Redes de ordenadores

Xavier Vilajosana Guillén
Miquel Font Rosselló
Eduard Lara Ochoa
René Serral i Gracià

PID_00171189

Universitat Oberta de Catalunya
www.uoc.edu

Índice

Introducción

Las redes de ordenadores actuales son una composición de dispositivos, técnicas y sistemas de comunicación que han ido apareciendo desde finales del siglo XIX con la invención del teléfono. El teléfono se desarrolló exclusivamente para transmitir voz, aunque hoy todavía se utiliza, en muchos casos, para conectar ordenadores entre sí. Desde entonces han aparecido las redes locales, las conexiones de datos a larga distancia con enlaces transoceánicos o satélites, Internet, la telefonía móvil, etc.

Dedicaremos este módulo a introducir las ideas y los conceptos básicos de las redes de ordenadores que trataremos en profundidad a partir de ahora. En primer lugar, introduciremos los conceptos fundamentales de una red: las topologías de red y los conceptos de conmutación, el hardware y el software. Es importante tener una visión general de la tipología de red, normalmente clasificada por su alcance. En segundo lugar, presentaremos las diferentes tecnologías de red más relevantes en la actualidad (Ethernet u 802.3 es la más usada en redes de área local por cable). Las tecnologías de red inalámbricas se han estandarizado en la última década y tienen su mayor exponente en el 802.11 o WiFi, que es usado por la mayoría de dispositivos de usuario en red.

El módulo profundiza en la definición de una red de ordenadores y nos presenta el modelo de referencia de una red, constituida por diferentes niveles, que permiten abstraer las complejidades derivadas de la transmisión de la información. Como veremos, cada nivel de la red ofrece servicios al nivel que le precede mientras usa los servicios del anterior. Cuando se quiere transmitir una información, ésta se transmite entre los diferentes niveles de la red, encapsulando la información de los niveles que le preceden y añadiendo nueva información que le permite al receptor recuperar la información original.

Veremos que, en un principio, se definió una jerarquía de siete niveles denominada OSI que evolucionó hacia el modelo de red actual, el modelo TCP/IP que en la actualidad rige el funcionamiento de Internet. Por último, el módulo repasa brevemente la historia de las comunicaciones. Conocer la historia nos permite tener una buena perspectiva de estas tecnologías y entender por qué se han creado, cómo han evolucionado y por qué tenemos el modelo de comunicación actual.

1. Concepto de red

Durante las dos primeras décadas de existencia de los ordenadores, éstos eran sistemas hardware muy centralizados y normalmente estaban ubicados en un único espacio físico. Las empresas y los centros que poseían un ordenador guardaban en éste todas las necesidades computacionales de la institución. A medida que las capacidades de los ordenadores aumentaban, la centralización se convirtió en un problema tanto de gestión como de recursos.

El modelo centralizado se fue sustituyendo por un modelo en el que múltiples ordenadores con menor capacidad, pero interconectados entre sí, eran capaces de realizar las tareas de un ordenador centralizado. Esta nueva organización se denominó **red de ordenadores**.

El diseño y la arquitectura de la red son los aspectos que trataremos durante este curso.

1.1. Hardware de red

Las redes de computadores se pueden clasificar de diferentes modos. Generalmente, estas clasificaciones se realizan basándose en la topología, el tipo de conmutación, el alcance y la tecnología de la red, entre otros aspectos. Este bloque detalla tales diferencias de clasificación y ofrece la base necesaria para poder entender posteriormente el diseño de protocolos existentes en la actualidad.

1.1.1. Topologías de red

Una topología de red es el modo en el que están distribuidos los nodos que la forman. Las redes actuales están formadas por tres tipos de entidades: los equipos finales[1], los equipos intermedios (encaminadores[2] o conmutadores) y los enlaces[3], que unen los equipos finales y los encaminadores entre sí.

(1)En inglés, *hosts*.

(2)En inglés, *routers*.

(3)En inglés, *links*.

Las topologías más conocidas son:

1) Bus. Todos los equipos están conectados a un único medio de transmisión compartido entre todas las estaciones de la red, por lo tanto, es necesario establecer un sistema de acceso al medio para evitar que más de una estación transmita al mismo tiempo y se produzcan colisiones. En la figura 1a podemos ver un ejemplo de topología en bus.

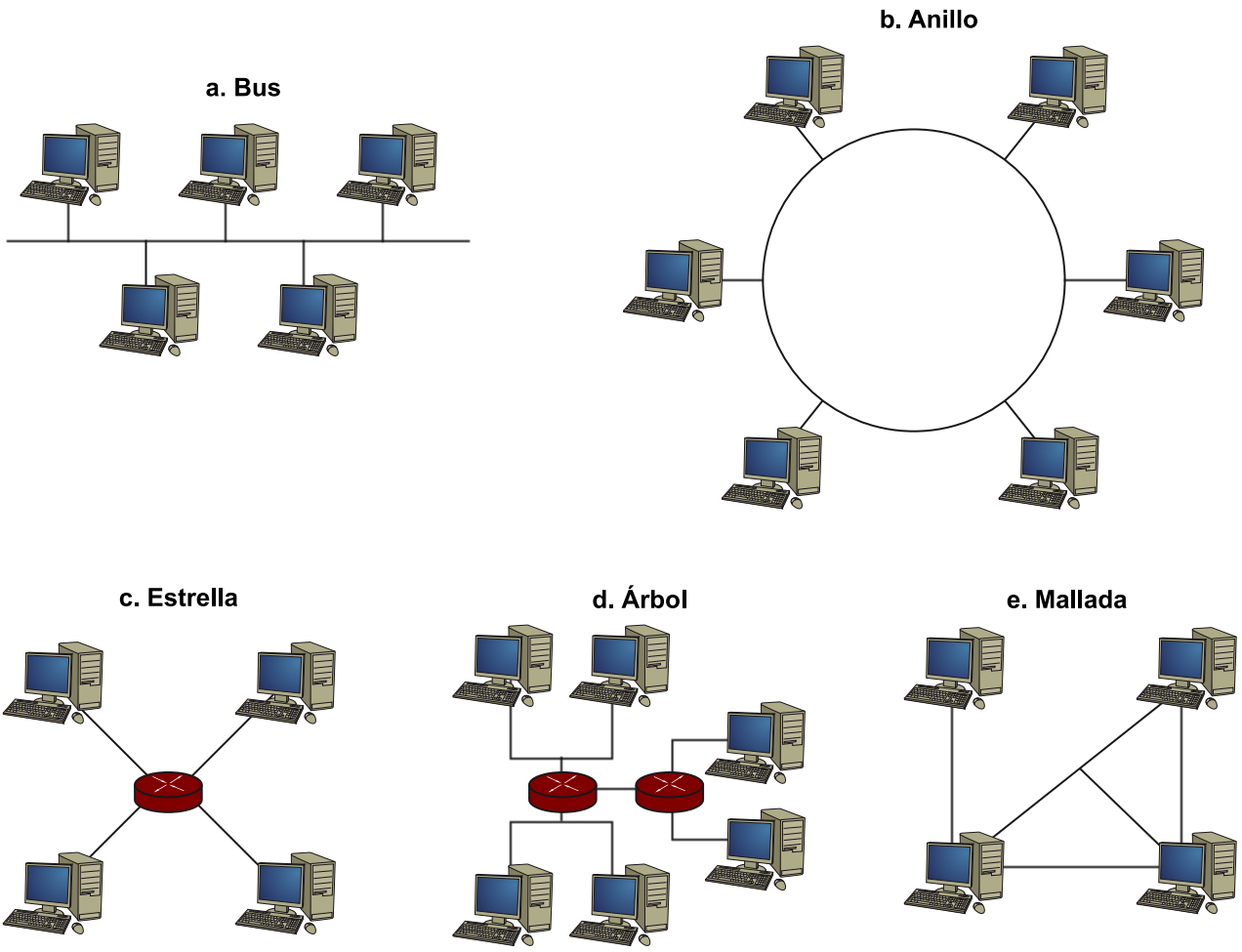
2) Anillo. Como muestra la figura 1b, una topología en anillo está formada por un enlace que forma un bucle, de manera que cada estación está conectada al anillo mediante dos enlaces, el de entrada y el de salida. Generalmente, cuando la estación emisora recibe su propio paquete lo elimina de la red.

3) Estrella. Esta topología (figura 1c) está formada por un nodo central, que actúa como nodo intermedio de la red (conmutador o encaminador) y gestiona el envío y la recepción de los datos. El resto de estaciones se conecta a este nodo principal.

4) Árbol. Una topología en árbol es una topología mixta de las topologías en bus y en estrella. A veces también se conoce como topología jerárquica. Un ejemplo es el de la figura 1d, en la que varios nodos intermedios se conectan entre sí y a su vez tienen conectados equipos finales. Esta topología es la más utilizada en la actualidad.

5) Mallada. La topología mallada es aquella en la que todos los equipos están conectados con todos los del resto. Existen casos de redes malladas parciales, es decir, en los que las estaciones no forman una malla completa. Generalmente, esta topología se emplea en el núcleo de grandes redes, como Internet, en la que sólo se conectan equipos intermedios, no finales.

Figura 1. Ejemplos típicos de topologías de red



1.1.2. Tipos de conmutación

En el ámbito de las redes, la conmutación hace referencia al establecimiento de un circuito (real o lógico) entre dos puntos de la red que permite la interconexión y, por lo tanto, el traspaso de información entre esos puntos. En esencia, esta conmutación se puede dividir en dos clases diferentes: la conmutación de circuitos y la conmutación de paquetes.

Conmutación de circuitos

La conmutación de circuitos se basa en la creación de un circuito físico entre los dos interlocutores de la red. Este circuito físico se establece antes de transmitir cualquier tipo de información y está formado por diferentes enlaces entre los nodos.

RTB

El ejemplo clásico de conmutación de circuitos es la antigua red telefónica básica (RTB), en la que, mediante centralitas situadas jerárquicamente en la red, se multiplexan los circuitos de voz y se dirigen a su destinatario. En la actualidad, en plena era digital, este establecimiento del circuito se produce sólo desde el teléfono del usuario hasta la centralita más próxima, en la que se digitaliza la voz y se utilizan otras técnicas para enviar la información, como la conmutación de paquetes.

En conmutación de circuitos se distinguen tres fases para el envío de información:

1) Establecimiento del circuito. Esta fase se encarga de buscar un camino entre los nodos intermedios que lleven al destino. La estación origen pide la creación del circuito al nodo al que está conectada, que a su vez envía la petición al siguiente nodo. Este otro nodo hará lo mismo respecto al siguiente, y así hasta llegar al destino final. A medida que se va formando el circuito, cada nodo intermedio verifica la existencia de suficientes recursos para establecerlo, y en el caso de que no sea así se aborta la petición de circuito. En el caso de que el establecimiento no sea viable, cuando llegue al destino éste enviará una señal al origen para comunicar que ya puede enviar información.

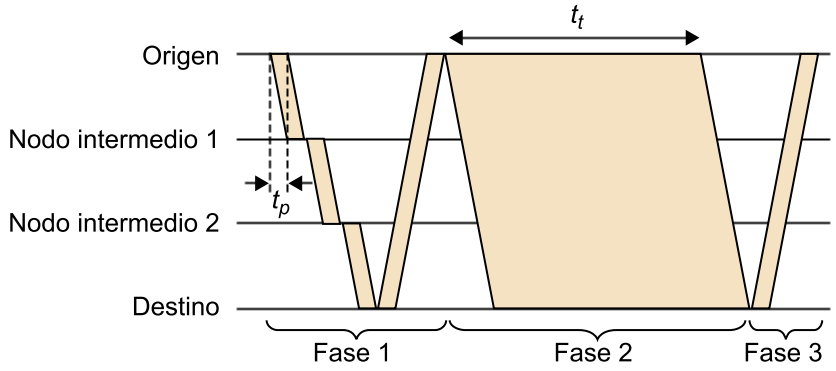
2) Transferencia de datos. En este caso las estaciones pueden intercambiar la información deseada.

3) Desconexión. Una vez que se ha acabado la comunicación se deben liberar los recursos, para estar más adelante a disposición de otras conexiones.

Ejemplo de creación de circuitos

Un ejemplo de creación de circuitos es el que se muestra en el diagrama de tiempo en la figura 2. La figura muestra las tres fases en el caso de que haya dos nodos intermedios. El diagrama de tiempo se debe interpretar de izquierda a derecha, con la evolución temporal, en la que cada bloque representa el envío de información al siguiente nodo.

Figura 2. Diagrama de tiempo del establecimiento de un circuito



Como se puede ver en la figura, las líneas tienen una cierta inclinación, lo que indica el tiempo de propagación de la señal, mientras que el grueso de cada bloque indica el tiempo de transmisión necesario para enviarla. Inicialmente, en el establecimiento del circuito cada equipo intermedio tiene que procesar la señal y enviarla al siguiente nodo, por ello, antes de enviarlo hay que contar con toda la información del circuito. Una vez establecida, ya puede funcionar de un extremo a otro, con transparencia y sin más retrasos adicionales por parte de los nodos intermedios.

Conmutación de paquetes

Uno de los principales problemas que encontramos en la conmutación de circuitos es la exclusividad de los recursos, ya que, cuando existe un circuito creado, aunque no haya datos pasando por el circuito, los recursos están reservados y no pueden ser utilizados por ninguna otra estación. El problema se ve agravado porque en conexiones de datos como las actuales el tráfico, en

lugar de ser constante, llega a ráfagas. Por ejemplo, cuando el usuario carga una página web, la carga sólo implica unos pocos centenares de milisegundos, mientras que su lectura puede suponer minutos. Otro problema impuesto por la conmutación de circuitos es el de la necesidad de que todos los nodos de la comunicación trabajen a la misma velocidad, ya que los nodos intermedios no realizan ningún proceso de información, hecho que no es cierto en una red actual, en la que cada usuario tiene una velocidad diferente que, a la vez, es distinta de la que disponen los operadores.

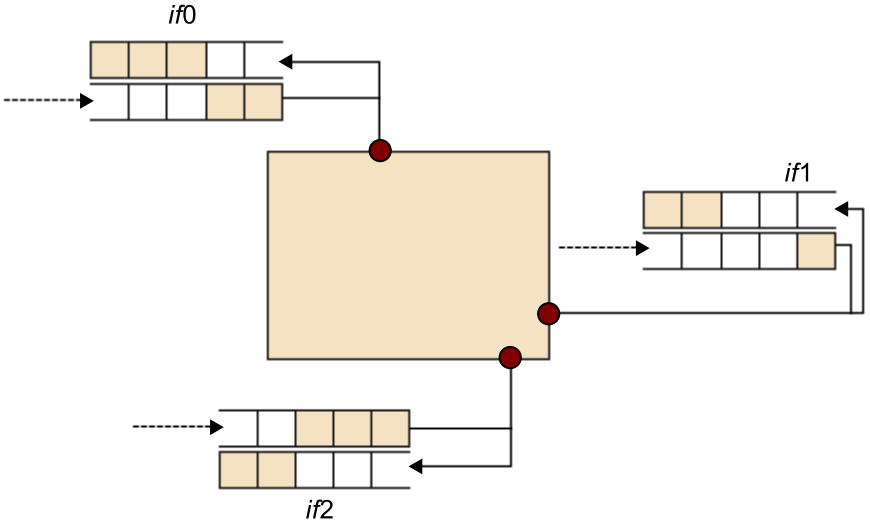
Así, con el fin de mejorar la conmutación de circuitos en estas nuevas necesidades, se diseñó la conmutación de paquetes con los siguientes objetivos:

- Optimizar el empleo de los canales de comunicación.
- Interconectar terminales con diferentes velocidades.
- Crear conexiones simultáneas sin reserva de recursos.

De este modo, la conmutación de paquetes, en lugar de reservar recursos con un circuito, dota a los nodos intermedios de capacidad de proceso y de un sistema de colas que permite almacenar temporalmente un paquete, localizar a su destinatario y enviarlo al nodo que corresponda.

Como se ha comentado, la conmutación de paquetes debe permitir diferentes velocidades de transmisión, por esa razón se utilizan las colas de recepción y transmisión, tal como muestra la figura 3. En ésta se puede comprobar que un nodo de conmutación está compuesto por interfaces, que a su vez están formadas, entre otras cosas, por una cola de entrada y otra de salida al sistema, y que son utilizadas para controlar el acceso al nodo de conmutación, que ahora, en lugar de ser pasivo, procesa todos los paquetes que llegan por las colas de entrada y los sitúa en la cola de salida de la interfaz correspondiente para ser enviados.

Figura 3. Colas en la conmutación de paquetes



Las colas del nodo de conmutación tendrán un tamaño determinado, lo que implica que si una cola se llena antes de ser procesada, habrá paquetes que deben ser descartados.

Ved también

Ved cómo la red gestiona y evita la pérdida de paquetes descartados en el apartado 3 de este módulo didáctico.

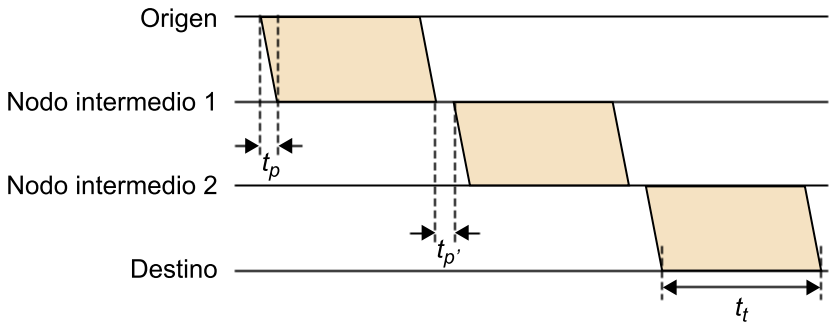
Otra consideración importante en este entorno es el tamaño del paquete que se quiere transmitir. En un principio, se pensó que los paquetes tuvieran el mismo tamaño que el mensaje que iba a ser enviado (conmutación de mensajes), pero enseguida se vio que para mensajes grandes los nodos intermedios necesitaban demasiada memoria (ya que almacenan el paquete en su totalidad antes de enviarlo y, por ello, requieren demasiado tiempo para procesarlo). En consecuencia, hoy se dividen los mensajes en un tamaño máximo fijado (generalmente, 1.500 bytes).

Conmutación de mensajes y de paquetes

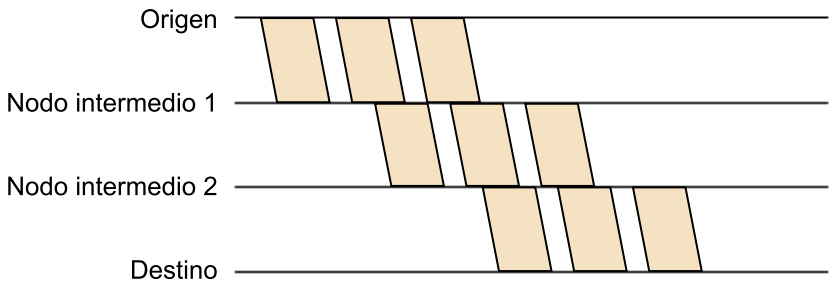
Un ejemplo de esto se puede encontrar en la figura 4, en la que las dos subfiguras muestran el envío del mismo mensaje, primero con conmutación de mensajes y después con conmutación de paquetes. Como se puede ver en este ejemplo, el mensaje ha sido enviado con tres paquetes diferentes de tamaño inferior. Debido al almacenamiento en los nodos intermedios (*store and forward*), la conmutación de paquetes es generalmente más rápida.

Figura 4. Funcionamiento de la conmutación de paquetes y mensajes

a. Conmutación de mensajes



b. Conmutación de paquetes



t_p: Tiempo de propagación $t_{p'}$: Tiempo de proceso t_t: Tiempo de transmisión

Conmutación de paquetes con circuito virtual

Aunque la conmutación de paquetes es mejor que la conmutación de mensajes, ambas soluciones tienen el problema de que, según el tamaño y el estado de las colas de los nodos intermedios, el retraso en la llegada de la información varía, lo que implica que en comunicaciones críticas en tiempo (como

una conversación de voz), esto pueda llegar a ser un problema. Por ejemplo, si un paquete de voz llega demasiado tarde, no podrá ser decodificado y el interlocutor notará un pequeño corte en la conversación. Para minimizar este problema apareció la denominada conmutación de paquetes con circuito virtual, cuyo objetivo es asumir las ventajas de los dos paradigmas. Así, en lugar de enviar independientemente todos los paquetes de una conexión, los circuitos virtuales deciden antes el camino (como sucede en la conmutación de circuitos), pero manteniendo el envío de paquetes individuales. De este modo, todos los paquetes seguirán el mismo camino y podremos contar con una reserva de recursos.

1.1.3. Alcance de las redes

Una clasificación bastante clásica de las redes es aquella que valora su alcance, aunque según el entorno esta clasificación puede cambiar. Generalmente se consideran dos categorías: las redes de gran alcance (WAN[4]) y las redes de alcance local (LAN[5]).

(4)WAN es la sigla de *wide area networks*.

(5)LAN es la sigla de *local area networks*.

