

# Conceptos de redes de computadores

Xavier Vilajosana Guillén

PID\_00147725



Universitat Oberta  
de Catalunya

[www.uoc.edu](http://www.uoc.edu)



# Índice

<b>Introducción</b> .....	5
<b>Objetivos</b> .....	6
<b>1. Conceptos de redes y comunicaciones en Internet</b> .....	7
<b>2. Qué es Internet y qué es un protocolo</b> .....	8
<b>3. Hardware de red</b> .....	9
3.1. Topologías de red .....	9
3.2. Tipo de conmutación .....	10
3.2.1. Conmutación de circuitos .....	10
3.2.2. Conmutación de paquetes .....	11
3.2.3. Conmutación de paquetes con circuito virtual .....	14
3.3. Alcance de las redes .....	15
3.3.1. Redes de gran alcance .....	16
3.3.2. Redes de área local .....	16
3.4. Tecnologías de red .....	16
3.4.1. Tecnologías de red cableada .....	17
3.4.2. Tecnologías de red sin hilos .....	17
<b>4. Dispositivos de red</b> .....	19
<b>5. Software de red</b> .....	21
5.1. Arquitectura de la red: diseño por capas .....	22
5.2. Consideraciones de diseño .....	25
<b>6. Jerarquía de protocolos y cabecera</b> .....	27
<b>7. Interfaces y servicios</b> .....	29
7.1. Tipo de conexión de servicios .....	33
<b>8. Modelos de referencia</b> .....	35
8.1. Necesidad de estandarización .....	35
8.2. El modelo de referencia OSI .....	36
8.2.1. Proceso de encapsulación y desencapsulación .....	38
8.3. Modelo TCP/IP .....	39
8.3.1. Encapsulación de la información en el modelo TCP/IP .....	41
8.4. Modelo OSI comparado con modelo TCP/IP .....	42

<b>9. Breve historia de las comunicaciones.....</b>	<b>44</b>
<b>Resumen.....</b>	<b>56</b>
<b>Bibliografía.....</b>	<b>59</b>

## Introducción

Las redes de ordenadores actuales son una composición de dispositivos, técnicas y sistemas de comunicación que han ido apareciendo desde el final del siglo XIX con la invención del teléfono. Éste se desarrolló exclusivamente para transmitir voz, aunque todavía hoy 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 por satélite, 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, abordaremos 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. Seguidamente, el módulo introduce las diferentes tecnologías de red más relevantes en la actualidad, Ethernet u 802.3 es la más usada en redes de área local cableadas. Las tecnologías de redes sin hilos se han estandarizado en la última década y tienen su mayor exponente en el 802.11 o WiFi, que también es usado por la mayoría de dispositivos de usuario en red.

El módulo profundiza en la definición de una red de computadores 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 a su nivel predecesor mientras que usa los servicios de su nivel antecesor. Cuando se quiere transmitir una información, ésta se transmite entre los diferentes niveles de la red a la vez que se encapsula la información de los niveles precedentes y se añade nueva información que le permite al receptor recuperar la información original.

Veremos que en un principio se definió una jerarquía llamada Open Systems Interconnection (OSI) con siete niveles y que ésta evolucionó hacia el modelo de red actual, el modelo TCP/IP que rige hoy en día el funcionamiento de Internet. Finalmente, el módulo hace un breve repaso de 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.

## Objetivos

Al finalizar el estudio de este módulo, tendréis que haber alcanzado los objetivos siguientes:

- 1.** Conocer el concepto de red de computadores, servicio y protocolo e Internet.
- 2.** Conocer los componentes de una red de computadores, tanto los de hardware como los de software.
- 3.** Conocer la arquitectura de una red de computadores, la separación por capas o niveles y los modelos de referencia fundamentales.
- 4.** Saber diferenciar las redes por su alcance.
- 5.** Tener una visión general de la evolución de las redes de computadores desde sus inicios.

## 1. Conceptos de redes y comunicaciones en Internet

Durante las dos primeras décadas de existencia de los computadores, éstos eran sistemas hardware fuertemente centralizados, normalmente ubicados en un único espacio físico. Las empresas y centros que poseían un computador hacían que éste cubriera todas las necesidades computacionales de la institución. A medida que las capacidades de los computadores crecieron, la centralización se convirtió en un problema tanto de gestión como de recursos. De esta manera, se fue sustituyendo el modelo centralizado por un modelo en el que múltiples computadores con menos capacidad pero interconectados entre sí eran capaces de realizar las tareas de un computador centralizado. A esta nueva organización se la denominó **red de computadores**. El diseño y arquitectura de la red son los aspectos que trataremos durante este curso.

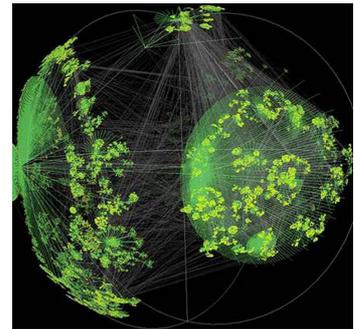
La evolución de las tecnologías ha llevado a un crecimiento progresivo del uso de los sistemas en red hasta llegar al modelo de hoy en día, en el que no se puede concebir un sistema informático sin la presencia de los elementos de comunicación. Internet ha sido la materialización de la red de computadores y se ha convertido en el eje principal de las tecnologías de la información. La comunicación en Internet no deja de ser una jerarquización de la comunicación en red. Internet es una gran red constituida por una infinidad de pequeñas redes interconectadas entre sí.

## 2. Qué es Internet y qué es un protocolo

La idea de Internet apareció a mediados de los años sesenta cuando la Agencia de Proyectos de Investigación Avanzada (ARPA, por sus siglas en inglés), en el seno del Departamento de Defensa de Estados Unidos financió un proyecto denominado ARPANET que pretendía interconectar diferentes ordenadores distribuidos en sus sedes.

Desde entonces, Internet ha evolucionado hasta el sistema de hoy en día, en el que millones de máquinas están interconectadas y acceden a contenidos distribuidos por todas partes. La estructura de la red es compleja y no podemos pensar en una conexión de todos con todos, pues ello haría que el sistema fuera completamente inoperante e inviable tecnológicamente. Internet sigue una estructura jerárquica en la que unos pocos nodos están conectados con muchos otros, mientras que la mayoría mantiene una conexión con su proveedor de servicio.

Para hacer posible toda la complejidad de Internet y permitir que la infinidad de aplicaciones de hoy en día se puedan comunicar mediante la red hace falta un conjunto de reglas que rijan las comunicaciones y regulen cómo y cuándo los nodos de la red se pueden comunicar. Las reglas y convenciones que permiten que eso sea posible se llaman **protocolos**.



Conectividad en Internet

### 3. Hardware de red

Las redes de computadores se pueden clasificar de diferentes formas. Generalmente, estas clasificaciones se hacen basándose en la topología, el tipo de conmutación, el alcance y la tecnología de la red, entre otros. Este apartado detalla estas diferentes clasificaciones que proporcionan la base necesaria para poder entender posteriormente el diseño de los protocolos existentes en la actualidad.

#### 3.1. Topologías de red

Una topología de red es la manera como están distribuidos los nodos que la forman.

Las redes actuales están formadas por tres tipos de entidades: los equipos finales (*hosts*), los equipos intermedios (conmutadores o routers) y los enlaces (*links*) que unen los equipos finales y los routers entre sí.

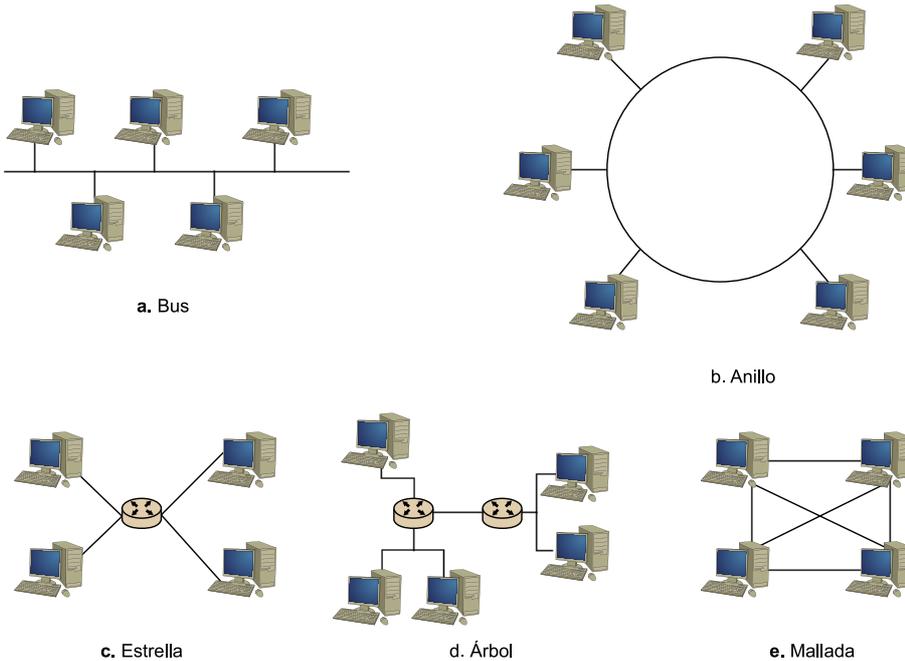
Las topologías más conocidas son las de:

- **Bus.** Todos los equipos están conectados a un único medio de transmisión compartido por todas las estaciones de la red, por lo que resulta necesario establecer un sistema de acceso al medio con el fin de evitar que haya más de una estación transmitiendo en el mismo instante de tiempo y se produzcan colisiones. Un ejemplo de una topología en bus se puede ver en la figura siguiente.
- **Anillo.** Como muestra la figura, una topología en anillo está formada por un enlace que forma un bucle, de manera que cada estación está conectada al anillo a través de dos enlaces, el de entrada y el de salida. Generalmente, cuando la estación emisora recibe su propio paquete lo elimina de la red.
- **Estrella.** Esta topología está formada por un nodo central, que actúa como nodo intermedio de la red (conmutador o router) y es el que gestiona el envío y la recepción de los datos; el resto de las estaciones se conectan a este nodo principal.
- **Árbol.** La topología en árbol se considera una topología mixta de las topologías en bus y en estrella, y a veces también se la conoce como topología jerárquica. Un ejemplo se puede ver en la figura, donde diversos nodos

intermedios se conectan entre sí y, a su vez, tienen conectados equipos finales. Esta topología es la más utilizada actualmente.

- **En malla.** La topología en malla es aquella en la que todos los equipos están conectados contra todo el resto. Hay casos de redes en malla no totales, en las que las estaciones no forman una malla completa. Generalmente, esta topología es la utilizada en el núcleo de las grandes redes como Internet, donde sólo se conectan equipos intermedios, y no equipos finales.

Ejemplos típicos de topologías de red



### 3.2. Tipo de conmutación

En el entorno 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 los puntos. Esencialmente, esta conmutación se puede dividir en dos clases diferentes: la conmutación de circuitos y la conmutación de paquetes.

#### 3.2.1. Conmutación de circuitos

La conmutación de circuitos se basa en establecer un circuito físico entre los dos interlocutores de la red. Dicho circuito físico se establece antes de que se pueda transmitir ningún tipo de información y está conformado por diferentes enlaces entre los nodos. 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 hacia el destino; así la estación origen solicita la creación del circuito al nodo al que está conectada, el cual envía la

petición al nodo siguiente. Este otro nodo hará lo mismo hacia el siguiente, y así hasta llegar al destino final. A medida que se va formando el circuito, cada nodo intermedio verifica que haya bastantes recursos para establecerlo, y, en el caso de que no sea así, se aborta la petición de circuito. Por el contrario, en el caso de que el establecimiento sea viable, una vez llegado al destino, éste enviará una señal al origen para hacerle saber que ya puede enviar información.

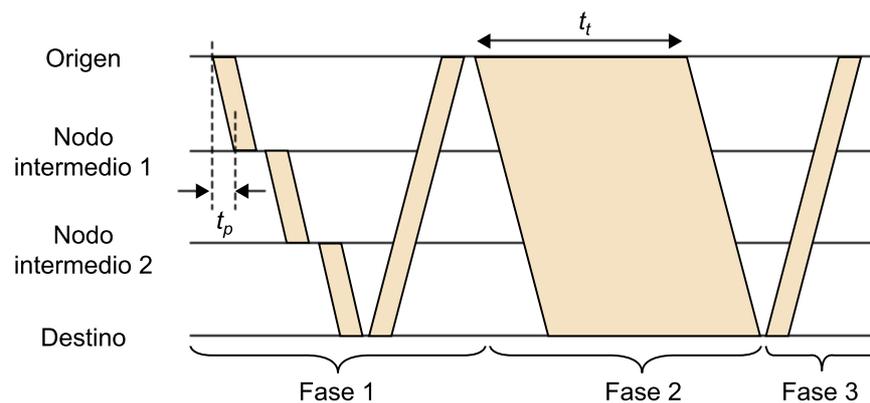
2) **Transferencia de datos.** Ahora, las estaciones ya pueden intercambiar la información deseada.

3) **Desconexión.** Una vez se ha acabado la comunicación es obligatorio liberar recursos, a fin de que estén disponibles más adelante para otras conexiones.

### Ejemplo de creación de circuitos

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

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 grosor 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 eso, antes de enviarla se tiene que esperar a tener toda la información del circuito. Que una vez establecida, ya puede funcionar de extremo a extremo de forma transparente y sin más retardos adicionales de los nodos intermedios.

### Red telefónica básica

El ejemplo más clásico de la conmutación de circuitos es la antigua red telefónica básica (XTB), en la que, por medio de las centralitas situadas de forma jerárquica por medio de toda la red, se iban multiplexando los circuitos de voz y dirigiéndolos hacia su destinatario. Hoy día, con la era digital, este establecimiento del circuito se produce sólo desde el teléfono del usuario hacia la centralita más próxima, donde se digitaliza la voz y se utilizan otras técnicas como, por ejemplo, la conmutación de paquetes, para enviar la información.

