el formato de la trama Ethernet. Quizá sea entonces esta la única pieza verdaderamente importante del estándar Ethernet.

6.4.3 Switches de la capa de enlace

Hasta el momento no hemos entrado en detalles sobre lo que realmente hace un switch y cómo funciona. La función de un switch es recibir las tramas de la capa de enlace entrantes y reenviarlas a los enlaces de salida; en esta subsección vamos a estudiar la función de reenvío en detalle. El propio switch es **transparente** para los hosts y los routers de la subred; es decir, un host/router dirige una trama a otro host/router (en lugar de dirigirla al switch) y la envía a la red LAN, sin ser consciente de que un switch recibirá la trama y la reenviará. La velocidad a la que llegan las tramas a cualquiera de las interfaces de salida del switch puede ser temporalmente mayor que la capacidad del enlace de dicha interfaz. Para enfrentarse a este problema, las interfaces de salida del switch disponen de buffers, de forma muy parecida a como las interfaces de salida de un router disponen de buffers para los datagramas. Veamos ahora detenidamente cómo funciona un switch.

Reenvío y filtrado

El **filtrado** es la función del switch que determina si una trama debe ser reenviada a alguna interfaz o debe ser descartada. El **reenvío** es la función del switch que determina las interfaces a las que una trama debe dirigirse y luego envía la trama a esas interfaces. Las funciones de filtrado y reenvío del switch se realizan utilizando la **tabla de conmutación**. Esta tabla contiene entradas para algunos de los hosts y routers, no necesariamente todos, de una red LAN. Una entrada de la tabla de conmutación contiene (1) una dirección MAC, (2) la interfaz del switch que lleva hacia dicha dirección MAC y (3) el instante en el que la entrada fue incluida en la tabla. Un ejemplo de tabla de conmutación para el switch superior de la Figura 6.15 se muestra en la Figura 6.22. Esta descripción del reenvío de tramas puede parecer muy similar a lo que hemos visto sobre el reenvío de datagramas en el Capítulo 4. Efectivamente, en nuestra exposición sobre el reenvío generalizado de la Sección 4.4 vimos que es posible configurar muchos conmutadores de paquetes modernos para la función de reenvío basándose en las direcciones MAC de destino de capa 2 (es decir, función como switch de capa 2) o en las direcciones IP de destino de capa 3 (es decir, función como router de la capa 3). No obstante, es importante resaltar que los conmutadores reenvían los paquetes basándose en las direcciones MAC, en lugar de en las direcciones IP. También veremos que la tabla de un switch tradicional (es decir, en un contexto no SDN) se construye de forma muy distinta a como se crea la tabla de reenvío de un router.

Para comprender cómo funciona el filtrado y el reenvío en un switch, suponga que una trama con la dirección de destino DD-DD-DD-DD-DD-DD llega a la interfaz *x* del switch. Este buscará en su tabla la dirección MAC DD-DD-DD-DD-DD-DD. Se plantean tres posibilidades:

- No hay ninguna entrada en la tabla para DD-DD-DD-DD-DD-DD. En este caso, el switch reenvía copias de la trama a los buffers de salida que preceden a *todas* las interfaces salvo a la interfaz *x*. En otras palabras, si no hay ninguna entrada para la dirección de destino, el switch difunde la trama.
- Existe una entrada en la tabla que asocia DD-DD-DD-DD-DD-DD con la interfaz *x*. En este caso, la trama procede de un segmento de la LAN que contiene al adaptador DD-DD-DD-DD-DD-DD. Al no existir la necesidad de reenviar la trama a ninguna de las restantes interfaces, el switch lleva a cabo la función de filtrado descartando la trama.
- Existe una entrada en la tabla que asocia DD-DD-DD-DD-DD-DD con la interfaz $y \neq x$. En este caso, la trama tiene que ser reenviada al segmento de la LAN conectado a la interfaz *y*. El switch lleva a cabo su función de reenvío colocando la trama en un buffer de salida que precede a la interfaz *y*.

Apliquemos estas reglas al switch de la parte superior de la Figura 6.15 y a su tabla mostrada en la Figura 6.22. Suponga que una trama con la dirección de destino 62-FE-F7-11-89-A3 llega al switch desde la interfaz 1. El switch examina su tabla y ve que el destino está en el segmento de LAN conectado a la interfaz 1 (es decir, Ingeniería Eléctrica). Esto significa que la trama ya ha sido difundida en el segmento de LAN que contiene el destino. Por tanto, el switch filtra (es decir, descarta) la trama. Suponga ahora que una trama con la misma dirección de destino llega de la interfaz 2. De nuevo, el switch examina su tabla y ve que el destino está en la dirección de interfaz 1; por tanto, reenvía la trama al buffer de salida que precede a la interfaz 1. Con este ejemplo debería quedar claro que, siempre que la tabla de conmutación sea completa y precisa, el switch reenvía las tramas hacia los destinos sin llevar a cabo ninguna difusión.

En este sentido, un switch es "más inteligente" que un hub. Pero, ¿cómo se configura la tabla de conmutación? ¿Existen equivalentes para la capa de enlace de los protocolos de enrutamiento de la capa de red? ¿O tiene un administrador sobrecargado de trabajo que configurar manualmente la tabla de conmutación?

Auto-aprendizaje

Los switches tienen la fantástica propiedad (especialmente para los administradores de redes sobrecargados de trabajo) de que su tabla se construye de forma automática, dinámica y autónoma, sin intervención de un administrador de red ni de ningún protocolo de configuración. En otras palabras, los switches poseen la característica de **auto-aprendizaje**. Esta capacidad se lleva cabo de la forma siguiente:

1. Inicialmente, la tabla de conmutación está vacía
2. Para cada trama entrante recibida en una interfaz, el switch almacena en su tabla (1) la dirección MAC especificada en el *campo dirección de origen* de la trama, (2) la interfaz de la que procede la trama y (3) la hora actual. De esta forma, el switch registra en su tabla el segmento de la LAN en la que reside el emisor. Si todos los hosts de la LAN terminan enviando una trama, entonces todos los host terminarán estando registrados en la tabla.
3. El switch borra una dirección de la tabla si no se recibe ninguna trama con esa dirección como dirección de origen transcurrido un cierto periodo de tiempo (el **tiempo de envejecimiento**). De esta forma, si un PC es sustituido por otro (con un adaptador diferente), la dirección MAC del PC original será eliminada de la tabla de conmutación.

Examinemos la propiedad de auto-aprendizaje del switch superior de la Figura 6.15 y su tabla de conmutación correspondiente, mostrada en la Figura 6.22. Suponga que a las 9:39 una trama con la dirección de origen 01-12-23-34-45-56 llega procedente de la interfaz 2. Suponga también que esa dirección no está incluida en la tabla de conmutación. Entonces el switch añade una nueva entrada, como se muestra en la Figura 6.23.

Continuando con el mismo ejemplo, suponga que el tiempo de envejecimiento para este switch es de 60 minutos, y que entre las 9:32 y las 10:32 no le llega ninguna trama con la

Dirección	Interfaz	Hora
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....	....	....

Figura 6.22 ♦ Parte de la tabla de conmutación del switch superior de la Figura 6.15.

Dirección	Interfaz	Hora
01-12-23-34-45-56	2	9:39
62-FE-F7-11-89-A3	1	9:32
7C-BA-B2-B4-91-10	3	9:36
....	....	....

Figura 6.23 ♦ El switch aprende la ubicación de un adaptador con la dirección 01-12-23-34-45-56.

dirección de origen 62-FE-F7-11-89-A3. Entonces, a las 10:32 el switch eliminará esta dirección de su tabla.

Los switches son **dispositivos plug-and-play** porque no requieren intervención ni de un administrador de redes ni de los usuarios. Un administrador de redes que desee instalar un switch no tiene que hacer nada más que conectar los segmentos de la LAN a las interfaces del switch. El administrador no tiene que configurar las tablas de conmutación en el momento de la instalación ni cuando se elimina un host de uno de los segmentos de la LAN. Los switches también permiten la comunicación *full-duplex*, lo que significa que cualquier interfaz del switch puede enviar y recibir al mismo tiempo.

Propiedades de la conmutación de la capa de enlace

Una vez que hemos descrito el funcionamiento básico de un switch de la capa de enlace, vamos a pasar a ver sus características y propiedades. Podemos identificar varias ventajas de utilizar switches, en lugar de enlaces de difusión como las topologías de bus o basadas en hubs.

- *Eliminación de las colisiones*. En una red LAN construida con switches (y sin hubs) no se desperdicia ancho de banda a causa de las colisiones. Los switches almacenan las tramas en un buffer y nunca transmiten más de una trama a un segmento simultáneamente. Al igual que con los routers, la tasa máxima de transferencia agregada de un switch es la suma de todas las tasas de las interfaces del switch. Por tanto, los switches proporcionan una mejora significativa de rendimiento respecto al de las redes LAN con enlaces de difusión.
- *Enlaces heterogéneos*. Dado que un switch aísla un enlace de otro, los distintos enlaces de una LAN pueden operar a velocidades diferentes y pueden utilizar diferentes medios físicos. Por ejemplo, el switch superior de la Figura 6.15 puede tener tres enlaces de cobre 1000BASE-T a 1 Gbps, dos enlaces de fibra 100BASE-FX a 100 Mbps y un enlace de cobre 100BASE-T. Por tanto, un switch es ideal para combinar equipos heredados con equipos nuevos.
- *Administración.* Además de proporcionar una seguridad mejorada (véase el recuadro dedicado a la seguridad), un switch también facilita las tareas de gestión de la red. Por ejemplo, si un adaptador de red funciona mal y envía continuamente tramas Ethernet, un switch puede detectar el problema y desconectar internamente el adaptador que está funcionando incorrectamente. Con esta característica, el administrador de la red no tiene que levantarse de la cama y conducir hasta la oficina para corregir el problema. Del mismo modo, un corte en un cable solo desconecta al host que está usando el cable cortado para conectarse al switch. En la época del cable coaxial, los administradores de red pasaban muchas horas "recorriendo las líneas" (o dicho de forma más precisa, "arrastrándose por el suelo") hasta localizar el cable roto que había hecho que se cayera toda la red. Los switches también recopilan estadísticas acerca del uso del ancho de banda, de las tasas de colisión y de los tipos de tráfico, y ponen esta información a disposición

del administrador de la red. Esta información puede emplearse para depurar y corregir problemas y para planificar cómo deberá evolucionar la red LAN en el futuro. Los investigadores están explorando la adición de todavía más funcionalidades de gestión a las redes LAN Ethernet en implantaciones de prototipos [Casado 2007; Koponen 2011].

Switches frente a routers

Como hemos visto en el Capítulo 4, los routers son dispositivos de conmutación de paquetes de almacenamiento y reenvío que reenvían los paquetes utilizando direcciones de la capa de red. Aunque un switch también es un dispositivo de conmutación de paquetes de almacenamiento y reenvío, es fundamentalmente diferente de un router porque reenvía los paquetes utilizando direcciones MAC. Mientras que un router es un dispositivo de conmutación de paquetes de la capa 3, un switch es un dispositivo de conmutación de paquetes de la capa 2. Sin embargo, recuerde de la Sección 4.4 que los switches modernos que utilizan el paradigma "correspondencia-acción" pueden usarse tanto para reenviar una trama de la capa 2 según la dirección MAC de destino como un datagrama de la capa 3 usando la dirección IP de destino del datagrama. De hecho, vimos que los switches que utilizan el estándar OpenFlow pueden llevar a cabo un reenvío generalizado de los paquetes, basándose en hasta once campos diferentes de las cabeceras de trama, de datagrama y de la capa de transporte.