Antes de detallar qué son las LAN y las WAN, es conveniente introducir los conceptos de redes de difusión y redes punto-a-punto. Una red de difusión[6] es aquella en la que el medio es compartido por las estaciones que forman la red, de manera que todos los equipos reciben todos los paquetes, aunque sólo procesan los dirigidos a ellos. Entre otras cosas, esto implica serios problemas de privacidad, por ello, en este tipo de redes es recomendable utilizar mecanismos de cifrado en las conexiones, como en las redes inalámbricas.

Otras redes según su alcance

Existen otras categorías, como las redes metropolitanas (MAN, *metropolitan area networks*) o las redes personales (PAN, *personal area networks*), pero normalmente pueden ser incluidas dentro de las redes LAN.

Las redes punto-a-punto, en contraposición a las redes de difusión, son aquellas en las que las conexiones se encuentran entre dos puntos determinados de la red. A pesar de que un enlace punto-a-punto puede parecer poco flexible, en realidad es el tipo de conexión más utilizado actualmente, ya que puede ser extendido para formar topologías de estrella, árbol o malladas de un modo muy sencillo. Los enlaces punto-a-punto, según el sentido de la comunicación que permiten, pueden ser:

(6)En inglés, *broadcast*.

- **Simplex**: la comunicación es unidireccional, de los dos puntos, uno siempre es el origen y el otro, el destino.

- **Semidúplex**[7]: la comunicación puede ser bidireccional, pero siempre y cuando los dos puntos de la comunicación alternen en la generación de tráfico, dado que si la enviaran al mismo tiempo, se produciría una colisión que invalidaría ambas transmisiones.

(7)En inglés, *half-duplex*.

- **Dúplex**[8]: el caso más común actualmente. Es cuando el medio está preparado para poder enviar y recibir información de manera simultánea sin ningún problema.

(8)En inglés, *full-duplex*.

Debemos señalar que con las comunicaciones bidireccionales la velocidad puede ser igual (conexión simétrica) o diferente, en función del sentido de la comunicación (conexión asimétrica).

Redes de gran alcance

Las redes de gran alcance son aquellas que se utilizan en espacios geográficos extensos. Generalmente, las WAN se encargan de la interconexión de LAN, lo que facilita la conexión de los usuarios de diferentes localizaciones.

La transmisión de los datos suele realizarse mediante grandes operadoras de comunicaciones con líneas de comunicación contratadas[9], utilizando infraestructuras que se consideran públicas (para evitar monopolios). Las conexiones WAN son prácticamente siempre punto-a-punto, exceptuando los enlaces vía satélite, que por el hecho de utilizar el aire como medio de transmisión son inherentemente medios de difusión. Por su gran extensión, las redes WAN, en general, están compuestas por una topología de árbol, que a su vez está conectada a topologías malladas, formadas por miles de nodos.

[9] En inglés, *leased lines*.

Redes de área local

Por el contrario, las LAN están diseñadas para tener un alcance más reducido en las WAN. Esta distancia puede oscilar entre unos pocos kilómetros y algunos metros (e incluso centímetros).

Las tecnologías LAN están pensadas para conectar usuarios con pocos equipos, edificios empresariales e incluso campus enteros. Normalmente, estas LAN se acaban conectando a WAN. En la actualidad, esta interconexión masiva de LAN y WAN se suele conocer como Internet.

Las LAN se han caracterizado por emplear un medio de difusión para enviar información, pero desde la aparición de conmutadores y otros equipamientos más actuales, han pasado, mediante topologías de árbol y estrella, a ser un conjunto de conexiones punto-a-punto. La excepción a esta regla vuelven a ser las redes que utilizan el aire como medio de transmisión, es decir, las redes inalámbricas que emplean difusión para enviar la información. Cabe señalar que existen muchos tipos de redes inalámbricas y que no todos pueden ser clasificados como LAN. Por ejemplo, las redes de telefonía móvil.

1.1.4. Tecnologías de red

La última clasificación del hardware de red hace referencia a las diferentes tecnologías existentes para crear una red. La lista de tecnologías de red existentes en la actualidad es demasiado extensa para poder listarla. A continuación enunciaremos las tecnologías más importantes en la actualidad. La lista incluye las tecnologías por cable y las tecnologías inalámbricas.

Tecnologías de red cableada

Dentro de las redes cableadas, la familia de tecnologías por excelencia es Ethernet (definida en estándar IEEE 802.3). Ésta empezó como una tecnología en 10Mbps con una topología de bus y medio compartido, y ha ido evolucionando a una topología de estrella de 1Gbps (Gigabit Ethernet) pasando por Fast Ethernet, muy utilizada en la actualidad a 100Mbps.

Asimismo, existen modelos de 10 Gigabit Ethernet, pero su implantación todavía está en sus inicios. A pesar de empezar siendo una tecnología limitada a LAN, el bajo coste y su gran adopción permitieron que Ethernet evolucionara hasta el punto de existir hoy enlaces WAN construidos con esta tecnología.

Respecto a las topologías basadas en anillo, como Token Ring (IEEE 802.5) y FDDI (definido en el estándar ANSI X3T12), éstas han ido cayendo en desuso, comparadas con Ethernet. La razón principal es su elevado coste y su peor rendimiento. Actualmente, una topología de anillo muy utilizada es *resilient packet ring* (IEEE 802.17), una tecnología para transportar otras tecnologías mediante anillos de fibra óptica, y que en general transporta directamente tráfico Ethernet y servicios IP.

Tecnologías de red inalámbricas

Un punto en el que ha habido una gran expansión en los últimos años es el de la aparición de tecnologías de red inalámbricas. De este tipo de redes se pueden extraer principalmente dos tipos, las redes de telefonía móvil y las redes inalámbricas de más corto alcance.

Existen muchos tipos de redes de telefonía móvil. Podemos destacar el GSM[10], que fue uno de los primeros sistemas que apareció y que permitió un envío de datos de 9.6Kbps, hasta convertirse en el actual GPRS[11], que posee un ancho de banda máximo teórico de 171.2Kbps, y cuyos canales efectivos de descarga y de subida son 64Kbps y 14Kbps, respectivamente. La última implementación en tecnologías de redes móviles es UMTS[12], también conocido como

(10)GSM es la sigla de *global system for mobile communications*.

(11)GPRS es la sigla de *general packet radio service*.

(12)UMTS es la sigla de *universal mobil telecommunication services*.

sistema de tercera generación (3 GR). Sus sistemas más avanzados permiten alcanzar velocidades teóricas de 21Mbps, aunque sus velocidades efectivas son de 7,2Mbps para descarga y 384Kbps para subida.

Respecto a las redes inalámbricas de más corto alcance, la tecnología usada por excelencia es la LAN inalámbrica[13] (WiFi - IEEE 802.11), que inicialmente fue definida con una velocidad de 11Mbps, pero cuyas posteriores revisiones del estándar permitieron un diseño capaz de soportar velocidades de 54Mbps, con un alcance aproximado de 100 m. En los últimos años, con el fin de reducir el consumo energético de las comunicaciones inalámbricas con equipos de baja potencia, ha aparecido el estándar *de facto* para la comunicación de equipos pequeños (móviles, PDA, etc.). Nos referimos a *Bluetooth*, que posee una velocidad de 1Mbps y un alcance aproximado de 10 m, además de contar con un consumo energético muy bajo que lo hace muy atractivo para transferencias de datos cortos.

(13)En inglés, *wireless LAN* (*WiFi*).

Finalmente, una tecnología situada entre el corto y el largo alcance es WiMAX (IEEE 802.16), una tecnología inalámbrica muy utilizada en la actualidad para dar conectividad a zonas aisladas y de difícil acceso, en las que la comunicación cableada resulta muy cara. WiMAX tiene una velocidad máxima aproximada de 150Mbps de descarga y 35Mbps de subida, con un alcance de unos 70 km.

1.2. Software de red

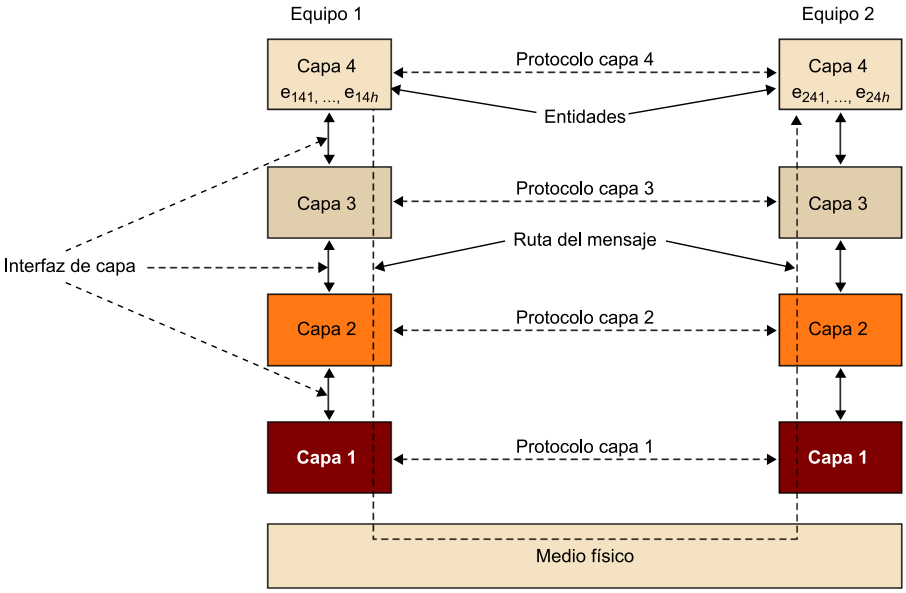
Al principio, cuando aparecieron las redes de ordenadores, los fabricantes realizaban los diseños pensando en que todo el proceso de red se efectuaría mediante hardware, y asumían que los protocolos y los mecanismos empleados serían propietarios, sin un sistema estándar ni un consentimiento conjunto entre los fabricantes para interactuar.

En cualquier caso, a medida que fueron evolucionando las redes se observó que si no se planteaba algún tipo de estandarización, una vía común que permitiera interconectar tecnologías y utilizar mecanismos regulados, los esfuerzos de cada fabricante serían demasiado grandes y la lucha no beneficiaría nadie. Fue entonces cuando fabricantes como IBM comprendieron que era más viable pasar una buena parte de la carga de la red al software, mucho más flexible y barato de producir que el hardware. De este modo apareció lo que se conoce como las arquitecturas de red organizadas por capas, cuyos ejemplos más importantes son OSI[14] y TCP/IP[15].

(14)OSI es la sigla de *open systems interconnection*. En castellano, *interconexión de sistemas abiertos*.

(15)TCP/IP es la sigla de *transmission control protocol/Internet Protocol*.

Figura 5. Ejemplo de arquitectura de red con 4 capas



1.2.1. Arquitectura de la red: diseño por capas

Históricamente, las primeras redes se designaron básicamente teniendo en cuenta sólo el hardware de las comunicaciones. Esta estrategia no tuvo mucho futuro. En la actualidad, el software de red está muy estructurado.

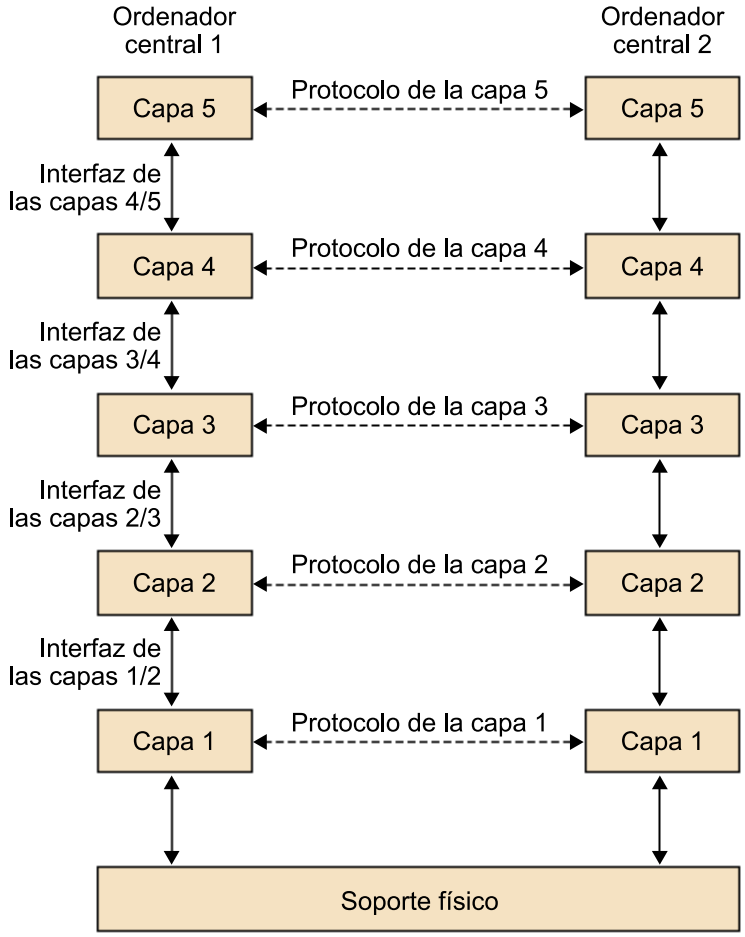
Para reducir la complejidad del diseño, las redes están organizadas en una serie de capas o niveles, cada una situada sobre otra. El número, el nombre, el contenido de cada capa y las funciones de cada capa difieren de un tipo de red a otra. En todas las redes, el objetivo de cada capa es el de ofrecer determinados servicios en las capas superiores, escondiendo en las capas inferiores los detalles sobre el modo en el que se implementan los servicios ofrecidos.

La capa de nivel *N* de un ordenador mantiene comunicación con la capa de nivel *N* de otro ordenador. Estas reglas y convenciones usadas en la capa de nivel *N* se denominan *protocolo*. En esencia, un protocolo es un acuerdo entre las partes de la comunicación sobre cómo se realiza ésta.

En la figura 6 se muestra una pila de protocolos: las entidades que utilizan las correspondientes capas en los diferentes ordenadores se denominan *par*[16]. Es decir, los pares se comunican usando un protocolo.

(16)En inglés, *peers*.

Figura 6



En realidad, la información no se transfiere directamente de una capa *N* de una máquina a la capa *N* de otra máquina. Cada capa pasa la información y el control de ésta a la capa inmediatamente inferior, y así sucesivamente hasta llegar a la última capa. Esta última capa se denomina *capa física*, en la que se produce la comunicación real. En la figura 6, la comunicación virtual (capa *N* con capa *N*) se muestra en líneas punteadas, y la comunicación física o real en la capa física.

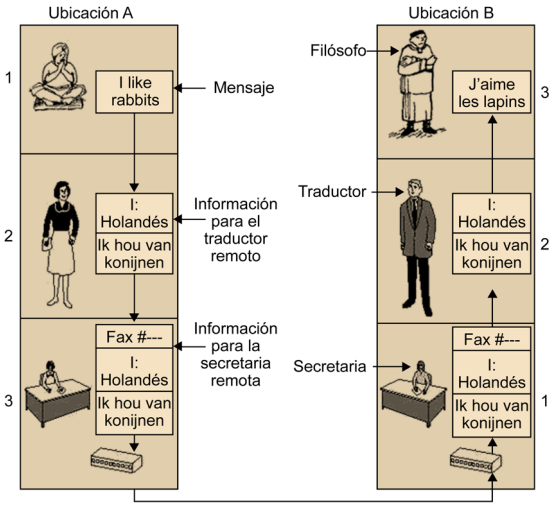
Entre cada par de capas adyacentes existe una interfaz. La interfaz define las operaciones primitivas y los servicios que la capa inferior ofrece en la capa superior. Cada capa ofrece una colección de funciones perfectamente definidas. De ahí que sea muy fácil reemplazar la implementación de una capa por otra capa con diferente implementación (si queremos cambiar el medio de transmisión de la información, basta con sustituir la capa de nivel 1; por ejemplo, cambiar las líneas telefónicas por canales de satélite, manteniendo el resto intacto).

El conjunto de capas y protocolos se denomina **arquitectura de la red**. La lista de protocolos, un protocolo por capa, se conoce como **pila de protocolos**.

Comunicaciones multi-capa

Para comprender las comunicaciones multi-capa, observemos la figura 7:

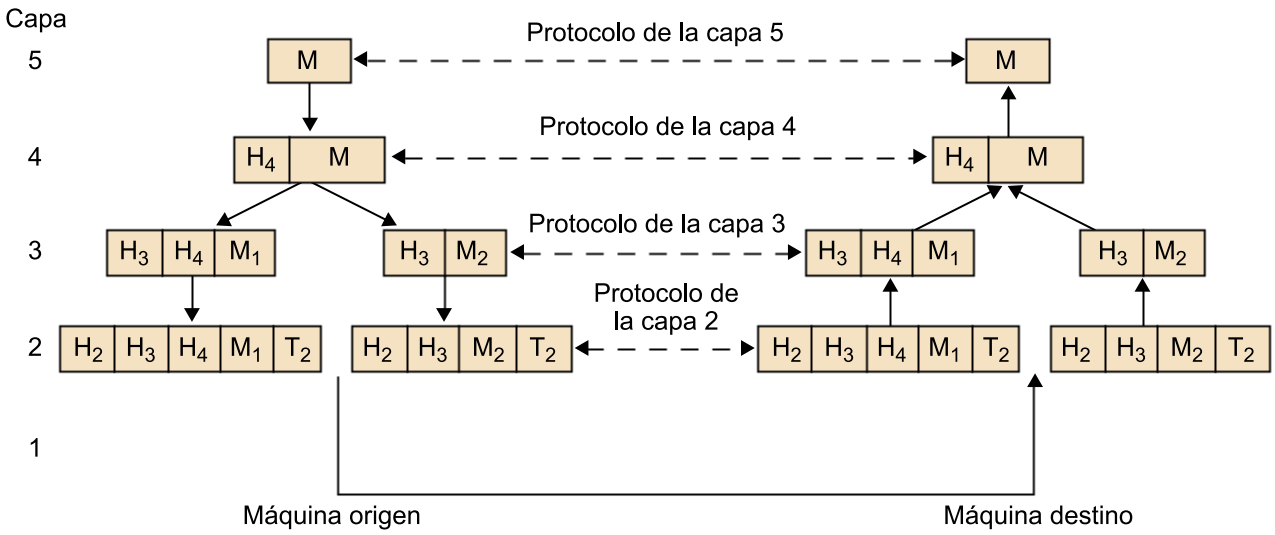
Figura 7



Imaginemos que tenemos dos filósofos (procesos pares, capa 3). Un filósofo habla urdu e inglés, y el otro filósofo, chino y francés. Dado que no hablan ninguna lengua en común, necesitan un traductor (capa 2), y cada traductor se pone en contacto con su secretaria (capa 1) para enviar la información remotamente al otro filósofo. El filósofo 1 quiere enviar un mensaje al filósofo 2. Así, pasa el mensaje en inglés mediante la interfaz 2/3 a su traductor, que traduce el mensaje a una lengua neutral (holandés). La elección de la lengua de la capa 2 es la misma en las dos entidades remotas. Después, el traductor pasa el mensaje a la secretaria, para que lo transmita vía fax (capa 1) a la otra secretaria. Cuando el mensaje llega a la secretaria remota, ésta lo pasa al traductor remoto (capa 2) y traduce el mensaje al francés para finalmente pasarlo al filósofo remoto. Debemos tener en cuenta que cada protocolo es independiente de los otros en la pila de protocolos, y podemos cambiar un protocolo por otro mientras las interfaces no cambien. Por ejemplo, la secretaria podría optar por transmitir el mensaje vía fax, enviarlo por correo postal, por teléfono o por correo electrónico, simplemente cambiando la capa 1, sin cambiar la interfaz 2/1.

Observemos la figura 8. Consideremos que se produce la comunicación de la capa superior. Un mensaje M es producido por un programa (o proceso) que funciona en la capa de nivel 5. La capa 5 envía el mensaje M a la capa 4. La capa 4 pone la cabecera antes del mensaje para identificarlo y pasa el resultado a la capa 3. La cabecera incluye el control de la información como contador de control de secuencia, para permitir que la capa 4 de la máquina de destino reciba los mensajes en el orden correcto, ya que las capas inferiores no tienen ninguna obligación de mantener la secuencia. En las otras capas, las cabeceras mantienen tamaños, tiempo y otros campos de control.

