

tamente al medio y convierte la cadena $[g(t)]$ en la señal a transmitir $[s(t)]$; posteriormente en el Capítulo 5 se describirán las distintas alternativas para esta conversión.

Al transmitir $s(t)$ a través del medio, antes de llegar al receptor, aparecerán una serie de dificultades que se estudiarán en el Capítulo 3. Por lo tanto, la señal recibida $r(t)$ puede diferir de alguna manera de la transmitida $s(t)$. El receptor intentará estimar la señal original $s(t)$, a partir de la señal $r(t)$ y de su conocimiento acerca del medio, obteniendo una secuencia de bits $g'(t)$. Estos bits se envían al computador de salida, donde se almacenan temporalmente en memoria como un bloque de bits (g'). En muchos casos, el destino intentará determinar si ha ocurrido un error, y en su caso, cooperar con el origen para eventualmente conseguir el bloque de datos completo y sin errores. Los datos, finalmente se presentan al usuario a través del dispositivo de salida, que por ejemplo puede ser la impresora o la pantalla de su terminal. El mensaje recibido por el usuario (m') será normalmente una copia exacta del mensaje original (m).

Consideremos ahora una conversación telefónica. En este caso, la entrada al teléfono es un mensaje (m) consistente en unas ondas sonoras. Dichas ondas se convierten en el teléfono en señales eléctricas de la misma frecuencia. Estas señales se transmiten sin modificación a través de la línea telefónica. Por tanto, la señal de entrada $g(t)$ y la señal transmitida $s(t)$ son idénticas. La señal $s(t)$ sufrirá algún tipo de distorsión a través del medio, de tal manera que $r(t)$ no será idéntica a $s(t)$.

No obstante, la señal $r(t)$ se convierte recuperando una onda sonora, sin aplicar ningún tipo de corrección o mejora de la calidad. Por lo tanto, m' no es una réplica exacta de m . Sin embargo, el mensaje sonoro recibido es normalmente comprensible por el receptor.

En la discusión aquí realizada, no se han considerado otros aspectos fundamentales en las comunicaciones de datos, como lo son las técnicas de control del enlace, necesarias para regular el flujo de información, o como la detección y corrección de errores; tampoco se han considerado las técnicas de multiplexación, necesarias para conseguir una utilización eficaz del medio de transmisión. Todos estos aspectos se estudian en la Parte II.

1.3. COMUNICACIÓN DE DATOS A TRAVÉS DE REDES

A veces no es práctico que dos dispositivos de comunicaciones se conecten directamente mediante un enlace punto a punto. Esto es debido a alguna (o a las dos) de las siguientes circunstancias:

- Los dispositivos están muy alejados. En este caso no estaría justificado, por ejemplo, utilizar un enlace dedicado entre cada dos dispositivos, que puedan estar separados por miles de kilómetros.
- Hay un conjunto de dispositivos que necesitan conectarse entre ellos en instantes de tiempo diferentes. Un ejemplo de esta necesidad es la red telefónica mundial, o el conjunto de computadores pertenecientes a una compañía. Salvo el caso de que el número de dispositivos sea pequeño, no es práctico utilizar un enlace entre cada dos.

La solución a este problema es conectar cada dispositivo a una red de comunicación. La Figura 1.3 relaciona este concepto dentro del modelo de comunicaciones de la Figura 1.1a y a la vez sugiere dos grandes categorías en las que se clasifican tradicionalmente las redes: redes de área amplia (WAN, Wide Area Networks) y redes de área local (LAN, Local Area Networks). Recientemente, las diferencias entre estas dos categorías son cada vez más difusas, tanto en términos tecnológicos como de posibles aplicaciones; no obstante, es una forma natural y didáctica de organizar su estudio, por lo que aquí se adoptará dicha clasificación.

REDES DE ÁREA AMPLIA

Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una

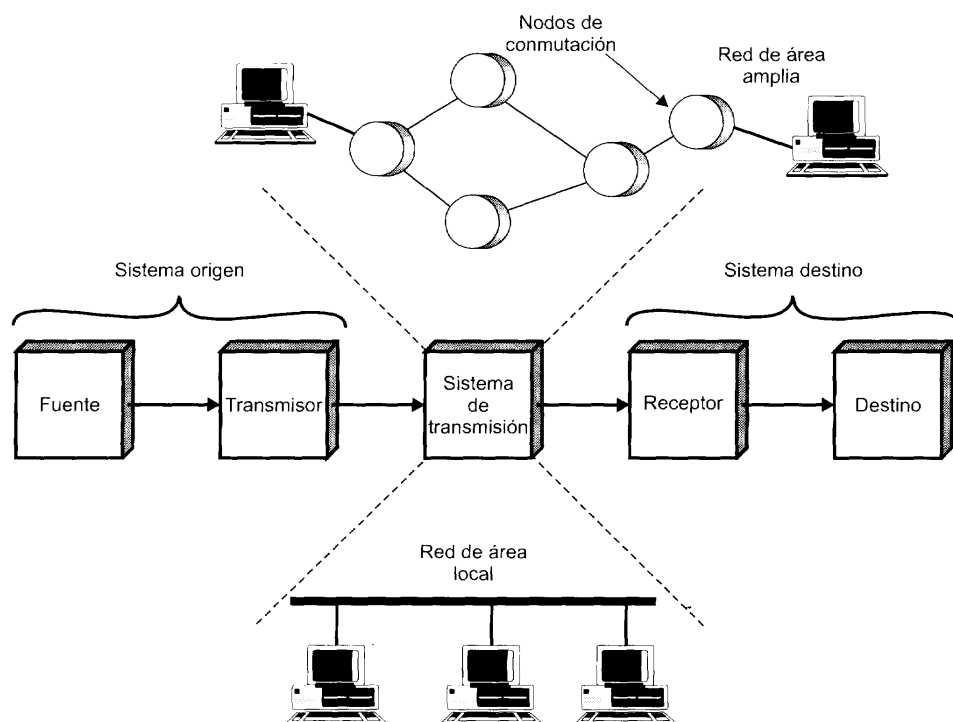


Figura 1.3. Modelos simplificados de redes.

serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo a los situados en los contornos) no les concierne el contenido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Tradicionalmente, las WAN se han implementando usando una de las dos tecnologías siguientes: conmutación de circuitos y conmutación de paquetes. Aunque últimamente, se está empleando como solución la técnica de retransmisión de tramas («frame relay»), así como las redes ATM.

Conmutación de circuitos

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red telefónica.

Conmutación de paquetes

Un enfoque diferente al anterior es el adoptado en redes de conmutación de paquetes. En este caso, no es necesario hacer una reserva a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y la

destino. En cada nodo, el paquete se recibe completamente, se almacena durante un intervalo breve y posteriormente se transmite al siguiente nodo. Las redes de conmutación de paquetes se usan fundamentalmente para comunicaciones terminal-computador y computador-computador.

Retransmisión de tramas (Frame Relay)

La conmutación de paquetes se desarrolló en la época en la que los servicios de transmisión a larga distancia sufrían una tasa de error relativamente elevada, comparada con los servicios de los que se dispone actualmente. Por tanto, para compensar esos errores relativamente frecuentes, en los esquemas de conmutación de paquetes se realiza un esfuerzo considerable, que se traduce en añadir información redundante en cada paquete, así como la realización de un procesamiento extra, tanto en el destino final como en los nodos intermedios de conmutación, necesario para detectar los errores y en su caso, corregirlos.

