### CUESTIONES BÁSICAS

- Las funciones claves que generalmente lleva a cabo un protocolo comprenden el encapsulamiento, la fragmentación y el reensamblado, el control de la conexión, la entrega ordenada, el control de flujo, el control de errores, el direccionamiento y la multiplexación.
- Un conjunto de redes consta de múltiples redes separadas que están interconectadas por dispositivos de encaminamiento. Los datos se intercambian en paquetes entre un sistema origen y un destino a través de un camino que involucra múltiples redes y dispositivos de encaminamiento. Normalmente se utiliza un modo de operación no orientado a conexión o datagrama. Un dispositivo de encaminamiento acepta datagramas y los retransmite hacia su destino y es responsable de determinar la ruta, del mismo modo en el que actúa un nodo de conmutación de paquetes.
- El protocolo más comúnmente utilizado para la interconexión de redes es el Protocolo Internet (IP, *Internet Protocol*). IP incorpora una cabecera a los datos de la capa inmediatamente superior (por ejemplo, TCP) para formar un datagrama IP. La cabecera incluye las direcciones origen y destino, información utilizada para la fragmentación y el reensamblado, un campo de tiempo-de-vida, un campo de tipo de servicio y una suma de comprobación.
- Se ha definido un protocolo IP de nueva generación, conocido como IPv6. IPv6 proporciona campos de dirección más grandes y una mayor funcionalidad que el actual IP.

El propósito de este capítulo es examinar el Protocolo Internet, que constituye los fundamentos sobre los que se basan todos los protocolos de conjuntos de redes y la interconexión entre ellas. En primer lugar, será útil revisar las funciones básicas de los protocolos de red. Este repaso sirve para resumir parte del material introducido previamente y constituye un punto de comienzo en el estudio de los protocolos de interconexión de redes en la Parte V. A continuación, se expondrá una discusión sobre la interconexión de redes. El resto del capítulo está dedicado a los dos protocolos estándar de interconexión de redes: IPv4 e IPv6.

Se recomienda al lector repasar la Figura 2.15 para situar la posición de los protocolos que se discuten en este capítulo dentro del conjunto de protocolos TCP/IP.

## 18.1. FUNCIONES BÁSICAS DE LOS PROTOCOLOS

Antes de comenzar la discusión sobre los protocolos de interconexión de redes, consideremos un conjunto bastante pequeño de funciones que forman la base de todos los protocolos. No todos los protocolos poseen todas las funciones; esto implicaría una duplicación significativa del esfuerzo. Existen, no obstante, muchas instancias del mismo tipo de función presentes en los protocolos a distintos niveles.

Es posible agrupar las funciones de un protocolo dentro de las siguientes categorías:

- Encapsulamiento.
- Fragmentación y reensamblado.
- Control de conexión.
- Entrega ordenada.
- Control de flujo.

- Control de errores.
- Direccionamiento.
- Multiplexación.
- Servicios de transmisión.

## ENCAPSULAMIENTO

Prácticamente en todos los protocolos, los datos son transferidos en bloques, llamados unidades de datos del protocolo (PDU, *Protocol Data Unit*). Cada PDU contiene no solo datos, sino también información de control. Ciertamente, algunas PDU constan únicamente de información de control sin datos algunos. La información de control se puede clasificar en tres categorías generales:

- **Dirección:** la dirección del emisor y/o destinatario debe ser indicada.
- **Código de detección de errores:** se suele incluir algún tipo de secuencia de comprobación de la trama para detectar la ocurrencia de errores.
- **Control del protocolo:** se incluye información adicional para implementar las funciones de los protocolos enumeradas en lo que resta de esta sección.

La adición de información de control a los datos es lo que se conoce como **encapsulamiento**. Los datos son aceptados o generados por una entidad y encapsulados dentro de una PDU que contiene los datos más información de control. Numerosos ejemplos de PDU han aparecido en los capítulos precedentes (por ejemplo, TFTP (*véase* Figura 2.17), HDLC (*véase* Figura 7.7), retransmisión de tramas (*véase* Figura 10.19), ATM (*véase* Figura 11.4), AAL5 (*véase* Figura 11.15), LLC (*véase* Figura 15.7), IEEE 802.3 (*véase* Figura 16.3), IEEE 802.11 (*véase* Figura 17.8)).