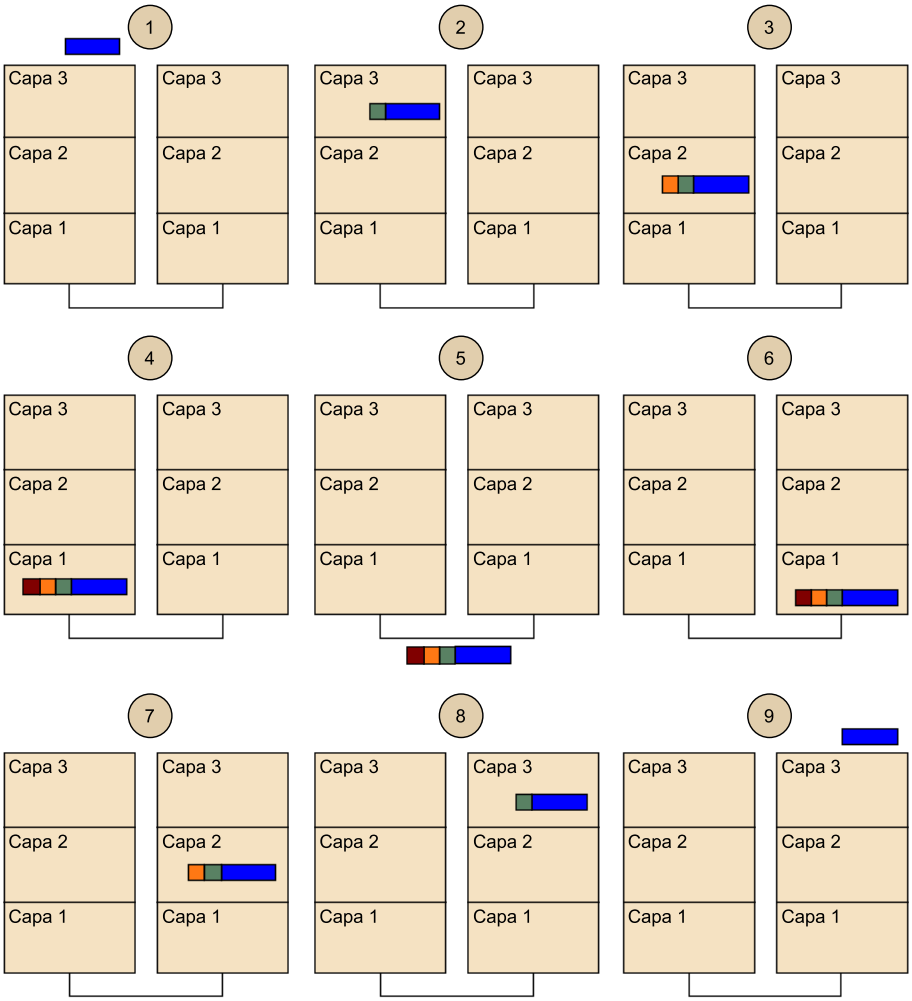
Figura 8



En muchas redes, no existe límite en el tamaño de los mensajes transmitidos en la capa de nivel 4, pero muchas veces el protocolo de nivel 3 sí que impone restricciones. En consecuencia, la capa 3 debe romper el mensaje que le envía la capa superior en varias unidades menores, denominadas *paquetes*; la capa de nivel 3 introduce una cabecera de nivel 3 en cada paquete. En este ejemplo, M se divide en dos partes, M1 y M2.

La capa de nivel 3 decide por qué línea de salida transmitirá los paquetes en la capa de nivel 2. La capa de nivel 2 añade una cabecera en cada trozo y ofrece el resultado en la capa de nivel 1 (física) para su transmisión. En el ordenador que recibe la información, el mensaje se mueve por arriba, capa por capa, con las cabeceras que se van eliminando a medida que se progresa capa por capa por arriba.

Figura 9



1.2.2. Consideraciones de diseño

El nivel por capas nos ofrece un modo estructurado de diseñar y abstraer las tareas necesarias, con el fin de enviar información a través de la red, pero aparte de las capas, cuando se diseña una arquitectura de red existen muchos otros factores que se deben considerar. Los más relevantes son:

1) Identificación: cada nodo de la red debe poder ser identificado de forma única, con el fin de poder identificar a sus interlocutores.

2) Encaminamiento: los nodos de la red deben tener mecanismos que permitan enviar la información a cualquier interlocutor de la misma red.

3) Control de errores: una de las partes más importantes de cualquier comunicación es garantizar que cuando la información llega al otro nodo ésta lo haga sin errores. Hay que notar que los medios de transmisión no siempre son fiables, por lo tanto, se debe decidir cuál o qué capas verifican errores y cómo lo harán.

4) Modos de transferencia: qué soporte tendrá el protocolo para el envío de información, si se puede enviar información en modo dúplex, semidúplex o símplex. Y en el caso de que sea necesario, ¿habrá algún tipo de priorización en el envío?

5) Control de congestión: dado que muchas veces las velocidades de transmisión de una red no siempre son homogéneas y puede haber unos enlaces con más carga que otros, cualquier protocolo debe considerar la posibilidad de disminuir la velocidad en la que se envían los datos, y en el caso de que algún paquete no llegue al destino, se habrá de reenviar de un modo transparente al usuario.

6) Tamaño de los paquetes: como ya hemos visto anteriormente, enviar mensajes muy grandes no siempre es posible, por lo tanto, se debe decidir qué tamaño máximo podrán tener los paquetes que se envían por la red.

1.3. Jerarquía de protocolos y encabezamientos

Cada capa necesita un mecanismo para identificar al emisor y al receptor. En el momento en que una red tiene, en general, varios ordenadores, cada uno con múltiples procesos, es necesario un proceso informático que especifique con quién se quiere establecer comunicación. Como consecuencia de tener múltiples destinos, se necesita algún tipo de orientación que lo concrete.

Otra característica del diseño de un protocolo es si los datos viajan en un único sentido (comunicación símplex) o en las dos direcciones, pero no simultáneamente (comunicación semidúplex), o si los datos viajan en las dos direcciones simultáneamente (comunicación dúplex). El protocolo debe determinar cuántos canales lógicos ha de gestionar y las prioridades de estos canales. Muchas redes permiten como mucho dos canales lógicos, un canal para datos normales y otro para datos urgentes.

El control de los errores es otro aspecto importante, ya que los enlaces de comunicaciones físicos no son perfectos. Se emplean determinados códigos de detección y corrección de errores, y los ordenadores que se comunican se han de poner de acuerdo en la utilización de un código corrector/detector concreto. Además, el receptor de la información debe comunicar al emisor de los mensajes cuáles se han recibido correctamente y cuáles no.

No todos los canales de comunicación conservan la orden de envío de los mensajes. Para solucionar la posible pérdida de la secuencia de los mensajes, el protocolo debe gestionar los diferentes trozos de información en una memoria intermedia[17], para finalmente ordenarlos correctamente.

(17)En inglés, *buffer*.

Otro aspecto que se tiene en cuenta es cuándo transmite un emisor información muy rápidamente hacia un receptor lento. Se han implementado varias soluciones. Muchas utilizan una técnica que consiste en que el receptor envíe una señal al emisor indicándole su problema. Otras soluciones limitan la velocidad del emisor cuando supera un determinado umbral.

Otro problema es que determinados niveles acepten mensajes de longitud superior a un cierto límite. Por esa razón se utilizan mecanismos para desensamblar, transmitir y reensamblar mensajes.

La multiplexación y la desmultiplexación de la capa física se utiliza cuando el tráfico de todas las conexiones se debe transmitir en pocos circuitos físicos.

Cuando existen múltiples caminos entre el origen y el destino, se ha de elegir una ruta. A menudo, esta decisión se elige entre dos o más capas.

1.4. Interfaces y servicios

La función de cada capa es proporcionar servicios a la capa superior. En esta sección estudiaremos con más detalle lo que se denomina *servicios*.

Los elementos activos de cada capa son las entidades[18]. Cada entidad puede ser una entidad de software (como un proceso) o una entidad hardware (como un dispositivo inteligente de entrada salida). Las entidades de la misma capa de diferentes máquinas se denominan *entidades pares*[19]. La capa *N* puede usar los servicios de la capa *N* – 1 para proporcionar su propio servicio. Una capa puede ofrecer múltiples clases de servicios, por ejemplo, comunicaciones caras y rápidas, o comunicaciones lentas y baratas.

(18)En inglés, *entities*.

(19)En inglés, *peer entities*.

Los servicios están disponibles en los SAP[20]. El SAP de la capa *N* son los lugares en los que la capa *N* + 1 puede acceder a los servicios ofrecidos. Cada SAP tiene una dirección que la identifica. Por ejemplo, el SAP en el sistema de telefonía son los conectores a los que se conectan los aparatos de teléfono, y la dirección SAP es el número de teléfono de este conector. Y en el sistema postal, la dirección SAP es el nombre de la calle y el número de vivienda. Por lo tanto, para enviar una carta debes conocer la dirección SAP.

(20)SAP es la sigla de Service Access Point.

Para que dos capas intercambien información, se debe definir una serie de normas sobre la interfaz. En una interfaz típica la entidad de la capa *N* + 1 pasa una IDU[21] a la entidad de la capa *N* mediante el SAP, tal y como se muestra en la figura 10. La IDU consiste en una SDU[22] y determina la información de control[23]. La SDU es la información pasada a través de la red hacia la entidad par y después subida a la capa remota N + 1. La información de control es

(21)IDU es la sigla de *interface data unit*.

(22)SDU es la sigla de *service data unit*.

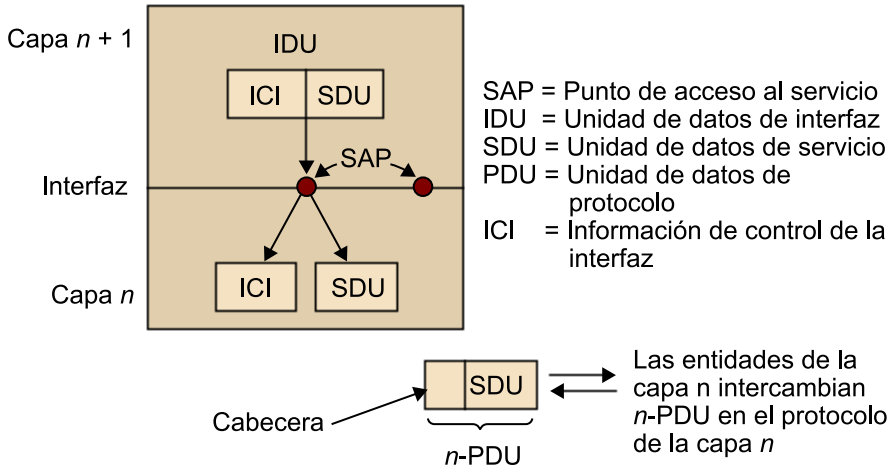
(23)En inglés, *interface control information*.

necesaria para ayudar a la capa inferior a realizar su trabajo (por ejemplo, para indicar el número de bytes del SDU), pero no forma parte de la información pura.

Para transmitir la SDU, la entidad de la capa *N* debe fragmentar ésta en varios trozos, asignarles una cabecera y enviarlos como una PDU[24] o paquete. Mediante las cabeceras de la PDU, la entidad identifica qué PDU contienen datos y cuáles contienen información de control, y proporciona números de secuencia y contadores.

[24]PDU es la sigla de *protocol data unit*.

Figura 10



Las capas pueden ofrecer dos tipos diferentes de servicios en las capas superiores: conexiones orientadas y no orientadas a conexión.

Un servicio orientado a conexión se forma como un sistema de telefonía: para hablar con alguien, primero debemos marcar el número de teléfono, después hablar y, por último, colgar el teléfono. Inicialmente se produce un establecimiento de conexión, luego se utiliza la conexión para hablar y transmitir información y al final se cierra la conexión. Esta conexión actúa como un tubo: el emisor envía objetos o bits al receptor, y el receptor los recibe en el mismo orden que le son enviados.

Un servicio no orientado a conexión se forma como un sistema postal. Cada mensaje o carta postal lleva la dirección completa del destinatario, y cada mensaje o carta es enviado por el sistema, independientemente de las otras cartas. En general, cuando dos mensajes son enviados al mismo destino, primero se recibe el que ha sido enviado en primer lugar. También es posible que el primer envío pueda sufrir un retraso y que, en consecuencia, el segundo mensaje llegue antes que aquél. En una conexión orientada a conexión eso es imposible.

Cada servicio está caracterizado por la denominada calidad de servicio. Muchos servicios son fiables en el sentido de que nunca pierden información. Normalmente, un servicio fiable se implementa mediante el envío de reconocimientos por parte del receptor de cada mensaje, y así el emisor sabe que el mensaje se ha recibido correctamente. El proceso de reconocimientos[25] introduce información de control redundante[26], no información útil, y un cierto retraso, lo que es deseable en términos de rendimiento de la red.

[25] En inglés, *acknowledgements*, abreviado *ack*.

[26] En inglés, *overhead*.

La típica situación en la que se utiliza un servicio fiable orientado a conexión es la transmisión de ficheros. El usuario del servicio desea que los bits del fichero lleguen íntegramente y en el orden en que fueron emitidos.

En muchas aplicaciones, los retrasos de los reconocimientos son inaceptables. Por ejemplo, en el caso del tráfico de voz digitalizada. Para los usuarios del teléfono es preferible oír por el auricular un poco de ruido en la línea o no entender una palabra de vez en cuando, que se produzca un retraso en la espera del reconocimiento. Cuando se transmite una película de vídeo, es preferible tener varios puntos[27] incorrectos (que en la práctica apenas es un problema) que ver la película con paradas para corregir los errores (esta situación es muy molesta).

[27] En inglés, *pixels*.

Las conexiones no fiables (con la no utilización del mecanismo de reconocimiento) y las no orientadas a conexión se denominan *servicio de datagrama* (por ejemplo, el envío de correo electrónico).

En aquellas situaciones en las que la fiabilidad es esencial, conviene que no sea necesario establecer una conexión para enviar un mensaje corto. Por eso se utilizan los servicios no orientados a conexión con reconocimiento. Por ejemplo, cuando se envía un correo electrónico, el receptor manda otro correo al emisor para indicarle que lo ha recibido.

Otro tipo de servicio es el *request-reply-service*: el emisor transmite un datagrama simple que contiene la petición. La respuesta contiene tanto la pregunta como la respuesta.

Figura 11

	Servicio	Ejemplo
Orientado a la conexión	Secuencia de mensajes fiable	Secuencia de páginas
	Secuencia de octetos fiable	Inicio de sesión remoto
	Conexión no fiable	Voz digitalizada
Sin conexión	Datagrama no fiable	Correo basura
	Datagrama reconocido	Correo certificado
	Solicitud de respuesta	Consulta a la base de datos

Formalmente, un servicio se especifica mediante un conjunto de primitivas (operaciones) disponibles para el usuario u otra entidad y que permiten acceder al servicio. Aquéllas ordenan al servicio que realice alguna acción o que devuelva el resultado de una acción de la entidad par. La siguiente tabla nos muestra las maneras de clasificar las primitivas del servicio:

Primitiva	Significado
Request	Una entidad quiere que el servicio realice alguna cosa.
Indication	Una entidad es informada de algún hecho.
Response	Una entidad quiere responder a algún hecho.
Confirm	Se confirma la respuesta a la última petición.

Consideremos cómo se establece y se libera una conexión. La entidad que establece la conexión realiza una CONNECT.request y el receptor recibe la CONNECT.indication anunciando que una entidad quiere conectarse al receptor. La entidad que recibe la CONNECT.indication utiliza la CONNECT.response para comunicar que acepta o rechaza la conexión propuesta. La entidad que realiza la petición de conectar recibe la aceptación o rechazo de su conexión a partir de la primitiva CONNECT.confirm.

Cada primitiva puede tener o no parámetros. Por ejemplo, la primitiva CONNECT.request debe especificar la dirección de la máquina a la que se quiere conectar, el tipo de servicio deseado y la longitud máxima del mensaje que utilizará durante la conexión. Los parámetros de la CONNECT.indication deben contener la identidad de quien realiza la llamada, el tipo de servicio deseado y la longitud máxima propuesta del mensaje. Si la entidad llamada no acepta la longitud máxima propuesta del mensaje, puede realizar con la primitiva response una nueva propuesta de longitud del mensaje. Los detalles de cada negociación forman parte de cada protocolo.

Los servicios pueden ser confirmados o no serlo. En un servicio confirmado se hallan las primitivas request, indication, response, confirm. En un servicio no confirmado sólo están las primitivas request e indication. El servicio CONNECT sólo se utiliza en los servicios confirmados porque la entidad remota debe dar el visto bueno al establecimiento de la conexión.

Las ocho primitivas de un servicio orientado a conexión son las siguientes:

1) CONNECT.request: pedir por el establecimiento de la conexión.

2) CONNECT.indication: indicar en la parte llamada un establecimiento de conexión.

3) CONNECT.response: utilizado por la parte llamada para aceptar/rechazar la conexión o llamada.

4) CONNECT.confirm: indicar al que llama si la conexión o llamada se ha aceptado.

5) DATA.request: indicar que la información se envía.

6) DATA.indication: indicar la llegada de la información.

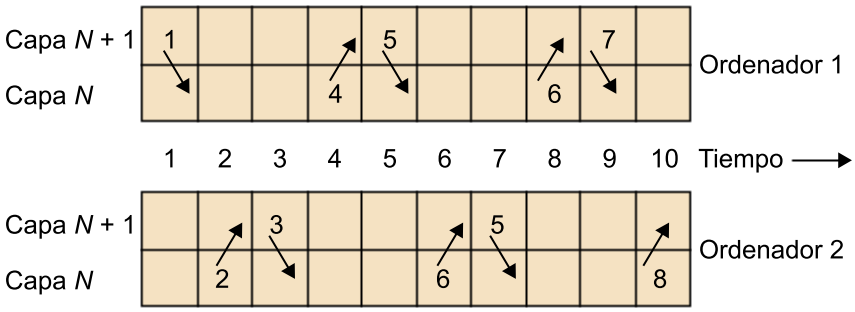
7) DISCONNECT.request: indicar que la conexión se ha cerrado.

8) DISCONNECT.indication: indicar a la otra entidad del cierre de la conexión.

En este ejemplo, el servicio CONNECT está confirmado, mientras que el servicio DISCONNECT no está confirmado.

La figura 12 muestra la misma secuencia antes descrita. Cada paso incluye una interacción entre dos capas de uno de los ordenadores. Cada petición o respuesta provoca una indicación o confirmación en la otra parte. El usuario del servicio está en la capa + *N* 1, y la capa *N* es la capa que ofrece el servicio:

Figura 12



Protocolos y servicios

Los protocolos y los servicios son dos conceptos distintos, aunque en general se suelen confundir. Un servicio es un conjunto de primitivas (operaciones) que una capa proporciona a la capa superior. El servicio define qué operaciones es capaz de ofrecer la capa, pero no dice nada sobre cómo están implementadas estas operaciones. Un servicio es una interfaz entre dos capas, mientras que la capa de nivel inferior es la que proporciona el servicio y la capa de nivel superior la que utiliza el servicio.

Un protocolo es un conjunto de normas que gobiernan el formato y el significado de las tramas, paquetes o mensajes que se intercambian por las entidades de una misma capa. Las entidades utilizan los protocolos para implementar las definiciones del servicio.

Un servicio sería un tipo abstracto de datos o un objeto en los lenguajes de programación. Define las operaciones que se pueden realizar sobre el objeto pero no especifica cómo se han implementado éstas. Un protocolo relata cómo se implementa el servicio y no es visible para el usuario del mismo.

1.4.1. Tipos de conexión de servicios

Cada servicio establece una conexión con el servicio análogo del equipo de destino, y en función de cómo se gestione esta conexión entre servicios, un servicio puede estar orientado a conexión o no orientado a conexión.

El servicio orientado a conexión previo al envío de información establece una conexión que se libera cuando la transferencia acaba. No hay que confundir un servicio orientado a conexión con la conmutación de circuitos vista anteriormente; en el servicio orientado a conexión no se realiza ninguna reserva de recursos, sino una estructura de datos que mantiene el estado de la conexión. El hecho de que un protocolo esté orientado a conexión implica que la información debe llegar ordenada y sin errores. Y dado que hay que mantener la conexión, ambos extremos son conocidos y no es necesario indicar qué destino tiene la comunicación. Este paso se realiza durante el establecimiento de la conexión.

Ved también

Ved el ejemplo por excelencia de un protocolo orientado a conexión, el TCP, en el subapartado 2.5 de este módulo.

Por su parte, los servicios no orientados a conexión no precisan ni asumen ninguna conexión previa entre los dos interlocutores. De este modo, la información se separa en paquetes (denominados datagramas en este tipo de servicios) y se envía a la red sin saber ni el camino que seguirá el paquete ni si llegará a su destino, ni siquiera en qué orden lo hará; cada datagrama se envía autónoma e independientemente del resto. Por lo tanto, para poder enviar un datagrama con un protocolo no orientado a conexión, el datagrama debe tener la dirección destino, y los elementos intermedios de la red han de tener información de cómo hacer llegar la información según el destino de cada datagrama recibido. El ejemplo por excelencia de servicios no orientados a conexión es IP. Curiosamente, HTTP también es un protocolo no orientado a conexión.

Ved también

Ved el protocolo IP en el apartado 3 de este módulo didáctico.

2. Modelos de referencia

Actualmente, las dos arquitecturas de red más conocidas son OSI, utilizada como modelo teórico, y TCP/IP, cuyo éxito en el mundo de las redes ha sido enorme.