Ahora bien, con los modernos sistemas de comunicaciones de alta velocidad, este esfuerzo adicional es innecesario y contraproducente. Es innecesario ya que la tasa de errores se ha reducido drásticamente y los escasos errores que aparecen se pueden tratar en el sistema final mediante dispositivos que operan por encima del nivel de la lógica dedicada a la conmutación de paquetes. A su vez es contraproducente ya que los bits redundantes significan un desperdicio de parte de la capacidad proporcionada por la red.

La retransmisión de tramas («frame relay») se ha desarrollado teniendo presente las mayores velocidades de transmisión que actualmente se disponen, así como de las bajas tasas de error. Mientras que las redes originales de conmutación de paquetes se diseñaron para ofrecer una velocidad de transmisión al usuario final de 64 kbps, las redes «frame relay» están diseñadas para operar eficazmente a velocidades de transmisión de usuario de 2 Mbps. La clave para conseguir estas velocidades reside en eliminar la mayor parte de la información redundante y el procesamiento asociado para el control de errores.

ATM

El Modo de Transferencia Asíncrono (ATM, Asynchronous Transfer Mode), a veces denominado como modo de retransmisión de celdas («cell relay»), es la culminación de todos los desarrollos en conmutación de circuitos y conmutación de paquetes realizados durante los últimos 25 años.

ATM se puede interpretar como una evolución de la retransmisión de tramas («frame relay»). La diferencia más obvia entre «frame relay» y ATM es que «frame relay» usa paquetes de longitud variable, llamados «tramas», y ATM usa paquetes de longitud fija denominadas «celdas». Al igual que en «frame relay», ATM introduce poca información adicional para el control de errores, confiando en la inherente robustez del medio de transmisión así como en la lógica adicional localizada en el sistema destino para detectar y corregir errores. Al utilizar paquetes de longitud fija, el esfuerzo adicional de procesamiento se reduce incluso todavía más aquí que en «frame relay». El resultado es que ATM se ha diseñado para trabajar a velocidades de transmisión del orden de 10 a 100 Mbps, e incluso del orden de Gbps.

ATM se puede considerar a su vez como una evolución de la conmutación de circuitos. En la conmutación de circuitos, se dispone solamente de circuitos a velocidad fija de transmisión entre los sistemas finales. ATM permite la definición de múltiples canales virtuales con velocidades de transmisión que se definen dinámicamente en el instante en que el canal virtual se crea. Mediante la utilización de celdas de tamaño fijo, ATM es tan eficaz que puede ofrecer un canal a velocidad de transmisión constante aunque esté usando una técnica de conmutación de paquetes. Por lo tanto, ATM es una ampliación de la conmutación de circuitos en la que se ofrecen varios canales, en los que la velocidad de transmisión para cada canal se fija dinámicamente según las necesidades.

RDSI y RDSÍ de banda ancha

La sinergia y evolución entre las comunicaciones y las tecnologías de la computación, junto con la creciente demanda de servicios eficaces de captación, procesamiento y diseminación de la información,

está desembocando en el desarrollo de sistemas integrados que transmiten y procesan todo tipo de datos. Una consecuencia significativa de esta tendencia ha sido el desarrollo de la Red Digital de Servicios Integrados (RDSI).

La RDSI se ha diseñado para sustituir a las redes públicas de telecomunicaciones existentes, proporcionando una gran variedad de servicios. La RDSI se define mediante la estandarización de las interfaces de usuario, y se ha implementado como un conjunto de conmutadores digitales y enlaces que proporcionan una gran variedad de tipos de tráfico, a la vez que servicios de valor añadido. En la práctica, se trata de múltiples redes, implementadas dentro de los límites nacionales, pero desde el punto de vista del usuario se considera como una única red mundial, uniformemente accesible.

A pesar de que la RDSI tiene todavía que conseguir la cobertura mundial para la que fue diseñada, está ya en su segunda generación. La primera generación, a veces denominada como **RDSI de banda estrecha**, se basa en el uso de canales de 64 kbps como unidad básica de conmutación, presentando una clara orientación hacia la conmutación de circuitos. Técnicamente hablando, la principal contribución de la RDSI de banda estrecha ha sido el «frame relay». La segunda generación, denominada **RDSI de banda ancha**, proporciona velocidades de transmisión muy elevadas (cientos de Mbps) y tiene una clara orientación hacia la conmutación de paquetes. La contribución técnica principal de la RDSI de banda ancha ha sido el modo de transferencia asíncrono (ATM), también denominado retransmisión de celdas «cell relay».

REDES DE ÁREA LOCAL

Al igual que las redes de área amplia, una red de área local es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos. No obstante, hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

1. La cobertura de una LAN es pequeña, típicamente un edificio o como mucho un conjunto de edificios próximos. Como se verá más adelante, esta diferencia en cuanto a la cobertura geográfica, condicionará la solución técnica finalmente adoptada.
2. Es común que la LAN sea propiedad de la misma entidad que es propietaria de los dispositivos conectados a la red. En WAN, esto no es tan corriente, o al menos una fracción significativa de recursos de la red son ajenos. Esto tiene dos implicaciones. La primera es que se debe cuidar mucho la elección de la LAN, ya que evidentemente, lleva acarreado una inversión substancial de capital (comparado con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto en la adquisición como en el mantenimiento. Segunda, la responsabilidad de la gestión de la red local recae solamente en el usuario.
3. Las velocidades de transmisión internas en una LAN son mucho mayores.

Tradicionalmente, en LAN se utiliza la difusión en lugar de utilizar técnicas de conmutación. En una red de difusión, no hay nodos intermedios. En cada estación hay un transmisor/receptor que se comunica con las otras estaciones a través de un medio compartido. Una transmisión desde cualquier estación se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el medio es compartido, una y sólo una estación en cada instante de tiempo podrá transmitir el paquete.

Más recientemente, la conmutación también se está utilizando en LAN, fundamentalmente en LAN tipo Ethernet. Otros dos ejemplos de especial relevancia son las LAN ATM, en las que se usa una red ATM como una red de área local, así como los Canales de Fibra. Estas LAN se estudiarán, junto con las basadas en difusión, en la Parte IV de este texto.

1.4. PROTOCOLOS Y ARQUITECTURA DE PROTOCOLOS

Cuando se realiza un intercambio de datos entre computadores, terminales y/o otros dispositivos de procesamiento, las cuestiones a estudiar son muchas más que las mencionadas en las Secciones 1.2 y 1.3.

2.3. ARQUITECTURA DE PROTOCOLOS TCP/IP

Durante muchos años, la literatura técnica que trataba las arquitecturas de protocolos estaba dominada por las discusiones relacionadas con OSI, así como por el desarrollo de protocolos y servicios para cada capa. Durante los años ochenta la creencia más extendida era que OSI llegaría a imponerse frente a arquitecturas comerciales como la SNA de IBM y frente a esquemas no propietarios («multivendor») como TCP/IP. Esta previsión nunca se cumplió. En los noventa, TCP/IP ha conseguido erigirse como la arquitectura comercial dominante, a la vez que se ha convertido en la familia o conjunto de protocolos sobre la que se desarrollaran los protocolos futuros.

