Las aplicaciones y los servicios de red en un dispositivo final pueden comunicarse con las aplicaciones y los servicios que se ejecutan en otro dispositivo final. ¿Cómo se comunican estos datos a través de la red de manera eficaz?

Los protocolos de la capa de red del modelo OSI especifican el direccionamiento y los procesos que permiten empaquetar y transportar los datos de la capa de transporte. La encapsulación de la capa de red permite transmitir los datos a un destino dentro de la red (o de otra red) con una sobrecarga mínima.

En este capítulo, se analiza la función de la capa de red. Se analiza cómo divide las redes en grupos de hosts para administrar el flujo de paquetes de datos dentro de una red. También se examina la forma en que se facilita la comunicación entre redes. A esta comunicación entre redes se la denomina enrutamiento.

La capa de red, o la capa 3 de OSI, proporciona servicios que permiten que los dispositivos finales intercambien datos a través de la red. Para lograr este transporte de extremo a extremo, la capa de red utiliza cuatro procesos básicos:

* **Direccionamiento de dispositivos finales:** de la misma manera en que un teléfono tiene un número telefónico único, los dispositivos finales deben configurarse con una dirección IP única para su identificación en la red. Un dispositivo final con una dirección IP configurada se denomina “host”.
* **Encapsulación:** la capa de red recibe una unidad de datos del protocolo (PDU) de la capa de transporte. En un proceso denominado “encapsulación”, la capa de red agrega la información del encabezado IP, como la dirección IP de los hosts de origen (emisor) y de destino (receptor). Una vez que se agrega la información de encabezado a la PDU, esta se denomina “paquete”.
* **Enrutamiento:** la capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para que el paquete se transfiera a otras redes, lo debe procesar un router. La función del router es seleccionar las rutas para los paquetes y dirigirlos hacia el host de destino en un proceso conocido como “enrutamiento”. Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Cada ruta que toma el paquete para llegar al host de destino se denomina “salto”.
* **Desencapsulación:** cuando un paquete llega a la capa de red del host de destino, el host revisa el encabezado IP del paquete. Si la dirección IP de destino en el encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Este proceso de eliminación de encabezados de las capas inferiores se conoce como “desencapsulación”. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene como resultado se transfiere al servicio correspondiente en la capa de transporte.

A diferencia de la capa de transporte (capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de la capa de red especifican la estructura y el procesamiento de paquete que se utilizan para transportar los datos desde un host hasta otro. Operar sin tener en cuenta los datos transportados en cada paquete permite que la capa de red transporte paquetes para diversos tipos de comunicaciones entre varios hosts.

Existen varios protocolos de capa de red; sin embargo, solo los dos que se incluyen a continuación se implementan con frecuencia, como se muestra en la ilustración:

* Protocolo de Internet versión 4 (IPv4)
* Protocolo de Internet versión 6 (IPv6)

Otros protocolos de capa de red antiguos que no tienen un uso muy difundido incluyen los siguientes:

* Intercambio Novell de paquetes de internetwork (IPX)
* AppleTalk
* Servicio de red sin conexión (CLNS/DECNet)

El análisis de estos protocolos antiguos será mínimo.

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos TCP/IP.

IP se diseñó como protocolo con baja sobrecarga. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. De ser necesarias, otros protocolos en otras capas llevan a cabo estas funciones.

Las características básicas del protocolo IP son las siguientes:

* **Sin conexión:** no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
* **Máximo esfuerzo (no confiable):** la entrega de paquetes no está garantizada.
* **Independiente de los medios:** la operación es independiente del medio que transporta los datos.

La función de la capa de red es transportar paquetes entre los hosts colocando la menor carga posible en la red. La capa de red no se ocupa ni está al tanto del tipo de comunicación contenida dentro de un paquete. IP es un protocolo sin conexión, lo que significa que no se crea ninguna conexión dedicada de extremo a extremo antes de enviar los datos. Conceptualmente, la comunicación sin conexión es similar a enviar una carta a alguien sin notificar al destinatario con anticipación.

Como se muestra en la figura 1, el servicio postal utiliza la información en una carta para entregarla a un destinatario. La dirección en el sobre no proporciona datos que indiquen si el receptor está presente, si la carta llegará a destino o si el receptor puede leerla. De hecho, el servicio postal no está al tanto de la información contenida dentro del paquete que entrega y, por lo tanto, no puede proporcionar ningún mecanismo de corrección de errores.

Las comunicaciones de datos sin conexión funcionan según el mismo principio.

IP es un protocolo sin conexión y, por lo tanto, no requiere ningún intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de reenviar los paquetes. Además, tampoco requiere campos adicionales en el encabezado de la unidad de datos del protocolo (PDU) para mantener una conexión establecida. Este proceso reduce en gran medida la sobrecarga del IP. Sin embargo, sin una conexión de extremo a extremo preestablecida, los emisores no saben si los dispositivos de destino están presentes y en condiciones de funcionamiento cuando envían los paquetes, y tampoco saben si el destino recibe el paquete o si puede acceder al paquete y leerlo. En la figura 2, se muestra un ejemplo de comunicación sin conexión.

A menudo, el protocolo IP se describe como un protocolo no confiable o de máximo esfuerzo de entrega. Esto no significa que IP a veces funcione bien y a veces funcione mal, ni que sea un protocolo de comunicación de datos deficiente. “No confiable” significa simplemente que IP no tiene la capacidad de administrar paquetes no entregados o dañados ni de recuperar datos de estos. Esto se debe a que los paquetes IP se envían con información sobre la ubicación de entrega, pero no contienen información que se pueda procesar para informar al emisor si la entrega se realizó correctamente. No se incluyen datos de sincronización en el encabezado del paquete para realizar un seguimiento del orden de entrega de los paquetes. Con el protocolo IP, tampoco hay acuses de recibo de la entrega de los paquetes ni datos de control de errores que permitan realizar un seguimiento de si los paquetes se entregaron sin daños. Los paquetes pueden llegar al destino dañados o fuera de secuencia, o pueden no llegar en absoluto. De acuerdo con la información proporcionada en el encabezado IP, no hay capacidad de retransmisión de paquetes si se producen errores como estos.

Si los paquetes faltantes o que no funcionan generan problemas para la aplicación que usa los datos, los servicios de las capas superiores, como TCP, deben resolver estos problemas. Esto permite que el protocolo IP funcione de forma muy eficaz. Si se incluyera la sobrecarga de confiabilidad en IP, las comunicaciones que no requieren conexión o confiabilidad se cargarían con el consumo de ancho de banda y la demora producidos por esta sobrecarga. En la suite TCP/IP, la capa de transporte puede utilizar el protocolo TCP o UDP, según la necesidad de confiabilidad en la comunicación. Dejar que la capa de transporte decida sobre la confiabilidad hace que el protocolo IP se adapte y se acomode mejor a los distintos tipos de comunicación.

En la ilustración, se muestra un ejemplo de comunicaciones IP. Los protocolos orientados a la conexión, como TCP, requieren el intercambio de datos de control para establecer la conexión. Para mantener la información sobre la conexión, TCP también requiere campos adicionales en el encabezado de la PDU.

La capa de red tampoco tiene la carga de las características de los medios por los cuales se transportan los paquetes. IP funciona con independencia de los medios que transportan los datos en las capas inferiores del stack de protocolos. Como se muestra en la figura, cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como señales de radio.

Es responsabilidad de la capa de enlace de datos del modelo OSI tomar un paquete IP y prepararlo para transmitirlo a través del medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

Sin embargo, existe una característica importante de los medios que la capa de red tiene en cuenta: el tamaño máximo de la PDU que cada medio puede transportar. Esta característica se denomina “unidad máxima de transmisión” (MTU). Parte de la comunicación de control entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo para el paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. A continuación, la capa de red determina cuán grandes pueden ser los paquetes.

En algunos casos, un dispositivo intermediario, generalmente un router, debe dividir un paquete cuando lo reenvía de un medio a otro con una MTU más pequeña. A este proceso se lo llama fragmentación de paquetes o fragmentación.

El protocolo IP encapsula o empaqueta el segmento de la capa de transporte agregando un encabezado IP. Este encabezado se utiliza para entregar el paquete al host de destino. El encabezado IP permanece en su lugar desde el momento en que el paquete abandona la capa de red del host de origen hasta que llega a la capa de red del host de destino.