Aunque los switches y los routers son fundamentalmente diferentes, los administradores de red a menudo tienen que elegir entre ellos a la hora de instalar un dispositivo de interconexión. Por ejemplo, en la red de la Figura 6.15 el administrador de red podría haber utilizado fácilmente un router en lugar de un switch para conectar las redes LAN departamentales, los servidores y el router de pasarela de Internet. De hecho, un router permitiría las comunicaciones entre departamentos sin crear colisiones. Puesto que tanto los switches como los routers son candidatos como dispositivos de interconexión, ¿cuáles son los pros y los contras de cada uno de ellos?

En primer lugar vamos a ocuparnos de los pros y los contras de los switches. Como hemos mencionado anteriormente, los switches son dispositivos plug-and-play, una propiedad muy apreciada por todos los administradores de red del mundo sobrecargados de trabajo. Los switches también ofrecen tasas de filtrado y reenvío relativamente altas (como se muestra en la Figura 6.24,

SEGURIDAD

HUSMEANDO EN UNA LAN CONMUTADA: ENVENENAMIENTO DE UN SWITCH

Cuando un host está conectado a un switch, normalmente solo recibe las tramas que le están siendo enviadas de forma explícita. Por ejemplo, considere la red LAN conmutada de la Figura 6.17. Cuando el host A envía una trama al host B y existe una entrada para el host B en la tabla del conmutador, este reenviará la trama *únicamente* al host B. Si el nodo C está ejecutando un programa husmeador (*sniffer*) no podrá husmear esta trama de A a B. Por tanto, en una LAN conmutada (en contraste con un entorno de enlaces de difusión como las redes LAN 802.11 o las redes LAN Ethernet basadas en hub) es más difícil para un atacante husmear las tramas. Sin embargo, dado que los switches difunden las tramas que tienen direcciones de destino que no están almacenadas en sus tablas de conmutación, el programa sniffer de C puede todavía husmear algunas tramas que no están explícitamente dirigidas a C. Además, un programa sniffer podrá husmear todas las tramas Ethernet de difusión que tengan la dirección de destino de difusión FF–FF–FF–FF–FF–FF. Un ataque bien conocido contra un switch, que recibe el nombre de **envenenamiento de switch**, consiste en enviar toneladas de paquetes al switch con muchas direcciones MAC de origen falsas diferentes, que rellenarán la tabla de conmutación con entradas falsas y no dejarán espacio para las direcciones MAC de los nodos legítimos. Esto hace que el switch difunda la mayor parte de las tramas, las cuales pueden ser seleccionadas por el husmeador [Skoudis 2006]. Dado que este ataque es bastante complejo incluso para un atacante avanzado, los switches son significativamente menos vulnerables a los sniffers que las redes LAN inalámbricas y basadas en hubs.

los switches tienen que procesar las tramas solo hasta la capa 2, mientras que los routers tienen que procesar los datagramas hasta la capa 3). Por otro lado, para impedir los ciclos de las tramas de difusión, la topología activa de una red conmutada está restringida a un árbol de recubrimiento. Además, una red conmutada grande requerirá tablas ARP grandes en los hosts y routers y generará una cantidad de procesamiento y tráfico ARP sustancial. Los switches tampoco ofrecen ninguna protección frente a las tormentas de difusión (si un host está descontrolado y transmite un flujo de tramas Ethernet de difusión sin fin, los switches reenviarán todas esas tramas, haciendo que toda la red colapse).

Consideremos ahora los pros y los contras de los routers. Puesto que frecuentemente el direccionamiento de red es jerárquico (y no plano, como el direccionamiento MAC), normalmente los paquetes no seguirán ciclos a través de los routers incluso cuando la red tenga rutas redundantes. (Sin embargo, los paquetes pueden seguir ciclos cuando las tablas del router están mal configuradas; pero como hemos estudiado en el Capítulo 4, IP utiliza un campo especial de la cabecera del datagrama para limitar estos ciclos.) Por tanto, los paquetes no están restringidos a un árbol de recubrimiento y pueden utilizar la mejor ruta entre el origen y el destino. Dado que los routers no tienen la restricción del árbol de recubrimiento, han permitido que Internet haya sido creada con una topología rica que incluye, por ejemplo, múltiples enlaces activos entre Europa y América del Norte. Otra funcionalidad de los routers es que proporcionan protección mediante cortafuegos frente a las tormentas de difusión de la capa 2. Quizá el inconveniente más significativo de los routers es que no son dispositivos plug-and-play (ellos, y los hosts conectados a ellos, necesitan que sus direcciones IP sean configuradas). Además, los routers suelen tener un tiempo de procesamiento por paquete mayor que los switches, ya que tienen que procesar campos hasta la capa 3. Por último, en inglés existen dos formas diferentes de pronunciar la palabra router (“rootor” o “rowter”), y la gente pierde mucho tiempo discutiendo acerca de la pronunciación apropiada [Perlman 1999].

Dado que tanto los switches como los routers tienen sus ventajas y sus inconvenientes (como se resume en la Tabla 6.1), entonces ¿cuándo debe utilizar una red institucional (por ejemplo, una red de un campus universitario o una red corporativa) switches y cuándo routers? Normalmente, las redes pequeñas que constan de unos pocos cientos de hosts tienen pocos segmentos de LAN. Los switches son suficientes para estas redes pequeñas, ya que localizan el tráfico y aumentan la tasa de transferencia agregada sin necesidad de configurar direcciones IP. Pero las redes de mayor tamaño que constan de miles de hosts suelen incluir routers dentro de la red (además de switches). Los routers proporcionan un aislamiento más robusto del tráfico, controlan las tormentas de difusión y utilizan rutas más “inteligentes” entre los hosts de la red.

Para ver una exposición sobre los pros y los contras de las redes conmutadas y enrutadas, así como un estudio de cómo la tecnología LAN conmutada puede ampliarse para acomodar dos órdenes de magnitud más de hosts que las redes Ethernet actuales, consulte [Meyers 2004; Kim 2008].

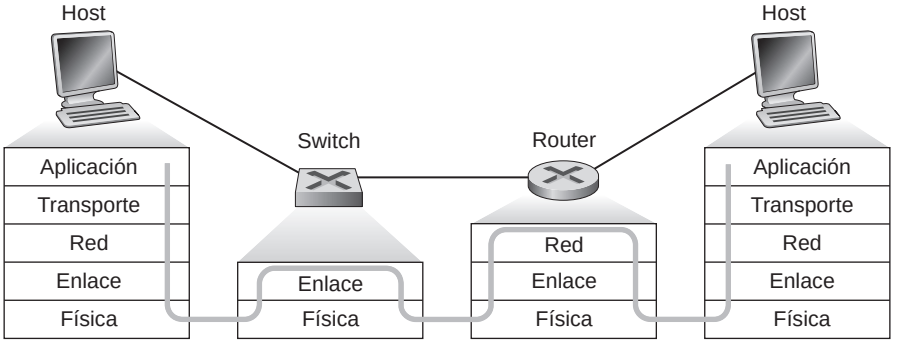

Figura 6.24 ♦ Procesamiento de paquetes en switches, routers y hosts.

	Hubs	Routers	Switches
Aislamiento del tráfico	No	Sí	Sí
Plug and play	Sí	No	Sí
Enrutamiento óptimo	No	Sí	No

Tabla 6.1 ♦ Comparación de funcionalidades típicas de dispositivos de interconexión populares.

6.4.4 Redes de área local virtuales (VLAN)

En nuestra explicación anterior de la Figura 6.15 hemos mencionado que las redes LAN institucionales modernas suelen estar configuradas de forma jerárquica, teniendo cada grupo de trabajo (departamento) su propia red LAN conmutada conectada a las redes LAN conmutadas de los otros grupos a través de una jerarquía de conmutadores. Aunque una configuración de este tipo funciona bien en un mundo ideal, el mundo real está bastante alejado del ideal.
En la configuración de la Figura 6.15 podemos identificar tres desventajas:

- *Falta de aislamiento del tráfico*. Aunque la jerarquía localiza el tráfico del grupo dentro de un mismo switch, el tráfico de difusión (por ejemplo, las tramas que transportan los mensajes ARP y DHCP o las tramas cuyo destino todavía no ha sido aprendido por un switch con auto-aprendizaje) tienen que atravesar toda la red institucional. Limitar el ámbito del tráfico de difusión mejoraría el rendimiento de la LAN. Quizá más importante, sería también deseable limitar el tráfico de difusión de la LAN por razones de seguridad y confidencialidad. Por ejemplo, si un grupo contiene al equipo de dirección de la empresa y otro grupo tiene empleados descontentos que ejecutan *sniffers* de paquetes Wireshark, probablemente el administrador de la red preferirá que el tráfico del equipo de dirección nunca llegue a los hosts de los empleados. Este tipo de aislamiento podría proporcionarse sustituyendo el switch central de la Figura 6.15 por un router. Enseguida veremos que este aislamiento también se puede conseguir a través de una solución conmutada (capa 2).
- *Uso ineficiente de los switches*. Si en lugar de tres grupos la institución tiene 10 grupos, entonces se necesitarían 10 switches de primer nivel. Si cada uno de los grupos es pequeño (por ejemplo, están formados por menos de 10 personas), entonces un único switch de 96 puertos sería lo suficientemente grande como para acomodar a todo el mundo, pero este único switch no proporcionaría la funcionalidad de aislamiento del tráfico.
- *Gestión de los usuarios*. Si un empleado se mueve entre grupos, el cableado físico debe modificarse para conectar al empleado a un switch diferente de la Figura 6.15. Los empleados que pertenecen a dos grupos constituyen incluso un problema mayor.

Afortunadamente, cada una de estas desventajas puede ser abordada por un switch compatible con **redes de área local virtuales** (**VLAN**, ***Virtual Local Area Network***). Como su nombre sugiere, un switch compatible con redes VLAN permite definir múltiples redes de área local *virtuales* sobre una única infraestructura de red de área local *física*. Los hosts de una VLAN se comunican entre sí como si solo ellos (y ningún otro host) estuvieran conectados al switch. En una VLAN basada en puertos, el administrador de la red divide los puertos (interfaces) del switch en grupos. Cada grupo constituye una VLAN, con los puertos de cada VLAN formando un dominio de difusión (es decir, el tráfico de difusión de un puerto solo puede llegar a los demás puertos del grupo). La Figura 6.25 muestra un único switch con 16 puertos. Los puertos 2 a 8 pertenecen a la VLAN IE, y los puertos 9 a 15 pertenecen a la VLAN CC (los puertos 1 y 16 no están asignados). Esta VLAN resuelve todas las dificultades mencionadas anteriormente: las tramas de las VLAN IE y CC están aisladas entre

sí, los dos switches de la Figura 6.15 se han sustituido por un único switch y si el usuario del puerto 8 del switch se une al departamento CC, el operador de red simplemente tendrá que reconfigurar el software de la VLAN de modo que el puerto 8 ahora esté asociado con la VLAN CC. Es fácil imaginar cómo se configura y funciona el switch para redes VLAN: el administrador de la red declara que un puerto pertenece a una determinada VLAN (los puertos no declarados pertenecen a una VLAN predeterminada) utilizando un software de gestión de switches; en el switch se mantiene una tabla de correspondencias entre puertos y redes VLAN y el hardware del switch solo entrega tramas entre puertos que pertenecen a la misma VLAN.