Existe una serie de razones que justifican el éxito de los protocolos TCP/IP sobre OSI. Entre ellas se pueden enumerar a las siguientes:

1. Los protocolos TCP/IP se especificaron y se utilizaron de una forma generalizada antes de la normalización ISO. Así, en los años ochenta las instituciones que tenían necesidades apremiantes de intercambio de información se enfrentaron al dilema de esperar a la disponibilidad del paquete siempre prometido y nunca entregado de OSI, o por el contrario utilizar el conjunto TCP/IP de disponibilidad inmediata y operatividad cada vez más contrastada. Una vez hecha la elección de TCP/IP, el coste y los riesgos de la migración a un entorno nuevo, inhibió la aceptación de ISO.
2. Los protocolos TCP/IP se desarrollaron inicialmente como resultado del esfuerzo investigador en el entorno militar de los EE.UU., financiado por el Departamento de Defensa (DOD, Department Of Defense). Aunque el DOD, como el resto del gobierno de los EE.UU., estaba involucrado en los procesos internacionales de normalizaciones, el DOD tenía una necesidad imperiosa e inmediata de conectividad, tal que no le permitía esperar hasta los años ochenta o incluso principios de los noventa a productos basados en OSI. Por consiguiente, el DOD exigió el uso de los protocolos TCP/IP en todas sus adquisiciones de software. Debido a que el DOD es el consumidor más grande de software en el mundo, esta política creó un mercado enorme, animando a los vendedores a desarrollar productos basados en TCP/IP.
3. Internet está construida sobre el conjunto de protocolos TCP/IP. El crecimiento impresionante de Internet y especialmente de la «World Wide Web» (red extendida mundial) ha cimentado la victoria de TCP/IP sobre OSI.

LA APROXIMACIÓN DE TCP/IP

El conjunto de protocolos TCP/IP reconoce que la tarea de la comunicación es lo suficientemente compleja y diversa como para realizarla en una única unidad. Consecuentemente, la tarea se descompone en diversos módulos o entidades, que se pueden comunicar con sus entidades pares del sistema remoto. Una entidad dentro de un sistema proporciona servicios a otras entidades y, a su vez, utiliza los servicios de otras entidades. Las reglas de diseño del software de calidad dictan que estas entidades se deben agrupar en una forma modular y jerárquica.

El modelo OSI se basa en el mismo razonamiento, pero introduce un paso más. El siguiente paso en OSI está en reconocer que, en muchos aspectos, los protocolos en el mismo nivel de la jerarquía tienen algunas características comunes. Esto desemboca ineludiblemente en el concepto de nivel o capa, así como en el intento de describir de una forma abstracta las características comunes de los protocolos en un nivel dado.

Como herramienta didáctica, un modelo en capas tiene un valor significativo y, de hecho, el modelo OSI se utiliza por ese motivo en muchos textos de telecomunicaciones. Los diseñadores del conjunto de protocolos TCP/IP ponen la objeción que el modelo OSI es más prescriptivo que descriptivo. El modelo OSI ordena que los protocolos dentro de una capa dada realicen unas determinadas funciones. Esto puede no ser siempre deseable. Es posible definir más de un protocolo en una capa dada, y en este caso

puede que la funcionalidad de estos protocolos no sea la misma o ni incluso similar. Ahora bien, lo que tienen en común un conjunto de protocolos de la misma capa es que se sustentan sobre el mismo conjunto de protocolos de la capa inferior adyacente.

Además, debido a que en el modelo OSI las interfaces entre capas están bien definidas es posible sustituir un protocolo de una capa por otra versión más reciente, sin que ello implique modificar las capas adyacentes (véase principio 6, Tabla 2.2). Esto no es siempre deseable o incluso posible. Por ejemplo, una LAN se presta fácilmente para un esquema de direccionamiento con difusión y multidifusión en el nivel de enlace. Si el nivel de enlace de IEEE 802 se situara debajo de una entidad de protocolo de red que no permitiera difusión ni multidifusión, este servicio sería inaccesible para las capas superiores en la jerarquía. Para eludir este tipo de problemas, los especificadores de OSI introducen el concepto de capas o subcapas nulas. A veces, parece que estos artificios salvan al modelo a expensas de diseño no adecuado de los protocolos.

En el modelo TCP/IP, el uso estricto de todas las capas no es obligatorio. Por ejemplo, hay protocolos de aplicación que operan directamente sobre IP.

LA ARQUITECTURA DE PROTOCOLOS TCP/IP

En el Capítulo 1 se presentó la familia de protocolos TCP/IP. Como ya se señaló no existe un modelo de protocolos TCP/IP «oficial». Sin embargo, es de utilidad considerar que el conjunto de protocolos está involucrado en cinco capas. Para resumir el Capítulo 1, estas capas son:

- **Capa de aplicación:** proporciona la comunicación entre procesos o aplicaciones de computadores separados.
- **Capa de transporte o extremo-a-extremo:** proporciona un servicio de transferencia de datos extremo-a-extremo. Esta capa puede incluir mecanismos de seguridad. Oculta los detalles de la red, o redes subyacentes, a la capa de aplicación.
- **Capa Internet:** relacionada con el encaminamiento de los datos del computador origen al destino a través de una o más redes conectadas por dispositivos de encaminamiento.
- **Capa de acceso a la red:** relacionada con la interfaz lógica entre un sistema final y una subred.
- **Capa física:** define las características del medio de transmisión, la tasa de señalización y el esquema de codificación de las señales.

FUNCIONAMIENTO DE TCP E IP

La Figura 2.4 muestra cómo se configuran los protocolos TCP/IP. Para conectar un computador a una subred se utiliza algún tipo de protocolo de acceso como, por ejemplo, Ethernet. Este protocolo permite al computador enviar datos a través de la subred a otro computador o, en caso de que el destino final esté en otra subred, a un dispositivo de encaminamiento. IP se implementa en todos los sistemas finales y dispositivos de encaminamiento. Actúa como un porteador que transportara bloques de datos desde un computador hasta otro, a través de uno o varios dispositivos de encaminamiento. TCP se implementa solamente en los sistemas finales; guarda un registro de los bloques de datos para asegurar que todos se entregan de forma segura a la aplicación apropiada.

Para tener éxito en la transmisión, cada entidad en el sistema global debe tener una única dirección. En realidad, se necesitan dos niveles de direccionamiento. Cada computador en la red debe tener una única dirección internet que permita enviar los datos al computador adecuado. Además, cada proceso que se ejecute dentro de un computador en red debe tener a su vez una dirección que sea única dentro del mismo; esto permite al protocolo extremo-a-extremo (TCP) entregar los datos al proceso adecuado. Estas últimas direcciones se denominan puertos.

A continuación, se va a describir paso a paso el funcionamiento de la Figura 2.4. Supóngase que un proceso, asociado al puerto 1 en el computador A, desea enviar un mensaje a otro proceso, asociado al puerto 2 del computador B. El proceso en A pasa el mensaje al TCP con la instrucción de enviarlo al puerto 2 del computador B. EL TCP pasa el mensaje al IP con instrucciones de que lo envíe al computador B. Obsérvese que no es necesario comunicarle al IP la identidad del puerto destino. Todo lo que necesita saber es que los datos van dirigidos al computador B. A continuación, IP pasa el mensaje a la capa de acceso a la red (por ejemplo, a la lógica Ethernet) con el mandato expreso de enviarlo al dispositivo de encaminamiento X (el primer salto en el camino a B).

