Disección del modelo OSI

Allá por 1977, la Organización Internacional de Normalización (ISO) desarrolló un subcomité para centrarse en la interoperabilidad de los sistemas de comunicaciones de múltiples proveedores. Lo que surgió de este subcomité fue la*Sistemas abiertos de interconexión*(OSI)*modelo de referencia*(comúnmente conocido como el*modelo OSI*o el*pila OSI*). Con este modelo, puede tomar casi cualquier tecnología de red y categorizar esa tecnología como residente en una o más de las siete capas del modelo.

Este capítulo define esas siete capas y proporciona ejemplos de lo que puede encontrar en cada capa. Finalmente, este capítulo contrasta el modelo OSI con otro modelo (el*pila TCP/IP*, también conocido como el*Departamento de Defensa*[DoD] *modelo*), que se centra en las comunicaciones del Protocolo de Internet (IP).

Temas de la Fundación

El propósito de los modelos de referencia

A lo largo de su carrera en redes, ya lo largo de este libro, encontrará varios protocolos y dispositivos que juegan un papel en su red. Sin embargo, para comprender mejor cómo encaja una tecnología en particular, es útil tener un punto de referencia común contra el cual se puedan comparar varias tecnologías de varios proveedores.

Una de las formas más comunes de categorizar la función de una tecnología de red es establecer en qué capa (o capas) del modelo OSI opera esa tecnología. En función de cómo esa tecnología realiza una determinada función en una determinada capa del modelo OSI, puede determinar mejor si un dispositivo podrá comunicarse con otro dispositivo, que podría o no estar utilizando una tecnología similar en esa capa de el modelo de referencia OSI.

Por ejemplo, cuando su computadora portátil se conecta a un servidor web en Internet, a su computadora portátil se le ha asignado una dirección IP. Del mismo modo, el servidor web al que se está comunicando tiene una dirección IP. Como verá en este capítulo, una dirección IP vive en la Capa 3 (la capa de red) del modelo OSI. Debido a que tanto su computadora portátil como el servidor web usan un protocolo común (es decir, IP) en la Capa 3, pueden comunicarse entre sí.

Personalmente, he estado en la industria de las redes informáticas desde 1989, y me han explicado el modelo OSI en muchas clases a las que he asistido y libros que he leído. De esto, he quitado una colección de metáforas para ayudar a describir el funcionamiento de las diferentes capas del modelo OSI. Algunas de las metáforas implican enviar una carta de un lugar a otro o colocar un mensaje en una serie de sobres. Sin embargo, mi forma favorita (y la más precisa) de describir el modelo OSI es simplemente pensar en él como algo análogo a una estantería, como la que se muestra en la Figura 2-1.

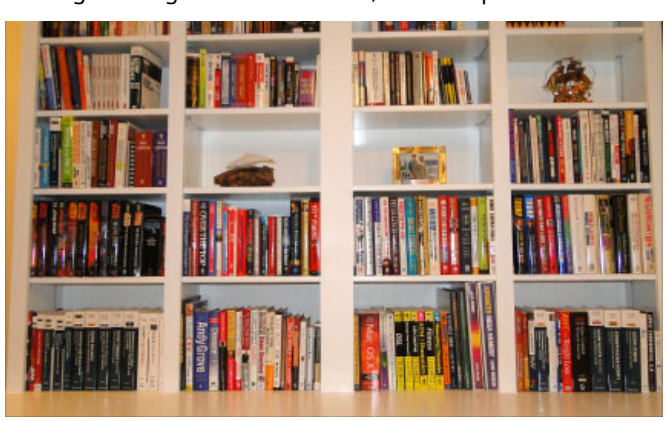

Figura 2-1 Una estantería es análoga al modelo OSI

Si miraras una estantería en mi casa, verías que organicé diferentes tipos de libros en diferentes estanterías. Un estante contiene mi colección de libros de Star Wars, otro estante contiene los libros que escribí para Cisco Press, otro estante contiene mis audiolibros, etc. Agrupé libros similares en un estante, tal como el modelo OSI agrupa protocolos y funciones similares en una capa.

Un escollo común al que se enfrentan mis estudiantes y lectores al estudiar el modelo OSI es tratar de encajar perfectamente todos los dispositivos y protocolos de su red en una de las siete capas del modelo OSI. Sin embargo, no todas las tecnologías encajan perfectamente en estas capas. De hecho, algunas redes pueden no tener ninguna tecnología operando en una o más de estas capas. Esto me recuerda mi afirmación favorita sobre el modelo OSI. Viene del libro de Rich Seifert.*El libro del interruptor*. En ese libro, Rich nos recuerda que el modelo OSI es un*referencia*modelo, no un *reverencia*modelo. Es decir, no existe una ley cósmica que establezca que todas las tecnologías deben conectarse limpiamente al modelo. Entonces, a medida que descubra las características de las capas del modelo OSI a lo largo de este capítulo, recuerde que estas capas son como estantes para organizar protocolos y funciones similares, no leyes inmutables.

El modelo OSI

Como se indicó anteriormente, el modelo OSI se compone de siete capas:

- **Capa 1:**La capa física
- **Capa 2:**La capa de enlace de datos
- **Capa 3:**La capa de red
- **Capa 4:**La capa de transporte
- **Capa 5:**La capa de sesión
- **Capa 6:**La capa de presentación
- **Capa 7:**La capa de aplicación

Gráficamente, estas capas generalmente se representan con la Capa 1 en la parte inferior de la pila, como se muestra en la Figura 2-2.

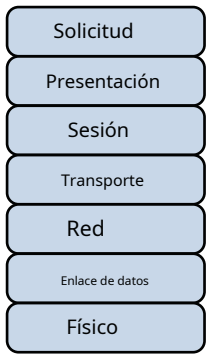

Figura 2-2"Pila" OSI

Hay varios mnemotécnicos disponibles para ayudar a memorizar estas capas en el orden correcto. Un acróstico de arriba hacia abajo (es decir, comenzando en la parte superior de la pila con la Capa 7 y bajando hasta la Capa 1) es*Todas las personas parecen necesitar procesamiento de datos*. Como un par de ejemplos, usando este acróstico, el*A*en*A*ll nos recuerda el*A*en*A*solicitud, y la*PAG*en *PAG*La gente nos recuerda la*PAG*en*PAG*resentimiento

En la capa física, las expresiones binarias (es decir, una serie de 1 y 0) representan datos. Una expresión binaria se compone de bits, donde un bit es un solo 1 o un solo 0. Sin embargo, en las capas superiores, los bits se agrupan en lo que se conoce como un*unidad de datos de protocolo*(PDU) o una*unidad de servicio de datos*.

El término*paquete*se usa de manera bastante genérica para referirse a estas PDU. Sin embargo, las PDU pueden tener un nombre adicional, según su capa OSI. La Figura 2-3 ilustra estos nombres de PDU. Una ayuda de memoria común para estas PDU es el acróstico*Algunas personas temen los cumpleaños*, donde el*S*en*S*ome nos recuerda a la*S*en*S*segmentos. El*PAG* en*PAG*La gente nos recuerda la*PAG*en*PAG*carteras, y el*F*en*F*el oído refleja el*F*en*F*rames. Finalmente, el*B*en*B*cumpleaños nos recuerda el*B*en*B*es.

Key Topic

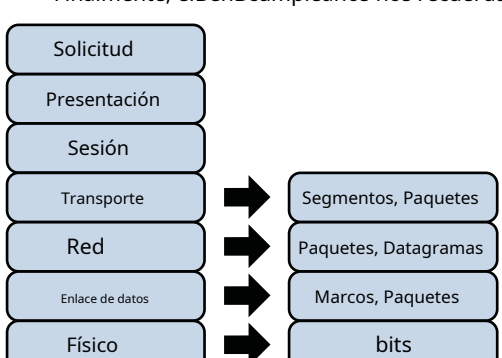

Figura 2-3 Nombres de PDU

Capa 1: La capa física

La capa física, como se muestra en la Figura 2-4, se ocupa de la transmisión de datos en la red.