### 3.2.2. Conmutación de paquetes

Uno de los principales problemas que encontramos con la conmutación de circuitos es la exclusividad de los recursos, ya que cuando hay un circuito creado, aunque no haya datos pasando por el circuito, los recursos están reserva-

dos y no pueden ser utilizados por ninguna otra estación. El problema se ve agravado ya que, para conexiones de datos como las que hay hoy día, el tráfico, en vez de ser constante, llega en ráfagas; por ejemplo, cuando el usuario carga una página web, la carga sólo supone unos pocos centenares de milisegundos, mientras que su lectura puede comportar unos cuantos minutos. Otro problema impuesto por la conmutación de circuitos es la necesidad de que todos los nodos de la comunicación trabajen a la misma velocidad, ya que los nodos intermedios no realizan ningún procesamiento de la información, cosa que en una red actual no es cierta; cada usuario tiene una velocidad diferente, que es a la vez diferente de la que utilizan los operadores.

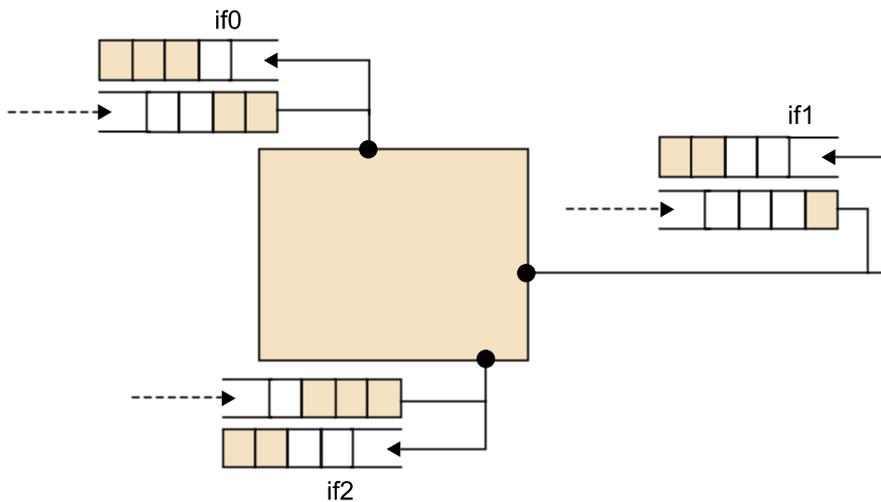
Así, con el fin de mejorar la conmutación de circuitos de cara a estas nuevas necesidades se diseñó la conmutación de paquetes con los siguientes objetivos:

- Optimización de la utilización de los canales de comunicación.
- Interconexión de terminales con diferentes velocidades.
- Creación de conexiones de forma simultánea sin reserva de recursos.

Así, la conmutación de paquetes, en vez de reservar recursos en un circuito, dota a los nodos intermedios de capacidad de proceso y de un sistema de colas que permite almacenar temporalmente un paquete, mirar cuál es su destinatario y enviarlo hacia el nodo que corresponda.

Como se ha dicho, la conmutación de paquetes tiene que permitir diferentes velocidades de transmisión; por eso se utilizan las colas de recepción y las colas de transmisión, tal como muestra la siguiente figura. Según se puede comprobar, un nodo de conmutación está compuesto por interfaces; estas interfaces están compuestas, entre otras cosas, por una cola de entrada y otra cola de salida al sistema, y se utilizan con el fin de controlar el acceso al nodo de conmutación, que, ahora, en vez de ser pasivo, procesará todos los paquetes que llegan por las colas de entrada y los colocará en la cola de salida de la interfaz correspondiente para ser enviados.

## Colas en la conmutación de paquetes

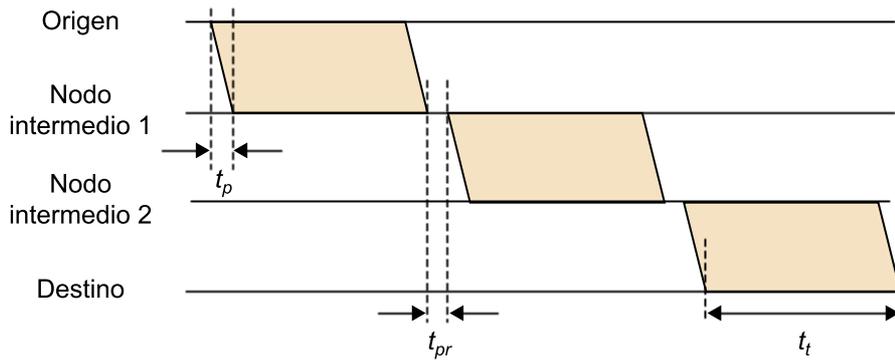


Las colas del nodo de conmutación tendrán un tamaño determinado, lo que implica que si una cola se llena antes de ser procesada, hay paquetes que tendrán que ser descartados. En módulos posteriores veremos cómo la red gestiona y evita estas pérdidas.

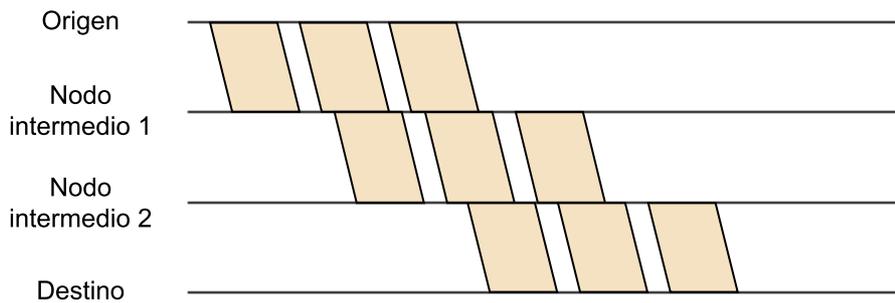
Otro importante factor a considerar en este entorno es el tamaño del paquete a transmitir; inicialmente se pensó en hacer los paquetes tan grandes como el mensaje a enviar (conmutación de mensajes), pero enseguida se vio que, para mensajes grandes, los nodos intermedios necesitaban demasiada memoria –ya que almacenan el paquete en su totalidad antes de enviarlo–, y demasiado tiempo para procesarlo. Así, lo que se hace actualmente es dividir los mensajes en fragmentos de un tamaño máximo fijado (generalmente 1.500 octetos).

Un ejemplo de eso se puede encontrar en la figura siguiente; 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 un tamaño inferior. A causa del almacenamiento en los nodos intermedios (denominado *store and forward*) la conmutación de paquetes es generalmente más rápida.

Funcionamiento de la conmutación de paquetes y de mensajes



a. Conmutación de mensajes



b. Conmutación de paquetes

$t_p$ : tiempo de propagación $t_{pr}$ : tiempo de proceso $t_t$ : tiempo de transmisión
--

### 3.2.3. 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, dependiendo del tamaño y el estado de las colas de los nodos intermedios, el retardo en la llegada de la información es variable. Ello implica que en comunicaciones críticas en tiempo (como una conversación de voz) se pueda llegar a crear un problema; por ejemplo, si un paquete de voz llega demasiado tarde, no podrá ser decodificado y el otro interlocutor notará un pequeño corte en la conversación.

Para minimizar este problema aparecieron lo que se conoce como conmutación de paquetes con circuito virtual, que tiene por objetivo reunir las ventajas de los dos paradigmas. Así, en vez de enviar de forma independiente todos los paquetes de una conexión, lo que hacen los circuitos virtuales es decidir el camino previamente (como con conmutación de circuitos), pero manteniendo el envío de paquetes individuales, de manera que ahora todos los paquetes seguirán el mismo camino, por lo que podemos tener una reserva de recursos.

### 3.3. Alcance de las redes

Una clasificación bastante clásica de las redes es la que se hace en función de su alcance, aunque, dependiendo del entorno, esta clasificación puede cambiar. Generalmente se consideran dos categorías: las redes de gran alcance<sup>1</sup> y las redes de alcance local<sup>2</sup>.

Antes de detallar qué son las LAN y las WAN es conveniente introducir en primer lugar los conceptos de redes de difusión y redes punto-a-punto.

Una red de difusión (o *broadcast*) es aquella en la que el medio es compartido por todas las estaciones que forman la red; así, todos los equipos reciben todos los paquetes, pero sólo procesan los dirigidos hacia ellos.

Entre otras cosas, una red de difusión comporta serios problemas de privacidad; por eso, en este tipo de redes es recomendable utilizar mecanismos de cifrado en las conexiones, como, por ejemplo, en las redes sin hilos.

Las redes punto-a-punto, en contraposición a las redes de difusión, son aquellas en las que las conexiones son dedicadas entre dos puntos determinados de la red.

A pesar de que un enlace punto-a-punto puede parecer poco flexible, en la realidad es el tipo de conexión más utilizado actualmente, ya que se puede desplegar para formar topologías en estrella, en árbol o en malla de forma muy sencilla. Dependiendo del sentido de la comunicación que permiten, los enlaces punto-a-punto pueden ser:

- **Simplex.** La comunicación es unidireccional, uno de los dos puntos es siempre el origen, y el otro, el destino.
- **Semidúplex (Half-duplex).** La comunicación puede ser bidireccional, pero siempre y cuando los dos puntos de la comunicación alternen la generación de tráfico, ya que si enviaran al mismo tiempo se provocaría una colisión que invalidaría ambas transmisiones.
- **Dúplex (Full-duplex).** El caso más común actualmente es cuando el medio está preparado para poder enviar y recibir información de forma simultánea sin ningún problema.

Hay que señalar que con las comunicaciones bidireccionales la velocidad puede ser igual (conexión simétrica) o diferente dependiendo del sentido de la comunicación (conexión asimétrica).

<sup>(1)</sup>En inglés, Wide Area Networks (WAN).

<sup>(2)</sup>En inglés, Local Area Networks (LAN).

#### Otras categorías de redes

Hay otras categorías de redes, como las redes metropolitanas (Metropolitan Area Network, MAN) o las redes personales (Personal Area Network, PAN), aunque normalmente se las puede incluir dentro de las redes LAN.

### 3.3.1. Redes de gran alcance

Redes de gran alcance<sup>3</sup> se consideran aquellas que se utilizan en espacios geográficos extensos. Generalmente, las WAN se encargan de la interconexión de las LAN, facilitando así la conexión de los usuarios de diferentes localizaciones. La transmisión de datos se suele hacer mediante grandes operadoras de comunicaciones con líneas de comunicación contratadas (*leased lines*), utilizando infraestructuras que se consideran públicas (para evitar monopolios).

<sup>(3)</sup>En inglés, Wide Area Networks (WAN).

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 topologías en árbol que están conectadas con topologías en malla, formadas por miles de nodos.

### 3.3.2. Redes de área local

Por el contrario, en las WAN, las redes de alcance local<sup>4</sup> están diseñadas para tener un alcance más reducido, que puede oscilar entre unos pocos kilómetros y algunos metros (incluso centímetros). Las tecnologías LAN están pensadas para conectar usuarios con pocos equipos, edificios empresariales o incluso campus enteros. Normalmente, estas LAN se acaban conectando en WAN; actualmente, esta interconexión masiva de LAN y WAN a escala global se conoce como Internet.

<sup>(4)</sup>En inglés, Local Area Networks (LAN).

Clásicamente, las LAN han utilizado un medio de difusión para enviar la información, pero desde la aparición de los conmutadores y otros equipamientos más actuales han pasado, mediante topologías en árbol y en 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, las redes sin hilos, que utilizan difusión para enviar la información.

#### Redes sin hilos

Hay muchos tipos de redes sin hilos, y no todos pueden ser clasificados como LAN, por ejemplo, el de las redes de telefonía móvil.

### 3.4. Tecnologías de red

La última clasificación del hardware de red hace referencia a las diferentes tecnologías existentes para hacer una red, la lista de tecnologías de red existentes en la actualidad es demasiado extensa para poder listarla; aquí se introducen las tecnologías más importantes en la actualidad, cuya lista comprende las tecnologías cableadas y las tecnologías sin hilos.

### 3.4.1. Tecnologías de red cableada

Dentro de las redes cableadas, la familia de tecnologías por excelencia es Ethernet (definido en el estándar IEEE 802.3)<sup>5</sup>, que empezó como una tecnología a 10 Mbps con una topología en bus y medio compartido, y que ha ido evolucionando a una topología en estrella a 1 Gbps (Gigabit Ethernet) pasando por Fast Ethernet, todavía muy utilizado en la actualidad a 100 Mbps.

A pesar de empezar siendo una tecnología limitada a LAN, Ethernet ha evolucionado tanto, gracias a su bajo coste y a su gran aceptación, que actualmente hay enlaces WAN construidos con esta tecnología.

Por lo que respecta a las topologías basadas en anillo, como Token Ring (IEEE 802.5) y FDDI (definido en el estándar ANSI X3T12), han ido cayendo en desuso, en relación con Ethernet, principalmente a causa de su coste más alto y peor rendimiento. Actualmente, una topología en anillo muy utilizada es Resilient Packet Ring (IEEE 802.17), una tecnología para transportar otras tecnologías a través de anillos de fibra óptica; normalmente se transporta directamente tráfico Ethernet y servicios IP.

### 3.4.2. Tecnologías de red sin hilos

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

Entre los muchos tipos de redes de telefonía móvil que hay se puede mencionar el del Global System for Mobile Communications (GSM), que fue de los primeros sistemas que apareció y permite el envío de datos a 9,6 Kbps, para evolucionar al más actual General Packet Radio Service (GPRS), con un ancho de banda máximo teórico de 171,2 Kbps, pero cuyo canal de bajada es efectivamente de 64 Kbps y el de subida de 14 Kbps. La última implementación en tecnologías de red móviles es la Universal Mobile Telecommunication Services (UMTS), también conocida como el sistema de tercera generación (3G), que, con unos sistemas más avanzados, es capaz de llegar a velocidades teóricas de 21 Mbps, pero con velocidades efectivas de 7,2 Mbps de bajada y 384 Kbps de subida.