Para controlar esta operación se debe transmitir información de control junto con los datos de usuario, como así se sugiere en la Figura 2.11. Supongamos que el proceso emisor genera un bloque de datos y lo pasa al TCP. El TCP puede que divida este bloque en fragmentos más pequeños para hacerlos más manejables. A cada uno de estos fragmentos le añade información de control, denominada cabecera TCP, formando un segmento TCP. La información de control la utilizará la entidad par TCP en el computador B. Entre otros, en la cabecera se incluyen los siguientes campos:

- **Puerto destino:** cuando la entidad TCP en B recibe el segmento, debe conocer a quién se le deben entregar los datos.
- **Número de secuencia:** TCP numera secuencialmente los segmentos que envía a un puerto destino dado, para que si llegan desordenados la entidad TCP en B pueda reordenarlos.
- **Suma de comprobación:** la entidad emisora TCP incluye un código calculado en función del resto del segmento. La entidad receptora TCP realiza el mismo cálculo y compara el resultado con el código recibido. Si se observa alguna discrepancia implicará que ha habido algún error en la transmisión.

A continuación, TCP pasa cada segmento al IP con instrucciones para que los transmita a B. Estos segmentos se transmitirán a través de una o varias subredes y serán retransmitidos en uno o más dispositivos de encaminamiento intermedios. Esta operación también requiere el uso de información de control. Así, el IP añade una cabecera de información de control a cada segmento para formar un datagrama IP. En la cabecera IP, además de otros campos, se incluirá la dirección del computador destino (en nuestro ejemplo B).

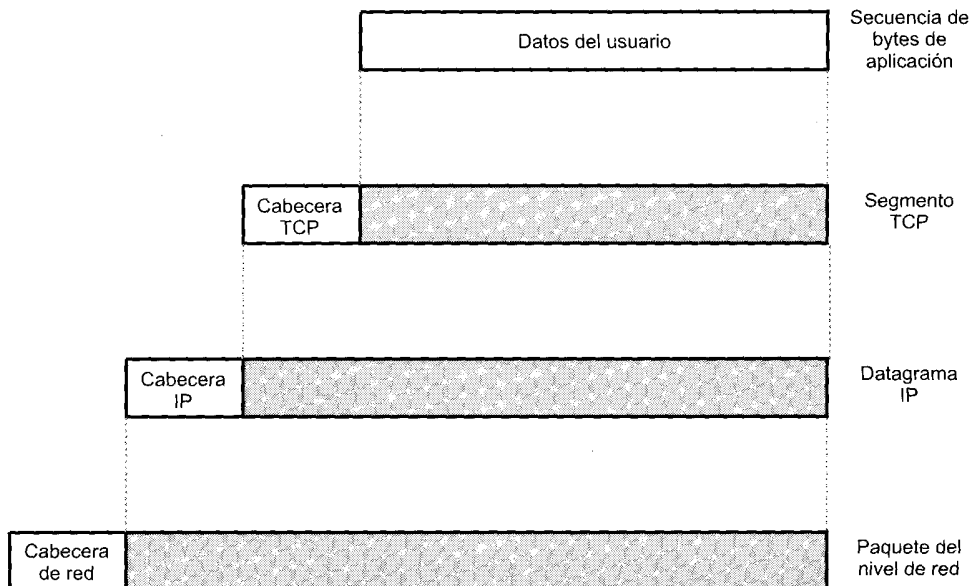


Figura 2.11. Unidades de datos de protocolo en la arquitectura TCP/IP.

Finalmente, cada datagrama IP se pasa a la capa de acceso a la red para que se envíe a través de la primera subred. La capa de acceso a la red añade su propia cabecera, creando un paquete, o trama. El paquete se transmite a través de la red al dispositivo de encaminamiento J. La cabecera del paquete contiene la información que la red necesita para transferir los datos. La cabecera puede contener, entre otros, los siguientes campos:

- **Dirección de la red destino:** la red debe conocer a qué dispositivo conectado se debe entregar el paquete.
- **Funciones solicitadas:** el protocolo de acceso a la red podría solicitar la utilización de ciertas funciones que ofrezca la red, como, por ejemplo, la utilización de prioridades.

En el dispositivo de encaminamiento J se elimina la cabecera del paquete y se examina la cabecera IP. El módulo IP del dispositivo de encaminamiento direcciona el paquete a través de la red 2 hacia B basándose en la dirección destino que contenga la cabecera IP. Para hacer esto, se le añade al datagrama una cabecera de acceso a la red.

Cuando se reciben los datos en B, ocurre el proceso inverso. En cada capa se elimina la cabecera correspondiente y el resto se pasa a la capa inmediatamente superior, hasta que los datos de usuario alcancen al proceso destino.

INTERFACES DE PROTOCOLO

En la familia de protocolos TCP/IP cada capa interacciona con sus capas adyacentes. En el origen, la capa de aplicación utilizará los servicios de la capa extremo-a-extremo, pasándole los datos. Este procedimiento se repite en la interfaz entre la capa extremo-a-extremo y la capa internet, e igualmente en la interfaz entre la capa internet y la capa de acceso a la red. En el destino, cada capa entrega los datos a la capa superior adyacente.

La arquitectura de TCP/IP no exige que se haga uso de todas las capas. Como así se sugiere en la Figura 2.12, es posible desarrollar aplicaciones que invoquen directamente los servicios de cualquier capa. La mayoría de las aplicaciones requieren un protocolo extremo-a-extremo seguro y por tanto utilizan TCP. Algunas de estas aplicaciones, como el protocolo sencillo de gestión de red (SNMP, Simple Network Management Protocol), utilizan un protocolo extremo-a-extremo alternativo denominado protocolo de datagrama de usuario (UDP, User Datagram Protocol); otras, en cambio, pueden hacer uso de IP directamente. Las aplicaciones que no necesiten interconexión de redes y que no necesiten TCP pueden invocar directamente los servicios de la capa de acceso a la red.

LAS APLICACIONES

La Figura 2.12 muestra la organización de los protocolos más importantes de la familia de TCP/IP. La mayoría de estos protocolos se estudiarán en la Parte V de este texto. En esta sección, resaltaremos tres protocolos que históricamente han sido considerados esenciales en TCP/IP, y que se diseñaron por el DOD como estándares militares junto a TCP e IP.

El **protocolo sencillo de transferencia de correo (SMTP, Simple Mail Transfer Protocol)** proporciona una función básica de correo electrónico. Proporciona un mecanismo para transferir mensajes entre computadores remotos. Entre las propiedades del SMTP cabe destacar la utilización de listas de mensajería, la gestión de acuses de recibo y el reenvío de mensajes. El protocolo SMTP no especifica cómo se crean los mensajes, para este fin se necesita un programa de correo electrónico nativo o un editor local. Una vez que se ha creado el mensaje, SMTP lo acepta y hace uso del TCP para enviarlo al módulo SMTP en el computador remoto. En el receptor, el módulo SMTP utilizará su aplicación de correo electrónico local para almacenar el mensaje recibido en el buzón de correo del usuario destino.