Key Topic

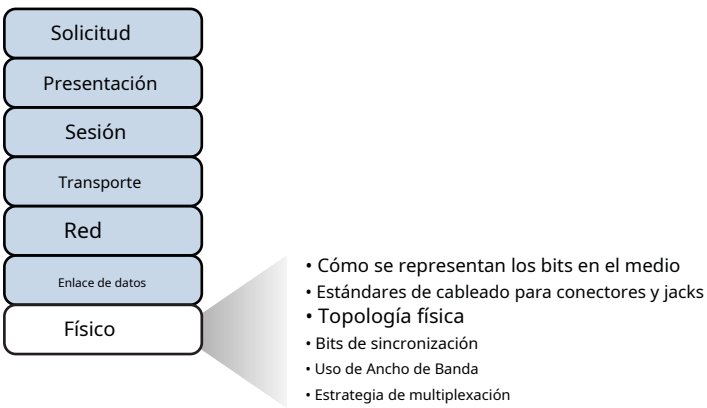

Figura 2-4 Capa 1: La capa física

Como algunos ejemplos, la capa física define

- **Cómo se representan los bits en el medio:**Los datos en una red informática son representado como una expresión binaria. El Capítulo 5, "Trabajar con direcciones IP", analiza el binario con mucho más detalle. El voltaje eléctrico (en el cableado de cobre) o la luz (transportada a través del cableado de fibra óptica) pueden representar estos 1 y 0.

  Por ejemplo, la presencia o ausencia de voltaje en un cable puede representar un 1 binario o un 0 binario, respectivamente, como se ilustra en la figura 2-5. De manera similar, la presencia o ausencia de luz en un cable de fibra óptica puede representar un 1 o un 0 en binario. Este tipo de enfoque se llama*modulación del estado actual*.

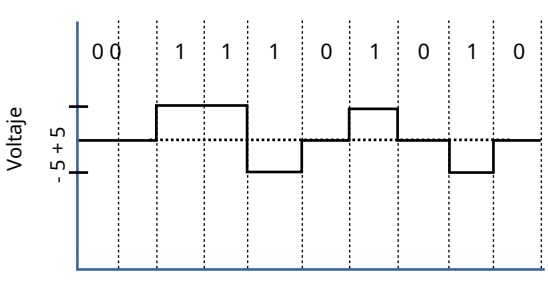

Figura 2-5 Modulación del estado actual

Un enfoque alternativo para representar datos binarios es*modulación de transición de estado*, como se muestra en la Figura 2-6, donde la transición entre voltajes o la presencia de luz indica un valor binario.

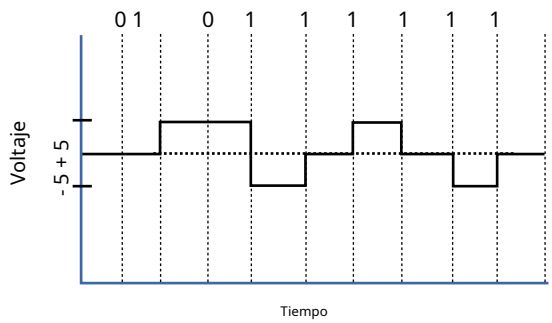

Figura 2-6 Modulación de Transición

NOTAOtros tipos de modulación con los que puede estar familiarizado de la radio incluyen la modulación de amplitud (AM) y la modulación de frecuencia (FM). AM utiliza una variación en la amplitud de una forma de onda (es decir, la intensidad de la señal) para representar la señal original. Sin embargo, FM usa una variación en la frecuencia para representar la señal original.

- **Estándares de cableado para conectores y jacks:**Varios estándares para la red. Los conectores se abordan en el Capítulo 3, "Identificación de los componentes de red". Sin embargo, como ejemplo, el estándar TIA/EIA-568-B describe cómo se debe cablear un conector RJ-45 para usar en una red Ethernet 100BASE-TX, como se muestra en la Figura 2-7.

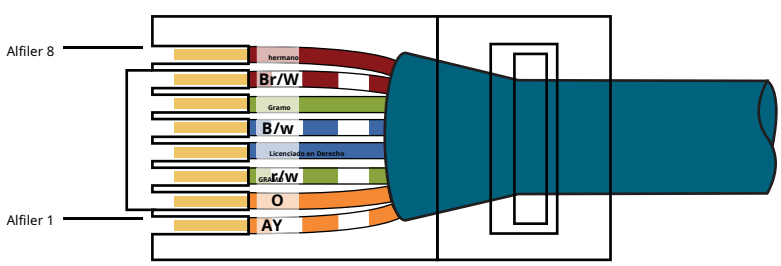

Figura 2-7 Estándar de cableado TIA/EIA-568-B para un conector RJ-45

- **Topología física:**Los dispositivos de capa 1 ven una red como una topología física (a diferencia de una topología lógica). Los ejemplos de una topología física incluyen topologías de bus, anillo y estrella, como se describe en el Capítulo 1, "Introducción a las redes informáticas".

- **Bits de sincronización:**Para que dos dispositivos en red se comuniquen con éxito en la capa física, deben acordar cuándo se detiene un bit y cuándo se inicia otro bit. Específicamente, lo que se necesita es un método para sincronizar los bits. Dos enfoques básicos para la sincronización de bits incluyen*asincrónico*y*sincrónico* sincronización:
  - **Asincrónico:**Con este enfoque, un emisor indica que está a punto de comenzar a transmitir enviando un bit de inicio al receptor. Cuando el receptor ve esto, inicia su propio reloj interno para medir los bits subsiguientes. Después de que el remitente transmite sus datos, envía un bit de parada para indicar que ha terminado su transmisión.
  - **Sincrónico:**Este enfoque sincroniza los relojes internos tanto del emisor como del receptor para garantizar que coincidan en el momento en que comienzan y terminan los bits. Un enfoque común para que se produzca esta sincronización es utilizar un reloj externo (por ejemplo, un reloj proporcionado por un proveedor de servicios), al que hacen referencia tanto el remitente como el receptor.
- **Uso de Ancho de Banda:**Los dos enfoques fundamentales para el uso del ancho de banda en una red son*banda ancha*y*banda base*:
  - **Banda ancha:**Las tecnologías de banda ancha dividen el ancho de banda disponible en un medio (por ejemplo, cableado de cobre o fibra óptica) en diferentes canales. A continuación, se transmiten diferentes flujos de comunicación a través de los distintos canales. Como ejemplo, considere*Multiplexación por división de frecuencia*(FDM) utilizado por un módem de cable. Específicamente, un módem por cable usa ciertos rangos de frecuencias en el cable que llega a su casa desde la compañía de cable local para transportar los datos entrantes, otro rango de frecuencias para los datos salientes y varios otros rangos de frecuencia para varias estaciones de TV.
  - **Banda base:**Las tecnologías de banda base, por el contrario, utilizan todas las frecuencias disponibles en un medio para transmitir datos. Ethernet es un ejemplo de una tecnología de red que utiliza banda base.
- **Estrategia de multiplexación:**La multiplexación permite que múltiples sesiones de comunicaciones compartan el mismo medio físico. La televisión por cable, como se mencionó anteriormente, le permite recibir múltiples canales a través de un solo medio físico (por ejemplo, un cable coaxial enchufado en la parte posterior de su televisor). Estos son algunos de los enfoques más comunes para la multiplexación:
  - **Multiplexación por división de tiempo (TDM):**TDM admite diferentes comunicaciones sesiones de comunicación (por ejemplo, diferentes conversaciones telefónicas en una red de telefonía) en un mismo soporte físico haciendo que las sesiones se realicen por turnos. Durante un breve período de tiempo, definido como un*franja horaria*, se enviarán los datos de la primera sesión, seguidos de los datos de las segundas sesiones. Esto continúa hasta que todas las sesiones hayan tenido su turno y el proceso se repite.

- **Multiplexación estadística por división de tiempo (StatTDM):**Una desventaja de TDM es que cada sesión de comunicación reciba su propio intervalo de tiempo, incluso si una de las sesiones no tiene ningún dato para transmitir en ese momento. Para hacer un uso más eficiente del ancho de banda disponible, StatTDM asigna dinámicamente intervalos de tiempo a las sesiones de comunicación según sea necesario.
- **Multiplexación por división de frecuencia (FDM):**FDM divide la frecuencia de un medio varían en canales, y diferentes sesiones de comunicación transmiten sus datos a través de diferentes canales. Como se describió anteriormente, este enfoque del uso del ancho de banda se denomina banda ancha.