En la figura 1, se muestra el proceso de creación de la PDU de la capa de transporte. En la figura 2, se muestra el proceso subsiguiente de creación de la PDU de la capa de red.

El proceso de encapsulación de datos capa por capa permite el desarrollo y el escalamiento de los servicios de las diferentes capas sin afectar otras capas. Esto significa que el protocolo IPv4 o IPv6, o cualquier protocolo nuevo que se desarrolle en el futuro, pueden empaquetar fácilmente los segmentos de la capa de transporte.

Los routers pueden implementar estos diferentes protocolos de capa de red para operar al mismo tiempo en una red desde y hacia el mismo host o hosts diferentes. El enrutamiento que realizan estos dispositivos intermediarios solo tiene en cuenta el contenido del encabezado del paquete que encapsula el segmento. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada, no se modifica durante los procesos de la capa de red.

IPv4 se utiliza desde 1983, cuando se implementó en la Advanced Research Projects Agency Network (ARPANET, Red de la Agencia de Proyectos de Investigación Avanzada), que fue la precursora de Internet. Internet se basa en gran medida en IPv4, que continua siendo el protocolo de capa de red que más se utiliza.

Los paquetes IPV4 tienen dos partes:

* **Encabezado IP:** identifica las características del paquete.
* **Contenido:** contiene la información del segmento de capa 4 y los datos propiamente dichos.

Como se muestra en la ilustración, los encabezados de paquetes IPV4 constan de campos que contienen información importante sobre el paquete. Estos campos contienen números binarios que se examinan en el proceso de capa 3. Los valores binarios de cada campo identifican las distintas configuraciones del paquete IP.

Los campos importantes del encabezado de IPv4 incluyen los siguientes:

* **Versión:** contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv4, este campo siempre se establece en 0100.
* **Servicios diferenciados (DS):** anteriormente denominado “Tipo de servicio” (ToS), se trata de un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los primeros 6 bits identifican el valor del Punto de código de servicios diferenciados (DSCP), utilizado por un mecanismo de calidad de servicio (QoS). Los últimos 2 bits identifican el valor de Notificación explícita de congestión (ECN), que se puede utilizar para evitar que los paquetes se descarten durante momentos de congestión de la red.
* **Tiempo de vida (TTL):** contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. Se especifica en segundos, pero comúnmente se denomina “conteo de saltos”. El emisor del paquete establece el valor inicial de tiempo de vida (TTL), el que disminuye un punto por cada salto, es decir, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a cero, el router descarta el paquete y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a la dirección IP de origen. El comando **traceroute** utiliza este campo para identificar los routers utilizados entre el origen y el destino.
* **Protocolo:** este valor binario de 8 bits indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Los valores comunes incluyen ICMP (1), TCP (6) y UDP (17).
* **Dirección IP de origen:** contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete.
* **Dirección IP de destino:** contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

Los dos campos que más comúnmente se toman como referencia son las direcciones IP de origen y de destino. Estos campos identifican de dónde proviene el paquete y adónde va. Por lo general, estas direcciones no se modifican durante la transferencia desde el origen hasta el destino.

Los campos restantes se utilizan para identificar y validar el paquete, o para volver a ordenar un paquete fragmentado.

Los campos utilizados para identificar y validar el paquete incluyen los siguientes:

* **Longitud del encabezado de Internet (IHL):** contiene un valor binario de 4 bits que identifica la cantidad de palabras de 32 bits en el encabezado. El valor de IHL varía según los campos Opciones y Relleno. El valor mínimo para este campo es 5 (es decir, 5×32 = 160 bits = 20 bytes), y el valor máximo es 15 (es decir, 15×32 = 480 bits = 60 bytes).
* **Longitud total:** en ocasiones denominado “Longitud del paquete”, este campo de 16 bits define el tamaño total del paquete (fragmento), incluidos el encabezado y los datos, en bytes. La longitud mínima de paquete es de 20 bytes (encabezado de 20 bytes + datos de 0 bytes), y la máxima es de 65 535 bytes.
* **Checksum del encabezado:** este campo de 16 bits se utiliza para la verificación de errores del encabezado IP. El checksum del encabezado se vuelve a calcular y se compara con el valor en el campo checksum. Si los valores no coinciden, se descarta el paquete.

Es posible que un router deba fragmentar un paquete cuando lo reenvía de un medio a otro que tiene una MTU más pequeña. Cuando esto sucede, se produce una fragmentación, y el paquete IPV4 utiliza los siguientes campos para llevar a cabo un seguimiento de los fragmentos:

* **Identificación:** este campo de 16 bits identifica de forma exclusiva el fragmento de un paquete IP original.
* **Indicadores:** este campo de 3 bits identifica cómo se fragmenta el paquete. Se utiliza con los campos Desplazamiento de fragmentos e Identificación para ayudar a reconstruir el paquete original con el fragmento.
* **Desplazamiento de fragmentos:** este campo de 13 bits identifica el orden en que se debe colocar el fragmento del paquete en la reconstrucción del paquete original sin fragmentar.

**Nota:** los campos Opciones y Relleno se utilizan con poca frecuencia y exceden el ámbito de este capítulo.

A través de los años, IPv4 se actualizó para enfrentar nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 continúa teniendo tres problemas importantes:

* **Agotamiento de direcciones IP:** IPv4 dispone de una cantidad limitada de direcciones IP públicas exclusivas. Si bien existen aproximadamente 4000 millones de direcciones IPv4, la cantidad creciente de dispositivos nuevos con IP habilitado, las conexiones permanentes y el crecimiento potencial de las regiones menos desarrolladas aumentan la necesidad de más direcciones.
* **Expansión de la tabla de enrutamiento de Internet:** los routers utilizan tablas de enrutamiento para determinar cuál es el mejor camino. A medida que aumenta la cantidad de servidores (nodos) conectados a Internet, también lo hace la cantidad de rutas de la red. Estas rutas IPv4 consumen muchos recursos de memoria y del procesador en los routers de Internet.
* **Falta de conectividad de extremo a extremo:** la traducción de direcciones de red (NAT) es una tecnología de implementación frecuente en las redes IPv4. La tecnología NAT proporciona una forma de que varios dispositivos compartan una misma dirección IP pública. Sin embargo, dado que comparten la dirección IP pública, la dirección IP de un host de red interno se oculta. Esto puede resultar problemático para las tecnologías que requieren conectividad de extremo a extremo.

A principios de los años noventa, el Internet Engineering Task Force (IETF) comenzó a preocuparse por los problemas de IPv4 y empezó a buscar un reemplazo. Esta actividad condujo al desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y constituye una mejora eficaz con características que se adaptan mejor a las demandas actuales y previsibles de las redes.

Las mejoras que proporciona IPv6 incluyen lo siguiente:

* **Mayor espacio de direcciones:** las direcciones IPv6 se basan en un direccionamiento jerárquico de 128 bits, mientras que en IPv4 es de 32 bits. El número de direcciones IP disponibles aumenta drásticamente.
* **Mejora del manejo de los paquetes:** el encabezado de IPv6 se simplificó con menos campos. Esto mejora el manejo de paquetes por parte de los routers intermediarios y también proporciona compatibilidad para extensiones y opciones para aumentar la escalabilidad y la duración.
* **Eliminación de la necesidad de NAT:** con tal cantidad de direcciones IPv6 públicas, no se necesita traducción de direcciones de red (NAT). Los sitios de los clientes, ya sean las empresas más grandes o unidades domésticas, pueden obtener una dirección de red IPv6 pública. Esto evita algunos de los problemas de aplicaciones debidos a NAT que afectan a las aplicaciones que requieren conectividad de extremo a extremo.
* **Seguridad integrada:** IPv6 admite capacidades de autenticación y privacidad de forma nativa. Con IPv4, se debían implementar características adicionales para este fin.

El espacio de direcciones IPv4 de 32 bits proporciona aproximadamente 4 294 967 296 direcciones únicas. De estas, solo 3700 millones de direcciones se pueden asignar, porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

Como se muestra en la ilustración, el espacio de direcciones IP versión 6 proporciona 340 282 366 920 938 463 463 374 607 431 768 211 456, o 340 sextillones de direcciones, lo que equivale a aproximadamente todos los granos de arena de la Tierra.

Una de las principales mejoras de diseño de IPv6 con respecto a IPv4 es el encabezado de IPv6 simplificado.

El encabezado de IPv4 consta de 20 octetos (hasta 60 bytes si se utiliza el campo Opciones) y 12 campos de encabezado básicos, sin incluir los campos Opciones y Relleno.

