Redes de Computadoras

Tercera edición

Andrew S. Tanenbaum

Vrije Universiteit
Amsterdam, The Netherlands

TRADUCCIÓN:

David Morales Peake

Traductor Profesional

REVISIÓN TÉCNICA:

Gabriel Guerrero Reyes

Doctor en Informática
Universidad de París VI

Pearson Educación

MÉXICO • ARGENTINA • BRASIL • COLOMBIA • COSTA RICA • CHILE
ESPAÑA • GUATEMALA • PERÚ • PUERTO RICO • VENEZUELA

EDICIÓN EN ESPAÑOL:

SUPERVISOR DE TRADUCCIÓN: TERESA SANZ FALCÓN
SUPERVISOR DE PRODUCCIÓN: ALEJANDRO A. GÓMEZ RUIZ

EDICIÓN EN INGLÉS:

Editorial/production manager: *Camille Trentacoste*
Interior design and composition: *Andrew S. Tanenbaum*
Cover design director: *Jerry Votta*
Cover designer: *Don Martinetti, DM Graphics, Inc.*
Cover concept: *Andrew S. Tanenbaum, from an idea by Marilyn Tremaine*
Interior graphics: *Hadel Studio*
Manufacturing manager: *Alexis R. Heydt*
Acquisitions editor: *Mary Franz*
Editorial Assistant: *Noreen Regina*

TANENBAUM: REDES DE COMPUTADORAS, 3a. Ed.

Prentice Hall Hispanoamericana, S.A.
Calle 4 Nº 25-2º piso Fracc. Ind. Alce Blanco,
Naucalpan de Juárez, Edo. de México,
C.P. 53370

ISBN 968-880-958-6

Miembro de la Cámara Nacional de la Industria Editorial, Reg. Núm. 1524.

Original English Language Edition Published by Prentice-Hall, Inc.
A Simon & Schuster Company

ISBN 0-13-349945-6

IMPRESO EN MÉXICO/PRINTED IN MEXICO

A Suzanne, Barbara, Marvin y el pequeño Bram

1

INTRODUCCIÓN

Los tres últimos siglos han estado dominados, cada uno de ellos, por una tecnología. El siglo XVIII fue la época de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la era de las máquinas de vapor. En el siglo XX, la tecnología clave ha sido la obtención, procesamiento y distribución de la información. Entre otros avances, hemos visto la instalación de redes telefónicas mundiales, la invención del radio y la televisión, el nacimiento y crecimiento sin precedentes de la industria de las computadoras y el lanzamiento de satélites de comunicación.

Debido al rápido progreso de la tecnología, estas áreas están convergiendo rápidamente, y las diferencias entre juntar, transportar, almacenar y procesar información desaparecen con rapidez. Las organizaciones con cientos de oficinas que se extienden sobre una amplia área geográfica esperan ser capaces de examinar la situación, aun de sus más remotos puestos de avanzada, oprimiendo un botón. Al crecer nuestra habilidad para obtener, procesar y distribuir información, también crece la demanda de técnicas de procesamiento de información más avanzadas.

Aunque la industria de la computación es joven comparada con otras industrias (por ejemplo, las de automóviles y transporte aéreo), las computadoras han logrado un progreso espectacular en un tiempo corto. Durante las dos primeras décadas de su existencia, los sistemas de cómputo eran altamente centralizados, por lo general, dentro de un cuarto grande. En muchos casos, este cuarto tenía paredes de vidrio a través de las cuales los visitantes podían asombrarse de la gran maravilla electrónica que se encontraba dentro. Una compañía de tamaño mediano o

una universidad tenía una o dos computadoras, mientras que una institución grande tenía cuando mucho unas cuantas docenas. La idea de que dentro de 20 años se pudieran producir en masa, por millones, computadoras de igual capacidad más pequeñas que las estampillas de correo, era pura ciencia ficción.

La fusión de las computadoras y las comunicaciones ha tenido una profunda influencia en la forma en que los sistemas de cómputo se organizan. El concepto de "centro de cómputo" como cuarto con una gran computadora a la cual los usuarios traían sus trabajos para procesar es ahora totalmente obsoleto. El viejo modelo de una sola computadora que atendía todas las necesidades de computación de la organización ha sido reemplazado por uno en el cual un gran número de computadoras separadas pero interconectadas hacen el trabajo. Estos sistemas se llaman **redes de computadoras**. El diseño y organización de estas redes es el tema de este libro.

A lo largo del libro usaremos el término "red de computadoras" para referirnos a una colección *interconectada* de computadoras *autónomas*. Se dice que dos computadoras están interconectadas si son capaces de intercambiar información. La conexión no tiene que ser por medio de un alambre de cobre; puede usarse fibra óptica, microondas y satélites de comunicación. Al indicar que las computadoras son autónomas, queremos excluir de nuestra definición a los sistemas en los que existe una clara relación amo-esclavo. Si una computadora puede arrancar, parar o controlar otra a voluntad, las computadoras no son autónomas. Un sistema con una unidad de control y muchos esclavos no es una red; tampoco lo es una computadora grande con impresoras y terminales remotas.

Existe en la bibliografía sobre el tema considerable confusión entre la red de computadoras y un **sistema distribuido**. La diferencia radica en que en el sistema distribuido la existencia de múltiples computadoras autónomas es transparente para el usuario (es decir, no es visible). El usuario puede teclear una orden para ejecutar un programa y éste se ejecutará. La tarea de seleccionar el mejor procesador, encontrar y transportar todos los archivos de entrada al procesador y poner los resultados en el lugar apropiado, corresponde al sistema operativo.

En otras palabras, el usuario de un sistema distribuido no está consciente de que haya múltiples procesadores; más bien, ve al sistema como un monoprocesador virtual. La asignación de trabajos a procesadores y de archivos a discos, el movimiento de archivos entre el lugar donde se almacenan y donde son necesarios, y todas las demás funciones del sistema, deben ser automáticas.

En una red, el usuario debe ingresar de forma *explícita* en una máquina, enviar los trabajos remotos *explícitamente*, mover *explícitamente* los archivos y, en general, llevar a cabo de manera personal el manejo de la red. En un sistema distribuido nada se tiene que hacer de forma explícita; el sistema lo hace todo automáticamente sin que el usuario tenga conocimiento de ello.

En efecto, un sistema distribuido es un sistema de *software* construido encima de una red, a la que el *software* confiere un alto grado de cohesión y transparencia. Así, la distinción entre una red y un sistema distribuido tiene que ver con el *software* más que con el *hardware* (especialmente el sistema operativo).

No obstante, los dos temas se superponen de manera considerable. Por ejemplo, tanto un sistema distribuido como una red de computadoras necesitan transferir archivos. La diferencia está en quién invoca la transferencia, el sistema o el usuario. Aunque el enfoque fundamental de

este libro es hacia las redes, muchos de los temas también son importantes en sistemas distribuidos. Si se desea mayor información sobre sistemas distribuidos, véase (Coulouris *et al.*, 1994; Mullender, 1993; y Tanenbaum, 1995).

1.1. USOS DE LAS REDES DE COMPUTADORAS

Antes de empezar a examinar los aspectos técnicos en detalle, es importante dedicar algún tiempo a entender por qué la gente está interesada en las redes de computadoras y para qué puede usarlas.

1.1.1. Redes para compañías

Muchas organizaciones tienen una cantidad importante de computadoras en operación, con frecuencia alejadas entre sí. Por ejemplo, una compañía con muchas fábricas puede tener una computadora en cada localidad para llevar el control de los inventarios, vigilar la productividad y pagar la nómina local. Inicialmente, cada una de estas computadoras puede haber trabajado aislada de las otras, pero en algún momento la gerencia decidió conectarlas para poder extraer y correlacionar información acerca de toda la compañía.

En términos más generales, la cuestión aquí es **compartir los recursos** y la meta es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red, sin importar la localización física de los recursos y de los usuarios. En otras palabras, el hecho de que un usuario esté a 1000 km de distancia de sus datos no deberá impedirle usar los datos como si fueran locales. Este objetivo puede resumirse diciendo que es un intento por acabar con la "tiranía de la geografía".

Una segunda meta es lograr una **alta confiabilidad** al contar con fuentes alternativas de suministro. Por ejemplo, todos los archivos podrían replicarse en dos o tres máquinas; así, si una de ellas no está disponible (debido a una falla del *hardware*), podrán usarse las otras copias. Además, la existencia de múltiples CPU significa que si una de ellas falla, las otras serán capaces de hacer su trabajo, aunque se reduzca el rendimiento. En aplicaciones militares, bancarias, de control de tráfico aéreo, seguridad de reactores nucleares y muchas otras, la capacidad para continuar operando pese a problemas de *hardware* es de suma importancia.

Otra meta es **ahorrar dinero**. Las computadoras pequeñas tienen una relación precio/rendimiento mucho mejor que las grandes. Las *mainframes* (computadoras del tamaño de un cuarto) son aproximadamente 10 veces más rápidas que las computadoras personales, pero cuestan mil veces más. Este desequilibrio ha ocasionado que muchos diseñadores construyan sistemas compuestos por computadoras personales, una por usuario, con los datos guardados en una o más máquinas **servidoras de archivos** compartidas. En este modelo, los usuarios se denominan **clientes**, y el arreglo completo se llama **modelo cliente-servidor**. Esto se ilustra en la figura 1-1.

En el modelo cliente-servidor, la comunicación generalmente adopta la forma de un mensaje de solicitud del cliente al servidor pidiendo que se efectúe algún trabajo. A continuación, el

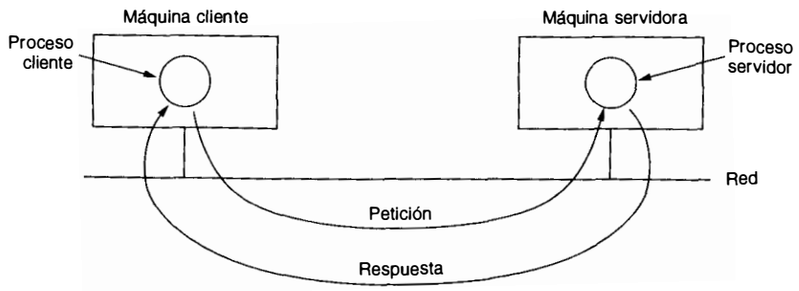

Figura 1-1. El modelo cliente-servidor.

servidor hace el trabajo y devuelve la respuesta. Por lo regular, muchos clientes utilizan un número pequeño de servidores.

Otra meta al establecer redes es la escalabilidad: la capacidad para incrementar el rendimiento del sistema gradualmente cuando la carga de trabajo crece, añadiendo solamente más procesadores. En el caso de *mainframes* centralizadas, cuando el sistema esté lleno hay que reemplazarlo por uno mayor, usualmente más caro, lo que implica largas interrupciones para los usuarios. Con el modelo cliente-servidor se pueden añadir nuevos clientes y nuevos servidores cuando es necesario.

Un objetivo más del establecimiento de una red de computadoras tiene poco que ver con la tecnología. Una red de computadoras puede proporcionar un potente **medio de comunicación** entre empleados que están muy distantes. Al usar una red, es fácil para dos o más personas que viven lejos escribir un informe juntas. Cuando un trabajador hace un cambio a un documento en línea, los demás pueden ver el cambio inmediatamente, sin tener que esperar varios días la llegada de una carta. Tal rapidez hace fácil la cooperación entre grupos de gente muy apartada, cosa que previamente era imposible. A largo plazo, el uso de redes para mejorar la comunicación entre las personas probablemente resultará más importante que las metas técnicas tales como la mejora de la confiabilidad.

1.1.2. Redes para la gente

Todas las motivaciones arriba citadas para construir redes de computadoras son de naturaleza esencialmente económica y tecnológica. Si *mainframes* suficientemente grandes y potentes estuvieran disponibles a precios aceptables, muchas compañías habrían optado por guardar todos sus datos en ellas y proporcionar a sus empleados terminales conectadas a estas máquinas. En la década de 1970 y a principios de la de 1980, casi todas las compañías operaban de esta forma. Las redes de computadoras llegaron a ser populares únicamente cuando las computadoras personales ofrecieron una descomunal ventaja precio/rendimiento sobre las *mainframes*.

Al iniciar la década de 1990, las redes de computadoras comenzaron a prestar servicios a particulares en su hogar. Estos servicios y la motivación para usarlos son muy diferentes del

modelo de "eficiencia corporativa" descrito en la sección anterior. A continuación esbozaremos tres de los más estimulantes aspectos de esta evolución:

1. Acceso a información remota.
2. Comunicación de persona a persona.
3. Entretenimiento interactivo.

El acceso a la información remota vendrá en muchas formas. Un área en la cual ya está sucediendo es el acceso a las instituciones financieras. Mucha gente paga sus facturas, administra sus cuentas bancarias y maneja sus inversiones en forma electrónica. Las compras desde el hogar se están haciendo populares, con la facilidad de inspeccionar los catálogos en línea de miles de compañías. Algunos de estos catálogos pronto ofrecerán un vídeo instantáneo de cualquier producto que se pueda ver con sólo hacer clic en el nombre del producto.

Los periódicos se publicarán en línea y serán personalizados. Podremos decirle al periódico que queremos saber todo lo que haya acerca de los políticos corruptos, los grandes incendios, los escándalos de celebridades y las epidemias, pero nada de fútbol, gracias. En la noche mientras usted duerme, el periódico se bajará al disco de su computadora o se imprimirá en su impresora láser. A pequeña escala, este servicio ya existe. El siguiente paso más allá de los periódicos (y de las revistas y publicaciones científicas) es la biblioteca digital en línea. Dependiendo del costo, tamaño y peso de las computadoras portátiles, los libros impresos quizá lleguen a ser obsoletos. Quienes lo duden deberían tomar nota de las consecuencias de la imprenta sobre los manuscritos medievales iluminados.

Otra aplicación en esta categoría es el acceso a sistemas de información como la actual red mundial (*World Wide Web*), la cual contiene información sobre arte, negocios, cocina, gobierno, salud, historia, aficiones, recreación, ciencia, deportes, viajes y muchos otros temas, demasiado numerosos para mencionarlos aquí.

Todas las aplicaciones antes mencionadas implican la interacción entre una persona y una base de datos remota. La segunda categoría extensa de redes que se usará implica la interacción persona a persona, básicamente la respuesta del siglo XXI al teléfono del siglo XIX. Millones de personas utilizan ya el correo electrónico o **email** y pronto contendrá en forma rutinaria audio y vídeo además de texto. El perfume en los mensajes tardará un poco más en perfeccionarse.

El correo electrónico de tiempo real permitirá a los usuarios remotos comunicarse sin retraso, posiblemente viéndose y escuchándose. Esta tecnología hace posible realizar reuniones virtuales, llamadas **videoconferencias**, entre gente muy alejada. A veces se dice que el transporte y la comunicación están en competencia, y cualquiera que gane hará al otro obsoleto. Las reuniones virtuales podrán servir para recibir enseñanza remota, obtener opiniones médicas de especialistas distantes y otras muchas aplicaciones.

Los grupos de noticias a nivel mundial, con discusiones sobre todos los temas concebibles, son ya comunes entre un grupo selecto de personas, y esto crecerá para incluir a la población en general. Estas discusiones en las cuales una persona pone un mensaje y los demás suscriptores al grupo de noticias pueden leerlo, van desde lo humorístico hasta lo apasionado.

La tercera categoría es el entretenimiento, que es una industria enorme y en crecimiento. La aplicación irresistible aquí (y que puede impulsar a todas las demás) es el vídeo por solicitud. Dentro de aproximadamente una década, será posible seleccionar cualquier película o programa de televisión creado en cualquier país y exhibirlo en la pantalla de forma instantánea. Algunas películas nuevas llegarán a ser interactivas, preguntándose al usuario ocasionalmente qué dirección debe seguir la historia (¿deberá MacBeth asesinar a Duncan o esperar su momento?) con argumentos alternativos para todos los casos. La televisión en vivo también puede llegar a ser interactiva, con el auditorio participando en concursos, escogiendo entre los concursantes, etcétera.

Por otro lado, tal vez la aplicación irresistible no sea la petición de vídeos, sino los juegos. Tenemos ya juegos de simulación en tiempo real multipersonales, como las aventuras en calabozos virtuales, y simuladores de vuelo en los que los jugadores de un equipo tratan de derribar a los del equipo contrario. Si esto se hace con anteojos que muestren imágenes en movimiento con calidad fotográfica en tiempo real tridimensional, tendremos una especie de realidad virtual compartida mundial.

En pocas palabras, la capacidad para combinar información, comunicación y entretenimiento seguramente hará surgir una nueva y enorme industria basada en las redes de computadoras.

1.1.3. Consideraciones sociales

La introducción ampliamente difundida de redes significará nuevos problemas sociales, éticos y políticos (Laudon, 1995). Sólo mencionaremos en forma breve algunos de ellos; un estudio minucioso requiere un libro completo, por lo menos. Una característica popular de muchas redes son los grupos de noticias o quioscos de anuncios en los que la gente puede intercambiar mensajes con individuos de gustos parecidos. Mientras los temas estén restringidos a asuntos técnicos o aficiones como la jardinería, no se presentarán muchos problemas.

El problema surge cuando los grupos de noticias tratan temas que a la gente en verdad le importan, como la política, la religión o el sexo. Las opiniones expresadas en tales grupos pueden ser profundamente ofensivas para algunas personas. Además, los mensajes no necesariamente están limitados al texto. Fotografías a color de alta definición e incluso pequeños *videoclips* pueden transmitirse ahora con facilidad por las redes de computadoras. Algunas personas adoptan una postura de vive y deja vivir pero otras sienten que enviar cierto material (por ejemplo, pornografía infantil) es simplemente inaceptable. Así pues, el debate sigue causando furor.

Hay gente que ha demandado a los operadores de redes, reclamando que son responsables por el contenido de lo que aquéllas acarrean, como los periódicos y revistas. La respuesta inevitable es que una red es como una compañía de teléfonos o como la oficina de correos y no puede esperarse que los operadores vigilen lo que los usuarios dicen. Por otro lado, si se obligara a los operadores de redes a censurar los mensajes, probablemente optarían por eliminar cualquier cosa que tuviera la más leve posibilidad de causar una demanda en su contra y por tanto violarían el derecho de los usuarios a hablar con libertad. Lo más seguro es que este debate continuará durante un tiempo.

Otra área divertida es el conflicto entre los derechos de los empleados y los derechos de los patrones. Muchas personas leen y escriben correo electrónico en su trabajo. Algunos patrones han reclamado el derecho a leer y posiblemente censurar los mensajes de los empleados, incluidos los mensajes enviados desde una terminal casera después de horas de trabajo. No todos los empleados están de acuerdo con esto (Sipior y Ward, 1995).

Aun si los patrones tienen poder sobre los empleados, ¿esta relación también gobierna a universidades y estudiantes? ¿Y qué hay acerca de las preparatorias y sus estudiantes? En 1994, la Universidad Carnegie-Mellon decidió bloquear la entrada de mensajes de algunos grupos de noticias que trataban el sexo porque la universidad sintió que el material era inapropiado para menores (es decir, los pocos estudiantes que tenían menos de 18 años). Las repercusiones de este suceso tardarán años en disiparse.

Las redes de computadoras ofrecen la posibilidad de enviar mensajes anónimos. En algunas situaciones, esta capacidad puede ser deseable. Por ejemplo, proporciona un mecanismo para que estudiantes, militares, empleados y ciudadanos llamen la atención sobre comportamientos ilegales por parte de profesores, oficiales, superiores y políticos sin miedo a represalias. Por otro lado, en Estados Unidos y muchas otras democracias la ley otorga específicamente a una persona acusada el derecho de enfrentar y recusar a su acusador en los tribunales. Las acusaciones anónimas no pueden aceptarse como pruebas.

En pocas palabras, las redes de computadoras, igual que la imprenta hace 500 años, permiten a los ciudadanos comunes distribuir sus puntos de vista en diferentes formas y a diferentes públicos que antes estaban fuera de su alcance. Esta nueva libertad trae consigo muchos problemas sociales, políticos y morales aún no resueltos. La resolución de estos problemas se deja como ejercicio para el lector.

1.2. *HARDWARE* DE RED

Ahora es tiempo de dejar a un lado las aplicaciones y los aspectos sociales de las redes para enfocarnos a los problemas técnicos que implica su diseño. No existe una taxonomía generalmente aceptada dentro de la cual quepan todas las redes de computadoras, pero dos dimensiones sobresalen como importantes: la tecnología de transmisión y la escala. Examinaremos ahora cada una de ellas por turno.

En términos generales, hay dos tipos de tecnología de transmisión:

1. Redes de difusión.
2. Redes punto a punto.

Las **redes de difusión** tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los mensajes cortos (llamados **paquetes** en ciertos contextos) que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir un paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a alguna otra máquina, lo ignora.

Como analogía, consideremos a una persona de pie e inmóvil al final de un corredor que da acceso a muchos cuartos y que grita: "Watson, ven aquí, te necesito". Aunque en realidad mucha gente puede recibir (oír) el paquete, únicamente Watson responderá; los otros lo ignorarán. Otro ejemplo es un anuncio en el aeropuerto, pidiendo a todos los pasajeros del vuelo 644 que se presenten en la sala 12.

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a *todos* los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama **difusión** (*broadcasting*). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo conocido como **multidifusión**. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes $n - 1$ bits de dirección pueden contener un número de grupo. Cada máquina se puede "suscribir" a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las máquinas que se suscribieron a ese grupo.

En contraste, las redes **punto a punto** consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo desempeñan un papel importante en las redes punto a punto. Como regla general (aunque hay muchas excepciones), las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

Distancia entre procesadores	Procesadores ubicados en el (la) mismo(a)	Ejemplo
0.1 m	Tarjeta de circuitos	Máquina de flujo de datos
1 m	Sistema	Multicomputadora
10 m	Cuarto	Red de área local
100 m	Edificio	
1 km	Campus	
10 km	Ciudad	Red de área metropolitana
100 km	País	Red de área amplia
1,000 km	Continente	
10,000 km	Planeta	La Internet

Figura 1-2. Clasificación de procesadores interconectados según su escala.

Un criterio alterno para clasificar las redes es su escala. En la figura 1-2 damos una clasificación de los sistemas de múltiples procesadores de acuerdo con su tamaño físico. En la parte superior están las **máquinas de flujo de datos**, computadoras con alto grado de paralelismo y muchas unidades funcionales, todas trabajando en el mismo programa. A continuación vienen las **multicomputadoras**, sistemas que se comunican enviando mensajes por *buses* muy cortos y

rápidos. Más allá de las multicomputadoras están las verdaderas redes, computadoras que se comunican intercambiando mensajes por cables largos. Éstas pueden dividirse en redes locales, metropolitanas y de área amplia. Finalmente, la conexión de dos o más redes es una interred. La red Internet, de alcance mundial, es un ejemplo muy conocido de interred. La distancia es importante como medio de clasificación porque se usan diferentes técnicas a diferentes escalas. En este libro nos ocuparemos únicamente de las redes verdaderas y de su interconexión. A continuación presentamos una breve introducción al tema de *hardware* de red.

1.2.1. Redes de área local

Las **redes de área local**, generalmente llamadas **LAN** (*local area networks*), son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de compañías y fábricas con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características: (1) su tamaño, (2) su tecnología de transmisión, y (3) su topología.

Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos, y también simplifica la administración de la red.

Las LAN a menudo usan una tecnología de transmisión que consiste en un cable sencillo al cual están conectadas todas las máquinas, como las líneas compartidas de la compañía telefónica que solían usarse en áreas rurales. Las LAN tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores. Las LAN más nuevas pueden operar a velocidades muy altas, de hasta cientos de megabits/seg. En este libro nos apegamos a la tradición y medimos la velocidad de las líneas en megabits/seg (Mbps), no megabytes/seg (MB/seg). Un megabit es 1,000,000 bits, no 1,048,576 (2^{20}) bits.

Las LAN de transmisión pueden tener diversas topologías; la figura 1-3 muestra dos de ellas. En una red de *bus* (esto es, un cable lineal), en cualquier instante una computadora es la

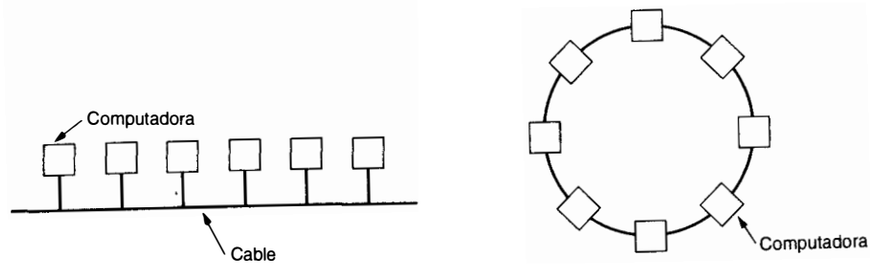

Figura 1-3. Dos redes de difusión. (a) *Bus*. (b) Anillo.

máquina maestra y puede transmitir; se pide a las otras máquinas que se abstengan de enviar mensajes. Es necesario un mecanismo de arbitraje para resolver conflictos cuando dos o más máquinas quieren transmitir simultáneamente. El mecanismo de arbitraje puede ser centralizado o distribuido. Por ejemplo, la IEEE 802.3, popularmente llamada **Ethernet**MR, es una red de transmisión basada en *bus* con control de operación descentralizado a 10 o 100 Mbps. Las computadoras de una Ethernet pueden transmitir cuando quieran; si dos o más paquetes chocan, cada computadora sólo espera un tiempo al azar y lo vuelve a intentar.

Un segundo tipo de sistema de difusión es el anillo. En un anillo, cada bit se propaga por sí mismo, sin esperar al resto del paquete al cual pertenece. Típicamente, cada bit recorre el anillo entero en el tiempo que toma transmitir unos pocos bits, a veces antes de que el paquete completo se haya transmitido. Como en todos los sistemas de difusión, se necesitan reglas para arbitrar el acceso simultáneo al anillo. Se emplean varios métodos que se analizarán más adelante en este libro. La IEEE 802.5 (el *token ring* de IBM), es una popular LAN basada en anillo que opera a 4 y 16 Mbps.

Las redes de difusión se pueden dividir también en estáticas y dinámicas, dependiendo de cómo se asigna el canal. Una asignación estática típica divide el tiempo en intervalos discretos y ejecuta un algoritmo de asignación cíclica, permitiendo a cada máquina transmitir únicamente cuando le llega su turno. La asignación estática desperdicia la capacidad del canal cuando una máquina no tiene nada que decir durante su segmento asignado, por lo que muchos sistemas intentan asignar el canal dinámicamente (es decir, por demanda).

Los métodos de asignación dinámica para un canal común son centralizados o descentralizados. En el método de asignación de canal centralizado hay una sola entidad, por ejemplo una unidad de arbitraje del *bus*, la cual determina quién es el siguiente. Podría hacer esto aceptando peticiones y tomando una decisión de acuerdo con un algoritmo interno. En el método de asignación de canal descentralizado no hay una entidad central; cada máquina debe decidir por sí misma si transmite o no. Podríamos pensar que esto siempre conduce al caos, pero no es así. Más adelante estudiaremos muchos algoritmos diseñados para poner orden en el caos potencial.