Pero a causa del completo aislamiento de las dos redes VLAN hemos introducido una nueva dificultad: ¿cómo puede enviarse el tráfico del departamento IE al departamento CC? Una forma de resolver esto sería conectando un puerto del conmutador VLAN (por ejemplo, el puerto 1 en la Figura 6.25) a un router externo y configurando dicho puerto para que pertenezca tanto a la VLAN IE como a la VLAN CC. En este caso, incluso aunque los departamentos IE y CC compartan el mismo switch físico, la configuración lógica sería como si dichos departamentos tuvieran switches separados conectados a través de un router. Un datagrama IP enviado desde el departamento IE al departamento CC primero atravesaría la VLAN IE para llegar al router y luego sería reenviado por el router por la VLAN CC hasta el host de CC. Afortunadamente, los fabricantes de switches hacen que dicha tarea de configuración resulte sencilla para los administradores de red, incorporando en un único dispositivo un switch VLAN *y* un router, con lo que no es necesario utilizar un router externo separado. En uno de los problemas de repaso del final del capítulo se examina este escenario más en detalle.

Volviendo de nuevo a la Figura 6.15, suponga ahora que en lugar de tener un departamento de Ingeniería de Computadoras separado algunos de los académicos de IE y CC están alojados en edificios diferentes, donde (¡por supuesto!) necesitan tener acceso a la red y (¡por supuesto también!) desean formar parte de la VLAN de su departamento. La Figura 6.26 muestra un segundo switch de 8 puertos, en el que los puertos se han definido como pertenecientes a la VLAN IE o a la VLAN CC, según sea necesario. Pero, ¿cómo deben interconectarse estos dos switches? Una solución fácil sería definir un puerto que perteneciera a la VLAN CC en cada conmutador (y lo mismo para la VLAN IE) y conectar estos puertos entre sí, como se muestra en la Figura 6.26(a). Sin embargo, esta solución no es escalable, ya que *N* redes VLAN requerirían *N* puertos en cada switch simplemente para interconectar los dos switches.

Un método más escalable consiste en interconectar los switches VLAN utilizando la técnica conocida como **troncalización VLAN (*VLAN Trunking*)**. Con esta técnica, mostrada en la Figura 6.26(b), un puerto especial de cada switch (el puerto 16 en el switch de la izquierda y el puerto 1 en el de la derecha) se configura como un puerto troncal para interconectar los dos switches VLAN. El puerto troncal pertenece a todas las VLAN y las tramas enviadas a cualquier VLAN son reenviadas a

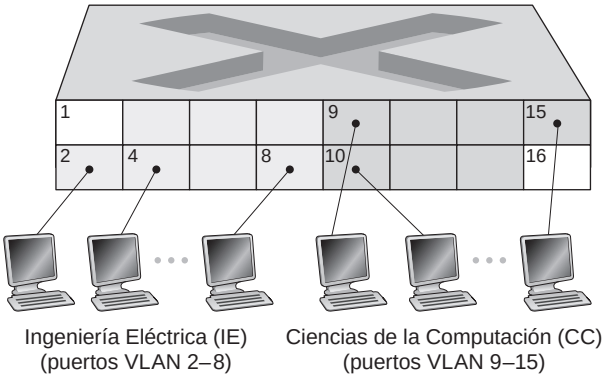

Figura 6.25 ♦ Un mismo conmutador con dos redes VLAN configuradas.

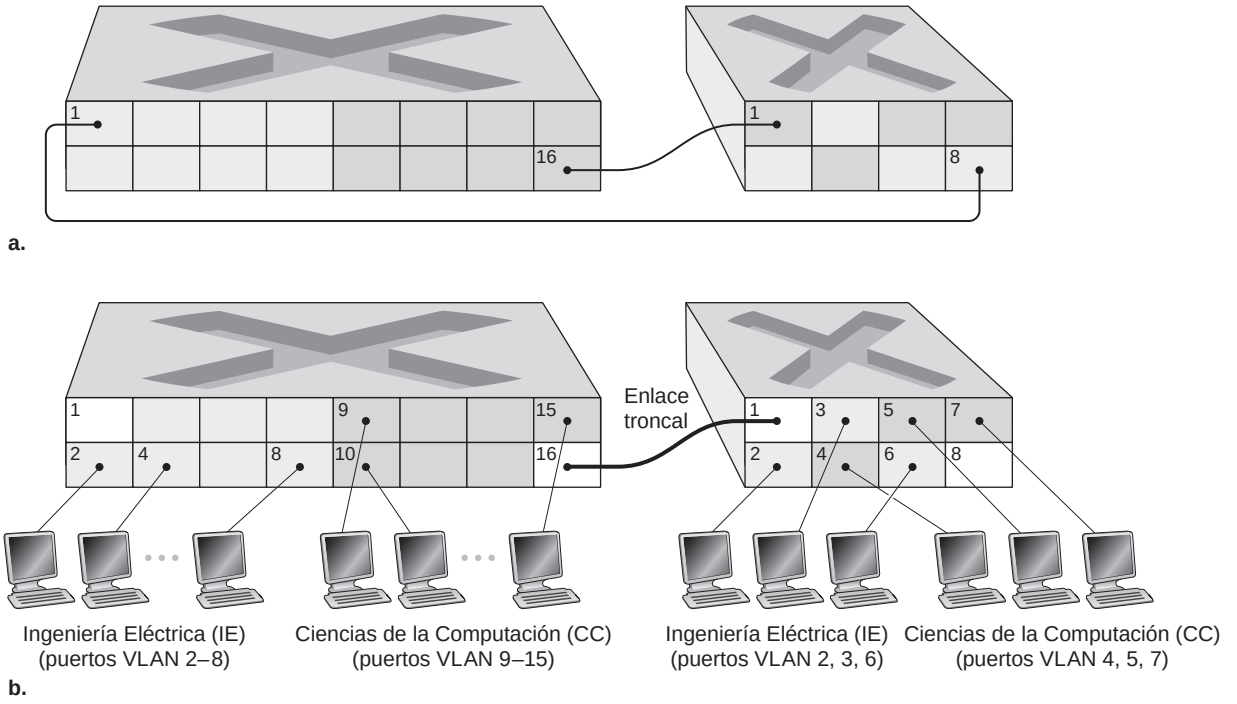

Figura 6.26 ♦ Conexión de dos switches VLAN con dos redes VLAN: (a) dos cables (b) enlace troncal.

través del enlace troncal hacia el otro switch. Pero esta solución nos conduce a otra pregunta: ¿cómo sabe un switch que una trama que ha llegado a un puerto troncal pertenece a una VLAN concreta? El IEEE ha definido un formato de trama Ethernet ampliado, 802.1Q, para las tramas que atraviesan un enlace troncal VLAN. Como se muestra en la Figura 6.27, la trama 802.1Q está formada por la trama Ethernet estándar más una **etiqueta VLAN** de cuatro bytes añadida a la cabecera, que transporta la identidad de la VLAN a la que pertenece la trama. El switch del lado emisor de un enlace troncal VLAN añade la etiqueta VLAN a la trama, la cual es analizada y eliminada por el switch del lado receptor del enlace troncal. La etiqueta VLAN en sí consta de un campo Identificador de protocolo de etiquetado (TPID, *Tag Protocol Identifier*) de 2 bytes (que tiene un valor hexadecimal fijo de 81-00) y de un campo Información de control de etiquetado (*Tag Control Information*) de 2 bytes, que contiene un campo identificador de VLAN de 12 bits y un campo de prioridad de 3 bits, cuya finalidad es similar a la del campo TOS de los datagramas IP.

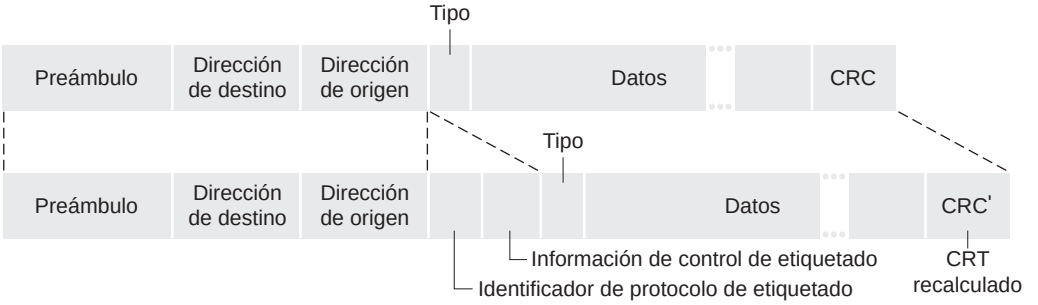

Figura 6.27 ♦ Trama Ethernet original (arriba), trama Ethernet con etiquetado 802.1Q (abajo).

En esta exposición hemos hablado muy brevemente de las redes VLAN y nos hemos centrado en las VLAN basadas en puertos. Debemos decir también que las redes VLAN se pueden definir de otras formas. En las VLAN basadas en direcciones MAC, el administrador de la red especifica el conjunto de direcciones MAC que pertenece a cada VLAN. Cuando un dispositivo se conecta a un puerto, el puerto se conecta a la VLAN apropiada basándose en la dirección MAC del dispositivo. Las redes VLAN también pueden definirse basándose en protocolos de la capa de red (como por ejemplo, IPv4, IPv6 o Appletalk) y en otros criterios. Las redes VLAN también pueden abarcar varios routers IP, lo que permite conectar islas de redes LAN con el fin de formar una única VLAN que podría abarcar todo el globo [Yu 2011]. Consulte el estándar 802.1Q [IEEE 802.1q 2005] para conocer más detalles.

6.5 Virtualización de enlaces: la red como una capa de enlace

Puesto que este capítulo está relacionado con los protocolos de la capa de enlace, y dado que estamos aproximándonos al final del capítulo, vamos a reflexionar acerca del modo en que ha evolucionado nuestra compresión acerca del término *enlace*. Al comenzar el capítulo, contemplábamos los enlaces como cables físicos que conectaban dos hosts que se comunicaban entre sí. Al estudiar los protocolos de acceso múltiple, hemos visto que podían conectarse varios hosts mediante un cable compartido y que el "cable" que conectaba esos hosts podía ser un espectro de radio u otro medio de comunicación. Esto nos llevó a considerar el enlace en forma algo más abstracta, más como un canal que como un cable. En nuestro estudio de las redes LAN Ethernet (Figura 6.15) hemos visto que los medios de interconexión podían ser, de hecho, una infraestructura conmutada bastante compleja. Sin embargo, a todo lo largo de esta evolución, los propios hosts mantenían la visión de que el medio de interconexión era simplemente un canal de la capa enlace que conectaba dos o más hosts. Vimos, por ejemplo, que un host Ethernet podía ser afortunadamente inconsciente de si estaba conectado a los otros hosts de la LAN mediante un único segmento LAN de corto alcance (Figura 6.17), o por una LAN conmutada geográficamente dispersa (Figura 6.15), o mediante una VLAN (Figura 6.26).

En el caso de una conexión mediante un módem telefónico entre dos hosts, el enlace que conecta los dos hosts es realmente la red telefónica: una red global de telecomunicaciones, lógicamente separada, con sus propios conmutadores, enlaces y pilas de protocolos para la transferencia de datos y la señalización. Sin embargo, desde el punto de vista de la capa de enlace de Internet, la conexión de acceso telefónico a través de la red de telefonía es contemplada como un simple "cable". En este sentido, Internet virtualiza la red telefónica, viéndola como una tecnología de la capa de enlace que proporciona conectividad de dicha capa entre dos hosts de Internet. Recordemos, de nuestro análisis de las redes solapadas en el Capítulo 2, que de forma similar las redes solapadas ven Internet como un medio de proporcionar conectividad entre los nodos solapados, buscando un solapamiento de Internet de la misma manera que Internet solapa la red telefónica.