## FRAGMENTACIÓN Y REENSAMBLADO[1]

Un protocolo se encarga del intercambio de flujos de datos entre dos entidades. Normalmente, la transferencia puede caracterizarse como una secuencia de PDU de algún tamaño acotado. En el nivel de aplicación, nos referimos a una unidad lógica de transferencia de datos como un mensaje. Independientemente de si la aplicación envía datos en mensajes o lo hace como un flujo continuo, los protocolos de niveles inferiores necesitarán separar los datos en bloques de un tamaño más reducido. Este proceso se denomina fragmentación.

En función del contexto, existe una serie de motivos para llevar a cabo la fragmentación. Algunas de las razones típicas para fragmentar se enumeran a continuación:

- La red de comunicaciones puede aceptar únicamente bloques de datos de un cierto tamaño como máximo. Por ejemplo, una red ATM está limitada a bloques de 53 octetos; Ethernet impone un tamaño máximo de 1526 octetos.
- El control de errores puede ser más eficiente con un tamaño de PDU más pequeño. Con PDU pequeñas se necesitan retransmitir menos bits cuando una PDU sufre un error.

[1] El término *segmentación* se utiliza en los documentos OSI, pero en la especificación de los protocolos relativos a TCP/IP se usa el término *fragmentación*. El significado de ambos es el mismo.

- Es posible proporcionar un acceso más equitativo y con menor retardo a los equipos de transmisión compartidos. Por ejemplo, sin un tamaño máximo de bloque, una estación podría monopolizar un medio multipunto.
- Un tamaño de PDU más pequeño supone que las entidades receptoras pueden reservar memorias temporales más pequeñas.
- Una entidad puede requerir que la transferencia de datos alcance algún tipo de terminación de vez en cuando, para efectuar controles y operaciones de reinicio/recuperación.

Existen varias desventajas en el uso de la fragmentación que hacen considerar tamaños de PDU tan grandes como sea posible:

- Como se acaba de explicar, cada PDU contiene una cierta cantidad de información de control. Por tanto, cuanto menor sea el bloque, mayor será el porcentaje de sobrecarga introducida.
- La llegada de una PDU puede generar una interrupción que debe ser atendida. A medida que el bloque sea más pequeño se generarán más interrupciones.
- Se requiere más tiempo para procesar muchas y pequeñas PDU.

Todos estos factores deben ser tomados en consideración por el diseñador de protocolos a la hora de determinar los tamaños de PDU máximos y mínimos.

El proceso inverso a la fragmentación es el reensamblado. Los datos segmentados pueden eventualmente ser reensamblados en mensajes apropiados en el nivel de aplicación. Si las PDU llegan fuera de orden, la tarea se complica.

El proceso de la fragmentación se ilustra en la Figura 2.4.

## CONTROL DE CONEXIÓN

Una entidad puede transmitir datos a otra entidad de tal forma que cada PDU sea tratada independientemente de sus predecesoras. Esto se conoce como transferencia de datos no orientada a conexión; un ejemplo es el uso del datagrama, descrito en el Capítulo 10. Pese a que este modo es útil, una técnica igualmente importante es la transferencia de datos orientada a conexión, de la cual el circuito virtual, también descrito en el Capítulo 10, es un ejemplo.

La transferencia orientada a conexión se prefiere (incluso se requiere) si las estaciones anticipan un intercambio de datos voluminoso y/o ciertos detalles del protocolo deben funcionar dinámicamente. Una asociación lógica, o conexión, se establece entre las entidades. Se suceden tres etapas (*véase* Figura 18.1):

- Establecimiento de la conexión.
- Transferencia de datos.
- Terminación de la conexión.

En protocolos más sofisticados pueden existir también fases de interrupción y recuperación de la conexión para hacer frente a los errores y otros tipos de interrupciones.