2.1. Antecedentes

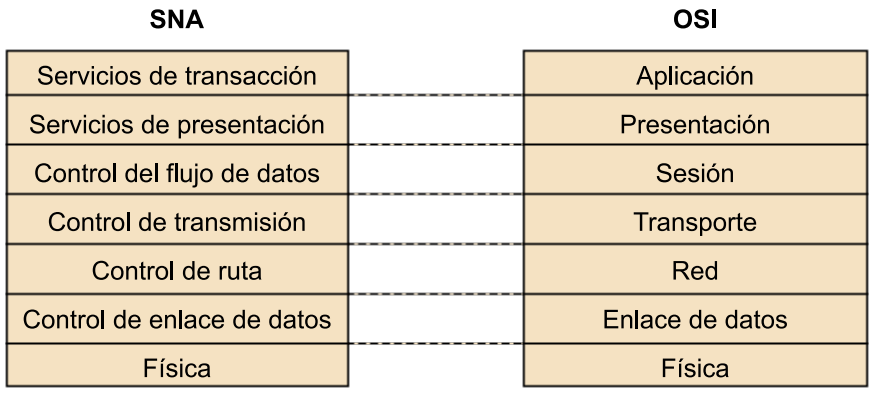
La fase inicial de la teleinformática se caracterizó por una gran confusión sobre dispositivos y normas de transmisión. Durante los años sesenta, setenta y ochenta se crearon diferentes arquitecturas comerciales de redes de ordenadores propietarias, en las que cada fabricante establecía sus propias normas de conexión y transmisión, que en general no coincidían con las de ningún otro fabricante. A continuación, destacamos las arquitecturas más importantes.

2.1.1. SNA de IBM

Es una arquitectura creada por la empresa IBM en 1974 (1.ª versión), basándose en un modelo de 7 niveles. La torre OSI se inspiró, fundamentalmente, en este modelo arquitectónico, dado que ambas tienen los mismos niveles y prácticamente las mismas funcionalidades.

La arquitectura SNA solucionó la complejidad producida por la multitud de productos de comunicaciones de IBM. Actualmente, se continúa utilizando en el sector bancario.

Figura 13



2.1.2. DNA de DEC (DECnet)

Grupo de productos de comunicaciones de red, desarrollado por Digital Equipment Corporation (DEC[28]), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y en sedes compatibles. Está muy extendido en el mundo académico.

[28]DEC es la sigla *digital equipment corporation*.

Se han lanzado al mercado varias versiones del DECnet desarrolladas en fases: fase I (1975), fase II, fase III y fase IV (1982), y fase V. La fase IV es la versión más extendida de las que se han ejecutado. Se basa en la arquitectura de red DNA, y se apoya en los protocolos propietarios de Digital y otros protocolos propietarios y estándares.

Figura 14

Ejemplo de arquitectura DECnet

La serie VAX de Digital es una de las máquinas que se han basado en esta arquitectura.

DECnet Phase IV protocol suite	
Application	DAP: Data Access Protocol CTERM: Command Terminal
Network Management	NICE: Network Information (and) Control Exchange MOP: Maintenance Operation Protocol
Session	SCP: Session Control Protocol
Transport	NSP: Network Service Protocol
Network	DRP: DECnet Routing Protocol
Data link	DDCMP: Digital Data Communications Message Protocol Ethernet, Token ring, HDLC, FDDI, ...
Physical	Ethernet, Token ring, FDDI, ...

2.1.3. XNS de Xerox

XNS[29] es un conjunto de protocolos desarrollados por la empresa Xerox Parc a principios de los años ochenta. XNS fue usado por 3Com y por otros sistemas comerciales como Novel NetWare y Banyan VINES. Influyó en el desarrollo del modelo de red OSI.

[29]XNS es la sigla de *xerox network services*.

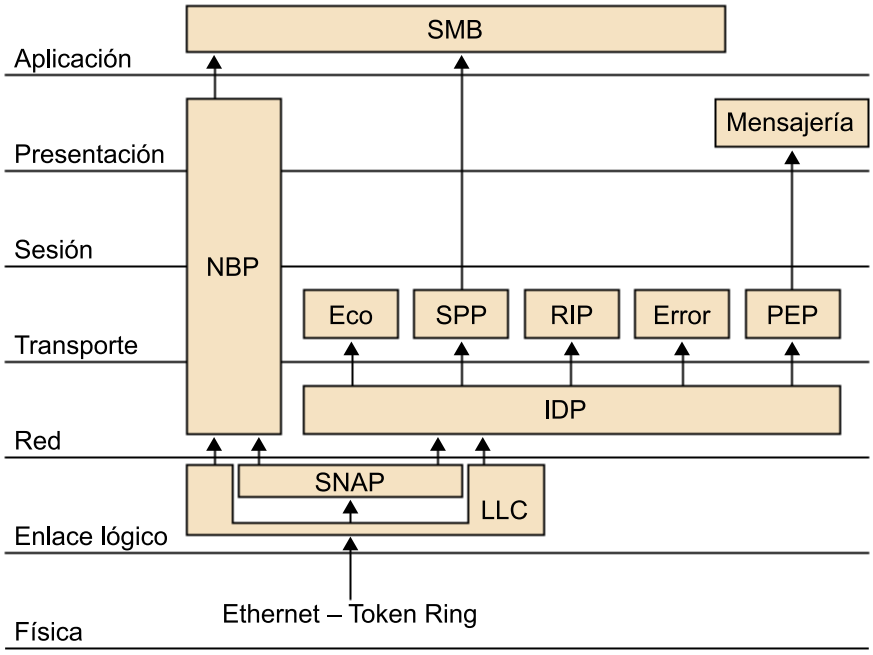
El principal protocolo de la capa de red fue el IDP[30], muy similar al protocolo IP del modelo TCP/IP. SPP[31] y PEP[32] fueron los dos principales protocolos de la capa de transporte, muy similares a los protocolos TCP y UDP de la torre TCP/IP, respectivamente.

[30]IDP es la sigla de *internet datagrama protocol*.

[31]SPP es la sigla de *sequenced packet protocol*.

[32]PEP es la sigla de *packet exchange protocol*.

Figura 15. Paquete de protocolos XML



El protocolo RIP, que fue usado como un protocolo de intercambio de información entre encaminadores, permanece en uso, con ligeras modificaciones, en la torre TCP/IP de Internet.

2.1.4. NetWare de Novel

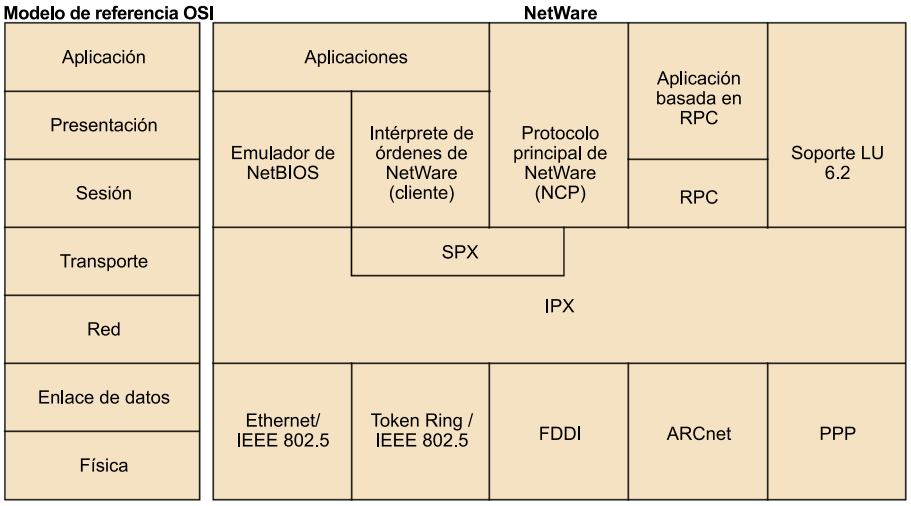
En sus diferentes versiones, el software de red de la empresa Novel llegó a ser el más usado en el mundo, hasta que fue desbancado por el modelo Windows, en sus versiones NT, 2000, 2003 y 2008. Era una de las plataformas de red más fiable para ofrecer acceso seguro y continuado a la red. Ofrece un alto rendimiento, gran capacidad de crecimiento (escalabilidad) y óptima gestión de los recursos de información (servidores de archivos).

La pila de protocolos propietarios en la que se basaba exclusivamente NetWare hasta la versión 4 era una versión modificada del XNS denominada SPX/IPX, que guardaba una cierta similitud con TCP/IP. Apareció antes que OSI y, por lo tanto, no se basa en esta especificación. Las últimas versiones, para adaptarse a la moda imperante, son capaces de utilizar plena y exclusivamente TCP/IP.

Desde sus inicios utilizó arquitecturas Ethernet o Token Ring en los niveles físico y de enlace. Las capas de sesión y presentación no existen, y en el nivel de aplicación se pueden usar diferentes protocolos.

En la actualidad, Netware está cada vez más centrado en los servicios de red (directorio activo, impresión, administración de redes, seguridad), y está abandonando progresivamente el papel de Sistema Operativo de Red, que Novel está trasladando a Linux, y para el que ha adquirido la compañía SuSe Linux.

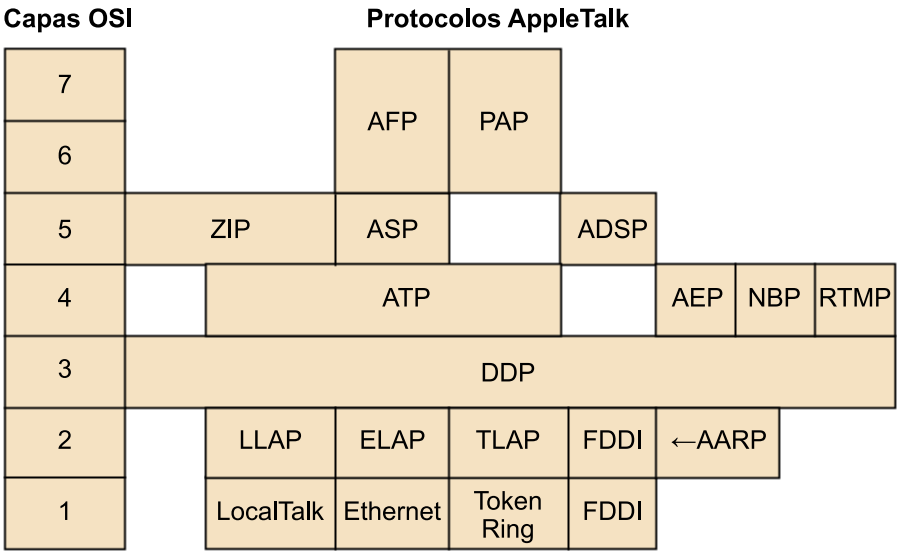
Figura 16



2.1.5. AppleTalk de Macintosh

AppleTalk es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984, pero actualmente ya no se suele utilizar en este tipo de ordenador, en favor de las redes TCP/IP.

Figura 17. Protocolos AppleTalk en el modelo OSI

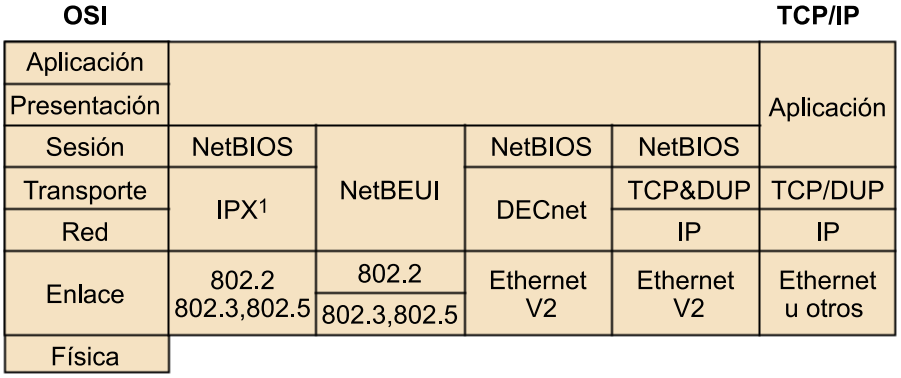


2.1.6. NETBEUI de Microsoft

Es un protocolo de nivel de red, sin encaminador y bastante sencillo, utilizado en las primeras redes de Microsoft. Fue desarrollado por las redes de IBM por Saytek. En 1987 Microsoft y Novel también usaron este protocolo para su red de los sistemas operativos LAN Manager, NetWare, Windows 3.x, Windows 95 y Windows NT. Debido a que NetBEUI no posee encaminador, sólo puede emplearse para comunicar terminales en el mismo segmento de red, o en dos

segmentos conectados mediante un puente de red. Se recomienda ser utilizado sólo para redes medianas o pequeñas. Cubre las funcionalidades de los niveles de red, transporte y sesión de la torre OSI.

Figura 18



2.1.7. TCP/IP del mundo militar

Proviene del mundo militar, en concreto del período de la Guerra Fría. Fue creado con la idea de diseñar un sistema de comunicaciones capaz de sobrevivir a un ataque nuclear. En sus inicios fue incorporado en el S.O. Unix, hecho que provocó que su utilización se extendiera mundialmente. Hoy en día, TCP/IP se ha convertido en un estándar *de facto*. La importancia de TCP/IP es tan grande que la mayor parte de las redes hablan TCP/IP, sin perjuicio de que también puedan incorporar otras familias nativas de protocolos. La tecnología TCP/IP está definida en un conjunto de documentos denominados RFC[33], publicados en la página oficial del IETF.

(33)RFC es la sigla de *request for comments*.

2.2. Necesidad de estandarización

Los primeros ordenadores realizaban trabajos concretos, ubicados en lugares cerrados y aislados. Cada fabricante vendía su sistema de comunicaciones integral a las empresas, y se encargaba de todos los aspectos relacionados con la red (equipos, software, cableado, etc.). Cuando una empresa necesitaba alguna ampliación y/o modificación, sólo podía contar con un único interlocutor para proporcionar los servicios necesarios. Esto implicaba determinados problemas, como:

- Los costes eran elevados porque los adaptadores se realizaban a medida.

- La interoperatividad era nula, ya que resultaba imposible interconectar unos sistemas con otros, a causa de la falta de compatibilidad entre dispositivos. Cuando se elegía un suministrador era para siempre.

Con estas limitaciones, a partir de los años ochenta empezaron a aparecer organizaciones que construían equipos para interconectar redes y pasarelas entre ordenadores de diferentes fabricantes. Podemos destacar los siguientes hitos:

1) 3 empresas: DEC, INTEL y XEROX (Consorcio **DIX**) se pusieron de acuerdo para crear un primer estándar para redes de área local para la red ETHERNET. En 1982, DIX distribuyó la versión II de Ethernet, que es la versión estándar para TCP/IP.

2) El comité 802.3 de IEEE se basó en la versión de DIX para trabajar en una red Ethernet mejorada. Ethernet tenía un coste bajo y unas altas prestaciones, además de ser fácil operar con ella.

3) El sistema operativo UNIX creado por BELL Laboratories, empezó a popularizarse y distintas organizaciones (empresas y universidades) lo implementaron en sus sistemas (BSD-UNIX de Berkeley, Xenix, SUNOS, HP-UX, etc.). Ésta fue la principal causa de la extensión de TCP/IP, dado que estaba incluido en su núcleo[34].

(34)En inglés, *kernel*.

4) Creación de un modelo de referencia OSI de ISO (lo trataremos a continuación).

Estos hechos provocaron que los sistemas que hasta ese momento ofrecían una arquitectura cerrada pasaran a contar con una arquitectura abierta y que las redes fuesen compatibles.

Se empezaron a estandarizar componentes y funcionalidades de cada nivel arquitectural para poder intercomunicar los sistemas heterogéneos. La información de los estándares se hace pública, circunstancia que no se daba con los sistemas propietarios.

Se crean foros externos a los organismos que pueden llegar a forzar a éstos a decidirse por uno u otro estándar (ATM Forum, Forum Gigabit Ethernet, Forum ADSL, etc.).

Podemos ver las ventajas y desventajas de la existencia de estándares en la tabla siguiente:

Ventajas estándares	Desventajas estándares
• Estimula la competitividad entre los fabricantes. • Evita monopolios. • Baja los precios. • Flexibilidad para instalar equipos. • Heterogeneidad de fabricantes.	• Tardanza en la aprobación. • Los fabricantes crean equipos en condiciones propietarias. • Los intereses de los fabricantes y organismos no siempre coinciden. • Posibilidad de acuerdos más políticos y comerciales que técnicos. • Los fabricantes son los que desarrollan más I+D, lo que provoca que se fuerce a los organismos a definirse. • Muchos organismos se pueden afectar en la estandarización, ya que se puede llegar a clasificar geográficamente, por industria, etc.

Existen importantes ganancias económicas para las empresas que han desarrollado un sistema y éste se ha convertido en estándar. Sin embargo, ello puede provocar que otras empresas salgan perjudicadas.

2.3. Organismos de estandarización

Dadas las ventajas e inconvenientes existentes, es necesario que existan organismos internacionales que regulen las comunicaciones. La siguiente tabla muestra una lista de los principales organismos internacionales:

Siglas	Nombre completo	Descripción
EIA	Electronic Industries Association	Se encarga de estándares físicos y de cableado.
IEEE	Industries of Electrical and Electronic Engineers	Organización profesional cuyo proyecto más conocido es la definición del estándar 802. Estandarización de las redes de área local.
ITU*	International Telecommunication Union	Organización responsable de toda la estandarización referente a los aspectos de comunicaciones en general (voz, datos). Operadores de telecomunicaciones.
ISOC	Internet Society	Este organismo consta de diferentes órganos referidos a Internet.
IAB	Internet Activities Board	Órgano encargado de determinar las necesidades técnicas y la toma de decisiones sobre la orientación tecnológica de Internet. Órgano que aprueba las recomendaciones y estándares de Internet que se recogen en los RFC.
IETF	Internet Engineering Task Force	Grupos de trabajo, dependientes de IAB, que se dedican al estudio de aspectos técnicos de Internet y que ratifican los estándares publicados como RFC.
IRTF	Internet Research Task Force	Foros y grupos de trabajo de Internet.
ANSI	American National Standards Institute	Miembro de la ISO conocido por la estandarización de FDDI.
CCITT	Consultative Conmite for International Telegraph and Telephone	Creó el estándar X.25.
ECMA	European Computer Manufactures Association	
ISO	International Organitation for Standardization	Define el modelo de referencia OSI. Estándares industriales.
TIA	Telecommunication Industry Association	Estándares de nivel físico y cableados.

* En 1865, los representantes de los países europeos vieron la necesidad de que hubiera una organización que se encargara de la estandarización de las comunicaciones por telégrafo.

Siglas	Nombre completo	Descripción
CEPT	Conference European of Postand Telecommunications	Organismo de las PTT. Sus documentos se denominan *norme européenne de telecommunications* (NET).
ETSI	European Telecommunications Standards Institute	Telecomunicaciones europeas (GSM, seguridad).
NIST	National Institute of Standards and Technology	Departamento de Comercio de Estados Unidos. Estándares en USA.

* En 1865, los representantes de los países europeos vieron la necesidad de que hubiera una organización que se encargara de la estandarización de las comunicaciones por telégrafo.

2.4. El modelo de referencia OSI

Entre los diferentes modelos propuestos por las diferentes organizaciones internacionales de normalización en la década de los ochenta, destacó una arquitectura de redes de ordenadores basada en niveles, el modelo OSI[35] definido por la organización ISO.

[35]Sigla de Organización Internacional de Estándares. En inglés, International Organization for Standardization.

A finales de los años setenta, la ISO fue definiendo la arquitectura de redes OSI con el fin de promover la creación de una serie de estándares que especificaran un conjunto de protocolos independientes de cualquier fabricante. Pretendía establecer las normas y los estándares para que el software y los dispositivos de diferentes fabricantes pudieran funcionar juntos.

Además de facilitar las comunicaciones entre sistemas diferentes, con OSI el ISO pretendía impedir que ninguna de las arquitecturas de fabricante existentes adquiriera una posición hegemónica, especialmente SNA de IBM.

Seguramente, la aportación más importante de la iniciativa OSI ha sido la definición teórica de su modelo arquitectónico. Ésta ha servido como marco de referencia para describir y estudiar redes "reales". Por este motivo, la arquitectura OSI se denomina, en general, *modelo de referencia OSI*.

El modelo OSI está compuesto por niveles o capas, y en cada nivel se agrupa una serie de funciones o protocolos necesarios para comunicar sistemas. Los principios que se aplicaron para establecer estos siete niveles fueron los siguientes:

- Una capa se creará en situaciones en las que se necesita un nivel diferente de abstracción.
- Cada capa deberá realizar una función bien definida.
- Los problemas se resuelven en una capa concreta sin afectar al resto de las capas.

- Cada capa se basa en los servicios de la capa inmediatamente inferior.

- Cada capa ofrecerá servicios en capas superiores sin que éstas sepan cómo se realizan los servicios.