En esta sección vamos a abordar las redes MPLS (*Multiprotocol Label Switching*, Conmutación de etiquetas multiprotocolo). A diferencia de la red telefónica de conmutación de circuitos, MPLS es una red de circuitos virtuales de conmutación de paquetes de pleno derecho. Tiene sus propios formatos de paquete y comportamientos de reenvío. Por tanto, desde el punto de vista pedagógico, el análisis de MPLS encaja bien en un estudio de la capa de red o de la capa de enlace. Sin embargo, desde el punto de vista de Internet podemos considerar MPLS, al igual que la red telefónica y las redes Ethernet conmutadas, como una tecnología de la capa de enlace que sirve para interconectar dispositivos IP. Por tanto, hemos incluido MPLS en nuestro estudio de la capa de enlace. Las redes Frame-Relay y ATM también pueden emplearse para interconectar dispositivos IP, aunque representan una tecnología algo más antigua (aunque todavía con implantación), de modo que no cubriremos esas redes aquí. Puede ver más detalles en el libro de [Goralski 1999]. Nuestro tratamiento de MPLS será necesariamente breve, ya que podrían escribirse (y se han escrito) libros completos sobre estas redes. Le recomendamos que lea [Davie 2000] para conocer más detalles sobre MPLS.

Aquí nos centraremos principalmente en el modo en que los servidores MPLS se interconectan con los dispositivos IP, aunque también profundizaremos algo más en las tecnologías subyacentes.

6.5.1 Conmutación de etiquetas multiprotocolo (MPLS)

La Conmutación de etiquetas multiprotocolo (MPLS) ha evolucionado a partir de una serie de desarrollos industriales que tuvieron lugar a mediados y finales de la década de 1990 y que buscaban mejorar la velocidad de reenvío de los routers IP, adoptando un concepto clave del mundo de las redes de circuitos virtuales: una etiqueta de longitud fija. El objetivo no era abandonar la infraestructura de reenvío de datagramas IP basada en el destino, sustituyéndola por otra basada en etiquetas de longitud fija y circuitos virtuales, sino expandir la infraestructura existente etiquetando selectivamente los datagramas y permitiendo a los routers reenviar esos datagramas basándose en etiquetas de longitud fija (en lugar de en direcciones IP de destino), siempre que fuera posible. Es importante observar que estas técnicas funcionan mano a mano con IP, utilizando el direccionamiento y el enrutamiento IP. El IETF unificó estos esfuerzos mediante el protocolo MPLS [RFC 3031, RFC 3032], consiguiendo así mezclar de forma efectiva las técnicas de circuitos virtuales en una red de datagramas enrutados.

Comencemos nuestro estudio sobre MPLS considerando el formato de una trama de la capa de enlace gestionada por un router compatible con MPLS. La Figura 6.28 muestra que una trama de la capa de enlace transmitida entre dispositivos compatibles con MPLS tiene una cabecera MPLS pequeña, que se añade entre la cabecera de la capa 2 (por ejemplo, Ethernet) y la cabecera de la capa 3 (es decir, IP). El documento RFC 3032 define el formato de la cabecera MPLS para tales enlaces; en otros RFC se definen también las cabeceras para las redes ATM y Frame-Relay. Entre los campos de la cabecera MPLS se encuentran la etiqueta, 3 bits reservados para su uso experimental, un único bit S que se utiliza para indicar el final de una serie de cabeceras MPLS "apiladas" (un tema avanzado del que no hablaremos aquí) y un campo de tiempo de vida.

Es evidente de manera inmediata, a partir de la Figura 6.28, que una trama ampliada MPLS solo se puede intercambiar entre routers compatibles con MPLS (dado que un router no compatible con MPLS se quedaría bastante confundido al encontrar una cabecera MPLS donde esperaba encontrar la cabecera IP). Los routers compatibles con MPLS se suelen denominar **routers de conmutación de etiquetas**, ya que reenvían las tramas MPLS buscando la etiqueta MPLS en su tabla de reenvío y luego pasando inmediatamente el datagrama a la interfaz de salida apropiada. Por tanto, el router compatible con MPLS *no* necesita extraer la dirección IP de destino y realizar una búsqueda del prefijo con la coincidencia más larga dentro de la tabla de reenvío. Pero, ¿cómo sabe un router si su vecino es compatible con MPLS y cómo sabe qué etiqueta asociar con la dirección IP de destino indicada? Para responder a estas preguntas, necesitamos examinar la interacción entre un grupo de routers compatibles con MPLS.

En el ejemplo de la Figura 6.29 los routers R1 a R4 son compatibles con MPLS. Los routers R5 y R6 son routers IP estándar. R1 ha anunciado a R2 y a R3 que él (R1) puede enrutar hacia el destino A y que una trama recibida con una etiqueta MPLS igual a 6 será reenviada al destino A. El router R3 ha anunciado al router R4 que puede realizar el enrutamiento hacia los destinos A y D, y

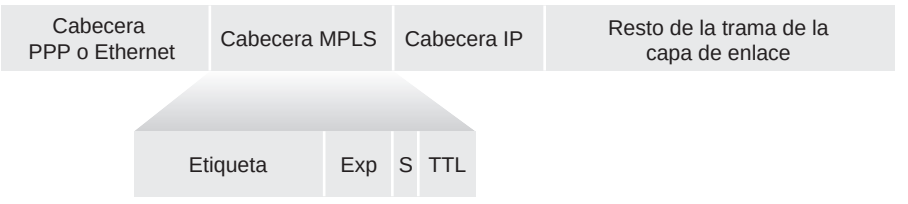

Figura 6.28 ♦ Cabecera MPLS: se localiza entre las cabeceras de la capa de enlace y de la capa de red.

que las tramas entrantes con etiquetas MPLS de valor 10 y 12, respectivamente, serán conmutadas hacia esos destinos. El router R2 también ha anunciado al router R4 que puede alcanzar el destino A y que una trama recibida con la etiqueta MPLS de valor 8 será conmutada hacia A. Observe que ahora el router R4 se encuentra en la interesante situación de tener dos rutas MPLS para llegar a A: a través de la interfaz 0 con etiqueta MPLS saliente igual a 10, y a través de la interfaz 1 con etiqueta MPLS igual a 8. El cuadro general de la estructura de red mostrada en la Figura 6.29 es que los dispositivos IP R5, R6, A y D están interconectados a través de una infraestructura MPLS (los routers compatibles con MPLS R1, R2, R3 y R4) de forma muy similar a como pueden conectarse entre sí diversos dispositivos IP mediante una red ATM o una LAN conmutada. Y al igual que sucede con una red ATM o una LAN conmutada, los routers R1 a R4 compatibles con MPLS se encargan de realizar esa conmutación *sin ni siquiera tocar la cabecera IP de los paquetes*.

En nuestra exposición anterior no hemos especificado el protocolo concreto que se utiliza para distribuir las etiquetas entre los routers compatibles con MPLS, ya que los detalles de este tipo de señalización caen fuera del alcance del libro. Sin embargo, tenemos que dejar constancia de que el grupo de trabajo de IETF dedicado a MPLS ha especificado en [RFC 3468] que el centro de sus esfuerzos dentro del campo de la señalización de MPLS será una extensión del protocolo RSVP, conocida como RSVP-TE [RFC 3209]. Tampoco hemos explicado cómo calcula MPLS en la práctica las rutas para los paquetes entre routers compatibles con MPLS, ni cómo recopila la información del estado de los enlaces (por ejemplo, la cantidad de ancho de banda del enlace no reservada por MPLS) que hay que utilizar en estos cálculos de rutas. Los algoritmos de enrutamiento existentes basados en el estado de los enlaces (por ejemplo, OSPF) han sido ampliados para inundar con estas informaciones los routers compatibles con MPLS. Merece la pena resaltar que los propios algoritmos de cálculo de las rutas no están estandarizados, siendo actualmente específicos del fabricante.

Hasta ahora, el énfasis de nuestro estudio sobre MPLS se ha centrado en el hecho de que MPLS realiza la conmutación basándose en etiquetas, sin necesidad de considerar la dirección IP de un paquete. Las verdaderas ventajas de MPLS y la razón del actual interés en este tipo de tecnología radica, sin embargo, no en los potenciales aumentos de las velocidades de conmutación, sino más bien en las nuevas capacidades de gestión del tráfico que MPLS posibilita. Como ya hemos indicado, R4 dispone de *dos* rutas MPLS hacia A. Si el reenvío se realizara más arriba, en la capa IP, basándose en la dirección IP, los protocolos de enrutamiento IP que hemos estudiado en el Capí-

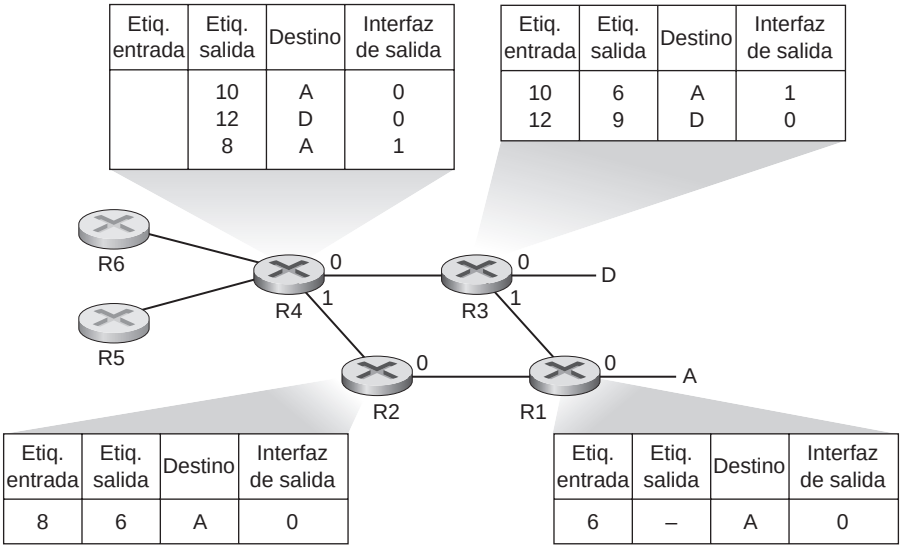

Figura 6.29 ♦ Reenvío mejorado mediante MPLS.

tulo 5 especificarían solamente una única ruta de coste mínimo hacia A. Por tanto, MPLS proporciona la capacidad de reenviar paquetes a través de rutas que no serían posibles utilizando los protocolos de enrutamiento IP estándar. Este es un tipo simple de **ingeniería de tráfico** utilizando MPLS [RFC 3346; RFC 3272; RFC 2702; Xiao 2000], mediante el que un operador de red puede anular el enrutamiento IP normal y forzar a que parte del tráfico dirigido hacia un cierto destino tome una determinada ruta, mientras que el resto del tráfico dirigido a ese mismo destino sigue una ruta distinta (por razones de política, de rendimiento o de algún otro tipo).

También se puede utilizar MPLS para muchos otros propósitos. Puede emplearse para llevar a cabo una restauración rápida de las rutas de reenvío de MPLS; por ejemplo, para volver a enrutar el tráfico a través de una ruta de reserva precalculada como respuesta a un fallo de un enlace [Kar 2000; Huang 2002; RFC 3469]. Por último, digamos que MPLS puede utilizarse (y de hecho se ha utilizado) para implementar las denominadas **redes privadas virtuales (VPN, *Virtual Private Network*)**. Al implementar una VPN para un cliente, un ISP utiliza su red compatible con MPLS para conectar entre sí las diversas redes del cliente. MPLS puede emplearse para aislar tanto los recursos como el direccionamiento empleados por la VPN del cliente con respecto a los de otros usuarios que también tengan que atravesar la red del ISP; consulte [DeClercq 2002] para ver más detalles.