El otro tipo de LAN se construye con líneas punto a punto. Las líneas individuales conectan una máquina específica a otra. Una LAN así es realmente una red de área amplia en miniatura. Veremos esto posteriormente.

1.2.2. Redes de área metropolitana

Una **red de área metropolitana**, o **MAN** (*metropolitan area network*) es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública. Una MAN puede manejar datos y voz, e incluso podría estar relacionada con la red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales. Al no tener que conmutar, se simplifica el diseño.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este estándar ya se está implementando: se llama **DQDB**

(*distributed queue dual bus*, o ***bus* dual de cola distribuida**) o, para la gente que prefiere números a letras, 802.6 (el número de la norma IEEE que lo define). El DQDB consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras, como se muestra en la figura 1-4. Cada *bus* tiene una cabeza terminal (*head-end*), un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el *bus* superior. El tráfico hacia la izquierda usa el de abajo.

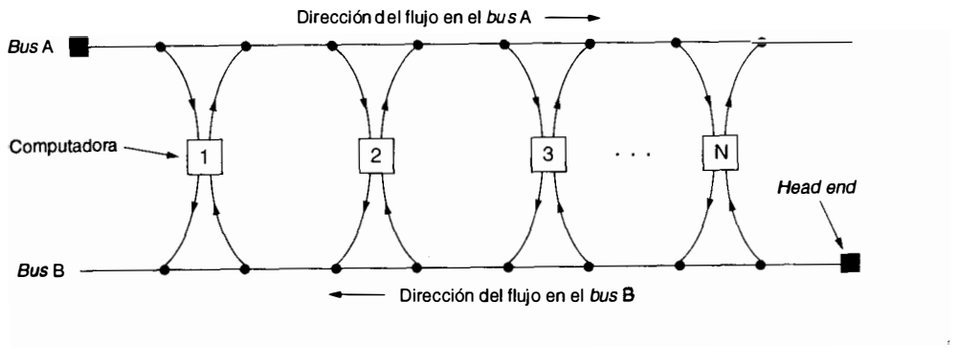

Figura 1-4. Arquitectura de la red de área metropolitana DQDB.

Un aspecto clave de las MAN es que hay un medio de difusión (dos cables, en el caso de la 802.6) al cual se conectan todas las computadoras. Esto simplifica mucho el diseño comparado con otros tipos de redes. Estudiaremos el DQDB con más detalle en el capítulo 4.

1.2.3. Redes de área amplia

Una **red de área amplia**, o **WAN** (*wide area network*), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (es decir, de aplicación). Seguiremos el uso tradicional y llamaremos a estas máquinas ***hosts***. El término **sistema terminal** (*end system*) se utiliza también ocasionalmente en la literatura. Las *hosts* están conectadas por una **subred de comunicación**, o simplemente **subred**. El trabajo de la subred es conducir mensajes de una *host* a otra, así como el sistema telefónico conduce palabras del que habla al que escucha. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (las *hosts*), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas **circuitos**, **canales** o **troncales**) mueven bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Desafortunadamente, no hay una

terminología estándar para designar estas computadoras; se les denomina **nodos conmutadores de paquetes**, **sistemas intermedios** y **centrales de conmutación de datos**, entre otras cosas. Como término genérico para las computadoras de conmutación, usaremos la palabra **enrutador**, pero conviene que el lector quede advertido de que no hay consenso sobre la terminología. En este modelo, mostrado en la figura 1-5, cada *host* generalmente está conectada a una LAN en la cual está presente un enrutador, aunque en algunos casos una *host* puede estar conectada directamente a un enrutador. La colección de líneas de comunicación y enrutadores (pero no las *hosts*) forman la subred.

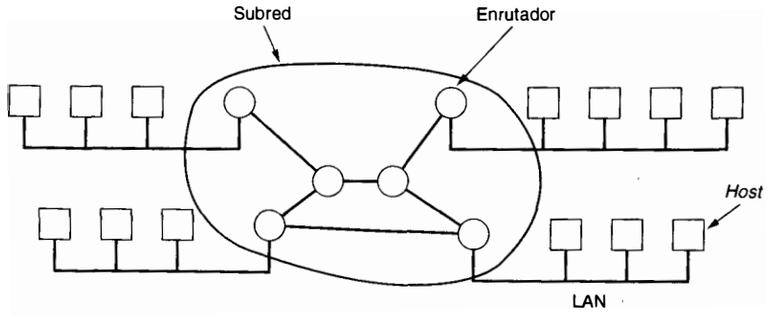

Figura 1-5. Relación entre las *hosts* y la subred.

Es pertinente un comentario al margen acerca del término "subred". Originalmente, sólo significaba la colección de enrutadores y líneas de comunicación que movían los paquetes de la *host* de origen a la *host* de destino. Sin embargo, algunos años después surgió un segundo significado en relación con la identificación de direcciones en la red (lo cual trataremos en el capítulo 5). Así, el término tiene cierta ambigüedad. Desafortunadamente, no existen opciones ampliamente aceptadas para su significado inicial, de modo que muy a pesar nuestro lo usaremos en ambos sentidos. Por el contexto, siempre quedará claro lo que significa la palabra.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de enrutadores. Si dos enrutadores que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de **punto a punto**, de **almacenar y reenviar**, o de **paquete conmutado**. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse **celdas**.

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del enrutador. La figura 1-6 muestra algunas posibles topologías. Las redes locales que fueron diseñadas como tales usualmente tienen una topología simétrica. En contraste, las redes de área amplia típicamente tienen topologías irregulares.

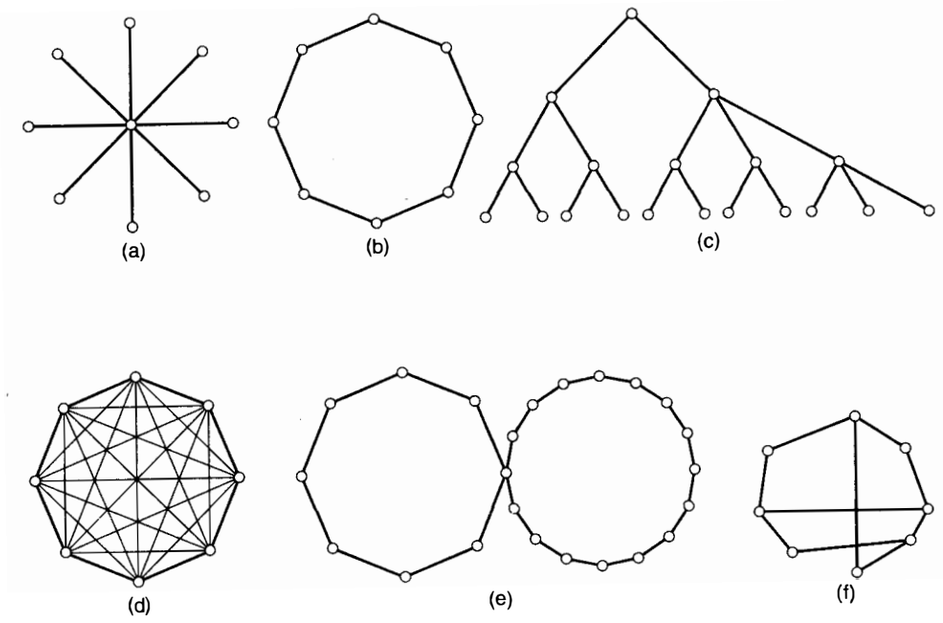

Figura 1-6. Posibles topologías para una subred punto a punto. (a) Estrella. (b) Anillo. (c) Árbol. (d) Completa. (e) Intersección de anillos. (f) Irregular.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada enrutador tiene una antena por medio de la cual puede enviar y recibir. Todos los enrutadores pueden oír las salidas enviadas *desde* el satélite y en algunos casos pueden también oír la transmisión ascendente de los otros enrutadores *hacia* el satélite. Algunas veces los enrutadores están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

1.2.4. Redes inalámbricas

Las computadoras portátiles, como las *notebooks* y los asistentes personales digitales (PDAs, *personal digital assistants*), son el segmento de más rápido crecimiento de la industria de la computación. Muchos de los dueños de estas computadoras tienen máquinas de escritorio conectadas a LAN y WAN en la oficina y quieren estar conectados a su base de operaciones aun cuando estén lejos de casa o de viaje. Puesto que tener una conexión por cable es imposible en autos y aeroplanos, existe mucho interés en las redes inalámbricas. En esta sección presentaremos brevemente el tema. (Nota: en este libro, consideramos secciones a las denotadas por un número de tres partes, como 1.2.4.)

En realidad, la comunicación inalámbrica digital no es una idea nueva. Ya en 1901 el físico italiano Guglielmo Marconi demostró un telégrafo inalámbrico de barco a costa usando el código Morse (los puntos y rayas son binarios, después de todo). Los sistemas inalámbricos digitales modernos tienen mejor rendimiento, pero la idea básica es la misma. Se puede encontrar información adicional acerca de estos sistemas en (Garg y Wilkes, 1996 y Pahlavan *et al.*, 1995).

Las redes inalámbricas tienen muchos usos. Uno común es la oficina portátil. La gente que viaja con frecuencia quiere usar su equipo electrónico portátil para enviar y recibir llamadas telefónicas, faxes y correo electrónico, leer archivos remotos, entrar en máquinas remotas etc., y hacer esto desde cualquier lugar ya sea en tierra, mar o aire.

Las redes inalámbricas son de gran valor para que las flotillas de camiones, taxis y autobuses, y las personas que hacen reparaciones, mantengan contacto con su base. También pueden usarlas los rescatistas en sitios de desastre (incendios, inundaciones, temblores, etc.) donde se ha dañado el sistema telefónico. Las computadoras pueden enviar mensajes, guardar registros, y muchas otras cosas.

Por último, las redes inalámbricas son importantes para los militares. Si hay necesidad de combatir en cualquier parte del mundo con poco tiempo de aviso, contar con el uso de la infraestructura local de las redes probablemente no sea una buena idea. Es mejor llevar una red propia.

Aunque las redes inalámbricas y las computadoras portátiles con frecuencia están relacionadas, no son idénticas, como lo muestra la figura 1-7. Las computadoras portátiles en ocasiones se conectan a redes alambradas. Por ejemplo, si un viajero conecta una computadora portátil al enchufe telefónico de un hotel, disfruta de movilidad sin una red inalámbrica. Otro ejemplo es cuando se lleva una computadora portátil mientras se inspecciona un tren en busca de problemas técnicos. Aquí el inspector puede arrastrar un cordón largo tras de sí (modelo "aspiradora").

Inalámbrica	Móvil	Aplicaciones
No	No	Estaciones de trabajo estacionarias en oficinas
No	Sí	Uso de una portátil en un hotel; mantenimiento de trenes
Sí	No	LAN en edificios viejos y sin alambrado
Sí	Sí	Oficina portátil; PDA para inventarios

Figura 1-7. Combinación de redes inalámbricas y computación móvil.

Por otro lado, algunas computadoras inalámbricas no son portátiles. Un ejemplo importante es una compañía que posee una construcción vieja, que no tiene instalado cable para red y quiere conectar sus computadoras. Para instalar una LAN inalámbrica sólo necesita comprar una pequeña caja con algo de electrónica y armar algunas antenas. Esta solución puede ser más económica que alambrar el edificio.

Aunque las LAN inalámbricas son fáciles de instalar, también tienen desventajas. Típicamente, su capacidad es de 1 a 2 Mbps, lo cual es mucho más lento que las LAN alambradas. Además las tasas de error son a veces mucho más altas, y las transmisiones desde diferentes computadoras pueden interferirse.

Desde luego, también están las aplicaciones inalámbricas verdaderamente móviles, que van desde la oficina portátil hasta personas que recorren una tienda haciendo el inventario con una PDA. En muchos aeropuertos concurridos, los empleados que reciben carros rentados trabajan en los estacionamientos con computadoras portátiles inalámbricas. Ellos teclean el número de matrícula de los carros devueltos, y su portátil, que tiene una impresora integrada, llama a la computadora principal, obtiene la información de la renta e imprime la factura allí mismo. La verdadera computación móvil se estudia más a fondo en (Forman y Zahorjan, 1994).

Las redes inalámbricas tienen muchas formas. Algunas universidades ya están instalando antenas por todo su campus para permitir a los estudiantes sentarse debajo de los árboles y consultar las tarjetas del catálogo de la biblioteca. Aquí las computadoras se comunican directamente con las LAN inalámbricas en forma digital. Otra posibilidad es usar un teléfono celular (es decir, portátil) con un módem analógico tradicional. El servicio celular digital directo, llamado **CDPD** (*celular digital packet data*, **paquete de datos celular digital**), ya está disponible en muchas ciudades; lo estudiaremos en el capítulo 4.

Finalmente, es posible tener diferentes combinaciones de redes alámbricas e inalámbricas. Por ejemplo, en la figura 1-8(a), se muestra un aeroplano con varias personas usando módems y teléfonos fijos al asiento para llamar a la oficina. Cada llamada es independiente de las otras. Sin embargo, una opción mucho más eficiente es la LAN volante de la figura 1-8(b). Aquí cada asiento viene equipado con una conexión Ethernet a la cual los pasajeros pueden conectar sus computadoras. Un enrutador simple en el avión mantiene un enlace de radio con algún enrutador en tierra, cambiando de enrutador según avanza el vuelo. Esta configuración es una LAN tradicional, excepto que su conexión al mundo externo resulta ser un enlace de radio en lugar de una línea alambrada.

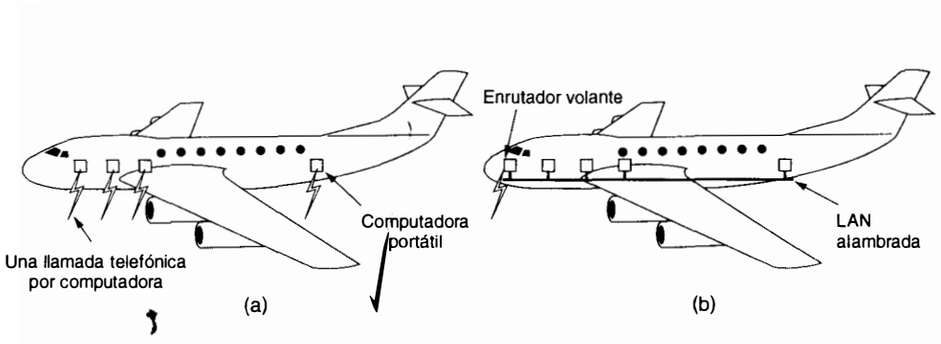

Figura 1-8. (a) Computadoras individuales móviles. (b) Una LAN volante.

Si bien muchas personas creen que las computadoras portátiles son la ola del futuro, se ha oído al menos una voz disidente. Bob Metcalfe, el inventor de la Ethernet, ha escrito: "Las computadoras móviles inalámbricas son como cuartos de baño móviles sin tubería: retretes portátiles. Llegarán a ser comunes en vehículos, en lugares de construcción y en conciertos de rock. Mi consejo es cablear su casa y permanecer ahí" (Metcalfe, 1995). ¿Seguirá la mayoría de la gente la advertencia de Metcalfe? El tiempo lo dirá.

1.2.5. Interredes

Existen muchas redes en el mundo, a veces con diferente *hardware* y *software*. La gente conectada a una red a menudo quiere comunicarse con gente conectada a una red distinta. Esto requiere conectar redes diferentes y con frecuencia incompatibles, algunas veces usando máquinas llamadas **pasarelas** para hacer la conexión y realizar la traducción necesaria, ambas en términos de *hardware* y *software*. Una colección de redes interconectadas se llama **interred**.

Una forma común de interred es una colección de LAN conectadas por una WAN. En efecto, si reemplazamos la etiqueta "subred" en la figura 1.5 por "WAN", nada más en la figura tendría que cambiar. En este caso la única distinción real entre una subred y una WAN es si están o no presentes las *hosts*. Si el sistema dentro de la curva cerrada contiene únicamente enrutadores, es una subred; si contiene tanto enrutadores como *hosts* con sus propios usuarios, es una WAN.

Para evitar confusión, por favor note que la palabra "interred"[1] siempre se usará en este libro en un sentido genérico. Por su parte, la **Internet** (note la I mayúscula) es una red específica mundial que se usa ampliamente para conectar universidades, oficinas de gobierno, compañías y finalmente individuos. Tendremos mucho que decir acerca de las interredes y la Internet más adelante en este libro.

Las subredes, redes e interredes con frecuencia se confunden. La subred tiene su sentido estándar en el contexto de una red de área amplia, donde se refiere a la colección de enrutadores y líneas de comunicación propiedad del operador de la red; por ejemplo, compañías como America Online y CompuServe. Como analogía, el sistema telefónico consiste en centrales telefónicas conectadas unas a otras por líneas de alta velocidad, y a casas y negocios por líneas de baja velocidad. Estas líneas y el equipo, propiedad de la compañía de teléfonos y administrado por ella, forman la subred del sistema telefónico. Los teléfonos por sí mismos (los nodos en esta analogía) no son parte de la subred. La combinación de una subred y sus nodos forma una red. En el caso de una LAN, el cableado y los nodos forman la red; realmente no hay subred.

Se forma una interred cuando se conectan distintas redes entre sí. Desde nuestro punto de vista, al conectar una LAN y una WAN o al conectar dos LAN formamos una interred, pero no hay mucho consenso en la industria acerca de la terminología en esta área.

1.3. *SOFTWARE* DE RED

Las primeras redes de computadoras se diseñaron con el *hardware* como preocupación principal y el *software* como una idea tardía. Esta estrategia ya no funciona; ahora el *software* de la red es altamente estructurado. En las siguientes secciones examinaremos en detalle la técnica de

[1] El comentario del autor se refiere a que el término "interred" corresponde en inglés a la palabra *internet* (naturalmente, con *i* minúscula, y que no debe confundirse con Internet, el nombre de la red mundial) o a *internetwork*. (*N. de supervisor.*)

estructuración del *software*. Los métodos descritos aquí son la piedra angular del libro entero y hablaremos de ellos repetidamente más adelante.

1.3.1. Jerarquías de protocolos

Para reducir la complejidad de su diseño, muchas redes están organizadas como una serie de **capas** o **niveles**, cada una construida sobre la inferior. El número de capas y el nombre, el contenido y la función de cada una difieren de red a red. Sin embargo, en todas las redes el propósito de cada capa es ofrecer ciertos servicios a las capas superiores de modo que no tengan que ocuparse del detalle de la implementación real de los servicios.

La capa *n* de una máquina lleva a cabo una conversación con la capa *n* de otra. Las reglas y convenciones que se siguen en esta conversación se conocen colectivamente como **protocolo** de la capa *n*. Básicamente, un protocolo es un acuerdo entre las partes que se comunican sobre cómo va a proceder la comunicación. Como analogía, cuando una mujer es presentada a un hombre, ella puede elegir entre extender su mano para saludar o no extenderla. Él, a su vez, puede decidir estrechar su mano o besarla, dependiendo, por ejemplo, de si ella es una abogada estadounidense en una reunión de negocios o una princesa europea en un baile de gala. Si se viola el protocolo, la comunicación será más difícil, si no imposible.

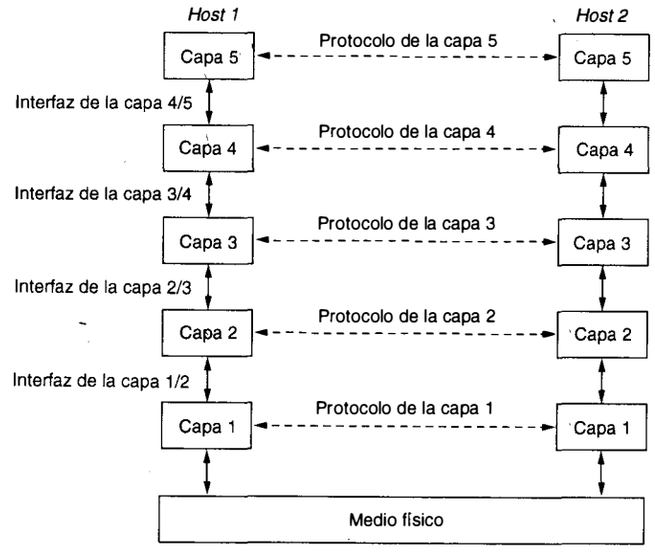

Figura 1-9. Capas, protocolos e interfaces.

En la figura 1-9 se ilustra una red de cinco capas. Las entidades que comprenden las capas correspondientes en las diferentes máquinas se denominan **pares**. En otras palabras, son los pares los que se comunican usando el protocolo.

En realidad, los datos no se transfieren directamente de la capa *n* de una máquina a la capa *n* de otra. Más bien, cada capa pasa datos e información de control a la capa que está inmediatamente debajo de ella, hasta llegar a la capa más baja. Bajo la capa 1 está el **medio físico** a través del cual ocurre la comunicación real. En la figura 1-9, se muestra en líneas punteadas la comunicación virtual y en líneas continuas la comunicación física.

Entre cada par de capas adyacentes hay una **interfaz**. La interfaz define cuáles operaciones y servicios primitivos ofrece la capa inferior a la superior. Cuando los diseñadores de redes deciden cuántas capas incluir en una red y lo que cada una debe hacer, una de las consideraciones más importantes es definir interfaces claras entre las capas. Esto requiere, a su vez, que cada capa ejecute una colección específica de funciones bien conocidas. Además de minimizar la cantidad de información que se debe pasar entre capas, las interfaces bien definidas también simplifican el reemplazo de la implementación de una capa con una implementación completamente diferente (por ejemplo, todas las líneas de teléfonos se reemplazan por canales de satélite), pues todo lo que se requiere de la nueva implementación es que ofrezca a su vecino de arriba exactamente el mismo conjunto de servicios que ofrecía la implementación vieja.

Un conjunto de capas y protocolos recibe el nombre de **arquitectura de red**. La especificación de una arquitectura debe contener información suficiente para que un implementador pueda escribir el programa o construir el *hardware* para cada capa de manera que cada una obedezca en forma correcta el protocolo apropiado. Ni los detalles de la implementación ni la especificación de las interfaces forman parte de la arquitectura porque se encuentran ocultas dentro de las máquinas y no son visibles desde fuera. Ni siquiera es necesario que las interfaces en todas las máquinas de una red sean iguales, siempre que cada máquina pueda usar correctamente todos los protocolos. La lista de protocolos empleados por cierto sistema, con un protocolo por capa, se llama **pila de protocolos**. Los temas de las arquitecturas de red, las pilas de protocolos y los protocolos mismos son la materia principal de este libro.

Una analogía puede ayudar a explicar la idea de la comunicación multicapas. Imagine a dos filósofos (procesos pares de la capa 3), uno de los cuales habla urdu e inglés y el otro habla chino y francés. Ya que no tienen un idioma en común, cada uno contrata un traductor (procesos pares de la capa 2), cada uno de los cuales, a su vez, establece contacto con una secretaria (procesos pares de la capa 1). El filósofo 1 desea comunicar a su par su afecto por el *oryctolagus cuniculus* (el conejo). Para hacerlo, pasa a su traductor un mensaje (en inglés), por conducto de la interfaz 2/3, que dice: "*I like rabbits*", como se ilustra en la figura 1-10. Los traductores acuerdan el uso de un idioma neutral, el holandés, así que el mensaje se convierte en "*Ik hou van konijnen*". El idioma elegido es el protocolo de la capa 2 y la elección corresponde a los procesos pares de la capa 2.

A continuación, el traductor entrega el mensaje a su secretaria para que lo transmita, por ejemplo, por fax (el protocolo de la capa 1). Cuando el mensaje llega, se traduce al francés y se pasa a través de la interfaz 2/3 al filósofo 2. Observe que cada protocolo es independiente por completo de los otros mientras las interfaces no cambien. Los traductores pueden cambiar a voluntad del holandés, por decir, al finlandés, siempre que ambos lo acuerden y que nada cambie su interfaz ya sea con la capa 1 o con la 3. De manera similar, las secretarias pueden cambiar de fax a correo electrónico o a teléfono sin molestar (o incluso sin informar) a las otras capas. Cada

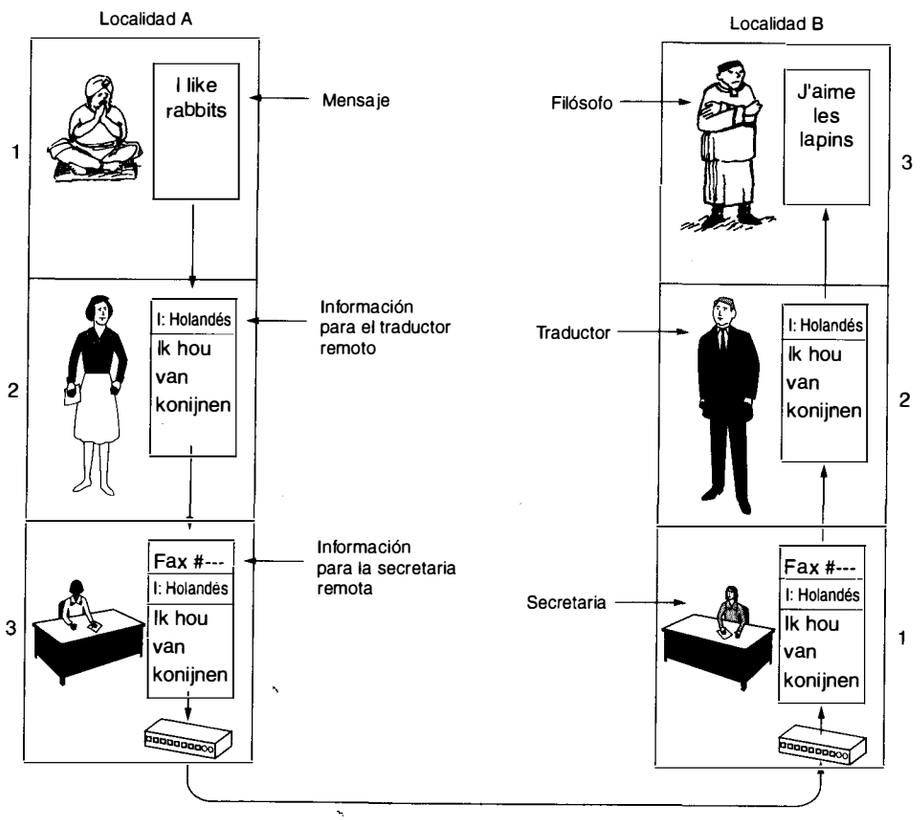

Figura 1-10. La arquitectura filósofo-traductor-secretaria.

proceso puede añadir algo de información dirigida únicamente a su par. Esta información no se pasa a la capa de arriba.