Con respecto a las redes sin hilos de más corto alcance, la tecnología por excelencia usada es la Wireless LAN (WiFi - IEEE 802.11), que inicialmente fue definida con una velocidad de 11 Mbps, pero que con posteriores revisiones del estándar se ha diseñado para soportar velocidades de 54 Mbps, con un alcance aproximado de 100 metros. En los últimos años, con el fin de reducir el consumo energético de las comunicaciones sin hilos con equipos de baja potencia, ha aparecido el estándar de facto para la comunicación de equipos

<sup>(5)</sup>IEEE es la abreviatura del Institute of Electronic and Electrical Engineers.

#### 10 Gigabit Ethernet

También existen modelos de 10 Gigabit Ethernet, pero su implantación todavía está en sus inicios.

pequeños (móviles, PDA...), que es Bluetooth, con una velocidad de 1 Mbps y un alcance aproximado de 10 metros, pero con un consumo energético muy bajo que lo hace muy atractivo para transferencias de datos cortas.

Finalmente, una tecnología que se queda entre el corto y el largo alcance es WiMAX (IEEE 802.16), una tecnología sin hilos muy utilizada en la actualidad para dar conectividad a zonas aisladas y de difícil acceso, donde la comunicación cableada es muy cara. WiMAX tiene una velocidad máxima aproximada de 150 Mbps de bajada y 35 Mbps de subida, con un alcance de unos 70 kilómetros.

## 4. Dispositivos de red

Las redes de hoy en día funcionan porque hay una serie de dispositivos que son capaces de gestionar tanto la información de control y presencia de los nodos de una red como la información que dichos nodos se transmiten. Básicamente, los dispositivos de red son los siguientes:

- **Encaminador o enrutador<sup>6</sup>**. Es un dispositivo de red de nivel 3 del modelo OSI<sup>7</sup>. Recoge la información del nivel de red (dirección IP) para tomar las decisiones de encaminamiento: escoger el camino o ruta más adecuada por donde reenviar los datos recibidos. La sucesión de decisiones de diferentes routers posibilita la llegada de la información desde su origen hasta el sistema informático de destino.
- **Concentrador<sup>8</sup>**. Es un dispositivo de red que permite agrupar un conjunto de dispositivos Ethernet en un mismo segmento de red. Actúa en el primer nivel del modelo OSI o nivel físico, sin entrar por lo tanto a analizar las direcciones MAC de destino. Por ello, todo lo que llega es reenviado indiscriminadamente a todos los ordenadores conectados.
- **Conmutador<sup>9</sup>**. Es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (*bridges*), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes que se fusionan en una sola. Igual que los puentes, ya que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LAN.
- **Puente de red<sup>10</sup>**. Es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Éste interconecta dos segmentos de red (o divide una red en segmentos) permitiendo el paso de datos de una red a otra mediante el uso de la dirección física de destino de cada paquete. Un *bridge* conecta dos segmentos de red como una sola red utilizando el mismo protocolo de establecimiento de red.
- **Tarjeta de interfaz de red**. Físicamente es una tarjeta de expansión insertada dentro del ordenador con una o más aberturas externas por donde se conecta el cable de red. En el plano conceptual, la tarjeta de red<sup>11</sup>, también llamada adaptador de red, permite la comunicación entre los diferentes dispositivos conectados entre sí y, asimismo, la distribución de recursos entre dos o más equipos. Hay diversos tipos de adaptadores en función del

<sup>(6)</sup>En inglés, *router*.

<sup>(7)</sup>OSI es la abreviatura de Open Systems Interconnection (interconexión de sistemas abiertos).



Router

<sup>(8)</sup>En inglés, *hub*.



Concentrador

<sup>(9)</sup>En inglés, *switch*.



Conmutador

<sup>(10)</sup>En inglés, *bridge*.



Puente de red

tipo de cableado o arquitectura que se utilice en la red (coaxial fino, coaxial grueso, Token Ring, etc.), pero el más común actualmente es el Ethernet, que utiliza una interfaz o conector RJ-45. Cada tarjeta de red tiene un número de identificación único de 48 bits en hexadecimal, denominado dirección MAC. Estas direcciones de hardware son únicas y están administradas por el Institute of Electronic and Electrical Engineers (IEEE).

<sup>(11)</sup> En inglés, *network interface card* (NIC).



Tarjeta de red

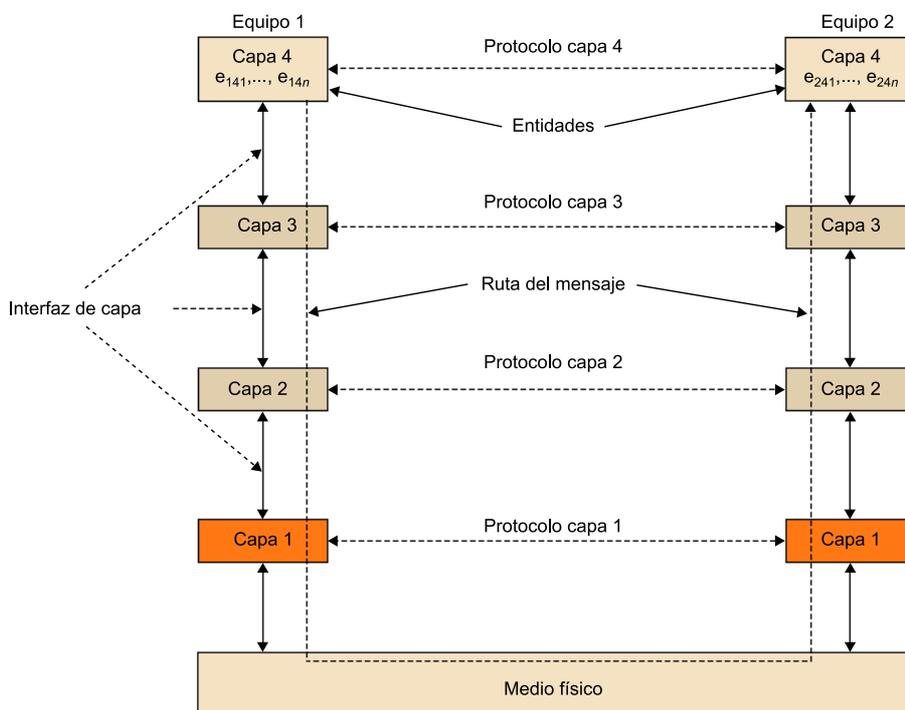
## 5. Software de red

Cuando aparecieron las redes de computadores, los fabricantes hacían el diseño pensando que todo el proceso de red se haría mediante hardware, y, además, asumían que los protocolos y los mecanismos a utilizar serían propietarios, sin un sistema estándar, y sin que hubiera un acuerdo conjunto entre los fabricantes para interactuar.

De todas formas, a medida que fueron evolucionando las redes, se vio que si no se planteaba algún tipo de estandarización, una vía común con el fin de interconectar tecnologías y utilizar mecanismos regulados, los esfuerzos de cada fabricante serían demasiados grandes y la lucha no beneficiaría a nadie. Fue entonces cuando algunos fabricantes, como IBM, empezaron a ver 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. Por eso apareció lo que se conoce como las arquitecturas de red organizadas por capas, cuyos ejemplos más importantes son OSI y TCP/IP<sup>12</sup>.

<sup>(12)</sup>TCP/IP es la abreviatura de Transmission Control Protocol/Internet Protocol.

Ejemplo de arquitectura de red con cuatro capas



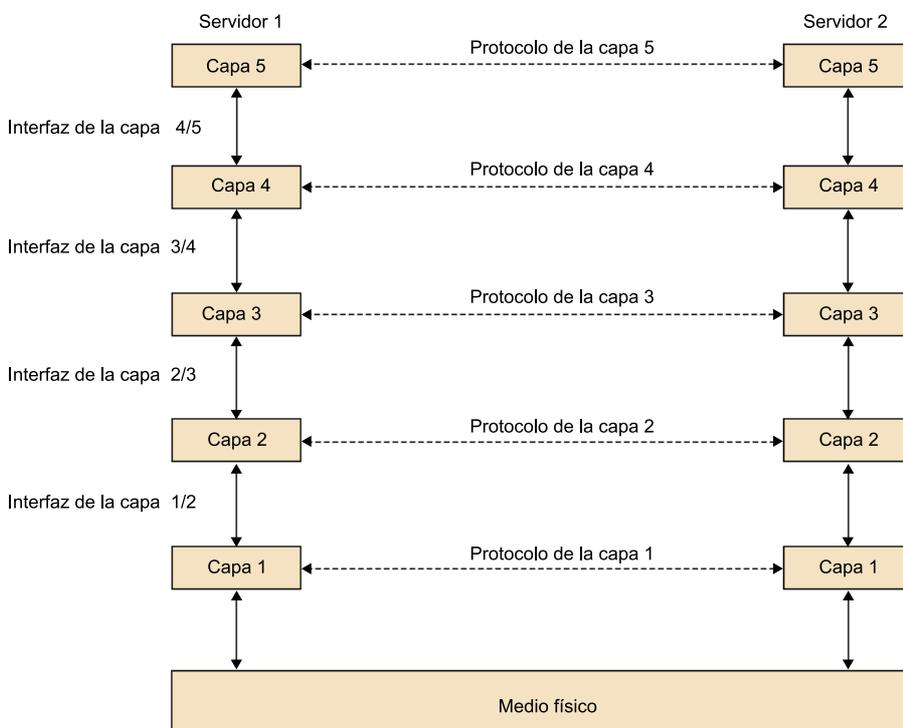
## 5.1. Arquitectura de la red: diseño por capas

Históricamente, las primeras redes se diseñaron teniendo sólo en cuenta el hardware de las comunicaciones. Esta estrategia no tuvo mucho futuro y las redes evolucionaron hacia una combinación de software de red muy estructurado y hardware genérico.

Para reducir la complejidad del diseño, las redes están organizadas en una serie de capas, situadas unas encima de otras. El número de capas, el nombre de cada una de ellas, su contenido y sus funciones difieren de un tipo de red a otro. En todas las redes, el objetivo de cada capa es ofrecer determinados servicios a las capas superiores, ocultándoles a éstas los detalles de cómo están implementados los servicios que se ofrecen.

La capa de nivel  $N$  de un ordenador mantiene comunicación con la capa de nivel  $N$  de otro ordenador. Las reglas y convenciones usadas en la capa de nivel  $N$  se denominan protocolos. Básicamente, un protocolo es un acuerdo entre las partes de la comunicación sobre cómo se realiza ésta.

En la siguiente figura se muestra una pila de protocolos: las entidades que utilizan las correspondientes capas en los diferentes ordenadores se llaman pares (*peers*). En otras palabras, los pares se comunican usando un protocolo.



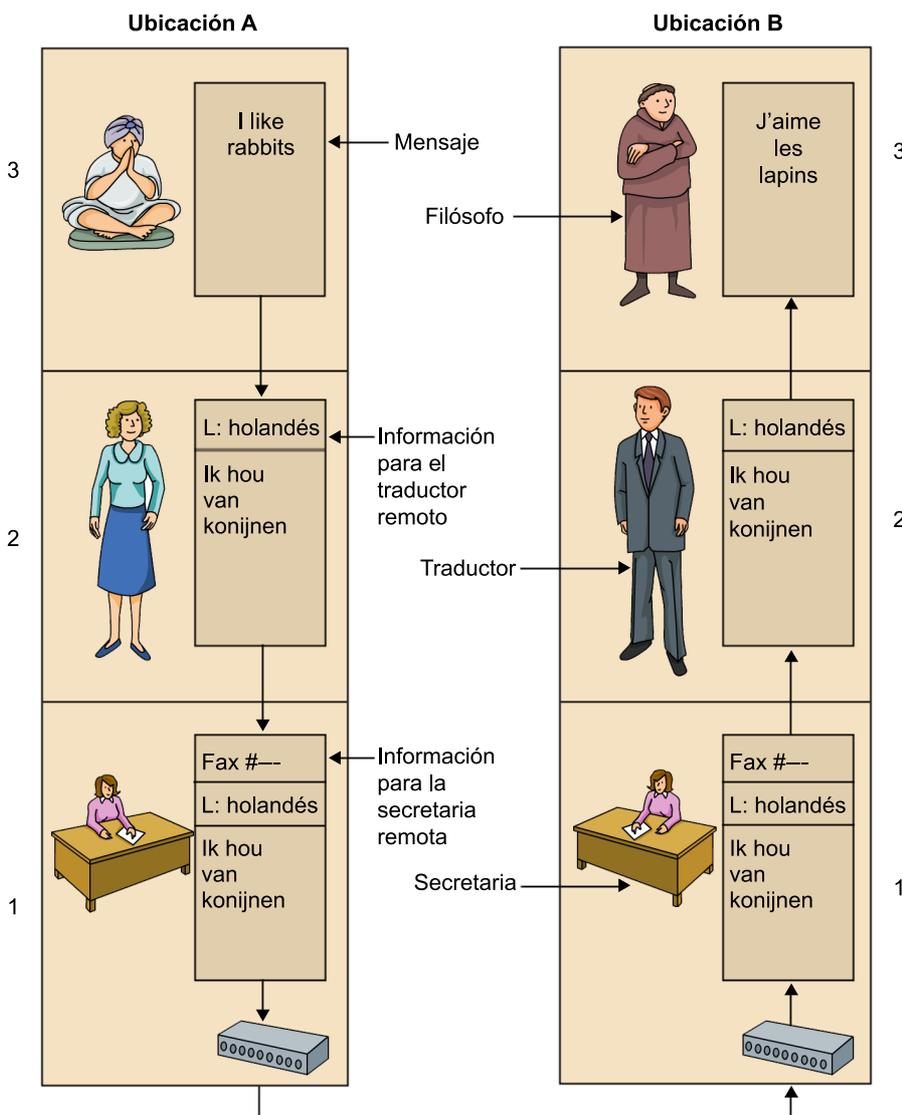
En la realidad, la información no se transfiere directamente de una capa  $N$  de una máquina a la capa  $N$  de otra máquina. Cada capa pasa la información y el control de ésta a la capa inmediatamente inferior, y así sucesivamente hasta llegar a la última capa. Esta última capa se denomina capa física, y es en ella

donde se produce la comunicación real. En la figura anterior, 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 a la capa superior. Cada capa ofrece una colección de funciones perfectamente definidas. Por ello, es muy sencillo reemplazar la implementación de una capa por otra capa con diferente implementación (si queremos cambiar el medio de transmisión de la información, sólo hay que cambiar la capa de nivel 1, por ejemplo, las líneas telefónicas por canales por satélite, manteniendo el resto intacto).