Nuestra exposición acerca de MPLS ha sido necesariamente breve y animamos al lector a consultar las referencias mencionadas. Hay que destacar que, con tantos posibles usos de MPLS, este protocolo parece estar convirtiéndose rápidamente en la "navaja multiusos" de la ingeniería de tráfico en Internet.

6.6 Redes para centros de datos

En los últimos años, empresas de Internet como Google, Microsoft, Facebook y Amazon (así como sus competidoras en Asia y Europa) han construido inmensos centros de datos, cada uno de los cuales alberga decenas o centenares de miles de hosts, y que soportan simultáneamente muchas aplicaciones diferentes en la nube (por ejemplo, búsquedas, correo electrónico, redes sociales y comercio electrónico). Cada centro de datos tiene su propia **red del centro de datos**, que interconecta entre sí sus hosts y conecta el centro de datos con Internet. En esta sección vamos a realizar una breve introducción a las redes para centros de datos para aplicaciones en la nube.

El coste de un gran centro de datos es enorme, de más de 12 millones de $ por mes para un centro de datos con 100.000 hosts [Greenberg 2009a]. De estos costes, aproximadamente un 45% puede atribuirse a los propios hosts (que necesitan ser sustituidos cada 3 o 4 años); el 25%, a infraestructura, incluyendo transformadores, sistemas de alimentación ininterrumpida (SAI), generadores para apagones de larga duración y sistemas de refrigeración; 15% son los costes de la factura eléctrica, por la energía consumida y el 15% restante corresponde a las redes, incluyendo los equipos de red (switches, routers y equilibradores de carga), enlaces externos y costes asociados al tráfico de tránsito. (En estos porcentajes, los costes de los equipos se amortizan, de modo que se aplica una métrica de costes común a las adquisiciones y a los gastos corrientes, como la electricidad.) Aunque el de las redes no es el mayor coste, la innovación en este terreno es clave para reducir el coste global y maximizar el rendimiento [Greenberg 2009a].

Las abejas obreras en un centro de datos son los hosts: sirven contenido (por ejemplo, páginas web y vídeos), almacenan correos electrónicos y documentos y realizan, colectivamente, cálculos masivamente distribuidos (por ejemplo, cálculos distribuidos de índices para motores de búsqueda). Los hosts de los centros de datos, a los que se denomina **servidores blade** (cuchilla) y que recuerdan a las cajas de pizza, suele ser hosts de bajo coste, que incorporan la CPU, memoria y almacenamiento en disco. Los hosts se apilan en bastidores (*racks*), soliendo tener cada bastidor entre 20 y 40 servidores blade. En la parte superior de cada bastidor hay un switch, denominado **switch TOR** (***Top of Rack,*** parte superior del bastidor), que interconecta los hosts entre sí y con otros switches del centro de datos. Para ser concretos, cada host del bastidor tiene una tarjeta de interfaz de red que está conectada con su switch TOR, y cada switch TOR tiene puertos adicionales que pueden conectarse a

otros switches. Los hosts actuales suelen tener conexiones Ethernet a 40 Gbps con sus switches TOR [Greenberg 2015]. A cada host se le asigna también su propia dirección IP, interna al centro de datos.

La red del centro de datos soporta dos tipos de tráfico: el tráfico que fluye entre los clientes externos y los hosts internos, y el tráfico que fluye entre los hosts internos. Para manejar los flujos entre los clientes externos y los hosts internos, la red del centro de datos incluye uno o más **routers de frontera**, que conectan la red del centro de datos con la Internet pública. La red del centro de datos, por tanto, interconecta los bastidores entre sí y con los routers de frontera. La Figura 6.30 muestra un ejemplo de red de centro de datos. El **diseño de redes para centros de datos**, que es el arte de diseñar la red de interconexión y los protocolos que conectan los bastidores entre sí y con los routers de frontera, ha pasado en los últimos años a ser un área de investigación importante dentro del campo de las redes de computadoras [Al-Fares 2008; Greenberg 2009a; Greenberg 2009b; Mysore 2009; Guo 2009; Wang 2010].

Equilibrado de carga

Un centro de datos en la nube, como los de Google o Microsoft, proporciona muchas aplicaciones de manera simultánea, como por ejemplo aplicaciones de búsqueda, de correo electrónico o de vídeo. Para soportar las solicitudes de los clientes externos, cada aplicación está asociada con una dirección IP pública visible, a la que los clientes envían sus solicitudes y de la que los clientes reciben sus respuestas. Dentro del centro de datos, las solicitudes externas se dirigen primero a un **equilibrador de carga** cuya misión consiste en distribuir las solicitudes entre los hosts, equilibrando la carga entre todos ellos en función de su carga actual. Un gran centro de datos tendrá, a menudo, varios equilibradores de carga, cada uno de ellos dedicado a un conjunto de aplicaciones específicas en la nube. A tales equilibradores de carga se los denomina a veces "conmutadores de la capa 4", ya que toman decisiones basándose tanto en el número de puerto de destino (capa 4) como en la dirección IP de destino del paquete. Al recibir una solicitud para una aplicación concreta, el equilibrador de carga la reenvía a uno de los hosts encargados de gestionar esa aplicación. (El host puede, a su vez, invo-

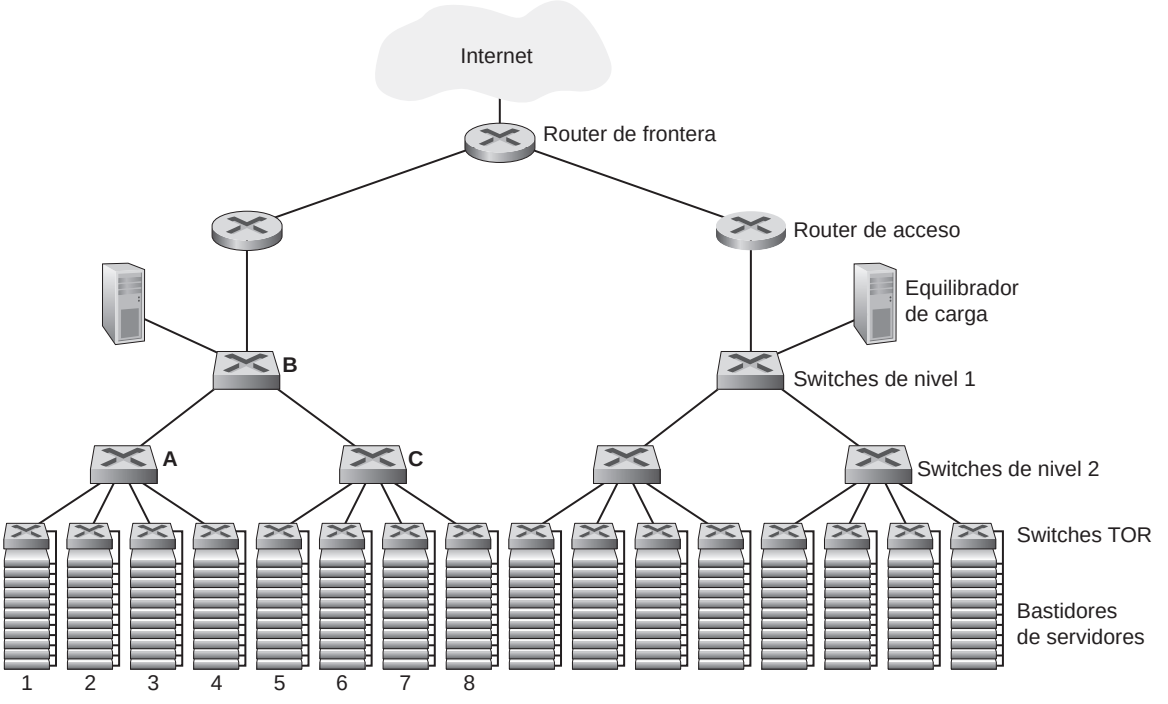

Figura 6.30 ♦ Una red de centro de datos con topología jerárquica.

car los servicios de otros hosts para que le ayuden a procesar la solicitud.) Cuando el host termina de procesar la solicitud, devuelve la respuesta al equilibrador de carga, que a su vez se la reenvía al cliente externo. El equilibrador no solo distribuye equitativamente la carga de trabajo entre los hosts, sino que también proporciona una función similar a NAT, traduciendo la dirección IP pública externa a la dirección IP interna del host apropiado, y luego realizando la traducción inversa para los paquetes que viajan en dirección contraria, hacia los clientes. Esto evita que los clientes contacten directamente con los hosts del centro de datos, lo que proporciona la ventaja de seguridad de ocultar la estructura interna de la red e impedir que los clientes interactúen directamente con los hosts.

Arquitectura jerárquica

Para un pequeño centro de datos que solo albergue unos pocos miles de hosts podría bastar una red simple, compuesta por un router de frontera, un equilibrador de carga y unas pocas decenas de bastidores, todos ellos interconectados mediante un único switch Ethernet. Pero para ampliar el centro a decenas o cientos de miles de hosts, los centros de datos emplean a menudo una jerarquía de routers y switches, como la topología mostrada en la Figura 6.30. En la parte superior de la jerarquía, el router de frontera está conectado con una serie de routers de acceso (en la Figura 6.30 solo se muestran dos, pero puede haber muchos más). Debajo de cada router de acceso hay tres niveles de switches. Cada router de acceso se conecta a un switch de nivel superior y cada switch de nivel superior se conecta a múltiples switches de segundo nivel y a un equilibrador de carga. Cada switch de segundo nivel se conecta, a su vez, con múltiples bastidores, a través de los switches TOR (switches de tercer nivel) de los propios bastidores. Todos los enlaces suelen usar Ethernet para sus protocolos de la capa física y de la capa de enlace, con una mezcla de cables de cobre y de fibra óptica. Con este tipo de diseño jerárquico, resulta posible ampliar un centro de datos hasta los cientos de miles de hosts.

Para un proveedor de aplicaciones en la nube resulta crítico proporcionar de modo continuo aplicaciones con una alta disponibilidad. Es por eso que los diseños de centros de datos también incluyen equipos de red redundantes y enlaces redundantes (estos recursos redundantes no se muestran en la Figura 6.30). Por ejemplo, cada switch TOR puede conectarse a dos switches de nivel 2, y cada router de acceso, switch de nivel 1 y switch de nivel 2 puede duplicarse e integrarse en el diseño [Cisco 2012; Greenberg 2009b]. En el diseño jerárquico de la Figura 6.30, observe que los hosts situados debajo de cada router de acceso forman una única subred. Para confinar el tráfico de difusión ARP, cada una de estas subredes se particiona, a su vez, en subredes VLAN más pequeñas, cada una de las cuales está compuesta por unos pocos cientos de hosts [Greenberg 2009a].