Los ejemplos de dispositivos definidos por los estándares de la capa física incluyen concentradores, puntos de acceso inalámbrico y cableado de red.

NOTAUn concentrador puede interconectar PC en una LAN. Sin embargo, se considera que es un dispositivo de capa física, porque un concentrador toma los bits que ingresan en un puerto y los retransmite a todos los demás puertos del concentrador. En ningún momento el concentrador interroga ninguna información de direccionamiento en los datos.

Capa 2: La capa de enlace de datos

La capa de enlace de datos, como se muestra en la Figura 2-8, se ocupa de empaquetar datos en marcos y transmitir esos marcos en la red, realizar la detección/corrección de errores, identificar de manera única los dispositivos de red con una dirección y manejar el control de flujo. Estos procesos se conocen colectivamente como*control de enlace de datos*(contenido descargable).

Key Topic

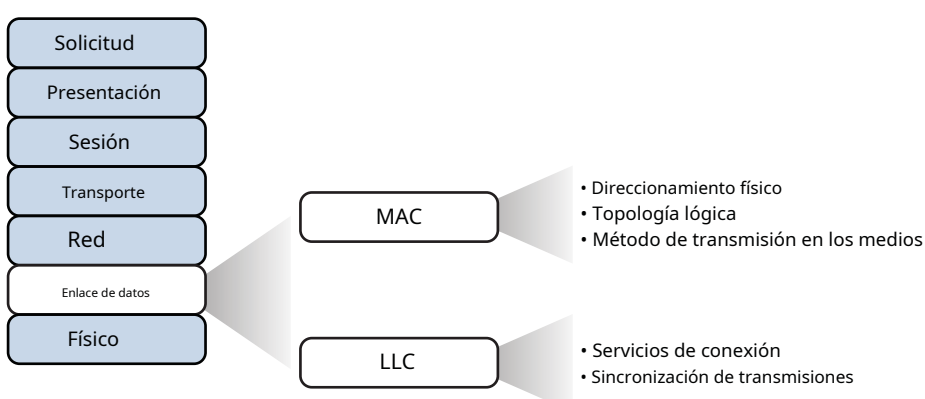

Figura 2-8 Capa 2: La capa de enlace de datos

De hecho, la capa de enlace de datos es única de las otras capas porque tiene dos subcapas propias: MAC y LLC.

El control de acceso a medios

Las características de la subcapa de control de acceso a medios (MAC) incluyen lo siguiente:

- **Direccionamiento físico:**Un ejemplo común de una dirección de capa 2 es una dirección MAC, que es una dirección de 48 bits asignada a la tarjeta de interfaz de red (NIC) de un dispositivo. La dirección se suele escribir en notación hexadecimal (por ejemplo, 58:55:ca:eb:27:83). Los primeros 24 bits de la dirección de 48 bits se conocen colectivamente como *Código de proveedor*. A los proveedores de equipos de red se les asigna uno o más códigos de proveedor únicos. Puede utilizar la lista de códigos de proveedor en http://standards.ieee.org/develop/regauth/oui/oui.txtpara determinar el fabricante de un dispositivo de red, en función de la primera mitad de la dirección MAC del dispositivo. Debido a que cada proveedor es responsable de usar valores únicos en los últimos 24 bits de una dirección MAC, y debido a que cada proveedor tiene un código de proveedor único, no hay dos direcciones MAC en el mundo que tengan el mismo valor.

- **Topología lógica:**Los dispositivos de capa 2 ven una red como una topología lógica. Los ejemplos de una topología lógica incluyen topologías de bus y anillo, como se describe en el Capítulo 1.

- **Método de transmisión en los medios:**Con varios dispositivos conectados a un red, debe haber alguna estrategia para determinar cuándo se permite que un dispositivo transmita en los medios. De lo contrario, varios dispositivos pueden transmitir al mismo tiempo e interferir con las transmisiones de los demás.

Control de enlace lógico

Las características de la subcapa de control de enlace lógico (LLC) incluyen lo siguiente:

- **Servicios de conexión:**Cuando un dispositivo en una red recibe un mensaje de otro dispositivo en la red, ese dispositivo receptor puede proporcionar comentarios al remitente en forma de un mensaje de reconocimiento. Las dos funciones principales proporcionadas por estos mensajes de reconocimiento son las siguientes:

  - **Control de flujo:**Limita la cantidad de datos que un remitente puede enviar a la vez; esto evita que el receptor se sienta abrumado con demasiada información.

  - **control de errores:**Permite que el destinatario de los datos informe al remitente si no se recibió el marco de datos esperado o si se recibió, pero está dañado. El destinatario determina si el marco de datos está corrupto matemáticamente

calcular una suma de comprobación de los datos recibidos. Si la suma de verificación calculada no coincide con la suma de verificación recibida con el marco de datos, el destinatario de los datos llega a la conclusión de que el marco de datos está dañado y luego puede notificar al remitente a través de un mensaje de reconocimiento.

- **Sincronización de transmisiones:**Los remitentes y los receptores de las tramas de datos deben coordinarse cuando se transmite y se debe recibir una trama de datos. Los tres métodos para realizar esta sincronización son los siguientes:

  - **Isócrono:**Con la transmisión isócrona, los dispositivos de red buscan un dispositivo común en la red como fuente de reloj, lo que crea intervalos de tiempo de duración fija. Los dispositivos de red pueden determinar cuánto espacio libre, si lo hay, está disponible dentro de un intervalo de tiempo e insertar datos en un intervalo de tiempo disponible. Un intervalo de tiempo puede acomodar más de un marco de datos. La transmisión isócrona no necesita proporcionar sincronización al comienzo de una cadena de datos (como ocurre con la transmisión síncrona) o para cada trama de datos (como ocurre con la transmisión asíncrona). Como resultado, la transmisión isócrona utiliza poca sobrecarga en comparación con los métodos de transmisión asíncrona o síncrona.

  - **Asincrónico:**Con la transmisión asíncrona, los dispositivos de red hacen referencia a sus propios relojes internos y los dispositivos de red no necesitan sincronizar sus relojes. En su lugar, el remitente coloca un bit de inicio al comienzo de cada trama de datos y un bit de parada al final de cada trama de datos. Estos bits de inicio y parada le dicen al receptor cuándo monitorear el medio para detectar la presencia de bits.

    También se puede agregar un bit adicional, llamado bit de paridad, al final de cada byte en un marco para detectar un error en el marco. Por ejemplo, si se utiliza la detección de errores de paridad par (en contraposición a la detección de errores de paridad impar), el bit de paridad (con un valor de 0 o 1) se agregaría al final de un byte, lo que provocaría el número total de 1 en el marco de datos sea un número par. Si el receptor de un byte está configurado para la detección de errores de paridad par y recibe un byte donde el número total de bits (incluido el bit de paridad) es par, el receptor puede concluir que el byte no se corrompió durante la transmisión.

NOTAEl uso de un bit de paridad para detectar errores puede no ser efectivo si un byte tiene más de un error (es decir, más de un bit cuyo valor original ha cambiado).

  - **Sincrónico:**Con la transmisión síncrona, dos dispositivos de red que desean comunicarse entre ellos deben acordar un método de sincronización

para indicar el comienzo y el final de las tramas de datos. Un enfoque para proporcionar este cronometraje es utilizar un canal de comunicaciones separado por el que se envía una señal de reloj. Otro enfoque se basa en combinaciones de bits específicas o caracteres de control para indicar el comienzo de una trama o un byte de datos.

Al igual que las transmisiones asíncronas, las transmisiones síncronas pueden realizar la detección de errores. Sin embargo, en lugar de usar bits de paridad, la comunicación síncrona ejecuta un algoritmo matemático en los datos para crear una *verificación de redundancia cíclica* (CDN). Si tanto el remitente como el receptor calculan el mismo valor de CRC para la misma porción de datos, el receptor puede concluir que los datos no se dañaron durante la transmisión.

Los ejemplos de dispositivos definidos por los estándares de la capa de enlace de datos incluyen conmutadores, puentes y tarjetas de interfaz de red (NIC).

NOTA Las NIC no están completamente definidas en la capa de enlace de datos, ya que se basan parcialmente en los estándares de la capa física, como el conector de red de una NIC.

Capa 3: La capa de red

La capa de red, como se muestra en la Figura 2-9, se ocupa principalmente del envío de datos en función de las direcciones lógicas.