El **protocolo de transferencia de ficheros (FTP, File Transfer Protocol)** se utiliza para enviar ficheros de un sistema a otro bajo el control del usuario. Se permite transmitir ficheros tanto de texto

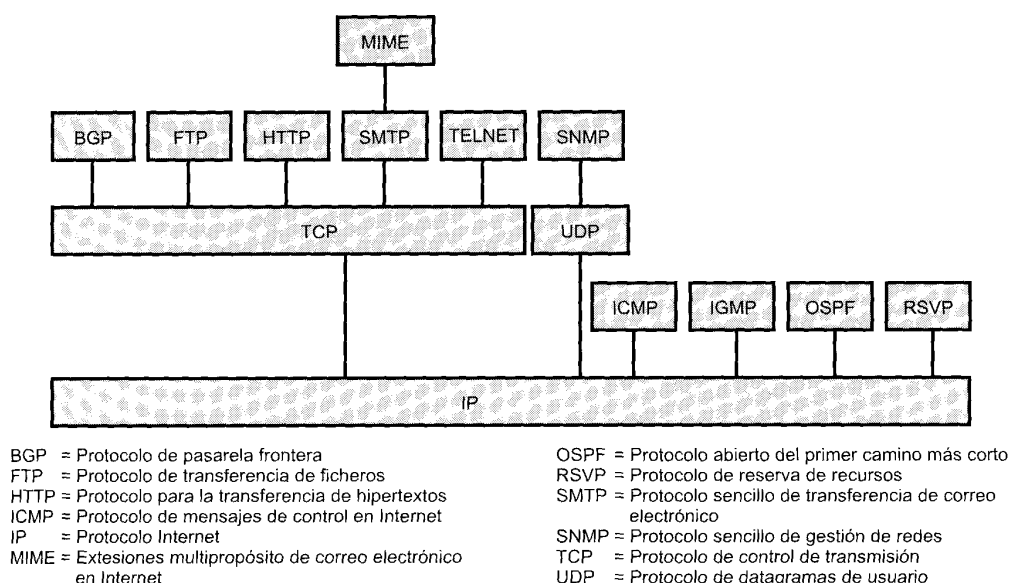


Figura 2.12. Algunos protocolos en la familia de protocolos TCP/IP.

como en binario, además el protocolo permite controlar el acceso de los usuarios. Cuando un usuario solicita la transferencia de un fichero, el FTP establece una conexión TCP con el sistema destino para intercambiar mensajes de control. Esta conexión permite al usuario transmitir su identificador y contraseña, además de la identificación del fichero junto con las acciones a realizar sobre el mismo. Una vez que el fichero se haya especificado y su transferencia haya sido aceptada, se establecerá una segunda conexión TCP a través de la cual se materializará la transferencia. El fichero se transmite a través de la segunda conexión, sin necesidad de enviar información extra, o cabeceras generadas por la capa de aplicación. Cuando la transferencia finaliza, se utiliza la conexión de control para indicar el fin, además esta misma conexión estará disponible para aceptar nuevas órdenes de transferencia.

TELNET facilita la posibilidad de conexión remota, mediante la cual el usuario en un terminal o computador personal se conecta a un computador remoto y trabaja como si estuviera conectado directamente a ese computador. El protocolo se diseñó para trabajar con terminales poco sofisticados en modo *scroll* (*avance de pantalla*). En realidad, TELNET se implementa en dos módulos: el usuario TELNET interactúa con el módulo de E/S para comunicarse con terminal local. Éste convierte las particularidades de los terminales reales a una definición normalizada de terminal de red, y viceversa. El servidor TELNET interactúa con la aplicación, actuando como un sustituto del gestor del terminal, para que de esta forma el terminal remoto le parezca local a la aplicación. El tráfico entre el terminal del usuario y el servidor TELNET se transmite sobre una conexión TCP.

2.4. LECTURAS RECOMENDADAS

Para el lector que tenga interés en conocer con mayor detalle el TCP/IP, existen dos trabajos de tres volúmenes que son más que adecuados. El trabajo de Comer y Stevens ha llegado a ser un clásico y se considera definitivo [COME99, COME97, COME95]. El trabajo de Stevens y Wright es también destacable, en él se presenta más detalles en lo referente al funcionamiento de los protocolos [STEV94, STEV96, WRIG95]. Un trabajo más compacto y muy útil es [MURP98], en el que se estudia el abanico

2. Indique la diferencia entre puente y conmutador.
3. ¿Que es un encaminador?
4. Identifique algunas relaciones sociales que se ajusten al modelo cliente/servidor.
5. Identifique algunos de los protocolos utilizados en la sociedad.
6. Resuma la distinción entre computación en cluster y computación en red.

4.2 Internet

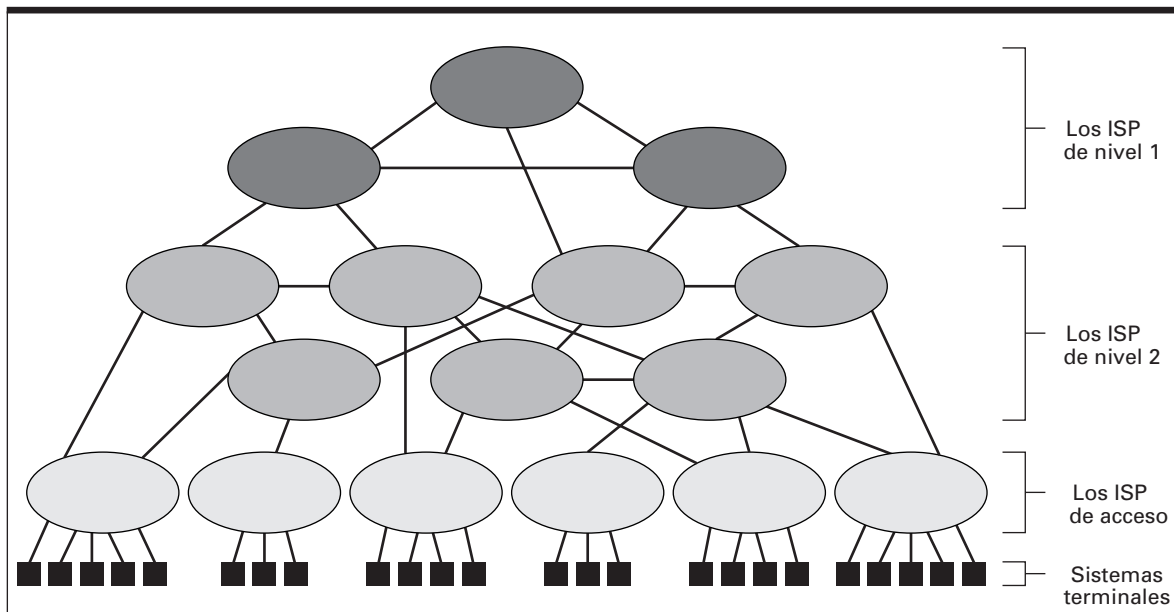
El ejemplo más notable de interred es **Internet**, que tiene su origen en una serie de proyectos de investigación que datan de principios de la década de 1960. El objetivo era desarrollar la capacidad de enlazar diversas redes de computadoras, para que pudieran funcionar como un sistema conectado que no se viera afectado en su operación global por desastres de escala local. Buena parte de este trabajo estaba patrocinado por el gobierno de Estados Unidos a través de la agencia DARPA (*Defense Advanced Research Projects Agency*, Agencia de Proyectos Avanzados de Investigación para la Defensa). A lo largo de los años, el desarrollo de Internet fue pasando de ser un proyecto patrocinado por el gobierno a un proyecto académico de investigación y actualmente es, en buena medida, un esfuerzo de carácter comercial que enlaza una combinación mundial de redes LAN, MAN y WAN que abarcan a millones de computadoras.