Aunque la arquitectura jerárquica convencional que acabamos de describir resuelve el problema de la escala, presenta el problema de la *limitada capacidad de host a host* [Greenberg 2009b]. Para entender esta limitación, fijémonos de nuevo en la Figura 6.30, y supongamos que cada host se conecta a su switch TOR a través de un enlace a 1 Gbps, mientras que los enlaces entre switches son enlaces Ethernet a 10 Gbps. Dos hosts del mismo bastidor siempre podrán comunicarse a la velocidad máxima de 1 Gbps, siendo el único factor limitante la velocidad de las tarjetas de interfaz de red del host. Sin embargo, si hay muchos flujos simultáneos en la red del centro de datos, la velocidad máxima entre dos hosts situados en diferentes bastidores puede ser muy inferior. Para entender el problema, considere un patrón de tráfico compuesto por 40 flujos simultáneos entre 40 pares de hosts situados en bastidores distintos. Específicamente, suponga que cada uno de los 10 hosts del bastidor 1 de la Figura 6.30 envía un flujo al host correspondiente del bastidor 5. Suponga también que, de modo similar, hay diez flujos simultáneos entre pares de hosts de los bastidores 2 y 6, diez flujos simultáneos entre los bastidores 3 y 7 y diez flujos simultáneos entre los bastidores 4 y 8. Si cada flujo comparte la capacidad de un enlace de modo equitativo con los otros flujos que estén atravesando el enlace, entonces a cada uno de los 40 flujos que atraviesan el enlace A-B de 10 Gbps (y también el enlace B-C de 10 Gbps) solo le corresponderán 10 Gbps / 40 = 250 Mbps, que es significativamente menor que la velocidad de 1 Gbps de la tarjeta de interfaz de red. El problema se agrava aún más para los flujos entre hosts que necesiten subir más arriba, dentro de la jerarquía de enlaces. Para resolver esta limitación, una posible solución es implantar switches y routers de

velocidad más alta. Pero esto incrementaría significativamente el coste del centro de datos, porque los switches y routers con altas velocidades de puerto son muy caros.

Soportar un gran ancho de banda de comunicación host a host es importante, porque uno de los requisitos clave de los centros de datos es la flexibilidad en la ubicación de la capacidad de cómputo y de los servicios [Greenberg 2009b; Farrington 2010]. Por ejemplo, un motor de búsqueda en Internet a gran escala puede ejecutarse en miles de hosts distribuidos entre múltiples bastidores, con unas necesidades de ancho de banda significativas entre todos los pares de hosts. De forma similar, un servicio de computación en la nube como EC2 podría necesitar albergar las múltiples máquinas virtuales que componen el servicio de un cliente en los hosts físicos que dispongan de mayor capacidad, independientemente de su ubicación en el centro de datos. Si estos hosts físicos están distribuidos entre múltiples bastidores, cuellos de botella en la red como los que hemos descrito anteriormente podrían provocar un bajo rendimiento.

Tendencias en las redes para centros de datos

Para reducir el coste de los centros de datos, y para mejorar al mismo tiempo su retardo de respuesta y su tasa de transferencia, gigantes de Internet en el campo de servicios en la nube, como Google, Facebook, Amazon y Microsoft, están continuamente implantando nuevos diseños de redes para centros de datos. Aunque estos diseños son exclusivos de esas empresas, podemos de todos modos identificar varias tendencias importantes.

Una de esas tendencias es la de implantar nuevas arquitecturas de interconexión y protocolos de red que resuelvan los problemas de los diseños jerárquicos tradicionales. Una de dichas soluciones consiste en sustituir la jerarquía de switches y routers por una **topología completamente conectada** [Facebook 2014; Al-Fares 2008; Greenberg 2009b; Guo 2009], como la mostrada en la Figura 6.31. En este diseño, cada switch de nivel 1 se conecta a todos los switches de nivel 2, de modo que (1) el tráfico de host a host nunca necesita subir por encima de los niveles de switches y (2) con n switches de nivel 1, entre cualesquiera dos switches de nivel 2 existirán n rutas disjuntas. Un diseño de este tipo puede mejorar significativamente la capacidad host a host. Para comprobarlo, considere de nuevo nuestro ejemplo de los 40 flujos. La topología de la Figura 6.31 puede gestionar perfectamente ese patrón de flujo, ya que existen cuatro rutas diferentes entre el primer switch de nivel 2 y el segundo, las cuales proporcionan una capacidad agregada de 40 Gbps entre los dos primeros switches de nivel 2. Este tipo de diseño no solo alivia la limitación de la capacidad host a host, sino que también crea un entorno más flexible de cómputo y de prestación de servicios, en el que la comunicación entre cualesquiera dos bastidores que no estén conectados al mismo switch es lógicamente equivalente, independientemente de dónde estén ubicados en el centro de datos.

Otra tendencia importante es la de emplear centros de datos modulares (MDC, *Modular Data Center*) basados en contenedores [Youtube 2009; Waldrop 2007]. En un MDC, una fábrica construye un "minicentro de datos" dentro de un contenedor estándar de 12 metros y envía el contenedor a las instalaciones del centro de datos. Cada contenedor tiene unos pocos miles de hosts, apilados en decenas de bastidores, que están densamente empaquetados. En las instalaciones del centro de datos se interconectan múltiples contenedores entre sí y con Internet. Una vez implantado un contenedor prefabricado en un centro de datos a menudo resulta difícil realizar su mantenimiento. Por ello, cada contenedor está diseñado para sufrir una degradación suave del rendimiento: a medida que los componentes (servidores y switches) van fallando con el tiempo, el contenedor continúa funcionando, pero con un rendimiento menor. Una vez que ha fallado un gran número de componentes y el rendimiento cae por debajo de un cierto umbral, se elimina todo el contenedor y se lo sustituye por uno nuevo.

La creación de centros de datos a partir de contenedores plantea nuevos desafíos relacionados con la red. En un MDC hay dos tipos de redes: las redes internas a los contenedores, confinadas dentro de los mismos, y la red principal que conecta a unos contenedores con otros [Guo 2009; Farrington 2010]. Dentro de un contenedor, a una escala de hasta unos pocos miles de hosts, resulta posible construir una red completamente conectada (como la que se ha descrito anteriormente)

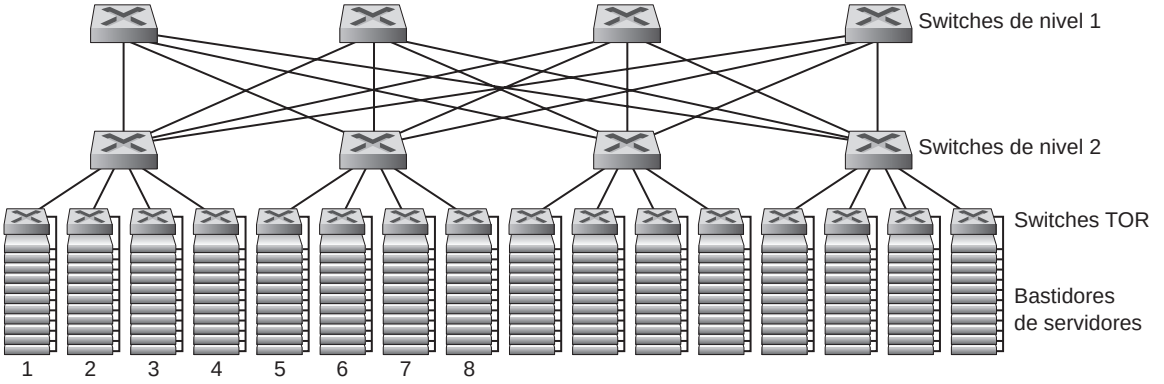

Figura 6.31 ♦ Topología altamente interconectada de red para centro de datos.

utilizando switches Gigabit Ethernet comerciales y baratos. Sin embargo, el diseño de la red principal, que interconecta cientos o miles de contenedores mientras proporciona un gran ancho de banda host a host entre contenedores, para las cargas de trabajo típicas, continúa planteando un desafío. En [Farrington 2010] se propone una arquitectura híbrida eléctrica/óptica de switches para interconectar los contenedores.

Al utilizar topologías altamente interconectadas, uno de los problemas principales es el de diseñar algoritmos de enrutamiento entre los switches. Una posibilidad [Greenberg 2009b] es emplear algún tipo de enrutamiento aleatorio. Otra posibilidad [Guo 2009] es incorporar múltiples tarjetas de interfaz de red en cada host, conectar cada host a múltiples switches comerciales de bajo coste y permitir que los propios hosts enruten el tráfico entre switches de forma inteligente. En los actuales centros de datos se están implantando hoy en día diversas extensiones y variantes de estas soluciones.

Otra tendencia importante es que los grandes proveedores en la nube construyen o personalizan cada vez más casi todos los equipos que incorporan a sus centros de datos, incluyendo los adaptadores de red, los switches, los routers, los TOR, el software y los protocolos de red [Greenberg 2015, Singh 2015]. Otra tendencia, de la que Amazon es pionero, es la de mejorar la fiabilidad mediante "zonas de disponibilidad" que lo que hacen, esencialmente, es duplicar los centros de datos en diferentes edificios cercanos. Al estar próximos los edificios (separados por solo unos kilómetros), los datos de las transacciones pueden sincronizarse entre los centros de datos pertenecientes a la misma zona de disponibilidad, proporcionando al mismo tiempo tolerancia ante fallos [Amazon 2014]. Resulta previsible que continúen produciéndose muchas más innovaciones en el diseño de centros de datos; animamos a los lectores interesados a que consulten los artículos y vídeos recientes sobre el diseño de redes para centros de datos.

6.7 Retrospectiva: un día en la vida de una solicitud de página web

Ahora que ya hemos cubierto el tema de la capa de enlace en este capítulo y las capas de red, de transporte y de aplicación en los anteriores, nuestro viaje de descenso por la pila de protocolos está completo. Al principio del libro (Sección 1.1) decíamos que "buena parte de este libro está relacionada con los protocolos de las redes de computadoras", y en los primeros cinco capítulo hemos visto que es así. Antes de zambullirnos en los capítulos temáticos de la segunda parte del libro, conviene finalizar nuestro viaje descendente por la pila de protocolos adoptando una vista integrada y holística de los protocolos que hemos estudiado hasta el momento. Una forma, por tanto,

de adoptar esta "vista panorámica" consiste en identificar los muchos (¡muchísimos!) protocolos implicados en satisfacer incluso la más simple de las solicitudes: la descarga de una página web. La Figura 6.32 ilustra el que será nuestro escenario de trabajo: un estudiante, Benito, conecta una computadora portátil al switch Ethernet de su facultad y descarga una página web (por ejemplo, la página principal de www.google.com). Como sabemos ahora, son *muchas* las cosas que suceden "entre bambalinas" para satisfacer esta solicitud aparentemente simple. Una práctica de laboratorio con Wireshark incluida al final del capítulo le permitirá examinar con mayor detalle una serie de archivos de traza que contienen varios de los paquetes implicados en escenarios similares.

6.7.1 Inicio: DHCP, UDP, IP y Ethernet

Supongamos que Benito arranca su computadora portátil y luego la conecta a un cable Ethernet conectado al switch Ethernet de la facultad, que a su vez está conectado al router de la facultad, como se muestra en la Figura 6.32. El router de la facultad está conectado a un ISP, que en este caso se llama comcast.net. En este ejemplo, comcast.net proporciona el servicio DNS para la facultad; por tanto, el servidor DNS reside en la red de Comcast, en lugar de en la red de la facultad. Supondremos que el servidor DHCP está ejecutándose dentro del router, como suele ser el caso.

Cuando Benito conecta por primera vez su portátil a la red no puede hacer nada (por ejemplo, descargar una página web) sin una dirección IP. Por tanto, la primera acción relacionada con la red que lleva a cabo la computadora portátil de Benito es ejecutar el protocolo DHCP para obtener una dirección IP, así como otras informaciones, desde el servidor DHCP local:

1. El sistema operativo del portátil de Benito crea un **mensaje de solicitud DHCP** (Sección 4.3.3) y lo incluye en un **segmento UDP** (Sección 3.3) con el puerto de destino 67 (servidor DHCP) y el puerto de origen 68 (cliente DHCP). A continuación, el segmento UDP es insertado dentro de un **datagrama IP** (Sección 4.3.1) con una dirección IP de destino de difusión (255.255.255.255) y una dirección IP de origen igual a 0.0.0.0, dado que la computadora portátil de Benito no tiene todavía una dirección IP.