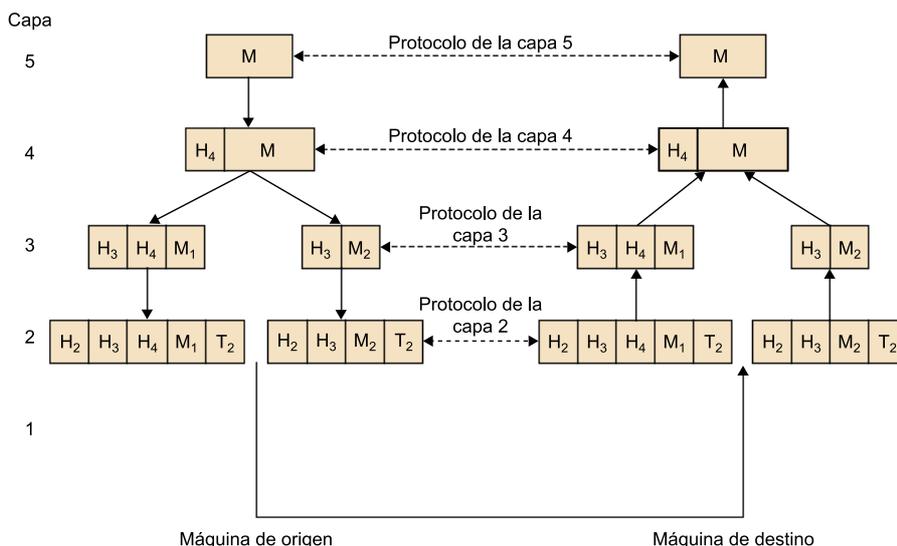
El conjunto de capas y protocolos se denomina arquitectura de la red. La lista de protocolos, un protocolo por capa, se llama la pila de protocolos.

Para explicar las comunicaciones multicapa, observemos la siguiente figura.



Imaginemos que tenemos dos filósofos (procesos pares (*peer*), capa 3). Un filósofo habla urdu e inglés, y el otro, chino y francés. Como 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 pues, pasa el mensaje en inglés a través de la interfaz 2/3 a su traductor, que traduce el mensaje en una lengua neutral (neerlandés). 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 ésta 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 pasarlo finalmente al filósofo remoto. Hay que tener en cuenta que cada protocolo es independiente de los otros en la pila de protocolos, y que podemos cambiar un protocolo por otro mientras las interfaces no cambien. Por ejemplo, la secretaria podría optar por transmitir los mensajes por fax o enviarlos por correo postal, teléfono o correo electrónico, sólo cambiando la capa 1 sin cambiar la interfaz 2/1.

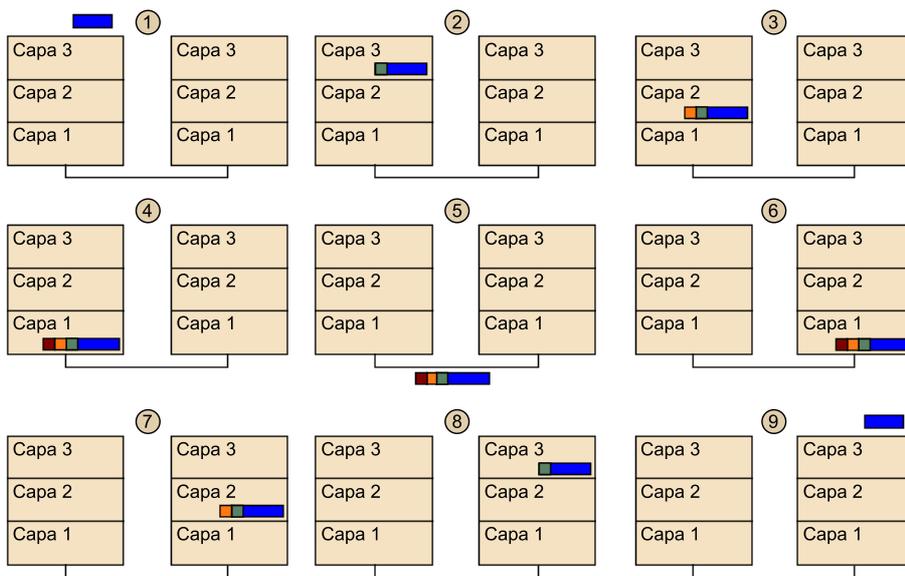
Observemos la siguiente figura. Consideremos que se produce la comunicación de la capa superior. Un mensaje *M* es producido por un programa (o proceso) que funciona en la capa de nivel 5. La capa 5 envía el mensaje *M* a la capa 4. La capa 4 pone la cabecera antes del mensaje para identificar el mensaje y le pasa el resultado a la capa 3. La cabecera incluye el control de la información, como los contadores de control de secuencia, para permitir que la capa 4 de la máquina 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, tiempos y otros campos de control.



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. Consecuentemente, la capa 3 tiene que partir 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,  $M$  queda dividido en dos partes,  $M_1$  y  $M_2$ .

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



## 5.2. Consideraciones de diseño

El nivel por capas se da una forma estructurada de diseñar y abstraer las tareas necesarias con el fin de enviar información a través de la red, pero cuando se diseña una arquitectura de red hay muchos más factores, aparte de las capas, que se tienen que considerar. Los siguientes son los más relevantes:

- 1) **Identificación:** cada nodo de la red se tiene que poder identificar de forma única con el fin de identificar a sus interlocutores.
- 2) **Encaminamiento:** los nodos de la red han de 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 llegue al otro nodo, lo haga sin errores. Hay que señalar que los medios de transmisión no siempre son fiables, por lo que se tiene que decidir cuál o cuáles capas verificarán 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 *full duplex*, *half duplex* o *simplex*. Y, caso de que sea necesario, si habrá algún tipo de priorización en el envío.

5) **Control de congestión:** dado que las velocidades de transmisión de una red no siempre son homogéneas y que a veces habrá enlaces con más carga que otros, cualquier protocolo tiene que considerar la posibilidad de que se tenga que disminuir la velocidad a la que se envían los datos, o bien, en el caso de que algún paquete no llegue al destino, de que se tenga que reenviar de forma transparente al usuario.

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

## 6. Jerarquía de protocolos y cabecera

Cada capa necesita un mecanismo para identificar al emisor y el receptor. Una red tiene diversos nodos y en cada uno de ellos se ejecutan múltiples procesos. Cada proceso tiene que saber con quién se quiere comunicar, teniendo en cuenta que los destinos pueden ser diversos. De esta manera se hace necesaria una forma de direccionamiento que nos permita determinar un destino específico.

Otra característica del diseño de un protocolo es si los datos sólo viajan en un solo sentido (comunicación *simplex*) o lo hacen en las dos direcciones, pero no simultáneamente (comunicación *half duplex*), o viajan en las dos direcciones simultáneamente (comunicación *full duplex*). El protocolo tiene que determinar cuántos canales lógicos tiene que gestionar, y las prioridades de estos canales. Muchas redes permiten como mucho dos canales lógicos, un canal para datos normales y un canal para datos urgentes.

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

No todos los canales de comunicación preservan el orden de envío de los mensajes. Para solucionar la posible pérdida de la secuencia de los mensajes, el protocolo tiene que gestionar los diferentes trozos de información en una memoria (*buffer*) para finalmente ordenarlos correctamente.

Otro aspecto que se tiene en cuenta es el de cuando un emisor transmite información muy rápidamente hacia un receptor lento. Muchas soluciones utilizan una técnica que consiste en que el receptor envíe una señal al emisor indicándole su problemática. Otras soluciones limitan la velocidad del emisor cuando supera un cierto umbral.

Otro problema es que determinados niveles acepten mensajes de una longitud que supere un cierto límite. Por eso se utilizan mecanismos para desensamblar, transmitir y reensamblar mensajes.

A veces, el canal físico de transmisión es compartido por muchas conexiones que intentan transmitir a la vez sobre un mismo enlace. En este caso, la multiplexación y demultiplexación de la capa física nos permite transmitir mucha información sobre pocos circuitos físicos.

Cuando existen múltiples caminos entre el origen y el destino se tiene que elegir una ruta. Esta decisión se toma muchas veces entre dos o más capas.

## 7. Interfaces y servicios

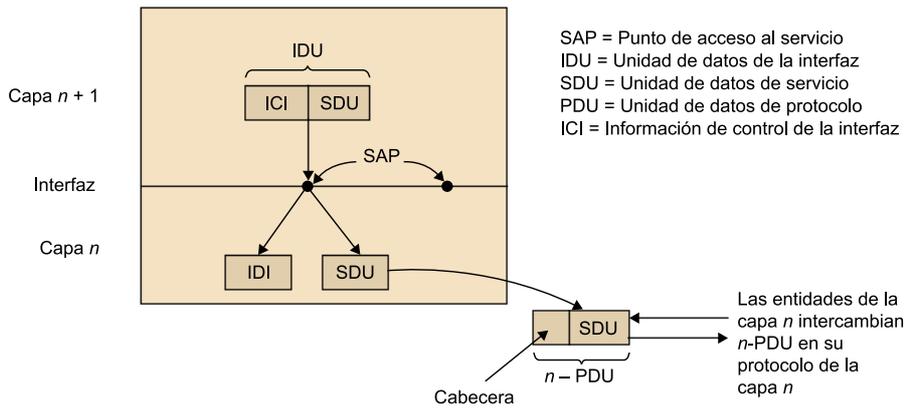
La función de cada capa es proporcionar servicios a la capa superior. En este apartado estudiaremos con más detalle lo que se denominan servicios.

Los elementos activos de cada capa se llaman entidades (*entities*). Cada entidad puede ser una entidad de software (como un proceso) o de hardware (como un dispositivo inteligente de entrada-salida). Las entidades de la misma capa de diferentes máquinas se llaman *peer entities*. 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.

Los servicios están disponibles en los *Service Access Point* (SAP). 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 única que lo identifica. Para hacer este punto más claro, 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. En el sistema postal, la dirección SAP es el nombre de la calle y el número de la vivienda. Para enviar una carta postal, tienes que conocer la dirección SAP.

A fin de que dos capas se intercambien información, se tienen que definir una serie de normas sobre la interfaz. En una interfaz típica, la entidad de la capa  $N + 1$  pasa una *Interface Data Unit* (IDU) hacia la entidad de la capa  $N$  a través del SAP tal como se muestra en la siguiente figura. La IDU consiste en un *Service Data Unit* (SDU) y determinada información de control (*Interface Control Information*). La SDU es la información pasada a través de la red hacia la *peer entity* y subida después hacia la capa remota  $N + 1$ . La información de control se necesita para ayudar a la capa inferior a realizar su trabajo (por ejemplo, indicar el número de bytes del SDU), pero no forma parte de la información pura.

Para transmitir la SDU, la entidad de la capa  $N$  tiene que fragmentar ésta en varios trozos, a cada uno de los cuales se asigna una cabecera, que se envían como un *Protocol Data Unit* (PDU) o paquete. A través de las cabeceras de la PDU, la *peer entity* identifica qué PDU contienen datos y cuáles contienen información de control, proporcionando números de secuencia y contadores.



Las capas pueden ofrecer dos tipos diferentes de servicios a las capas superiores: conexiones orientadas y no orientadas a conexión. Un servicio orientado a conexión se modela como un sistema de telefonía: para hablar con alguien, primero tenemos que marcar el número de teléfono, después, hablar, y, finalmente, colgar el teléfono. Así, inicialmente se produce un establecimiento de conexión, después se utiliza la conexión para hablar y transmitir información, y, finalmente, se cierra la conexión. Esta conexión actúa como un tubo: el emisor envía objetos o bits hacia el receptor, y el receptor los coge en el mismo orden en que le son enviados.

Un servicio no orientado a conexión se modela como un sistema postal. Cada mensaje o carta postal lleva la dirección completa del destinatario, y cada carta la envía el sistema independientemente de las otras cartas. Normalmente, de dos mensajes que se envían al mismo destino, el primero que se envíe será el primero que se recibirá. También es posible que el enviado en primer lugar sufra algún retardo y que el enviado en segundo lugar llegue antes que el que se envió primero. En una conexión orientada a conexión eso es imposible.

Cada servicio está caracterizado por lo que se denomina 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 (ACK) introduce *overhead* (información de control redundante, no información útil) y un cierto retardo, cosa que normalmente no es deseable en términos de rendimiento de la red.

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 en el orden en que fueron emitidos, y que lleguen todos los bits del fichero.

Para muchas aplicaciones, los retardos 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 de la línea o una palabra mal entendida de vez en cuando, que soportar que se produzca

un retardo en la espera del reconocimiento. También cuando se transmite una película de vídeo es preferible tener varios puntos (píxeles) incorrectos (que en la práctica casi no son ningún problema) que tener que ver la película con paradas para corregir los errores (es muy irritante).

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

También en algunas situaciones es conveniente no tener que establecer una conexión para enviar un mensaje corto, pero en el que la fiabilidad tiene que ser esencial. Por eso se utilizan los servicios no orientados a conexión con reconocimiento (ACK). Por ejemplo, cuando se envía un *e-mail*, el receptor del correo electrónico, cuando lo ha recibido, le devuelve un *e-mail* 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.