Arquitectura de Internet

Como ya hemos mencionado, Internet es un conjunto de redes conectadas. En general, estas redes son construidas y mantenidas por organizaciones denominadas **Proveedores de servicios de Internet** (ISP, *Internet Service Provider*). También resulta bastante común utilizar el término ISP para hacer referencia a las propias redes. Así, podemos utilizar expresiones como conectarse a un ISP, cuando lo que realmente queremos decir es conectarse a la red proporcionada por un ISP.

El sistema de redes operado por los ISP puede clasificarse en una jerarquía de acuerdo con el papel que desempeñan en la estructura global de Internet (Figura 4.7). En la parte superior de esta jerarquía se encuentra un número relativamente pequeño de proveedores **ISP de nivel 1**, que están compuestos por redes WAN internacionales de alta velocidad y alta capacidad. Estas redes se consideran la red troncal de Internet. Normalmente, son operadas por grandes empresas que trabajan en el sector de las comunicaciones. Un ejemplo sería una empresa cuyo origen fuera el de una empresa de telefonía tradicional que hubiera expandido su ámbito de actuación para proporcionar otros servicios de comunicaciones.

Conectados a los ISP de nivel 1 se encuentran los **ISP de nivel 2**, que tienden a tener un ámbito más regional y que son menos potentes en lo que a sus capacidades se refiere (la distinción entre los ISP de nivel 1 y nivel 2 es, a menudo, una cuestión debatible). De nuevo, estas redes tienden a ser operadas por empresas que pertenecen al sector de las comunicaciones.

Figura 4.7 Composición de Internet.

Los ISP de nivel 1 y nivel 2 son básicamente redes de encaminadores que proporcionan de manera colectiva la infraestructura de comunicaciones de Internet. Teniendo en cuenta el papel que desempeñan podemos considerar que representan el auténtico núcleo de Internet. El acceso a este núcleo suele ser proporcionado por un intermediario denominado ISP de acceso. Un **ISP de acceso** es esencialmente una interred independiente, en ocasiones denominada **intranet**, operada por una única autoridad cuyo negocio consiste en suministrar acceso a Internet a los usuarios individuales. Como ejemplos podríamos citar empresas tales como AOL, Microsoft y las empresas locales de telefonía y cable que facturan por su servicio, además a algunas otras organizaciones como universidades o corporaciones, que se encargan de proporcionar acceso a Internet a los individuos que forman parte de sus organizaciones.

Los dispositivos con los que los usuarios individuales se conectan a los ISP de acceso se conocen con el nombre de **sistemas terminales, hosts o anfitriones**. Estos sistemas terminales no necesariamente son computadoras en el sentido tradicional de la palabra. Existe un amplio rango de dispositivos que pueden actuar como sistemas terminales incluyendo teléfonos, videocámaras, automóviles y electrodomésticos. Después de todo, Internet es esencialmente un sistema de comunicaciones, por lo que cualquier dispositivo que pudiera beneficiarse de la comunicación con otros dispositivos sería un sistema terminal en potencia.

La tecnología mediante la cual los sistemas terminales se conectan a los ISP de acceso también es muy variable. Quizá el tipo que más rápidamente está creciendo son las conexiones inalámbricas basadas en la tecnología WiFi. La estrategia consiste en conectar el punto de acceso de la red WiFi a un ISP de acceso, proporcionando así acceso a Internet a través de ese ISP a los sistemas terminales que se encuentran dentro del alcance de las emisiones del punto de acceso de

la red WiFi. El área de la zona de cobertura del punto de acceso de la red WiFi en la cual se proporciona acceso a Internet se suele denominar **punto caliente**. Los puntos calientes y las agrupaciones de puntos calientes son cada vez más comunes, pudiendo encontrarse en domicilios particulares, en hoteles, edificios de oficinas, pequeñas empresas, aparcamientos y en algunos casos, ciudades enteras. Una tecnología similar es la que se emplea en el sector de la telefonía móvil en la que los puntos calientes se conocen con el nombre de celdas y los “encaminadores” que generan las celdas se coordinan para proporcionar un servicio continuo, a medida que un sistema terminal se desplaza de una celda a otra.

Otras técnicas populares para la conexión con los ISP de acceso utilizan líneas telefónicas o sistemas por cable/satélite. Estas tecnologías pueden emplearse para proporcionar conexión directa a un sistema terminal o al encaminador de un cliente, al cual se conectarán múltiples sistemas terminales. Esta última táctica está siendo cada vez más popular en el mercado residencial, en el que se crea un punto caliente local en un domicilio mediante un encaminador/punto de acceso conectado a un ISP de acceso a través de las líneas telefónicas o de cable ya existentes.

Los enlaces por cable y vía satélite ya existentes son inherentemente más compatibles con la transferencia de datos a alta velocidad que las líneas telefónicas tradicionales, que se instalaron originalmente teniendo presentes las necesidades de la comunicación por voz. Sin embargo, se han desarrollado varios esquemas muy inteligentes para ampliar esos enlaces de voz con el fin de admitir la transmisión de datos digitales. Estas soluciones hacen uso de unos dispositivos denominados **modems** (modulador/demodulador) que convierten los datos digitales que hay transferir a un formato compatible con el medio de transmisión que se está utilizando. Un ejemplo sería **DSL** (*Digital Subscriber Line*, Línea digital de abonado) en donde se reserva el rango de frecuencias situado por debajo de 4 KHz (4 kilociclos por segundo) para la comunicación tradicional por voz, mientras que las frecuencias más altas se emplean para la transferencia de datos digitales. Otro enfoque más antiguo consiste en convertir los datos digitales en sonido y transmitir dicho sonido de la misma forma que se hace con la voz. Esta solución se conoce como acceso **telefónico**, en referencia al hecho de que se utiliza para conexiones temporales en las que el usuario establece una llamada telefónica tradicional con el encaminador del ISP y luego conecta su teléfono al sistema terminal que va a emplear. Aunque se trata de una solución barata y de alta disponibilidad, el acceso telefónico proporciona una tasa de transferencia de datos relativamente lenta, lo que hace que cada vez sea menos capaz de gestionar las aplicaciones Internet actuales, que tienden a depender de la comunicación de vídeo en tiempo real y de la transmisión de grandes bloques de datos. Debido a ello, un número creciente de pequeñas empresas y de domicilios particulares se conectan a sus ISP de acceso mediante tecnologías de banda ancha, incluyendo conexiones de televisión por cable, líneas telefónicas de datos dedicadas, antenas de comunicación vía satélite e incluso cables de fibra óptica.