Consideremos ahora un ejemplo más técnico: cómo proveer la comunicación a la capa superior de la red de cinco capas de la figura 1-11. Se produce un mensaje *M* por un proceso de aplicación que se ejecuta en la capa 5 y se entrega a la capa 4 para su transmisión. La capa 4 coloca un **encabezado** al principio del mensaje para identificarlo y pasa el resultado a la capa 3. El encabezado incluye información de control, como números de secuencia, para que la capa 4 en la máquina de destino pueda entregar los mensajes en el orden correcto si las capas inferiores no mantienen la secuencia. En algunas capas, los encabezados contienen también tamaños, horas y otros campos de control.

En muchas redes no hay límite al tamaño de los mensajes que se transmiten en el protocolo de la capa 4, pero casi siempre existe un límite impuesto por el protocolo de la capa 3. En consecuencia, la capa 3 debe dividir los mensajes que le llegan en unidades más pequeñas,

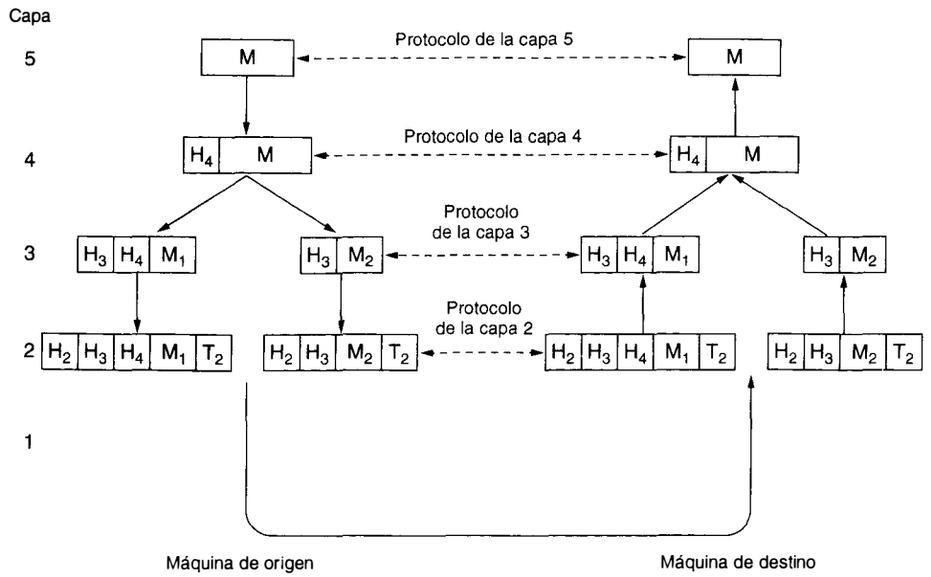

Figura 1-11. Ejemplo del flujo de información que apoya la comunicación virtual en la capa 5.

paquetes, anexando un encabezado de la capa 3 a cada paquete. En este ejemplo, *M* se divide en dos partes, M_1 y M_2.

La capa 3 decide cuál de las líneas que salen usará y pasa los paquetes a la capa 2. La capa 2 no solamente añade un encabezado a cada pieza sino también un apéndice, y entrega la unidad resultante a la capa 1 para su transmisión física. En la máquina receptora el mensaje se mueve hacia arriba, de capa en capa, perdiendo los encabezados conforme avanza. Ninguno de los encabezados para capas inferiores a la *n* pasa hasta la capa *n*.

Lo que es importante recordar de la figura 1-11 es la relación entre la comunicación virtual y la real y la diferencia entre protocolos e interfaces. Por ejemplo, los procesos pares de la capa 4 piensan que su comunicación es "horizontal" empleando el protocolo de la capa 4. Cada uno probablemente tiene un procedimiento llamado algo así como *EnvíaAlOtroLado* y *TomaDelOtroLado,* aunque en realidad estos procedimientos se comunican con capas más bajas a través de la interfaz 2/3, no con el otro lado.

La abstracción de procesos pares es básica para todo diseño de red. Al usarla, la inmanejable tarea de diseñar la red completa se puede dividir en varios problemas de diseño más chicos y manejables, es decir, el diseño de las capas individuales.

Aunque la sección 1.3 se llame "*Software* de red", conviene señalar que las capas más bajas de una jerarquía de protocolos con frecuencia se instrumentan en *hardware* o *firmware*. Sin embargo, implican algoritmos de protocolo complejos, aun si están incluidos (totalmente o en parte) en el *hardware*.

1.3.2. Consideraciones de diseño para las capas

Algunos de los problemas clave en el diseño de redes de computadoras se presentan en varias capas. A continuación mencionaremos en forma breve algunos de los más importantes.

Cada capa necesita un mecanismo para identificar emisores y receptores. Puesto que una red normalmente tiene muchas computadoras, algunas de las cuales tienen múltiples procesos, se requiere un mecanismo para que un proceso en una máquina especifique con quién quiere conversar. Como consecuencia de tener destinos múltiples, se necesita alguna forma de direccionamiento que permita determinar un destino específico.

Otro conjunto de decisiones de diseño concierne a las reglas de la transferencia de datos. En algunos sistemas, los datos viajan solamente en una dirección (**comunicación símplex**). En otros, los datos pueden viajar en cualquier dirección, pero no en forma simultánea (**comunicación semidúplex**). En otras más, los datos viajan en ambas direcciones a la vez (**comunicación dúplex**). El protocolo debe determinar también cuántos canales lógicos corresponden a la conexión y cuáles son sus prioridades. Muchas redes proveen al menos dos canales lógicos por conexión, uno para datos normales y otro para datos urgentes.

El control de errores es una consideración importante porque los circuitos de comunicación física no son perfectos. Se conocen muchos códigos de detección y de corrección de errores, pero ambos extremos de la conexión deben acordar cuál se va a usar. Además, el receptor debe tener alguna forma de indicar al emisor cuáles mensajes se han recibido correctamente y cuáles no.

No todos los canales de comunicación mantienen el orden de los mensajes que se envían. Para lidiar con una posible pérdida de secuencia, el protocolo debe incluir un mecanismo que permita al receptor volver a unir los pedazos en forma apropiada. Una solución obvia es numerar los pedazos, pero esta solución deja abierta la pregunta de qué se debe hacer con los pedazos que llegaron en desorden.

Una consideración importante en todos los niveles es cómo evitar que un emisor rápido sature de datos a un receptor lento. Se han propuesto varias soluciones y se verán más adelante. Algunas de ellas implican una realimentación del receptor al emisor, ya sea en forma directa o indirecta, respecto a la situación actual del receptor. Otras limitan al emisor a una velocidad de transmisión previamente convenida.

Otro problema que se debe resolver en varios niveles es la incapacidad de algunos procesos para aceptar mensajes de longitud arbitraria. Esta propiedad conduce a mecanismos para desensamblar, transmitir y después reensamblar los mensajes. Un problema relacionado es qué hacer cuando los procesos insisten en transmitir datos en unidades tan pequeñas que el envío de cada una por separado es ineficiente. La solución aquí es juntar varios mensajes pequeños dirigidos a un destino común en un solo mensaje largo y desmembrar el mensaje largo en el otro lado.

Cuando no es conveniente o económico establecer una conexión individual para cada par de procesos en comunicación, la capa inferior puede decidir usar la misma conexión para múltiples conversaciones, no relacionadas entre sí. Mientras esta multiplexión y desmultiplexión se haga de manera transparente, se puede usar con cualquier capa. La multiplexión se necesita en la capa

física, por ejemplo, donde se tiene que enviar todo el tráfico para todas las conexiones, cuando mucho, por unos cuantos circuitos físicos.

Cuando entre el origen y el destino hay múltiples trayectorias, se debe elegir una ruta. A veces esta decisión se debe dividir entre dos o más capas. Por ejemplo, para enviar datos de Londres a Roma, podría requerirse una decisión de alto nivel para pasar por Francia o por Alemania basándose en sus leyes de confidencialidad respectivas, y puede que se tuviera que tomar una decisión de bajo nivel para elegir uno de los muchos circuitos disponibles basándose en la carga de tráfico actual.

1.3.3. Interfaces y servicios

La función de cada capa es proporcionar servicios a la capa que está encima de ella. En esta sección veremos precisamente lo que es un servicio con más detalle, pero primero presentaremos algo de terminología.

Los elementos activos de cada capa generalmente se llaman **entidades**. Una entidad puede ser de *software* (como un proceso), o de *hardware* (como un circuito integrado inteligente de entrada/salida). Las entidades de la misma capa en máquinas diferentes se llaman **entidades pares**. Las entidades de la capa n implementan un servicio que usa la capa $n + 1$. En este caso la capa n se llama **proveedor del servicio** y la capa $n + 1$ es el **usuario del servicio**. La capa n puede usar los servicios de la capa $n - 1$ con el fin de proveer su propio servicio; puede ofrecer varias clases de servicio, por ejemplo: comunicación rápida cara y comunicación lenta barata.

Los servicios están disponibles en los **SAP** (*service access points,* **puntos de acceso al servicio**). Los SAP de la capa n son los lugares en los que la capa $n + 1$ puede tener acceso a los servicios ofrecidos. Cada SAP tiene una dirección que lo identifica de manera única. Para aclarar este punto, los SAP del sistema telefónico son los enchufes en los que se pueden conectar los teléfonos modulares, y las direcciones de los SAP son los números telefónicos de estas tomas. Para llamar a alguien necesitamos saber la dirección de SAP de quien debe recibir la llamada. De manera similar, en el sistema postal las direcciones de SAP son las direcciones de calle y de número de apartado postal. Para mandar una carta debemos conocer la dirección de SAP del destinatario.

Para que dos capas intercambien información, tiene que haber un acuerdo sobre el conjunto de reglas relativas a la interfaz. En una interfaz típica, la entidad de la capa $n + 1$ pasa una **IDU** (*interface data unit,* **unidad de datos de la interfaz**) a la entidad de la capa n a través del SAP como se muestra en la figura 1-12. La IDU consiste en una **SDU** (*service data unit,* **unidad de datos de servicio**) y cierta información de control. La SDU es la información que se pasa mediante la red a la entidad par y después hasta la capa $n + 1$. La información de control es necesaria para ayudar a la capa inferior a efectuar su trabajo (por ejemplo, la cantidad de bytes en la SDU) pero no forma parte de los datos mismos.

Para que se transfiera la SDU, la entidad de la capa n puede tener que fragmentarla en varios pedazos, a cada uno de los cuales se le da un encabezado y se envía como una **PDU** (*protocol data unit,* **unidad de datos de protocolo**) independiente, que podría ser un paquete. Las entidades pares usan los encabezados de las PDU para acarrear su protocolo de par. Los encabezados

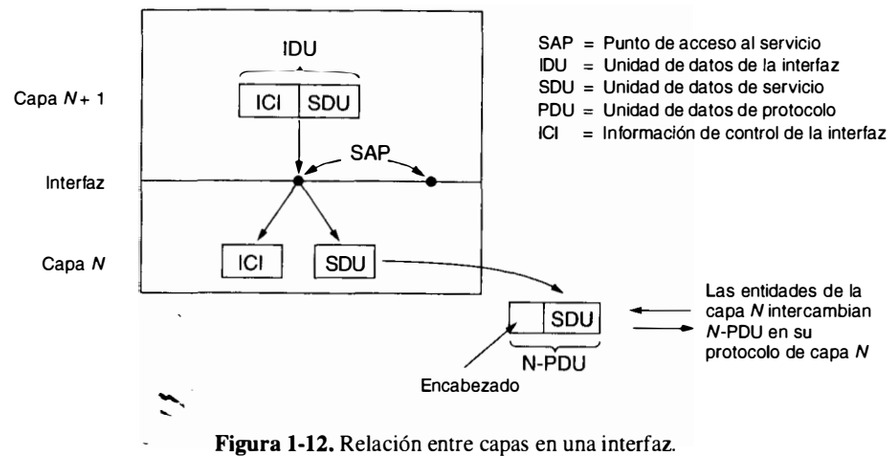

Figura 1-12. Relación entre capas en una interfaz.

indican cuáles PDU contienen datos y cuáles contienen información de control, proveen números de secuencia y cuentas, y otras cosas.

1.3.4. Servicios orientados a conexión y sin conexión

Las capas pueden ofrecer dos tipos diferentes de servicio a las capas que se encuentran sobre ellas, los orientados a la conexión y los que carecen de conexión. En esta sección veremos estos dos tipos y examinaremos las diferencias entre ellos.

El **servicio orientado a la conexión** encuentra su modelo en el sistema telefónico. Para conversar con alguien, descolgamos el teléfono, marcamos el número, hablamos y después colgamos. De manera similar, para usar un servicio de red orientado a la conexión, el usuario del servicio establece primero una conexión, la usa y después la libera. El aspecto esencial de una conexión es que actúa como un tubo: el emisor empuja objetos (bits) por un extremo y el receptor los saca en el mismo orden por el otro extremo.

En contraste, el **servicio sin conexión** toma su modelo del sistema postal. Cada mensaje (carta) lleva la dirección completa de destino, y cada uno se encamina a través del sistema de forma independiente de todos los demás. Normalmente, cuando se envían dos mensajes al mismo destino, el primero que se envió será el primero en llegar. Sin embargo, es posible que el primero que se envió se retrase tanto que el segundo llegue primero. Con un servicio orientado a la conexión, esto es imposible.

Cada servicio se puede caracterizar por una **calidad de servicio**. Algunos servicios son confiables en el sentido de que nunca pierden datos. Usualmente, un servicio confiable se implementa haciendo que el receptor acuse el recibo de cada mensaje, de modo que el emisor esté seguro de que llegó. El proceso de acuse de recibo introduce una sobrecarga y retardos que con frecuencia valen la pena pero que algunas veces son intolerables.

Una situación típica en la que un servicio confiable orientado a la conexión es apropiado es la transferencia de archivos. El propietario del archivo quiere asegurarse de que todos los bits lleguen correctamente y en el mismo orden en que se enviaron. Muy pocos clientes de transferencia de archivos preferirían un servicio que revolviera o perdiera algunos bits ocasionalmente, aun si fuera mucho más rápido.

Los servicios confiables orientados a la conexión tienen dos variantes menores: secuencias de mensajes y corrientes de bytes. En la primera, se mantienen los límites del mensaje. Cuando se envían dos mensajes de 1 kB, llegan como dos mensajes distintos de 1 kB, nunca como un mensaje de 2 kB. (Nota: kB significa kilobytes; kb significa kilobits). En la segunda, la conexión es simplemente una corriente de bytes, sin fronteras entre mensajes. Cuando llegan 2 kB al receptor, no hay forma de saber si se enviaron como un mensaje de 2 kB, dos mensajes de 1 kB o 2048 mensajes de 1 byte. Si las páginas de un libro se enviaran por la red como mensajes separados a una máquina de composición fotográfica, podría ser importante preservar los límites entre los mensajes. Por otra parte, con una terminal que se conecta a un sistema remoto de tiempo compartido, todo lo que se necesita es una corriente de bytes de la terminal a la computadora.

Como se mencionó con anterioridad, en ciertas aplicaciones los retrasos que introducen los acuses de recibo son inaceptables. Una de tales aplicaciones es el tráfico de voz digitalizada. Para los usuarios de teléfonos es preferible oír un poco de ruido en la línea o una palabra confusa de vez en cuando que introducir un retardo para esperar acuses de recibo. De manera similar, al transmitir una videocinta, tener algunos pixeles equivocados no es mayor problema, pero ver la película a jalones conforme el flujo se detiene para corregir errores resulta exasperante.

No todas las aplicaciones requieren conexiones. Por ejemplo, a medida que el correo electrónico se vuelve más común, ¿puede estar muy lejano el correo electrónico chatarra? El que envió el correo electrónico de propaganda probablemente no quiera tomarse la molestia de establecer y después liberar una conexión sólo para enviar un artículo. Tampoco es esencial una entrega 100% confiable, en especial si cuesta más. Todo lo que se necesita es una forma de enviar un solo mensaje que tenga una probabilidad elevada de llegar, aunque no esté garantizada. El servicio sin conexión no confiable (lo que significa sin acuse de recibo) con frecuencia recibe el nombre de **servicio de datagramas**, en analogía con el servicio de telegramas, que tampoco proporciona al emisor un acuse de recibo.

En otras situaciones, es deseable la comodidad de no tener que establecer una conexión para enviar un mensaje corto, pero la confiabilidad es esencial. Para estas aplicaciones se puede proporcionar el **servicio de datagrama con acuse**. Es como mandar una carta certificada y pedir recibo. Cuando el recibo regresa, el remitente tiene la seguridad absoluta de que la carta se entregó a la parte interesada y de que no se perdió en el camino.

Un servicio más es el **servicio de petición y respuesta**. En este servicio el remitente transmite un datagrama sencillo que contiene una petición; la repuesta contiene la contestación. Por ejemplo, una consulta a la biblioteca local para averiguar dónde se habla uighur cae en esta categoría. La petición/respuesta se usa mucho para instrumentar la comunicación en el modelo cliente-servidor; el cliente emite una petición y el servidor le responde. La figura 1-13 resume los tipos de servicio que hemos visto.

	Servicio	Ejemplo
Orientado a la conexión	Flujo de mensaje confiable	Secuencia de páginas
	Flujo de *bytes* confiable	Ingreso remoto
	Conexión no confiable	Voz digitalizada
Sin conexión	Datagrama no confiable	Correo electrónico chatarra
	Datagrama con acuse de recibo	Correo registrado
	Petición/respuesta	Consulta de base de datos

Figura 1-13. Seis tipos diferentes de servicio.

1.3.5. Primitivas de servicios

Un servicio se especifica de manera formal con un conjunto de (operaciones) **primitivas** disponibles para que un usuario u otra entidad acceda al servicio. Estas primitivas ordenan al servicio que ejecute alguna acción o que informe de una acción que haya tomado una entidad par. Una forma de clasificar las primitivas de servicio es dividirlas en cuatro clases según se muestra en la figura 1-14.

Primitiva	Significado
Petición	Una entidad quiere que el servicio haga un trabajo
Indicación	Se le informa a una entidad acerca de un suceso
Respuesta	Una entidad quiere responder a un suceso
Confirmación	Ha llegado la respuesta a una petición anterior

Figura 1-14. Cuatro clases de primitivas de servicio.

Para ilustrar los usos de las primitivas, consideremos cómo se establece y libera una conexión. La entidad que inicia efectúa una petición de conexión *CONNECT.request* que resulta en el envío de un paquete. A continuación, el receptor recibe una indicación de conexión *CONNECT.indication* que le anuncia que en alguna parte una entidad quiere establecer una comunicación con él. Después, la entidad que recibe la indicación usa la primitiva de respuesta a la conexión *CONNECT.response* para indicar si quiere aceptar o rechazar la conexión propuesta. En cualquier caso, la entidad que emite la petición inicial averigua qué sucedió por medio de una primitiva confirmación de conexión *CONNECT.confirm*.

Las primitivas pueden tener parámetros, y la mayor parte de ellas los tiene. Los parámetros de una petición de conexión pueden especificar la máquina a la que se va a conectar, el tipo de servicio deseado y el tamaño máximo de mensaje a usar en la conexión. Los parámetros de una indicación de conexión podrían contener la identidad de quien llama, el tipo de servicio deseado y el tamaño de mensaje máximo propuesto. Si la entidad llamada no está de acuerdo con el tamaño

máximo propuesto, podría presentar una contrapropuesta en su primitiva de *respuesta*, que se pondría a disposición del originador de la llamada en la *confirmación*. Los detalles de esta **negociación** son parte del protocolo. Por ejemplo, en el caso de dos propuestas en conflicto acerca del tamaño máximo del mensaje, el protocolo podría especificar que siempre se elija el más pequeño.

En lo que toca a la terminología, evitaremos cuidadosamente los términos "abrir una conexión" y "cerrar una conexión", porque para los ingenieros en electrónica un "circuito abierto" es uno con una separación o interrupción. La electricidad solamente puede fluir por "circuitos cerrados". Los científicos de la computación nunca estarán de acuerdo en que haya flujo de información por un circuito cerrado. Para pacificar ambos dominios usaremos los términos "establecer una conexión" y "liberar una conexión".

Los servicios pueden ser **confirmados** o **no confirmados**. En un servicio confirmado, existe una *petición,* una *indicación,* una *respuesta* y una *confirmación*. En un servicio no confirmado únicamente hay una *petición* y una *indicación*. El servicio CONNECT (conexión) siempre es un servicio confirmado porque el par remoto debe estar de acuerdo con el establecimiento de una conexión. Por otro lado, la transferencia de datos puede ser confirmada o no confirmada, dependiendo de si el emisor necesita acuse de recibo o no. En las redes se usan ambas clases de servicio.

Para concretar más el concepto de servicio, consideremos como ejemplo un servicio simple orientado a la conexión con las siguientes ocho primitivas de servicio:

1. CONNECT.*request* - Petición para establecer una conexión.
2. CONNECT.*indication* - Envía una señal a la parte llamada.
3. CONNECT.*response* - La usa el receptor para aceptar o rechazar llamadas.
4. CONNECT.*confirm* - Indica al originador si se aceptó o no la llamada.
5. DATA.*request* - Petición de envío de datos.
6. DATA.*indication* - Señal de llegada de los datos.
7. DISCONNECT.*request* - Petición para liberar una conexión.
8. DISCONNECT.*indication* - Indica al par la petición.

En este ejemplo, CONNECT es un servicio confirmado (requiere una respuesta específica), mientras que DISCONNECT es no confirmado (no hay respuesta).

Puede ser de utilidad hacer una analogía con el sistema telefónico para ver cómo se usan estas primitivas. Para esta analogía, considere los pasos que se requieren para llamar por teléfono a la tía Graciela e invitarla a su casa a tomar el té:

1. CONNECT.*request* - Marcar el número de teléfono de la tía Graciela.
2. CONNECT.*indication* - El teléfono de la tía suena.
3. CONNECT.*response* - Ella descuelga el teléfono.
4. CONNECT.*confirm* - Usted escucha que ya no llama.

5. DATA.*request* - Usted la invita a tomar el té.
6. DATA.*indication* - Ella escucha su invitación.
7. DATA.*request* - Ella dice que estaría encantada de ir.
8. DATA.*indication* - Usted escucha que ella acepta.
9. DISCONNECT.*request* - Usted cuelga el teléfono.
10. DISCONNECT.*indication* - Ella escucha y también cuelga el teléfono.

La figura 1-15 muestra esta misma secuencia de pasos como una serie de primitivas de servicio, incluida la confirmación final de desconexión. Cada paso implica una interacción entre dos capas en una de las computadoras. Cada *petición* o *respuesta* causa una *indicación* o *confirmación* en el otro extremo un poco después. En este ejemplo, los usuarios del servicio (usted y la tía Graciela) están en la capa $N + 1$ y el proveedor del servicio (el sistema de teléfonos) está en la capa N.

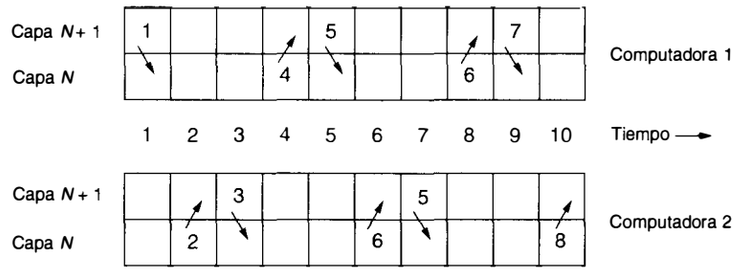

Figura 1-15. Cómo una computadora invitaría al té a la tía Graciela. Los números junto a la cola de cada flecha se refieren a las ocho primitivas de servicio que se vieron en esta sección.

1.3.6. La relación entre servicios y protocolos

Los servicios y los protocolos son conceptos distintos, aunque con frecuencia se les confunde. Sin embargo, esta distinción es tan importante que la subrayamos aquí de nuevo. Un *servicio* es un conjunto de (operaciones) primitivas que ofrece una capa a la que está por encima de ella. El servicio define cuáles son las operaciones que la capa está preparada para ejecutar en beneficio de sus usuarios, pero nada dice respecto de cómo se van a instrumentar estas operaciones. El servicio se refiere a la interfaz entre dos capas, siendo la capa inferior la que provee el servicio y la capa superior la que hace uso de él.

En contraste, un *protocolo* es un conjunto de reglas que gobiernan el formato y el significado de los marcos, paquetes o mensajes que se intercambian entre las entidades pares dentro de una

capa. Las entidades usan protocolos con el fin de instrumentar sus definiciones de servicios; son libres de cambiar sus protocolos a voluntad, siempre que no cambien el servicio visible a sus usuarios. De esta manera el servicio y el protocolo están desacoplados por completo.

Vale la pena hacer una analogía con los lenguajes de programación. Un servicio es como un tipo de datos abstracto o como un objeto en un lenguaje orientado a objetos. Define las operaciones que se pueden ejecutar con un objeto pero no especifica cómo se implementan éstas. Un protocolo se refiere a la *implementación* del servicio y como tal no es visible al usuario del mismo.

Muchos de los protocolos más antiguos no distinguían el servicio del protocolo. En efecto, una capa típica podía haber tenido una primitiva de servicio *ENVIAR PAQUETE* y el usuario proporcionaba un apuntador hacia un paquete totalmente ensamblado. Este arreglo significaba que todos los cambios al protocolo eran visibles de inmediato a los usuarios. La mayoría de diseñadores de redes reconocen ahora tal diseño como un disparate.

1.4. MODELOS DE REFERENCIA

Ya que analizamos en lo abstracto las redes basadas en capas, es hora de ver algunos ejemplos. En las próximas dos secciones veremos dos arquitecturas de red importantes: el modelo de referencia OSI y el modelo de referencia TCP/IP.

1.4.1. El modelo de referencia OSI

El modelo OSI se muestra en la figura 1-16 (menos el medio físico). Este modelo se basa en una propuesta que desarrolló la Organización Internacional de Normas (ISO, por sus siglas en inglés) como primer paso hacia la estandarización internacional de los protocolos que se usan en las diversas capas (Day y Zimmermann, 1983). El modelo se llama **modelo de referencia OSI** (*open systems interconnection,* **interconexión de sistemas abiertos**) **de la ISO** puesto que se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están abiertos a la comunicación con otros sistemas. Usualmente lo llamaremos sólo modelo OSI para acortar.

El modelo OSI tiene siete capas. Los principios que se aplicaron para llegar a las siete capas son los siguientes:

1. Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.
4. Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.

5. La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

Más adelante estudiaremos cada capa del modelo en orden, empezando por la capa del fondo. Note que el modelo de OSI en sí no es una arquitectura de red porque no especifica los servicios y protocolos exactos que se han de usar en cada capa; sólo dice lo que debe hacer cada capa. Sin embargo, la ISO también ha elaborado estándares para todas las capas, aunque no sean parte del modelo de referencia mismo. Cada uno se ha publicado por separado como norma internacional.