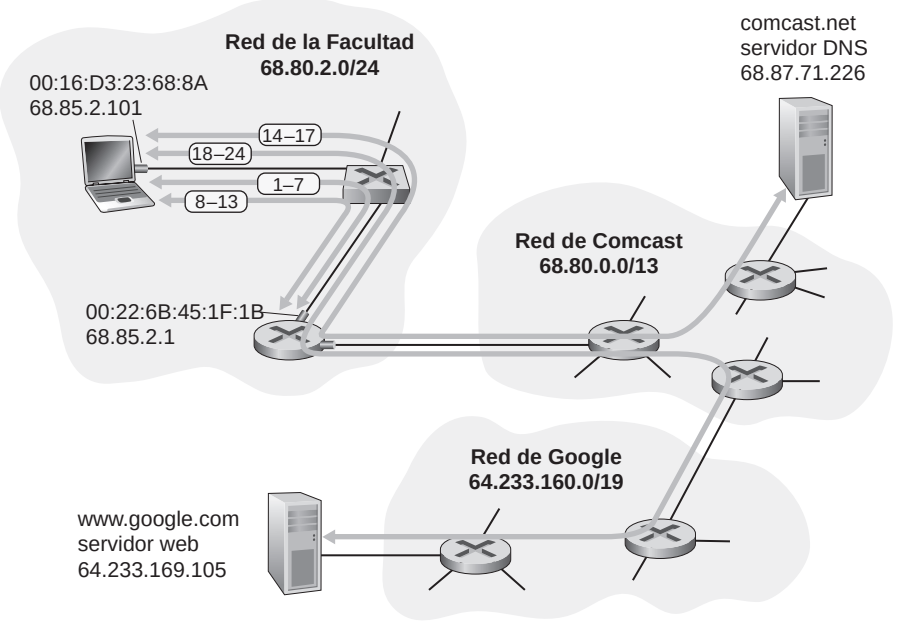

Figura 6.32 ♦ Un día en la vida de una solicitud de una página web: configuración y acciones de red.

2. El datagrama IP que contiene el mensaje de solicitud DHCP se inserta entonces en una **trama Ethernet** (Sección 6.4.2). La trama Ethernet tiene una dirección MAC de destino igual a FF:FF:FF:FF:FF:FF, de modo que la trama será difundida a todos los dispositivos conectados al switch (entre los que cabe esperar que se encuentre un servidor DHCP); la dirección MAC de origen de la trama es la de la computadora portátil de Benito, 00:16:D3:23:68:8A.
3. La trama Ethernet de difusión que contiene la solicitud DHCP es la primera trama enviada por la computadora de Benito al switch Ethernet. El switch difunde la trama entrante a todos los puertos de salida, incluyendo el puerto conectado al router.
4. El router recibe la trama Ethernet de difusión que contiene la solicitud DHCP a través de su propia interfaz con dirección MAC 00:22:6B:45:1F:1B, extrayendo el datagrama IP de la trama Ethernet. La dirección IP de destino de difusión contenida en el datagrama indica que este datagrama IP tiene que ser procesado por los protocolos de la capa superior existentes en este nodo, de modo que se **demultiplexa** (Sección 3.2) la carga útil del datagrama (un segmento UDP) y se entrega esa carga útil a UDP, tras lo cual se extrae del segmento UDP el mensaje de solicitud DHCP. Ahora el servidor DHCP dispone del mensaje de solicitud DHCP.
5. Supongamos que el servidor DHCP que se está ejecutando en el router puede asignar direcciones IP dentro del bloque **CIDR** (Sección 4.3.3) 68.85.2.0/24. En este ejemplo, todas las direcciones IP utilizadas dentro de la Facultad se encuentran dentro del bloque de direcciones de Comcast. Supongamos que el servidor DHCP asigna la dirección 68.85.2.101 al portátil de Benito. El servidor DHCP creará un **mensaje ACK DHCP** (Sección 4.3.3) que contendrá esta dirección IP, así como la dirección IP del servidor DNS (68.87.71.226), la dirección IP del router de pasarela predeterminado (68.85.2.1) y el bloque de subred (68.85.2.0/24) (o, lo que es lo mismo, la "máscara de red"). El mensaje DHCP se inserta dentro de un segmento UDP, que a su vez se incluye dentro de un datagrama IP, que se inserta en una trama Ethernet. La trama Ethernet tiene una dirección MAC de origen que será igual a la de la interfaz entre el router y la red doméstica (00:22:6B:45:1F:1B) y una dirección MAC de destino que será igual a la de la computadora portátil de Benito (00:16:D3:23:68:8A).
6. La trama Ethernet que contiene la respuesta ACK DHCP se envía (unidifusión) desde el router hacia el switch. Puesto que el switch tiene la característica de **auto-aprendizaje** (Sección 6.4.3) y ha recibido anteriormente una trama Ethernet (la que contenía la solicitud DHCP) desde el portátil de Benito, el switch sabe reenviar una trama dirigida a 00:16:D3:23:68:8A únicamente hacia el puerto de salida que conduce al portátil de Benito.
7. La computadora portátil de Benito recibe la trama Ethernet que contiene la respuesta ACK DHCP, extrae el datagrama IP de la trama Ethernet, extrae el segmento UDP del datagrama IP y extrae el mensaje ACK DHCP del segmento UDP. A continuación, el cliente DHCP de Benito anota su dirección IP y la dirección IP de su servidor DNS. También instala la dirección del router de pasarela predeterminado en su **tabla de reenvío IP** (Sección 4.1). El portátil de Benito enviará hacia el router de pasarela predeterminado todos los datagramas cuya dirección de destino caiga fuera de su subred 68.85.2.0/24. Llegados a este punto, la computadora portátil de Benito ha inicializado sus componentes de red y está lista para comenzar a procesar la extracción de la página web. (Observe que solo son necesarios los dos últimos pasos DHCP de los cuatro presentados en el Capítulo 4.)

6.7.2 Seguimos con el inicio: DNS y ARP

Cuando Benito escribe la dirección URL correspondiente a www.google.com en su navegador web, comienza la larga cadena de sucesos que terminará por hacer que se muestre la página de inicio de Google en su navegador web. El navegador de Benito comienza creando un **socket TCP** (Sección 2.7) que se utilizará para enviar la **solicitud HTTP** (Sección 2.2) hacia www.google.com. Para crear el socket, la computadora portátil de Benito necesita conocer la dirección IP de www.google.com. En la Sección 2.5 hemos visto que se utiliza el **protocolo DNS** para proporcionar este servicio de traducción de nombres a direcciones IP.

8. El sistema operativo de la computadora de Benito crea por tanto un **mensaje de consulta DNS** (Sección 2.5.3), incluyendo la cadena "www.google.com" en la sección de consulta del mensaje DNS. Después, este mensaje DNS se inserta dentro de un segmento UDP con un puerto de destino igual a 53 (servidor DNS). Después el segmento UDP se inserta dentro de un datagrama IP con una dirección IP de destino igual a 68.87.71.226 (la dirección del servidor DNS devuelta en el mensaje ACK DHCP en el Paso 5) y una dirección IP de origen igual a 68.85.2.101.
9. La computadora portátil de Benito inserta entonces el datagrama que contiene el mensaje de consulta DNS dentro de una trama Ethernet. Esta trama será enviada (direccionada en la capa de enlace) al router de pasarela de la red de la facultad de Benito. Sin embargo, aún cuando el portátil de Benito conoce la dirección IP del router de pasarela de la facultad (68.85.2.1), gracias al mensaje ACK DHCP del Paso 5 anterior, no sabe la dirección MAC del router de pasarela. Para obtener la dirección MAC de este router de pasarela, el portátil de Benito necesita utilizar el **protocolo ARP** (Sección 6.4.1).
10. La computadora portátil de Benito crea un mensaje de **consulta ARP** con una dirección IP de destino igual a 68.85.2.1 (el router de pasarela predeterminado), incluye el mensaje ARP dentro de una trama Ethernet con una dirección de destino de difusión (FF:FF:FF:FF:FF:FF) y envía la trama Ethernet hacia el switch, que entrega la trama a todos los dispositivos conectados, incluyendo al router de pasarela.
11. El router de pasarela recibe la trama que contiene el mensaje de solicitud ARP a través de la interfaz con la red de la facultad y se encuentra con que la dirección IP de destino, 68.85.2.1, contenida en el mensaje ARP, coincide con la dirección IP de su propia interfaz. El router de pasarela prepara en consecuencia una **respuesta ARP**, indicando que su dirección MAC 00:22:6B:45:1F:1B se corresponde con la dirección IP 68.85.2.1. A continuación, inserta el mensaje de respuesta ARP en una trama Ethernet, con una dirección de destino igual a 00:16:D3:23:68:8A (la de la computadora portátil de Benito) y envía la trama al switch, que la entrega al portátil de Benito.
12. El portátil de Benito recibe la trama que contiene el mensaje de respuesta ARP y extrae la dirección MAC del router de pasarela (00:22:6B:45:1F:1B) de ese mensaje.
13. La computadora portátil de Benito podrá ahora (*¡finalmente!*) dirigir la trama Ethernet que contiene la consulta DNS hacia la dirección MAC del router de pasarela. Observe que el datagrama IP de esta trama tiene la dirección IP de destino 68.87.71.226 (el servidor DNS), mientras que la trama tiene la dirección de destino 00:22:6B:45:1F:1B (el router de pasarela). El portátil de Benito envía esta trama al switch, que la entrega al router de pasarela.

6.7.3 Seguimos con el inicio: enrutamiento dentro del dominio al servidor DNS

14. El router de pasarela recibe la trama y extrae el datagrama IP que contiene la consulta DNS. El router busca la dirección de destino de este datagrama (68.87.71.226) y determina a partir de su tabla de reenvío que el datagrama debe enviarse al router situado más a la izquierda dentro de la red de Comcast de la Figura 6.32. El datagrama IP se inserta dentro de una trama de la capa de enlace que resulte apropiada para el enlace que conecta el router de la facultad con el router de Comcast situado más a la izquierda, después de lo cual la trama se envía a través de ese enlace.
15. El router situado más a la izquierda dentro de la red de Comcast recibe la trama, extrae el datagrama IP, examina la dirección de destino del datagrama (68.87.71.226) y determina, gracias a su tabla de reenvío, la interfaz de salida a través de la cual debe reenviar el datagrama hacia el servidor DNS. La tabla de reenvío habrá sido previamente rellenada mediante el protocolo interno del dominio de Comcast (por ejemplo **RIP**, **OSPF** o **IS-IS**, Sección 5.3), así como mediante el **protocolo entre dominios de Internet**, **BGP** (Sección 5.4).
16. Finalmente, el datagrama IP que contiene la consulta DNS terminará por llegar al servidor DNS, el cual extrae el mensaje de consulta DNS, busca el nombre www.google.com en su base de datos DNS (Sección 2.5) y encuentra el **registro de recurso DNS** que contiene la dirección

IP (64.233.169.105) para www.google.com (suponiendo que esa dirección esté actualmente almacenada en la caché del servidor DNS). Recuerde que estos datos de caché tienen su origen en el **servidor DNS autoritativo** (Sección 2.5.2) correspondiente a google.com. El servidor DNS compondrá un **mensaje de respuesta DNS** con la correspondencia entre el nombre de host y la dirección IP, después de lo cual inserta el mensaje de respuesta DNS en un segmento UDP e inserta este segmento en un datagrama IP dirigido a la computadora portátil de Benito (68.85.2.101). Este datagrama será reenviado de vuelta a través de la red de Comcast hasta el router de la facultad, y desde allí, a través del switch Ethernet, a la computadora de Benito.