Key Topic

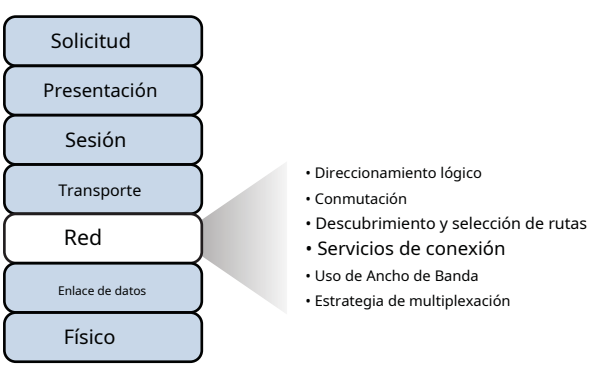

Figura 2-9 Capa 3: La capa de red

Aunque muchos administradores de red piensan inmediatamente en el enrutamiento y el direccionamiento IP cuando oyen hablar de la capa de red, esta capa es en realidad responsable de una variedad de tareas:

- **Direccionamiento lógico:**Aunque la capa de enlace de datos usa direcciones físicas para tomar decisiones de reenvío, la capa de red usa direccionamiento lógico para tomar decisiones de reenvío. Una variedad de protocolos enrutados (por ejemplo, AppleTalk e IPX) tienen sus propios esquemas de direccionamiento lógico, pero, con mucho, el protocolo enrutado más implementado es el Protocolo de Internet (IP). El direccionamiento IP se analiza en detalle en el Capítulo 5, “Trabajar con direcciones IP”.

- **Traspuesta:**El término*traspuesta*a menudo se asocia con tecnologías de capa 2; sin embargo, el concepto de conmutación también existe en la Capa 3. La conmutación, en esencia, es tomar decisiones sobre cómo se deben reenviar los datos. En la Capa 3, existen tres técnicas de conmutación comunes:

  - **Conmutación de paquetes:**Con la conmutación de paquetes, un flujo de datos se divide en paquetes. Cada paquete tiene un encabezado de capa 3, que incluye una dirección de capa 3 de origen y de destino. Otro término para la conmutación de paquetes es*enrutamiento*, que se analiza con más detalle en el Capítulo 6, “Enrutamiento del tráfico”.

  - **Cambio de circuito:**La conmutación de circuitos presenta dinámicamente un enlace de comunicación dedicado entre dos partes para que esas partes se comuniquen.

    Como un ejemplo simple de conmutación de circuitos, piense en hacer una llamada telefónica desde su hogar a una empresa. Suponiendo que tiene una línea fija tradicional que da servicio a su teléfono, el equipo de conmutación de la compañía telefónica interconecta el teléfono de su casa con el sistema telefónico de la empresa a la que llama. Esta interconexión (es decir,*circuito*) solo existe mientras dura la llamada telefónica.

  - **Conmutación de mensajes:**A diferencia de las tecnologías de conmutación de paquetes y conmutación de circuitos, la conmutación de mensajes no suele ser adecuada para aplicaciones en tiempo real, debido al retraso que conlleva. Específicamente, con la conmutación de mensajes, un flujo de datos se divide en mensajes. Cada mensaje está etiquetado con una dirección de destino y los mensajes viajan de un dispositivo de red a otro dispositivo de red en el camino a su destino. Debido a que estos dispositivos pueden almacenar brevemente los mensajes antes de reenviarlos, una red que usa conmutación de mensajes a veces se denomina red.*almacenamiento y reenvío*red. Metafóricamente, podría visualizar el cambio de mensajes como enrutar un mensaje de correo electrónico, donde el mensaje de correo electrónico podría almacenarse brevemente en un servidor de correo electrónico antes de reenviarse al destinatario.

- **Descubrimiento y selección de rutas:**Debido a que los dispositivos de Capa 3 toman decisiones de reenvío en función de las direcciones de red lógicas, es posible que un dispositivo de Capa 3 necesite saber cómo llegar a varias direcciones de red. Por ejemplo, un dispositivo común de capa 3 es un enrutador. Un enrutador puede mantener una tabla de enrutamiento que indique cómo reenviar un paquete en función de la dirección de red de destino del paquete.

La tabla de enrutamiento de un enrutador puede completarse a través de la configuración manual (es decir, ingresando rutas estáticas), a través de un protocolo de enrutamiento dinámico (por ejemplo, RIP, OSPF o EIGRP), o simplemente por el hecho de que el enrutador está conectado directamente a ciertas redes.

NOTALos protocolos de enrutamiento se analizan en el Capítulo 6.

- **Servicios de conexión:**Así como la capa de enlace de datos proporcionó servicios de conexión para el control de flujo y control de errores, también existen servicios de conexión en la capa de red. Los servicios de conexión en la capa de red pueden mejorar la confiabilidad de la comunicación, en caso de que la subcapa LLC del enlace de datos no esté realizando servicios de conexión.

  Las siguientes funciones son realizadas por los servicios de conexión en la capa de red:

  - **Control de flujo (también conocido como control de congestión):**Ayuda a evitar que un remitente de enviar datos más rápidamente de lo que el receptor es capaz de recibir los datos.

  - **Reordenación de paquetes:**Permite que los paquetes se coloquen en la secuencia adecuada a medida que se envían al receptor. Esto podría ser necesario, porque algunas redes admiten el equilibrio de carga, en el que se utilizan varios enlaces para enviar paquetes entre dos dispositivos. Debido a que se utilizan múltiples enlaces, los paquetes pueden llegar desordenados.

Los ejemplos de dispositivos que se encuentran en la capa de red incluyen enrutadores y conmutadores multicapa. El protocolo de Capa 3 más común que se usa en la actualidad, y el protocolo en el que se basa Internet, es IP.

Un protocolo de capa 3 menos popular es el de Novell.*Intercambio de paquetes entre redes*(IPX), que tiene su propio formato para el direccionamiento de Capa 3. Aunque IPX es un protocolo desarrollado por Novell, la mayoría de las redes Novell modernas utilizan IP como protocolo de capa 3.

NOTALos enrutadores y conmutadores multicapa se analizan en el Capítulo 3.

Capa 4: La capa de transporte

La capa de transporte, como se muestra en la Figura 2-10, actúa como una línea divisoria entre las capas superior e inferior del modelo OSI. Específicamente, los mensajes se toman de las capas superiores (capas 5 a 7) y se encapsulan en segmentos para su transmisión a las capas inferiores (capas 1 a 3). De manera similar, los flujos de datos provenientes de las capas inferiores se desencapsulan y se envían a la Capa 5 (la capa de sesión) o a alguna otra capa superior, según el protocolo.

Key Topic

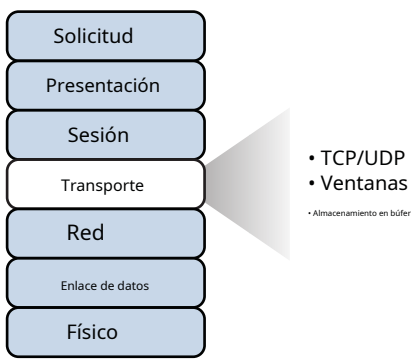

Figura 2-10 Capa 4: La capa de transporte

Dos protocolos de capa de transporte comunes incluyen *Protocolo de Control de Transmisión* (TCP) y *Protocolo de datagramas de usuario* (UDP):

- **Protocolo de control de transmisión (TCP):** Un protocolo de transporte orientado a la conexión. Los protocolos de transporte orientados a la conexión proporcionan un transporte confiable, en el sentido de que si se descarta un segmento, el remitente puede detectarlo y retransmitirlo. Específicamente, un receptor reconoce los segmentos que recibe. Según esos reconocimientos, un remitente puede determinar qué segmentos se recibieron con éxito y qué segmentos deben transmitirse nuevamente.
- **Protocolo de datagramas de usuario (UDP):** Un protocolo de transporte sin conexión. Los protocolos de transporte sin conexión proporcionan un transporte poco fiable, en el sentido de que si se descarta un segmento, el remitente no se da cuenta de la caída y no se produce ninguna retransmisión.