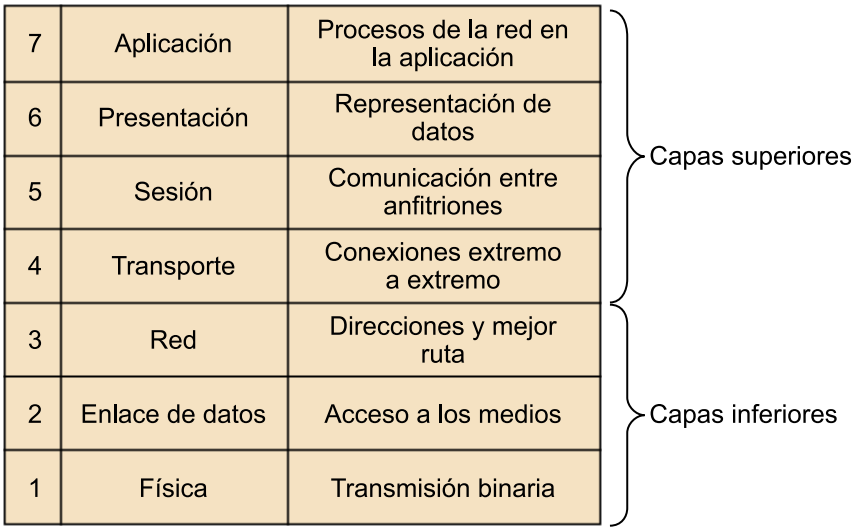
- La función que realizará cada capa deberá ser seleccionada con la intención de definir protocolos normalizados internacionalmente.

- Los límites de las capas deberán ser seleccionados teniendo en cuenta la reducción obligada del nivel información que hay que pasar entre capas. La frontera entre capas debe ser lo más sencilla posible.

- El número de capas debe ser lo bastante grande para que funciones diferentes no necesiten ponerse juntas en la misma capa. También habrá de ser lo bastante pequeño para que su arquitectura no sea difícil de manejar.

Las capas se pueden ver en la figura 19:

Figura 19



Las capas se pueden agrupar en dos subconjuntos convenientemente diferenciados:

1) Capas inferiores: son proveedoras de servicios de transporte de las capas superiores. Tratan problemas como errores del sistema de transmisión, búsqueda de rutas óptimas, etc.

2) Capas superiores: su misión es dar servicios al usuario del sistema de comunicaciones. Confían en las prestaciones de los niveles inferiores.

OSI y SNA

Debemos señalar la sospechosa coincidencia del número de capas de OSI con el de SNA, la arquitectura de red para grandes sistemas de IBM, que estaba en pleno apogeo en el momento en el que se definió OSI.

El objetivo del modelo es el desarrollo de protocolos para crear redes internacionales. Algunos protocolos se desarrollaron, pero otros se dejaron de lado en favor de Internet (TCP/IP).

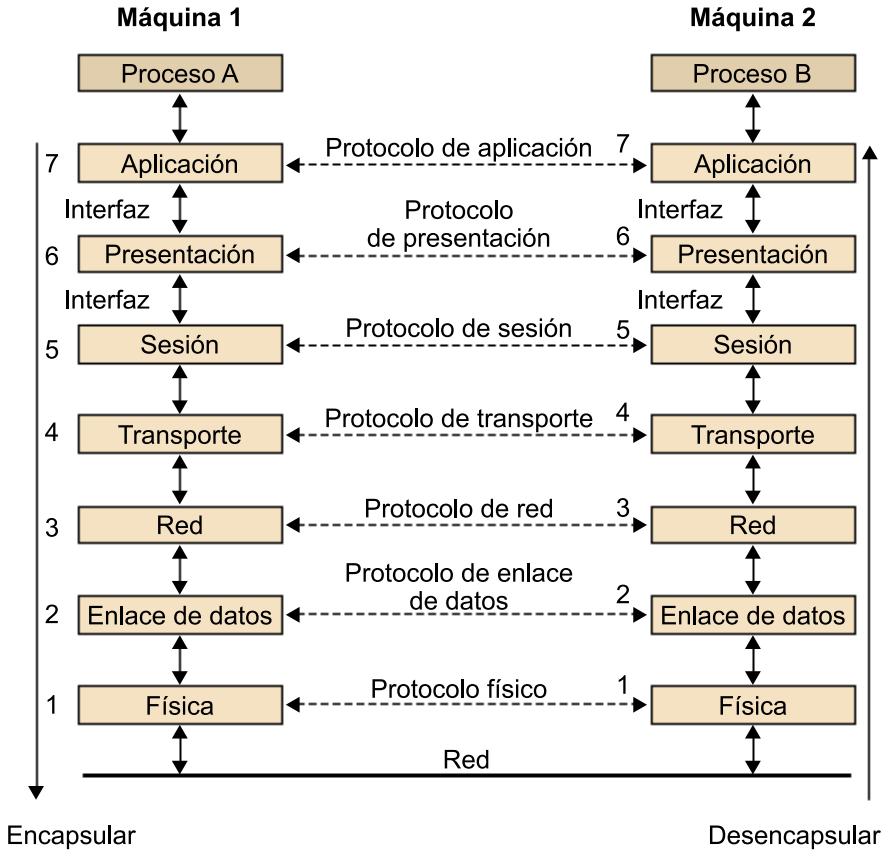
2.4.1. Proceso de encapsulación y desencapsulación

El modelo OSI describe cómo se desplaza la información desde los programas de aplicación de diferentes ordenadores en un medio de la red. Cada capa realiza dos procesos de comunicación:

1) Comunicación horizontal: comunicación cuya capa es igual a la del otro sistema, que recibe el nombre de *protocolo*.

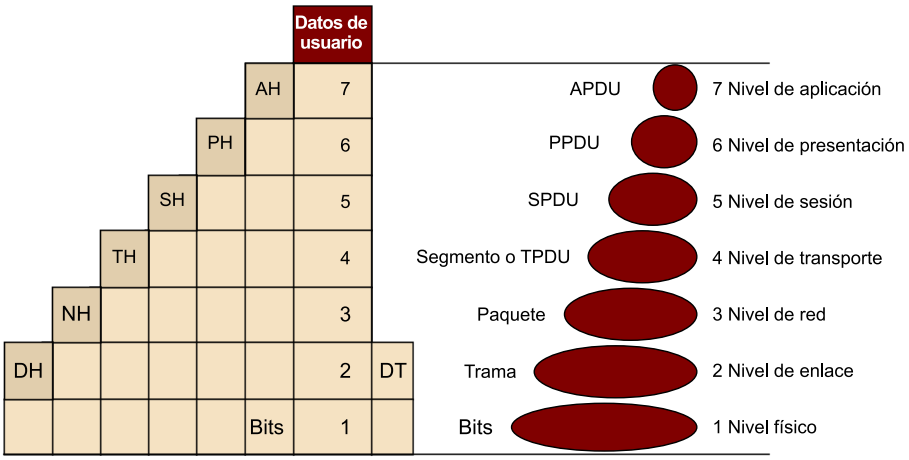
2) Comunicación vertical: comunicación con sus niveles inmediatamente superior e inferior, que recibe el nombre de *primitivas de servicio*.

Figura 20



Cuando un usuario necesita transmitir datos a un destino, el sistema de red va añadiendo información de control (cabeceras) para cada uno de los servicios que utilizará la red para ejecutar la orden de transmisión.

Figura 21



En un breve resumen adecuadamente ampliado en temas posteriores, veremos cuál es la utilidad de cada una de estas capas.

2.4.2. La capa física

Es la capa de menor nivel de la torre OSI, la más próxima al hardware, la que se encarga de definir las características físicas del medio de transmisión. La función de la capa física es proporcionar al nivel de enlace un acceso al sistema de comunicaciones que sea independiente de los detalles técnicos y funcionales de éste.

Su diseño incluye cuatro aspectos:

1) Mecánico. Indica las especificaciones de los conectores, el tamaño y la forma, el grosor del cable, el tipo de aislante, el número de *pins*, etc.

2) Eléctrico/óptico/electromagnético. Indica cómo se representan los bites: duración de los pulsos eléctricos/ópticos, voltaje, tipo de señal de salida, impedancia, velocidad de transmisión, características y naturaleza del medio (por ejemplo, con eléctrico nos referimos a la conducción dentro de un cable coaxial; con óptico, a la conducción por fibra óptica; y con electromagnéticas, a la propagación de ondas en el espacio).

3) Funcional. Funciones de los circuitos de una interfaz del sistema: codificación, modulación, etc.

4) De procedimiento. Secuencia de acontecimientos en el intercambio de flujo.

Ejemplos de protocolos de la capa física

Son ejemplos de la capa física las normas EIA RS-232-C, utilizada por los puertos serie de los ordenadores personales, EIA-RS-449, ITU-T V.24/V.28/V.35, etc. En cuanto a las redes locales de difusión, el nivel físico se suele incluir en el subnivel MAC[36] del nivel de enlace. Corresponden a este subnivel las especificaciones IEEE 802.3, 802.4, 802.5, etc.

Los equipos que podemos encontrar en este nivel son los siguientes: Hubs Ethernet (LAN), MAU Token Ring (LAN), multiplexores, módems, conmutadores de circuitos (WAN).

[36]MAC es la sigla de *medium access control*.

2.4.3. La capa de enlace

Su principal objetivo consiste en ofrecer a la capa inmediatamente superior (nivel de red) una comunicación fiable de bits a través de un medio físico de transmisión.

Entre las funcionalidades de este nivel podemos destacar:

a) Sincronización a nivel de trama. Agrupa los bits en tramas, la mínima unidad de información con la que trabaja el nivel de enlace, y establece delimitadores de origen y destino para que sea detectada correctamente en la recepción.

b) Control de flujo: la estación emisora y la receptora deben ponerse de acuerdo en el ritmo de transmisión de datos, con el fin de no saturar las memorias del nodo receptor y no perder información.

c) Control de errores: los enlaces de datos no son perfectos y pueden introducir errores. Es necesario controlar que no se produzcan errores de transmisión, de manera que los datos en la recepción se correspondan con los datos en el origen.

d) Dirección: si existe más de un posible destino para un mensaje es necesario identificarlo perfectamente.

e) Gestión del enlace: todo el proceso de inicio, mantenimiento y finalización de la transmisión requiere un considerable esfuerzo de gestión y coordinación. También se proporcionan los medios para activar, mantener y desactivar el enlace.

f) Control de acceso al medio: funcionalidad necesaria en redes de difusión, en la que todos los terminales comparten un medio único físico (en banda base, sin multiplexar). Cuando varios equipos acceden simultáneamente, se

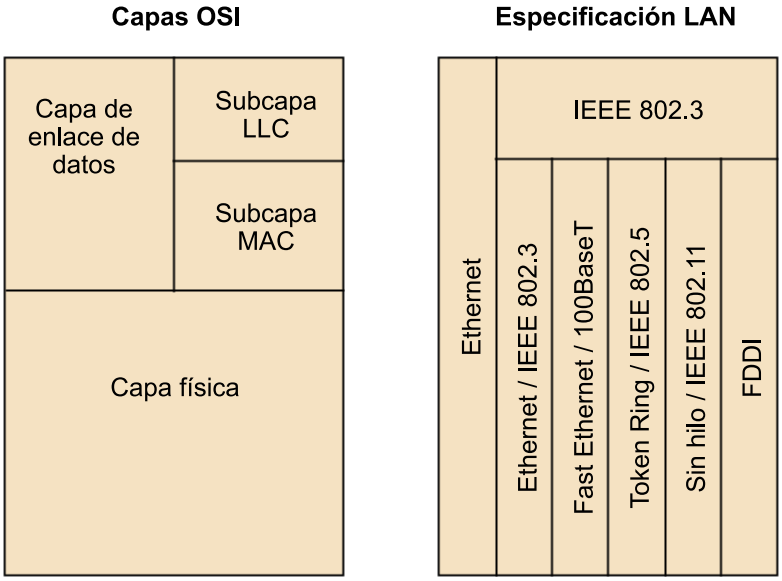
pueden generar conflictos, también denominados *colisiones*. Es necesario un control de acceso al medio en redes *broadcast*. El IEEE divide la capa de enlace en dos subcapas:

- Subcapa inferior MAC, que se ocupa de resolver el problema de acceso al medio.

- Subcapa superior LLC[37], que cumple una función equivalente a la de la capa de enlace en las líneas punto a punto: es responsable de la identificación de la forma lógica de los diferentes tipos de protocolo y su encapsulación.

[37]LLC es la sigla de *logical link control*.

Figura 22



Ejemplos de protocolos de la capa de enlace

Ejemplos de protocolos de la capa de enlace son: SDLC de IBM, HDLC del ISO y el conjunto de protocolos LAP (capa de enlace en ITU-T X.25).

Los protocolos más representativos de la subcapa MAC, citados anteriormente, son IEEE 802.3 (también conocido como Ethernet), 802.4 (Token Bus), 802.5 (Token Ring) y ANSI X3T9.5/ISO 9314 (FDDI). El protocolo de la subcapa LLC para todas las redes locales de difusión es IEEE 802.2.

Los equipos que podemos encontrar en este nivel son: tarjetas de red Ethernet, interruptores Ethernet y Token Ring (LAN), interruptores de conmutación de paquetes Frame relay o ATM (WAN).

2.4.4. La capa de red

El objetivo funcional fundamental de la capa de red es encaminar los paquetes (unidad de información del nivel de red) desde un origen a un destino mediante los nodos de la red.

Para conseguirlo, la capa debe conocer la topología de la red, intentando evitar las conexiones congestionadas y gestionando cuestiones como la ubicación de los ordenadores origen y destino en subredes diferentes. No obstante, y como en las otras capas, la misión principal de la capa de red es proporcionar servicios en la capa superior, el nivel de transporte. Los servicios mencionados, en una visión resumida, son los siguientes:

a) Encaminamiento. La capa de red debe determinar cómo encaminar los paquetes del origen al destino. Para ello utilizará una tabla con información sobre los destinos conocidos.

b) Determinación de ruta. Funcionalidad muy ligada a la anterior. Consiste en elegir la mejor ruta entre las disponibles. La capa de red debe conocer la topología de la subred en términos de ciertos parámetros técnicos (número de saltos, ancho de banda, etc.) para poder elegir el mejor recorrido hasta el destino.

c) Control de congestión. Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruyen, lo que da lugar a un cuello de botella y a una degradación del rendimiento. Para evitar la congestión, el nivel de red implementa una serie de mecanismos. El control de congestión y el encaminamiento están estrechamente relacionados.

d) Tratamiento de congestión. Mediante un mensaje ICMP, se notifica al origen los paquetes descartados a causa de problemas de congestión en las colas de los encaminadores.

e) Fragmentación de paquetes. Si una red no admite paquetes de las mismas dimensiones que la primera, el nivel de red fragmenta los paquetes para superar esta situación.

f) Interconexión de redes (conexión de dos o más redes). Cuando la fuente y el destino se encuentran en redes diferentes, surgirán una serie de problemas (encaminamiento o redes con diferentes protocolos) que deberá resolver la capa de red.

Ejemplos de protocolos de la capa de red

Algunos ejemplos de protocolos utilizados en la capa de red son ITU-T X.25 y X.75 (pasarelas entre redes X.25), el IP y su sucesor IPv6, el protocolo de encaminamiento OSPF o la capa de red en ATM. Los equipos que trabajan en este nivel son los encaminadores.

2.4.5. La capa de transporte

La función principal del nivel de transporte es aceptar los datos de las capas superiores (muchas veces las propias aplicaciones de usuario), fragmentarlos, si es necesario, en unidades más pequeñas, pasarlos al nivel de red y garantizar que lleguen al destino de manera segura y económica, independientemente de la red o de las redes físicas que se encuentren en uso.

El diálogo entre entidades de transporte es de extremo a extremo y no por saltos, como en los de niveles inferiores. Dado que el objetivo de la red de comunicación es posibilitar un diálogo directo entre sistemas finales, el nivel o la capa de transporte podría considerarse el corazón de toda la jerarquía. Desde el punto de vista del usuario que necesita conectar varios equipos remotos, el servicio de transporte es el que resuelve su problema.

Las principales funciones de la capa de transporte son:

- Establecer, mantener y acabar las conexiones entre dos ordenadores principales o entre un servidor y un ordenador principal.
- Controlar el flujo extremo a extremo entre dos estaciones finales.
- Controlar la congestión producida en los encaminadores intermedios que forman parte del recorrido entre el origen y el destino.
- Fragmentar la información de la capa de sesión en segmentos más pequeños.
- Recomponer la información en el destino.
- Mejorar la calidad de servicio suministrada por la capa de red. Garantiza una transmisión fiable, sin errores, extremo en extremo, independiente del tipo de red.
- Responsable de qué que los datos lleguen ordenadas, sin perdidas, sin errores y sin duplicaciones al destinatario.
- Multiplexar diferentes conexiones de transporte sobre una misma conexión de red, utilizando uno o más puertos de salida para la misma comunicación.

Ejemplos de protocolos de la capa de transporte

Entre los protocolos del nivel de transporte podemos destacar: TCP y UDP (TCP/IP), SPX (Netware), etc. No suele haber dispositivos en la red que trabajen en el nivel 4, exceptuando los terminales y servidores finales de una red. No obstante, los encaminadores con funciones cortafuegos también trabajan en este nivel.

2.4.6. La capa de sesión

La capa de sesión es un concepto que aparece por primera vez con OSI. Por lo tanto, se trata de una innovación del OSI.

Entre sus funciones podemos destacar:

- Administra el intercambio de datos, asegurando la entrega correcta de la información.
- Se encarga de establecer, mantener y cerrar el diálogo entre los ordenadores principales que se están comunicando. Esto incluye el establecimiento, la detección y la sincronización de los dos ordenadores principales (servicio de conexión, sincronismo, etc.).
- Controlar la orden de intervención de los interlocutores en ciertos diálogos, indicando quién debe emitir en cada instante.
- Mejora el servicio de la capa de transporte: se encarga de la resincronización de la transferencia, lo que permite a los usuarios la vuelta a un estado anterior después de un problema (por ejemplo, para recuperar una sesión después de un reset, volver a un estado conocido, etc.).

Ejemplos de protocolos de la capa de sesión

Como ejemplos de protocolos de este nivel tenemos: FTP, TELNET; SMTP, TFTP, RPC[38], que es un mecanismo para efectuar llamadas en procedimientos remotos, SNMP, etc.

[38] RPC es la sigla de Remote Procedure Call.

2.4.7. La capa de presentación

El principal objetivo de la capa de presentación es eliminar los problemas que puedan surgir al comunicar datos entre diferentes arquitecturas. Cada arquitectura de ordenadores puede tener su propia estructura de representación interna de los datos que no tienen por qué ser compatibles. El trabajo de la capa de presentación se concreta en una tarea de traducción, asegurando el entendimiento entre sistemas diferentes mediante acuerdos y conversiones de datos.

Básicamente, la capa de presentación recibe datos de la capa de aplicación y los codifica antes de su transmisión para adaptarlos a la manera de codificación propia del sistema de transmisión. Ya en el destino, los descodifica según el sistema de representación que se utilice en el mencionado extremo. Entre sus funcionalidades podemos destacar:

a) Se ocupa de la sintaxis y de la semántica de la información que se pretende transmitir. Compatibiliza arquitecturas con estructura de datos diferentes.

b) Describe el formato de los datos que se intercambiarán entre las aplicaciones:

- Comprensión de datos (reducción tamaño): elimina aquellos componentes superfluos de los mensajes que van a transmitirse. Después pueden ser añadidos directamente en el extremo receptor.

- Encriptación de la información (privacidad): codifica la información transmitida, de manera que una hipotética escucha del sistema no pueda recuperar el mensaje original si no conoce el código de descodificación.

- Estándares para el intercambio de voz y vídeo.

Ejemplos de protocolos de la capa de presentación

En protocolos de este nivel podemos destacar: RFS, SMB, NCP, NFS, etc.

2.4.8. La capa de aplicación

Es la capa superior del modelo de referencia OSI, que define la interfaz y los protocolos que utilizarán los procesos de los usuarios o aplicaciones. En esta capa se sitúan tanto las aplicaciones propias del usuario como una serie de utilidades estándares de uso. Éstas son tan comunes en el mundo informático que se decidió elaborar normas para el desarrollo de soluciones universales (acceso al terminal, acceso a los servidores y ordenadores principales remotos, etc.).

La función de este nivel consiste en proporcionar:

- Procedimientos precisos que permitan a los usuarios ejecutar los pedidos relativos a sus propias aplicaciones.

- Un medio para que los procesos de las aplicaciones accedan al entorno OSI, utilizando los servicios que ofrece la capa de presentación para las necesidades de comunicación.

- Interacción entre aplicaciones e intercambio de datos.