El encabezado de IPv6 consta de 40 octetos (en gran medida, debido a la longitud de las direcciones IPv6 de origen y de destino) y 8 campos de encabezado (3 campos de encabezado IPv4 básicos y 5 campos de encabezado adicionales).

En la figura 1, se muestra la estructura del encabezado de IPv4. Como se muestra en la ilustración, en IPv6 algunos campos permanecen iguales, algunos campos del encabezado de IPv4 no se utilizan, y algunos campos tienen nombres y posiciones diferentes.

Además, se agregó un nuevo campo a IPv6 que no se utiliza en IPv4. El encabezado de IPv6 simplificado se muestra en la figura 2.

El encabezado de IPv6 simplificado ofrece varias ventajas respecto de IPv4:

* Mayor eficacia de enrutamiento para un buen rendimiento y una buena escalabilidad de velocidad de reenvío.
* Sin requisito de procesamiento de checksums.
* Mecanismos de encabezado de extensión simplificados y más eficaces (en comparación con el campo Opciones de IPv4).
* Un campo Identificador de flujo para procesamiento por flujo, sin necesidad de abrir el paquete interno de transporte para identificar los distintos flujos de tráfico.

Los campos de encabezado de paquetes IPv6 incluyen los siguientes:

* **Versión:** este campo contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre se establece en 0110.
* **Clase de tráfico:** este campo de 8 bits equivale al campo Servicios diferenciados (DS) de IPv4. También contiene un valor de Punto de código de servicios diferenciados (DSCP) de 6 bits utilizado para clasificar paquetes y un valor de Notificación explícita de congestión (ECN) de 2 bits utilizado para controlar la congestión del tráfico.
* **Identificador de flujo:** este campo de 20 bits proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen.
* **Longitud de contenido:** este campo de 16 bits equivale al campo Longitud total del encabezado de IPv4. Define el tamaño total del paquete (fragmento), incluidos el encabezado y las extensiones optativas.
* **Siguiente encabezado:** este campo de 8 bits equivale al campo Protocolo de IPv4. Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Este campo también se usa si se agregan encabezados de extensión optativos al paquete IPv6.
* **Límite de saltos:** este campo de 8 bits reemplaza al campo TTL de IPv4. Cuando cada router reenvía un paquete, este valor disminuye en un punto. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino.
* **Dirección de origen:** este campo de 128 bits identifica la dirección IPv6 del host emisor.
* **Dirección de destino:** este campo de 128 bits identifica la dirección IPv6 del host receptor.

Los paquetes IPv6 también pueden contener encabezados de extensión (EH), que proporcionan información optativa de la capa de red. Los encabezados de extensión son optativos y se colocan entre el encabezado de IPv6 y el contenido. Los EH se utilizan para realizar la fragmentación, aportar seguridad, admitir la movilidad, y más.

Al ver las capturas de IPv6 de Wireshark, observe que el encabezado de IPv6 tiene muchos menos campos que un encabezado de IPv4. Esto hace que el encabezado de IPv6 sea más fácil y más rápido de procesar para el router.

La dirección IPv6 propiamente dicha es muy distinta. Debido al mayor tamaño de las direcciones IPv6, de 128 bits, se utiliza el sistema de numeración hexadecimal para simplificar la representación de las direcciones. En las direcciones IPv6, se utilizan dos puntos para separar las entradas en una serie de bloques hexadecimales de 16 bits.

En la captura de muestra de la figura 1, se muestra el contenido del paquete número 46. El paquete contiene el mensaje inicial del protocolo TCP de enlace de tres vías entre un host IPv6 y un servidor IPv6. Observe los valores en la sección expandida del encabezado de IPv6. Observe, además, que se trata de un paquete TCP y que no contiene más información más allá de la sección TCP.

En la captura de muestra de la figura 2, se muestra el contenido del paquete número 49. El paquete contiene el mensaje GET inicial del protocolo de transferencia de hipertexto (HTTP) para el servidor. Observe que se trata de un paquete HTTP y que ahora contiene información más allá de la sección TCP.

Por último, en la captura de muestra de la figura 3, se muestra el contenido del paquete número 1. El paquete de muestra es un mensaje ICMPv6 de solicitud de vecino. Observe que no hay información de TCP o UDP.

Otra función de la capa de red es dirigir los paquetes entre los hosts. Un host puede enviar un paquete:

* **A sí mismo:** en este caso, se utiliza una dirección IP especial, 127.0.0.1, que se denomina “interfaz loopback”. Esta dirección de loopback se asigna automáticamente a un host cuando se ejecuta TCP/IP. La capacidad de un host de enviarse un paquete a sí mismo mediante la funcionalidad de la red resulta útil para realizar pruebas. Cualquier dirección IP dentro de la red 127.0.0.0/8 se refiere al host local.
* **A un host local:** un host en la misma red que el host emisor. Los hosts comparten la misma dirección de red.
* **A un host remoto:** un host en una red remota. Los hosts no comparten la dirección de red.

Para determinar si un paquete está destinado a un host local o un host remoto, se compara la combinación de la dirección IP y la máscara de subred del dispositivo de origen (o emisor) con la dirección IP y la máscara de subred del dispositivo de destino.

En una red doméstica o comercial, es posible que tenga varios dispositivos conectados por cable o inalámbricos interconectados mediante un dispositivo intermediario, como un switch LAN o un punto de acceso inalámbrico (WAP). Este dispositivo intermediario proporciona interconexiones entre los hosts locales en la red local. Los hosts locales pueden comunicarse y compartir información sin necesidad de ningún dispositivo adicional. Si un host envía un paquete a un dispositivo que está configurado con la misma red IP que el dispositivo host, el paquete tan solo se reenvía por la interfaz del host, a través del dispositivo intermediario, directamente al dispositivo de destino.

Por supuesto, en la mayoría de las situaciones deseamos que los dispositivos puedan conectarse más allá del segmento de red local: a otros hogares, a otras empresas y a Internet. Los dispositivos que están más allá del segmento de red local se conocen como “hosts remotos”. Cuando un dispositivo de origen envía un paquete a un dispositivo de destino remoto, se necesita la ayuda de routers y el enrutamiento. El enrutamiento es el proceso mediante el cual se identifica el mejor camino hacia un destino. El router conectado al segmento de red local se denomina **gateway predeterminado**.

El gateway predeterminado es el dispositivo que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. En un entorno doméstico o de pequeña empresa, el gateway predeterminado se suele utilizar para conectar la red local a Internet.

Si el host envía un paquete a un dispositivo en otra red IP, debe reenviar el paquete al gateway predeterminado a través del dispositivo intermediario. Esto se debe a que los dispositivos host no mantienen la información de enrutamiento más allá de la red local para llegar a destinos remotos; esto lo hace el gateway predeterminado. El gateway predeterminado, que en general es un router, mantiene una tabla de enrutamiento. Una tabla de enrutamiento es un archivo de datos que se encuentra en la RAM y que se utiliza para almacenar información de la ruta sobre la red conectada directamente, así como las entradas de redes remotas descubiertas por el dispositivo. El router utiliza la información en la tabla de enrutamiento para determinar cuál es el mejor camino para llegar a esos destinos.

¿Cómo decide un host si debe o no debe reenviar paquetes al gateway predeterminado? Los hosts deben poseer una tabla de enrutamiento local propia para asegurarse de que los paquetes de la capa de red se dirijan a la red de destino correcta. La tabla local del host generalmente contiene lo siguiente:

* **Conexión directa:** se trata de una ruta a la interfaz loopback (127.0.0.1).
* **Ruta de red local:** la red a la cual está conectado el host se completa automáticamente en la tabla de enrutamiento del host.
* **Ruta predeterminada local:** la ruta predeterminada representa la ruta que los paquetes deben seguir para llegar a todas las direcciones de redes remotas. La ruta predeterminada se crea cuando hay una dirección de gateway predeterminado en el host. La dirección de gateway predeterminado es la dirección IP de la interfaz de red del router que está conectada a la red local. La dirección de gateway predeterminado se puede configurar en el host de forma manual o se puede descubrir de manera dinámica.

Es importante observar que la ruta predeterminada y, por lo tanto, el gateway predeterminado, se utilizan solo cuando un host debe reenviar paquetes a una red remota. No se requieren, ni es necesario configurarlos, si solo se envían paquetes a dispositivos en la red local.