Durante la etapa de establecimiento de la conexión, dos entidades aceptan intercambiar datos. Generalmente, una estación emitirá una solicitud de conexión (de forma no orientada a conexión) hacia la otra. Es posible que una autoridad central esté involucrada. En los protocolos más simples,

la entidad receptora acepta o rechaza la solicitud y, en el primero de los casos, la conexión se considera establecida. En propuestas más complejas, esta fase incluye una negociación en lo tocante a la sintaxis, semántica y temporización del protocolo. Por supuesto, ambas entidades deben utilizar el mismo protocolo. Pero el protocolo puede permitir ciertas funcionalidades opcionales y éstas deben ser consensuadas mediante una negociación. Por ejemplo, el protocolo puede especificar un tamaño de PDU de hasta 8.000 octetos; una estación puede desear restringir este tamaño a 1.000 octetos.

Tras el establecimiento de la conexión se entra en la etapa de transferencia de datos. Durante esta fase se intercambian datos e información de control (por ejemplo, control de flujo y control de errores). La Figura 18.1 muestra una situación en la cual todos los datos fluyen en un sentido, con acuses de recibos devueltos en el otro. Más generalmente, tanto los datos como los acuses de recibo fluyen en ambos sentidos. Finalmente, una de las partes desea terminar la conexión y lo hace enviando una solicitud de terminación. Alternativamente, una autoridad central podría terminar la conexión forzosamente.

Una característica clave de muchos protocolos de transferencia de datos orientados a conexión es la utilización de secuenciación (por ejemplo, HDLC e IEEE 802.11). Cada una de las partes numera secuencialmente las PDU que envía a la otra. Dado que cada parte recuerda que se encuentra en una conexión lógica, puede mantener una lista de los números salientes que genera y los números entrantes producidos por la otra parte. Ciertamente, uno puede definir en esencia una transferencia de datos orientada a conexión como aquella en la que ambas partes numeran las PDU y mantienen un registro de los números salientes y entrantes. La secuenciación es la base para tres funciones básicas: entrega ordenada, control de flujo y control de errores.

La secuenciación no se encuentra presente en todos los protocolos orientados a conexión. Algunos ejemplos son la retransmisión de tramas y ATM. Sin embargo, todos los protocolos orientados a conexión incluyen en el formato de la PDU alguna forma de identificar la conexión, bien mediante un identificador único o bien mediante una combinación de las direcciones del origen y el destino.

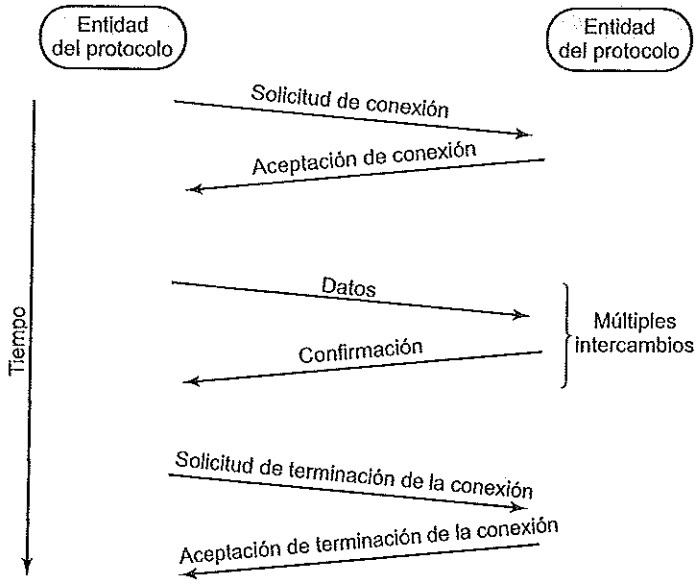


**Figura 18.1.** Etapas de una transferencia de datos orientada a conexión.

## ENTREGA ORDENADA

Si dos entidades comunicantes se encuentran en diferentes anfitriones[2] (*hosts*) conectados por una red, existe el riesgo de que las PDU no lleguen a su destino en el orden en que fueron enviadas debido a la posibilidad de que atraviesen caminos diferentes a través de la red. En los protocolos orientados a conexión se requiere generalmente que el orden de las PDU se mantenga. Por ejemplo, si un archivo es transferido entre dos sistemas, sería deseable que se asegurara que los registros del archivo recibido están en el mismo orden que los del archivo transmitido, y no mezclados. Si cada PDU recibe un número único y los números se asignan secuencialmente, lógicamente es una tarea simple para la entidad receptora el reordenar las PDU recibidas basándose en los números de secuencia. Un problema con este esquema es que, con un campo de número de secuencia finito, los números se repiten (módulo algún número máximo). Evidentemente, el número máximo de secuencia debe ser mayor que el máximo número de PDU que podrían estar pendientes en cualquier instante de tiempo. De hecho, se puede necesitar que el número máximo sea el doble que el máximo número de PDU que puedan estar pendientes (por ejemplo, ARQ de repetición selectiva; *véase* Capítulo 7).