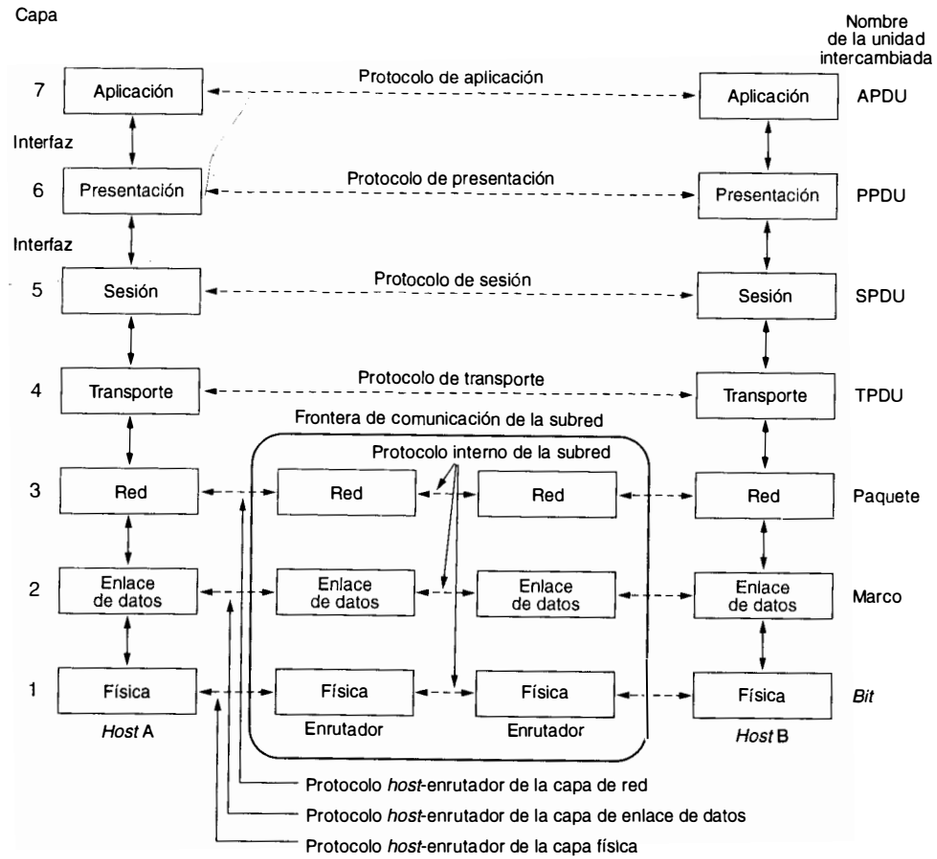

Figura 1-16. El modelo de referencia OSI.

La capa física

La **capa física** tiene que ver con la transmisión de bits por un canal de comunicación. Las consideraciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado envíe un bit 1, se reciba en el otro lado como bit 1, no como bit 0. Las preguntas típicas aquí son: cuántos volts deberán usarse para representar un 1 y cuántos para un 0; cuántos microsegundos dura un bit; si la transmisión se puede efectuar simultáneamente en ambas direcciones o no; cómo se establece la conexión inicial y cómo se interrumpe cuando ambos lados han terminado; y cuántas puntas tiene el conector de la red y para qué sirve cada una. Aquí las consideraciones de diseño tienen mucho que ver con las interfaces mecánica, eléctrica y de procedimientos, y con el medio de transmisión físico que está bajo la capa física.

La capa de enlace de datos

La tarea principal de la **capa de enlace de datos** es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión no detectados a la capa de red. Esta tarea la cumple al hacer que el emisor divida los datos de entrada en **marcos de datos** (unos cientos o miles de bytes, normalmente), que transmita los marcos en forma secuencial y procese los **marcos de acuse de recibo** que devuelve el receptor. Puesto que la capa física solamente acepta y transmite una corriente de bits sin preocuparse por su significado o su estructura, corresponde a la capa de enlace de datos crear y reconocer los límites de los marcos. Esto se puede lograr añadiendo patrones especiales de bits al principio y al final del marco. Si estos patrones de bits ocurrieran en los datos por accidente, se debe tener cuidado especial para asegurar que estos patrones no se interpreten incorrectamente como delimitadores de marcos.

Una ráfaga de ruido en la línea puede destruir por completo un marco. En este caso, el *software* de la capa de enlace de datos de la máquina fuente puede retransmitir el marco. Sin embargo, las transmisiones repetidas del mismo marco introducen la posibilidad de duplicar marcos. Se podría enviar un marco duplicado si se perdiera el marco del acuse de recibo que el receptor devuelve al emisor. Corresponde a esta capa resolver el problema provocado por los marcos dañados, perdidos y duplicados. La capa de enlace de datos puede ofrecer varias clases de servicio distintas a la capa de la red, cada una con diferente calidad y precio.

Otra consideración que surge en la capa de enlace de datos (y también de la mayor parte de las capas más altas) es cómo evitar que un transmisor veloz sature de datos a un receptor lento. Se debe emplear algún mecanismo de regulación de tráfico para que el transmisor sepa cuánto espacio de almacenamiento temporal (*buffer*) tiene el receptor en ese momento. Con frecuencia esta regulación de flujo y el manejo de errores están integrados.

Si se puede usar la línea para transmitir datos en ambas direcciones, esto introduce una nueva complicación que el *software* de la capa de enlace de datos debe considerar. El problema es que los marcos de acuse de recibo para el tráfico de *A* a *B* compiten por el uso de la línea con marcos de datos para el tráfico de *B* a *A*. Ya se inventó una solución inteligente (plataformas transportadoras) que veremos en detalle más adelante.

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos se encarga de este problema, la subcapa de acceso al medio.

La capa de red

La **capa de red** se ocupa de controlar el funcionamiento de la subred. Una consideración clave de diseño es determinar cómo se encaminan los paquetes de la fuente a su destino. Las rutas se pueden basar en tablas estáticas que se "alambran" en la red y rara vez cambian. También se pueden determinar al inicio de cada conversación, por ejemplo en una sesión de terminal. Por último, pueden ser altamente dinámicas, determinándose de nuevo con cada paquete para reflejar la carga actual de la red.

Si en la subred se encuentran presentes demasiados paquetes a la vez, se estorbarán mutuamente, formando cuellos de botella. El control de tal congestión pertenece también a la capa de red.

En vista de que los operadores de la subred podrían esperar remuneración por su labor, con frecuencia hay una función de contabilidad integrada a la capa de red. Cuando menos, el *software* debe contar cuántos paquetes o caracteres o bits envía cada cliente para producir información de facturación. Cuando un paquete cruza una frontera nacional, con tarifas diferentes de cada lado, la contabilidad se puede complicar.

Cuando un paquete debe viajar de una red a otra para alcanzar su destino, pueden surgir muchos problemas. El tipo de direcciones que usa la segunda red puede ser diferente del de la primera; puede ser que la segunda no acepte en absoluto el paquete por ser demasiado grande; los protocolos pueden diferir y otras cosas. La capa de red debe resolver todos estos problemas para lograr que se interconecten redes heterogéneas.

En las redes de difusión el problema del ruteo es simple y la capa de red con frecuencia es delgada o incluso inexistente.

La capa de transporte

La función básica de la **capa de transporte** es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Además, todo esto se debe hacer de manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del *hardware.*

En condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión. Sin embargo, si la conexión de transporte requiere un volumen de transmisión alto, la capa de transporte podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones para aumentar el volumen. Por otro lado, si es costoso crear o mantener una conexión de red, la capa de transporte puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo. En todos los casos, la capa de transporte debe lograr que la multiplexión sea transparente para la capa de sesión.

La capa de transporte determina también qué tipo de servicio proporcionará a la capa de sesión y, finalmente, a los usuarios de la red. El tipo más popular de conexión de transporte es un canal de punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otras posibles clases de servicio de transporte son el transporte de mensajes aislados sin garantía respecto al orden de entrega y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina al establecer la sesión.

La capa de transporte es una verdadera capa de extremo a extremo, del origen al destino. En otras palabras, un programa en la máquina fuente sostiene una conversación con un programa similar en la máquina de destino, haciendo uso de los encabezados de mensajes y de los mensajes de control. En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas, y no entre las máquinas de origen y destino, que pueden estar separadas por muchos enrutadores. La diferencia entre las capas 1 a la 3, que están encadenadas, y las capas 4 a la 7, que son de extremo a extremo, se ilustra en la figura 1-16. Muchos nodos están multiprogramados, lo que implica que múltiples conexiones entran y salen de cada nodo. En este caso se necesita una manera de saber cuál mensaje pertenece a cuál conexión. El encabezado de transporte (H_4 en la figura 1-11), es una opción para colocar esta información.

Además de multiplexar varias corrientes de mensajes por un canal, la capa de transporte debe cuidar de establecer y liberar conexiones a través de la red. Esto requiere alguna clase de mecanismo de asignación de nombres, de modo que un proceso en una máquina pueda describir con quién quiere conversar. También debe haber un mecanismo para regular el flujo de información, a fin de que un nodo rápido no pueda saturar a uno lento. Tal mecanismo se llama **control de flujo** y desempeña un papel clave en la capa de transporte (también en otras capas). El control de flujo entre nodos es distinto del control de flujo entre enrutadores, aunque después veremos que se aplican principios similares a ambos.

La capa de sesión

La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos, como lo hace la capa de transporte, pero también proporciona servicios mejorados que son útiles en algunas aplicaciones. Se podría usar una sesión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sesión es manejar el control del diálogo. Las sesiones pueden permitir que el tráfico vaya en ambas direcciones al mismo tiempo, o sólo en una dirección a la vez. Si el tráfico puede ir únicamente en un sentido a la vez (en analogía con una sola vía de ferrocarril), la capa de sesión puede ayudar a llevar el control de los turnos.

Un servicio de sesión relacionado es el **manejo de fichas**. Para algunos protocolos es esencial que ambos lados no intenten la misma operación al mismo tiempo. A fin de controlar estas actividades, la capa de sesión proporciona fichas que se pueden intercambiar. Solamente el lado que posea la ficha podrá efectuar la operación crítica.

Otro servicio de sesión es la **sincronización**. Considere los problemas que pueden ocurrir cuando se trata de efectuar una transferencia de archivos de 2 horas de duración entre dos

máquinas que tienen un tiempo medio entre rupturas de 1 hora. Cada transferencia, después de abortar, tendría que empezar de nuevo desde el principio y probablemente fallaría también la siguiente vez. Para eliminar este problema, la capa de sesión ofrece una forma de insertar puntos de verificación en la corriente de datos, de modo que después de cada interrupción sólo se deban repetir los datos que se transfirieron después del último punto de verificación.

La capa de presentación

La **capa de presentación** realiza ciertas funciones que se piden con suficiente frecuencia para justificar la búsqueda de una solución general, en lugar de dejar que cada usuario resuelva los problemas. En particular, y a diferencia de todas las capas inferiores que se interesan sólo en mover bits de manera confiable de acá para allá, la capa de presentación se ocupa de la sintaxis y la semántica de la información que se transmite.

Un ejemplo típico de servicio de presentación es la codificación de datos en una forma estándar acordada. La mayor parte de los programas de usuario no intercambian cadenas de bits al azar; intercambian cosas como nombres de personas, fechas, cantidades de dinero y cuentas. Estos elementos se representan como cadenas de caracteres, enteros, cantidades de punto flotante y estructuras de datos compuestas de varios elementos más simples. Las diferentes computadoras tienen códigos diferentes para representar cadenas de caracteres (por ejemplo, ASCII y Unicode), enteros (por ejemplo, en complemento a uno y en complemento a dos), y demás. Con el fin de hacer posible la comunicación entre computadoras con representaciones diferentes, las estructuras de datos por intercambiar se pueden definir en forma abstracta, junto con un código estándar que se use "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y las convierte de la representación que se usa dentro de la computadora a la representación estándar de la red y viceversa.

La capa de aplicación

La **capa de aplicación** contiene varios protocolos que se necesitan con frecuencia. Por ejemplo, existen cientos de tipos de terminales incompatibles en el mundo. Considere la situación de un editor de pantalla completa que debe trabajar en una red con muchos tipos diferentes de terminal, cada uno con formatos diferentes de pantalla, secuencias de escape para insertar y eliminar texto, mover el cursor, etcétera.

Una forma de resolver este problema es definir una **terminal virtual de red** abstracta que los editores y otros programas puedan manejar. Para cada tipo de terminal, se debe escribir un programa para establecer la correspondencia entre las funciones de la terminal virtual de red y las de la terminal real. Por ejemplo, cuando el editor mueva el cursor de la terminal virtual a la esquina superior izquierda de la pantalla, este *software* debe emitir la secuencia apropiada de órdenes a la terminal real para poner su cursor en ese lugar. Todo el *software* de terminal virtual está en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Los diferentes sistemas de archivos tienen convenciones diferentes para nombrar los archivos, formas diferentes de

representar líneas de texto, etc. La transferencia de un archivo entre dos sistemas diferentes requiere la resolución de éstas y otras incompatibilidades. Este trabajo también pertenece a la capa de aplicación, lo mismo que el correo electrónico, la carga remota de trabajos, la búsqueda en directorios y otros recursos de uso general y especial.

Transmisión de datos en el modelo OSI

La figura 1-17 muestra un ejemplo de cómo se pueden transmitir datos empleando el modelo OSI. El proceso remitente tiene algunos datos que quiere enviar al proceso receptor, así que entrega los datos a la capa de aplicación, la cual añade entonces al principio el encabezado de aplicación *AH* (que puede ser nulo) y entrega el elemento resultante a la capa de presentación.

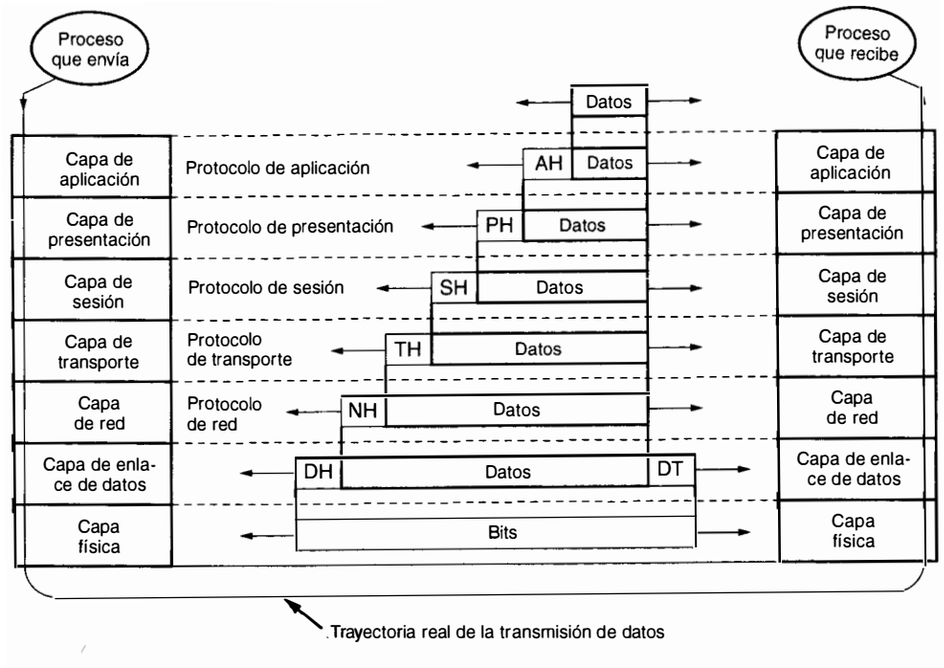

Figura 1-17. Ejemplo de uso del modelo OSI. Algunos de los encabezados pueden ser nulos. (Fuente: H.C. Folts. Usado con autorización.)

La capa de presentación puede transformar este elemento de diferentes maneras y posiblemente añadir al principio un encabezado, entregando el resultado a la capa de sesión. Es importante darse cuenta que la capa de presentación no sabe cuál porción de los datos entregados a ella por la capa de aplicación es la *AH,* si existe, y cuáles son en verdad los datos del usuario.

Este proceso se repite hasta que los datos alcanzan la capa física, donde son transmitidos realmente a la máquina receptora. En esa máquina se retiran los distintos encabezados, uno por

uno, conforme el mensaje se propaga hacia arriba por las capas hasta que por fin llega al proceso receptor.

La idea clave en todo este proceso es que aunque la transmisión real de los datos es vertical en la figura 1-17, cada capa se programa como si fuera horizontal. Por ejemplo, cuando la capa de transporte emisora recibe un mensaje de la capa de sesión, le añade un encabezado de transporte y lo envía a la capa de transporte receptora. Desde su punto de vista, el hecho de que en realidad debe dirigir el mensaje a la capa de red de su propia máquina es un tecnicismo sin importancia. A manera de analogía, cuando un diplomático que habla tagalog se dirige a las Naciones Unidas, piensa que se dirige a los demás diplomáticos de la asamblea. El hecho de que en realidad sólo hable con su traductor se ve como un detalle técnico.

1.4.2. El modelo de referencia TCP/IP

Pasemos ahora del modelo de referencia OSI al modelo que se usa en la abuela de todas las redes de computadoras, la ARPANET, y su sucesora, la Internet mundial. Aunque más adelante presentaremos una breve historia de la ARPANET, es de utilidad mencionar ahora algunos de sus aspectos. La ARPANET era una red de investigación patrocinada por el DoD (Departamento de Defensa de Estados Unidos). Al final conectó a cientos de universidades e instalaciones del gobierno usando líneas telefónicas rentadas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura de referencia nueva. Así, la capacidad de conectar entre sí múltiples redes de manera inconsútil fue uno de los principales objetivos de diseño desde el principio. Esta arquitectura se popularizó después como el **modelo de referencia TCP/IP**, por las iniciales de sus dos protocolos primarios. Este modelo se definió por primera vez en (Cerf y Kahn, 1974). En (Leiner *et al.*, 1985) se da una perspectiva posterior. La metodología de diseño en que se basa el modelo se aborda en (Clark, 1988).

Debido a la preocupación del DoD por que alguno de sus costosos nodos, enrutadores o pasarelas de interredes pudiera ser objeto de un atentado en cualquier momento, otro de los objetivos principales fue que la red fuera capaz de sobrevivir a la pérdida del *hardware* de subred sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones permanecieran intactas mientras las máquinas de origen y destino estuvieran funcionando, aun si alguna de las máquinas o de las líneas de transmisión en el trayecto dejara de funcionar en forma repentina. Es más, se necesitaba una arquitectura flexible, pues se tenía la visión de aplicaciones con requerimientos divergentes, abarcando desde la transferencia de archivos hasta la transmisión de discursos en tiempo real.

La capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred carente de conexiones. Esta capa, llamada **capa de interred**, es el eje que mantiene unida toda la arquitectura. La misión de esta capa es permitir que los nodos

inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en una red diferente). Los paquetes pueden llegar incluso en un orden diferente a aquel en que se enviaron, en cuyo caso corresponde a las capas superiores reacomodarlos, si se desea la entrega ordenada. Nótese que aquí se usa "interred" en un sentido genérico, aunque esta capa esté presente en la Internet.

Aquí la analogía es con el sistema de correos (lento). Una persona puede depositar una secuencia de cartas internacionales en un buzón en un país, y con un poco de suerte, casi todas se entregarán en la dirección correcta en el país de destino. Es probable que las cartas viajen a través de una o más pasarelas internacionales de correo en el camino, pero esto es transparente para los usuarios. Más aún, los usuarios no necesitan saber que cada país (esto es, cada red), tiene sus propias estampillas, tamaños preferidos de sobres y reglas de entrega.

La capa de interred define un formato de paquete y protocolo oficial llamado **IP** (*Internet protocol,* **protocolo de interred**). El trabajo de la capa de interred es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida en funcionalidad a la capa de red OSI. La figura 1-18 muestra la correspondencia.

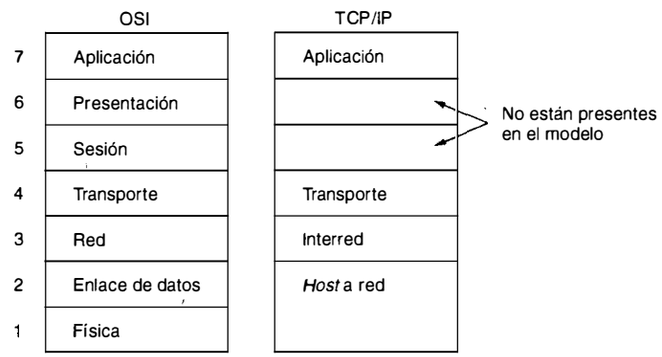

Figura 1-18. El modelo de referencia TCP/IP.

La capa de transporte

La capa que está sobre la capa de interredes en el modelo TCP/IP se llama usualmente ahora **capa de transporte**. Esta capa se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI. Aquí se definieron dos protocolos de extremo a extremo. El primero, **TCP** (*transmission control protocol,* **protocolo de control de la transmisión**) es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante

de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento con más mensajes de los que pueda manejar.

El segundo protocolo de esta capa, el **UDP** (*user datagram protocol,* **protocolo de datagrama de usuario**), es un protocolo sin conexión, no confiable, para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios. Este protocolo también se usa ampliamente para consultas de petición y respuesta de una sola ocasión, del tipo cliente-servidor, y en aplicaciones en las que la entrega pronta es más importante que la entrega precisa, como las transmisiones de voz o vídeo. La relación entre IP, TCP y UDP se muestra en la figura 1-19. Desde que se desarrolló el modelo, el IP se ha implementado en muchas otras redes.

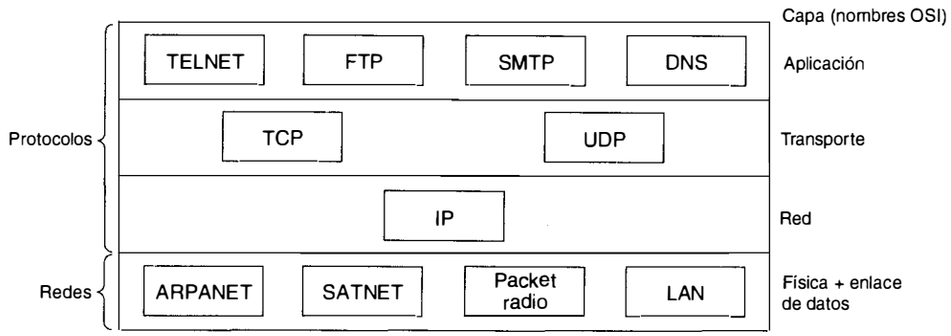

Figura 1-19. Protocolos y redes en el modelo TCP/IP inicial.

La capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias, así que no se incluyeron. La experiencia con el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayor parte de las aplicaciones.

Encima de la capa de transporte está la **capa de aplicación**, que contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de terminal virtual (TELNET), el de transferencia de archivos (FTP) y el de correo electrónico (SMTP), según se muestra en la figura 1-19. El protocolo de terminal virtual permite que un usuario en una máquina ingrese en una máquina distante y trabaje ahí. El protocolo de transferencia de archivos ofrece un mecanismo para mover datos de una máquina a otra en forma eficiente. El correo electrónico fue en sus orígenes sólo una clase de transferencia de archivos, pero más adelante se desarrolló para él un protocolo especializado; con los años, se le han añadido muchos otros protocolos, como el servicio de nombres de dominio (DNS) para relacionar los nombres de los nodos con sus

direcciones de la red; NNTP, el protocolo que se usa para transferir artículos noticiosos; HTTP, el protocolo que se usa para recuperar páginas en la *World Wide Web* y muchos otros.

La capa del nodo a la red

Bajo la capa de interred está un gran vacío. El modelo de referencia TCP/IP realmente no dice mucho de lo que aquí sucede, fuera de indicar que el nodo se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP. Este protocolo no está definido y varía de un nodo a otro y de red a red. Los libros y artículos sobre el modelo TCP/IP rara vez hablan de él.

1.4.3. Comparación de los modelos de referencia OSI y TCP

Los modelos de referencia OSI y TCP/IP tienen mucho en común. Ambos se basan en el concepto de un gran número de protocolos independientes. También la funcionalidad de las capas es muy similar. Por ejemplo, en ambos modelos las capas por encima de la de transporte, incluida ésta, están ahí para prestar un servicio de transporte de extremo a extremo, independiente de la red, a los procesos que deseen comunicarse. Estas capas forman el proveedor de transporte. También en ambos modelos, las capas encima de la de transporte son usuarios del servicio de transporte orientados a aplicaciones.

A pesar de estas similitudes fundamentales, los dos modelos tienen también muchas diferencias. En esta sección enfocaremos las diferencias clave entre los dos modelos de referencia. Es importante notar que aquí estamos comparando los *modelos de referencia,* no las *pilas de protocolos* correspondientes. Los protocolos mismos se estudiarán después. Un libro dedicado a comparar y contrastar TCP/IP y OSI es (Piscitello y Chapin, 1993).

En el modelo OSI, tres conceptos son fundamentales:

1. Servicios.
2. Interfaces.
3. Protocolos.

Es probable que la contribución más importante del modelo OSI sea hacer explícita la distinción entre estos tres conceptos. Cada capa presta algunos servicios a la capa que se encuentra sobre ella. La definición de *servicio* dice lo que la capa hace, no cómo es que las entidades superiores tienen acceso a ella o cómo funciona la capa.

La *interfaz* de una capa les dice a los procesos de arriba cómo acceder a ella; especifica cuáles son los parámetros y qué resultados esperar; nada dice tampoco sobre cómo trabaja la capa por dentro.

Finalmente, los *protocolos* pares que se usan en una capa son asunto de la capa. Ésta puede usar los protocolos que quiera, siempre que consiga que se realice el trabajo (esto es, que provea los servicios que ofrece). La capa también puede cambiar los protocolos a voluntad sin afectar el *software* de las capas superiores.

Estas ideas ajustan muy bien con las ideas modernas acerca de la programación orientada a objetos. Al igual que una capa, un objeto tiene un conjunto de métodos (operaciones) que los procesos pueden invocar desde fuera del objeto. La semántica de estos métodos define el conjunto de servicios que ofrece el objeto. Los parámetros y resultados de los métodos forman la interfaz del objeto. El código interno del objeto es su protocolo y no está visible ni es de la incumbencia de las entidades externas al objeto.

El modelo TCP/IP originalmente no distinguía en forma clara entre servicio, interfaz y protocolo, aunque se ha tratado de reajustarlo después a fin de hacerlo más parecido a OSI. Por ejemplo, los únicos servicios reales que ofrece la capa de interred son SENT IP PACKET y RESEIVE IP PACKET para enviar y recibir paquetes de IP, respectivamente.

Como consecuencia, en el modelo OSI se ocultan mejor los protocolos que en el modelo TCP/IP y se pueden reemplazar con relativa facilidad al cambiar la tecnología. La capacidad de efectuar tales cambios es uno de los principales propósitos de tener protocolos por capas en primer lugar.