Por ejemplo, considere una impresora o un escáner de red. Si la impresora de red tiene una dirección IP y una máscara de subred configuradas, los hosts locales pueden enviar documentos a la impresora para imprimirlos. Además, la impresora puede reenviar los documentos escaneados a cualquier host local. En tanto la impresora se use solo de forma local, no se requiere una dirección de gateway predeterminado. De hecho, al no configurar una dirección de gateway predeterminado en la impresora, se deniega de manera eficaz el acceso a Internet, lo que puede ser una acertada decisión de seguridad. Sin acceso a Internet, no existe riesgo de seguridad. Si bien algunos dispositivos, como las impresoras, pueden ofrecer la capacidad de realizar actualizaciones automáticas por Internet, por lo general es más fácil y más seguro obtener esas mismas actualizaciones a través de cargarlas en forma local desde un host local protegido, como una PC.

En un host de Windows, se pueden utilizar los comandos **route print** o **netstat -r** para ver la tabla de enrutamiento del host. Los dos comandos provocan al mismo resultado. Al principio, los resultados pueden parecer abrumadores, pero son bastante fáciles de entender.

Al introducir el comando **netstat -r** o su equivalente, **route print**, se ven tres secciones relacionadas con las conexiones de red TCP/IP actuales:

* **Lista de interfaces:** enumera las direcciones de control de acceso al medio (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
* **Tabla de rutas IPv4:** enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.
* **Tabla de rutas IPv6:** enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.

**Nota:** los resultados del comando varían según cómo esté configurado el host y los tipos de interfaz que tenga.

En la ilustración, se muestra la sección de la tabla de rutas IPv4 de los resultados. Observe que los resultados se dividen en cinco columnas que identifican lo siguiente:

* **Destino de red:** enumera las redes que se pueden alcanzar.
* **Máscara de red:** incluye una máscara de subred que le indica al host cómo determinar las porciones de red y de host de la dirección IP.
* **Puerta de acceso:** indica la dirección que utiliza la PC local para llegar a un destino en una red remota. Si un destino es directamente accesible, se muestra como “En enlace” en esta columna.
* **Interfaz:** indica la dirección de la interfaz física utilizada para enviar el paquete al gateway que se emplea para llegar al destino de red.
* **Métrica:** indica el costo de cada ruta y se utiliza para determinar la mejor ruta a un destino.

Para ayudar a simplificar el resultado, las redes de destino se pueden agrupar en cinco secciones, identificadas por las áreas resaltadas en la ilustración:

**0.0.0.0**

La ruta predeterminada local. Todos los paquetes con destinos que no coincidan con otras direcciones especificadas en la tabla de enrutamiento se reenvían al gateway. Por lo tanto, todas las rutas de destino que no coincidan se envían al gateway con la dirección IP 192.168.10.1 (R1) que sale de la interfaz con la dirección IP 192.168.10.10. Observe que la dirección de destino final especificada en el paquete no cambia; en realidad, el host simplemente sabe que debe reenviar el paquete al gateway para su procesamiento posterior.

**127.0.0.0 – 127.255.255.255**

Todas estas direcciones de loopback se relacionan con la conexión directa y proporcionan servicios al host local.

**192.168.10.0 - 192.168.10.255**

Todas estas direcciones se relacionan con el host y la red local. Todos los paquetes con direcciones de destino dentro de esta categoría salen por la interfaz 192.168.10.10.

* **192.168.10.0:** dirección de la ruta de red local que representa todas las PC en la red 192.168.10.x.
* **192.168.10.10:** dirección del host local.
* **192.168.10.255:** dirección de broadcast de la red, que envía mensajes a todos los hosts en la ruta de red local.

**224.0.0.0**

Direcciones multicast de clase D especiales reservadas para usar mediante la interfaz loopback (127.0.0.1) o la dirección IP del host (192.168.10.10).

**255.255.255.255**

Las últimas dos direcciones representan los valores de direcciones IP de broadcast limitado para usar mediante la interfaz loopback (127.0.0.1) o la dirección IP del host (192.168.10.10). Estas direcciones se pueden utilizar para buscar un servidor de DHCP antes de que se determine la dirección IP local.

Por ejemplo, si la PC1 desea enviarle un paquete a 192.168.10.20, debería hacer lo siguiente:

1. Consultar la tabla de rutas IPv4.

2. Encontrar la correspondencia entre la dirección IP de destino y la entrada de destino de red 192.168.10.0 para determinar que el host está en la misma red (En enlace).

3. Luego, la PC1 enviaría el paquete hacia el destino final mediante su interfaz local (192.168.10.10).

En la figura 1, se destaca la ruta en que se encontró coincidencia.

Si la PC1 desea enviar un paquete a un host remoto ubicado en 10.10.10.10, debería hacer lo siguiente:

1. Consultar la tabla de rutas IPv4.

2. Determinar que no hay una coincidencia exacta para la dirección IP de destino.

3. Elegir la ruta predeterminada local (0.0.0.0) para descubrir que debe reenviar el paquete a la dirección de gateway 192.168.10.1.

4. Luego, la PC1 reenvía el paquete al gateway para usar su interfaz local (192.168.10.10). A continuación, el dispositivo de gateway determina la siguiente ruta para que el paquete llegue a la dirección de destino final 10.10.10.10.

En la figura 2, se destaca la ruta en que se encontró coincidencia.

El resultado de la tabla de rutas IPv6 difiere en los encabezados de las columnas y el formato, debido a que las direcciones IPv6 son más largas.

En la sección de la tabla de rutas IPv6, se muestran cuatro columnas que identifican lo siguiente:

* **Si:** incluye los números de interfaz de la sección Lista de interfaces del comando **netstat –r**. Los números de interfaz corresponden a las interfaces con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
* **Métrica:** indica el costo de cada ruta a un destino. Los números más bajos indican las rutas preferidas.
* **Destino de red:** enumera las redes que se pueden alcanzar.
* **Puerta de acceso:** indica la dirección que utiliza el host local para reenviar paquetes a un destino de red remoto. “En enlace” indica que el host actualmente está conectado.

Por ejemplo, en la ilustración, se muestra la sección de rutas IPv6 generada mediante el comando **netstat – r** para mostrar los siguientes destinos de red:

* **::/0:** equivalente en IPv6 a la ruta predeterminada local.
* **::1/128:** equivale a la dirección de loopback IPv4 y proporciona servicios al host local.
* **2001::/32:** prefijo de red unicast global.
* **2001:0:9d38:953c:2c30:3071:e718:a926/128:** dirección IPv6 unicast global de la PC local.
* **fe80::/64:** dirección de la ruta de red de enlace local, que representa todas las PC en la red IPv6 de enlace local.
* **fe80::2c30:3071:e718:a926/128:** dirección IPv6 link-local de la PC local.
* **ff00::/8:** direcciones multicast de clase D especiales y reservadas que equivalen a las direcciones IPv4 224.x.x.x.

**Nota:** en general, las interfaces en IPv6 tienen dos direcciones IPv6: una dirección link-local y una dirección unicast global. Asimismo, observe que no hay direcciones de broadcast en IPv6. Las direcciones IPv6 se analizan en mayor detalle en el capítulo siguiente.

Cuando un host envía un paquete a otro host, utiliza la tabla de enrutamiento para determinar adónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la dirección de un dispositivo de gateway.

¿Qué sucede cuando un paquete llega a una interfaz del router? El router examina la tabla de enrutamiento para determinar adónde reenviar los paquetes.

La tabla de enrutamiento de un router almacena información sobre lo siguiente:

* **Rutas conectadas directamente:** estas rutas provienen de las interfaces del router activas. Los routers agregan una ruta conectada directamente cuando se configura una interfaz con una dirección IP y se activa. Cada una de las interfaces del router se conecta a un segmento de red diferente. En la tabla de enrutamiento, los routers mantienen información acerca de los segmentos de red a los que están conectados.
* **Rutas remotas:** estas rutas provienen de las redes remotas conectadas a otros routers. El administrador de red puede configurar las rutas a estas redes de forma manual en el router local, o estas se pueden configurar de forma dinámica habilitando al router local para que intercambie información de enrutamiento con otros routers mediante protocolos de enrutamiento dinámico.

En la ilustración, se identifican las redes conectadas directamente y las redes remotas del router R1.

En una tabla de enrutamiento de host, solo se incluye información sobre las redes conectadas directamente. Un host requiere un gateway predeterminado para enviar paquetes a un destino remoto. La tabla de enrutamiento de un router contiene información similar, pero también puede identificar redes remotas específicas.

