CAPÍTULO 6. CAPA DE RED

Las aplicaciones y servicios de red de un terminal se pueden comunicar con las aplicaciones y servicios que se ejecutan en otro terminal. ¿Cómo se comunican los datos en la red de manera eficaz?

Los protocolos de la capa de red del modelo OSI especifican el direccionamiento y los procesos que permiten que se armen y se transporten los paquetes de datos de la capa de red. El encapsulamiento de capa de red permite que se transfieran los datos a un destino dentro de una red (o a otra red) con una sobrecarga mínima.

En este capítulo, nos concentraremos en el rol de la capa de red. Se examina cómo divide las redes en grupos de hosts para administrar el flujo de paquetes de datos dentro de una red. También se explica cómo se facilita la comunicación entre las redes. Esta comunicación entre redes se denomina "routing".

6.1.1.1 La capa de red

La capa de red o la capa OSI 3, brinda servicios para permitir que los terminales puedan intercambiar datos en la red. Para lograr el transporte completo, la capa de red utiliza cuatro procesos básicos:

- **Direccionamiento de terminales:** Los terminales se deben configurar con una dirección IP única para identificarlos en la red.

- **Encapsulamiento:** La capa de red encapsula la unidad de datos del protocolo (PDU) de la capa de transporte a un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores).

- **Routing:** La capa de red brinca servicios para dirigir paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "routing". Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.

- **Desencapsulamiento:** Cuando el 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 dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte.

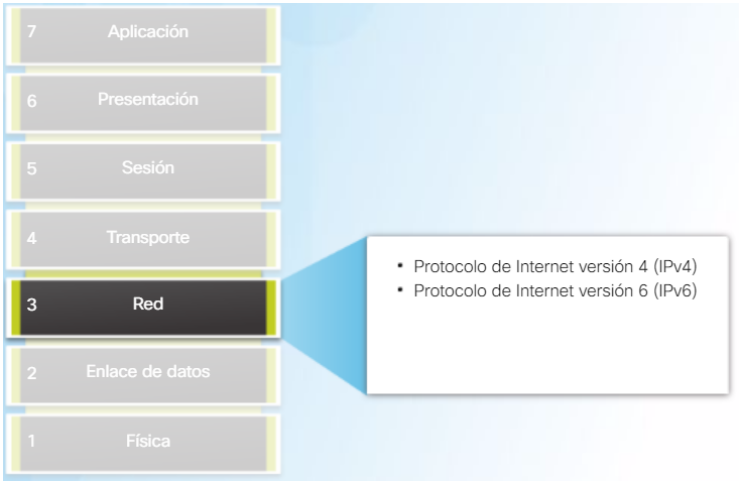
A diferencia de la capa de transporte (la capa OSI 4), que administra el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de capa de red especifican la estructura de paquete y los procesos que se utilizan para transportar la información de un host a otro. La capa de red puede transportar paquetes de varios tipos de comunicación entre varios hosts porque funciona sin tener en cuenta los datos que contiene cada paquete.

6.1.1.2 Protocolos de la capa de red

Existen varios protocolos de capa de red. Sin embargo, como se muestra en la ilustración, solo hay dos protocolos de capa de red que suelen implementarse:

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

Nota: Los protocolos de capa de red antiguos no se muestran en la ilustración y no se analizan en este curso.