	Servicio	Ejemplo
Orientado a la conexión	Flujo de mensaje fiable	Secuencia de páginas
	Flujo de bytes fiable	Conexión remota
	Conexión poco fiable	Voz digitalizada
Sin conexión	Datagrama poco fiable	Correo basura electrónico
	Datagrama reconocido	Correo registrado
	Solicitud-respuesta	Solicitud de base de datos

Un servicio se especifica formalmente con un conjunto de primitivas (operaciones) de las que el usuario u otra entidad puede disponer para acceder al servicio. Esas primitivas mandan realizar al servicio alguna acción o devolver el resultado de una acción de la entidad par (*peer entity*). La siguiente tabla nos muestra las maneras de clasificar las primitivas del servicio:

Primitiva	Significado
<b>Request</b>	Una entidad quiere que el servicio realice alguna cosa.
<b>Indication</b>	Una entidad es informada de algún evento.
<b>Response</b>	Una entidad quiere responder a algún evento.
<b>Confirm</b>	La respuesta a la última petición se confirma.

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 se quiere conectar 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 el rechazo de su conexión a partir de la primitiva *CONNECT.confirm*.

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

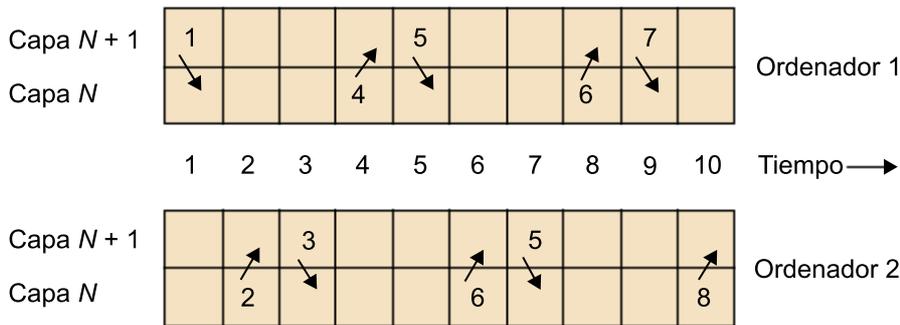
Los servicios pueden ser confirmados o no ser confirmados. En un servicio confirmado están las primitivas *request*, *indication*, *response*, *confirm*. En un servicio no confirmado sólo están las primitivas *request* e *indication*. El servicio *CONNECT* sólo se utiliza en los servicios confirmados porque la entidad remota tiene que 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 el establecimiento de la conexión.
- 2) *CONNECT.indication*: indicar a la parte solicitada un establecimiento de conexión.
- 3) *CONNECT.response*: utilizado por la parte solicitada para aceptar/rechazar la conexión o llamada.
- 4) *CONNECT.confirm*: indicar al que la ha solicitado si la conexión o la petición ha sido aceptada.
- 5) *DATA.request*: indicar que se envía la información.
- 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 el cierre de la conexión.

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

La siguiente figura muestra la misma secuencia antes descrita. Cada paso incluye una interacción entre dos capas de una de las computadoras. 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.



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 de cómo están implementadas estas operaciones. Un servicio es una interfaz entre dos capas, siendo la capa de nivel inferior la que proporciona el servicio, y la capa de nivel superior la que lo utiliza.

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

Un servicio sería como 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 implementan las operaciones. Un protocolo relata cómo se implementa el servicio y, si es posible, cómo hacer que no sea visible para el usuario del servicio.

### 7.1. Tipo de conexión de servicios

Cada servicio establece una conexión con el servicio análogo del equipo de destino; dependiendo de cómo se gestione esta conexión entre servicios, un servicio puede ser orientado a conexión o no orientado a conexión.

El servicio orientado a conexión previo al envío de información se 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 sea orientado a conexión implica que la información tiene que llegar ordenada y sin errores. El hecho de mantener la conexión implica que ambos extremos son conocidos y, por lo tanto, no es necesario indicar qué destino tiene la comunicación. Este paso se realiza durante el establecimiento de la conexión.

Por su parte, los servicios no orientados a conexión no precisan ni asumen ninguna conexión previa entre los dos interlocutores; de esta manera, la información se separa en paquetes (denominados datagramas en este tipo de servicios) y se envía a la red sin conocer el camino que seguirán los paquetes, ni saber si llegarán a su destino, ni siquiera en qué orden lo harán, cada datagrama se envía de forma autónoma e independiente del resto. Por lo tanto, para poder enviar un datagrama con un protocolo no orientado a conexión, el datagrama tiene que tener la dirección destino, y los elementos intermedios de la red tienen que tener información de cómo hacer llegar la información dependiendo del destino de cada datagrama recibido.

**Protocolo orientado a conexión**

El ejemplo por excelencia de un protocolo orientado a conexión es el TCP.

**Servicios no orientados a conexión**

El ejemplo por excelencia de servicios no orientados a conexión es IP. Curiosamente, HTTP es también un protocolo no orientado a conexión.

## 8. Modelos de referencia

Las dos arquitecturas de red más conocidas hoy en día son la Open Systems Interconnection (OSI), utilizada como modelo teórico, y la Transmission Control Protocol/Internet Protocol (TCP/IP), cuyo éxito en el mundo de las redes ha sido enorme.

### 8.1. 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, encargándose 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 proporcionarle los servicios necesarios. Eso acarreaba varios problemas, tales como:

- Los costes eran elevados, ya que los adaptadores eran a medida.
- Nula interoperabilidad, 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) Tres empresas, DEC, INTEL y XEROX (Consortio 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 recogió la versión de DIX y empezó a trabajar en una trama Ethernet mejorada. La red Ethernet tenía un coste bajo y altas prestaciones, junto con una sencillez de operación.

3) El sistema operativo UNIX, creado por BELL Laboratories, empezó a popularizarse, y diversas 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 *kernel*.

#### 4) Creación de un modelo de referencia OSI de ISO.

Estos hechos provocaron que los sistemas que hasta este momento ofrecían una arquitectura cerrada pasaran a una arquitectura abierta y que las redes empezaran a ser 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, hecho que no pasaba con los sistemas propietarios.

Se crean fóruns 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.).

La existencia de estándares tiene las siguientes ventajas y desventajas, que se muestran en la tabla siguiente.

Ventajas	Desventajas
<ul style="list-style-type: none"> <li>• Estimula la competitividad entre los fabricantes</li> <li>• Evita monopolios</li> <li>• Baja los precios</li> <li>• Flexibilidad de instalar equipos</li> <li>• Heterogeneidad de fabricantes</li> </ul>	<ul style="list-style-type: none"> <li>• Tardanza al aprobarse</li> <li>• Los fabricantes crean equipos en condiciones propietarias</li> <li>• Los intereses de los fabricantes y los organismos no siempre son los mismos</li> <li>• Posibilidad de acuerdos más políticos y comerciales que técnicos</li> <li>• Los fabricantes son los que desarrollan más I+D, lo cual provoca que los organismos tengan que definirse</li> <li>• Muchos organismos pueden afectar a la estandarización, ya que se puede llegar a clasificar geográficamente, por industria, etc.</li> </ul>

#### Perjuicios económicos

Hay importantes ganancias económicas para las empresas que han desarrollado un sistema y éste se convierte en estándar. No obstante, ello puede provocar que otras empresas salgan perjudicadas.

## 8.2. El modelo de referencia OSI

Entre los diferentes modelos propuestos por las diferentes organizaciones internacionales de normalización en la década de los ochenta, destaca una arquitectura de redes de ordenadores basada en niveles, el modelo OSI, definido por la Organización Internacional de Estándares (ISO, International Organization for Standardization).

A finales de los 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 estándares para que el software y los dispositivos de diferentes fabricantes pudieran funcionar juntos.

Además de facilitar las comunicaciones entre sistemas diferentes, la ISO pretendía con OSI impedir que ninguna de las arquitecturas de fabricante existentes adquiriera una posición hegemónica, especialmente la SNA<sup>13</sup> de IBM.

<sup>(13)</sup>SNA es la abreviatura de System Network Architecture.

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

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

- 1) Una capa se creará en situaciones donde se necesite un nivel diferente de abstracción.
- 2) Cada capa tendrá que realizar una función bien definida.
- 3) Los problemas se resuelven en una capa concreta sin afectar al resto de las capas.
- 4) Cada capa se basa en los servicios de la capa inmediatamente inferior.
- 5) Cada capa ofrecerá servicios a las capas superiores sin que éstas sepan cómo se realizan los servicios.
- 6) La función que realizará cada capa se tendrá que seleccionar con la intención de definir protocolos normalizados internacionalmente.
- 7) Los límites de las capas se habrán de seleccionar teniendo en cuenta la necesidad de minimizar la cantidad de información que se tiene que pasar entre capas. La frontera entre capas tiene que ser la más sencilla posible.
- 8) El número de capas tiene que ser lo bastante grande para que funciones diferentes no tengan que ponerse juntas en la misma capa. También tendrá que ser lo bastante pequeño para que su arquitectura no sea difícil de manejar.

Las capas son las que se muestran en la figura siguiente.

7	Aplicación	Procesos de la red a la aplicación	} Capas superiores
6	Presentación	Representación de datos	
5	Sesión	Comunicación entre <i>hosts</i>	
4	Transporte	Conexiones extremo a extremo	} Capas inferiores
3	Red	Direcciones y mejor ruta	
2	Enlace de datos	Acceso a los medios	
1	Física	Transmisión binaria	

Las capas se pueden agrupar en dos subconjuntos convenientemente diferenciados:

- **Capas inferiores.** Son proveedoras de servicios de transporte de las capas superiores. Tratan problemas tales como errores del sistema de transmisión, búsqueda de rutas óptimas, etc.
- **Capas superiores.** Su misión es dar servicios al usuario del sistema de comunicaciones. Confían en las prestaciones de los niveles inferiores.

#### Nota

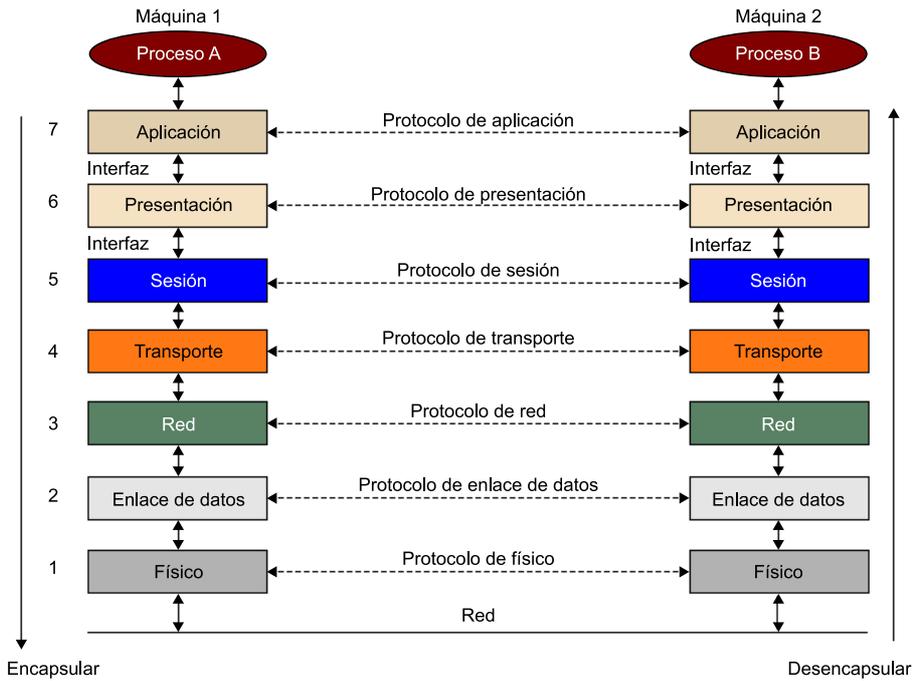
Hay que señalar la sospechosa coincidencia del número de capas de OSI con el de SNA, la arquitectura de red para grandes sistemas de IBM, que estaba en pleno apogeo en el momento en que se definió OSI.

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

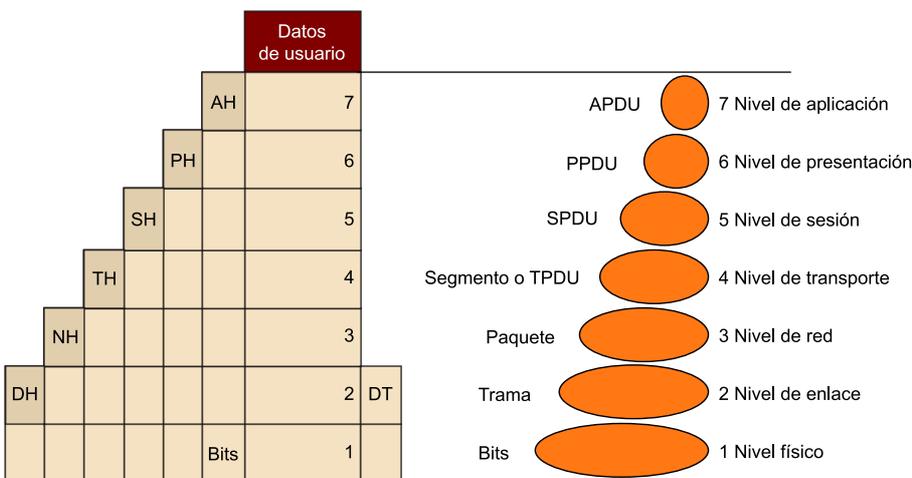
### 8.2.1. Proceso de encapsulación y desencapsulación

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:

- **Comunicación horizontal.** Comunicación con su capa de igual nivel del otro sistema, que recibe el nombre de protocolo.
- **Comunicación vertical.** Comunicación con sus niveles inmediatamente superior e inferior, que recibe el nombre de primitivas de servicio.



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.