Ejemplos de protocolos de la capa de aplicación

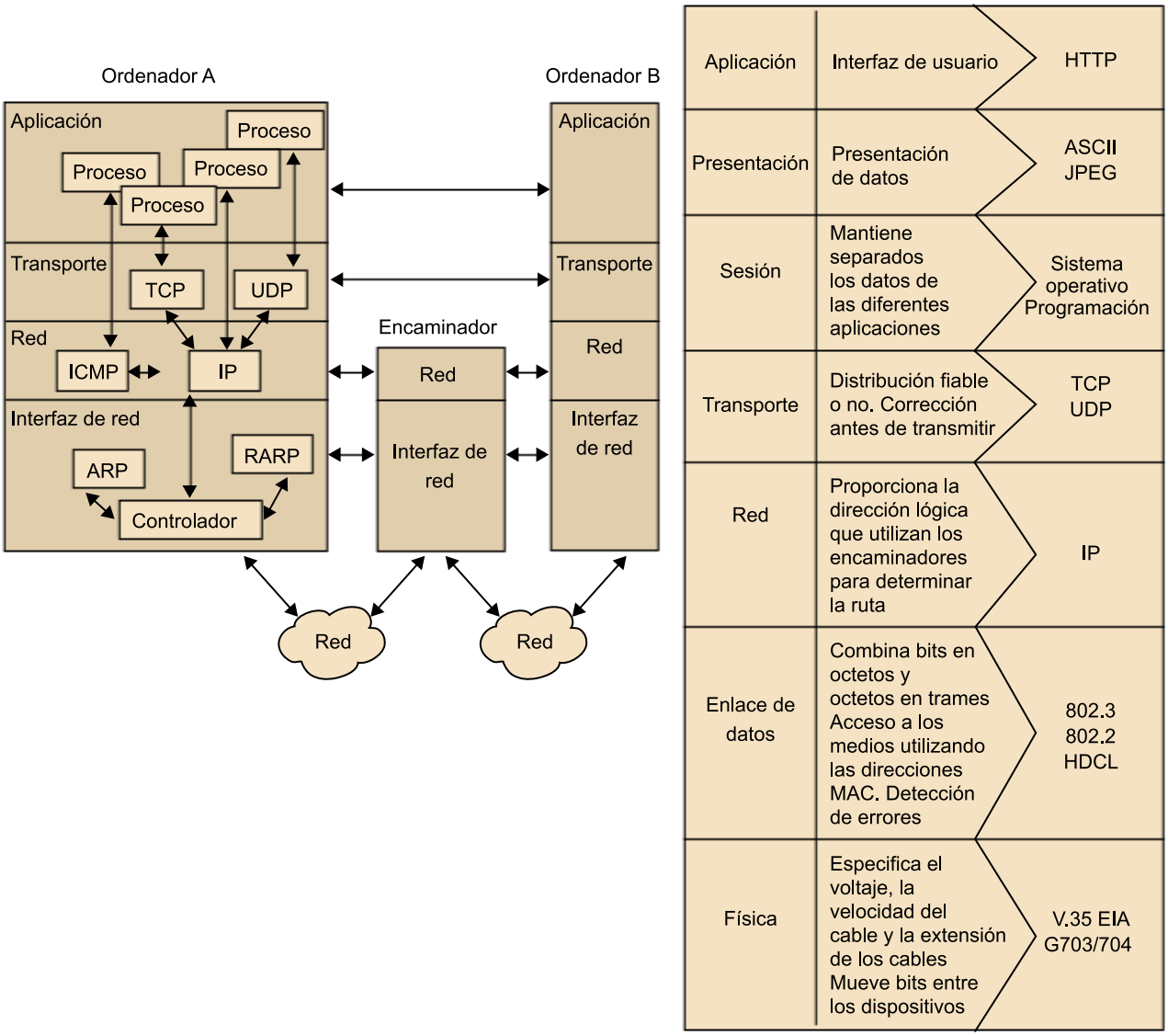
Dos normas muy conocidas de este nivel son: FTAM (transferencia de ficheros), X.400 (correo electrónico) y X.500 (directorio) del CCITT; también destacan las normas ISO 8649, 8650 y 8571.

Los equipos que encontramos en este nivel son los terminales (clientes y servidores) y los gateways de aplicación o proxys.

2.5. Modelo TCP/IP

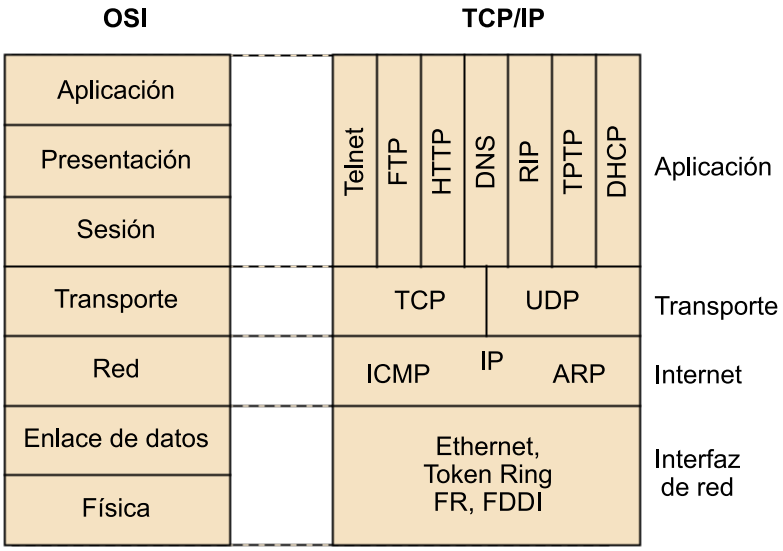
En el modelo TCP/IP se pueden distinguir cuatro capas: la capa interfaz de red, la capa de red o Internet, la capa de transporte y la capa de aplicación.

Figura 23



La comparación de los modelos arquitectónicos de OSI y TCP/IP es la siguiente:

Figura 24

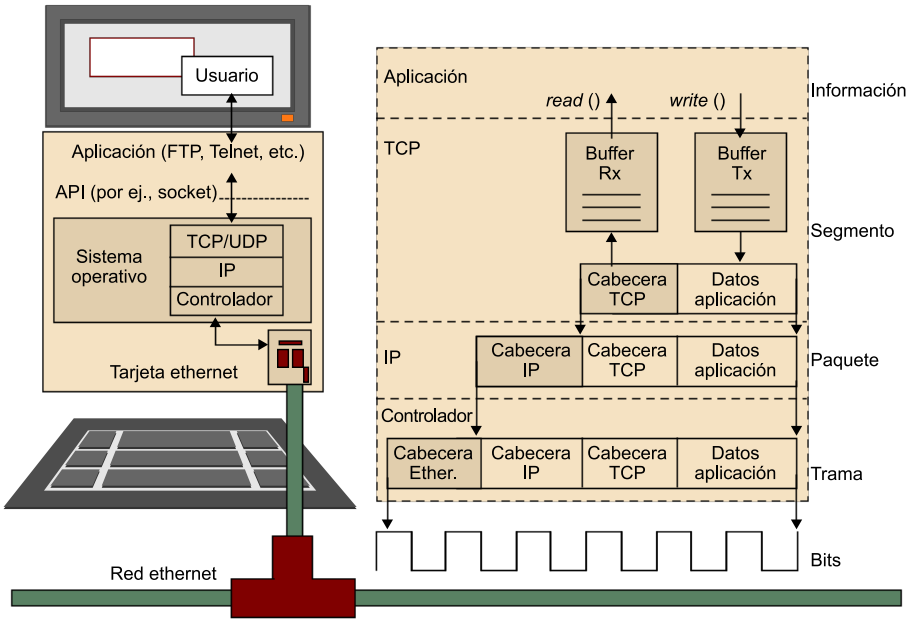


El modelo OSI tiene siete capas, mientras que el modelo TCP/IP sólo tiene cuatro. Las capas de transporte y de Internet coinciden plenamente con los niveles 3 y 4 de la torre OSI. La capa de aplicación engloba los niveles 5, 6 y 7 de OSI (sesión, representación y aplicación). La capa interfaz de red incluye los niveles físico y enlace de la torre OSI.

2.5.1. Encapsulación de la información torre TCP/IP

El funcionamiento del modelo OSI con la encapsulación de los datos se puede observar en la figura 25.

Figura 25



Los datos de información del nivel aplicación son encapsulados en la capa de transporte, a la que se añade la cabecera del protocolo TCP. De este modo, se constituye la unidad de información denominada **segmento**. Cuando el seg-

mento es enviado al nivel de red, es encapsulado dentro de la cabecera del protocolo IP, en el que se indican las direcciones IP de la unidad de información denominada **paquete** en este nivel. Este paquete es enviado a la tarjeta de red y aquí es encapsulado según las normas del protocolo del nivel de enlace. Normalmente, añade una cabecera de protocolo de enlace al principio del paquete. En muchos protocolos, también se añade una cola de datos que sirve para la detección de errores al final del paquete. La unidad de información recibe aquí el nombre de **trama**. Por último, los datos son enviados por el medio de transmisión como impulsos electromagnéticos o bits.

2.5.2. La capa interfaz de red

En Internet, por debajo del nivel de red, existe lo que Tanenbaum (2003) denomina "un gran vacío".

Lectura recomendada

Andrew S. Tanenbaum (2003). *Redes de ordenadores* (4.ª ed.). Pearson.

Esta capa es una especie de "caja negra" que engloba las funciones de las capas física y enlace del modelo OSI. El modelo TCP/IP sólo especifica que esta capa debe ser capaz de conectar el ordenador principal a la red por medio de algún protocolo que permita enviar paquetes IP.

Cuando aparece una nueva tecnología de red, se debe especificar de qué modo se pueden enviar paquetes IP mediante la nueva tecnología.

Los dos primeros protocolos diseñados para enviar paquetes IP fueron SLIP[39] y, sobre todo, PPP[40]. Estos protocolos también se pueden usar para las conexiones entre nodos en líneas dedicadas a subredes de Internet.

[39]SLIP es la sigla de Serial Line IP.

[40]PPP es la sigla de Point to Point Protocol.

2.5.3. La capa de red (Internet)

Esta capa es el eje de la maquinaria que mantiene unida la red. Sus funciones encajan completamente en la especificación OSI, esto es, encaminamiento y control de congestión, principalmente. Como es sabido, Internet surgió a partir de un proyecto del Departamento de Defensa de Estados Unidos, en cuyo diseño la resistencia a interrupciones en líneas de la subred era uno de sus principales. Ésta es la principal razón de que la capa Internet proporcione un único servicio de conmutación de paquetes no orientado a conexión.

El principal protocolo de la capa de red en Internet es IP. Las especificaciones de IP establecen que es posible que paquetes de una misma conversación lleguen a su destino en diferente orden a como fueron depositados en la red. Este funcionamiento se denomina transmisión en modo datagrama.

En este caso, la reordenación es responsabilidad de las capas superiores (este papel lo asume el eficaz protocolo de nivel de transporte de Internet, TCP).

Con respecto al encaminamiento, IP establece un esquema de direcciones jerárquico para el reconocimiento de redes y subredes.

La versión original de IP fue IPv4. Sus carencias respecto al explosivo crecimiento de la red han motivado la definición de un sucesor IPv6, que se está implantando gradualmente.

Los protocolos de nivel 3 se dividen en protocolos encaminados[41] y de encaminamiento[42]:

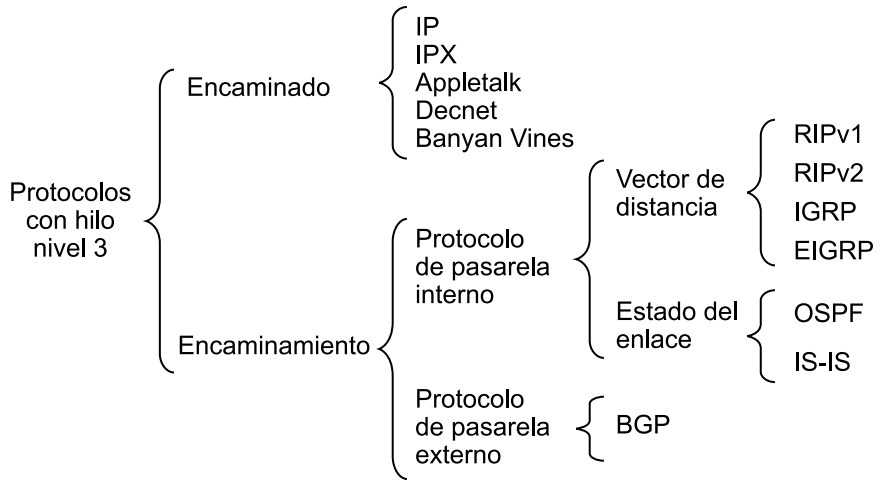
(41) En inglés, *routed*.

(42) En inglés, *routing*.

1) Protocolos encaminados: son los protocolos que llevan información de usuario desde un origen a un destino.

2) Protocolos de encaminamiento: son los protocolos de control que utilizan los nodos de la red para conocer las rutas hacia los destinos y elegir las mejores.

Figura 26



El nivel de red de TCP/IP también define dos protocolos auxiliares que ayudan a IP a realizar sus funciones: ARP, que mantiene la correspondencia entre direcciones lógicas con físicas, e ICMP (protocolo de control de mensajes y errores).

2.5.4. La capa de transporte

Esta capa también encaja perfectamente en la definición del nivel de transporte del modelo de referencia OSI.

Su función es ofrecer a las aplicaciones del nivel superior un canal de comunicaciones extremo a extremo[43] (denominado *socket* en UNIX) en nivel de transporte. El nivel de transporte define un sistema de multiplexación y demultiplexación de aplicaciones, de manera que cada aplicación de red tiene un número asociado denominado *puerto* que permite al protocolo de transporte identificarla.

(43)Canal denominado *socket* en UNIX.

El nivel de transporte de Internet se organiza en dos protocolos:

1) TCP[44], que ofrece un servicio fiable orientado a conexión, con el que los paquetes (denominados *segmentos* en este nivel TCP/IP) llegan ordenados y sin errores. Efectúa retransmisiones, control de flujo y de congestión extremo a extremo (para aplicaciones de datos).

(44)TCP es la sigla de *transmission control protocol*.

2) UDP[45], que ofrece un servicio de datagramas no orientado a conexión y no fiable. UDP no realiza retransmisión de paquetes, ni control de flujo ni de congestión, tareas que quedan encomendadas a los servicios de nivel superior que usen este protocolo. Sólo detecta errores extremo a extremo. Las aplicaciones típicas que utilizan UDP son aquellas en las que la velocidad de transmisión interesa más que la precisión en la entrega, como el envío de voz o vídeo (para aplicaciones en tiempo real).

(45)UDP es la sigla de *user datagrama protocol*.

2.5.5. La capa de aplicación

El nivel de aplicación es el que entra en contacto con los usuarios finales. Tiene la particularidad de que incluye cualquier función o servicio que se utilice en la red y que no se suministre en los niveles anteriores.

En el modelo TCP/IP, esta capa aglutina las funciones de las capas de sesión, presentación y aplicación del modelo OSI. Se ha constatado empíricamente que las capas de sesión y presentación son de poca utilidad, debido a que su contenido es escaso y redundante, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

Así, se puede resumir la funcionalidad de la capa de aplicación en:

1) Un conjunto de servicios de soporte necesarios para el funcionamiento de las aplicaciones:

- Compresión de la información transmitida: ZIP o RAR
- Seguridad y confidencialidad: SSL
- Gestión de red: SNMP
- Gestión y conversión de nombres de dominio: DNS

2) Las aplicaciones propias que ofrecen servicios a los usuarios. Entre ellas podemos destacar:

- Correo electrónico (*e-mail*, POP3, SMTP, IMAP)
- Transferencia de ficheros (FTP y SFTP)
- World Wide Web (HTTP y HTTPS)
- Terminal remoto (Telnet)

2.6. Modelo OSI comparado con modelo TCP/IP

El modelo OSI, de orientación más académica, es más coherente y modular y está menos condicionado por ningún protocolo en concreto. Por ello, se utiliza principalmente como modelo de referencia para describir otros tipos de arquitecturas, como la TCP/IP (el modelo TCP/IP nunca se utiliza para describir otras arquitecturas que no sean la suya). El modelo OSI hace una distinción muy clara entre servicios, interfaces y protocolos, conceptos que a menudo se confunden en el modelo TCP/IP.

No obstante, el modelo OSI nunca ha pasado de ser un bonito desarrollo teórico, aunque la mayoría de los grandes fabricantes de ordenadores y compañías telefónicas impulsaron su utilización ofreciendo productos y servicios basados en ellos. Las razones principales que motivaron este fenómeno se resumen en:

- OSI apareció tarde. Como todo estándar, se tardó años en definir una arquitectura de capas con funcionalidades y servicios perfectamente definidos. Este retraso motivó que OSI fuera adelantado por TCP/IP, que en aquella época ya se utilizaba profusamente.

- OSI, al inspirarse en SNA de IBM, que es una arquitectura compleja, resulta muy difícil y a menudo repite las mismas funciones en diferentes capas. El nacimiento de TCP/IP se desarrolló al contrario: primero se especificaron los protocolos y después se definió el modelo como una simple descripción de los protocolos ya existentes. Por este motivo el modelo TCP/IP es más simple que el OSI.

- Los productos comerciales que se basaron en OSI eran malos y caros. La poca demanda obligaba a las empresas que los desarrollaban a poner unos altos precios con el fin de recuperar sus altísimas inversiones. Por el contrario, TCP/IP fue rápidamente incorporado en el UNIX de Berkeley, donde funcionaba bastante bien, y además a un precio sensiblemente menor: ¡era gratuito!

- Mientras que TCP/IP era visto como algo independiente de UNIX, es decir, un modelo que realmente funcionaba y existía al margen de toda sospecha de parcialidad, OSI era considerado un invento de la Administración para controlar las telecomunicaciones (un engendro político-burocrático).

Por ello, TCP/IP se convirtió en el líder mundial absoluto en interconexión de redes. No obstante, TCP/IP tampoco se libró de la crítica. En primer lugar, no distingue conceptos tan importantes como servicio, interfaz y protocolo. En segundo lugar, el modelo TCP/IP no es ningún modelo, es decir, resulta bastante inútil para su utilización como esquema de referencia en el estudio de otras arquitecturas. Y en tercer lugar, nos encontramos con la capa ordenador principal-red, que en el modelo TCP/IP parece más una interfaz que una capa, ya que lo único que se especifica de ella es que ha de ser capaz de transmitir paquetes IP.

Actualmente, TCP/IP se ha difundido por toda Europa, mientras que los servicios basados en protocolos OSI prácticamente han desaparecido.

3. Breve historia de las comunicaciones

La década de los sesenta asistió a la aparición de los primeros ordenadores comerciales. Eran grandes, caros y poco potentes. Sólo organismos oficiales, grandes empresas o universidades los podían comprar, y lo habitual es que sólo compraran uno (o algunos, pero no uno para cada usuario, como hoy estamos acostumbrados a ver). Por ello, estos ordenadores tenían sistemas operativos multitarea y multiusuario, para que diferentes usuarios, realizando diferentes trabajos, los pudieran utilizar simultáneamente. El acceso a estos ordenadores se hacía mediante terminales sin ninguna capacidad de proceso, eran pasivos.

Sin embargo, no tardó mucho en surgir la necesidad de poder alejar los terminales de la unidad central para conectarse, por ejemplo, desde casa o desde una delegación al ordenador principal.

Para lograr este acceso remoto, la primera solución que aportaron los ingenieros informáticos de la época fue utilizar la red telefónica que, por su ubicuidad, les evitaba generar cualquier nueva infraestructura. Sólo era necesario un aparato que adaptara los bits a la red (recordad que la red telefónica sólo deja pasar sonidos entre unos márgenes de frecuencia). Estos aparatos son los módems.

Figura 27. Módems de los años ochenta

Los primeros módems eran de 300 bps y generaban dos tonos diferentes: uno para el 1 lógico y otro para el 0. Actualmente, son de 56.000 bps, que es el máximo que permite la red telefónica convencional. Los módems no sólo servían para poder alejar los terminales pasivos de los ordenadores principales, también permitían interconectar ordenadores entre sí, de manera que desde un terminal se podía acceder a otro y viceversa.

Originalmente, la tecnología de conmutación de circuitos se desarrolló para las comunicaciones telefónicas, y una de sus características fundamentales era la ocupación exclusiva de los recursos mientras duraba la conexión, hecho que (como ya hemos visto) justificaba la tarifación por tiempo. Pero las comunicaciones informáticas no son breves, intensas y esporádicas como las de voz. Al conectar un terminal a un ordenador principal mediante dos módems, no se pasan datos durante todo el tiempo que dura la conexión: puede haber largos períodos en los que no pase ningún bit y otros en los que haya un intercambio de datos intenso, aunque sea a una velocidad de transmisión mucho más baja que la que se puede mantener entre el terminal y el ordenador conectados directamente. Las facturas telefónicas empezaron a ser astronómicas y desproporcionadas respecto al uso real de la red.

Breve historia de las comunicaciones I

Internet es, como tantas otras tecnologías innovadoras, un invento militar. Nació por el interés del Ejército norteamericano en los años sesenta en conseguir comunicaciones fiables y descentralizadas. Es decir, para evitar que un misil bien dirigido pudiera volar

por los aires un centro vital de comunicaciones. Se pueden establecer cuatro períodos clave en la historia de Internet.

Primer período: 1957-1970. Nacimiento de Internet

- 1945: publicación de la primera referencia a una red electrónica similar a Internet: Memex, citado en el artículo "As We May Think", por Vannevar Bush (director de la Oficina de Investigación Científica y de Desarrollo norteamericana).

- 1957: durante la Guerra Fría la Unión Soviética lanza el Sputnik, el primer satélite artificial de comunicación. En respuesta a este hecho, Estados Unidos crea ARPA (), en el seno del Departamento de Defensa de Estados Unidos.

- 1961: Leonard Kleinrock (MIT) publica el primer artículo sobre la teoría de conmutación de paquetes.