Direccionamiento Internet

Como hemos visto en la Sección 4.1, una interred necesita un sistema de direccionamiento global que asigne una dirección unívoca de identificación a cada

Internet2

Ahora que Internet ha pasado de ser un proyecto de investigación a un producto de consumo doméstico, la comunidad científica ha pasado a centrar su atención en un proyecto denominado Internet2. Internet2 está pensado como un sistema únicamente académico e implica a numerosas universidades, que trabajan en colaboración con empresas y con el gobierno. El objetivo es llevar a cabo una serie de investigaciones en aplicaciones interred que requieren comunicación de banda ancha, como por ejemplo el control y acceso remoto a costosos equipos avanzados, como pueden ser telescopios y dispositivos de diagnóstico médico. Un ejemplo de esos proyectos actuales de investigación implica la cirugía remota realizada por una serie de manos robóticas que remedan las manos de un cirujano distante que observa al paciente por vídeo. Si desea obtener más información acerca de Internet2 consulte <http://www.internet2.org>.

computadora del sistema. En Internet, estas direcciones se conocen con el nombre de **direcciones IP**; el término *IP* hace referencia a “Internet Protocol” (Protocolo Internet), que es un término sobre el que hablaremos en la Sección 4.4. Originalmente, cada dirección IP era un patrón de 32 bits, pero para proporcionar un conjunto mayor de direcciones, actualmente está en marcha el proceso de conversión a direcciones de 128 bits (consulte las explicaciones acerca de IPv6 en la Sección 4.4). **ICANN** (*Internet Corporation for Assigned Names and Numbers*, Corporación Internet para la asignación de nombres y números), que es una organización sin ánimo de lucro establecida para coordinar el funcionamiento de Internet, se encarga de asignar a los ISP bloques de direcciones IP con numeración consecutiva. A los ISP se les permite entonces asignar las direcciones de los bloques que tienen concedidos a una serie de máquinas situadas dentro de su región de autoridad. De ese modo, se asignan direcciones IP unívocas a todas las máquinas de Internet.

Las direcciones IP se escriben tradicionalmente en **notación decimal con puntos** en la que los bytes de la dirección se separan mediante puntos y cada byte se expresa como un entero representado en notación tradicional de base diez. Por ejemplo, con la notación decimal con puntos, el patrón 5.2 representaría el patrón de dos bytes de longitud 0000010100000010, que está compuesto por el byte 00000101 (representado por el 5) seguido del byte 00000010 (representado por el 2). Por su parte, el patrón 17.12.25 representa un patrón de tres bytes de longitud compuesto por el byte 00010001 (que es 17 en notación binaria), seguido del byte 00001100 (12 en binario) y seguido del byte 00011001 (25 en binario). En resumen, una dirección IP de 32 bits podría aparecer escrita como 192.207.177.133 al ser expresada en notación decimal con puntos.

Las direcciones expresadas como un patrón de bits (incluso cuando se las comprime utilizando la notación decimal con puntos) no se prestan mucho a su manipulación por parte de los seres humanos. Por esta razón, Internet dispone de un sistema de direccionamiento alternativo en el que las máquinas se identifican mediante nombres mnemónicos. Este sistema de direccionamiento está basado en el concepto de **dominio**, que puede considerarse como una “región” de Internet operada por una única autoridad, como por ejemplo una universidad, un club, una empresa o un organismo gubernamental (ponemos entre

comillas la palabra región porque, como pronto veremos, ese tipo de región puede no corresponderse con un área física de Internet). Es necesario registrar cada dominio ante el ICANN, que es un proceso que se encargan de realizar una serie de empresas denominadas **registradoras**, a las que el ICANN ha asignado dicho papel. Como parte de este proceso de registro, a cada dominio se le asigna un **nombre de dominio** mnemónico, que es único entre todos los nombres de dominio de Internet. Los nombres de dominio suelen ser descriptivos de la organización que está registrando dicho dominio, lo que maximiza la utilidad de estos nombres para los seres humanos.

Por ejemplo, el nombre de dominio de la editorial Addison-Wesley es `aw.com`. Observe el sufijo situado a continuación del punto. Ese sufijo se emplea para reflejar la clasificación del dominio, que en este caso es “comercial”, como indica el sufijo `com`. Estos sufijos se denominan **dominios de nivel superior** (TLD, *Top-Level Domain*). Otros TLD serían `edu` para instituciones educativas, `gov` para organismos gubernamentales de Estados Unidos, `org` para organizaciones sin ánimo de lucro, `museum` para museos, `info` para uso no restringido y `net`, que originalmente estaba pensado para los ISP pero que ahora se utiliza de forma mucho más general. Además de estos TLD generales, también están los TLD de dos letras para países específicos (denominados **TLD de código de país**), como por ejemplo `au` para Australia y `ca` para Canadá.

Una vez registrado el nombre mnemónico de un dominio, la organización que ha registrado dicho nombre es libre de ampliarlo para obtener identificadores mnemónicos para determinados elementos individuales dentro del dominio. Por ejemplo, una máquina individual dentro de Addison-Wesley podría estar identificada como `ssenterprise.aw.com`. Observe que los nombres de dominio se amplían hacia la izquierda y que las ampliaciones se separan mediante un punto. En algunos casos, se emplean múltiples extensiones, denominadas **subdominios**, como medio de organizar los nombres dentro de un dominio. Estos subdominios representan a menudo diferentes redes dentro de la jurisdicción del dominio. Por ejemplo, si a la Universidad Desconocida se le asignara el nombre de dominio `desconocida.edu`, entonces una computadora individual en la Universidad Desconocida podría tener un nombre como `r2d2.medicina.desconocida.edu`, lo que significa que la computadora `r2d2` se encuentra en el subdominio `medicina` dentro del dominio `desconocida` del TLD `edu`. (Hay que hacer hincapié que la notación con puntos utilizada en las notaciones mnemónicas no guarda ninguna relación con la notación decimal con puntos empleada para representar las direcciones en formato de patrón de bits.)

Aunque las direcciones mnemónicas resultan cómodas para los seres humanos, los mensajes siempre se transmiten a través de Internet mediante direcciones IP. Así, si un ser humano quiere enviar un mensaje a una máquina distante e identifica el destino por medio de una dirección mnemónica, el software que esté utilizando tiene que ser capaz de convertir dicha dirección en una dirección IP antes de transmitir el mensaje. Esta conversión se realiza con la ayuda de numerosos servidores, denominados **servidores de nombres**, que son esencialmente directorios que proporcionan servicios de traducción de direcciones a los clientes. Colectivamente, estos servidores de nombres se utilizan como un sistema de directorios global conocido como **Sistema de nombres de dominio** (DNS, *Domain Name System*). El proceso de utilizar el sistema DNS para realizar una traducción se denomina búsqueda **DNS**.

De esta forma, para que una máquina pueda ser accesible por medio de un nombre de dominio mnemónico, dicho nombre debe estar representado en alguno de los servidores de nombres del DNS. En aquellos casos en los que la entidad que ha establecido el dominio dispone de los recursos necesarios, puede establecer y mantener también su propio servidor de nombres que contenga todos los nombres pertenecientes a dicho dominio. De hecho, este es el modelo en el que se basaba originalmente el sistema de nombres de dominio. Cada dominio registrado representaba una región física de Internet, que era operada por algún tipo de autoridad local, como por ejemplo una empresa, una universidad o un organismo gubernamental. Esta autoridad era, en esencia, un ISP de acceso que proporcionaba a sus miembros acceso a Internet por medio de su propia intranet, la cual estaba conectada a Internet. Como parte de este sistema, la organización mantenía su propio servidor de nombres, que facilitaba los servicios de traducción para todos los nombres utilizados dentro de su dominio.