## CONTROL DE FLUJO

El control de flujo es una función realizada por una entidad receptora para limitar la cantidad o la tasa de datos que es enviada por una entidad transmisora.

La forma más simple de control de flujo es un procedimiento de parada y espera, en el cual la recepción de cada PDU debe ser confirmada antes de que la siguiente sea enviada. Protocolos más eficientes incluyen algún tipo de crédito proporcionado al emisor, que es la cantidad de datos que pueden ser enviados sin acuse de recibo. La técnica de ventana deslizante de HDLC es un ejemplo de este mecanismo (*véase* Capítulo 7).

El control de flujo es un buen ejemplo de una función que debe ser implementada en varios protocolos. Considérese una vez más la Figura 2.3. La red necesitará efectuar un control de flujo sobre X a través del protocolo de acceso a la red para forzar el control sobre el tráfico de red. Al mismo tiempo, el módulo de acceso a la red Y posee únicamente un espacio limitado de memoria temporal y necesita efectuar un control de flujo sobre el módulo de acceso a la red X empleando el protocolo de transporte. Finalmente, aunque el módulo de acceso a la red Y pueda controlar su flujo de datos, la aplicación de Y puede ser vulnerable a un desbordamiento. Por ejemplo, la aplicación podría suspenderse mientras espera espacio en disco. Así, el control de flujo debe aplicarse también a los protocolos orientados a aplicación.

## CONTROL DE ERRORES

Las técnicas de control de errores son necesarias para la prevención frente a pérdidas y daños en los datos y la información de control. El control de errores se implementa generalmente como dos funciones separadas: detección de errores y retransmisión. Para conseguir la detección de errores, el emisor inserta un código de detección de errores en la PDU transmitida, que es una función de los otros bits en la PDU. El receptor comprueba el valor del código en la PDU recibida. Si se detecta un error, el receptor descarta la PDU. En caso de no recibir el acuse de recibo de la PDU

[2] El término *anfitrión* alude a cualquier sistema final conectado a una red, como un PC, una estación de trabajo o un servidor.

en un tiempo razonable, el emisor la retransmite. Algunos protocolos emplean también un código de corrección de errores, que habilita al receptor no sólo para detectar errores sino para corregirlos en algunos casos.

Al igual que con el control de flujo, el control de errores es una función que debe ser realizada en varias capas de protocolos. Considérese de nuevo la Figura 2.3. El protocolo de acceso a la red debería incluir el control de errores para asegurar que los datos se intercambian correctamente entre la estación y la red. Sin embargo, un paquete de datos puede perderse dentro de la red y el protocolo de transporte debería ser capaz de recuperarse ante la pérdida.

## DIRECCIONAMIENTO

El concepto de direccionamiento en una arquitectura de comunicaciones es una noción compleja y abarca una serie de cuestiones, incluyendo:

- Nivel de direccionamiento.
- Alcance del direccionamiento.
- Identificadores de conexión.
- Modo de direccionamiento.

Durante la discusión, ilustraremos los conceptos utilizando la Figura 18.2, que repite la Figura 2.13 y muestra una configuración utilizando la arquitectura TCP/IP. Los conceptos son esencialmente los mismos que para la arquitectura OSI o cualquier otra arquitectura de comunicaciones.