El modelo de referencia OSI se desarrolló *antes* de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos, lo cual lo convirtió en algo muy general. El lado malo de este orden es que los diseñadores no tenían mucha experiencia con el asunto y no supieron bien cuál funcionalidad poner en cuál capa.

Por ejemplo, la capa de enlace de datos originalmente tenía que ver sólo con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que insertar una nueva subcapa en el modelo. Cuando la gente empezó a construir redes reales haciendo uso del modelo OSI y de los protocolos existentes, descubrió que no cuadraban con las especificaciones de servicio requeridas (maravilla de maravillas), de modo que se tuvieron que injertar en el modelo subcapas de convergencia que permitieran "tapar" las diferencias. Por último, el comité esperaba originalmente que cada país tuviera una red controlada por el gobierno que usara los protocolos OSI, de manera que no se pensó en la interconexión de redes. Para no hacer el cuento largo, las cosas no salieron como se esperaba.

Lo contrario sucedió con TCP/IP: primero llegaron los protocolos, y el modelo fue en realidad sólo una descripción de los protocolos existentes. No hubo el problema de ajustar los protocolos al modelo; se ajustaban a la perfección. El único problema fue que el *modelo* no se ajustaba a ninguna otra pila de protocolos; en consecuencia, no fue de mucha utilidad para describir otras redes que no fueran del tipo TCP/IP.

Pasando de temas filosóficos a otros más específicos, una diferencia obvia entre los dos modelos es la cantidad de capas: el modelo OSI tiene siete capas y el TCP/IP cuatro. Ambos tienen capas de (inter)red, de transporte y de aplicación, pero las otras capas son diferentes.

Otra diferencia se tiene en el área de la comunicación sin conexión frente a la orientada a la conexión. El modelo OSI apoya la comunicación tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte donde es más importante (porque el servicio de transporte es visible a los usuarios) lo hace únicamente con la comunicación orientada a la conexión. El modelo TCP/IP sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos modos en la capa de transporte, con lo que ofrece una alternativa a los usuarios. Esta elección es importante sobre todo para los protocolos simples de petición y respuesta.

1.4.4. Una crítica del modelo y los protocolos OSI

Ni el modelo OSI y sus protocolos ni el modelo TCP/IP y sus protocolos son perfectos. Se puede criticar bastante a ambos, y así se ha hecho. En esta sección y en la siguiente veremos algunas de estas críticas. Empezaremos por OSI y examinaremos TCP/IP más adelante.

Al momento de publicarse la segunda edición de este libro (1989), pareció a los más expertos en este campo que el modelo OSI y sus protocolos iban a conquistar el mundo y a desalojar de su camino todo lo demás. Esto no sucedió. ¿Por qué? Una mirada en retrospectiva a algunas de las lecciones puede ser de utilidad. Estas lecciones se pueden resumir como:

1. Mala sincronización.
2. Mala tecnología.
3. Malas instrumentaciones.
4. Mala política.

Mala sincronización

Veamos primero la razón número uno: la mala sincronización. El momento en el que se establece un estándar es absolutamente crucial para su éxito. David Clark del M.I.T. tiene una teoría de los estándares que llama el *apocalipsis de los dos elefantes,* y que se ilustra en la figura 1-20.

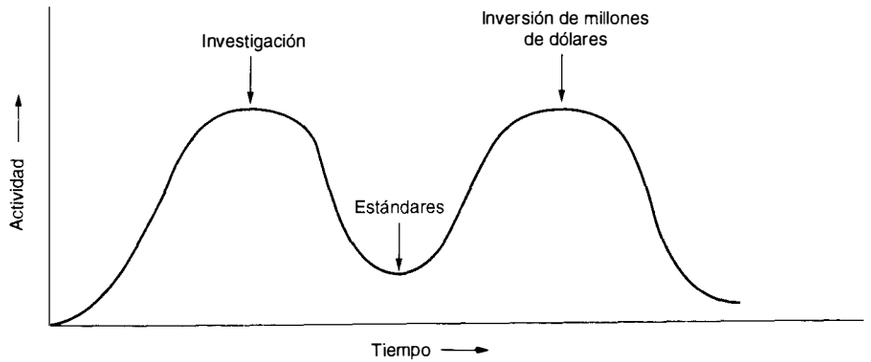

Figura 1-20. El apocalipsis de los dos elefantes.

Esta figura muestra la cantidad de actividad que rodea a un tema nuevo. Cuando se descubre inicialmente el tema, hay un frenesí de actividad de investigación en forma de discusiones, documentos y reuniones. Al cabo de un tiempo, esto disminuye, las corporaciones descubren el tema y llega la ola de inversión de millones de dólares.

Es esencial que se escriban los estándares en el intermedio entre los dos "elefantes". Si se escriben demasiado pronto, antes de que termine la investigación, el tema todavía no se entiende bien, lo que conduce a malos estándares. Si se escriben demasiado tarde, es probable que muchas compañías ya hayan hecho inversiones importantes en diferentes formas de hacer las cosas, de modo que los estándares se ignoran en la práctica. Si el intervalo entre los dos elefantes es muy corto (porque todos tienen prisa por empezar), la gente que desarrolla los estándares puede quedar aplastada.

Parece que ahora los protocolos estándar de OSI han quedado aplastados. Los protocolos competidores de TCP/IP ya se usaban ampliamente en universidades que hacían investigación cuando aparecieron los protocolos de OSI. Antes de que llegara la ola de inversión de millones de dólares, el mercado académico tenía el tamaño suficiente para que los proveedores empezaran a ofrecer con cautela los productos TCP/IP. Cuando el OSI llegó, no quisieron apoyar una segunda pila de protocolos hasta que se les forzó, de modo que no hubo ofertas iniciales. Al estar cada compañía en espera de que otra tomara la iniciativa, ninguna compañía lo hizo y OSI nunca sucedió.

Mala tecnología

La segunda razón por la que OSI nunca prendió es que tanto el modelo como los protocolos son imperfectos. La mayor parte de las explicaciones acerca del modelo de las siete capas da la impresión de que la cantidad y el contenido de las capas finalmente seleccionadas eran el único camino o, al menos, el camino obvio. Esto está lejos de ser verdad. La capa de sesión tiene poco uso en la mayor parte de las aplicaciones, y la capa de presentación casi está vacía. De hecho, la propuesta inglesa a la ISO tenía sólo cinco capas, no siete. En contraste con las capas de sesión y de presentación, las capas de enlace de datos y de red están tan llenas que en trabajos posteriores se dividieron en múltiples subcapas, cada una con funciones distintas.

A pesar de que casi nadie lo admite en público, la verdadera razón de que el modelo OSI tenga siete capas es que en el momento en que se diseñó IBM tenía un protocolo patentado de siete capas llamado **SNA**[MR] (*systems network architecture,* **arquitectura de red de sistemas**). En esa época, IBM dominaba la industria de la computación a tal grado que todo el mundo, incluidas las compañías de teléfonos, las compañías de computadoras de la competencia y hasta los principales gobiernos sentían pánico de que IBM usara su fuerza en el mercado para obligar prácticamente a todos a usar SNA, el cual podría cambiar en el momento que quisiera. Lo que se pretendía con OSI era crear un modelo de referencia y pila de protocolos semejante al de IBM que se pudiera convertir en el estándar mundial y estuviera controlado no por una compañía sino por una organización neutral, la ISO.

El modelo OSI, junto con las correspondientes definiciones y protocolos de servicios, es extraordinariamente completo. Si se apilan, los estándares impresos ocupan una fracción significativa de un metro de papel. También son difíciles de implementar e ineficientes en su operación. En este contexto, viene a la memoria un acertijo de Paul Mockapetris citado en (Rose, 1993):

P: ¿Qué se obtiene cuando se cruza un pandillero con un estándar internacional?
R: Alguien que te hace una oferta que no puedas comprender.

Otro problema con OSI, además de ser incomprensible, es que algunas funciones, como el direccionamiento, el control de flujo y el control de errores reaparecen una y otra vez en cada capa. Por ejemplo, Saltzer *et al*. (1984), han señalado que, para ser eficaz, el control de errores se debe hacer en la capa más alta, de modo que repetirlo una y otra vez en cada una de las capas inferiores con frecuencia es innecesario e ineficiente.

Otra consideración es que la decisión de colocar ciertas funciones en capas particulares no siempre es obvia. El manejo de una terminal virtual (ahora en la capa de aplicación) estuvo en la capa de presentación durante gran parte del desarrollo del estándar. Se pasó a la capa de aplicación porque el comité tuvo problemas para decidir para qué servía la capa de presentación. La seguridad de los datos y el cifrado eran tan polémicos que nadie podía ponerse de acuerdo en cuál capa ponerlos, así que se dejaron fuera. La administración de la red se omitió también del modelo por razones parecidas.

Otra crítica del estándar original es que ignoró por completo los servicios y protocolos carentes de conexión, a pesar de que casi todas las redes de área local trabajan de esa manera. Adiciones subsecuentes (conocidas en el mundo del *software* como parches) corrigieron este problema.

Quizá la crítica más seria es que el modelo está dominado por una mentalidad de comunicaciones. La relación entre la computación y las comunicaciones apenas si se menciona, y muchas de las decisiones tomadas son completamente inapropiadas para la forma en que trabajan las computadoras y el *software*. Como ejemplo, considere las primitivas de OSI, listadas en la figura 1-14. En particular, piense con cuidado en las primitivas y en cómo las podría usar en un lenguaje de programación.

La primitiva *CONNECT.request* es sencilla. Podemos imaginar un procedimiento de biblioteca, *conectar*; que los programas pueden llamar para establecer una conexión. Ahora piense en *CONNECT.indication*. Cuando llega un mensaje, se debe indicar esto al proceso de destino. En efecto, tiene que manejar una interrupción —un concepto difícilmente apropiado para programas escritos en cualquier lenguaje moderno de alto nivel—. Desde luego, en la capa más baja sí ocurre una indicación (interrupción).

Si el programa estuviera esperando una llamada, podría invocar un procedimiento de biblioteca, *recibir*, para bloquearse a sí mismo. Pero si esto es así, ¿por qué no fue la primitiva *recibir* en lugar de *indicación*? *Recibir* se orienta claramente hacia la forma en que trabajan las computadoras, mientras que *indicación* se orienta de forma igualmente clara hacia la forma en que trabajan los teléfonos. Las computadoras son diferentes de los teléfonos. Los teléfonos suenan. Las computadoras no suenan. En resumen, el modelo semántico de un sistema controlado por interrupciones no es una buena idea en lo conceptual y está totalmente en desacuerdo con las ideas modernas de la programación estructurada. Langsford (1984) analiza este problema y otros similares.

Malas instrumentaciones

Dada la enorme complejidad del modelo y los protocolos, no caerá de sorpresa que las implementaciones iniciales fueran enormes, inmanejables y lentas. Todos los que las probaron se arrepintieron. No tuvo que pasar mucho tiempo para que la gente asociara a "OSI" con la

"mala calidad". Mientras los productos mejoraban con el paso del tiempo, la imagen empeoraba.

En contraste, una de las primeras implementaciones de TCP/IP fue parte del UNIX® de Berkeley y era bastante buena (y, además, gratuita). La gente comenzó rápidamente a usarla, lo cual condujo a una gran comunidad de usuarios, lo que condujo a mejoras, lo que condujo a una comunidad todavía mayor. Aquí la espiral era hacia arriba en lugar de hacia abajo.

Mala política

Gracias a la implementación inicial, mucha gente, en especial los académicos, pensaban en TCP/IP como parte de UNIX, y UNIX en la década de 1980 era para los académicos algo así como la tarta de manzana para los estadounidenses comunes.

En cambio, se veía a OSI como una invención de los ministerios europeos de telecomunicaciones, de la Comunidad Europea y, más tarde, del gobierno de Estados Unidos. Esta creencia no era del todo justificada, pero la mera idea de un montón de burócratas tratando de obligar a los pobres investigadores y programadores que estaban en las trincheras desarrollando redes de computadoras reales a que aceptaran un estándar técnicamente inferior no ayudó mucho. Algunos vieron este intento como algo similar a cuando IBM anunció en la década de 1960 que PL/I era el lenguaje del futuro, o cuando DoD corrigió esto más tarde anunciando que en realidad era Ada®.

A pesar de que el modelo y los protocolos de OSI han sido algo menos que un sonado éxito, todavía hay algunas organizaciones interesadas en él, principalmente las PTT europeas que aún tienen un monopolio de las telecomunicaciones. En consecuencia, se ha hecho un esfuerzo débil por actualizar OSI, dando por resultado un modelo revisado que se publicó en 1994. Si desea saber qué se cambió (poco) y qué debió haberse cambiado (y mucho), consulte (Day, 1995).

1.4.5. Una crítica del modelo de referencia TCP/IP

También el modelo y los protocolos de TCP/IP tienen sus problemas. Primero, el modelo no distingue con claridad los conceptos de servicio, interfaz y protocolo. La práctica correcta de la ingeniería de *software* requiere la diferenciación entre las especificaciones y la implementación, algo que OSI hace con mucho cuidado y que TCP/IP no. En consecuencia el modelo de TCP/IP no es una buena guía para diseñar redes nuevas utilizando tecnologías nuevas.

Segundo, el modelo TCP/IP no es general en absoluto y no resulta apropiado para describir cualquier pila de protocolos distinta de TCP/IP. Por ejemplo, tratar de describir SNA mediante el modelo TCP/IP sería casi imposible.

Tercero, la capa de nodo a red en realidad no es una capa en el sentido normal en que se usa el término en el contexto de los protocolos de capas. Es una interfaz (entre la red y las capas de enlace de datos). La distinción entre interfaz y capa es crucial y hay que ser muy minuciosos al respecto.

Cuarto, el modelo TCP/IP no distingue entre la capa física (a la que ni siquiera menciona) y la de enlace de datos. Estas capas son completamente diferentes. La capa física tiene que ver con las características de transmisión del alambre de cobre, la fibra óptica y la comunicación inalámbrica. La tarea de la capa de enlace de datos es delimitar el inicio y el fin de los marcos y transferirlos de un lado a otro con el grado deseado de confiabilidad. Un modelo apropiado debería incluir ambas como capas separadas. El modelo TCP/IP no lo hace.

Por último, aunque los protocolos IP y TCP se pensaron y se implementaron con cuidado, muchos otros protocolos se fueron creando conforme surgía la necesidad, producidos por lo general por un par de estudiantes graduados que trabajaban hasta agotarse. A continuación, las implementaciones de los protocolos se distribuían gratuitamente, lo cual resultó en que se utilizaran con amplitud, atrincherándose y dificultando mucho su reemplazo. Algunos de ellos están ahora en apuros. Por ejemplo, el protocolo de terminal virtual, TELNET, se diseñó para una terminal mecánica Teletype de 10 caracteres por segundo; nada sabe de interfaces gráficas con el usuario ni de ratones. Sin embargo, 25 años después, todavía está en amplio uso.

En síntesis, a pesar de sus problemas, el *modelo* OSI (quitando las capas de sesión y de presentación) ha demostrado ser excepcionalmente útil para estudiar las redes de computadoras. En contraste, los *protocolos* de OSI no se han hecho populares. Lo contrario sucede con TCP/IP: el *modelo* prácticamente es inexistente, pero los *protocolos* se usan mucho. Puesto que los científicos de la computación gustan de tener su pastel y además comérselo, también, en este libro usaremos un modelo OSI modificado pero nos concentraremos principalmente en los protocolos TCP/IP y los que se relacionan con él, así como en los más nuevos, incluidos SMDS, *frame relay*, SONET y ATM. En efecto, en este libro usaremos el modelo híbrido de la figura 1-21 como marco de trabajo.

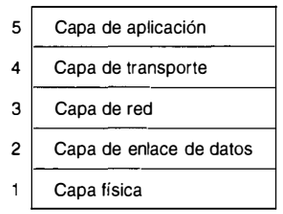

Figura 1-21. El modelo de referencia híbrido que se usa en este libro.

1.5. EJEMPLOS DE REDES

En la actualidad operan en el mundo numerosas redes. Algunas son redes públicas operadas por empresas de comunicaciones o PTT, otras son redes de investigación, otras más son redes cooperativas operadas por sus usuarios y todavía otras son redes comerciales o corporativas. En las siguientes secciones echaremos una mirada a algunas redes actuales e históricas para tener una idea de cómo funcionan (o funcionaban) y en qué difieren unas de otras.

Las redes difieren en su historia, su administración, los recursos que ofrecen, su diseño técnico y sus comunidades de usuarios. La historia y la administración pueden variar desde una red planeada con cuidado por una sola organización con un objetivo bien definido hasta una colección *ad hoc* de máquinas que se han conectado una con otra al paso de los años sin un plan maestro ni una administración central. Los recursos disponibles van desde la comunicación arbitraria entre procesos hasta el correo electrónico, la transferencia de archivos, el ingreso remoto (*login*) y la ejecución remota. Los diseños técnicos pueden diferir en los medios de transmisión empleados, los algoritmos de nomenclatura y ruteo, la cantidad y el contenido de las capas presentes y los protocolos utilizados. Por último, la comunidad de usuarios puede variar desde una sola corporación a todos los computólogos académicos del mundo industrializado.

En las siguientes secciones veremos algunos ejemplos. Éstos son: el popular paquete comercial de LAN, NetWare® de Novell; la Internet mundial (lo que incluye a sus predecesores, ARPANET y NSFNET), y las primeras redes de gigabits.

1.5.1. NetWare de Novell

El sistema de redes más popular en el mundo PC es **NetWare** de **Novell**. Se diseñó para que lo usaran compañías que deseaban cambiar su *mainframe* por una red de PC. En tales sistemas, cada usuario tiene una computadora de escritorio que funciona como cliente. Además, varias PC de alta capacidad operan como servidores para proveer de servicios de archivos, de bases de datos y otros a una colección de clientes. En otras palabras, el NetWare de Novell se basa en el modelo de cliente-servidor.

NetWare usa una pila de protocolos patentada que se ilustra en la figura 1-22 y que se basa en el antiguo Xerox Network System, XNS[MR] pero con varias modificaciones. NetWare de Novell es previo a OSI y no se basa en él. Si acaso, se parece más a TCP/IP que a OSI.

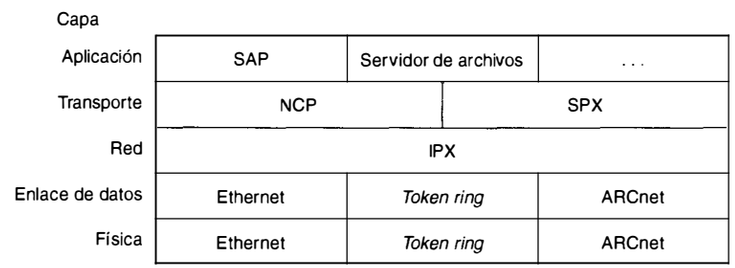

Figura 1-22. El modelo de referencia Novell NetWare.

Las capas física y de enlace de datos se pueden escoger de entre varios estándares de la industria, lo que incluye Ethernet, el *token ring* de IBM y ARCnet. La capa de red utiliza un

protocolo de interred no confiable, sin conexión, llamado **IPX**. Este protocolo transfiere paquetes del origen al destino en forma transparente, aun si la fuente y el destino se encuentran en redes diferentes. En lo funcional, IPX es similar a IP, excepto que usa direcciones de 10 bytes en lugar de direcciones de 4 bytes. La sabiduría de esta elección se hará evidente en el capítulo 5.

Por encima de IPX está un protocolo de transporte orientado a la conexión que se llama **NCP** (*network core protocol,* **protocolo central de red**). El NCP proporciona otros servicios además del transporte de datos de usuario y en realidad es el corazón de NetWare. También está disponible un segundo protocolo, **SPX**, pero sólo proporciona transporte. Otra opción es TCP. Las aplicaciones pueden seleccionar cualquiera de ellos. Por ejemplo, el sistema de archivos usa NCP y Lotus Notes® usa SPX. Las capas de sesión y de presentación no existen. En la capa de aplicación están presentes varios protocolos de aplicación.

Igual que en TCP/IP, la clave de toda la arquitectura es el paquete de datagrama de interred sobre el cual se construye todo lo demás. En la figura 1-23 se muestra el formato de un paquete IPX. El campo *Suma de verificación* pocas veces se usa, puesto que la capa de enlace subyacente también proporciona una suma de verificación. El campo *Longitud del paquete* indica qué tan grande es el paquete, encabezado más datos. El campo *Control de transporte* cuenta cuántas redes ha atravesado el paquete; cuando se excede un máximo, el paquete se descarta. El campo *Tipo de paquete* sirve para marcar varios paquetes de control. Cada una de las dos direcciones contiene un número de red de 32 bits, un número de máquina de 48 bits (la dirección 802 LAN) y la dirección local (*socket*) de 16 bits en esa máquina. Por último, tenemos los datos que ocupan el resto del paquete, cuyo tamaño máximo está determinado por la capa subyacente.

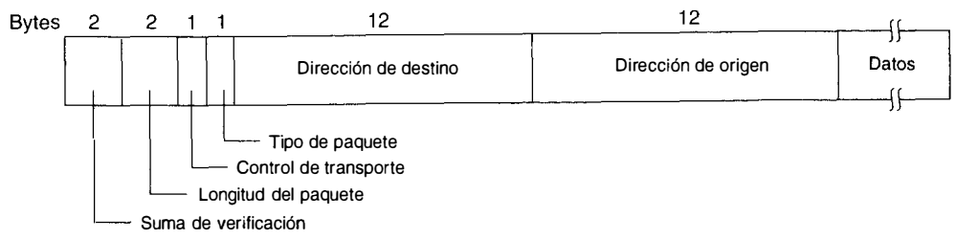

Figura 1-23. Un paquete IPX de Novell NetWare.

Aproximadamente cada minuto, cada servidor difunde un paquete con su dirección que indica cuáles servicios ofrece. Estas difusiones usan el **SAP** (*service advertising protocol,* **protocolo de publicidad del servicio**). Procesos de agentes especiales que se ejecutan en las máquinas enrutadoras que detectan y recopilan los paquetes. Los agentes usan la información contenida en los paquetes para construir bases de datos que indican cuáles servidores se ejecutan y dónde.

Cuando se arranca una máquina cliente, emite una petición en la que pregunta dónde está el servidor más cercano. El agente en la máquina del enrutador local detecta esta solicitud y busca

en su base de datos de servidores cuál es el mejor servidor para su solicitud. A continuación se devuelve al cliente la dirección del mejor servidor a usar. Ahora el cliente puede establecer una conexión NCP con el servidor. Mediante esta conexión, el cliente y el servidor negocian el tamaño máximo de paquete. De aquí en adelante, el cliente puede acceder al sistema de archivos y a otros servicios usando esta conexión. También puede hacer consultas a la base de datos de servidores para buscar otros servidores (más distantes).

1.5.2. La ARPANET

Pasemos ahora de las LAN a las WAN. A mediados de la década de 1960, en la cúspide de la Guerra Fría, el DoD quería una red de comando y control que pudiera sobrevivir a una guerra nuclear. Las redes telefónicas tradicionales de circuito conmutado se consideraban muy vulnerables, puesto que la pérdida de una línea o un conmutador ciertamente terminaría toda conversación que los estuviera usando y podría incluso partir la red. Para resolver este problema, el DoD acudió a su rama de investigación, ARPA o Advanced Research Projects Agency (más tarde DARPA y ahora ARPA de nuevo), es decir, la Agencia (de Defensa, periódicamente) de Proyectos de Investigación Avanzados.

ARPA se creó en respuesta al lanzamiento del Sputnik de la Unión Soviética en 1957 y tuvo la misión de desarrollar tecnologías que pudieran ser útiles a la milicia. ARPA nunca tuvo científicos ni laboratorios, de hecho, no tenía más que una oficina y un presupuesto pequeño (para los estándares del Pentágono). Cumplió con su trabajo al ofrecer financiamiento y contratos a universidades y compañías cuyas ideas le parecían prometedoras.

Varias de las primeras subvenciones se concedieron a las universidades para investigar la idea entonces radical de la conmutación de paquetes, algo que Paul Baran había sugerido en una serie de informes de la RAND Corporation que se publicaron a principios de la década de 1960. Después de discusiones con varios expertos, la ARPA decidió que la red que necesitaba el DoD debía ser una red de paquete conmutado, que consistía en una subred y computadoras *host*s.

La subred consistiría en minicomputadoras llamadas **IMP** (*interface message processors,* **procesadores interfaz de mensajes**) conectadas por líneas de transmisión. Para lograr alta confiabilidad, cada IMP se conectaría al menos a otras dos. La subred iba a ser una subred de datagrama, de modo que si algunas líneas e IMP resultaban destruidas, los mensajes se podrían reencaminar de forma automática a través de trayectorias alternas.

Cada nodo de la red consistiría en un IMP y una *host* en el mismo cuarto, conectados por un cable corto. Una *host* podría enviar mensajes de hasta 8063 bits a su IMP, que entonces los dividiría en paquetes de 1008 bits a lo sumo y los reenviaría a su destino en forma independiente. Cada paquete se recibía en su totalidad antes de reenviarse, por lo que la subred fue la primera red electrónica de conmutación de paquetes de almacenar y reenviar.

A continuación, la ARPA lanzó un ofrecimiento para construir la subred. Doce compañías licitaron. Después de evaluar todas las propuestas, la ARPA seleccionó a BBN, una firma de consultores de Cambridge, Massachusetts, y en diciembre de 1968 le concedió un contrato para construir la subred y escribir el *software* de la misma. BBN eligió usar como IMP las minicomputadoras DDP-316 de Honeywell, modificadas especialmente, con 12K palabras de

16 bits de memoria central. Los IMP no tenían discos, pues las partes móviles se consideraban no confiables. Los IMP se interconectaron con líneas de 56 kbps rentadas a compañías de teléfonos.

El *software* se dividió en dos partes: subred y *host*. El *software* de la subred consistió en el extremo IMP de la conexión *host*-IMP, el protocolo IMP-IMP y un protocolo de IMP fuente a IMP destino diseñado para mejorar la confiabilidad. El diseño original de la ARPANET se muestra en la figura 1-24.

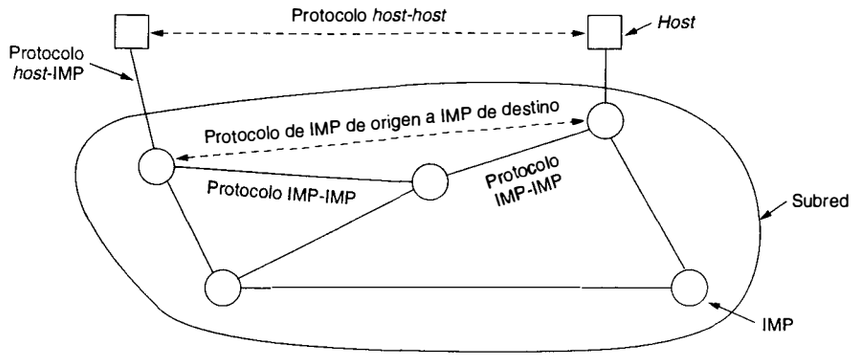

Figura 1-24. El diseño original de la ARPANET.