La tabla de enrutamiento de un router es similar a la tabla de enrutamiento de un host. Ambas identifican lo siguiente:

* Red de destino
* Métrica asociada a la red de destino
* Gateway para llegar a la red de destino

En un router Cisco IOS, se puede utilizar el comando **show ip route** para ver la tabla de enrutamiento. Un router también proporciona información adicional de la ruta, incluida la forma en que se descubrió la ruta, cuándo se actualizó por última vez y qué interfaz específica se debe utilizar para llegar a un destino predefinido.

Cuando un paquete llega a la interfaz del router, este examina el encabezado del paquete para determinar la red de destino. Si la red de destino coincide con una ruta de la tabla de enrutamiento, el router reenvía el paquete utilizando la información especificada en la tabla. Si hay dos o más rutas posibles hacia el mismo destino, se utiliza la métrica para decidir qué ruta aparece en la tabla de enrutamiento.

En la ilustración, se muestra la tabla de enrutamiento del R1 en una red simple. A diferencia de la tabla de enrutamiento de host, no hay encabezados de columna que identifiquen la información incluida en una entrada de la tabla de enrutamiento. Por lo tanto, es importante conocer el significado de los distintos tipos de información incluidos en cada entrada.

Cuando se configura una interfaz del router activa con una dirección IP y una máscara de subred, automáticamente se crean dos entradas en la tabla de enrutamiento. En la ilustración, se muestran las entradas de la tabla de enrutamiento en el R1 para la red conectada directamente 192.168.10.0. Estas entradas se agregaron de forma automática a la tabla de enrutamiento cuando se configuró y se activó la interfaz GigabitEthernet 0/0. Las entradas contienen la siguiente información:

**Origen de la ruta**

El origen de la ruta se rotula como “A” en la ilustración. Identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de la ruta.

* **C:** identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.
* **L:** identifica que la ruta es link-local. Las redes link-local se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.

**Red de destino**

La red de destino se rotula como “B” en la ilustración. Identifica la dirección de la red remota.

**Interfaz de salida**

La interfaz de salida se rotula como “C” en la ilustración. Identifica la interfaz de salida que se debe utilizar al reenviar paquetes a la red de destino.

**Nota:** las entradas de la tabla de enrutamiento de link-local no aparecían en las tablas de enrutamiento antes de la versión 15 de IOS.

En general, los routers tienen varias interfaces configuradas. La tabla de enrutamiento almacena información sobre las rutas conectadas directamente y las remotas. Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta. Por ejemplo, los códigos comunes para las redes remotas incluyen lo siguiente:

* **S:** indica que un administrador creó la ruta manualmente para llegar a una red específica. Esto se conoce como “ruta estática”.
* **D:** indica que la ruta se obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento de gateway interior mejorado (EIGRP).
* **O:** indica que la ruta se obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento Open Shortest Path First (OSPF).

**Nota:** otros códigos exceden el ámbito de este capítulo.

En la ilustración, se muestra una entrada de la tabla de enrutamiento en el R1 para la ruta a la red remota 10.1.1.0. La entrada indica la siguiente información:

* **Origen de la ruta:** identifica el modo en que se descubrió la ruta.
* **Red de destino:** identifica la dirección de la red remota.
* **Distancia administrativa:** identifica la confiabilidad del origen de la ruta.
* **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
* **Siguiente salto:** identifica la dirección IP del router siguiente para reenviar el paquete.
* **Marca de hora de la ruta:** identifica cuándo fue la última comunicación con la ruta.
* **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

El siguiente salto es la dirección del dispositivo que procesará el paquete a continuación. Para un host en una red, la dirección del gateway predeterminado (interfaz del router) es el siguiente salto para todos los paquetes que se deben enviar a otra red. En la tabla de enrutamiento de un router, cada ruta a una red remota incluye un siguiente salto.

Cuando un paquete destinado a una red remota llega al router, este busca una correspondencia entre la red de destino y una ruta en la tabla de enrutamiento. Si se encuentra una coincidencia, el router reenvía el paquete a la dirección IP del router de siguiente salto mediante la interfaz que se identificó con la entrada de la ruta.

Un router de siguiente salto es el gateway a las redes remotas.

Por ejemplo, en la ilustración, un paquete que llega al R1 destinado a la red 10.1.1.0 o la red 10.1.2.0 se reenvía a la dirección de siguiente salto 209.165.200.226 mediante la interfaz serial 0/0/0.

Las redes conectadas directamente a un router no tienen dirección de siguiente salto, porque los routers pueden reenviar los paquetes en forma directa a los hosts en esas redes mediante la interfaz designada.

El router no puede reenviar los paquetes sin una ruta para la red de destino en la tabla de enrutamiento. Si no hay una ruta que represente la red de destino en la tabla de enrutamiento, el paquete se descarta (es decir, no se reenvía).

Sin embargo, de la misma manera en que un host puede utilizar un gateway predeterminado para reenviar un paquete a un destino desconocido, un router también se puede configurar para que utilice una ruta estática predeterminada para crear un gateway de último recurso. El gateway de último recurso se aborda en mayor detalle en el curso de enrutamiento de CCNA.

Suponga que la PC1 con la dirección IP 192.168.10.10 desea enviar un paquete a otro host en la misma red. La PC1 revisaría la tabla de rutas IPv4 según la dirección IP de destino. Luego, la PC1 descubriría que el host está en la misma red y, simplemente, lo enviaría por su interfaz (En enlace).

**Nota:** el R1 no participa en la transferencia del paquete. Si la PC1 reenvía un paquete a cualquier red que no sea su red local, debe utilizar los servicios del router R1 y reenviar el paquete a su ruta predeterminada local (192.168.10.1).

Los siguientes ejemplos muestran cómo un host y un router toman decisiones de enrutamiento de paquetes consultando sus respectivas tablas de enrutamiento:

Ejemplo 1: la PC1 desea verificar la conectividad a su gateway predeterminado local en 192.168.10.1 (la interfaz del router).

1. La PC1 consulta la tabla de rutas IPv4 sobre la base de la dirección IP de destino.

2. La PC1 descubre que el host está en la misma red y simplemente envía un paquete ping por la interfaz (En enlace).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino.

4. El R1 consulta la tabla de enrutamiento.

5. El R1 busca en esa tabla la entrada que coincide con la dirección IP de destino, la entrada **L 192.168.10.1/32**, y descubre que esta corresponde a su propia interfaz local, como se muestra en la figura 1.

6. El R1 abre el resto del paquete IP y responde en consecuencia.

Ejemplo 2: la PC1 desea enviar un paquete a la PC2 (192.168.11.10).

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la red de todas las rutas (0.0.0.0) y envía el paquete mediante la ruta predeterminada local (192.168.10.1).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (192.168.11.10).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada **C 192.168.11.0/24**, como se muestra en la figura 2.

5. El R1 reenvía el paquete por la interfaz Gigabit Ethernet 0/1 (G0/1) conectada directamente.

6. La PC2 recibe el paquete y consulta la tabla de enrutamiento IPv4 de host.

7. La PC2 descubre que el paquete está dirigido a ella, abre el resto del paquete y responde en consecuencia.

Ejemplo 3: la PC1 desea enviar un paquete a 209.165.200.226.

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la ruta predeterminada (0.0.0.0/0) y envía el paquete mediante el gateway predeterminado (192.168.10.1).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (209.165.200.226).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada **C 209.165.200.224/30**, como se muestra en la figura 3.

5. La R1 reenvía el paquete por la interfaz serial 0/0/0 (S0/0/0) conectada directamente.

Ejemplo 4: la PC1 desea enviar un paquete al host con la dirección IP 10.1.1.10.

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la red de todas las rutas (0.0.0.0) y envía el paquete a su ruta predeterminada local (192.168.10.1).

3. El R1 recibe el paquete en la interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (10.1.1.10).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada **D 10.1.1.0/24**, como se muestra en la figura 4.

5. El R1 descubre que debe enviar el paquete a la dirección de siguiente salto 209.165.200.226.

6. Nuevamente, el R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada **C 209.165.200.224/30**, como se muestra en la figura 4.