El **nivel de direccionamiento** se refiere al nivel en la arquitectura de comunicaciones en el cual una entidad es designada. Generalmente se asocia una dirección única con cada sistema final

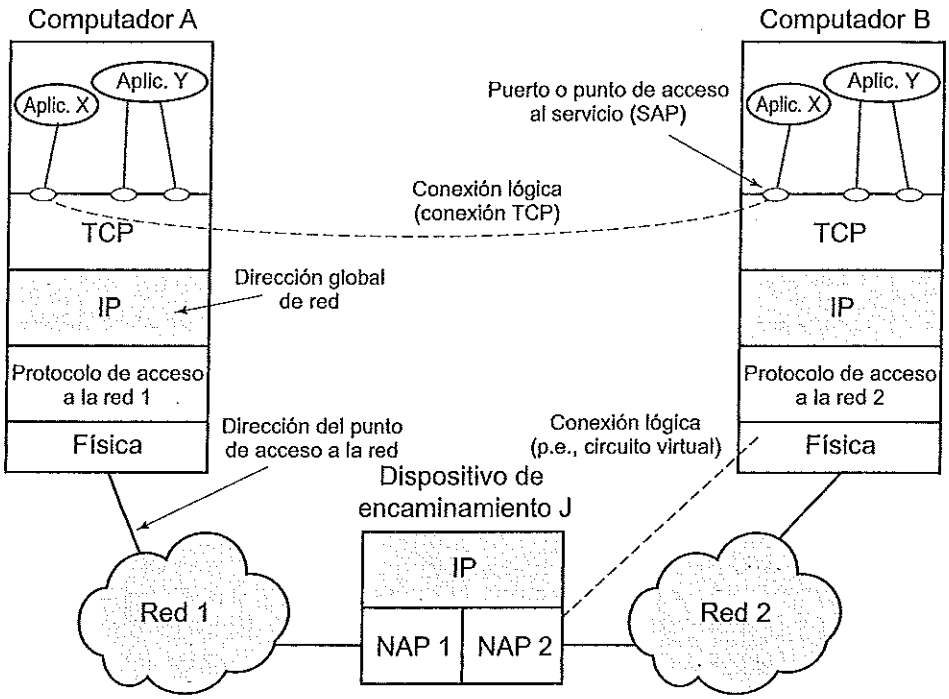


**Figura 18.2.** Conceptos TCP/IP.

(por ejemplo, una estación de trabajo o un servidor) y cada sistema intermedio (por ejemplo, un dispositivo de encaminamiento) en la configuración. Tal dirección es, en general, una dirección en el nivel de red. En el caso de la arquitectura TCP/IP, ésta es referida como dirección IP o, simplemente, dirección internet. En el caso de la arquitectura OSI, nos referimos a ella como punto de acceso al servicio de red (NSAP, *Network Service Access Point*). La dirección en el nivel de red se utiliza para encaminar una PDU a través de una o varias redes hasta el sistema indicado por la dirección en el nivel de red contenida en la PDU.

Una vez que los datos alcanzan el sistema destino, éstos deben ser dirigidos a algún proceso o aplicación en el sistema. Generalmente, un sistema soporta múltiples aplicaciones y una aplicación soporta varios usuarios. Cada aplicación, y quizá cada usuario concurrente de una aplicación, recibe un identificador único denominado puerto en la arquitectura TCP/IP y punto de acceso al servicio (SAP, *Service Access Point*) en la arquitectura OSI. Por ejemplo, un sistema podría soportar tanto una aplicación de correo electrónico como una de transferencia de archivos. Cada aplicación debería tener como mínimo un número de puerto o SAP que fuese único dentro del sistema. Además, la aplicación de transferencia de archivos podría soportar múltiples transferencias simultáneas, en cuyo caso a cada transferencia se le asignaría dinámicamente un número de puerto o SAP único.

La Figura 18.2 ilustra dos niveles de direccionamiento dentro de un sistema. Éste es generalmente el caso en la arquitectura TCP/IP. No obstante, podría existir direccionamiento en cada una de las capas de una arquitectura. Por ejemplo, se podría asignar un SAP único en cada nivel de la arquitectura OSI.

Otra cuestión relacionada con la dirección de un sistema final o intermedio es el **alcance del direccionamiento.** La dirección internet o dirección NSAP referida previamente es una dirección global. Las características clave de una dirección global son las siguientes:

- **Ausencia de ambigüedad global:** una dirección global identifica únicamente un sistema. Se permiten los sinónimos. Esto es, un sistema puede tener más de una dirección global.
- **Aplicabilidad global:** es posible que desde cualquier dirección global se identifique cualquier otra dirección global, ubicada en cualquier sistema, mediante la utilización de la dirección global del otro sistema.