- 1962: Licklider (MIT) lanza la idea de "Galactic Network", una red interconectada globalmente por la que cada uno pudiera acceder desde cualquier lugar a datos y programas. Licklider fue el principal responsable del programa de investigación en ordenadores de la Agencia de Proyectos de Investigación Avanzada del Pentágono.

- 1964: Paul Baran (RAND Corporation) realiza sus estudios sobre "Redes de Comunicación Distribuidas o descentralizadas". También promueve el uso de redes de conmutación de paquetes de datos (en inglés, *packet switching networks*).

- 1961-1965: la idea de red de paquetes descentralizada fue desarrollada por tres grupos de investigación americanos simultáneamente, sin que uno supiera la existencia y el trabajo de los otros. Estos grupos fueron y estuvieron formados por:
  1) MIT (1961-1967): Licklider, Roberts, Kleinrock.
  2) RAND (1962-1965): Paul Baran.
  3) NPL (1964-1967): Donald Davies y Roger Scantlebury.
  El término *paquete* (en inglés, *packet*) fue adoptado a partir del trabajo del NPL.

- 1965: el Ministerio de Defensa norteamericano inicia un proyecto de interconexión de ordenadores denominado ARPANet, el antecesor de lo que después sería Internet.

- 1966: se desarrolla el concepto de red de ordenadores denominado ARPANet, que podía interconectar los diferentes ordenadores de los investigadores que se fueran conectando a esta red, lo que permitió a su vez el nacimiento de Backbone Network.

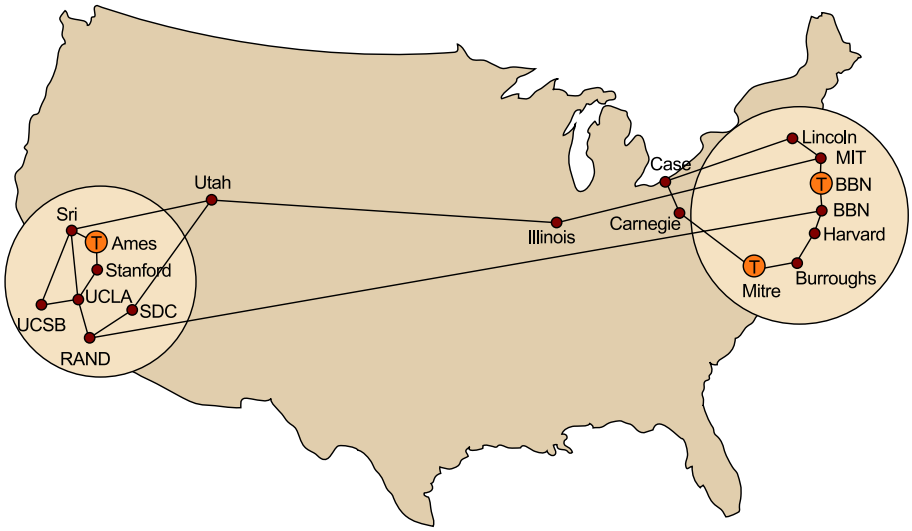
- 1967: la nueva red ARPANet inicia su andadura. Un año más tarde, se diseñan los primeros programas y el primer hardware específico para redes.

- 1969: existen cuatro centros interconectados, mediante sus IMP (Internet embrionaria). UCLA (Los Angeles) es seleccionada para ser el primer nodo de ARPANet. El centro de investigación de Standford (SRI) proporcionó un segundo nodo. El tercer nodo se situó en la Universidad de California, en Santa Bárbara. Y el cuarto nodo se estableció en la Universidad de Utah. Estos cuatro nodos constituyeron la red original de ARPANet.

Pronto, las grandes empresas presionaron a las compañías telefónicas del momento para que desarrollaran redes pensadas para transportar datos, cuyo sistema de tarifación se ajustara al tráfico de datos real y permitiera más velocidad que los escasos 300 o 1.200 bps de la época, que se alcanzaban utilizando la red telefónica. La respuesta fueron las redes de conmutación de paquetes. El envío de datos no debe realizarse necesariamente en tiempo real (las transmisiones de voz, sí). Por lo tanto, ni es necesario establecer el camino entre los dos puntos antes de empezar la transmisión ni mantenerlo mientras dura el intercambio de datos. En lugar de eso, se empaquetan los bits que se han de transmitir y se presentan en la central más próxima para que ésta los envíe cuando pueda a la siguiente, y así sucesivamente hasta que lleguen a

su destino. Si cuando un paquete llega a una central todos los enlaces con la siguiente están ocupados, no pasa nada, se coloca en una cola para enviarlo cuando haya un enlace disponible.

Figura 28. Nodos en ARPANET en septiembre de 1971



El CCITT es un organismo internacional patrocinado por las operadoras de telefonía que se dedica a tareas de normalización a nivel de las telecomunicaciones. El 1 de marzo de 1993 pasó a denominarse ITU-T[46].

[46]ITU-T es la sigla de International Telecommunication Union Standardisation Sector.

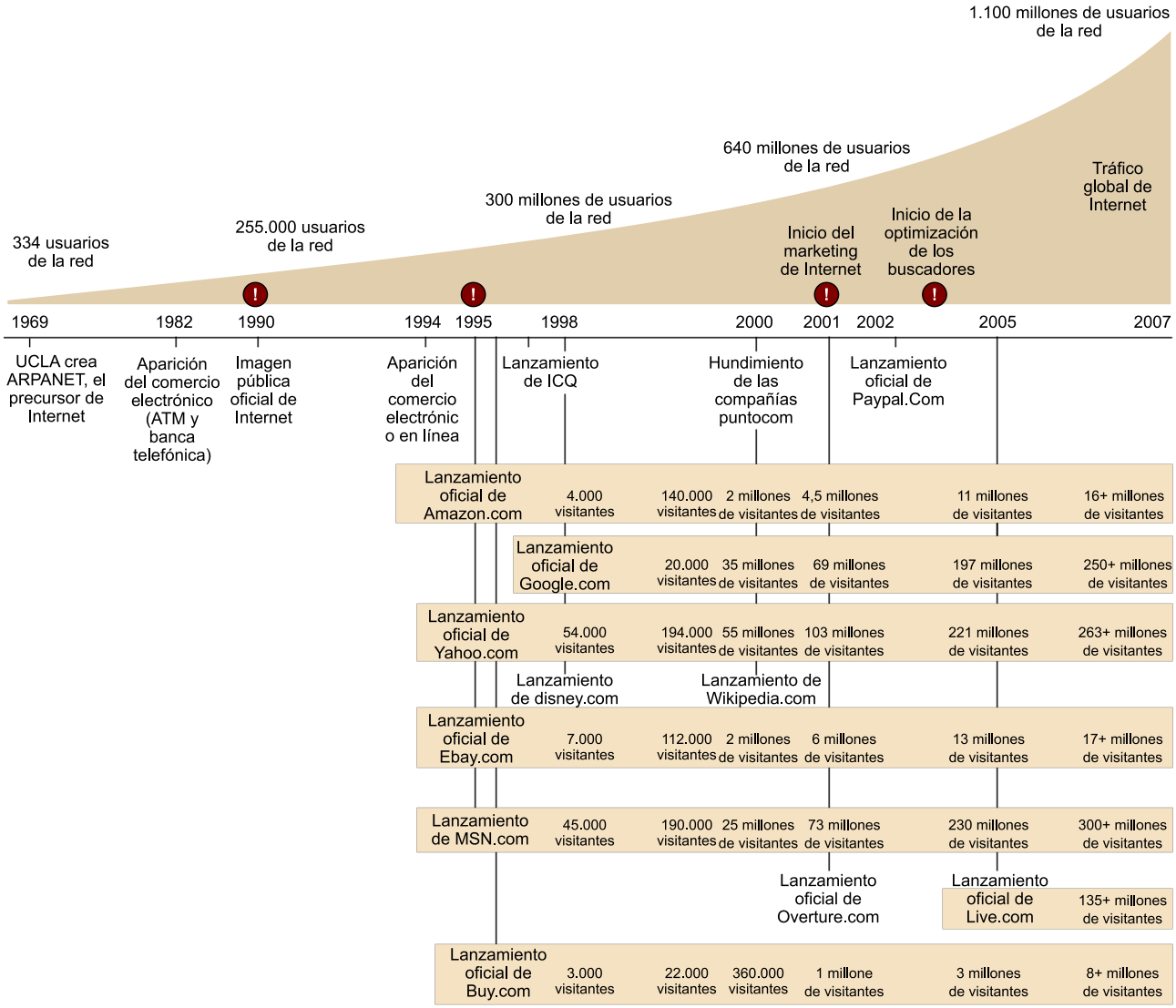
La transmisión por paquetes tiene la ventaja de que sólo ocupa los recursos cuando realmente se utilizan. Como contrapartida, se debe soportar el retraso que pueda producirse entre el tiempo que los paquetes salen del origen y llegan a su destino. Este período es variable, ya que las esperas en las colas son aleatorias al depender del estado de la red. Pero, como hemos dicho, eso, en comunicación de datos, es hasta cierto punto tolerable. Con respecto a la cuestión económica, no tiene sentido que se cobre por tiempo de conexión: en las redes de datos se paga por bits transmitidos.

Existe otro peligro, que los paquetes se pierdan. Hay que tener presente que las colas son limitadas y, si llega un paquete cuando una ya está llena, éste no se podrá guardar y se perderá. Por lo tanto, se deben prever mecanismos que eviten estas pérdidas y regulen el flujo de información entre los nodos de conmutación.

Las compañías telefónicas desarrollaron redes de este tipo, y el CCITT emitió un estándar, el X.25, que a la larga es el que ha seguido todo el mundo hasta hace poco.

Breve historia de las comunicaciones II

Figura 29



Segundo período: 1970-1990. Del Ejército a la Universidad

- Años setenta: durante este período, esta red fue de acceso restringido a los investigadores y a las empresas privadas que participaban en proyectos financiados por la Administración.

- 1970: el NWG (*Network Working Group*), liderado por S. Crocker, acabó el protocolo ordenador central a ordenador central inicial para ARPANet, denominado NCP (*network control protocol*, en castellano, *protocolo de control de red*). Kevin MacKenzie inventa el primer emoticono: :-). Vinton Cerf escribe por primera vez la palabra y es considerado el padre de la Red. Más tarde, diseñó el protocolo TCP/IP, que actualmente rige las comunicaciones por Internet.

- 1971: Ray Tomlison (BBN) crea los protocolos básicos del correo electrónico (*e-mail*), incluyendo la convención de la arroba para separar el nombre de la persona del identificador del ordenador.

- 1972: Se presenta públicamente ARPANet en la International Computer Communication Conference. Investigadores del MIT dieron a luz el germen de lo que sería el sistema de transferencia de archivos FTP y Telnet. El Sistema de Agencias de Información de Defensa crea IANA o Autoridad de Asignación de Números de Internet, responsable de asignar una dirección única a cada ordenador conectado a Internet.

- 1973: Vinton Cerf y Bob Kahn especifican la primera versión del programa de control de transmisión (TCP), que fue desarrollado hasta convertirse en el *transmission control protocol/internet protocol* (TCP/IP), los protocolos que actualmente permiten el

funcionamiento de Internet. Berkeley desarrolló el BSD UNIX. ARPA dio una copia de TCP/IP a Berkeley y se este software incorporó a la versión UNIX. Nace la posibilidad de realizar un FTP.

- 1979: nace Usenet. Creada por tres estudiantes, Tom Truscott, Jim Ellis y Steve Bellovin, Usenet es un servicio de grupos de noticias, las populares *news*.

- 1980: aparecen las primeras aplicaciones TCP/IP. Internet ya cuenta con 212 servidores.

- 1981: En el año 1981, IBM lanza el primer PC, con el sistema operativo de una pyme denominada Microsoft.

- 1982: ARPANet adopta el protocolo TCP/IP como estándar. Se crea la EUNet (*european unix network*). El EUNet, conectado a ARPANet, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diferentes organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.

- 1983: en este año se considera que nació realmente Internet, al separarse la parte militar y la civil de la red. Hasta el 1 de enero de 1983, la reciente Internet funcionó con un antecesor de los protocolos TCP/IP; aquel día, los ya miles de ordenadores conectados se cambiaron al nuevo sistema. En ese momento, Internet disponía de 562 servidores (ordenadores interconectados). Ese mismo año se crea el sistema de nombres de dominios (.com, .edu, etc., más las siglas de los países), que prácticamente se ha mantenido hasta ahora.

- 1984: el ordenador pasa a estar al alcance de la gente, y su implantación se acelera cuando se presenta el Macintosh. El número de servidores conectados a la red había superado ya los 1.000. Al año siguiente, se implanta Well, la primera comunidad comercial de usuarios. En Winsconsin se crea el primer servidor de nombres (en inglés, *name server*), con el que basta conocer el camino (en inglés, *path*) de localización de un ordenador, precursor del servicio DNS (*domain name server*) de Internet.

- 1985: entra en funcionamiento el DNS, un método para resolver nombres de direcciones numéricas. El primer dominio se otorga el 15 de marzo a symbolics.com. Internet tiene ya 1961 servidores y sufijos como .net y .org añadidos. En abril aparecen los primeros dominios con letra, que fueron: acmu.edu, purdue.edu, rice.edu y ucla.edu, todos ellos de ámbito universitario y todavía en activo. En junio del mismo año apareció el primer dominio gubernamental, css.gov, y en julio, mitre.org. El primer dominio de un país se le atribuyó a Gran Bretaña un mes más tarde: co.uk.
  En España, los ordenadores de diferentes universidades se conectaban entre sí y mediante el CERN (Centro Europeo de Física de Partículas). El Ministerio de Educación y Ciencia, por medio de la Secretaría de Universidades, elaboró un plan para interconectar los centros de cálculo de las universidades. Asimismo, un grupo de expertos de las universidades, centros de cálculo, organismos públicos de investigación y Telefónica, bajo la coordinación de Fundesco, realizó el informe conocido como Proyecto IRIS (interconexión de recursos informáticos).

- 1987: nace la primera versión de Windows. Existen más de 10.000 servidores en todo el mundo.

- 1988: se produce el primer gran ataque vírico de Internet. El denominado "Gusano de Morris" contagió 6.000 de los 60.000 ordenadores que entonces formaban parte de la red. Fue creado por el estudiante predoctoral Robert T. Morris, como un experimento: el gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el ordenador. A raíz del "gusano de Morris" se crea el CERT[47] (*Computer Emergency Response Team*). Jarkko Oikarinen, un joven finlandés, decidió modificar el comando Talk de Unix para permitir que distintas personas pudieran hablar simultáneamente. Así nace el chat, el IRC (*Internet Relay Chat*), que permite que se pueda conversar en línea.
  En 1988 también nace el programa IRIS dentro del Plan nacional de investigaciones y desarrollo tecnológico para dar conectividad a científicos e investigadores. La financiación y la supervisión de esta red las efectuaría la Comisión Interministerial de Ciencia y Tecnología, gestionada y dirigida por Fundesco.

- 1989: nace RIPE para interconectar las redes europeas. El número de servidores conectados a Internet alcanza ya los 100.000. Ese mismo año, se inauguró la primera conexión de un sistema de correo electrónico comercial a Internet (MCI y Compuserve).
  Hasta aquel momento, nadie se había planteado nunca la hipótesis de que en Internet las cosas pudieran tener un orden, mediante la creación de un directorio. Las direcciones eran tan pocas que se suponía que todo el mundo las conocía. Por este motivo se crea el primer catálogo (un programa denominado Archie). Archie tuvo

tal éxito que colapsó el tráfico en Estados Unidos y Canadá en cuanto se conoció su existencia. En consecuencia, la Universidad MacGill de Montreal obligó a su autor a cerrarlo. Afortunadamente, lo hizo después de que Archie estuviera repetido en otros ordenadores. Archie fue el precedente de Gopher y Veronica y, en cierto modo, el primer intento de directorio de recursos de Internet.

(47)CERT es un equipo de respuesta de emergencia de ordenadores, que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

Cuando empezó a ser habitual disponer de más de un ordenador en la misma instalación, apareció la necesidad de interconectarlos para poder compartir los diferentes recursos: dispositivos caros, como impresoras de calidad, un disco duro que almacenara los datos de la empresa, un equipo de cinta para hacer copias de seguridad, etc.

El diseño de las redes de área local siguió caminos completamente diferentes de los que se siguieron para las redes de gran alcance. Habitualmente, en las redes de área local es necesario establecer comunicaciones "muchos en uno" y "uno en muchos", algo difícil de conseguir con las redes de conmutación, pensadas para interconectar dos estaciones. Para este tipo de redes es más adecuada la difusión con medio compartido, por la que los paquetes que salen de una estación llegan a al resto simultáneamente. En la recepción, las estaciones los aceptan o ignoran en función de si son las destinatarias o no.

Se habla de difusión porque los paquetes se difunden por todas partes, y de medio compartido porque esta difusión se efectúa sobre un medio común que las estaciones comparten.

De la década de los sesenta también datan los primeros estándares de arquitecturas de protocolos. Hay que tener presente que el intercambio de información entre ordenadores cuenta con una serie de implicaciones, entre las que destacan:

- Aspectos eléctricos: los cables, los conectores, las señales, etc.

- La manera de agrupar los bits para formar paquetes y el modo de evitar que no se produzcan errores de transmisión.

- La identificación de los ordenadores dentro de la red y la manera de conseguir que la información que cualquier ordenador genera llegue a quien se pretende que lo haga.

Atacar todos estos aspectos de una manera global no es viable: demasiadas cosas y demasiado diferentes entre sí. Por esta razón, desde el principio, se desarrollaron modelos estructurados en niveles: en cada nivel se lleva a cabo una tarea, y la cooperación de todos los niveles proporciona la conectividad deseada por los usuarios.

Debemos tener presente que, en la época que nos ocupa, la informática estaba en manos de muy pocos fabricantes e imperaba la filosofía del servicio integral: cada fabricante lo proporcionaba todo (ordenadores, cables, periféricos, sistema operativo y software). Por lo tanto, cuando una empresa se quería informatizar, elegía una marca y quedaba ligada a ella para toda la vida.

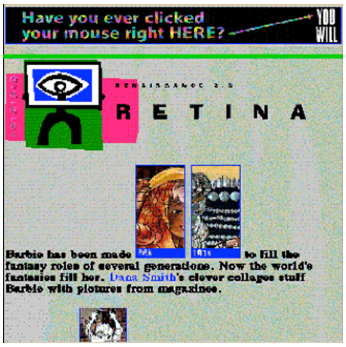
En la década de los setenta, el panorama cambió radicalmente, sobre todo a causa de tres acontecimientos:

1) La propuesta del protocolo Ethernet para redes locales.

2) La aparición del sistema operativo Unix, no ligado a ninguna marca comercial y compatible con todas las plataformas de hardware existentes.

3) La invención de los protocolos TCP/IP, embrión de la actual Internet.

Se había allanado el camino para la aparición de los sistemas abiertos: no era necesario atarse a ninguna marca para tenerlo todo. El hardware podía ser de un proveedor, el sistema operativo de otro, las aplicaciones de un tercero y los protocolos, públicos.



Primer banner de Internet (parte superior de la imagen) en HotWired (1994)

Breve historia de las comunicaciones III

Tercer período: 1990-1995. Expansión fuera de los ámbitos militares y universitarios

- 1990: nace el primer proveedor de acceso a Internet comercial, y el EFF (Electronic Frontiers Foundation), una ONG de defensa de ciberderechos. La red tiene ya centenares de miles de servidores (313.000). El mismo año aparece Windows 3.0. En España, Fundesco cambió el nombre Programa IRIS por el de REDIRIS, y se conectó a la "columna vertebral" (*backbone*) de Internet (NSFNET), junto a Argentina, Brasil, Chile, la India, Suiza, Austria, Irlanda y Corea del Sur.

- 1991: Tim Berners-Lee, investigador en el centro europeo CERN de Suiza, elaboró su propuesta de un sistema de hipertexto compartido: era el primer boceto de la World Wide Web. Como ARPANet veinte años atrás, su propósito era poner en comunicación a los científicos. La WWW es una creación europea fruto del trabajo de Tim Berners-Lee y Robert Cailauu. Su objetivo era buscar una herramienta de trabajo para crear y leer textos a través de una red que permitiera intercomunicar a los físicos de todo el mundo. Berners-Lee creó el HTML, el HTTP y las URL.

- 1992: nace la Internet Society, la "autoridad" de la red. Aparecía como el lugar en el que pactar los protocolos que permitirían la comunicación. La IAB (Internet Activities Board) se integra en la Internet Society. En la IAB destacó la IETF (Internet Engineering Task Force), cuya función era desarrollar Internet a corto plazo y responsabilizarse de la dirección técnica. La mayor parte de los RFC se elaboraron en la IETF, y éstos iban aumentando cada año. Internet cuenta entonces con 1.136.000 de servidores. En España aparece Goya Servicios Telemáticos, el primer proveedor de acceso comercial.