7. La R1 reenvía el paquete por la interfaz serial 0/0/0 (S0/0/0) conectada directamente.

Existen muchos tipos de routers de infraestructura. De hecho, los routers Cisco están diseñados para satisfacer las siguientes necesidades:

* **De sucursal:** trabajadores a distancia, pequeñas empresas y sucursales medianas. Incluye los routers de servicios integrados (ISR) Cisco 800, 1900, 2900 y 3900 de segunda generación (G2).
* **De WAN:** grandes empresas y organizaciones. Incluye los switches de la serie Cisco Catalyst 6500 y el router de servicios de agregación (ASR) Cisco 1000.
* **De proveedor de servicios:** grandes proveedores de servicios. Incluye los routers Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System y los de la serie 7600.

La certificación de CCNA se centra en la familia de routers de sucursal. En la ilustración, se muestra la familia de routers ISR G2 Cisco 1900, 2900 y 3900.

Más allá de su función, su tamaño o su complejidad, todos los modelos de routers son, básicamente, computadoras. Al igual que las computadoras, las tablet PC y los dispositivos inteligentes, los routers también requieren lo siguiente:

* Sistemas operativos (OS)
* Unidades centrales de proceso (CPU)
* Memoria de acceso aleatorio (RAM)
* Memoria de solo lectura (ROM)

Los routers también tienen una memoria especial, que incluye memoria flash y memoria de acceso aleatorio no volátil (NVRAM).

Al igual que las computadoras, las tablet PC y los dispositivos inteligentes, los dispositivos Cisco requieren una CPU para ejecutar las instrucciones del OS, como la inicialización del sistema y las funciones de enrutamiento y conmutación.

La CPU requiere un OS para ofrecer funciones de enrutamiento y conmutación. El Sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco es el software de sistema usado para la mayoría de los dispositivos Cisco, independientemente del tamaño y el tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbrico, grandes routers con decenas de interfaces y muchos otros dispositivos.

El componente destacado en la ilustración es la CPU de un router Cisco 1941 con disipador térmico acoplado.

Los routers tienen acceso a cuatro tipos de memoria: RAM, ROM, NVRAM y flash.

**RAM**

La RAM se utiliza para almacenar diversas aplicaciones y procesos, incluido lo siguiente:

* **Cisco IOS:** el IOS se copia en la RAM durante el arranque.
* **Archivo de configuración en ejecución:** este es el archivo de configuración que almacena los comandos de configuración que el IOS del router utiliza actualmente. También se conoce como “running-config”.
* **Tabla de enrutamiento IP:** este archivo almacena información sobre las redes conectadas directamente y remotas. Se utiliza para determinar el mejor camino para reenviar paquetes.
* **Caché ARP:** esta caché contiene la asignación de direcciones IPv4 a direcciones MAC y es similar a la caché de protocolo de resolución de direcciones (ARP) de una PC. La caché ARP se utiliza en routers que tienen interfaces LAN, como interfaces Ethernet.
* **Búfer de paquetes:** los paquetes se almacenan temporalmente en un búfer cuando se reciben en una interfaz o antes de salir por una.

Al igual que las PC, los routers Cisco utilizan memoria de acceso aleatorio dinámica (DRAM). La DRAM es un tipo muy común de RAM que almacena las instrucciones y los datos necesarios para su ejecución por parte de la CPU. A diferencia de la ROM, la memoria RAM es volátil y requiere alimentación constante para mantener la información. Pierde todo el contenido cuando se apaga o se reinicia el router.

De manera predeterminada, los routers 1941 vienen con 512 MB de DRAM soldada en la placa de sistema principal (incorporada) y una ranura para módulo de memoria en línea doble (DIMM) para realizar actualizaciones de memoria de hasta 2,0 GB adicionales. Los modelos Cisco 2901, 2911 y 2921 vienen con 512 MB de DRAM incorporada. Observe que la primera generación de ISR y los routers Cisco más antiguos no tienen RAM incorporada.

**ROM**

Los routers Cisco usan la memoria ROM para almacenar lo siguiente:

* **Instrucciones de arranque:** proporcionan las instrucciones de inicio.
* **Software de diagnóstico básico:** realiza el autodiagnóstico al encender (POST) de todos los componentes.
* **IOS limitado:** proporciona una versión limitada de respaldo del OS, en caso de que el router no pueda cargar el IOS con todas las funciones.

La ROM consiste en un firmware incorporado en un circuito integrado en el router y no pierde el contenido cuando el router se reinicia o se apaga.

**NVRAM**

El Cisco IOS usa la NVRAM como almacenamiento permanente para el archivo de configuración de inicio (startup-config). Al igual que la ROM, la NVRAM no pierde el contenido cuando se apaga el dispositivo.

**Memoria Flash**

La memoria flash es memoria de PC no volátil que se utiliza como almacenamiento permanente para el IOS y otros archivos relacionados con el sistema. El IOS se copia de la memoria flash a la RAM durante el proceso de arranque.

Los routers Cisco 1941 vienen con dos ranuras externas para memoria Compact Flash. En cada ranura, la densidad de almacenamiento de alta velocidad puede alcanzar los 4 GB.

En la ilustración, se resumen los cuatro tipos de memoria.

Aunque existen diferentes tipos y modelos de routers, todos tienen los mismos componentes generales de hardware.

En la ilustración, se muestra el interior de un ISR Cisco 1841 de primera generación. Haga clic en los componentes para ver una breve descripción.

Observe que en la ilustración también se destacan otros componentes que se encuentran en un router, como la fuente de energía, el ventilador de refrigeración, los protectores térmicos y un módulo de integración avanzada (AIM), los cuales exceden el ámbito de este capítulo.

**Nota:** los profesionales de red deben conocer y comprender la función de los principales componentes internos de un router más que la ubicación exacta de dichos componentes en un router específico. Según el modelo, esos componentes se encuentran en diferentes lugares dentro del router.

Los routers Cisco 1941 incluyen las siguientes conexiones:

* **Puertos de consola:** dos puertos de consola para acceder a la administración de la configuración inicial y de la interfaz de línea de comandos (CLI) mediante un puerto RJ-45 común y un nuevo conector USB de tipo B (USB mini-B).
* **Puerto auxiliar:** un puerto RJ-45 para el acceso a la administración remota; es similar al puerto de consola.
* **Dos interfaces LAN:** dos interfaces Gigabit Ethernet para obtener acceso a LAN.
* **Ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas (EHWIC):** dos ranuras que proporcionan modularidad y flexibilidad al permitir que el router admita distintos tipos de módulos de interfaz, incluidos serial, línea de suscriptor digital (DSL), puerto de switch y tecnología inalámbrica.

El ISR Cisco 1941 también tiene ranuras de almacenamiento para admitir capacidades expandidas. Las ranuras para memoria Compact Flash doble admiten tarjetas Compact Flash de 4 GB cada una para aumentar el espacio de almacenamiento. Se incluyen dos puertos de host USB para obtener espacio de almacenamiento adicional y proteger la capacidad de token.

La memoria Compact Flash puede almacenar la imagen del software Cisco IOS, archivos de registro, archivos de configuración de voz, archivos HTML, configuraciones de respaldo o cualquier otro archivo necesario para el sistema. De manera predeterminada, solo la ranura 0 está ocupada con una tarjeta Compact Flash de fábrica y es la ubicación de arranque predeterminada.

En la ilustración, se identifica la ubicación de estas conexiones y ranuras.

Por lo general, los dispositivos, routers y switches Cisco interconectan numerosos dispositivos. Por esta razón, estos dispositivos tienen varios tipos de puertos e interfaces. Estos puertos e interfaces se utilizan para conectar cables al dispositivo.

Las conexiones de un router Cisco se pueden agrupar en dos categorías:

* **Puertos de administración:** estos son los puertos de consola y los puertos auxiliares utilizados para configurar y administrar el router, así como para resolver problemas del dispositivo. A diferencia de las interfaces LAN y WAN, los puertos de administración no se utilizan para el reenvío de paquetes.
* **Interfaces del router en banda:** estas son las interfaces LAN y WAN configuradas con direccionamiento IP para transportar el tráfico de los usuarios. Las interfaces Ethernet son las conexiones LAN más frecuentes, mientras que las conexiones WAN comunes incluyen las interfaces seriales y DSL.

En la ilustración, se destacan los puertos y las interfaces de un router ISR Cisco 1941 G2.

Al igual que muchos dispositivos de red, los dispositivos Cisco utilizan indicadores de diodos emisores de luz (LED) para proporcionar información de estado. Un LED de interfaz indica la actividad de la interfaz correspondiente. Si un LED está apagado cuando la interfaz está activa y la interfaz está conectada correctamente, puede ser señal de un problema en la interfaz. Si la interfaz está extremadamente ocupada, el LED permanece encendido.