Dado que una dirección global es única y aplicable globalmente, permite a una colección de redes encaminar datos procedentes de cualquier sistema conectado a una red hacia otro sistema conectado a cualquier otra red.

La Figura 18.2 ilustra que podría requerirse otro nivel de direccionamiento. Cada red debe mantener una dirección única para cada interfaz de dispositivo en la red. Ejemplos de ello son las direcciones MAC en una red IEEE 802 y las direcciones de anfitriones en ATM. Esta dirección permite a la red encaminar unidades de datos (por ejemplo, tramas MAC y celdas ATM) a través de la red y entregarlas al sistema pertinente. Podemos referirnos a tales direcciones como *direcciones del punto de acceso a la red.*

Generalmente, la cuestión del alcance del direccionamiento es sólo relevante para direcciones en el nivel de red. Un puerto o SAP por encima del nivel de red es único dentro de un sistema dado pero no necesita ser globalmente único. Por ejemplo, en la Figura 18.2 puede haber un puerto 1 en el sistema A y un puerto 1 en el sistema B. La designación completa de estos dos puertos podría ser expresada como A.1 y B.1, que son nombres únicos.

El concepto de **identificadores de conexión** aparece en escena cuando consideramos transferencias orientadas a conexión (por ejemplo, circuitos virtuales) en lugar de transferencias no orien-

tadas a conexión (por ejemplo, datagramas). En transferencias no orientadas a conexión se utiliza un identificador global para cada transmisión de datos. En el caso de las transferencias orientadas a conexión, es deseable en algunas ocasiones usar solamente un identificador de conexión durante la fase de transferencia de datos. El escenario es éste: la entidad 1 en el sistema A solicita una conexión a la entidad 2 en el sistema B, usando quizá la dirección global B.2. Cuando B.2 acepta la conexión se proporciona un identificador de conexión (normalmente un número) que es usado por ambas entidades para futuras transmisiones. El uso de un identificador de conexión presenta varias ventajas:

- **Reducción de la sobrecarga:** los identificadores de conexión son generalmente más cortos que los identificadores globales. Por ejemplo, en el protocolo de retransmisión de tramas (analizado en el Capítulo 10), los paquetes de solicitud de conexión contienen campos para la dirección de origen y la dirección de destino. Tras el establecimiento de la conexión lógica, denominada conexión de enlace de datos, las tramas de datos contienen un identificador de conexión del enlace de datos (DLCI, *Data Link Connection Identifier*) de 10, 16 o 23 bits.
- **Encaminamiento:** en la configuración de una conexión se puede definir una ruta fija. El identificador de la conexión sirve para identificar la ruta en los sistemas intermedios, como nodos de conmutación de paquetes, para manejar las futuras PDU.
- **Multiplexación:** trataremos esta función en términos más generales después. Aquí haremos la observación de que una entidad puede desear disfrutar de más de una conexión simultáneamente. Así, las PDU entrantes deben ser identificadas por su identificador de conexión.
- **Uso de información de estado:** una vez que una conexión está establecida, los sistemas finales pueden mantener información de estado concerniente a la misma. Esto permite funciones como el control de flujo y el control de errores utilizando números de secuencia. Vemos ejemplos de esto con HDLC (*véase* Capítulo 7) e IEEE 802.11 (*véase* Capítulo 17).

La Figura 18.2 muestra varios ejemplos de conexiones. La conexión lógica entre el dispositivo de encaminamiento J y el computador B se produce en el nivel de red. Por ejemplo, si la red 2 es una red de retransmisión de tramas, entonces esta conexión lógica sería una conexión de enlace de datos. En niveles superiores, muchos protocolos en el nivel de transporte, como TCP, soportan las conexiones lógicas entre usuarios del servicio de transporte. Así, TCP puede mantener una conexión entre dos puertos situados en sistemas diferentes.

