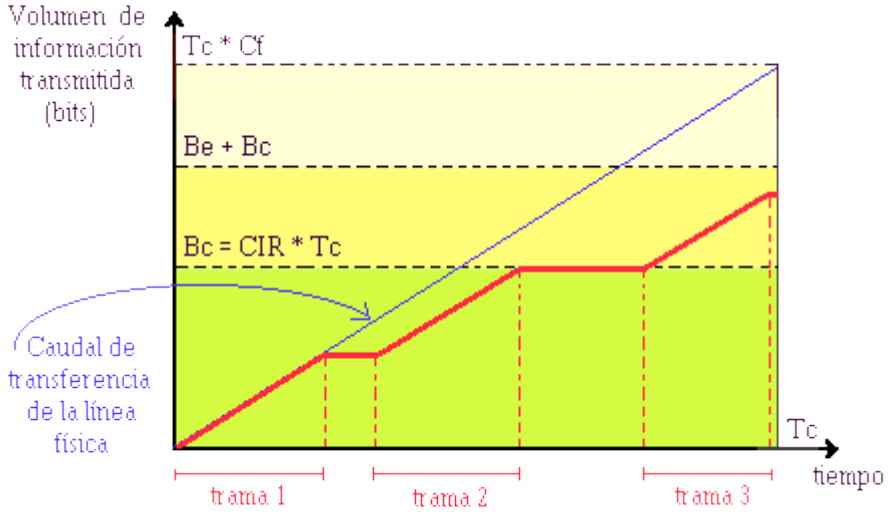


Fig. 46: *Parámetros de transmisión en FR.*

Se puede observar que el volumen de información (bits) generado por las tramas 1 y 2 se encuentra por debajo del máximo garantizado Be y por tanto se nos garantiza que estas dos tramas serán cursadas por la red sin ningún problema. Con la trama 3, sin embargo, se excede el límite Be, pero sin llegar a la cantidad Be + Bc. La red marca esta trama poniendo su bit DE a '1' lo que indica que si hay que descartar tramas por congestión, esta trama se descartará en preferencia al resto.

Si se diera el caso de transmitir durante todo Tc de forma que con una cuarta trama se sobrepasara Be + Bc, esta trama sería incondicionalmente descartada en el nodo que está conectado al sistema que la ha enviado.

Pregunta:

Ahora nos surge la siguiente pregunta: Manteniendo el CIR, ¿qué le conviene más a un abonado, un Tc grande o pequeño? Al usuario le resulta atractivo que Tc sea muy grande, porque Bc también lo será, y aunque en media se deba mantener la velocidad CIR, está capacitado para enviar ráfagas de datos mayores, pues el límite de datos máximo (Bc) ha aumentado.

Para el operador es conveniente que Tc baje. Con Tc grande, si todos los usuarios deciden mandar simultáneamente ráfagas de tráfico de longitud máxima Bc, podría encontrar problemas para cursar todo el tráfico por la red
Generalmente cuando se envía una trama se desconoce el estado de la red. Tramas por encima de Bc son susceptibles de ser descartadas cuando la congestión de la red aumenta en las rutas que atraviesan dichas tramas. Por ello la red notifica este aumento de la probabilidad de descarte de tramas mediante los bits FECN y BECN. Se requiere que los terminales actúen de forma coherente y reduzcan el tráfico enviado a la red, porque de lo contrario las tramas de usuario que superen Bc están en peligro de ser descartadas en nodos de red congestionados.

Hay que señalar que la congestión es unidireccional, pues puede haber caminos distintos para los dos sentidos de la transmisión y mientras uno puede estar sufriendo problemas de tráfico, el otro puede no tenerlos. Los bits FECN y BECN notifican congestión a los dos extremos de una conexión de la siguiente forma: A una trama que atraviesa una zona congestionada se le pone su bit FECN a '1'. La red identifica las tramas de esa conexión que circulan en sentido contrario y en ellas marca el bit BECN también a '1'.

Pregunta:
¿ Por qué se notifica al destino la congestión? Para que sea consciente de que se pueden estar perdiendo tramas que tienen marcado el bit DE a '1', y porque algunos protocolos de niveles superiores tienen capacidad de control de flujo extremo a extremo y pueden tomar medidas al respecto.

13.6. Algunas conclusiones

Frame Relay no es un protocolo especialmente diseñado para soportar tráfico multimedia, audio y vídeo en tiempo real. No hay garantías sobre el retardo de tránsito, pero en la práctica las redes suelen estar bien dimensionadas y el retardo de tránsito es pequeño y no varía apreciablemente.

Además la disponibilidad de estas redes es muy alta, y por todo ello muchas compañías usan redes FR para cursar este tipo de tráfico. En general se considera que son suficientemente buenas para cursar tráfico telefónico, en el que lo más importante (más que la probabilidad de error) es tener una elevada disponibilidad.