17. La computadora portátil de Benito extrae la dirección IP del servidor www.google.com del mensaje DNS. *Finalmente*, después de un *montón* de trabajo, la computadora portátil de Benito estará ya lista para contactar con el servidor www.google.com.

6.7.4 Interacción web cliente-servidor: TCP y HTTP

18. Ahora que el portátil de Benito dispone de la dirección IP de www. google.com puede crear el **socket TCP** (Sección 2.7) que se utilizará para enviar el mensaje **GET HTTP** (Sección 2.2.3) a www.google.com. Cuando Benito crea el socket TCP, el protocolo TCP de su portátil tiene que llevar a cabo primero un **proceso de acuerdo en tres fases** (Sección 3.5.6) con el TCP de www. google.com. El portátil de Benito creará primero, por tanto, un segmento **SYN TCP** con puerto de destino 80 (para HTTP), insertará el segmento TCP dentro de un datagrama IP con una dirección de destino IP igual a 64.233.169.105 (www.google.com), incluirá el datagrama dentro de una trama con una dirección MAC de destino igual a 00:22:6B:45:1F:1B (el router de pasarela) y enviará la trama al switch.
19. Los routers de la red de la facultad, de la red de Comcast y de la red de Google reenvían el datagrama que contiene el segmento SYN TCP hacia www.google.com, utilizando la tabla de reenvío de cada router, como sucedía en los pasos 14–16 anteriores. Recuerde que las entradas de las tablas de reenvío de los routers que gobiernan el reenvío de paquetes a través del enlace entre dominios entre las redes de Comcast y de Google son determinadas mediante el protocolo **BGP** (Capítulo 5).
20. En algún momento, el datagrama que contiene el segmento SYN TCP llegará a www.google.com. El mensaje SYN TCP será extraído del datagrama y demultiplexado para ser entregado al socket de escucha asociado con el puerto 80. Se crea entonces un socket de conexión (Sección 2.7) para la conexión TCP entre el servidor HTTP de Google y la computadora portátil de Benito. Se genera después un segmento SYNACK TCP (Sección 3.5.6), se inserta dentro de un datagrama dirigido al portátil de Benito y, finalmente, se inserta dicho datagrama dentro de una trama de la capa de enlace que resulte apropiada para el enlace que conecta www.google.com con su router de primer salto.
21. El datagrama que contiene el segmento SYNACK TCP se reenvía a través de las redes de Google, de Comcast y de la facultad, terminando por llegar hasta la tarjeta Ethernet del portátil de Benito. El datagrama es demultiplexado dentro del sistema operativo y entregado al socket TCP creado en el Paso 18, con lo que entrará en estado conectado.
22. Ahora que el socket del portátil de Benito está (*¡finalmente!*) listo para enviar bytes a www.google.com, el navegador de Benito crea el mensaje GET HTTP (Sección 2.2.3) que contiene el URL que quiere extraer. Entonces, el mensaje GET HTTP se escribe en el socket con el mensaje GET pasando a constituir la carga útil de un segmento TCP. El segmento TCP se incluye en un datagrama y se envía y se entrega a www.google.com como en los Pasos 18–20.
23. El servidor HTTP en www.google.com lee el mensaje GET HTTP del socket TCP, crea un mensaje de **respuesta HTTP** (Sección 2.2), inserta el contenido de la página web solicitada en el cuerpo del mensaje de respuesta HTTP y envía el mensaje a través del socket TCP.
24. El datagrama que contiene el mensaje de respuesta HTTP se reenvía a través de las redes de Google, de Comcast y de la facultad y llega a la computadora portátil de Benito. El navegador web de Benito lee la respuesta HTTP del socket, extrae el código HTML correspondiente a la

página web del cuerpo de la respuesta HTTP y, finalmente, (*¡finalmente!*) muestra la página web.

El escenario descrito cubre una gran cantidad de aspectos de la comunicación por red. Si ha comprendido la mayor parte del ejemplo anterior o todo él, entonces habrá avanzado mucho desde que leyera por primera vez la Sección 1.1, donde decíamos que "buena parte de este libro trata de los protocolos de redes de computadoras", momento en el que posiblemente se estaba preguntando qué es un protocolo. Aunque el ejemplo anterior puede parecer bastante detallado, hemos omitido varios posibles protocolos adicionales (como por ejemplo, NAT ejecutándose en el router de pasarela de la facultad, el acceso inalámbrico a dicha red, los protocolos de seguridad para el acceso a red o para cifrar segmentos y datagramas, o los protocolos de gestión de red), así como diversas consideraciones adicionales (el almacenamiento en caché web, la jerarquía DNS) que podemos encontrar en la red Internet pública. Hablaremos de algunos de estos temas y otros en la segunda parte del libro.

Por último, cabe recalcar que el ejemplo anterior era una visión integrada y holística, aunque también refleja los componentes esenciales de muchos de los protocolos que hemos estudiado en esta primera parte del libro. El ejemplo pretendía centrarse más en el "cómo" que en el "por qué". Si desea una visión más amplia y reflexiva del diseño de los protocolos de red en general, consulte [Clark 1988, RFC 5218].

6.8 Resumen

En este capítulo hemos examinado la capa de enlace: sus servicios, los principios que subyacen a su funcionamiento y una serie de protocolos específicos importantes que utilizan esos principios a la hora de implementar servicios de la capa de enlace.

Hemos visto que el servicio básico de la capa de enlace consiste en mover un datagrama de la capa de red desde un nodo (host, switch, router, punto de acceso WiFi) hasta otro nodo adyacente. También hemos visto que todos los protocolos de la capa de enlace operan encapsulando un datagrama de la capa de red dentro de una trama de la capa de enlace antes de transmitir la trama a través del enlace existente hasta el nodo adyacente. Sin embargo, y yendo más allá de esta función común de entramado, hemos estudiado que los diferentes protocolos de la capa de enlace proporcionan servicios muy distintos de acceso al enlace, entrega y transmisión. Estas diferencias se deben en parte a la amplia variedad de tipos de enlace sobre los que deben operar los protocolos de la capa de enlace. Un simple enlace punto a punto tiene un único emisor y un único receptor que se comunican a través de único "cable". Los enlaces de acceso múltiple, por su parte, son compartidos por varios emisores y receptores; en consecuencia, el protocolo de la capa de enlace para un canal de acceso múltiple dispone de un protocolo (su protocolo de acceso múltiple) para la coordinación del acceso al enlace. En el caso de MPLS, el "enlace" que conecta dos nodos adyacentes (por ejemplo, dos routers IP que sean adyacentes en sentido IP, es decir, que ambos son routers IP del siguiente salto hacia un determinado destino) puede ser en realidad una *red* en sí misma. En un cierto sentido, la idea de una red considerada como un enlace no debería resultar demasiado extraña. Un enlace telefónico que conecta una computadora/módem doméstico con un módem/router remoto, por ejemplo, es en realidad una ruta que pasa a través de una sofisticada y compleja *red* telefónica.

Entre los principios que subyacen a la comunicación de la capa de enlace, hemos examinado las técnicas de detección y corrección de errores, los protocolos de acceso múltiple, el direccionamiento de la capa de enlace, la virtualización (redes VLAN), la construcción de redes LAN ampliadas y las redes para centros de datos. Gran parte de la atención hoy en día, en la capa de enlace, está puesta en estas redes conmutadas. En el caso de la detección y corrección de errores, hemos examinado cómo es posible añadir bits adicionales a la cabecera de una trama con el fin de detectar, y en algunos casos de corregir, errores de inversión de bit que puedan producirse al transmitir la trama a través

de un enlace. Hemos analizado los esquemas simples de paridad y de suma de comprobación, así como los códigos de redundancia cíclica más robustos. Después, hemos pasado a analizar el tema de los protocolos de acceso múltiple. Hemos identificado y estudiado tres enfoques generales para la coordinación del acceso a un canal de difusión: técnicas de particionamiento del canal (TDM, FDM), técnicas de acceso aleatorio (los protocolos ALOHA y CSMA) y técnicas de toma de turnos (sondeo y paso de testigo). Hemos estudiado la red de acceso por cable y determinado que emplea muchos de estos métodos de acceso. Hemos visto que una consecuencia de hacer que múltiples nodos compartan un único canal de difusión era la necesidad de proporcionar direcciones de nodo en la capa de enlace. Hemos observado que las direcciones de la capa de enlace son muy distintas de las direcciones de la capa de red y que, en el caso de Internet, se utiliza un protocolo especial (ARP, Protocolo de resolución de direcciones) para traducir entre estos dos tipos de direccionamiento, y hemos analizado el utilizadísimo protocolo Ethernet en detalle. Después hemos examinado cómo los nodos que comparten un canal de difusión forman una red LAN y cómo pueden conectarse entre sí varias redes LAN para formar otras redes LAN de mayor tamaño, todo ello *sin* la intervención del enrutamiento de la capa red para interconectar esos nodos locales. También hemos visto cómo se pueden crear múltiples redes LAN virtuales sobre una única infraestructura de LAN física.

Hemos terminado nuestro estudio de la capa de enlace centrándonos en cómo las redes MPLS proporcionan servicios de la capa de enlace cuando interconectan routers IP y proporcionando también una introducción a los diseños de red para los centros de datos masivos actuales. Hemos concluido el capítulo (y de hecho los primeros cinco capítulos) identificando los muchos protocolos necesarios para acceder a una simple página web. Habiendo cubierto la capa de enlace, *hemos concluido nuestro viaje descendente por la pila de protocolos*. Verdaderamente, la capa física se encuentra por debajo de la capa de enlace, pero quizá sea mejor dejar los detalles de la capa física para otro curso (por ejemplo, un curso sobre teoría de la comunicación, más que sobre redes de computadoras). No obstante, es cierto que hemos tocado varios aspectos de la capa física en este capítulo y en el Capítulo 1 (nuestra exposición acerca de los medios físicos de la Sección 1.2). Consideraremos de nuevo la capa física cuando estudiemos las características de los enlaces inalámbricos en el siguiente capítulo.

Aunque nuestro viaje por la pila de protocolos ya haya concluido, nuestro estudio de las redes de computadoras no ha terminado en modo alguno. En los siguientes tres capítulos nos ocuparemos de las redes inalámbricas, la seguridad de red y las redes multimedia. Estos tres temas no encajan de manera natural en ninguna de las capas que conocemos. De hecho, cada uno de ellos cruza muchas de esas distintas capas. Comprender estos temas (que se califican de temas avanzados en algunos libros de texto) requiere por tanto un sólido conocimiento de todas las capas de la pila de protocolos, un conocimiento que nuestro estudio de la capa de enlace de datos nos ha permitido terminar de adquirir.

Problemas y cuestiones de repaso

Capítulo 6 Cuestiones de repaso

SECCIONES 6.1–6.2

R1. Considere la analogía de los transportes de la Sección 6.1.1. Si el pasajero es análogo a un datagrama, ¿qué sería análogo a la trama de la capa de enlace?

R2. Si todos los enlaces de Internet tuvieran que proporcionar un servicio de entrega fiable, ¿sería el servicio de entrega fiable de TCP redundante? ¿Por qué?

R3. ¿Cuáles son algunos de los posibles servicios que puede ofrecer un protocolo de la capa de enlace a la capa de red? ¿Cuáles de estos servicios de la capa de enlace tienen servicios correspondientes en IP? ¿Y en TCP?