Un protocolo de Capa 4 menos popular es el de Novell. *Intercambio de paquetes secuenciados* (SPX). Similar a la pila de protocolos TCP/IP, la solución de Novell (mucho más popular a mediados de la década de 1990) fue la pila de protocolos IPX/SPX. Sin embargo, la mayoría de las redes Novell modernas se basan en TCP/IP en lugar de IPX/SPX.

NOTA Microsoft presentó su propia implementación de IPX/SPX de Novell, que se denominó *Enlace NW IPX/SPX*.

Así como la Capa 2 y la Capa 3 ofrecen servicios de control de flujo, también existen servicios de control de flujo en la Capa 4. Dos enfoques comunes de control de flujo en la Capa 4 son los siguientes:

- **Ventanas:**La comunicación TCP utiliza ventanas, en el sentido de que se envían uno o más segmentos a la vez, y un receptor puede acusar recibo de todos los segmentos en una ventana con un único acuse de recibo. En algunos casos, como se ilustra en la Figura 2-11, TCP usa una ventana deslizante, donde el tamaño de la ventana comienza con un segmento. Si hay un acuse de recibo exitoso de ese segmento (es decir, el receptor envía un acuse de recibo solicitando el siguiente segmento), el tamaño de la ventana se duplica a dos segmentos. Tras la recepción exitosa de esos dos segmentos, la siguiente ventana contiene cuatro segmentos. Este aumento exponencial en el tamaño de la ventana continúa hasta que el receptor no reconoce la recepción exitosa de todos los segmentos dentro de un cierto período de tiempo (conocido como tiempo de ida y vuelta [RTT], que a veces se denomina tiempo de transferencia real),

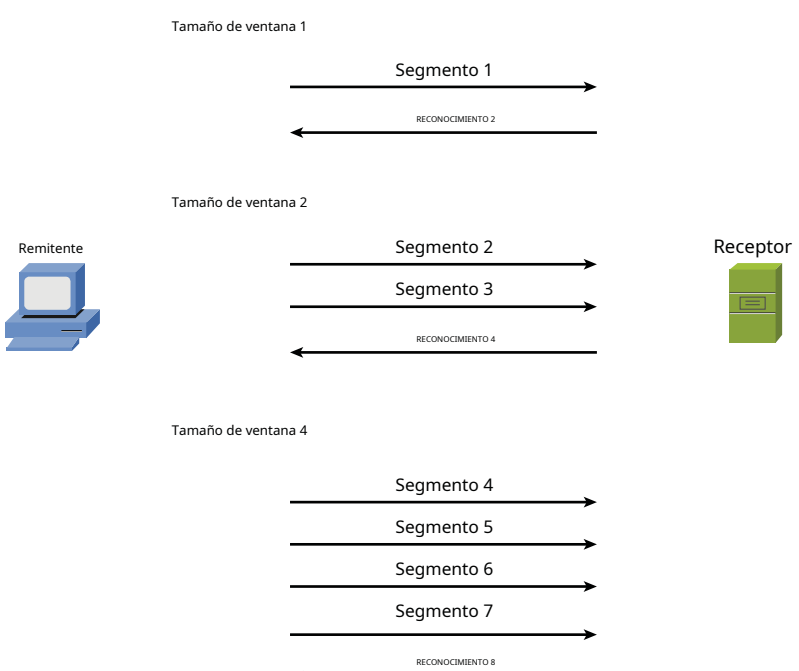

Figura 2-11 Ventana deslizante TCP

- **Almacenamiento en búfer:**Con el almacenamiento en búfer, un dispositivo (por ejemplo, un enrutador) asigna una parte de la memoria (a veces llamada búfer o cola) para almacenar segmentos si el ancho de banda no está disponible actualmente para transmitir esos segmentos. Sin embargo, una cola tiene una capacidad finita y puede desbordarse (es decir, perder segmentos) en caso de una congestión sostenida de la red.

Además de TCP y UDP, *Protocolo de mensajes de control de Internet* (ICMP) es otro protocolo de capa de transporte que probablemente encontrará. ICMP es utilizado por utilidades como ping y traceroute, que se analizan en el Capítulo 10, "Uso de utilidades de línea de comandos".

Capa 5: La capa de sesión

La capa de sesión, como se muestra en la Figura 2-12, es responsable de configurar, mantener y eliminar sesiones. Se puede pensar en una sesión como una conversación que debe tratarse por separado de otras sesiones para evitar la mezcla de datos de diferentes conversaciones.

Key Topic

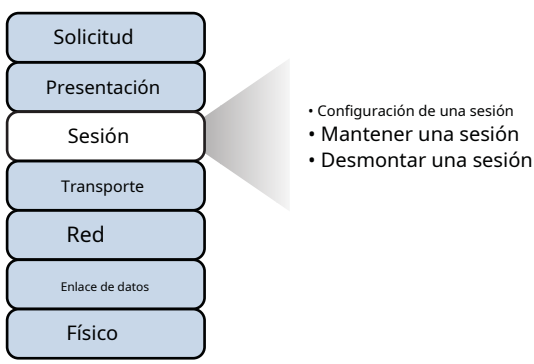

Figura 2-12 Capa 5: La capa de sesión

- **Configuración de una sesión:** Ejemplos de los procedimientos involucrados en la configuración de una sesión incluyen:
  - Comprobación de las credenciales de usuario (por ejemplo, nombre de usuario y contraseña)
  - Asignación de números a los flujos de comunicaciones de una sesión para identificar de forma única cada flujo
  - Servicios de negociación requeridos durante la sesión
  - Negociar qué dispositivo comienza a enviar datos
- **Mantenimiento de una sesión:** Ejemplos de los procedimientos involucrados en el mantenimiento de una sesión incluyen:
  - Transferencia de datos
  - Restablecimiento de una sesión desconectada
  - Acusar recibo de datos

- **Desmontar una sesión:**Una sesión se puede desconectar según el acuerdo mutuo de los dispositivos en la sesión. Alternativamente, una sesión puede interrumpirse porque una de las partes se desconecta (ya sea intencionalmente o debido a una condición de error). En caso de que una de las partes se desconecte, la otra parte puede detectar una pérdida de comunicación con esa parte y cortar su parte de la sesión.

H.323 es un ejemplo de un protocolo de capa de sesión, que puede ayudar a configurar, mantener y desconectar una conexión de voz o video. Tenga en cuenta, sin embargo, que no todas las aplicaciones de red se asignan directamente a las siete capas del modelo OSI. La capa de sesión es una de esas capas en las que podría no ser posible identificar qué protocolo en un escenario determinado está operando en esta capa.*Sistema básico de entrada/salida de red*(NetBIOS) es un ejemplo de un protocolo de capa de sesión.

NOTANetBIOS es un*Interfaz de programación de aplicaciones*(API) que se desarrolló a principios de la década de 1980 para permitir la comunicación de computadora a computadora en una LAN pequeña (específicamente,*Red de PC*, que era la tecnología LAN de IBM en ese momento). Más tarde, IBM necesitaba admitir la comunicación de computadora a computadora a través de redes Token Ring más grandes. Como resultado, IBM mejoró la escalabilidad y las características de NetBIOS con un emulador de NetBIOS llamado *Interfaz de usuario extendida de NetBIOS*(NetBEUI).

Capa 6: La capa de presentación

La capa de presentación, como se muestra en la Figura 2-13, es responsable del formato de los datos que se intercambian y de proteger esos datos con cifrado.

Key Topic

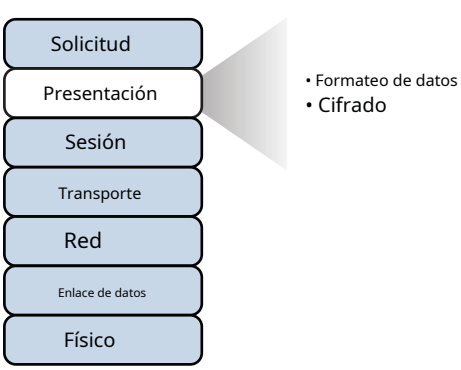

Figura 2-13 Capa 6: La capa de presentación

A continuación se describe con más detalle la función de formato y cifrado de datos:

- **Formateo de datos:**Como ejemplo de cómo la capa de presentación maneja el formato de datos, considere cómo se formatea el texto. Algunas aplicaciones pueden formatear texto utilizando el Código estándar estadounidense para el intercambio de información (ASCII), mientras que otras aplicaciones pueden formatear texto utilizando el Código de intercambio decimal codificado en binario extendido (EBCDIC). La capa de presentación es responsable de dar formato al texto (u otros tipos de datos, como archivos multimedia o gráficos) en un formato que permita la compatibilidad entre los dispositivos de comunicación.
- **Cifrado:**Imagine que está enviando información confidencial a través de una red (por ejemplo, su número de tarjeta de crédito o contraseña bancaria). Si un usuario malintencionado interceptara su transmisión, podría obtener esta información confidencial. Para agregar una capa de seguridad para dichas transmisiones, se puede usar el cifrado para cifrar (cifrar) los datos de tal manera que si los datos fueran interceptados, un tercero no podría descifrarlos (descifrarlos). Sin embargo, el destinatario previsto podría descifrar la transmisión.