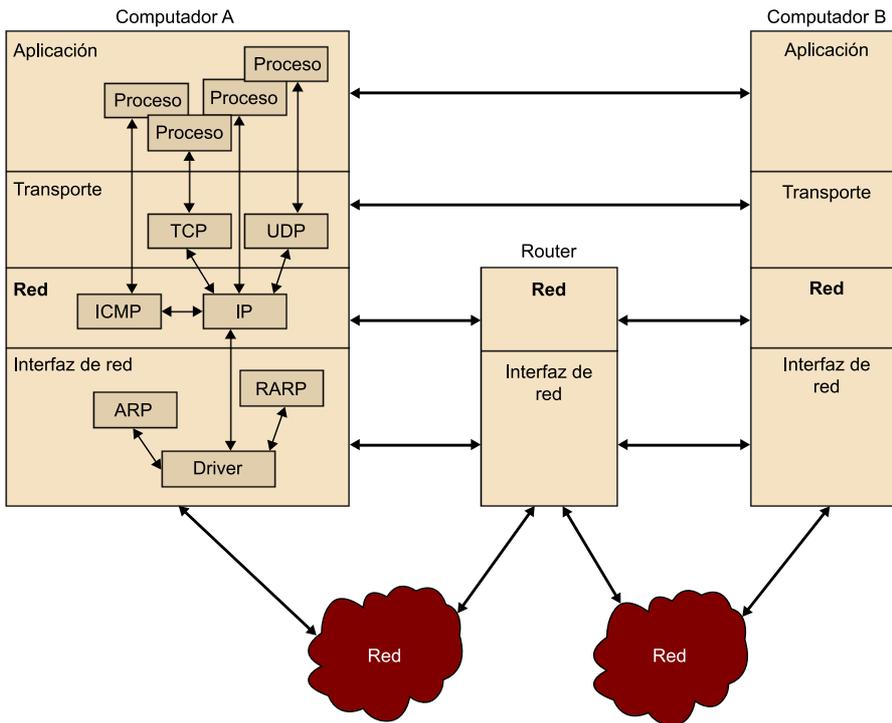
### 8.3. Modelo TCP/IP

En el modelo TCP/IP<sup>14</sup> se pueden distinguir cuatro capas:

- La capa interfaz de red.
- La capa de red o Internet.
- La capa de transporte.
- La capa de aplicación.

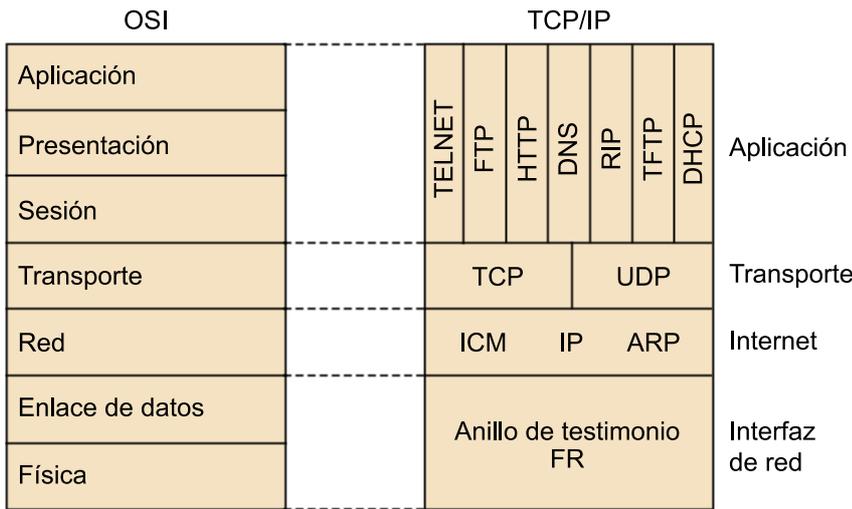
<sup>(14)</sup>TCP/IP es la abreviatura de Transmission Control Protocol/Internet Protocol.

Pasemos a describirlas brevemente.



Aplicación	Interfaz de usuario	Telnet HTTP
Presentación	Presentación de datos	ASCII JPEG
Sesión	Mantiene separados los datos de las distintas aplicaciones	Sistema operativo Programación
Transporte	Distribución fiable o no. Corrección antes de transmitir	TCP UDP
Red	Proporciona el direccionamiento lógico que los routers utilizan para determinar la ruta	IP
Enlace de datos	Combina bits en bytes y bytes en <i>frames</i> . Acceso a los medios utilizando las direcciones MAC. Detección de errores.	802.3 303.3 HDL
Física	Especifica el voltaje, velocidad del cable y la extensión de los cables. Mueve bits entre dispositivos.	V 35 EIA G703/704

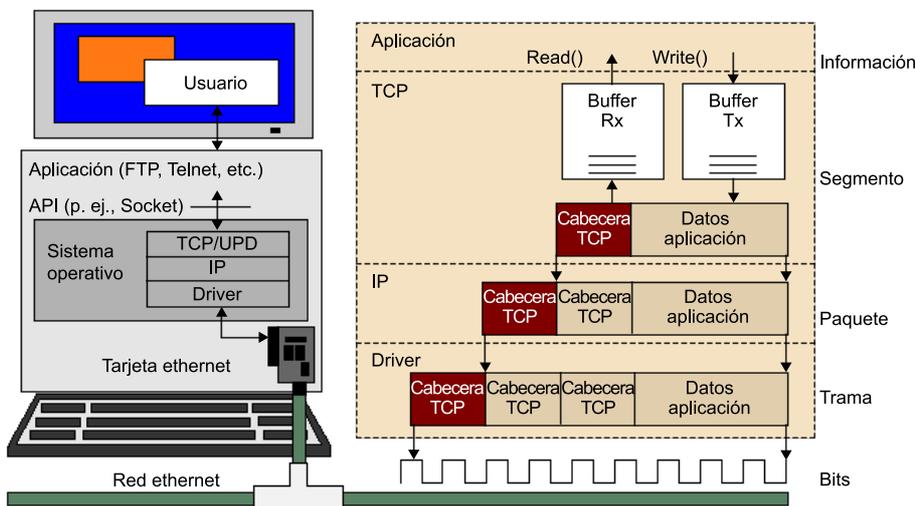
La comparación de los modelos arquitectónicos de OSI y TCP/IP es la siguiente.



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.

### 8.3.1. Encapsulación de la información en el modelo TCP/IP

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



Los datos de información del nivel aplicación son encapsulados en la capa de transporte, donde se le añade la cabecera del protocolo TCP, conformando la unidad de información denominada *segmento*. Cuando se envía el segmento al nivel de red, queda encapsulado dentro de la cabecera del protocolo IP donde se indican las direcciones IP de la unidad de información llamada *paquete* en este nivel. Este paquete es enviado a la tarjeta de red y allí es encapsulado según las normas del protocolo del nivel de enlace. Normalmente añade una cabecera del protocolo de enlace al principio del paquete. En muchos proto-

colos también se añade una cola de datos que sirve para la detección de errores al final del paquete. La unidad de información aquí recibe el nombre de *trama*. Finalmente, los datos son enviados por el medio de transmisión en forma de impulsos electromagnéticos o bits.

#### 8.4. Modelo OSI comparado con modelo TCP/IP

El modelo OSI, de orientación más académica, es más coherente y modular y está menos condicionado por cualquier protocolo en particular. 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 propia). El modelo OSI hace una distinción muy clara entre servicios, interfaces y protocolos, conceptos que a menudo se confunden en el modelo TCP/IP.

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 él. Las razones principales que motivaron este fenómeno se resumen como sigue:

- OSI apareció tarde. Como todo estándar, se tardaron 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 I retraso BM, que es una arquitectura compleja, es muy complicado y muchas veces repite en diferentes capas las mismas funciones. El nacimiento de TCP/IP fue a la inversa: 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 desarrolladoras a fijar altos precios con el fin de recuperar sus costosísimas inversiones. En contraste, TCP/IP fue rápidamente incorporado al UNIX de Berkeley donde funcionaba bastante bien, y todo eso a un precio sensiblemente menor: ¡era gratuito!
- Mientras que TCP/IP era visto como parte de UNIX, es decir, una cosa que realmente funcionaba y estaba al margen de toda sospecha de parcialidad, OSI era considerado un invento de la Administración para controlar las telecomunicaciones (un engendro político-burocrático).

Por todo eso, TCP/IP se convirtió en el líder mundial absoluto en interconexión de redes. No obstante, TCP/IP tampoco se libró de la crítica. Por una parte, no distingue conceptos tan importantes como servicio, interfaz y protocolo. En segundo lugar, el modelo TCP/IP no es ningún modelo, es decir, su utilización como esquema de referencia resulta bastante inútil en el estudio de otras arquitecturas. En tercer lugar, en el modelo TCP/IP la capa ordenador principal-red es más bien una interfaz que una capa, ya que la única cosa que se especifica de ella es que tiene que ser capaz de transmitir paquetes IP.

**Difusión de TCP/IP y del modelo OSI**

Hoy en día, la difusión de TCP/IP por toda Europa es completa, mientras que los servicios basados en protocolos OSI han desaparecido prácticamente.

## 9. Breve historia de las comunicaciones

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

No tardó mucho en aparecer 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 poder hacer 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 tener que generar ninguna infraestructura nueva. Sólo hacía falta un aparato que adaptara los bits a la red<sup>15</sup>. Estos aparatos son los módems.

Los primeros módems eran de 300 bps y generaban dos tonos diferentes: uno para el 1 lógico y otro para el 0. Actualmente, van a 56.000 bps, que es el máximo que permite la actual 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 los terminales de uno se podía acceder a los de otro y viceversa.

La tecnología de conmutación de circuitos se desarrolló originalmente para las comunicaciones telefónicas, y una de sus características fundamentales era la ocupación en exclusiva de los recursos mientras duraba la conexión, cosa que, como ya hemos visto, justificaba la tarificación por tiempo. Pero las comunicaciones informáticas no son cortas, 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 rato que dura la conexión: puede haber largos períodos de tiempo en los que no pase ningún bit y ratos en los que haya un intercambio de datos intenso, aunque, desde luego, 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 del uso real de la red.

### Períodos en la historia de Internet

Internet es, como tantas otras tecnologías innovadoras, un invento militar. Nació del interés del ejército norteamericano en los años sesenta por conseguir comunicaciones

(15) Recordad que la red telefónica sólo deja pasar sonidos entre unos márgenes de frecuencia.



Módems de los años ochenta

fiables y descentralizadas. Es decir, para evitar que un misil bien dirigido pudiera hacer saltar 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.
- Segundo período: 1970-1990. Del Ejército a la Universidad.
- Tercer período: 1990-1995. Expansión fuera de los ámbitos militares y universitarios.
- Cuarto período: 1996-Actualidad. Multimedia y cientos de millones de usuarios.

### **Primer período: 1957-1970. Nacimiento de Internet**

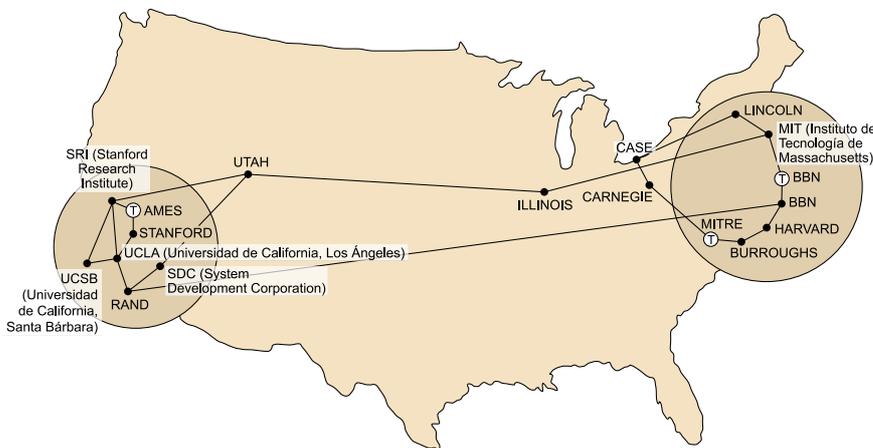
Dentro del primer período de la historia de Internet podemos destacar los siguientes acontecimientos:

- **1945:** Publicación de la primera referencia a una red electrónica similar a Internet: "Memex", citado en el artículo "As We May Think", de Vannevar Bush (director de la Oficina de Investigación Científica y Desarrollo norteamericana).
- **1957:** Durante la guerra fría, la Unión Soviética lanza el Sputnik, el primer satélite artificial de comunicaciones. En respuesta a este hecho, Estados Unidos crea el ARPA<sup>16</sup>, en el seno del Departamento de Defensa estadounidense.
- **1961:** Leonard Kleinrock (MIT) publica el primer artículo sobre la teoría de conmutación de paquetes.
- **1962:** Licklider (MIT) lanza la idea de la "Galactic Network", una red interconectada globalmente a través de la que cualquiera podría acceder desde cualquier lugar a datos y programas. Licklider fue el principal responsable del programa de investigación en ordenadores en ARPA, la agencia 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 (Packet Switching Networks).
- **1961-1965:** La idea de red de paquetes descentralizada había sido trabajada en paralelo por tres grupos de investigación americanos, sin que los investigadores conocieran el trabajo de los otros.
  - MIT (1961-67): Licklider, Roberts, Kleinrock.
  - RAND (1962-65): Paul Baran.
  - NPL (1964-67): Donald Davies y Roger Scantlebury. La palabra *packet* (paquete) fue adoptada a partir del trabajo del NPL<sup>17</sup>.
- **1965:** El Ministerio de Defensa norteamericano (ARPA) inicia un proyecto de interconexión de computadores, que se llamó ARPANET y fue el antecesor de lo que después se llamaría Internet.
- **1966:** Se desarrolla el concepto de red de ordenadores, que se llamaría ARPANET. La red ARPANET podía interconectar los diferentes ordenadores de los investigadores que se fueran conectando a esta red, naciendo así el Backbone Network.
- **1967:** La nueva red, denominada ARPANet, recibe la señal de salida. Un año más tarde se diseñan los primeros programas y el primer hardware específico para redes.
- **1969:** Hay cuatro centros interconectados a través de sus IMP (Internet embrionaria). UCLA (Los Ángeles) es seleccionada para ser el primer nodo de ARPANET. El centro de investigación de Standford (SRI) proporciona un segundo nodo. El tercer nodo en la Universidad de California, Santa Bárbara, y el cuarto nodo en la Universidad de Utah. Estos cuatro nodos constituyeron la red original de ARPANet.

<sup>(16)</sup>ARPA es la abreviatura en inglés de la Agencia de Proyectos de Investigación Avanzada.