Fuera de la subred también se necesitaba *software,* a saber, el extremo *host* de la conexión *host*-IMP, el protocolo *host-host* y el *software* de aplicación. Pronto quedó claro que, según BBN, una vez que aceptaba un mensaje por un cable *host*-IMP y lo colocaba en el cable *host*-IMP de su destino, su trabajo estaba hecho.

Para enfrentar el problema del *software* de la *host*, Larry Roberts de ARPA convocó a una reunión de investigadores de redes, la mayoría estudiantes graduados, en Snowbird, Utah, en el verano de 1969. Los estudiantes graduados esperaban que un experto en redes les explicara el diseño de la red y su *software* y luego les asignara el trabajo de escribir una parte del mismo a cada uno de ellos. Quedaron pasmados cuando no hubo experto en redes y tampoco un gran diseño. Tuvieron que descifrar qué hacer por sí mismos.

Sin embargo, de alguna forma, una red experimental entró en funciones en diciembre de 1969 con cuatro nodos en UCLA, UCSB, SRI y la Universidad de Utah. Estas cuatro se eligieron porque todas tenían gran cantidad de contratos con ARPA, y todas tenían computadoras *host* diferentes y completamente incompatibles (sólo para hacerlo más divertido). La red creció rápidamente conforme se fueron entregando e instalando más IMP; pronto abarcó todo Estados Unidos. La figura 1-25 muestra con qué rapidez creció la ARPANET en los primeros tres años.

Más tarde, el *software* de IMP se cambió para permitir que las terminales se conectaran de forma directa a un IMP especial llamado **TIP** (*terminal interface processor,* **procesador de interfaz de terminal**) sin tener que pasar por una *host*. Los cambios subsecuentes incluyeron el tener múltiples *hosts* por cada IMP (para ahorrar dinero), *hosts* que se comunicaban con múltiples IMP (para protegerse de fallas del IMP) y *hosts* e IMP separadas por una gran distancia (para alojar a las *hosts* situadas lejos de la subred).

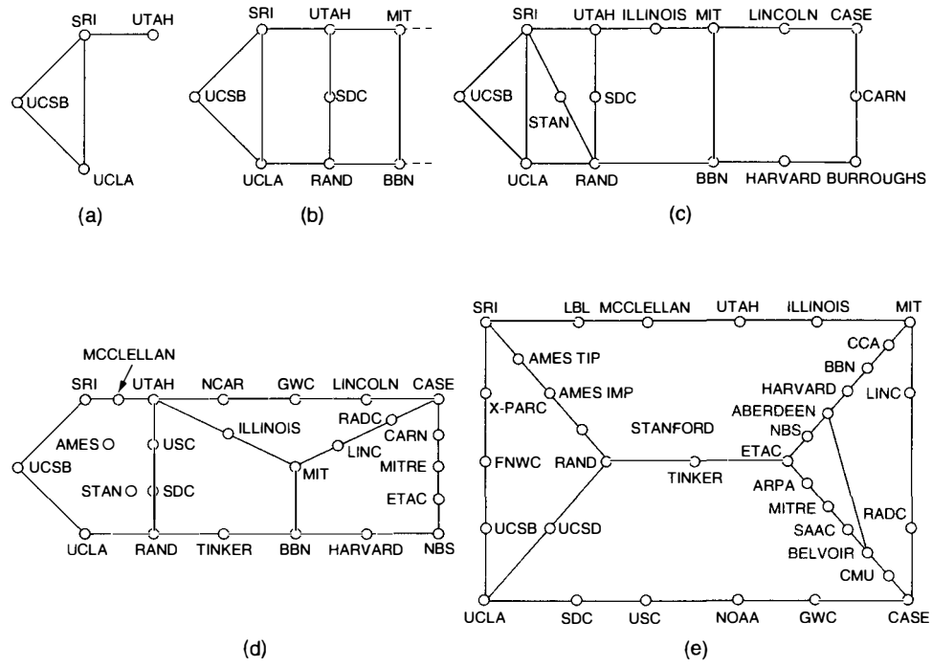

Figura 1-25. Crecimiento de la ARPANET. (a) Dic. 1969. (b) Julio 1970. (c) Marzo 1971. (d) Abril 1972. (e) Sept. 1972.

Además de ayudar al crecimiento de la novel ARPANET, ARPA financió también investigaciones sobre redes de satélites y redes de radio de paquetes móviles. En una demostración famosa, un camión que recorría California usó la red radial de paquetes para enviar mensajes a SRI, que entonces los reenvió por conducto de ARPANET a la Costa Este, desde donde se transmitieron a la University College en Londres mediante una red de satélites. Esto permitió a un investigador en el camión usar una computadora en Londres mientras conducía por California.

Este experimento demostró también que los protocolos de ARPANET existentes no eran apropiados para funcionar en múltiples redes. Esta observación condujo a más investigaciones sobre protocolos, lo que culminó con la invención del modelo y los protocolos TCP/IP (Cerf y Kahn, 1974). TCP/IP se diseñó de manera específica para manejar la comunicación en las interredes, algo que se volvió cada vez más importante al conectarse más y más redes a la ARPANET.

Para fomentar la adopción de estos protocolos nuevos, la ARPA concedió varios contratos a BBN y a la Universidad de California en Berkeley para integrarlos en el UNIX de Berkeley. Los investigadores de Berkeley desarrollaron una interfaz de programa conveniente para la red

(*sockets*) y escribieron muchos programas de aplicación, utilería y administración para facilitar el trabajo con redes.

El momento era ideal. Muchas universidades acababan de adquirir su segunda o tercera computadora VAX y una LAN para conectarlas, pero no tenían *software* de red. Cuando el 4.2BSD hizo su arribo, junto con TCP/IP, los *sockets* y muchas utilerías de red, el paquete completo se adoptó de inmediato. Además, con TCP/IP era fácil que las LAN se conectaran a la ARPANET, y muchas lo hicieron.

Para 1983 la ARPANET gozaba de estabilidad y éxito, con más de 200 IMP y cientos de *hosts*. En este momento, ARPA cedió el manejo de la red a la Agencia de Comunicaciones de la Defensa (DCA), para hacerla funcionar como una red de operaciones. Lo primero que hizo la DCA fue separar la porción militar en una subred independiente, **MILNET** (cerca de 160 IMP, de los cuales 110 estaban en Estados Unidos y 50 en otros países), con pasarelas estrictas entre MILNET y la red de investigación restante.

Durante la década de 1980, se conectaron a la ARPANET redes adicionales, sobre todo LAN. Al aumentar la escala, encontrar *hosts* era algo que se hizo cada vez más costoso, así que se creó el **DNS** (*domain naming system,* **sistema de designación de dominios**) para organizar las máquinas en dominios y establecer correspondencias entre los nombres de las *hosts* y las direcciones de IP. Desde entonces, el DNS se ha convertido en un sistema distribuido y generalizado de bases de datos para almacenar diversa información referente a los nombres. Estudiaremos el DNS con detalle en el capítulo 7.

Para 1990, la ARPANET había sido rebasada por redes más nuevas que ella misma había engendrado, de manera que se clausuró y desmanteló, pero aún vive en los corazones y las mentes de los investigadores de redes en todas partes. En cambio, MILNET continúa operando.

1.5.3. NSFNET

A finales de la década de 1970, la NSF (*National Science Foundation,* **Fundación Nacional de la Ciencia** de Estados Unidos) vio el impacto enorme que había tenido ARPANET en la investigación universitaria al permitir que científicos de todo el país compartieran datos y colaboraran en proyectos de investigación. Sin embargo, para introducirse en la ARPANET, una universidad debía tener un contrato de investigación con el DoD, cosa que muchas no tenían. Esta falta de acceso universal motivó a la NSF a establecer una red virtual, **CSNET**, centrada en una sola máquina en BBN que permitía el uso de líneas de acceso por discado y tenía conexiones con la ARPANET y otras redes. Mediante CSNET, los investigadores académicos podían hacer llamadas y dejar correo electrónico para que otras personas lo recogieran más tarde. Era simple, pero funcionaba.

En 1984, la NSF empezó a diseñar un sucesor de alta velocidad para la ARPANET que se abriría a todos los grupos universitarios de investigación. A fin de tener algo en concreto con lo cual empezar, la NSF decidió construir una red de *backbone* (tronco o columna vertebral) para conectar sus seis centros de supercomputadoras en San Diego, Boulder, Champaign, Pittsburgh, Ithaca y Princeton. A cada supercomputadora se le dio un hermanito que consistía en una

microcomputadora LSI-11 a la que llamaron ***fuzzball***. Las *fuzzballs* se conectaron con líneas rentadas de 56 kbps y formaron la subred, la misma tecnología de *hardware* que usó ARPANET. Sin embargo, la tecnología de *software* era diferente: las *fuzzballs* hablaban TCP/IP desde un principio, convirtiéndose en la primera WAN de TCP/IP.

La NSF financió también algunas redes regionales (finalmente cerca de 20), que se conectaron a la *backbone* para permitir a los usuarios de miles de universidades, laboratorios de investigación, bibliotecas y museos acceder a cualquiera de las supercomputadoras y comunicarse entre sí. La red completa, que incluía la *backbone* y las redes regionales, se llamó **NSFNET**. La NSFNET se conectó a la ARPANET mediante un enlace entre un IMP y una *fuzzball* en el cuarto de máquinas de Carnegie-Mellon. En la figura 1-26 se ilustra la primera *backbone* de NSFNET.

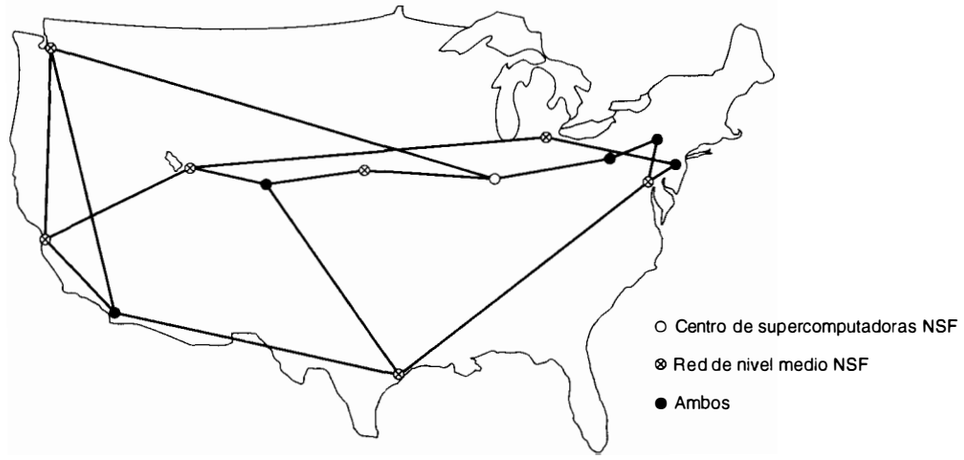

Figura 1-26. La columna vertebral (*backbone*) de NSFNET en 1988.

La NSFNET fue un éxito instantáneo y se sobrecargó desde el primer momento. La NSF comenzó de inmediato a planear a su sucesor y concedió un contrato al consorcio MERIT de Michigan para que lo operara. Se rentaron a la MCI canales de fibra óptica a 448 kbps para establecer la versión 2 de la *backbone*. Como enrutadores se usaron equipos IBM RS6000. También esta *backbone* resultó superada en poco tiempo, y para 1990 se había subido de nivel a la segunda *backbone*, a 1.5 Mbps.

Al continuar el crecimiento, la NSF se dio cuenta que el gobierno no podía seguir financiando eternamente el uso de redes. Más aún, las organizaciones comerciales querían unirse pero los estatutos de la NSF les prohibían usar redes pagadas por la propia Fundación. En consecuencia, la NSF animó a MERIT, MCI e IBM a formar una corporación no lucrativa, **ANS** (**Advanced Network and Services**) como un paso hacia la comercialización. En 1990, ANS tomó la NSFNET y subió el nivel de los enlaces de 1.5 Mbps a 45 Mbps para formar **ANSNET**.

En diciembre de 1991, el Congreso de Estados Unidos aprobó un documento que autorizaba a la **NREN**, la **Red Nacional Educativa y de Investigación**, como sucesora de investigación de la NSFNET, sólo que operando a velocidades de gigabits. La meta era una red nacional que funcionara a 3 Gbps antes del milenio. Esta red iba a actuar como prototipo para la tan discutida supercarretera de la información.

Para 1995, la *backbone* NSFNET ya no era necesaria para interconectar las redes regionales de la NSF porque un gran número de compañías operaba con redes comerciales IP. Cuando se vendió la ANSNET a America Online en 1995, las redes regionales de la NSF tuvieron que comprar el servicio comercial de IP para interconectarse.

Para facilitar la transición y asegurar que cada red regional se pudiera comunicar con todas las demás redes regionales, la NSF otorgó contratos a cuatro operadores de redes diferentes para establecer un **NAP** (*network access point,* **punto de acceso a la red**). Estos operadores eran PacBell (San Francisco), Ameritech (Chicago), MFS (Washington, D.C.) y Sprint (Nueva York, donde, para propósitos de NAP, Pennsauken, N.J. cuenta como la ciudad de Nueva York). Cada operador de red que quisiera proporcionar el servicio de *backbone* a las redes regionales de la NSF debía conectarse a todos los NAP. Este arreglo significaba que un paquete que se originara en cualquier red regional podía elegir entre varias portadoras de *backbone* para ir desde su NAP al NAP de destino. En consecuencia, las portadoras de *backbone* se vieron forzadas a competir para que las redes regionales las escogieran con base en el servicio y el precio, que desde luego era lo que se buscaba. Además de los NAP de la NSF, ya se habían creado varios NAP del gobierno (por ejemplo, FIX-E, FIX-W, MAE-East y MAE-West) y comerciales (por ejemplo, CIX), así que el concepto de una *backbone* solitaria por omisión fue sustituido por una infraestructura competitiva regida por lo comercial.

Otros países y regiones están construyendo redes comparables a NSFNET. En Europa, por ejemplo, EBONE es una *backbone* IP para organizaciones de investigación y EuropaNET es una red más orientada hacia lo comercial. Ambas conectan gran cantidad de ciudades en Europa con líneas de 2 Mbps y se están instalando mejoras de nivel a 34 Mbps. Cada país de Europa tiene una o más redes nacionales, lo cual es comparable en forma aproximada a las redes regionales de la NSF.

1.5.4. La Internet

La cantidad de redes, máquinas y usuarios conectados a la ARPANET creció con rapidez después de que TCP/IP se convirtió en el único protocolo oficial el 1° de enero de 1983. Cuando se interconectaron la NSFNET y la ARPANET, el crecimiento se hizo exponencial; se unieron muchas redes regionales y se hicieron conexiones con redes en Canadá, Europa y el Pacífico.

En algún momento de mediados de la década de 1980, la gente empezó a ver la aglomeración de redes como una interred, y más tarde como la Internet, aunque no hubo dedicatoria oficial con algún político rompiendo una botella de champagne sobre una *fuzzball*.

El crecimiento continuó en forma exponencial, y para 1990 la Internet había crecido a 3000 redes y 200,000 computadoras. En 1992 se adhirió la *host* número un millón. Para 1995, había múltiples redes de *backbones*, cientos de redes de nivel medio (esto es, regionales), decenas de

miles de LAN, millones de *hosts* y decenas de millones de usuarios. El tamaño se duplica aproximadamente cada año (Paxson, 1994).

Gran parte del crecimiento se debe a la conexión de redes existentes a la Internet. En el pasado, éstas incluyeron: SPAN, la red de física del espacio de la NASA, HEPNET, una red de física de alto nivel, BITNET, la red de *mainframes* de IBM, EARN, una red académica europea que ahora se usa ampliamente en Europa del Este, y muchas otras. Se utilizan numerosos enlaces trasatlánticos que operan desde 64 kbps hasta 2 Mbps.

El aglutinante de Internet es el modelo de referencia TCP/IP y la pila de protocolos de TCP/IP. El TCP/IP hace posible el servicio universal y se puede comparar con el sistema de teléfonos o la adopción del ancho de vía universal para los ferrocarriles en el siglo XIX.

¿Qué significa en realidad estar en Internet? Nuestra definición es que una máquina está en Internet si opera con la pila de protocolos de TCP/IP, tiene una dirección de IP y es capaz de enviar paquetes de IP a todas las demás máquinas de Internet. La mera capacidad de enviar y recibir correo electrónico no es suficiente, pues el correo electrónico se distribuye a muchas redes fuera de Internet. Sin embargo, el asunto pierde claridad en cierta forma por el hecho de que muchas computadoras personales tienen la capacidad de llamar a un proveedor de servicios de Internet mediante un módem, recibir la asignación de una dirección de IP temporal y enviar paquetes IP a otras *hosts* de Internet. Tiene sentido considerar que tales máquinas están en Internet mientras están conectadas al enrutador del proveedor de servicios.

Con el crecimiento exponencial, la antigua manera informal de operar la Internet ya no funciona. En enero de 1992 se integró la **Sociedad Internet** para promover el uso de Internet y quizá en algún momento hacerse cargo de su gestión.

Tradicionalmente, Internet ha tenido cuatro aplicaciones principales, que son las siguientes:

1. **Correo electrónico**. La capacidad de redactar, enviar y recibir correo electrónico ha estado disponible desde los primeros días de la ARPANET y es enormemente popular. Mucha gente recibe docenas de mensajes al día y lo considera su forma primaria de interactuar con el mundo externo, dejando muy atrás al teléfono y al correo lento. En estos días, los programas de correo electrónico están disponibles virtualmente en todo tipo de computadoras.

2. **Noticias**. Los grupos de noticias son foros especializados en los que usuarios con un interés común pueden intercambiar mensajes. Existen miles de grupos de noticias, con temas técnicos y no técnicos, lo que incluye computadoras, ciencia, recreación y política. Cada grupo de noticias tiene su propia etiqueta, estilo y costumbres, y ¡ay de cualquiera que los viole!

3. **Sesión remota**. Mediante el uso de Telnet, Rlogin u otros programas, los usuarios en cualquier lugar de la Internet pueden ingresar en cualquier otra máquina en la que tengan una cuenta autorizada.

4. **Transferencia de archivos**. Con el programa FTP, es posible copiar archivos de una máquina en Internet a otra. De esta manera está disponible una vasta cantidad de artículos, bases de datos y otra información.

Hasta casi fines de la década de 1990, la Internet se poblaba en gran medida de investigadores académicos, del gobierno y de la industria. Una aplicación nueva, la **WWW** (*world wide web,* **red mundial**) cambió todo eso y atrajo millones de nuevos usuarios no académicos a la red. Esta aplicación, inventada por el físico del CERN Tim Berners-Lee, no cambió ninguno de los recursos subyacentes pero los hizo más fáciles de usar. Junto con el visor de Mosaic, escrito en el Centro Nacional para Aplicaciones de Supercomputadoras, la WWW hizo posible que una localidad estableciera varias páginas de información conteniendo texto, dibujos, sonido y hasta vídeo con enlaces intercalados a otras páginas. Al accionar el ratón en un enlace, el usuario se ve transportado de inmediato a la página a la que apunta ese enlace. Por ejemplo, muchas compañías tienen una página local con entradas que apuntan a otras páginas que ofrecen información de productos, listas de precios, ventas, apoyo técnico, comunicación con los empleados, información para accionistas y muchas cosas más.

En un tiempo muy corto han aparecido muchos otros tipos de páginas, incluso mapas, tablas del mercado de valores, catálogos de tarjetas de bibliotecas, programas de radio grabados y hasta una página que apunta al texto completo de muchos libros cuyos derechos de autor han expirado (Mark Twain, Charles Dickens, etc.). Mucha gente tiene también páginas personales (páginas locales).

El primer año en que salió a la luz Mosaic, la cantidad de servidores de WWW creció de 100 a 7000. Sin duda el crecimiento en los años por venir continuará siendo enorme, y es probable que sea la fuerza que impulse la tecnología y el uso de Internet hacia el próximo milenio.

Se han escrito muchos libros respecto a la Internet y sus protocolos. Para más información, véase (Black, 1995; Carl-Mitchell y Quarterman, 1993; Comer, 1995, y Santifaller, 1994).

1.5.5. Plataformas de pruebas de gigabits

Las redes de *backbones* de Internet operan a velocidades de megabits, de modo que para la gente que quiere forzar los límites de la tecnología, el próximo paso es el uso de redes de gigabits. Con cada incremento en el ancho de banda de la red, se hacen posibles nuevas aplicaciones, y las redes de gigabits no son la excepción. En esta sección hablaremos primero un poco sobre las aplicaciones de gigabits, mencionaremos dos de ellas y a continuación listaremos algunas plataformas de pruebas de gigabits que se han construido.

Las redes de gigabits proporcionan mayor ancho de banda que las redes de megabits, pero no siempre reducen mucho los retardos. Por ejemplo, enviar un paquete de 1 kB de Nueva York a San Francisco a 1 Mbps toma 1 mseg para sacar los bits y 20 mseg para el retardo transcontinental, dando un total de 21 mseg. Una red de 1 Gbps puede reducir esto a 20.001 mseg. Aunque los bits van saliendo más rápido, el retardo transcontinental no cambia, puesto que la velocidad de la luz en la fibra óptica (o en el alambre de cobre) es cercana a los 200,000 km/seg y es independiente de la velocidad de transmisión de los datos. Así, para aplicaciones de área amplia en las que el retardo es crítico, ir a velocidades más altas no puede ayudar mucho. Por fortuna, para algunas aplicaciones el ancho de banda es lo que cuenta, y éstas son las aplicaciones en las que las redes de gigabits implicarán una gran diferencia.

Una aplicación es la telemedicina. Mucha gente piensa que una forma de reducir los costos médicos es reintroducir los médicos familiares y las clínicas familiares en gran escala, de modo que todo mundo tenga acceso cómodo a atención médica de primera línea. Cuando ocurra un problema médico serio, el médico familiar podrá ordenar análisis e imágenes de laboratorio, tales como rayos X, exploraciones CAT y de MRI. Después, los resultados e imágenes se podrían enviar en forma electrónica a un especialista, quien a continuación daría el diagnóstico.

Por lo general, a los doctores no les gusta hacer diagnósticos a partir de imágenes de computadora, a menos que la calidad de la imagen transmitida sea tan buena como la del original. Este requerimiento significa que las imágenes probablemente necesitarán $4K \times 4K$ pixeles, con 8 bits por pixel (imágenes en blanco y negro) o 24 bits por pixel (imágenes en color). Puesto que muchos exámenes requieren hasta 100 imágenes (por ejemplo, diferentes secciones transversales del órgano en cuestión), una sola serie para un paciente puede generar 40 gigabits. Las imágenes en movimiento (por ejemplo, un corazón que late) generan todavía más datos. La compresión puede ayudar un poco, pero los doctores están recelosos de ella, pues los algoritmos más eficientes reducen la calidad de la imagen. Además, todas las imágenes se deben almacenar durante años, pero podría ser necesario recuperarlas de inmediato en el caso de una emergencia médica. Los hospitales no quieren convertirse en centros de cómputo, de manera que es esencial el almacenamiento fuera de la localidad en combinación con la recuperación electrónica de alto ancho de banda.

Otra aplicación de gigabits es la reunión virtual. Cada sala de juntas contiene una cámara esférica y una o más personas. Las corrientes de bits de cada cámara se combinan en forma electrónica para dar la ilusión de que todos los participantes están en la misma sala. Cada persona ve esta imagen con anteojos de realidad virtual. De esta forma, las reuniones se pueden efectuar sin viajes pero, una vez más, las velocidades de transmisión de datos requeridas son enormes.

A partir de 1989, la ARPA y la NSF acordaron en forma conjunta financiar varias plataformas de pruebas de gigabits en universidades y en la industria y más tarde como parte del proyecto NREN. En algunas de ellas, la velocidad de los datos en cada dirección era de 622 Mbps, así que solamente contando los datos en ambas direcciones se lograba un gigabit. A veces a esta clase de gigabit se le llama "gigabit del gobierno". (Algunos cínicos lo llaman gigabit después de impuestos.) A continuación mencionaremos en forma breve los primeros cinco proyectos que ya han cumplido con su misión y se han clausurado, pero merecen cierto crédito como pioneros, de la misma manera en que lo merece la ARPANET.

1. **Aurora** era una plataforma de pruebas que enlazaba a cuatro localidades del noreste de Estados Unidos: el M.I.T., la Universidad de Pennsylvania, el laboratorio T. J. Watson de IBM y Bellcore (Morristown, N. J.) a 622 Mbps mediante el uso de fibra óptica proporcionada por MCI, Bell Atlantic y NYNEX. Aurora se diseñó principalmente para ayudar a depurar el conmutador Sunshine de Bellcore y el conmutador (patentado) plaNET de IBM mediante el uso de redes paralelas. Las consideraciones de investigación incluyeron la tecnología de conmutación, los protocolos de gigabits, el ruteo, el control de red, la memoria virtual distribuida y la colaboración mediante videoconferencias. Para mayor información, véase (Clark *et al.*, 1993).

2. **Blanca** originalmente fue un proyecto de investigación llamado XUNET en el que intervinieron los Laboratorios Bell de AT&T, Berkeley y la Universidad de Wisconsin. En 1990 se añadieron algunas localidades nuevas (LBL, Cray Research y la Universidad de Illinois) y se logró financiamiento de NSF/ARPA. Una parte operaba a 622 Mbps, pero otras lo hacían a velocidades más bajas. Blanca fue la única plataforma de pruebas de cobertura nacional; el resto fueron regionales. En consecuencia, gran parte de la investigación se ocupaba de los efectos del retardo de la velocidad de la luz. Aquí el interés estaba en los protocolos, en especial los protocolos de control de red, las interfaces de *hosts* y las aplicaciones de gigabits, como las imágenes médicas, los modelos meteorológicos y la radioastronomía. Para más información, véase (Catlett, 1992, y Fraser, 1993).

3. **CASA** estaba dirigido a la investigación en aplicaciones de supercomputadoras, sobre todo aquellas en las que una parte del problema se ejecutaba mejor en un tipo de supercomputadora (por ejemplo, una Cray vectorial), y otra parte se ejecutaba mejor en una clase diferente de supercomputadora (por ejemplo, una paralela). Las aplicaciones que se investigaron incluyeron aplicaciones de geología (mediante el análisis de las imágenes del Landsat), modelado del clima, y comprensión de reacciones químicas. CASA operaba en California y Nuevo México y conectaba a Los Álamos, Cal Tech, JPL y el Centro de Supercomputadoras de San Diego.

4. **Nectar** difirió de las tres plataformas mencionadas anteriormente en que fue una MAN experimental de gigabits que operaba desde la CMU al Centro de Supercomputadoras de Pittsburgh. Los diseñadores estaban interesados en aplicaciones relacionadas con la diagramación de procesos químicos y la investigación de operaciones, así como las herramientas para depurarlos.