Este modelo sigue siendo común hoy día. Sin embargo, muchas empresas o pequeñas organizaciones quieren tener presencia en Internet y disponer de su propio dominio, pero sin dedicar los recursos necesarios para darle soporte. Por ejemplo, podría ser beneficioso para un club de ajedrez local tener presencia en Internet mediante el nombre de dominio `KingsandQueens.org`, pero es bastante probable que el club no disponga de los recursos necesarios para establecer su propia red, para mantener un enlace desde dicha red a Internet y para implementar su propio servidor de nombres. En este caso, el club puede firmar un contrato con un ISP de acceso para crear la apariencia de un dominio registrado utilizando los recursos que ya ha puesto en marcha el ISP. Normalmente, el club, quizá con la ayuda del ISP, registrará el nombre que el club haya seleccionado y firmará un contrato con el ISP para que dicho nombre se incluya en el servidor de nombres del ISP. Esto significa que todas las búsquedas DNS relativas al nuevo nombre de dominio serán dirigidas al servidor de nombres del ISP del que se obtendrá la traducción adecuada. De esta forma, en un mismo ISP pueden residir muchos dominios registrados, dándose a menudo el caso de que cada uno de ellos ocupa solamente una pequeña porción de una misma computadora.

Aplicaciones de Internet

En este apartado veremos algunas aplicaciones de Internet, comenzando con tres aplicaciones *tradicionales*. Sin embargo, estas aplicaciones “convencionales” no consiguen mostrar adecuadamente todo el interés que Internet suscita en la actualidad. De hecho, la distinción entre una computadora y otros dispositivos electrónicos va siendo cada vez más difusa. Los teléfonos, las televisiones, los aparatos de reproducción de sonido, las alarmas antirrobo, los hornos microondas y las videocámaras son, todos ellos, “dispositivos Internet” en potencia. A su vez, las aplicaciones tradicionales de Internet están viéndose empujadas por una marea en expansión de nuevas aplicaciones, incluyendo la mensajería instantánea, la videoconferencia, la telefonía Internet y la radio Internet. Después de todo, Internet es simplemente un sistema de comunicaciones por el que pueden transferirse datos. A medida que la tecnología continúa incrementando las tasas de transferencia de dicho sistema, el contenido de los datos que se transmiten solo está limitado por nuestra propia ima-

2. ¿Qué es DNS?
3. ¿Qué patrón de bits está representado por 3.6.9 en notación decimal con puntos? Exprese el patrón de bits 0001010100011100 utilizando notación decimal con puntos.
4. ¿En qué forma es la estructura de la dirección mnemónica de una computadora de Internet (como `r2d2.medicina.desconocida.edu`) similar a una dirección postal tradicional? ¿Tienen las direcciones IP esta misma estructura?
5. Cite tres tipos de servidores que pueden encontrarse en Internet e indique qué hace cada uno de ellos.
6. ¿Por qué se considera que SSH es superior a telnet?
7. ¿Cuáles son las diferencias entre las técnicas de emisión radio vía Internet basadas en P2P y en multidifusión y la técnica basada en N-unidifusión?
8. ¿Qué criterios hay que tener en cuenta a la hora de seleccionar uno de los cuatro tipos de VoIP?

4.3 La World Wide Web

En esta sección vamos a centrarnos en una aplicación Internet que permite diseminar información multimedia a través de Internet. Está basada en el concepto de **hipertexto**, un término que originalmente hacía referencia a documentos de texto que contenían enlaces, denominados **hipervínculos**, a otros documentos. Hoy día, el hipertexto se ha ampliado para incluir también imágenes, audio y vídeo, y a causa de esta expansión de su ámbito de actuación en ocasiones se denomina **hipermedia**.

Cuando se emplea una interfaz gráfica de usuario, el lector de un documento de hipertexto puede seguir los hipervínculos asociados con el mismo apuntando y haciendo clic con su ratón. Por ejemplo, suponga que en un documento de hipertexto aparece la frase “La interpretación del Bolero de Maurice Ravel por la orquesta fue excepcional” y que el nombre *Maurice Ravel* está vinculado a otro documento, que quizá proporcione información acerca del compositor. Un lector podría elegir ver ese material asociado apuntando al nombre *Maurice Ravel* con el ratón y haciendo clic en el botón del ratón. Además, si se instalan los hipervínculos apropiados, el lector podría escuchar una grabación de audio del concierto haciendo clic en la palabra *Bolero*.

De esta forma, un lector de documentos de hipertexto puede explorar documentos relacionados o seguir la línea de pensamiento de un documento a otro. A medida que se vinculan partes de documentos con otros documentos se va desarrollando una especie de tela de araña de información relacionada. Cuando se implementa en una red de computadoras este tipo de sistema, los documentos que componen esa “tela de araña” pueden residir en diferentes máquinas, formando una red de documentos global. Esa red de documentos que ha evolucionado en Internet tiene alcance mundial y se conoce como **World Wide Web** (también se la denomina **WWW**, **W3** o simplemente **Web**). A un documento de hipertexto en la World Wide Web a menudo se le llama

El Consorcio World Wide Web

El Consorcio World Wide Web (W3C) fue formado en 1994 para promocionar la World Wide Web desarrollando estándares de protocolos (conocidos como estándares W3C). W3C tiene su sede en el CERN, el laboratorio de partículas de alta energía de Ginebra, Suiza. El CERN es donde se desarrolló el lenguaje de composición HTML original, así como el protocolo HTTP para transferir documentos HTML a través de Internet. Hoy día, W3C es la fuente de muchos estándares (incluyendo estándares para XML y numerosas aplicaciones multimedia) que permiten la compatibilidad entre una amplia gama de productos Internet. Puede obtener más información acerca de W3C en su sitio web en la dirección <http://www.w3c.org>.

página web. Un conjunto de páginas web estrechamente relacionadas se conoce con el nombre de **sitio web**.

La World Wide Web tiene su origen en el trabajo de Tim Berners-Lee, que se dio cuenta del potencial que presentaba la combinación del concepto de documentos vinculados con la tecnología de interredes y que desarrolló el primer software para implementar la WWW en diciembre de 1990.

Implementación de la Web

Los paquetes software que permiten a los usuarios acceder a hipertexto en Internet caen en una de dos categorías: paquetes que desempeñan el papel de clientes y paquetes que desempeñan el papel de servidores. Un paquete de cliente reside en la computadora del usuario y se encarga de la tarea de obtener los materiales solicitados por el usuario y presentárselos de una forma organizada. Es el cliente que proporciona la interfaz de usuario el que permite a los usuarios navegar a través de la Web. De ahí que a ese cliente se le denomine a menudo navegador o **explorador** (*browser*), o en ocasiones explorador web. El paquete servidor (a menudo denominado **servidor web**) reside en una computadora que contiene los documentos de hipertexto a los que se puede acceder. Su tarea consiste en proporcionar acceso controlado a los documentos, según los vayan solicitando los clientes. En resumen, un usuario obtiene acceso a los documentos de hipertexto por medio de un explorador que reside en su computadora. Este explorador, que desempeña el papel de cliente, obtiene dichos documentos solicitando los servicios de servidores web dispersos por todo Internet. Normalmente, los documentos de hipertexto se transfieren entre los exploradores y los servidores web utilizando el protocolo **HTTP** (*Hypertext Transfer Protocol*, Protocolo de transferencia de hipertexto).

Para poder localizar y extraer documentos en la World Wide Web, a cada documento se le asigna una dirección unívoca denominada **URL** (*Uniform Resource Locator*, Localizador uniforme de recursos). Cada URL contiene la información necesaria para que un explorador contacte con el servidor apropiado y solicite el documento deseado. Así, para ver una página web, una persona proporciona a su explorador el URL del documento deseado y luego le ordena que lo extraiga y lo muestre.

En la Figura 4.8 se muestra un URL típico. Está formado por cuatro segmentos: el protocolo que hay que utilizar para comunicarse con el servidor que