<sup>(17)</sup>NPL es la abreviatura de National Physical Laboratories (institución del Reino Unido).

Pronto, las grandes empresas presionaron a las compañías telefónicas del momento para que desarrollaran redes pensadas para transportar datos, con un sistema de tarificación que se ajustara al tráfico de datos real y permitiera más velocidad que los escasos 300 o 1.200 bps que se alcanzaban en aquella época utilizando la red telefónica. La respuesta fueron las redes de conmutación de paquetes. El envío de datos no se tiene que hacer necesariamente en tiempo real (las transmisiones de voz, sí). Por lo tanto, no hace falta establecer el camino entre los dos puntos antes de empezar la transmisión y mantenerlo mientras dura el intercambio de datos. En lugar de eso, se empaquetan los bits que se tienen que transmitir y se dan a la central más próxima para que los envíe cuando pueda a la siguiente, y así sucesivamente, hasta que lleguen a su destino. Si cuando llega un paquete a una central todos los enlaces con la siguiente están ocupados, no pasa nada, se le hace esperar poniéndolo en una cola para enviarlo cuando haya un enlace disponible.



Nodos en ARPANET en 1971

La transmisión por paquetes tiene la ventaja de que sólo ocupa los recursos cuando realmente se utilizan, no todo el tiempo. Pero, como contrapartida, se tiene que soportar el retardo que pueda haber desde que los paquetes salen del origen hasta que llegan a su destino, y que es variable, porque las esperas en las colas son aleatorias, dependen 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.

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

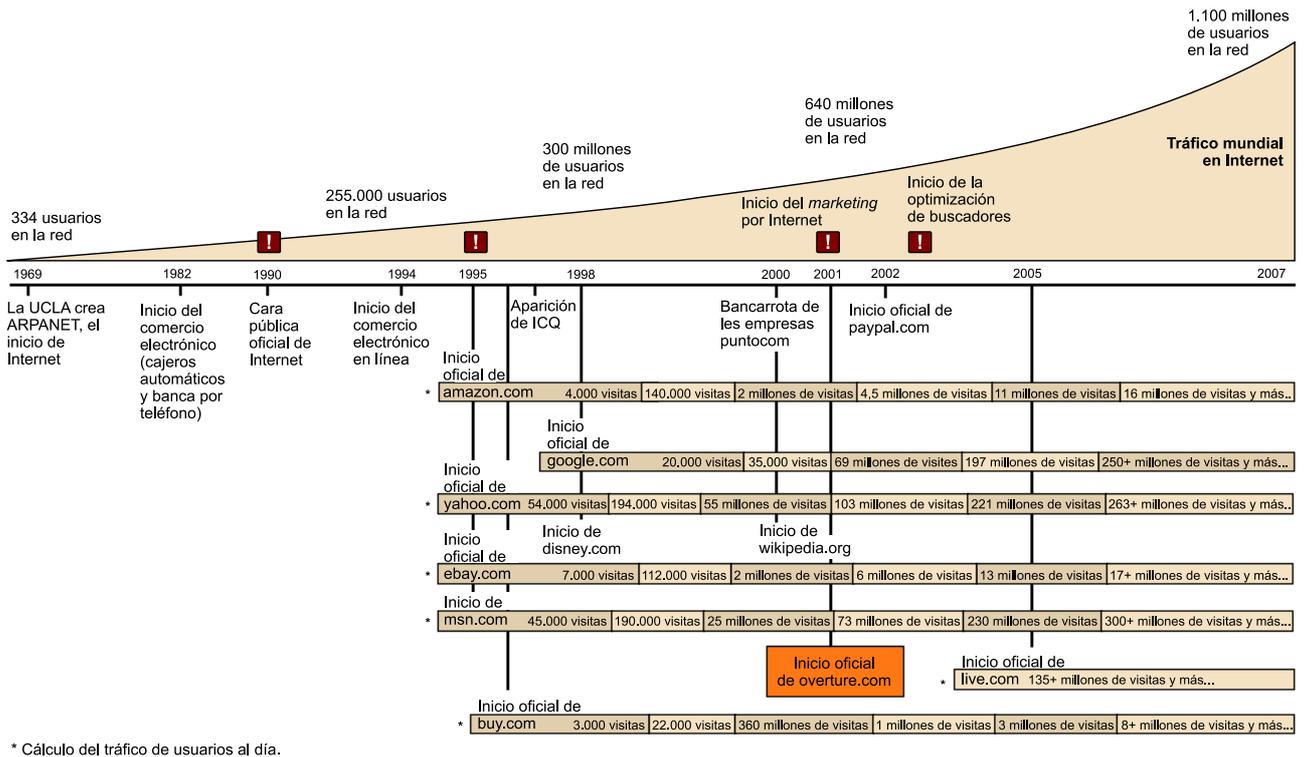
Las compañías telefónicas desarrollaron redes de este tipo, y el CCITT emitió un estándar, el X.25, que ha sido en definitiva el que ha adoptado todo el mundo hasta hace poco.

### CCITT

El CCITT es un organismo internacional patrocinado por las operadoras de telefonía, dedicado a tareas de normalización en el ámbito de las telecomunicaciones. El 1 de marzo de 1993 pasó a llamarse International Telecommunication Union Standardization Sector (ITU-T).

### CERT

El Computer Emergency Response Team (CERT) es un equipo de respuesta de emergencia de ordenadores que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.



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

Dentro del segundo período de la historia de Internet podemos destacar los siguientes acontecimientos:

- **Años 1970.** Durante este período, la red fue de acceso restringido a los investigadores y a las empresas privadas que participaban en proyectos financiados por la Administración.
- **1970.** El Network Working Group (NWG), liderado por S. Crocker, acabó el protocolo ordenador principal a ordenador principal inicial para ARPANET, denominado Network Control Protocol (NCP, protocolo de control de red). Kevin MacKenzie inventa el primer emoticón: :-). Vinton Cerf escribe por primera vez la palabra Internet. Está considerado el padre de la red. Más tarde diseñó el protocolo TCP/IP, que actualmente rige las comunicaciones por Internet.
- **1971.** Ray Tomlison (BBN<sup>18</sup>) crea los protocolos básicos del correo (*e-mail*), incluida 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 la IANA o Autoridad de asignación de números de Internet, responsable de asignar una dirección única a cada computador conectado a Internet.
- **1973.** Vint Cerf y Bob Kahn especifican la primera versión del programa de control de transmisión (TCP), que se desarrolló después hasta convertirlo 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 incorporó este software 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 tiene 212 servidores.
- **1981.** 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). La European Unix Network (EuNet), conectada a ARPANet, se creó en 1982 para proporcionar servicios de correo electrónico y servicios Usenet a diversas organizaciones usuarias en los Países Bajos, Dinamarca, Suecia e Inglaterra.
- **1983.** Considerado como el año en que nació realmente Internet al separarse la parte militar y la civil de la red. Hasta el 1 de enero de 1983, la incipiente Internet estuvo funcionando con un antecesor de los protocolos TCP/IP; aquel día, los ya miles de ordenadores conectados se cambiaron al nuevo sistema. Internet ya dispone de 562 servidores (ordenadores interconectados). El mismo año se creó 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 forjaba Well, la primera comunidad comercial de usuarios. Se crea en Wisconsin el primer *name server*, con lo que ya no se necesita conocer el *path* de localización de un computador, precursor del servicio DNS de Internet.
- **1985.** Entra en funcionamiento el Domain Name Server (DNS), un método para resolver nombres en direcciones numéricas. El primer dominio se otorga el 15 de marzo a Symbolics.com. Internet ya tiene 1.961 servidores y los sufijos .com, .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 todavía en activo sin duda, y todos universitarios, también sin duda. En junio del mismo año aparece el primer dominio gubernamental, css.gov, y en julio, mitre.org. El primer dominio de un país se atribuyó en julio de aquel mismo año a Gran Bretaña: co.uk. En España, los ordenadores de diferentes universidades se conectaban entre sí y con el Centro Europeo de Física de Partículas (CERN). El Ministerio de Educación y Ciencia, a través 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 un informe que se llamó Proyecto IRIS (Interconexión de Recursos Informáticos).
- **1987.** Nace la primera versión de Windows. Hay más de 10.000 servidores en todo el mundo.
- **1988.** Se produce el primer gran ataque vírico de Internet, cuando el "gusano de Morris" hace caerse 6.000 de los 60.000 ordenadores que entonces la formaban. Creado por el estudiante de doctorado 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 Computer Emergency Response Team (CERT). Jarkko Oikarinen, un joven finlandés, decide modificar el comando talk del Unix para permitir que diversas personas puedan charlar de forma simultánea. Así nace el chat, el Internet Relay Chat (IRC), que permite que se pueda conversar en línea en la red. En 1988 nace el programa IRIS dentro del Plan Nacional de Investigaciones y Desarrollo Tecnológico para dar conectividad a científicos e investigadores. La financiación y supervisión de esta red correría a cargo de la Comisión Interministerial de Ciencia y Tecnología, y de su gestión y dirección se encargaría Fundesco.
- **1989.** Nace RIPE para interconectar las redes europeas. El número de servidores conectados a Internet alcanza ya los 100.000. Este mismo año, se inaugura también la primera conexión de un sistema de correo electrónico comercial en Internet (MCI y CompuServe). Nace Archie. Hasta aquel momento nadie se había planteado nunca la hipótesis de que en Internet las cosas pudieran tener un orden, ni de crear 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 tuvo noticia de su existencia. Por este motivo, la Universidad McGill de Montreal obligó a su autor a cerrarlo. Por suerte, lo hizo después de que Archie ya estuviera replicado en otros ordenadores. Archie fue el precedente de Gopher y Veronica y, de alguna remota manera, el primer intento de directorio de recursos de Internet.

<sup>(18)</sup>BBN es la abreviatura de la empresa Bolt, Beranek and Newman.

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 utilizaron para las redes de gran alcance. En las redes de área local se necesita, habitualmente, establecer comunicaciones "de muchos a uno" y "de uno a muchos", cosa 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, en la que los paquetes que salen de una estación llegan a todo el resto simultáneamente. En la recepción, las estaciones los aceptan o ignoran según que sean sus destinatarias o no.

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

De la década de los sesenta son también los primeros estándares de arquitecturas de protocolos. Hay que tener presente que el intercambio de información entre ordenadores tiene toda una serie de implicaciones, entre las que se incluyen las siguientes:

- Aspectos eléctricos: los cables, los conectores, las señales, etc.
- La manera de agrupar los bits para formar paquetes y la de controlar 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 la reciba.

Abordar todos estos aspectos de una manera global resulta inviable: demasiadas cosas demasiado diferentes entre sí. Por eso, ya 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 querida por los usuarios.

Hay que 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, escogía una marca y quedaba ligada a ella para toda vida.

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

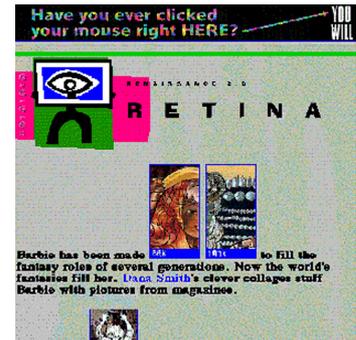
- La propuesta del protocolo Ethernet para redes locales.
- La aparición del sistema operativo Unix, no ligado a ninguna marca comercial, compatible con todas las plataformas de hardware que había.
- La invención de los protocolos TCP/IP, embrión de la actual Internet.

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

### Tercer período: 1990-1995. Expansión fuera de los ámbitos militar y universitario

Dentro del tercer período de la historia de Internet podemos destacar los siguientes acontecimientos:

- **1990.** Nacen el primer proveedor de acceso a Internet comercial y el Electronic Frontiers Foundation (EFF), una ONG de defensa de ciberderechos. La red tiene ya centenares de miles de servidores (313.000). Este año también aparece Windows 3.0. En España, Fundesco cambia el nombre del programa IRIS por REDIRIS y se conecta al *backbone* de Internet (NSFNET<sup>19</sup>), al lado de Argentina, Brasil, Chile, India, Suiza, Austria, Irlanda y Corea del Sur.
- **1991.** Tim Berners-Lee, investigador en el centro europeo CERN, en Suiza, elaboró su propuesta de un sistema de hipertexto compartido: era el primer esbozo de la World Wide Web. Como el 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. Surgía como el lugar donde pactar los protocolos que harían posible la comunicación. El Internet Activities Board (IAB) se integra en la Internet Society. En el IAB destacó la Internet Engineering Task Force (IETF), que tenía como función el desarrollo de Internet a corto plazo y la responsabilidad de la dirección técnica. La mayor parte de los Request For Comments (RFC) se elaboran en el IETF, y éstos iban aumentando cada año. Internet ya tiene 1.136.000 servidores. En España aparece Goya Servicios Telemáticos, 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, donde ya había 10 nodos y 15.000 máquinas bajo el dominio .es.
- **1994.** Año del primer spam: los abogados de Arizona Canter & Siegel lanzan el 5 de marzo de 1994 un anuncio en 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 (una marca de refrescos) ponen los primeros *banners* comerciales de la historia en Hotwired. Pero no todo son desgracias: también se 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, al que bautizan Yahoo! Lycos. Se difunde la versión comercial del navegador Netscape Navigator. En España nace Servicom.



En la parte superior de la imagen se puede ver el primer *banner* de Internet en HotWired (1994).

- 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 el sitio de subastas eBay. Hay más de 5 millones de servidores conectados a Internet. La espina dorsal de NSFNET empieza a ser sustituida por proveedores comerciales interconectados. Salida a bolsa de Netscape, la tercera *major* hasta entonces, que marca el comienzo del *boom* de Internet.