5. **VISTAnet** fue una pequeña plataforma de pruebas de gigabits en Research Triangle Park, Carolina del Norte, que conectaba a la Universidad de Carolina del Norte, la Universidad Estatal de Carolina del Norte y MCNC. Aquí el interés estaba en un prototipo para una red pública conmutada de gigabits en la que los conmutadores tenían cientos de líneas de gigabits, lo que significaba que los conmutadores tenían que ser capaces de procesar terabits/seg. La investigación científica se centró en el uso de imágenes en tercera dimensión para planear la terapia con radiaciones de pacientes de cáncer, en la que el oncólogo fuera capaz de variar los parámetros del haz y ver en forma instantánea las dosis de radiación que llegaban al tumor y a los tejidos circundantes (Ransom, 1992).

1.6. EJEMPLOS DE SERVICIOS DE COMUNICACIÓN DE DATOS

Las compañías de teléfonos y de otro tipo ya empezaron a ofrecer servicios de red a cualquier organización que desee suscribirse. La subred es propiedad del operador de la red y proporciona el servicio de comunicación a las *hosts* y terminales del cliente. Tal sistema se llama **red**

pública; es análogo al sistema telefónico público y con frecuencia es parte de él. En la figura 1-4 vimos ya en forma breve un servicio nuevo, DQDB. En las siguientes secciones estudiaremos otros cuatro ejemplos de servicios: SMDS, X.25, relevo de marcos (*frame relay*) y la ISDN de banda ancha.

1.6.1. SMDS — Servicio de datos conmutado de multimegabits

El primer servicio que veremos, **SMDS** (*switched multimegabit data service,* **servicio de datos conmutado de multimegabits**) se diseñó para conectar entre sí múltiples LAN, en muchos casos en las sucursales y en las fábricas de una sola compañía. SMDS fue diseñado por Bellcore en la década de 1980 y fue puesto en funciones a principios de la década de 1990 por portadoras regionales y algunas de larga distancia. La meta era producir un servicio de datos de alta velocidad e inaugurarlo con un mínimo de escándalo. SMDS fue el primer servicio conmutado de banda ancha (esto es, de alta velocidad) que se ofreció al público.

Como ejemplo de situación en la que es útil el SMDS, consideremos una compañía con cuatro oficinas en cuatro ciudades diferentes, cada una con su propia LAN. A la compañía le gustaría conectar todas las LAN, de modo que los paquetes puedan ir de una LAN a otra. Una solución sería rentar seis líneas de alta velocidad y conectar por completo las LAN, según se muestra en la figura 1-27(a). Ciertamente, tal solución es posible pero cara.

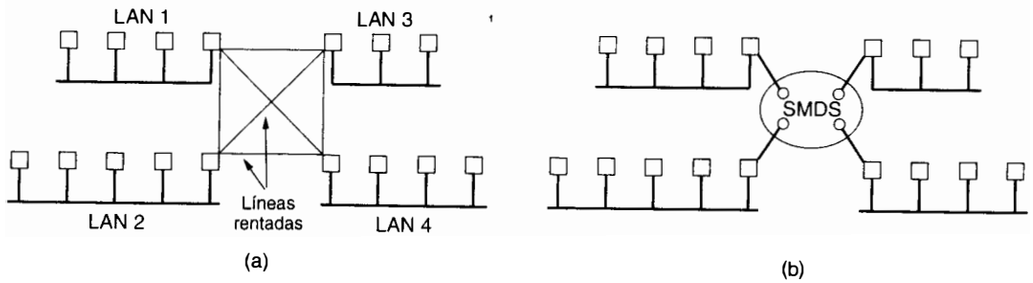

Figura 1-27. (a) Cuatro LAN interconectadas con líneas rentadas. (b) Interconexión mediante SMDS.

Una solución alterna es usar SMDS, como se muestra en la figura 1-27(b). La red SMDS actúa como un *backbone* de LAN de alta velocidad que permite que fluyan los paquetes de una LAN a cualquier otra. Entre las LAN de las oficinas del cliente y la red SMDS en las oficinas de la compañía de teléfonos está una línea de acceso (corta) rentada a la compañía de teléfonos. Por lo general, esta línea es una MAN y usa DQDB, pero también podría haber otras opciones.

Mientras que la mayoría de los servicios de las compañías de teléfonos se diseñan para tráfico continuo, SMDS está diseñado para manejar tráfico en ráfagas. En otras palabras, muy de vez en cuando se tiene que transportar con rapidez un paquete de una LAN a otra, pero gran parte del tiempo no hay tráfico de LAN a LAN. La solución de la línea rentada de la figura 1-27(a) tiene el problema de las altas cuentas mensuales; una vez instaladas, el cliente debe pagar las

líneas, se usen o no en forma continua. Para tráfico intermitente, las líneas rentadas son una solución cara, y SMDS tiene un precio muy competitivo. Con n LAN, una red de líneas rentadas completa requiere rentar $n(n-1)/2$ líneas que podrían ser largas (es decir, caras), mientras que SMDS requiere rentar solamente n líneas cortas de acceso al enrutador de SMDS más cercano.

Puesto que el objetivo de SMDS es transportar tráfico de LAN a LAN, debe tener la suficiente rapidez para efectuar el trabajo. La velocidad estándar es de 45 Mbps, aunque a veces se puede optar por velocidades más bajas. Las MAN también pueden operar a 45 Mbps pero no son conmutadas; esto es, para conectar cuatro LAN mediante una MAN, la compañía de teléfonos tendría que operar un solo cable de la LAN 1 a la LAN 2 a la LAN 3 a la LAN 4, lo que sólo es posible si están en la misma ciudad. Con SMDS, cada LAN se conecta con el conmutador de una compañía de teléfonos que encamina paquetes por conducto de la red SMDS según se necesite para alcanzar el destino, posiblemente atravesando múltiples conmutadores en el proceso.

El servicio básico de SMDS es un simple servicio de entrega de paquetes sin conexión. El formato del paquete se muestra en la figura 1-28 y tiene tres campos: el destino (a dónde va el paquete), la fuente (quién lo envía) y un campo de longitud variable que es la carga útil de hasta 9188 bytes de datos de usuario. En la LAN que envía, la máquina conectada a la línea de acceso pone el paquete en dicha línea, y SMDS hace su mejor esfuerzo por entregarlo en el destino correcto. No se da garantía.

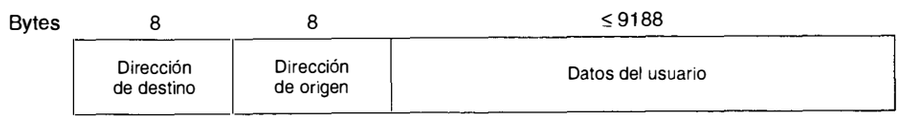

Figura 1-28. Formato del paquete SMDS.

Las direcciones de origen y de destino consisten en un código de 4 bits seguido de un número telefónico de hasta 15 dígitos decimales. Cada dígito se codifica en un campo de 4 bits. Los números telefónicos contienen el código del país, el código de área y el número de suscriptor, de modo que el servicio podría llegar a ofrecerse a nivel internacional. Se pensó que tener números telefónicos decimales como direcciones de red haría que el nuevo servicio pareciera familiar a los usuarios recelosos.

Cuando un paquete llega a la red SMDS, el primer enrutador verifica que la dirección de origen corresponda a la línea entrante, para prevenir fraudes de facturación. Si la dirección es incorrecta el paquete simplemente se descarta; si es correcta, el paquete se envía hacia su destino.

La difusión es una característica útil de SMDS. El cliente puede especificar una lista de números telefónicos de SMDS y pedir que se asigne un número especial a la lista completa. Cualquier paquete que se envíe a ese número se entregará a todos los miembros de la lista. La Asociación Nacional de Comerciantes en Valores de Estados Unidos usa esta característica del servicio SMDS de MCI para difundir los precios de acciones nuevos a todos sus 5000 miembros.

Una función de usuario adicional es la preselección de direcciones de los paquetes tanto salientes como entrantes. Con la preselección saliente, el cliente puede dar una lista de números de teléfono y especificar que no se envíen paquetes a ninguna otra dirección. Con preselección entrante, sólo se aceptarán los paquetes de ciertos números de teléfono preespecificados. Cuando se habilitan ambas funciones, el usuario puede construir efectivamente una red privada sin conexiones SMDS al mundo exterior. Para las compañías con datos confidenciales, esta función es muy valiosa.

La carga útil puede contener cualquier secuencia de bytes que desee el usuario, hasta 9188 bytes; SMDS no la ve. La carga puede contener un paquete Ethernet, un paquete *token ring* de IBM, un paquete IP o cualquier otro. Cualquier cosa presente en el campo de carga útil se transferirá sin modificaciones de la LAN de origen a la de destino.

SMDS maneja el tráfico por ráfagas de la manera siguiente. El enrutador conectado a cada línea de acceso contiene un contador que se incrementa a velocidad constante, digamos una vez cada 10 mseg. Cuando llega un paquete al enrutador, se verifica si el contador es mayor que la longitud del paquete en bytes. Si lo es, el paquete se envía sin retardo y el contador disminuye en un número igual a la longitud del paquete. Si la longitud del paquete es mayor que el contador, el paquete se descarta.

En efecto, con un pulso cada 10 μseg, el usuario puede enviar a una velocidad *promedio* de 100,000 bytes/seg, pero la velocidad de ráfaga puede ser mucho mayor. Por ejemplo, si la línea ha estado desocupada durante 10 mseg, el contador estará en 1000 y se permitirá al usuario que envíe una ráfaga de 1 kB a la velocidad máxima de 45 Mbps, de modo que se transmitirá en aproximadamente 180 μseg. Con una línea rentada de 100,000 bytes/seg, el mismo kilobyte tardaría 10 mseg. Así, SMDS ofrece retardos cortos para ráfagas de datos independientes muy espaciadas, mientras que la velocidad promedio permanece por debajo del valor acordado. Este mecanismo pro-porciona respuesta rápida cuando se necesita pero evita que los usuarios utilicen más ancho de banda del que han acordado pagar.

1.6.2. Redes X.25

Muchas redes públicas antiguas, en especial fuera de Estados Unidos, siguen un estándar llamado **X.25** que la CCITT desarrolló durante la década de 1970 para proveer una interfaz entre las redes públicas de conmutación de paquetes y sus clientes.

El protocolo de la capa física, llamado **X.21**, especifica la interfaz física, eléctrica y de procedimientos entre el *host* y la red. En realidad, muy pocas redes públicas manejan este estándar, pues requiere señalamiento digital en lugar de analógico en las líneas telefónicas. Como medida provisional, se definió una interfaz analógica similar al estándar RS-232, tan conocido.

El estándar de la capa de enlace de datos tiene algunas variaciones (ligeramente incompatibles), todas las cuales se diseñaron para manejar los errores de transmisión en la línea telefónica entre el equipo del usuario (*host* o terminal) y la red pública (enrutador).

El protocolo de la capa de red se ocupa de la asignación de direcciones, el control de flujo, la confirmación de entrega, las interrupciones y otras consideraciones relacionadas. Básicamente, este protocolo permite al usuario establecer circuitos virtuales y después enviar paquetes de

hasta 128 bytes a través de ellos. Estos paquetes se entregan en forma confiable y en orden. La mayor parte de las redes X.25 trabajan a velocidades de hasta 64 kbps, lo cual las hace obsoletas para muchos propósitos. No obstante, su uso aún es extenso, por lo que conviene que los lectores sepan de su existencia.

X.25 está orientado a la conexión y trabaja con circuitos virtuales tanto conmutados como permanentes. Un **circuito virtual conmutado** se crea cuando una computadora envía un paquete a la red y pide que se haga una llamada a una computadora remota. Una vez establecida la conexión, los paquetes se pueden enviar por ella y siempre llegarán en orden. X.25 proporciona control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento u ocupado.

Un **circuito virtual permanente** se usa de la misma forma que uno conmutado pero se establece previamente por un acuerdo entre el cliente y la portadora; siempre está presente y no se requiere una llamada que lo establezca para poder usarlo. Un circuito de este tipo es semejante a una línea rentada.

Puesto que el mundo todavía está lleno de terminales que no hablan X.25, se definió otro grupo de normas que describen cómo una terminal ordinaria (no inteligente) se comunica con una red pública X.25. En efecto, el usuario o el operador de la red instala una "caja negra" a la que se pueden conectar estas terminales. La caja negra se llama **PAD** (*packet assembler disassembler,* **ensamblador-desensamblador de paquetes**) y su función se describe en un documento denominado **X.3**. Se definió un protocolo estándar entre la terminal y el PAD, el **X.28**, y existe otro protocolo estándar entre el PAD y la red, el **X.29**. Estas tres recomendaciones juntas se conocen como **triple X**.

1.6.3. *Frame relay*

El ***frame relay*** (retransmisión de marco) es un servicio para personas que quieren una forma lo más austera posible, orientada a la conexión, para mover bits de *A* a *B* a una velocidad razonable y bajo costo (Smith, 1993). Su existencia se debe a cambios en la tecnología en las últimas dos décadas. Hace 20 años, la comunicación a través de líneas telefónicas era lenta, analógica y no confiable, y las computadoras eran lentas y caras. En consecuencia, se requirieron protocolos complejos para enmascarar los errores, pero las computadoras de los usuarios eran demasiado caras para ponerlas a hacer este trabajo.

La situación ha cambiado en forma radical. Ahora, las líneas telefónicas rentadas son rápidas, digitales y confiables, y las computadoras son rápidas y baratas. Esto sugiere el uso de protocolos simples, con la mayor parte del trabajo realizada por las computadoras de los usuarios en vez de la red. Éste es el ambiente para el que está pensado el *frame relay.*

Se puede pensar en el *frame relay* como una línea virtual rentada. El cliente renta un circuito virtual permanente entre dos puntos y entonces puede enviar marcos o *frames* (es decir, paquetes) de hasta 1600 bytes entre ellos. También es posible rentar circuitos virtuales permanentes entre un lugar determinado y muchas otras localidades, de modo que cada marco lleve un número de 10 bits que le diga cuál circuito virtual usar.

La diferencia entre una línea rentada real y una virtual es que, con una real, el usuario puede enviar tráfico durante todo el día a máxima velocidad. Con una línea virtual se pueden enviar ráfagas de datos a toda velocidad, pero el uso promedio a largo plazo deberá ser inferior a un

nivel predeterminado. A cambio, la portadora cobra mucho menos por una línea virtual que por una física. Además de competir con las líneas rentadas, el *frame relay* también compite con los circuitos virtuales permanentes de X.25, excepto que opera a altas velocidades, usualmente a 1.5 Mbps, y ofrece menos funciones.

El *frame relay* proporciona un servicio mínimo que básicamente es una forma de determinar el inicio y el fin de cada marco y de detectar errores de transmisión. Si se recibe un marco defectuoso, el *frame relay* simplemente lo descarta. Corresponde al usuario descubrir que se perdió un bloque y emprender la acción necesaria para recuperarlo. A diferencia de X.25, *frame relay* no proporciona acuses de recibo ni control de flujo normal. Sin embargo, tiene un bit en el encabezado que un extremo de la conexión puede encender para indicar al otro que hay problemas. El uso de este bit es opción de los usuarios.

1.6.4. ISDN de banda ancha y ATM

Aun si los servicios antes mencionados llegaran a ser populares, las compañías telefónicas enfrentan todavía un problema mucho más fundamental: las redes múltiples. El POTS o *plain old telephone service* (el antiguo servicio telefónico ordinario) y Telex utilizan la red antigua de circuitos conmutados. Todos los nuevos servicios de datos, como SMDS y *frame relay*, emplean sus propias redes de conmutación de paquetes. DQDB es diferente, y la red interna de administración de llamadas de la compañía de teléfonos (SSN 7) es otra red adicional. Mantener todas estas redes individuales es un dolor de cabeza mayúsculo, y existe otra red, la de televisión por cable, que las compañías de teléfonos no controlan pero que les gustaría controlar.

La solución que se percibe es inventar una nueva red única para el futuro que reemplazará a todo el sistema telefónico y a todas las redes especializadas por una sola red integrada para todos los tipos de transferencia de información. Esta nueva red tendrá una velocidad de transmisión muy elevada en comparación con todos servicios y redes existentes y hará posible ofrecer una gran variedad de servicios nuevos. Este proyecto no es pequeño y ciertamente no va a suceder de la noche a la mañana, pero ya está en camino.

El nuevo servicio de área amplia se llama **B-ISDN** (*broadband integrated services digital network,* **red digital de servicios integrados de banda ancha**); ofrecerá vídeo sobre pedido, televisión en vivo de muchas fuentes, correo electrónico en multimedia de movimiento total, música con calidad de disco compacto, interconexión de LAN, transporte de alta velocidad para datos científicos e industriales y muchos otros servicios en los que ni siquiera se ha pensado, todo por la línea telefónica.

La tecnología subyacente que hace posible la B-ISDN se llama **ATM** (*asynchronous transfer mode*, **modo de transferencia asíncrono**) debido a que no es síncrono (atado a un reloj maestro), como lo está la mayor parte de las líneas telefónicas de larga distancia. Cabe señalar que el acrónimo ATM nada tiene que ver aquí con los cajeros automáticos o *automated teller machines* que ofrecen muchos bancos (aunque un cajero automático puede usar una red ATM para hablar con su banco).

Se ha trabajado mucho en ATM y en el sistema B-ISDN que lo usa, aunque todavía hay más por hacer. Para más información sobre este tema, véase (Fischer *et al.*, 1994; Gasman, 1994; Goralski, 1995; Kim *et al.*, 1994; Kyas, 1995; McDysan y Spohn, 1995, y Stallings, 1995a).

La idea en que se basa la ATM consiste en transmitir toda la información en paquetes pequeños de tamaño fijo llamados **células**. Las celdas tienen una longitud de 53 bytes, de los cuales cinco son de encabezado y 48 de carga útil, según se muestra en la figura 1-29. ATM es tanto una tecnología (oculta a los usuarios) como un servicio potencial (visible a los usuarios). A veces se llama al servicio **cell relay**, como analogía con *frame relay*.

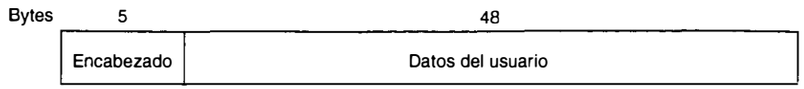

Figura 1-29. Una celda ATM.

El uso de una tecnología de conmutación de celdas es un rompimiento drástico con la tradición centenaria de la conmutación de circuitos (estableciendo una trayectoria de cobre) dentro del sistema de teléfonos. Son muchas las razones por las que se escogió la conmutación de celdas, entre ellas están las siguientes. Primero, la conmutación de celdas es altamente flexible y puede manejar con facilidad tanto tráfico de velocidad constante (audio, vídeo) como variable (datos). Segundo, a las velocidades tan altas que se contemplan (los gigabits por segundo están al alcance de la mano), la conmutación digital de las celdas es más fácil que el empleo de las técnicas tradicionales de multiplexión, en especial si se usa fibra óptica. Tercero, para la distribución de televisión es esencial la difusión; esto lo puede proporcionar la conmutación de celdas pero no la de circuitos.

Las redes ATM son orientadas a la conexión. Para hacer una llamada primero se debe enviar un mensaje para establecer la conexión. Después, todas las celdas subsecuentes siguen la misma trayectoria al destino. La entrega de celdas no está garantizada, pero sí su orden. Si las celdas 1 y 2 se envían en ese orden, y ambas llegan, lo harán en ese orden, nunca la 2 primero y después la 1.

Las redes ATM se organizan como las WAN tradicionales, con líneas y conmutadores (enrutadores). Las velocidades pretendidas para las redes ATM son de 155 Mbps y 622 Mbps, con la posibilidad de tener velocidades de gigabits más adelante. La velocidad de 155 Mbps se escogió porque es cercana a lo que se necesita para transmitir televisión de alta definición. La elección exacta de 155.52 Mbps se hizo por compatibilidad con el sistema de transmisión SONET de AT&T. La velocidad de 622 Mbps se eligió para que se pudieran mandar por ella cuatro canales de 155 Mbps. Ahora debe quedar claro por qué algunas de las plataformas de pruebas de gigabits operaban a 622 Mbps; usaban ATM.

Cuando se propuso ATM, virtualmente toda la discusión (esto es, la propaganda) era acerca del vídeo sobre pedido en cada hogar y el reemplazo del sistema de telefonía, según se describió antes. Desde entonces se han vuelto importantes otros avances. Muchas organizaciones han agotado el ancho de banda en las LAN de sus campus o edificios y se están viendo forzadas a recurrir a alguna clase de sistema de conmutación que tenga más ancho de banda que una sola LAN. También, en la computación cliente-servidor algunas aplicaciones necesitan hablar con ciertos servidores a velocidad elevada. Ciertamente, ATM es un candidato importante para ambos tipos de aplicación. Sin embargo, resulta un poco frustrante pasar de la meta de reemplazar todo el sistema telefónico de baja velocidad por uno digital de alta velocidad, a la meta de

tratar de conectar todas las Ethernets de una universidad. La interconexión de LAN mediante ATM se trata en (Kavak, 1995; Newman, 1994, y Truong *et al.*, 1995).

También vale la pena señalar que las diferentes organizaciones comprometidas con ATM tienen diversos intereses (financieros). Las portadoras de telefonía de larga distancia y las PTT se interesan principalmente en usar ATM para elevar el nivel del sistema telefónico y competir con las compañías de televisión por cable en la distribución electrónica de vídeo. Los vendedores de computadoras ven las LAN de ATM para universidades como el gran negocio (para ellos). Todos estos intereses opuestos no hacen más fácil, rápido ni coherente el proceso de estandarización actual. También, la política y el poder dentro de la organización que estandariza ATM (el ATM Forum) tienen una influencia considerable sobre la dirección que seguirá ATM.

El modelo de referencia B-ISDN ATM

Regresemos ahora a la tecnología de ATM, especialmente su aplicación en el sistema telefónico (futuro). La ISDN de banda ancha con ATM tiene su propio modelo de referencia, diferente del modelo OSI y también del modelo TCP/IP. Este modelo se muestra en la figura 1-30 y consiste en tres capas: la capa física, la capa ATM y la capa de adaptación de ATM, más cualquier cosa que los usuarios quieran poner encima.

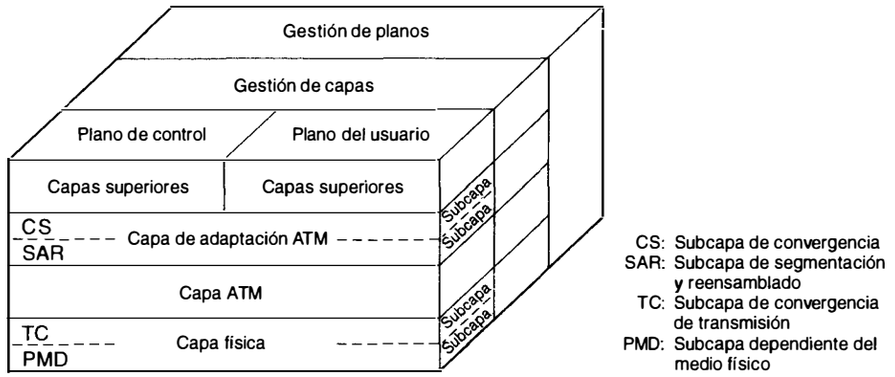

Figura 1-30. El modelo de referencia B-ISDN ATM.

La capa física tiene que ver con el medio físico: voltajes, temporización de bits y varias consideraciones más. ATM no prescribe un conjunto de reglas en particular, pero en cambio dice que las celdas ATM se pueden enviar por sí solas por un cable o fibra o bien se pueden empacar dentro de la carga útil de otros sistemas portadores. En otras palabras, ATM se diseñó para que fuera independiente del medio de transmisión.

La **capa ATM** tiene que ver con las celdas y su transporte; define la organización de las celdas y dice lo que significan los campos del encabezado. Esta capa también tiene que ver con el establecimiento y la liberación de circuitos virtuales y aquí es donde se localiza el control de la congestión.

Se ha definido una capa sobre la capa ATM que permita a los usuarios enviar paquetes mayores que una celda porque la mayor parte de las aplicaciones no quieren trabajar de manera directa con celdas (aunque algunas puedan hacerlo). La interfaz ATM segmenta estos paquetes, transmite las celdas en forma individual y las reensambla en el otro extremo. Esta capa es la **AAL** (*ATM adaptation layer,* **capa de adaptación de ATM**).

A diferencia de los antiguos modelos de referencia bidimensionales, el modelo ATM se define en tres dimensiones, como se muestra en la figura 1-30. El **plano de usuario** se encarga del transporte de los datos, el control de flujo, la corrección de errores y otras funciones de usuario. En contraste, el **plano de control** tiene que ver con la administración de la conexión. Las funciones de gestión de capas y planos se relacionan con la administración de recursos y la coordinación intercapas.

Las capas física y AAL se dividen, cada una, en dos subcapas, una en el fondo que hace el trabajo y una subcapa de convergencia en la parte superior que proporciona la interfaz adecuada con la capa de arriba. En la figura 1-31 se indican las funciones de las capas y subcapas.

Capa OSI	Capa ATM	Subcapa ATM	Funcionalidad
3/4	AAL	CS	Proporciona la interfaz estándar (convergencia)
		SAR	Segmentación y reensamblado
2/3	ATM		Control de flujo Generación/extracción de encabezados de la celda Gestión de circuitos/trayectorias virtuales Multiplexión/desmultiplexión de celdas
2	Física	TC	Desacoplamiento de la velocidad de envio de celdas Generación y comprobación de la suma de verificación del encabezado Generación de celdas Empacado/desempacado de celdas de la envoltura que las encierra Generación de marcos
1		PMD	Temporización de bits Acceso físico a la red

Figura 1-31. Las capas y subcapas de ATM y sus funciones.

La subcapa **PMD** (*physical medium dependent,* **dependiente del medio físico**) establece la interfaz con el cable real; transfiere los bits y controla su temporización. Esta capa es diferente para diferentes portadoras y cables.

La otra subcapa de la capa física es la subcapa **TC** (*transmission convergence,* **convergencia de transmisión**). Cuando se transmiten las celdas, la capa TC las envía como una corriente de bits a la capa PMD, lo cual es fácil de hacer. En el otro extremo, la subcapa TC obtiene una corriente entrante de puros bits de la subcapa PMD; su trabajo es convertir esta corriente de bits

en una corriente de celdas para la capa ATM. La subcapa TC se encarga de todas las consideraciones que se relacionan con determinar dónde empiezan y dónde terminan las celdas en la corriente de bits. En el modelo ATM, esta funcionalidad pertenece a la capa física. En el modelo OSI y en casi todas las demás redes, el trabajo de enmarcar, esto es, de convertir una corriente de bits en bruto en una secuencia de marcos o celdas, es tarea de la capa de enlace de datos. Por esa razón la estudiaremos en este libro junto con la capa de enlace de datos, no con la capa física.