- 1993: aparece el primer visualizador gráfico de páginas web, Mosaic, el antecesor de Netscape. Hasta aquel momento la red era sólo texto: ahora, sobre un fondo gris, aparecen documentos con gráficos y enlaces en azul. El crecimiento de Internet supera el 350.000% (casi dos millones de ordenadores). Marc Andreeseen, cocreador de Mosaic, funda Netscape junto con el veterano ejecutivo de Silicon Valley Jim Clarke. En septiembre, la Universidad Juan Carlos I de Castellón publica el primer servidor web de España, en el que ya había 10 nodos y 15.000 máquinas bajo el dominio .es.

- 1994: surge el primer spam. El 5 de marzo de 1994, los abogados de Arizona Canter & Siegel envían un anuncio a 6.000 grupos de noticias, y son perseguidos por los furiosos internautas, que consiguen que los expulsen de su ISP (y de la abogacía). En octubre, ATT y Zima (un refresco) publican los primeros *banners* comerciales de la historia en Hotwired. Pero no todo son desgracias: también abren el primer centro

comercial, la primera radio y el primer banco en la red. El número de servidores de Internet alcanza los 3.800.000. En la Universidad de Stanford dos estudiantes crean un directorio de cosas interesantes de la red que bautizan como Yahoo! Lycos. Se difunde la versión comercial del navegador Netscape Navigator. En España nace Servicom.

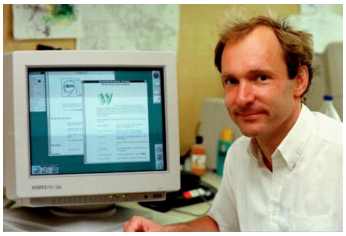
- 1995: se empiezan a cobrar los dominios. Sun crea Java y RealAudio incorpora sonido en la red. Microsoft lanza con gran publicidad Windows 95 y anuncia un giro estratégico hacia Internet. El fabricante Digital (DEC) crea AltaVista, un buscador de Internet. Nacen la librería Amazon.com y la web de subastas eBay. En ese momento, había más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empezaba a ser sustituida por proveedores comerciales interconectados. La salida a bolsa de Netscape, el tercer navegador más importante hasta entonces, marca el comienzo del "boom" de Internet.

TCP/IP nació a partir de un encargo de DARPA en la comunidad científica americana para tener una red mundial que fuera reconfigurable, fácil y automáticamente, en caso de destrucción de algún nodo o de algún enlace.

DARPA

El término DARPA corresponde a las siglas Defense Advanced Research Project Agency (Agencia de Proyectos de Investigación Avanzada para la Defensa).

La pila TCP/IP es una jerarquía de protocolos que ofrecía conectividad y, a pesar de tener poco que ver con las que ya existían, era una opción más en el mercado. Ante una oferta tan grande y dispar de protocolos, la ISO y el CCITT propusieron un modelo nuevo que, de alguna manera, intentaba reunir todo lo que ya se había propuesto, ser más completo y racional y estar muy bien estructurado (TCP/IP tiene fama de ser una pila de protocolos anárquica), con la intención, por lo tanto, de convertirse en un modelo de referencia. Nos referimos a la denominada pila de protocolos OSI. Internet, que nació y creció en las universidades, empezó a popularizarse en la década de los noventa, a medida que los que conocían la red la iban "enseñando", y su popularización se expandió cuando saltó al mundo de la empresa, en todas sus vertientes: como escaparate de productos o como canalizador de contactos comerciales.



Tim Berners Lee. Creador del WWW

Sin embargo, ese origen universitario ha marcado su evolución en muchos sentidos. Por ejemplo, en el modelo cliente/servidor de aplicaciones distribuidas. Es un modelo sencillo y al mismo tiempo potente, y casi todas las aplicaciones que se emplean en Internet lo siguen. Telnet, o apertura de sesión remota, la transferencia de ficheros (FTP), el correo electrónico y, sobre todo, la WWW son ejemplos claros de aplicaciones que siguen este modelo. Las dos primeras han caído algo en desuso, pero tanto el correo como la WWW son las estrellas actuales en Internet. Poco a poco, aparecen nuevas propuestas de aplicaciones, pero la WWW, que nació como un servicio de páginas estáticas enlazadas por hiperenlaces, se está convirtiendo en la interfaz de usuario de toda la red, ya que actualmente se utiliza para servir páginas dinámicas (se crean en el momento en que se sirven) e incluso código que se ejecuta en el ordenador cliente (*applets*).

En este momento tenemos dos redes completamente independientes entre sí, pero superpuestas en cierta medida:

1) Una red analógica, con conmutación de circuitos, pensada para voz.

2) Una red digital, con conmutación de paquetes, pensada para datos.

La red telefónica, tal como lo hemos descrito hasta ahora, es completamente analógica: la señal electromagnética que viaja desde un teléfono hasta otro es analógica (varía continuamente y a cada momento puede tomar cualquier valor) y los circuitos electrónicos que componen la red también lo son.

Los enlaces entre centrales de la red telefónica se realizan mediante señales analógicas, con muchos canales multiplexados en frecuencia que, a veces, debían recorrer grandes distancias. La atenuación de la señal inherente a la distancia que debía recurrir se tenía que corregir mediante repetidores que lo amplificaban, hecho que aumentaba el ruido presente en la línea. Muy a menudo, la señal recibida era de una calidad muy baja porque la transmisión analógica no permite eliminar el ruido y las interferencias en la recepción. No hay modo de saber exactamente qué se ha enviado desde el origen y qué es ruido añadido. En 1972 se publicaron los primeros resultados del tratamiento digital de la señal aplicada a audio, básicamente orientado a su almacenaje. El CD estaba viendo la luz. Convertir un sonido (una magnitud física que puede tomar cualquier valor en cualquier momento) en una serie de 0 y 1 (dos únicos valores, conocidos) permitía corregir fácilmente cualquier ruido añadido.

El descubrimiento del procesamiento digital de la señal, y sus aplicaciones en los campos del sonido y la imagen, ha sido un hito primordial en el mundo de las comunicaciones. Básicamente, ha permitido reducir drásticamente el efecto del ruido, lo que ha permitido, por una parte, incrementar la calidad de recepción del señales y, por otra, aumentar la velocidad de transmisión con los mismos medios.

Las compañías telefónicas empezaron a sustituir los enlaces internos (entre centrales) por señales digitales, pero manteniendo el bucle de abonado (línea y terminal) analógico. La digitalización de la señal de sonido se hace dentro de la central local, después del filtro de 4 kHz, y se vuelve a pasar a analógico en la central correspondiente en el otro extremo de la comunicación. Esto ha llevado a cambiar sustancialmente los procesos de conmutación: ahora se debe trabajar con bits y, por lo tanto, las centrales electromecánicas se han de sustituir por ordenadores.

Esta digitalización de la parte interna de la red de voz provocó que, de alguna manera, las dos redes, la telefónica y la de datos, confluyeran: los enlaces digitales entre centrales se utilizaban indistintamente para paquetes de datos y para transmisiones de voz.

Breve historia de las comunicaciones IV

Cuarto período, 1996-Actualidad. Multimedia, cientos de millones de usuarios

- 1996: el 98% de los navegadores eran Netscape, y se considera que la red puede acabar con el sistema operativo. Microsoft responde lanzando Explorer, lo que da inicio a la "guerra de los navegadores". Internet ya tiene más de 9.400.000 servidores. En España hay más de 100.000 ordenadores bajo el dominio .es. Salen a bolsa Yahoo! y Excite

con grandes beneficios. Estados Unidos lanza la Communications Decency Act, que será anulada en 1997. Se propone la creación de siete nuevos dominios genéricos. tv.com se vende a CNET por 15.000 dólares. Procter&Gamble, el mayor anunciante del mundo, impone el pago por clicar, que dominará la publicidad en línea (en inglés, *online*). Se incluyen contenidos multimedia: técnica de *streaming* para la transmisión fluida de vídeo.

- 1997: business.com se vende por 150.000 dólares. En 1997 ya existen 17 millones de servidores en la red. En España se crea ESPANIX para intercambiar tráfico local; a finales de año hay 500 proveedores y un millón de internautas, gracias a Infovía.

- 1998: Microsoft, con su Explorer, tiene más del 80% de los navegadores, y es demandado por abuso de posición dominante. La Red tiene 300 millones de páginas. Nace Google y AOL compra Netscape. Se registra el dominio comercial 2 millones. El Gobierno de Estados Unidos anuncia un plan para privatizar Internet que se rechaza; un segundo plan es mejor recibo.

- 1999: nace Napster, el primer programa de intercambio de ficheros (P2P). En España, Telefónica desactiva Infovía y funda Terra (que saldrá a bolsa con gran éxito), a la que dota de cifras con la compra del buscador Olé. Parte del equipo fundacional abandona para crear Ya.com. Se pagan 7,5 millones de dólares por business.com. A finales de año, el índice NASDAQ alcanza cifras desmesuradas. España tiene 300.000 ordenadores bajo el dominio .es y 2 millones de navegantes. El formato de sonido MP3 desestabiliza a las multinacionales del disco.

- 2000: el temido "Efecto 2000" apenas genera problemas. En el intermedio de la Super Bowl de fútbol americano, a mediados de enero, se anuncian 17 compañías "puntocom", que pagan 2 millones de dólares por 30 segundos de anuncio cada una. En marzo, el índice NASDAQ alcanza su pico histórico: 5.048 puntos; durante el verano se inicia una larga caída. Terra compra Lycos por 12.500 millones de dólares, y junto a Telefónica empieza a ofrecer ADSL. Los operadores de cable comienzan a dar servicio de banda ancha doméstico en España. La tienda de ropa Boo.com bate récords, con una facturación en 6 meses de 160 millones de dólares. Microsoft es condenado por abusar de su cuasi-monopolio en sistemas operativos. Se considera que la web supera los 1.000 millones de páginas.

- 2001: arranca con la presentación de un nuevo pleito de las discográficas contra Napster por favorecer la piratería. La causa concluye con el cierre de aquél en julio por orden judicial, aunque resurgirá como servicio de pago (en febrero, había batido su propio récord, con 13,6 millones de usuarios). America Online compra en enero Time Warner, el mayor grupo mediático del mundo, en lo que se considera el triunfo definitivo de los nuevos medios sobre los viejos. La empresa Kozmo, de venta por Internet con entrega rápida, se declara en bancarrota en abril. Su competidor, Webvan, sufrirá idéntica suerte. En mayo, se lanza el programa SETI@Home, el primer gran proyecto de computación distribuida (en menos de un mes proporciona más potencia de cálculo que el mayor superordenador existente entonces).

- 2002: la crisis puntocom continúa extendiéndose. Los dominios se convierten en noticia con la apertura de tres nuevos dominios de máximo nivel (.name para personas, .coop para cooperativas y .aero para empresas aeronáuticas), que no tendrán mucho éxito. En octubre, un ataque concertado consigue desconectar a 8 de los 13 ordenadores de los que depende todo el sistema de dominios, lo que acelera los planes para reforzarlo. Se produce una explosión en el uso de las bitácoras (en inglés, *weblogs* o, abreviado, *blogs*): páginas escritas por los cibernautas en las que explican anécdotas de sus propias vidas y dan a conocer sus opiniones. Lo que queda de Napster es adquirido por el conglomerado alemán Bertelsmann.

- 2003: año de la música. La patronal musical de Estados Unidos (RIAA) denuncia por primera vez a usuarios por intercambiar música en redes P2P. Apple saca su tienda iTunes de música, asociada al reproductor iPod. Después de dos años de continua caída de valor, AOL Time Warner elimina "AOL" de su nombre. WiFi se erige como alternativa de acceso sin hilo. Varias plagas barrieron Internet; desde Slammer, que se extendió en 10 minutos y provocó la caída de 8 servidores raíz, afectando a bancos y al tráfico aéreo, hasta SobigF y Blaster. Después de un cierto paro durante los años 2001 y 2002, el vigoroso ritmo de crecimiento del número de servidores en la red se recupera. Este año empieza también el ataque judicial de SCO contra Linux.

- 2004: empieza la recuperación. Sale a bolsa Google, que lanza su correo web de 1 Gb en Gmail. Guerra de buscadores: Yahoo! abandona Google y compra varias empresas; Microsoft potencia MSN Search y Amazon lanza A9. El ámbito de la música de pago también se caldea con la entrada de Wal-Mart, Sony, Virgin, eBay y Microsoft; iTunes acumula el 70% del mercado. El navegador Firefox v1.0 abre hueco en el dominio

de Explorer de Microsoft al arrancarle un 5%. En Estados Unidos la banda ancha supera a los módem y la campaña de las presidenciales demuestra el poder de las bitácoras Rathergate; el precandidato Howard Dean usa la red para la movilización y recaudación de fondos. En España, Terra vende Lycos por 105 millones de dólares. Copyleft avanza con la extensión de las licencias Creative Commons.

- 2005: existen más servidores raíz fuera de Estados Unidos que en su propio territorio. La Red tiene más de 300 millones de ordenadores principales, casi 60 millones de dominios activos, más de 4.000 millones de páginas web indexadas por Google y más de 900 millones de navegantes. Suecia tiene la penetración más alta (74% de la población), y España es la 22.ª por accesos de banda ancha (casi 2,5 millones) y la 12.ª por total de navegantes (14 millones), pero está por debajo de la media europea en penetración. Distintos accidentes y ataques revelan información privada en la red. Microsoft responde a Firefox con el lanzamiento de una versión no prevista de Explorer. Apple presenta el iPod Shuffle, basado en memoria flash. El mercado de la publicidad en línea se despierta, y varios medios españoles relanzan sus páginas web.

- 2006: Aparecen los principales exponentes de la revolución de la web 2.0: YouTube, Facebook y GoogleEarth. El fenómeno de la red interactiva y dinámica empieza a extenderse. Se empiezan a esbozar nuevas tendencias de computación distribuida. Aparece el término *cloud computing*.

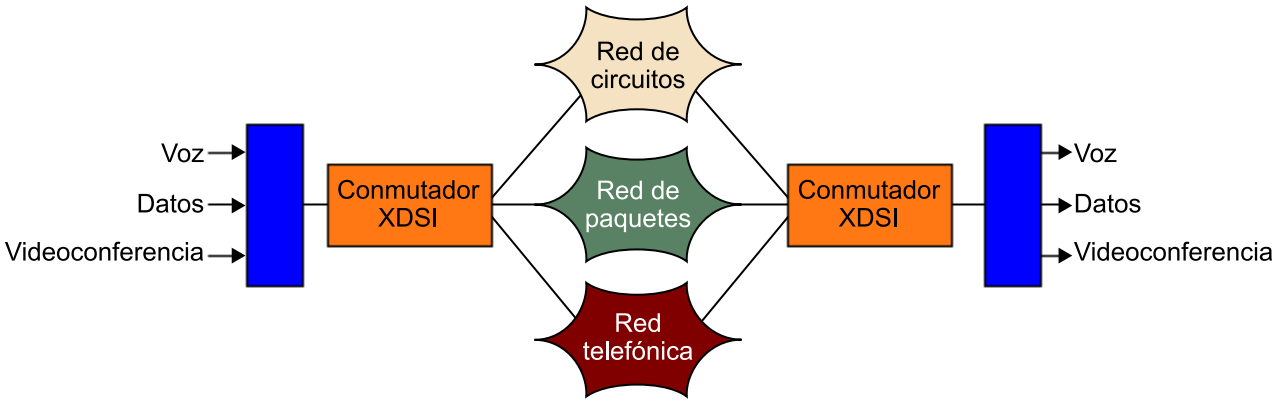
- 2007: Las plataformas de descarga de contenidos basadas en tecnologías P2P aglutinan la mayoría del tráfico de la Red. XMPP deviene el estándar *de facto* para las comunicaciones en mensajería instantánea. Gmail deja de ser beta y se convierte en accesible para todo el mundo. Writely, adquirido por Google en el año anterior, es denominado Google Docs. Nace Android como sistema operativo para dispositivos móviles.

- 2008: Auge en el acceso a Internet mediante dispositivos móviles. Amplia adopción de la tecnología 3G. Quincuagésimo aniversario del nacimiento de la Red. El gobierno chino construye un sistema de filtrado y censura la Red para controlar los contenidos que llegan a los usuarios del país asiático.

- 2009: Se esboza la Internet de las cosas. Aparece 6LowPan como iniciativa para proveer de direccionamiento IPv6 a las redes de sensores. Se extiende la oferta de servicios en la Red. Auge del *cloud computing*.

- 2010: Facebook llega a los 400 millones de usuarios. Google es boicoteado en China. Amazon EC2 y Google Application Engine se disputan el mercado del *cloud*. IBM se desmarca de la competencia por el mercado *cloud* ofreciendo soluciones basadas en escritorios remotos (eyeOS). Se empieza a hablar de redes cognitivas. Aparece el Iphone 4, que marca una nueva tendencia; Internet aparece cada vez más desvinculada del ordenador, los dispositivos móviles toman el protagonismo.

Figura 30



Una vez digitalizada la red telefónica, el paso siguiente debía ser llevar la transmisión de bits hasta las casas. Esto permitía, por una parte, ofrecer a los usuarios la transmisión de datos en su propio hogar, además de la tradicional de voz; por otra parte, permitía presentar a los abonados un abanico de nuevos servicios asociados a una comunicación enteramente digital de punta a punta. Este servicio de transmisión digital mediante la red telefónica se conoce como red digital de servicios integrados (RDSI). Ofrece dos canales independientes de 64 kbps, que permiten hablar y conectarse a Internet simultáneamente, o, con el hardware adecuado, aprovechar los dos canales juntos para navegar a 128 kbps.

RDSI

La red digital de servicios integrados (RDSI) corresponde a las siglas RDSI en castellano y ISDN (Integrated Services Digital Network) en inglés.

El uso de la red telefónica para transmitir datos tiene una limitación importante en cuanto al máximo de bits por segundo permitidos, y las redes específicas de datos son muy caras para el uso doméstico. Desde la década de los noventa, se han estudiado maneras de conseguir llevar hasta los hogares o las empresas un buen caudal de bits por segundo (banda ancha) a un precio razonable, de manera que las nuevas aplicaciones multimedia se puedan explotar al máximo. Para conseguir esta banda ancha, se han seguido dos caminos completamente diferentes. Por un lado, se han promovido cableados nuevos con fibra óptica que permitan este gran caudal, a menudo llevados a cabo por empresas con afán competidor contra los monopolios dominantes. Estas redes aprovechan para dar un servicio integral: televisión, teléfono y datos. Por otro lado, las compañías telefónicas de toda la vida han querido sacar partido del cableado que ya tienen hecho y, por eso, se han desarrollado las tecnologías ADSL, que permiten la convivencia en el bucle de abonado la señal telefónica y una señal de datos que puede llegar a los 8 Mbps (o 20 Mbps con tecnología ADSL+).

Resumen

En este módulo se han introducido los conceptos fundamentales de las redes de computadores. Hemos visto que las redes de computadores sueño una composición de sistemas hardware, software y protocolos, que permiten la comunicación entre dispositivos remotos. Hemos visto las topologías más comunes de las redes de comunicación y que éstas también se pueden clasificar por su alcance.

La arquitectura de las redes de computadores esta estructurada en diferentes niveles. Hemos visto que existe un modelo de referencia denominado OSI y que define 7 niveles de red. Los niveles más bajos se preocupan de los aspectos físicos de la comunicación, desde la caracterización del medio como la codificación de la información transmitida. Las capas superiores usan las interfaces de abstracción de sus capas subyacentes, lo que permite construir un sistema complejo y una transmisión estructurada de información entre dispositivos remotos. La división en capas y las interfaces permiten la abstracción de las funcionalidades de las capas subyacentes en las capas superiores y que las capas se puedan modificar y/o cambiar sin que eso afecte al comportamiento de la red. Los conceptos de interfaz y encabezamiento son clave para entender la estructuración en capas de una red.

Por otro lado, hemos visto que el modelo OSI es complejo y no ha sido utilizado más allá de modelo de referencia. En realidad, Internet usa un modelo TCP/IP más simple pero funcional. El módulo ha presentado a ambos modelos y les ha comparado con detalle, capa a capa. Finalmente, el módulo repasa la historia de las comunicaciones. Conocer la historia ayuda a entender el porqué de determinadas particularidades de las redes de comunicación actuales.

En los próximos módulos se profundizará en el conocimiento de cada uno de los niveles de la red. En este curso hemos adquirido un enfoque *Top-down*, es decir, desde los niveles más próximos a la aplicación hasta los niveles más específicos del hardware. Esta aproximación puede diferir de algunos otros documentos de referencia en los que las redes se presentan de manera inversa, primero conociendo los niveles físicos y finalmente presentando los niveles de aplicación. Cabe señalar que en este curso no trataremos los aspectos relacionados con la capa de aplicación, dado que éstos se introducen en otras asignaturas de la titulación. Nosotros empezaremos por el nivel de transporte.

El módulo 2 se centra en el nivel de transporte; el módulo 3 es primordial y profundiza en el nivel de red. Los módulos 4 y 5 introducen los principales conceptos de los niveles de enlace de datos y físico, que como veréis están estrechamente relacionados.

Bibliografía

Kurose, James F.; Ross, Keith W. (2005). *Computer networking: a top-down approach featuring the Internet*. Addison-Wesley.

Tanenbaum, Andrew S. (2003). *Redes de computadores* (4.ª ed.). Pearson.