El cifrado se analiza en detalle en el Capítulo 12, "Seguridad de una red".

Capa 7: La capa de aplicación

La capa de aplicación, como se muestra en la Figura 2-14, proporciona servicios de aplicación a una red. Un concepto importante, ya menudo mal entendido, es que las aplicaciones de usuario final (por ejemplo, Microsoft Word) no residen en la capa de aplicación. En cambio, la capa de aplicación admite los servicios utilizados por las aplicaciones de los usuarios finales. Por ejemplo, el correo electrónico es un servicio de capa de aplicación que reside en la capa de aplicación, mientras que Microsoft Outlook (un ejemplo de un cliente de correo electrónico) es una aplicación de usuario final que no reside en la capa de aplicación. Otra función de la capa de aplicación es anunciar los servicios disponibles.

Key Topic

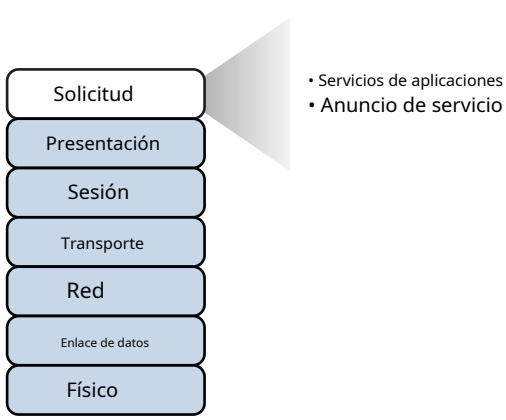

Figura 2-14 Capa 7: La capa de aplicación

A continuación se describen las funciones de la capa de aplicación con más detalle:

- **Servicios de aplicación:**Los ejemplos de los servicios de aplicación que residen en la capa de aplicación incluyen el uso compartido de archivos y el correo electrónico.
- **Anuncio de servicio:**Los servicios de algunas aplicaciones (por ejemplo, algunas impresoras en red) envían anuncios periódicamente, lo que hace que otros dispositivos de la red conozcan la disponibilidad de su servicio. Sin embargo, otros servicios se registran a sí mismos y a sus servicios en un directorio centralizado (por ejemplo, Microsoft Active Directory), que puede ser consultado por otros dispositivos de red que busquen dichos servicios.

Recuerde que aunque la capa de aplicación se numera como Capa 7, se considera que está en la parte superior de la pila OSI porque sus funciones están más cerca del usuario final.

La pila TCP/IP

La ISO desarrolló el modelo de referencia OSI para que fuera genérico, en términos de qué protocolos y tecnologías podrían ser categorizados por el modelo. Sin embargo, la gran mayoría del tráfico en Internet (y el tráfico en las redes corporativas) se basa en el conjunto de protocolos TCP/IP. Por lo tanto, un modelo más relevante para muchos diseñadores y administradores de redes es un modelo desarrollado por el Departamento de Defensa de los Estados Unidos (DoD). Este modelo es conocido como el*modelo del Departamento de Defensa*o el*pila TCP/IP*.

NOTAUn protocolo más antiguo, que es similar al conjunto de protocolos TCP/IP, que puede encontrar en la literatura sobre redes es*Protocolo de control de red*(NCP). NCP era un protocolo utilizado en*ARPANET*(el predecesor de Internet), y proporcionaba funciones similares (aunque no tan sólidas) a las proporcionadas por el conjunto de protocolos TCP/IP en Internet.

Capas de la pila TCP/IP

La pila TCP/IP tiene solo cuatro capas definidas, a diferencia de las siete capas del modelo OSI. La Figura 2-15 contrasta estos dos modelos para una comprensión ilustrativa.

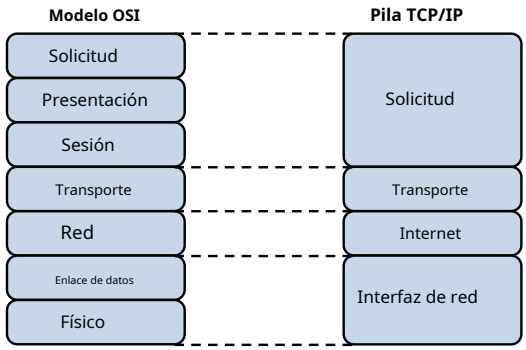

Figura 2-15 Pila TCP/IP

La pila TCP/IP se compone de las siguientes capas:

- **Interfaz de red:**La capa de interfaz de red de la pila TCP/IP abarca las tecnologías abordadas por las Capas 1 y 2 (capas de enlace de datos y física) del modelo OSI.

NOTACierta literatura se refiere a la capa de interfaz de red como la*capa de acceso a la red*.

- **Internet:**La capa de Internet de la pila TCP/IP se asigna a la Capa 3 (la capa de red) del modelo OSI. Aunque varios protocolos enrutados (por ejemplo, IP, IPX y AppleTalk) residen en la capa de red del modelo OSI, la capa de Internet de la pila TCP/IP se centra en IP como el protocolo que se enruta a través de una red. La Figura 2-16 muestra el formato de un paquete IP versión 4.

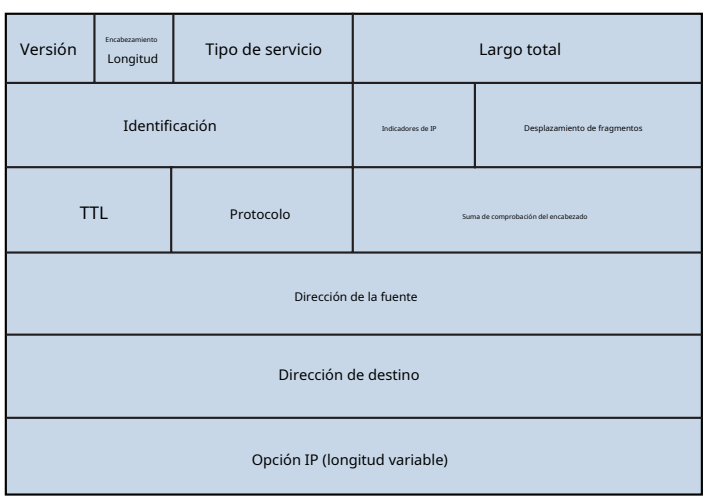

Figura 2-16 Formato de paquete IP versión 4

Observe que hay campos en el encabezado del paquete IP tanto para una dirección IP de origen como de destino. El campo Protocolo identifica el protocolo de la capa de transporte desde el que se envió el paquete o al que se debe enviar el paquete. También es de destacar el *Tiempo para vivir* (TTL) campo. El valor de este campo se reduce en uno cada vez que este paquete se enruta de una red IP a otra (es decir, pasa a través de un enrutador). Si el valor TTL alguna vez llega a 0, el paquete se descarta de la red. Este comportamiento ayuda a evitar bucles de enrutamiento.

- **Transporte:** La capa de transporte de la pila TCP/IP se asigna a la Capa 4 (la capa de transporte) del modelo OSI. Los dos protocolos principales que se encuentran en la capa de transporte de la pila TCP/IP son TCP y UDP.

  La Figura 2-17 detalla la estructura de un segmento TCP. Observe los campos para los puertos de origen y destino. Como se describe más adelante en este capítulo, estos puertos identifican a qué protocolo de capa superior se deben reenviar los datos o desde qué protocolo de capa superior se envían los datos.