Como mencionamos al principio, la capa ATM maneja celdas, lo que incluye su generación y transporte. Aquí se localiza la mayor parte de los aspectos interesantes de ATM. La capa ATM es una mezcla de las capas de enlace de datos y de red de OSI, pero no se divide en subcapas.

La capa AAL se divide en la subcapa **SAR** (*segmentation and reassembly,* **segmentación y rensamblado**) y la **CS** (*convergence sublayer,* **subcapa de convergencia**). La subcapa inferior divide los paquetes en celdas en el lado de la transmisión y los vuelve a armar de nuevo en el destino. La subcapa superior hace posible tener sistemas ATM que ofrezcan diferentes clases de servicios a diferentes aplicaciones (por ejemplo, la transferencia de archivos y el vídeo sobre pedido tienen diferentes necesidades en lo concerniente a manejo de errores, temporización, etcétera).

Perspectiva de ATM

En gran medida, ATM es un proyecto inventado por la industria telefónica porque después de que se instaló ampliamente Ethernet, la industria de las computadoras nunca apoyó una tecnología de redes de alta velocidad específica para hacerla estándar. Las compañías de teléfonos llenaron este vacío con ATM, aunque en octubre de 1991 muchos proveedores de computadoras se unieron con las compañías de teléfonos para armar el **ATM Forum**, un grupo de industriales que guiará el futuro de ATM.

Aunque ATM promete tener la capacidad de entregar la información en cualquier parte a velocidades que pronto excederán de 1 Gbps, el cumplimiento de esta promesa no será fácil. Básicamente, ATM es un conmutador de paquetes de alta velocidad, una tecnología con la que las compañías de teléfonos tienen poca experiencia. Lo que sí tienen es una inversión enorme en una tecnología diferente (la conmutación de circuitos) que en concepto no ha cambiado desde los días de Alexander Graham Bell. No es necesario decir que esta transición no ocurrirá rápidamente, sobre todo porque es un cambio revolucionario en lugar de ser evolucionario, y las revoluciones nunca ocurren suavemente.

También se deben considerar los aspectos económicos de instalar ATM en todo el mundo. Se tendrá que reemplazar una fracción sustancial del sistema telefónico existente. ¿Quién pagará esto? ¿Cuánto están dispuestos a pagar los usuarios por obtener una película sobre pedido en forma electrónica, cuando pueden obtener una en la tienda local de vídeos por un par de dólares? Finalmente, la pregunta de dónde se proveerán muchos de los servicios avanzados es crucial. Si la red los suministra, las compañías telefónicas se beneficiarán con ellos. Si los proporcionan computadoras conectadas a la red, los fabricantes y operadores de estos aparatos obtendrán las ganancias. Puede que a los usuarios no les importe, pero sin duda a las compañías de teléfonos y a los fabricantes de computadoras sí les importará, y de seguro que esto afectará su interés en lograr que ATM tenga éxito.

1.6.5. Comparación de los servicios

El lector podrá preguntarse por qué existen tantos servicios incompatibles y que se traslapan, incluidos DQDB, SMDS, X.25, *frame relay,* ATM y otros más. La razón fundamental es la decisión tomada en 1984 de dividir la AT&T y fomentar la competencia en la industria de las telecomunicaciones. Ahora, varias compañías con intereses y tecnologías diferentes están en libertad de ofrecer cualquier servicio para el que crean que existe una demanda, y muchas de ellas hacen esto sin contemplaciones.

Para repasar un poco sobre los servicios que hemos mencionado en este capítulo: DQDB es una tecnología de MAN no conmutada que permite enviar celdas de 53 bytes (de los cuales 44 son carga útil) por una línea larga dentro de una ciudad. SMDS es una tecnología de datagramas conmutados para enviar datagramas a cualquier punto de una red a 45 Mbps. X.25 es una tecnología antigua de redes orientada a la conexión para transmitir paquetes pequeños de tamaño variable a 64 kbps. *Frame relay* es un servicio que proporciona líneas rentadas virtuales con velocidades de alrededor de 1.5 Mbps. Finalmente, ATM se diseñó para reemplazar todo el sistema de teléfonos de conmutación de circuitos por uno de conmutación de celdas y poder manejar tanto datos como televisión. En la figura 1-32 se resumen algunas diferencias entre estos competidores.

Aspecto	DQDB	SMDS	X.25	*Frame relay*	ATM AAL
Orientado a la conexión	Sí	No	Sí	Sí	Sí
Velocidad normal (Mbps)	45	45	.064	1.5	155
Conmutado	No	Sí	Sí	No	Sí
Carga útil de tamaño fijo	Sí	No	No	No	No
Carga útil máxima	44	9188	128	1600	Variable
Circuitos virtuales permanentes	No	No	Sí	Sí	Sí
Multidifusión	No	Sí	No	No	Sí

Figura 1-32. Diferentes servicios de redes.

1.7. ESTANDARIZACIÓN DE REDES

Hay muchos proveedores de servicios de red, cada uno con sus propias ideas acerca de cómo deben hacerse las cosas. Sin coordinación, existiría un caos completo, y los usuarios nunca lograrían hacer nada. La única manera es acordar ciertos estándares de redes.

Los estándares no sólo permiten a diferentes computadoras comunicarse, sino que también incrementan el mercado para los productos que se ajustan a la norma, lo cual conduce a la

producción en masa, las economías de escala en la producción, las implementaciones VLSI, y otros beneficios que disminuyen el precio y aumentan la aceptación posterior. En las siguientes secciones veremos rápidamente el importante pero poco conocido mundo de la estandarización internacional.

Las normas se dividen en dos categorías: *de facto* y *de jure*. ***De facto*** (del latín "del hecho") son aquellos estándares que simplemente aparecieron, sin ningún plan formal. La PC de IBM y sus sucesores son normas *de facto* para computadoras pequeñas de oficina porque docenas de fabricantes decidieron copiar las máquinas IBM con mucha exactitud. UNIX es el estándar *de facto* para los sistemas operativos en los departamentos de ciencias de la computación de las universidades.

Los estándares **de jure** (del latín "por ley"), en contraste, son estándares formales y legales adoptados por algún organismo de estandarización autorizado. Las autoridades internacionales de estandarización generalmente se dividen en dos clases: las establecidas por tratados entre los gobiernos de las naciones y las organizaciones voluntarias, no surgidas de un tratado. En el área de las normas para redes de computadoras existen varias organizaciones de cada tipo, las cuales veremos a continuación.

1.7.1. Quién es quién en el mundo de las telecomunicaciones

La situación legal de las compañías telefónicas del mundo varía considerablemente de un país a otro. En un extremo está Estados Unidos, con 1500 compañías telefónicas privadas. Antes de que la AT&T se dividiera en 1984 era la corporación más grande del mundo y dominaba completamente la escena; proporcionaba servicio telefónico a cerca del 80% de los teléfonos instalados en Estados Unidos, distribuidos en la mitad de su área geográfica, y todas las demás compañías combinadas daban servicio a los clientes restantes (en su mayoría rurales). Desde su división, AT&T continúa proporcionando servicio de larga distancia, aunque ahora en competencia con otras compañías. Las siete compañías operadoras Bell regionales que se separaron de AT&T y 1500 independientes proporcionan servicio telefónico local y celular. Algunas de estas compañías independientes, como GTE, son muy grandes.

Las compañías estadounidenses, que proporcionan servicios de comunicación al público se llaman **portadoras comunes**. Los precios y servicios de estas empresas están descritos en un documento llamado **tarifa**, el cual debe ser aprobado por la Comisión Federal de Comunicaciones para el tráfico interestatal e internacional, y por las comisiones de servicios públicos para el tráfico intraestatal.

En el otro extremo se encuentran los países en los que el gobierno nacional tiene un monopolio completo de todas las comunicaciones, incluidos el correo, el telégrafo, el teléfono, y frecuentemente también el radio y la televisión. La mayor parte del mundo pertenece a esta categoría. En algunos casos, la autoridad de telecomunicaciones es una compañía nacionalizada; en otros, es simplemente una rama del gobierno, usualmente conocida como la **PTT** (administración de **correo**, **telégrafo** y **teléfono**). La tendencia mundial es hacia la liberalización y competencia, alejándose del monopolio gubernamental.

Con todos estos proveedores de servicios diferentes, existe una clara necesidad de lograr la compatibilidad a escala mundial para asegurar que las personas (y las computadoras) de un país puedan llamar a sus homólogos en algún otro. En realidad, esta necesidad ha existido desde hace mucho tiempo. En 1865, representantes de muchos gobiernos europeos se reunieron para formar el predecesor de la actual **ITU** (*International Telecom Union,* **Unión Internacional de Telecomunicaciones**). La misión de la ITU fue estandarizar las telecomunicaciones internacionales, lo que en esos días significaba telegrafía. Aun entonces era claro que si una mitad de los países usaba código Morse y la otra usaba algún otro código, se iba a presentar un problema. Cuando el teléfono se convirtió en un servicio internacional, la ITU emprendió la tarea de estandarizar también la telefonía. En 1947 la ITU llegó a ser una agencia de las Naciones Unidas.

La ITU tiene tres sectores principales:

1. Sector de radiocomunicaciones (ITU-R).
2. Sector de estandarización de telecomunicaciones (ITU-T).
3. Sector de desarrollo (ITU-D).

La ITU-R se ocupa de la asignación de frecuencias de radio en todo el mundo a los grupos de interés en competencia. A nosotros nos concierne principalmente la ITU-T, que está relacionada con los sistemas telefónicos y de comunicación de datos. De 1956 a 1993, la ITU-T fue conocida como **CCITT** por las iniciales de su nombre en francés: Comité Consultatif International Télégraphique et Téléphonique. El 1° de marzo de 1993 se reorganizó el CCITT para hacerlo menos burocrático y cambió de nombre para reflejar su nuevo papel. Tanto la ITU-T como el CCITT emitieron recomendaciones en el área de las comunicaciones telefónicas y de datos. Entre las recomendaciones del CCITT hay una que todavía está en uso; tal es la X.25 de CCITT, aunque desde 1993 las recomendaciones llevan la etiqueta ITU-T.

La ITU-T tiene cinco clases de miembros:

1. Administraciones (PTT nacionales).
2. Operadores privados reconocidos (por ejemplo, AT&T, MCI, British Telecom).
3. Organizaciones regionales de telecomunicaciones (por ejemplo, la ETSI europea).
4. Organizaciones comerciales y científicas de telecomunicaciones.
5. Otras organizaciones interesadas (por ejemplo, redes bancarias y de aerolíneas).

La ITU-T tiene cerca de 200 administraciones, 100 operadores privados y varios cientos de miembros más. Únicamente las administraciones pueden votar, pero todos los miembros pueden participar en el trabajo de la ITU-T. Como Estados Unidos no tiene una PTT, alguien más tiene que representarlo en la ITU-T. Esta tarea recayó en el Departamento de Estado, probablemente con la excusa de que ITU-T tenía que ver con países extranjeros, la especialidad del Departamento de Estado.

La tarea de la ITU-T es hacer recomendaciones técnicas acerca de las interfaces de telefonía, telegrafía y comunicación de datos. A menudo estos estándares lograron reconocimiento internacional; por ejemplo, V.24 (también conocida como EIA RS-232 en Estados Unidos), que especifica la disposición y significado de las clavijas en el conector utilizado por la mayor parte de las terminales asíncronas.

Cabe señalar que las recomendaciones de la ITU-T técnicamente sólo son sugerencias que los gobiernos pueden adoptar o ignorar, según lo deseen. En la práctica, un país que desee adoptar un estándar telefónico distinto al del resto del mundo es libre de hacerlo, pero a expensas de aislarse de todos los demás. Esto podría funcionar en Albania, pero en cualquier otro lugar sería un problema real. La ficción de llamar a los estándares de la ITU-T "recomendaciones" fue y es necesaria para mantener apaciguadas a las fuerzas nacionalistas en muchos países.

El trabajo real de la ITU-T se realiza en grupos de estudio, que frecuentemente llegan a incluir hasta 400 personas. Para lograr que se haga algo, los grupos de estudio se dividen en partidas de trabajo, las cuales a su vez se dividen en equipos de expertos, mismos que se subdividen en grupos *ad hoc*. Los burócratas nunca dejarán de serlo.

A pesar de todo esto, la ITU-T ha conseguido que se hagan las cosas. Su producción actual es de cerca de 5000 páginas de recomendaciones al año. Los miembros contribuyen con cuotas para cubrir los gastos de la ITU. Los países grandes y ricos supuestamente pagan hasta 30 unidades de contribución al año; los países pequeños y pobres pueden arreglárselas para pagar sólo 1/16 de una unidad de contribución (que asciende a unos 250,000 dólares). Un testimonio del valor de la ITU-T lo constituye el hecho de que casi todo el mundo paga su contribución justa aun cuando las contribuciones son completamente voluntarias.

Conforme las telecomunicaciones completan la transición iniciada en la década de 1980 de ser enteramente nacionales a ser enteramente globales, las normas se harán cada vez más importantes y más y más organizaciones van a querer participar en su fijación. Para más información acerca de la ITU, véase (Irmer, 1994).

1.7.2. Quién es quién en el mundo de los estándares internacionales

Los estándares internacionales son producidos por la **ISO** (*International Standards Organization*†, **Organización Internacional de Estándares**), una organización voluntaria, no surgida de un tratado, fundada en 1946. Sus miembros son las organizaciones nacionales de estándares de los 89 países miembros. Estos miembros incluyen ANSI (Estados Unidos), BSI (Gran Bretaña), AFNOR (Francia), DIN (Alemania) y otros 85.

La ISO emite estándares sobre un vasto número de temas, que van desde tuercas y pernos (literalmente) al revestimiento de los postes telefónicos. Se han emitido más de 5000 estándares, incluido el estándar OSI. La ISO tiene casi 200 comités técnicos (TC), numerados en el orden de su creación, cada uno de los cuales se hace cargo de un tema específico. El TC1 se ocupa de tuercas y pernos (estandarizando los pasos de la rosca de los tornillos). El TC97 se ocupa de computadoras y procesamiento de información. Cada TC tiene subcomités (SC) divididos en grupos de trabajo (WG).

† Para los puristas, el verdadero nombre de la ISO es International Organization for Standardization.

El trabajo real se hace en gran parte en los WG por más de 100,000 voluntarios en todo el mundo. Muchos de estos "voluntarios" son asignados para trabajar en asuntos de la ISO por sus patrones, cuyos productos se están estandarizando. Otros voluntarios son oficiales gubernamentales interesados en que la forma en que se hacen las cosas en su país llegue a ser el estándar internacional. También participan expertos académicos en muchos de los WG.

En cuestiones de estándares de telecomunicaciones, la ISO y la ITU-T a menudo cooperan para evitar la ironía de tener dos estándares internacionales oficiales y mutuamente incompatibles (la ISO es un miembro de la ITU-T).

El representante de Estados Unidos en la ISO es el **ANSI** (*American National Standards Institute,* **Instituto Nacional Estadounidense de Estándares**), el cual, a pesar de su nombre, es una organización privada, no gubernamental y no lucrativa. Sus miembros son fabricantes, empresas de telecomunicaciones y otros particulares interesados. La ISO a menudo adopta los estándares ANSI como estándares internacionales.

El procedimiento que sigue la ISO para adoptar estándares está diseñado para lograr el mayor consenso posible. El proceso se inicia cuando una de las organizaciones nacionales de estándares siente la necesidad de un estándar internacional en alguna área. A continuación se forma un grupo de trabajo para proponer un **CD** (*committee draft,* **borrador de comité**). Luego se circula el CD a todos los miembros, los cuales tienen seis meses para criticarlo. Si una mayoría considerable aprueba el CD, se produce un documento revisado, llamado **DIS** (*draft international standard,* **borrador de estándar internacional**), y se circula para ser comentado y votado. Con base en los resultados de esta vuelta se prepara el texto final del **IS** (*international standard,* **estándar internacional**), se aprueba y se publica. En áreas de mucha controversia, un CD o un DIS podría pasar por varias versiones antes de obtener suficientes votos, y el proceso completo puede tardar años.

El **NIST** (*National Institute of Standards and Technology,* **Instituto Nacional de Estándares y Tecnología**) es una agencia del Departamento de Comercio de Estados Unidos, antiguamente conocida como Oficina Nacional de Estándares. Este organismo emite estándares que son obligatorios para las compras hechas por el gobierno de Estados Unidos, excepto las del Departamento de la Defensa, que tiene sus propios estándares.

Otro protagonista importante en el mundo de los estándares es el **IEEE** (*Institute of Electrical and Electronics Engineers,* **Instituto de Ingenieros Eléctricos y Electrónicos**), la organización profesional más grande del mundo. Además de publicar revistas y organizar numerosas conferencias cada año, el IEEE tiene un grupo de estandarización que elabora estándares en las áreas de ingeniería eléctrica y computación. El estándar 802 del IEEE para redes de área local es el estándar clave para las LAN, y posteriormente fue adoptado por la ISO como base para el estándar ISO 8802.

1.7.3. Quién es quién en el mundo de los estándares de Internet

El amplio mundo de la Internet tiene sus propios mecanismos de estandarización, muy diferentes de los de la ITU-T y la ISO. La diferencia puede resumirse en forma burda diciendo que la

gente que asiste a las juntas de estandarización de la ITU o la ISO usa traje. La gente que asiste a las juntas de estandarización de la Internet usa ya sea *jeans* o uniformes militares.

Las reuniones de la ITU-T y la ISO están pobladas por oficiales corporativos y burócratas para quienes la estandarización es su trabajo. Ellos consideran la estandarización como algo positivo y dedican sus vidas a ella. Por otro lado, la gente de Internet definitivamente prefiere la anarquía por cuestiones de principios, pero sabe que algunas veces se necesitan acuerdos para lograr que las cosas funcionen. Así pues, los estándares, aunque no debieran existir, son ocasionalmente necesarios.

Cuando se inició la ARPANET, el DoD creó un comité informal para supervisarla. En 1983, el comité fue rebautizado como **IAB** (*Internet Activities Board,* **Consejo de Actividades de Internet**) y se le encomendó una misión un poco más amplia, a saber, mantener a los investigadores que trabajaban con la ARPANET y la Internet apuntando más o menos en la misma dirección, una actividad no muy diferente de controlar una manada de gatos. El significado del acrónimo "IAB" se cambio más tarde a **Consejo de Arquitectura de Internet** (*Internet Architecture Board*).

Cada uno de los aproximadamente 10 miembros del IAB encabezó una fuerza de trabajo sobre algún aspecto de importancia. El IAB se reunía varias veces al año para comentar resultados y realimentar al DoD y a la NSF, quienes proporcionaban la mayor parte de los fondos en esa época. Cuando se necesitaba un estándar (por ejemplo, un algoritmo de ruteo nuevo), los miembros del IAB lo discutían y después anunciaban el cambio para que los estudiantes graduados, quienes eran el corazón de las labores de creación de *software*, pudieran implementarlo. La comunicación era a través de una serie de informes técnicos llamados **RFC** (*request for comments,* **petición de comentarios**). Los RFC se guardan en línea y pueden ser recuperados por cualquier interesado en ellos. Los RFC están numerados en orden cronológico de creación y ya hay cerca de 2000.

En 1989, la Internet había llegado a ser tan grande que este estilo tan informal ya no funcionaba. Para entonces, muchos proveedores ofrecían ya productos TCP/IP y no los querían cambiar sólo porque 10 investigadores habían tenido una mejor idea. En el verano de 1989, el IAB se reorganizó otra vez. Los investigadores pasaron a la **IRTF** (*Internet Research Task Force,* **Fuerza de Trabajo de Investigación sobre Internet**), la cual se hizo subsidiaria de IAB junto con la **IETF** (*Internet Engineering Task Force,* **Fuerza de Trabajo de Ingeniería de Internet**). El IAB se repobló con gente que representaba una gama amplia de organizaciones, no sólo la comunidad de investigación. Inicialmente, el IAB fue un grupo que se perpetuaba a sí mismo, pues sus miembros servían por un término de dos años y los nuevos miembros eran designados por los antiguos. Más tarde fue creada la **Internet Society**, formada por gente interesada en la Internet. Así, la Internet Society es en cierto sentido comparable con la ACM o el IEEE; está gobernada por administradores elegidos quienes designan a los miembros del IAB.

Lo que se buscaba con esta división era tener al IRTF concentrado en investigaciones a largo plazo, mientras que el IETF se encargaba de los problemas de ingeniería a corto plazo. El IETF se dividió en grupos de trabajo, cada uno con un problema específico por resolver. Los presidentes de estos grupos de trabajo inicialmente se reunían como un comité de conducción para dirigir los trabajos de ingeniería. Los temas del grupo de trabajo incluyen nuevas aplicaciones, información de usuarios, integración de OSI, ruteo y direccionamiento, seguridad, administración de

redes y estándares. Se llegaron a formar tantos grupos de trabajo (más de 70) que fue necesario agruparlos en áreas, y los presidentes de área formaron el comité de conducción.

Adicionalmente, se adoptó un proceso de estandarización más formal a imagen del de la ISO. Para convertirse en **propuesta de estándar**, la idea básica se debe explicar completamente en un RFC y debe generar suficiente interés en la comunidad para justificar su consideración. Para avanzar a la etapa de **borrador de estándar**, debe existir una implementación operante que haya sido probada concienzudamente por al menos dos sitios independientes durante cuatro meses. Si el IAB se convence de que la idea es buena y el software funciona, puede declarar que el RFC es un estándar de Internet. Algunos estándares de Internet han llegado a ser estándares del DoD (MIL-STD), volviéndose obligatorios para los proveedores del DoD. David Clark hizo una vez un comentario ahora famoso acerca de que la estandarización de Internet consistía en "consenso aproximado y código en operación".

1.8. ESQUEMA DEL RESTO DEL LIBRO

Este libro trata tanto los principios como la práctica de las redes de computadoras. La mayor parte de los capítulos empieza con una explicación de los principios pertinentes, seguida de varios ejemplos que ilustran estos principios. A lo largo del texto se usan dos redes como ejemplos continuos: las redes Internet y ATM. En cierta forma, las dos son complementarias: ATM tiene que ver en su mayor parte con las capas más bajas y la Internet está relacionada principalmente con las capas superiores. En el futuro, la Internet quizá opere en buena parte sobre una *backbone* de ATM, de modo que las dos podrían coexistir. Se darán otros ejemplos donde sean pertinentes.

El libro se estructura de acuerdo con el modelo híbrido de la figura 1-21. A partir del capítulo 2, comenzaremos a subir por la jerarquía de protocolos, empezando desde los cimientos. El segundo capítulo proporciona antecedentes en el campo de la comunicación de datos; cubre la transmisión analógica y digital, multiplexión, conmutación y el sistema telefónico pasado, presente y futuro. Este material concierne a la capa física, aunque sólo trataremos los aspectos arquitectónicos y no los de *hardware*. También veremos varios ejemplos de la capa física, tales como SONET y el radio celular.

El capítulo 3 se ocupa de la capa de enlace de datos y sus protocolos presentando varios ejemplos de complejidad creciente. También se hará un análisis de estos protocolos. Más adelante estudiaremos algunos protocolos importantes del mundo real, entre ellos: HDLC (que se usa en redes de velocidad baja y media), SLIP, PPP (que se usa en la Internet) y ATM (que se usa en B-ISDN).

El capítulo 4 se dedica a la subcapa de acceso al medio, que es parte de la capa de enlace de datos. La pregunta básica que aborda es cómo determinar quién puede ser el siguiente en usar la red cuando ésta consiste en un solo canal compartido, como en la mayor parte de las LAN y en algunas redes de satélites. Se dan muchos ejemplos del área de las LAN, las redes de fibra óptica y las redes de satélites. También se estudian aquí los puentes, que sirven para conectar entre sí las LAN.

El capítulo 5 trata la capa de red, en especial el ruteo, el control de congestión y la interconexión de redes. Veremos algoritmos tanto estáticos como dinámicos. Se cubre también el ruteo por difusión y se analiza en detalle el efecto del ruteo deficiente y la congestión. Conectar entre sí redes heterogéneas para formar interredes origina gran cantidad de problemas de los que hablaremos aquí. Se hará una amplia cobertura a las capas de red en la Internet y las redes ATM.

El capítulo 6 trata la capa de transporte. Se hará hincapié en los protocolos orientados a la conexión, pues muchas aplicaciones los necesitan. Se verá en detalle un ejemplo de servicio de transporte y su implementación. Estudiaremos en detalle tanto los protocolos de transporte de Internet (TCP y UDP) como los protocolos de transporte de ATM (AAL 1-5).

Las capas de sesión y de presentación de OSI no se verán en este libro pues no se utilizan ampliamente.

El capítulo 7 trata la capa de aplicación, sus protocolos y aplicaciones. Entre las aplicaciones que veremos están la seguridad, el uso de nombres, el correo electrónico, las noticias de red, la administración de redes, la Red Mundial y los multimedios.

El capítulo 8 contiene una lista anotada de lecturas recomendadas ordenadas por capítulo. Se pretende ayudar a aquellos lectores que quisieran continuar de manera más profunda su estudio de las redes. El capítulo contiene también una bibliografía en orden alfabético de todas las referencias citadas en este libro.

1.9. RESUMEN

Las redes de computadoras pueden prestar un gran número de servicios, tanto para compañías como para individuos. Para las compañías, las redes de computadoras personales que usan servidores compartidos ofrecen con frecuencia flexibilidad y una buena relación precio/rendimiento. Para los individuos, las redes ofrecen acceso a una variedad de recursos de información y distracción.

En términos aproximados, las redes se pueden dividir en LAN, MAN, WAN e interredes, cada una con sus características, tecnologías, velocidades y nichos propios. Las LAN abarcan un edificio, las MAN cubren una ciudad y las WAN un país o un continente. Las LAN y las MAN son no conmutadas (es decir, no tienen enrutadores); las WAN son conmutadas.

El *software* de red consiste en protocolos: reglas que rigen la comunicación entre procesos. Los protocolos pueden ser sin conexiones u orientados a la conexión. La mayor parte de las redes manejan las jerarquías de protocolos, en las que cada capa provee servicios a las capas que están sobre ella y las aísla de los detalles de los protocolos empleados en las capas más bajas. Las pilas de protocolos por lo regular se basan ya sea en el modelo OSI o en el TCP/IP. Los dos modelos tienen capas de red, de transporte y de aplicación, pero en las otras capas son diferentes.

Entre las redes más conocidas están NetWare de Novell, la ARPANET (ya difunta), la NSFNET, la Internet y varias plataformas de pruebas de gigabits. Entre los servicios de red han estado DQDB, SMDS, X.25, *frame relay* e ISDN de banda ancha. Todos están comercialmente disponibles de diversos proveedores. El mercado determinará quiénes sobrevivirán y quiénes no.