En forma similar a lo que sucede con los switches Cisco, existen varias maneras de acceder al entorno de la CLI de un router Cisco. Los métodos más comunes son los siguientes:

* **Consola:** utiliza conexiones seriales de baja velocidad o USB para proporcionar acceso de administración fuera de banda con conexión directa a un dispositivo Cisco.
* **Telnet o SSH:** dos métodos para acceder de forma remota a una sesión de CLI a través de una interfaz de red activa.
* **Puerto auxiliar:** se utiliza para la administración remota del router mediante una línea telefónica de dial-up y un módem.

El puerto de consola y el auxiliar están ubicados en el router.

Además de estos puertos, los routers también tienen interfaces de red para recibir y reenviar paquetes IP. Los routers tienen muchas interfaces que se usan para conectarse a múltiples redes. En general, las interfaces se conectan a distintos tipos de redes, lo que significa que se requieren distintos tipos de medios y de conectores.

Cada interfaz en el router es miembro o host de otra red IP. Cada interfaz se debe configurar con una dirección IP y una máscara de subred de una red diferente. Cisco IOS no permite que dos interfaces activas en el mismo router pertenezcan a la misma red.

Las interfaces del router se pueden agrupar en dos categorías:

* **Interfaces LAN Ethernet:** se utilizan para conectar cables que terminan en dispositivos LAN, como PC y switches. La interfaz también puede utilizarse para conectar routers entre sí. Existen varias convenciones de nomenclatura de uso frecuente para las interfaces Ethernet: Ethernet antigua, FastEthernet y Gigabit Ethernet. El nombre utilizado depende del tipo y el modelo de dispositivo.
* **Interfaces WAN seriales:** se utilizan para conectar routers a redes externas, generalmente a una distancia geográfica más extensa. Al igual que las interfaces LAN, cada interfaz WAN serial tiene su propia dirección IP y su máscara de subred, que la identifican como miembro de una red específica.

En la ilustración, se muestran las interfaces LAN y seriales del router.

Los detalles operativos de Cisco IOS varían de acuerdo con los diferentes dispositivos de internetworking, según el propósito y el conjunto de características del dispositivo. No obstante, Cisco IOS para routers proporciona lo siguiente:

* Direccionamiento
* Interfaces
* Enrutamiento
* Seguridad
* QoS
* Administración de recursos

El archivo de IOS propiamente dicho tiene varios megabytes y, al igual que en los switches Cisco IOS, se almacena en la memoria flash. El uso de la memoria flash permite actualizar el IOS a versiones más recientes o agregarle nuevas características. Durante el arranque, el IOS se copia de la memoria flash a la RAM. La DRAM es mucho más rápida que la memoria flash, por lo que copiar el IOS en la RAM aumenta el rendimiento del dispositivo.

Como se muestra en la ilustración, un router carga los siguientes dos archivos en la RAM durante el inicio:

* **Archivo de imagen de IOS:** el IOS facilita el funcionamiento básico de los componentes de hardware del dispositivo. El archivo de imagen de IOS se almacena en la memoria flash.
* **Archivo de configuración de inicio:** el archivo de configuración de inicio incluye los comandos que se utilizan para realizar la configuración inicial de un router y crear el archivo de configuración en ejecución almacenado en la RAM. El archivo de configuración de inicio se almacena en NVRAM. Todos los cambios de configuración se almacenan en el archivo de configuración en ejecución, y el IOS los implementa de inmediato.

La configuración en ejecución se modifica cuando el administrador de red realiza la configuración del dispositivo. Cuando se realizan cambios al archivo running-config, este se debe guardar en la NVRAM como archivo de configuración de inicio, en caso de que el router se reinicie o se apague.

El proceso de arranque que se muestra en la figura 1 consta de tres fases principales:

1. Llevar a cabo el POST y cargar el programa bootstrap.

2. Localizar y cargar el software Cisco IOS.

3. Localizar y cargar el archivo de configuración de inicio o ingresar al modo Setup.

**1. Llevar a cabo el POST y cargar el programa bootstrap (figura 2)**

La prueba de Autodiagnóstico al encender (POST, Power-On Self Test) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante este autodiagnóstico, el router ejecuta desde la ROM diagnósticos de varios componentes de hardware, incluidos la CPU, la RAM y la NVRAM. Una vez finalizado el POST, el router ejecuta el programa bootstrap.

Después del POST, el programa bootstrap se copia de la ROM a la RAM. Una vez en la RAM, la CPU ejecuta las instrucciones del programa bootstrap. La tarea principal del programa bootstrap es ubicar al Cisco IOS y cargarlo en la RAM.

**Nota:** en este momento, si existe una conexión de consola al router, comienzan a aparecer resultados en pantalla.

**2. Localizar y cargar Cisco IOS (figura 3)**

Por lo general, el IOS se almacena en la memoria flash y se copia en la RAM para que lo ejecute la CPU. Durante la autodescompresión del archivo de imagen de IOS, se muestra una cadena de símbolos de almohadilla (#).

Si la imagen de IOS no se encuentra en la memoria flash, el router puede buscarla con un servidor TFTP. Si no se puede localizar una imagen de IOS completa, se copia una versión reducida del IOS de la ROM a la RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

**3. Localizar y cargar el archivo de configuración (figura 4)**

A continuación, el programa bootstrap busca el archivo de configuración de inicio (también conocido como “startup-config”) en la NVRAM. El archivo contiene los parámetros y comandos de configuración guardados anteriormente. Si existe, se copia en la RAM como archivo de configuración en ejecución o “running-config”. El archivo running-config contiene direcciones de interfaz, inicia los procesos de enrutamiento, configura las contraseñas del router y define otras características del dispositivo.

Si el archivo startup-config no existe en la NVRAM, el router puede buscar un servidor de protocolo trivial de transferencia de archivos (TFTP). Si el router detecta que tiene un enlace activo a otro router configurado, envía un broadcast en busca de un archivo de configuración a través del enlace activo.

Si no se encuentra un servidor TFTP, el router muestra la petición de entrada del modo Setup. El modo Setup consiste en una serie de preguntas que solicitan al usuario información de configuración básica. El modo Setup no tiene como fin utilizarse para ingresar a configuraciones complejas del router y los administradores de red normalmente no lo usan.

**Nota:** en este curso, no se utiliza el modo Setup para configurar el router. Ante la petición de entrada del modo Setup, siempre se debe responder **no**. Si el usuario responde yes (sí) e ingresa al modo Setup, puede presionar **Ctrl**+**C** en cualquier momento para finalizar el proceso de configuración.

El comando **show version** se puede utilizar para revisar y resolver problemas de algunos de los componentes básicos de hardware y software del router. Este comando muestra información sobre la versión del software Cisco IOS que se encuentra en ejecución en el router, la versión del programa bootstrap y datos sobre la configuración de hardware, incluida la cantidad de memoria del sistema.

El resultado del comando **show version** incluye lo siguiente:

* **Versión de IOS:** la versión del software Cisco IOS que se encuentra en la RAM y que utiliza el router.
* **Programa bootstrap en la ROM:** muestra la versión del software bootstrap del sistema almacenado en la ROM que se utilizó inicialmente para arrancar el router.
* **Ubicación del IOS:** muestra dónde se encuentra el programa boostrap y dónde cargó el Cisco IOS, además del nombre de archivo completo de la imagen de IOS.
* **CPU y cantidad de RAM:** en la primera parte de esta línea, se muestra el tipo de CPU del router en cuestión. La última parte de esta línea muestra la cantidad de DRAM. Algunas series de routers, como el ISR Cisco 1941, utilizan una parte de la DRAM como memoria de paquetes. La memoria de paquetes se usa para paquetes de almacenamiento intermedio. Para determinar la cantidad total de DRAM en el router, se deben sumar ambos números.
* **Interfaces:** muestra las interfaces físicas del router. En este ejemplo, el ISR Cisco 1941 tiene dos interfaces Gigabit Ethernet y dos interfaces seriales de baja velocidad.
* **Cantidad de memoria NVRAM y flash:** esta es la cantidad de memoria NVRAM y flash del router. La memoria NVRAM se utiliza para almacenar el archivo startup-config, y la memoria flash se utiliza para almacenar Cisco IOS de forma permanente.