Key Topic

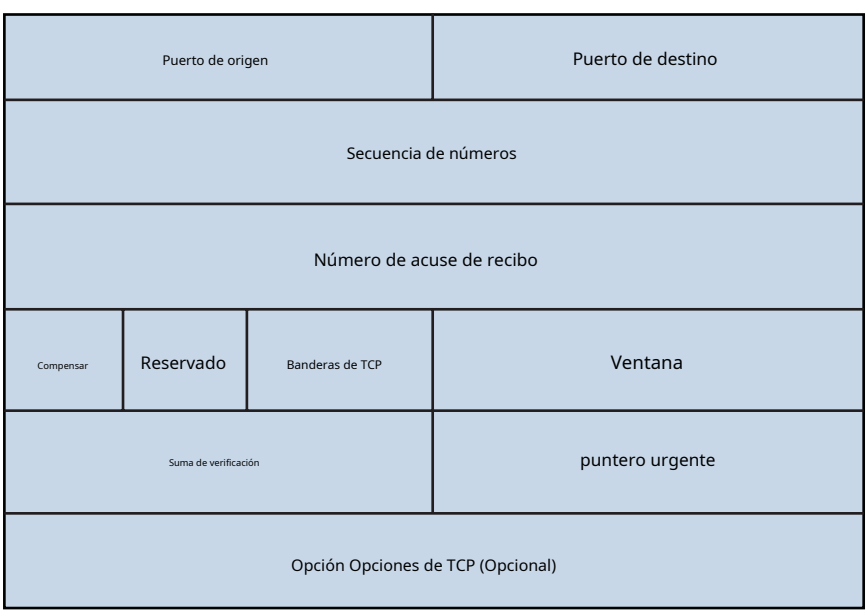

Figura 2-17 Formato de segmento TCP

Observe también el campo para el tamaño de la ventana. El valor de este campo determina cuántos bytes puede recibir un dispositivo antes de esperar un reconocimiento. Como se describió anteriormente, esta característica ofrece control de flujo.

El encabezado de un segmento TCP también contiene números de secuencia para segmentos. Con la numeración secuencial, si los segmentos llegan desordenados, el destinatario puede volver a colocarlos en el orden adecuado según estos números secuenciales.

El número de acuse de recibo en el encabezado indica el siguiente número de secuencia que el receptor espera recibir. Esta es una forma en que el receptor le permite al remitente saber que se han recibido todos los segmentos hasta ese punto inclusive.

La Figura 2-18 presenta la estructura de un segmento UDP. Debido a que UDP se considera un protocolo poco confiable y sin conexión, carece de la numeración de secuencia, el tamaño de la ventana y la numeración de reconocimiento presentes en el encabezado de un segmento TCP. Más bien, el encabezado del segmento UDP solo contiene números de puerto de origen y destino, una suma de verificación UDP (que es un campo opcional que se usa para detectar errores de transmisión) y la longitud del segmento (medida en bytes).

Key Topic

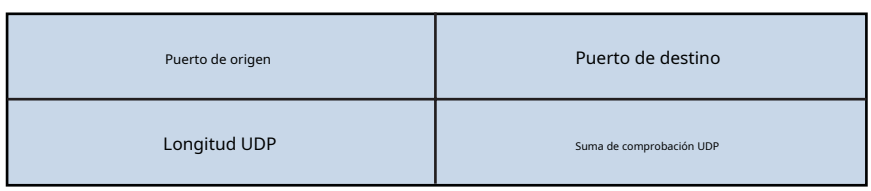

Figura 2-18 Formato de segmento UDP

Debido a que un encabezado UDP es mucho más pequeño que un encabezado TCP, UDP se convierte en un buen candidato para el protocolo de capa de transporte para aplicaciones que necesitan maximizar el ancho de banda y no requieren reconocimientos (por ejemplo, flujos de audio o video).

- **Solicitud:** La mayor diferencia entre la pila TCP/IP y el modelo OSI se encuentra en la capa de aplicación de la pila TCP/IP. Esta capa aborda los conceptos descritos por las capas 5, 6 y 7 (las capas de sesión, presentación y aplicación) del modelo OSI.

Con la complejidad reducida de un modelo de cuatro capas, como la pila TCP/IP, los diseñadores y administradores de redes pueden categorizar más fácilmente una tecnología de red dada en una capa específica. Por ejemplo, aunque H.323 se identificó anteriormente como un protocolo de capa de sesión dentro del modelo OSI, tendría que saber más sobre el comportamiento de H.323 para categorizarlo correctamente. Sin embargo, con la pila TCP/IP, podría determinar rápidamente que H.323 es un protocolo de nivel superior que se encapsula dentro de TCP y, por lo tanto, clasificar H.323 en la capa de aplicación de la pila TCP/IP.

Protocolos de aplicación comunes en la pila TCP/IP

Los protocolos de la capa de aplicación en la pila TCP/IP son identificables por *números de puerto*. Por ejemplo, cuando ingresa una dirección web en un navegador de Internet, se está comunicando (de manera predeterminada) con esa dirección web remota mediante el puerto TCP 80. Específicamente, el Protocolo de transferencia de hipertexto (HTTP), que es el protocolo comúnmente utilizado por los servidores web, usa un puerto TCP de 80. Por lo tanto, los datos que envía a ese servidor web remoto tienen un número de puerto de destino de 80. Luego, esos datos se encapsulan en un segmento TCP en la capa de transporte. Luego, ese segmento se encapsula en un paquete en la capa de Internet y se envía a la red utilizando una tecnología de capa de interfaz de red subyacente (por ejemplo, Ethernet).

Continuando con el ejemplo representado en la Figura 2-19, cuando envía tráfico a ese sitio web remoto, el paquete que envía a la red no solo necesita la dirección IP de destino (es decir, 172.16.1.2 en este ejemplo) del servidor web y el número de puerto para HTTP (es decir, 80), también necesita la dirección IP de su computadora (es decir, 10.1.1.1 en este ejemplo). Debido a que su computadora no actúa como un servidor web, su puerto no es 80. En su lugar, su computadora selecciona un número de puerto mayor que 1023. En este ejemplo, imaginemos que la PC cliente seleccionó un número de puerto de 1248.

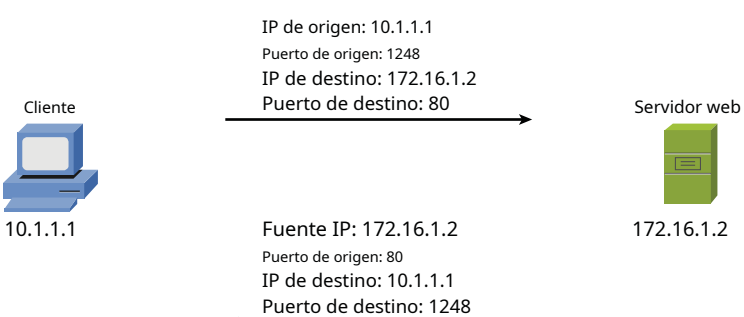

Figura 2-19 Ejemplo: números de puerto y direcciones IP

Tenga en cuenta que cuando el servidor web devuelve contenido a la PC, los datos se destinan a la dirección IP de la PC y al número de puerto asociado con esta sesión (1248 en este ejemplo). Con los números de puerto de origen y de destino, junto con las direcciones IP de origen y de destino, se hace posible la comunicación bidireccional.

NOTA Los puertos numerados 1023 e inferiores se denominan *bien conocido* puertos, mientras que los puertos numerados por encima de 1023 se denominan *puertos efímeros*. El valor máximo de un puerto es 65.535. Las asignaciones de números de puerto conocidos se pueden encontrar en www.iana.org/assignations/port-numbers.

La Tabla 2-1 sirve como referencia para algunos de los protocolos y aplicaciones de la capa de aplicación más populares que se encuentran en la pila TCP/IP. Algunos protocolos o aplicaciones (por ejemplo, DNS) pueden usar TCP o UDP para su transporte.