Otro concepto de direccionamiento es el de **modo de direccionamiento**. En su forma más común, una dirección se refiere a un sistema individual o a un puerto; en este caso nos referiremos a ella como una dirección individual o **unidifusión** (*unicast*). Es también posible que una dirección se refiera a más de una entidad o puerto. Tal dirección identifica simultáneamente a múltiples receptores para los datos. Por ejemplo, un usuario podría desear enviar unos apuntes a una serie de personas. El centro de control de red podría querer notificar a todos los usuarios que la red va a venirse abajo. Una dirección para múltiples receptores puede ser de **difusión** (*broadcast*), destinada a todas las entidades dentro de un dominio, o de **multidistribución** (*multicast*), para un subconjunto específico de entidades. La Tabla 18.1 ilustra los casos posibles.

## MULTIPLEXACIÓN

Relacionado con el concepto de direccionamiento se encuentra el de multiplexación. Una forma de multiplexación es soportada mediante múltiples conexiones en un solo sistema. Por ejemplo, con retransmisión de tramas pueden existir varias conexiones de enlace de datos que terminen en el

**Tabla 18.1.** Modos de direccionamiento.

| Destino | Dirección de red | Dirección de sistema | Dirección de puerto/SAP |
|---|---|---|---|
| Unidifusión (*unicast*) | Individual | Individual | Individual |
| Multidifusión (*multicast*) | Individual<br>Individual<br>Todos | Individual<br>Todos<br>Todos | Grupo<br>Grupo<br>Grupo |
| Difusión (*broadcast*) | Individual<br>Individual<br>Todos | Individual<br>Todos<br>Todos | Todos<br>Todos<br>Todos |

mismo sistema; podemos decir que estas conexiones de enlace de datos son multiplexadas sobre la interfaz física individual que existe entre el sistema final y la red. La multiplexación puede realizarse también mediante números de puerto, lo cual permite también múltiples conexiones simultáneas. Por ejemplo, puede haber varias conexiones TCP que finalicen en un sistema dado, cada una establecida entre un par de puertos diferentes.

La multiplexación es usada igualmente en otro contexto, referente a la asignación de conexiones de un nivel a otro. Considérese de nuevo la Figura 18.2. La red 1 podría proporcionar un servicio orientado a conexión. Para cada conexión proceso a proceso establecida en el siguiente nivel, una conexión de enlace de datos podría ser creada en el nivel de acceso a la red. Ésta es una relación uno a uno, pero no tiene por qué ser así necesariamente. La multiplexación puede usarse en una de dos direcciones. La multiplexación ascendente, o hacia dentro, ocurre cuando múltiples conexiones de un nivel superior son multiplexadas sobre, o comparten, una única conexión de más bajo nivel. Esto puede ser necesario para hacer un uso más eficiente de los servicios de niveles inferiores o para proporcionar varias conexiones en niveles superiores dentro de un entorno en el que sólo existe una conexión en niveles inferiores. La multiplexación descendente, o división, significa que una conexión individual de un nivel superior se sustenta sobre múltiples conexiones de niveles inferiores, siendo repartido el tráfico de la conexión superior entre las distintas conexiones inferiores. Esta técnica puede ser utilizada para proporcionar fiabilidad, rendimiento o eficiencia.

## SERVICIOS DE TRANSMISIÓN

Un protocolo puede proporcionar una variedad de servicios adicionales a las entidades que lo usan. Mencionamos aquí tres ejemplos comunes:

- **Prioridad:** ciertos mensajes, como los de control, pueden necesitar llegar a la entidad destino con un retardo mínimo. Un ejemplo sería una solicitud de terminación de la conexión. Así, la prioridad podría ser asignada en función del mensaje. Adicionalmente, se podría asignar en función de la conexión.
- **Calidad de servicio:** ciertas clases de datos pueden requerir un umbral de rendimiento mínimo o un umbral de retardo máximo.
- **Seguridad:** los mecanismos de seguridad, restringiendo el acceso, pueden ser invocados.

Todos estos servicios dependen del sistema subyacente de transmisión y de cualquier entidad de niveles inferiores que intervenga. Si es posible que estos servicios sean proporcionados desde abajo, las dos entidades podrán hacer uso de ellos mediante el protocolo.