En la última línea del comando **show version**, se muestra el valor configurado actualmente del registro de configuración del software en sistema hexadecimal. Si se muestra un segundo valor entre paréntesis, indica el valor del registro de configuración que se utilizará durante la siguiente recarga.

El registro de configuración tiene varios usos, incluida la recuperación de la contraseña. La configuración predeterminada de fábrica para el registro de configuración es 0x2102. Este valor indica que el router intenta cargar una imagen del software Cisco IOS desde la memoria flash y el archivo de configuración de inicio desde la NVRAM.

Los routers y los switches Cisco tienen muchas similitudes: admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial durante su implementación en una red son idénticos para ambos dispositivos.

De modo similar a lo que sucede al configurar un switch, se deben completar los siguientes pasos al configurar los parámetros iniciales de un router:

1. Asignar un nombre de dispositivo mediante el comando de configuración global **hostname** (figura 1).

2. Establecer contraseñas. (figura 2).

* Proteger el acceso al modo EXEC privilegiado mediante el comando **enable secret**.
* Proteger el acceso al modo EXEC con el comando **login** en el puerto de consola, y el comando **password** para establecer la contraseña.
* Proteger el acceso virtual. Esto se realiza de forma similar a la protección del acceso al modo EXEC, excepto que se lleva a cabo en el puerto de teletipo virtual (VTY).
* Utilizar el comando de configuración global **service password-encryption** para evitar que las contraseñas se muestren como texto no cifrado en el archivo de configuración.

3. Proporcionar notificaciones legales mediante el comando de configuración global de mensaje del día (MOTD) **banner motd** (figura 3).

4. Guardar la configuración mediante el comando **copy run start** (figura 4).

5. Verificar la configuración mediante el comando **show run**.

En la figura 5, se proporciona un verificador de sintaxis que le permite practicar estos pasos de configuración.

Para que los routers sean accesibles, se deben configurar sus interfaces. Por lo tanto, para habilitar una interfaz específica, ingrese al modo de configuración de interfaz con el comando del modo de configuración global **interface***tipo-y-número*.

Existen varios tipos de interfaces diferentes disponibles en los routers Cisco. En este ejemplo, el router Cisco 1941 cuenta con dos interfaces Gigabit Ethernet y una tarjeta de interfaz WAN (WIC) serial que consta de dos interfaces. Las interfaces se denominan de la siguiente manera:

* Gigabit Ethernet 0/0 (G0/0)
* Gigabit Ethernet 0/1 (G0/1)
* Serial 0/0/0 (S0/0/0)
* Serial 0/0/1 (S0/0/1)

Para habilitar una interfaz del router, configure lo siguiente:

* **Dirección IPv4 y máscara de subred:** configura la dirección IP y la máscara de subred mediante el comando del modo de configuración de interfaz **ip address***dirección máscara-de-subred*.
* **Active la interfaz:** de manera predeterminada, las interfaces LAN y WAN no están activadas. La interfaz se debe activar mediante el comando **no shutdown**. Es como encender la interfaz. La interfaz también debe estar conectada a otro dispositivo (un hub, un switch u otro router) para que la capa física esté activa.

Si bien no es necesario, es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. El texto de la descripción tiene un límite de 240 caracteres. En las redes de producción, una descripción puede ser útil para la resolución de problemas, dado que suministra información con respecto al tipo de red a la que está conectada la interfaz y si hay otros routers en esa red. Si la interfaz se conecta a un ISP o un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

En la figura 1, se muestra la configuración de las interfaces LAN conectadas al R1. En la figura 2, practique la configuración de una interfaz LAN.

**Nota:** para la configuración de Gigabit Ethernet 0/1 se utilizan abreviaturas de comandos.

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. El más útil de ellos es **show ip interface brief**. En el resultado generado, se muestran todas las interfaces, sus direcciones IP y su estado actual. Las interfaces configuradas y conectadas deben mostrar el valor “up” (conectado) en Status (Estado) y en Protocol (Protocolo). Cualquier otro valor indicaría un problema con la configuración o el cableado.

Puede verificar la conectividad desde la interfaz mediante el comando **ping**. Los routers Cisco envían cinco pings consecutivos y miden los tiempos de ida y vuelta mínimos, medios y máximos. Los signos de exclamación verifican la conectividad.

En la figura 1, se muestran los resultados del comando **show ip interface brief**, que revelan que las interfaces LAN y el enlace WAN están activos y operativos. Observe que el comando **ping** generó cinco signos de exclamación que verifican la conectividad al R2.

Otros comandos de verificación de interfaz incluyen los siguientes:

* **show ip route** **:** muestra el contenido de la tabla de enrutamiento IPv4 almacenada en la RAM.
* **show interfaces** **-**muestra estadísticas de todas las interfaces del dispositivo.
* **show ip interface** **:** muestra las estadísticas de IPv4 de todas las interfaces de un router.

En la figura 2, se muestra el resultado del comando **show ip route**. Observe las tres entradas de redes conectadas directamente y las entradas de las interfaces de enlace local.

Recuerde guardar la configuración mediante el comando **copy running-config startup-config**.

La mayoría de los routers tiene, como mínimo, dos interfaces. Cada interfaz se configura con una dirección IP distinta en una red diferente.

Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de gateway predeterminado. El gateway predeterminado se utiliza solo cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local del host. Si bien no importa qué dirección se configura realmente en la interfaz del router, la dirección IP del dispositivo host y la dirección de la interfaz del router deben estar en la misma red.

En las ilustraciones, se muestra la topología de un router con dos interfaces independientes. Cada interfaz está conectada a una red diferente. G0/0 está conectada a la red 192.168.10.0, mientras que G0/1 está conectada a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de gateway predeterminado correspondiente.

En la figura 1, la PC1 envía un paquete a la PC2. En este ejemplo, el gateway predeterminado no se utiliza; en cambio, la PC1 dirige el paquete con la dirección IP de la PC2 y reenvía el paquete directamente a dicha PC a través del switch.

En la figura 2, la PC1 envía un paquete a la PC3. En este ejemplo, la PC1 dirige el paquete con la dirección IP de la PC3, pero luego lo reenvía al router. El router acepta el paquete, accede a la tabla de rutas para determinar la interfaz de salida adecuada según la dirección de destino y reenvía el paquete por la interfaz apropiada para llegar a la PC3.

Todos los dispositivos que requieren el uso de un router utilizan un gateway predeterminado para precisar el mejor camino hacia un destino remoto. Los dispositivos finales requieren direcciones de gateway predeterminado, pero también las requieren los dispositivos intermediarios, como los switches Cisco IOS.

La información de dirección IP en un switch solo se necesita para administrar el switch de forma remota. Es decir, para acceder al switch mediante Telnet, este debe tener una dirección IP a la cual se pueda acceder mediante dicho sistema. Si se accede al switch solamente desde dispositivos dentro de la red local, solo se requiere una dirección IP.

La configuración de la dirección IP en un switch se realiza en la interfaz virtual de switch (SVI):

S1(config)# **interface vlan1**

S1(config-vlan)# **ip address 192.168.10.50 255.255.255.0**

S1(config-vlan)# **no shut**

Sin embargo, si dispositivos de otra red deben acceder al switch, este se debe configurar con una dirección de gateway predeterminado, ya que los paquetes que se originan en el switch se manejan como los paquetes que se originan en un dispositivo host. Por lo tanto, los paquetes que se originan en el switch y están destinados a un dispositivo en la misma red se reenvían directamente al dispositivo apropiado. Los paquetes que se originan en el switch y están destinados a un dispositivo en una red remota se deben reenviar al gateway predeterminado para precisar la ruta.

Para configurar un gateway predeterminado en un switch, utilice el siguiente comando de configuración global:

S1(config)# **ip default-gateway 192.168.10.1**

En la figura 1, se muestra un administrador que se conecta a un switch en una red remota. Para que el switch reenvíe los paquetes de respuesta al administrador, se debe configurar el gateway predeterminado.

Un concepto erróneo frecuente es que el switch utiliza la dirección de gateway predeterminado configurada para determinar adónde reenviar los paquetes que se originan en los hosts conectados al switch y que están destinados a los hosts en una red remota. En realidad, la información de dirección IP y de gateway predeterminado solo se utiliza para los paquetes que se originan en el switch. Los paquetes que se originan en los hosts conectados al switch ya deben tener configurada la información de gateway predeterminado para comunicarse en redes remotas. En la figura 2, practique la configuración de un gateway predeterminado en un switch.