Key Topic

Tabla 2-1 Protocolos/aplicaciones de la capa de aplicación

Protocolo	Descripción	Puerto TCP	El puerto UDP
FTP	**Protocolo de transferencia de archivos**: transfiere archivos con un host remoto (normalmente requiere la autenticación de las credenciales de usuario)	20 y 21	
SSH	**Cubierta segura**: Conéctese de forma segura a un host remoto (normalmente a través de un emulador de terminal)	22	
SFTP	**FTP seguro**: proporciona un servicio de transferencia de archivos FTP a través de una conexión SSH	22	
SCP	**Copia segura**: proporciona un servicio seguro de transferencia de archivos a través de una conexión SSH y ofrece la información de fecha y hora original de un archivo, que no está disponible con FTP	22	
Telnet	**Telnet**: se utiliza para conectarse a un host remoto (normalmente a través de un emulador de terminal)	23	
SMTP	**Protocolo simple de transferencia de correo**: Se utiliza para enviar correo electrónico	25	
DNS	**sistema de nombres de dominio**: resuelve los nombres de dominio en las direcciones IP correspondientes	53	53
TFTP	**Protocolo trivial de transferencia de archivos**: transfiere archivos con un host remoto (no requiere autenticación de credenciales de usuario)		69
DHCP	**protocolo de configuración huésped dinámico**: asigna dinámicamente la información de la dirección IP (por ejemplo, la dirección IP, la máscara de subred, la dirección IP del servidor DNS y la dirección IP de la puerta de enlace predeterminada) a un dispositivo de red		67
HTTP	**Protocolo de Transferencia de Hipertexto**: Recupera contenido de un servidor web	80	
POP3	**Protocolo de oficina de correos versión 3**: recupera el correo electrónico de un servidor de correo electrónico	110	
NNTP	**Protocolo de transporte de noticias de red**: admite la publicación y lectura de artículos en los servidores de noticias de Usenet	119	
NTP	**Protocolo de tiempo de red**: Utilizado por un dispositivo de red para sincronizar su reloj con un servidor horario (servidor NTP)		123

Tabla 2-1 Protocolos/aplicaciones de la capa de aplicación

Protocolo	Descripción	Puerto TCP	El puerto UDP
SNTP	**Protocolo de tiempo de red simple**: Admite sincronización de tiempo entre dispositivos de red, similar al Protocolo de tiempo de red (NTP), aunque SNTP usa un algoritmo menos complejo en su cálculo y es un poco menos preciso que NTP		123
IMAP4	**Protocolo de acceso a mensajes de Internet versión 4**: recupera el correo electrónico de un servidor de correo electrónico	143	
LDAP	**Protocolo ligero de acceso a directorios**: proporciona servicios de directorio (por ejemplo, un directorio de usuarios que incluye información sobre el nombre de usuario, la contraseña, el correo electrónico y el número de teléfono) a los clientes de la red	389	
HTTPS	**Protocolo de transferencia de hipertexto seguro**: se utiliza para recuperar contenido de forma segura de un servidor web	443	
rsh	**Carcasa remota:**Permite ejecutar comandos en una computadora desde un usuario remoto	514	
RTSP	**Protocolo de transmisión en tiempo real:**Se comunica con un servidor de medios (por ejemplo, un servidor de video) y controla la reproducción de los archivos de medios del servidor	554	554
PDR	**Protocolo de escritorio remoto:**Un protocolo de Microsoft que permite a un usuario ver y controlar el escritorio de una computadora remota	3389	

Resumen

Los principales temas tratados en este capítulo son los siguientes:

- El modelo de referencia OSI de ISO consta de siete capas: física (Capa 1), enlace de datos (Capa 2), red (Capa 3), transporte (Capa 4), sesión (Capa 5), presentación (Capa 6) y aplicación (Capa 7). Se presentó el propósito de cada capa, junto con ejemplos de tecnologías que residen en las distintas capas.
- La pila TCP/IP se presentó como un modelo alternativo al modelo de referencia OSI. La pila TCP/IP consta de cuatro capas: interfaz de red, Internet, transporte y aplicación. Estas capas se compararon y contrastaron con las siete capas del modelo OSI.
- Este capítulo analizó cómo se usan los números de puerto para asociar datos en la capa de transporte con un protocolo de capa de aplicación apropiado. Se presentaron ejemplos de protocolos de capa de aplicación comunes en la suite TCP/IP, junto con sus números de puerto.

Tareas de preparación de exámenes

Revise todos los temas clave

Revise los temas más importantes del interior del capítulo, señalados con el ícono de Tema clave en el margen exterior de la página. La Tabla 2-2 enumera estos temas clave y los números de página donde se encuentra cada uno.

Tabla 2-2 Temas clave para el Capítulo 2

Elemento de tema clave	Descripción	Número de página
Lista	Capas del modelo OSI	31
Figura 2-3	Nombres de unidades de datos de protocolo	32
Figura 2-4	Capa 1: La capa física	33
Figura 2-8	Capa 2: La capa de enlace de datos	36
Figura 2-9	Capa 3: La capa de red	39
Figura 2-10	Capa 4: La capa de transporte	42
Figura 2-11	Ventana deslizante TCP	43
Figura 2-12	Capa 5: La capa de sesión	44
Figura 2-13	Capa 6: La capa de presentación	45
Figura 2-14	Capa 7: La capa de aplicación	46
Figura 2-15	pila TCP/IP	48
Figura 2-16	Formato de paquete IP versión 4	48
Figura 2-17	Formato de segmento TCP	49
Figura 2-18	Formato de segmento UDP	50
Figura 2-19	Ejemplo: números de puerto y direcciones IP	51
Tabla 2-1	Protocolos/aplicaciones de la capa de aplicación	52

Completar Tablas y Listas de Memoria

Imprima una copia del Apéndice C, “Tablas de memoria” (que se encuentra en el DVD), o al menos la sección de este capítulo, y complete las tablas y listas de memoria. El Apéndice D, “Clave de respuestas para tablas de memoria”, también en el DVD, incluye las tablas y listas completas para que pueda verificar su trabajo.

Definir términos clave

Defina los siguientes términos clave de este capítulo y verifique sus respuestas en el Glosario:

Modelo de referencia de interconexión de sistemas abiertos (OSI), unidad de datos de protocolo (PDU), modulación de estado actual, modulación de transición de estado, verificación de redundancia cíclica (CRC), capa física, capa de enlace de datos, capa de red, capa de transporte (modelo OSI), capa de sesión , capa de presentación, capa de aplicación (modelo OSI), capa de interfaz de red, capa de Internet, capa de transporte (pila TCP/IP), capa de aplicación (pila TCP/IP), multiplexación por división de tiempo (TDM), Protocolo de control de transmisión (TCP) , Protocolo de datagramas de usuario (UDP), pila TCP/IP

Preguntas de revisión

Las respuestas a estas preguntas de revisión aparecen en el Apéndice A, “Respuestas a las preguntas de revisión”.

1. ¿Qué capa del modelo de referencia OSI contiene las subcapas MAC y LLC?

a. Capa de red

b. Capa de transporte

C. Capa fisica

d. Capa de enlace de datos

2. ¿Qué enfoque del uso del ancho de banda consume todas las frecuencias disponibles en un medio para transmitir datos?

a. banda ancha

b. banda base

C. Multiplexación por división de tiempo

d. símplex

3. ¿En qué capa del modelo de referencia OSI se proporcionan ventanas?

a. Capa de enlace de datos

b. Capa de red

C. Capa de transporte

d. Capa fisica

4.¿En qué capa del modelo de referencia OSI residen las direcciones IP?

a.Capa de red

b.Capa de sesión

C.Capa de enlace de datos

d.Capa de transporte

5.¿Cuál de los siguientes es un protocolo de capa de transporte sin conexión?

a.IP

b.TCP

C.UDP

d.H.323

6.Identifique las cuatro capas de la pila TCP/IP. (Elija cuatro.)

a.Capa de sesión

b.Capa de transporte

C.capa de Internet

d.Capa de enlace de datos

mi. Capa de red

F.Capa de aplicación

gramo. Capa de control de red

7.¿Cuál es el rango de puertos TCP y UDP conocidos?

a.Por debajo de 2048

b.Por debajo de 1024

C.16,384–32,768

d.Por encima de 8192

8.¿Qué protocolo admite una conexión segura a un host remoto a través del software de emulación de terminal?

a.Telnet

b.SSH

C.FTP

d.SFTP

9.Identifique el número de puerto conocido para NTP.

a.53

b.69

C.123

d.143

10Identifique tres protocolos de correo electrónico. (Elige tres.)

a.SNMP

b.SMTP

C.POP3

d.IMAP4