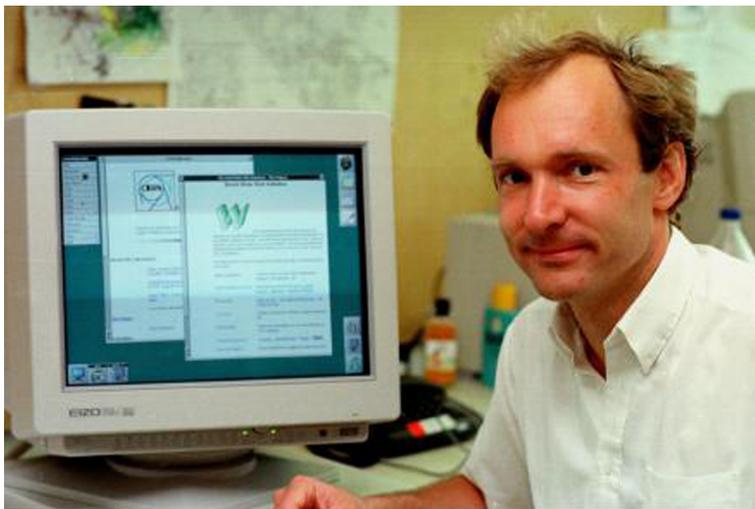
<sup>(19)</sup>Las siglas NSFNET corresponden a National Science Foundation Network.

TCP/IP nació a partir de un encargo de la Defense Advanced Research Project Agency<sup>20</sup> (DARPA) a la comunidad científica americana para tener una red mundial que fuera reconfigurable fácil y automáticamente en caso de destrucción de algún nodo o algún enlace.

<sup>(20)</sup>En castellano, 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 había, era una opción más en el mercado. Ante una oferta tan grande, y dispar, de protocolos, la ISO<sup>21</sup> y el CCITT propusieron un modelo nuevo que intentaba reunir de alguna manera todo lo que ya se había propuesto y que pretendía ser completo, racional y muy bien estructurado (la TCP/IP tiene fama de ser una pila de protocolos anárquica), con la intención, por lo tanto, de que se convirtiera en un modelo de referencia. Es la llamada pila de protocolos OSI (*open systems interconnection*). Internet, que nació y creció en las universidades, se empezó a hacer popular en la década de los noventa, a medida que los que conocían la red la iban "enseñando", y su popularización estalló cuando saltó al mundo de la empresa, en todas sus vertientes: como escaparate de productos o como canalizador de contactos comerciales.

<sup>(21)</sup>ISO son las siglas de la International Organization for Standardization, en castellano, Organización Internacional de Estandarización.



Tim Berners Lee. Creador de la WWW

Su origen universitario, sin embargo, ha marcado esta evolución en muchos sentidos. Por ejemplo, el modelo cliente/servidor de aplicaciones distribuidas. Es un modelo sencillo y al mismo tiempo potente, y casi todas las aplicaciones que se hacen servir en Internet lo siguen. El Telnet, o apertura de sesión remota, la transferencia de ficheros (FTP), el correo electrónico y, sobre todo, la WWW (World Wide Web) son ejemplos claros de aplicaciones que siguen

este modelo. Las dos primeras han caído en desuso un poco, pero tanto el correo como la WWW son las estrellas hoy en día en Internet. Tímidamente, aparecen nuevas propuestas de aplicaciones, pero la WWW, que nació como un servicio de páginas estáticas enlazadas con hiperenlaces, se está convirtiendo en la interfaz de usuario de toda la red, porque actualmente se utiliza para servir páginas dinámicas (se crean en el momento en que se sirven), e incluso, como código que se ejecuta en el ordenador cliente (*applets*).

En este momento tenemos dos redes completamente independientes entre sí, pero de alguna manera superpuestas:

- Una red analógica, con conmutación de circuitos, pensada para voz.
- Una red digital, con conmutación de paquetes, pensada para datos.

La red telefónica, tal como la hemos descrito hasta ahora, es completamente analógica: la señal electromagnética que viaja desde un teléfono hasta otro es analógica (varía continuamente y en 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 hacían con señales analógicas con muchos canales multiplexados en frecuencia, y tenían que recorrer, a veces, grandes distancias. La atenuación de la señal inherente a la distancia que había que recorrer se tenía que corregir mediante repetidores que la amplificaran, cosa 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 ni las interferencias en la recepción. No hay ninguna manera de saber exactamente qué se ha enviado desde el origen y qué es ruido añadido. En 1972 se hicieron públicos 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 cual ha permitido, por una parte, incrementar la calidad de recepción de las 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. Eso ha

hecho cambiar sustancialmente los procesos de conmutación: ahora se tiene que trabajar con bits y, por lo tanto, las centrales electromecánicas se tienen que sustituir por ordenadores.

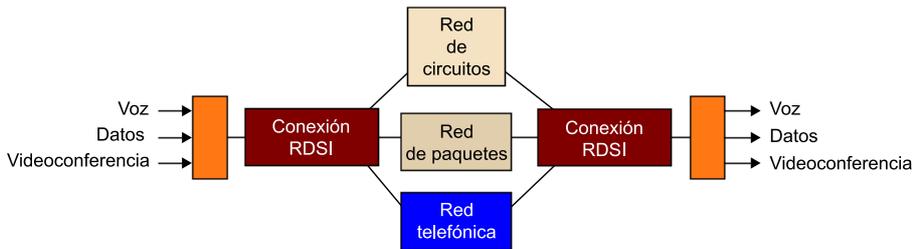
Esta digitalización de la parte interna de la red de voz hizo que confluyeran de alguna manera las dos redes, la telefónica y la de datos: los enlaces digitales entre centrales se utilizaban indistintamente para paquetes de datos y para transmisiones de voz.

#### **Cuarto período: 1996-Actualidad. Multimedia y cientos de millones de usuarios**

Dentro del cuarto período de la historia de Internet podemos destacar los siguientes acontecimientos:

- **1996.** El 98% de los navegadores son Netscape, y se piensa que la red puede acabar con el sistema operativo. Microsoft responde lanzando el Explorer, lo cual 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 clic, que dominará la publicidad en línea. Inclusión de contenidos multimedia: técnica de *streaming* para la transmisión fluida de vídeo.
- **1997.** Business.com se vende por 150.000 dólares. En 1997 ya hay 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 dos millones. El Gobierno estadounidense anuncia un plan para privatizar Internet que es rechazado; un segundo plan es mejor recibido.
- **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 fundar Ya.com. Terra sale a bolsa con gran éxito. Se pagan 7,5 millones de dólares por Business.com. A final de año, el índice NASDAQ alcanza cifras desmesuradas. España tiene 300.000 ordenadores bajo .es y 2 millones de internautas. El formato de sonido MP3 desestabiliza a las multinacionales del disco.
- **2000.** El temido efecto 2000 apenas provoca problemas. En el intermedio de la Super Bowl de fútbol americano, a mediados de enero, se anuncian 17 compañías "punto-com", 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 al lado de Telefónica empieza a ofrecer ADSL. Los operadores de cable empiezan a prestar servicio de banda ancha doméstica en España. La tienda de ropa Boo.com bate récords, con una facturación en seis meses de 160 millones de dólares. Microsoft es condenado por abusar de su cuasi-monopolio en sistemas operativos. Se calcula que la web supera los 1.000 millones de páginas.
- **2001.** Arranca con el pleito abierto de nuevo por las discográficas contra Napster por favorecer la piratería, pleito que acaba por provocar su cierre en julio por orden judicial (y su resurrección como servicio de pago). En febrero, Napster había batido su propio récord, con 13,6 millones de usuarios. Napster cierra en julio por orden judicial (volverá a salir como servicio de pago). America Online compra en enero Time Warner, el mayor grupo mediático del mundo, en lo que se considera el definitivo triunfo de los nuevos medios sobre los viejos. La empresa Kozmo de venta por Internet con entrega rápida quiebra en abril. Su competidora Webvan sufre igual 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 disponible entonces.

- **2002.** La crisis de las puntocom continúa profundizándose. Los dominios son 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 cual acelera los planes para reforzarlo. Explosión en el uso de los weblog o blogger: páginas escritas por los cibernautas en las que éstos 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 finales por intercambiar música en redes P2P. Apple lanza su tienda de música iTunes, asociada al reproductor iPod. Después de dos años de continua caída del valor AOL Time, Warner elimina el "AOL" de su nombre. WiFi se consolida como alternativa de acceso sin hilo. Diversas plagas ensucian Internet; desde Slammer, que se extendió en 10 minutos echando abajo a 8 servidores raíz y afectando a bancos y el tráfico aéreo, hasta SobigF y Blaster. Después de una cierta parada entre 2001 y 2002, se recupera el vigoroso ritmo de crecimiento del número de servidores en la red. Este año también empieza el ataque judicial de SCO contra Linux.
- **2004.** Empieza la recuperación. Sale a bolsa Google, que lanza su correo web de 1 Gb Gmail. Guerra de buscadores: Yahoo! abandona a Google y compra diversas empresas, Microsoft potencia MSN Search y Amazon lanza A9. La música de pago también se caldea, con la entrada de Wal-Mart, Sony, Virgin, eBay y Microsoft; iTunes tiene el 70% del mercado. El navegador Firefox v1.0 hace mella en el dominio del Explorer de Microsoft, al que arranca un 5%. En Estados Unidos, la banda ancha supera a los módems y la campaña de las presidenciales demuestra el poder de los blogs llamados "Rathergate"; el precandidato Howard Dean usa la red para la movilización del electorado y la recaudación de fondos. En España Terra vende Lycos por 105 millones de dólares. El copyleft avanza con la extensión de las licencias Creative Commons.
- **2005.** Existen más servidores raíz fuera de Estados Unidos que en su 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 internautas. Suecia tiene la penetración más alta (74% de la población), y España ocupa el puesto 22 por accesos de banda ancha (casi 2,5 millones) y el 12 por número de internautas (14 millones), pero está por debajo de la media europea en penetración. Diversos accidentes y ataques difunden información privada en la red. Microsoft responde a Firefox con el lanzamiento de una versión no prevista del Explorer. Apple presenta el iPod Shuffle, basado en memoria flash. El mercado de la publicidad en línea se despierta, y diversos medios españoles relanzan sus páginas web. A finales de este mismo año nace Youtube.
- **2006.** Aparecen los principales exponentes de la revolución de la Web 2.0: 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 basados en tecnologías p2p aglutinan la mayoría del tráfico de la Red. XMPP se convierte en estándar de facto para las comunicaciones de mensajería instantánea. Gmail deja de ser beta y se convierte en accesible para todo el mundo. Writely, adquirido por Google el año anterior, es llamado 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 filtraje y censura en 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 dirección IPv6 a las redes de sensores. Se extiende la oferta de servicios a 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.



Una vez digitalizada la red telefónica, el paso siguiente tenía que ser llevar la transmisión de bits hasta las casas. Eso permitía, por una parte, ofrecer a los usuarios en su casa la transmisión de datos además de la tradicional de voz y, por otra, ofrecer 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 un hardware adecuado, aprovechar los dos canales juntos para navegar a 128 kbps.

El uso de la red telefónica para transmitir datos tiene una limitación importante por lo que respecta al máximo de bits por segundo permitidos, y las redes específicas de datos son muy caras para su uso doméstico. Desde la década de los noventa se han estudiado maneras de conseguir llevar hasta las casas 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. Con respecto al primero, se han promovido cableados nuevos con fibra óptica que permiten ese gran caudal, a menudo llevados a cabo por empresas que pretenden competir con los monopolios dominantes. Estas redes se aprovechan para dar un servicio integral: televisión, teléfono y datos. Con respecto al segundo, las compañías telefónicas de toda la vida han querido sacar partido del cableado que ya tienen hecho y, por eso, han desarrollado las tecnologías ADSL, que permiten hacer convivir 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+).

#### RDSI

La red digital de servicios integrados (RDSI) corresponde a las siglas ISDN (*integrated services digital network*) en inglés.

## Resumen

El módulo ha introducido los conceptos fundamentales de las redes de computadores. Hemos visto que éstas son 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 está estructurada en diferentes niveles. Hemos visto que existe un modelo de referencia denominado OSI, que define siete niveles de red. Los niveles más bajos se ocupan de los aspectos físicos de la comunicación, desde la caracterización del medio a la codificación de la información transmitida. Las capas superiores usan las interfaces de abstracción de sus capas subyacentes construyendo así un sistema complejo que permite la 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 permitiendo así que las capas se puedan modificar y/o cambiar sin que ello afecte al comportamiento de la red. Los conceptos de interfaz y cabecera son clave para entender la estructuración en capas de una red.

No obstante, hemos visto también que el modelo OSI es complejo y no ha sido utilizado más que como modelo de referencia. En realidad, Internet usa un modelo TCP/IP más simple pero funcional. El módulo ha presentado ambos modelos y los ha comparado. Finalmente, el módulo repasa la historia de las comunicaciones. Conocer la historia nos ayuda a entender el porqué de determinadas particularidades de las redes de comunicaciones actuales.

En los próximos módulos profundizaremos en el conocimiento de los niveles de la red. En este curso hemos adoptado 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 la de algunos otros documentos de referencia, en los que las redes se presentan a la inversa, primero, conociendo los niveles físicos, y, finalmente, presentando los niveles de aplicación. El módulo "Las capas de la red de computadores" presenta en detalle los niveles de transporte, el nivel de red que es primordial, los principales conceptos de los niveles de enlace de datos y físico, que, como veréis, están fuertemente interrelacionados. El módulo "Seguridad en la red" adopta otro enfoque y nos presenta aspectos relacionados con la seguridad de las redes de computadores, hoy en día de primordial importancia. El módulo 4 nos presenta el nivel de aplicación donde se profundiza en los conceptos fundamentales que rigen las aplicaciones en Internet (el correo, la web, etc.). Finalmente, el módulo "Co-

municaciones inalámbricas" profundiza en el conocimiento de las comunicaciones sin hilos que se están convirtiendo en el eje principal de las tecnologías de red actuales.



## **Bibliografía**

**Kurose, J.; Ross, K.** (2005). *Computer Networking: a top-down approach featuring the Internet* (5.<sup>a</sup> ed.). Boston: Addison-Wesley Publishing Company.

**Tanenbaum, A. S.** (2003). *Redes de computadores* (4.<sup>a</sup> ed.). Nueva York: Prentice-Hall Professional Technical Reference.