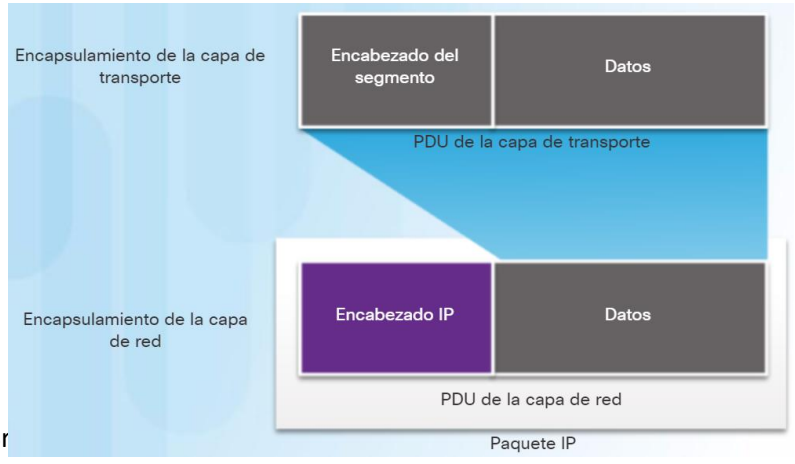


6.1.2.1 Encapsulamiento de IP

Para encapsular el segmento de capa de transporte u otros datos, IP le agrega un encabezado IP. Este encabezado se usa para entregar el paquete al host de destino. El encabezado IP permanece igual desde el momento en que el paquete deja el host de origen hasta que llega al host de destino.

El proceso de encapsulamiento de datos capa por capa permite que se desarrollen y se escalen los servicios en las diferentes capas sin afectar a las otras capas. Esto significa que IPv4 o IPv6 o cualquier protocolo nuevo que se desarrolle en el futuro puede armar sin inconvenientes un paquete con los segmentos de capa de transporte.

Los routers pueden implementar diferentes protocolos de capa de red para que funcionen simultáneamente en una red. El routing que realizan estos dispositivos intermediarios solo toma en cuenta el contenido del encabezado de paquetes de la capa de red. En ningún caso, la porción de datos del paquete, es decir, la PDU de capa de transporte encapsulada, se modifica durante los procesos de la capa de red.



6.1.2.2 Características de IP

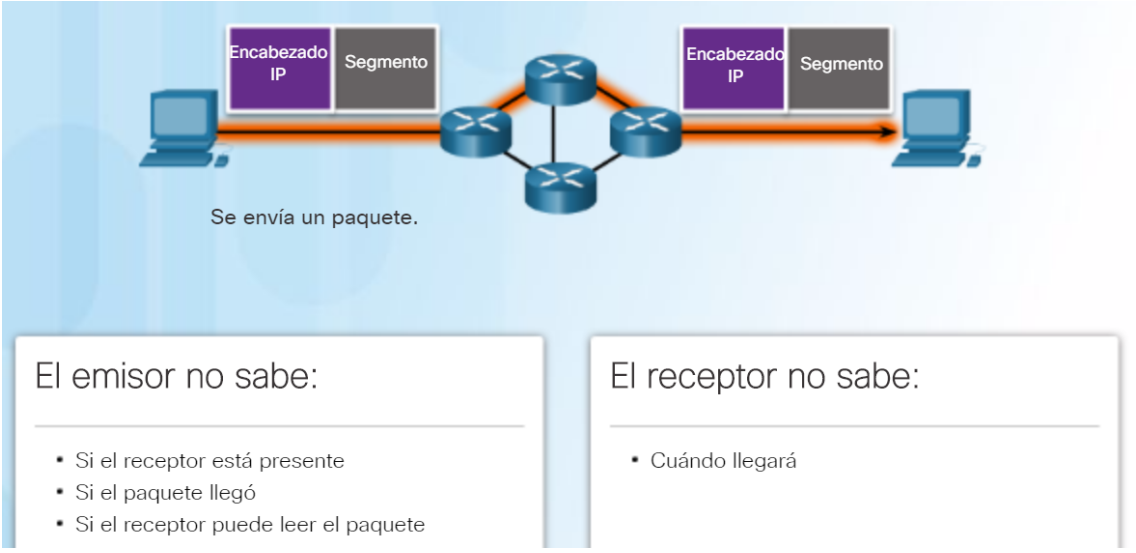
IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.

En la ilustración, se describen las características básicas de IP.

- Sin conexión: No se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
- Servicio mínimo: IP no es confiable por naturaleza, ya que la entrega de paquetes no está garantizada.
- Independiente de los medios: el funcionamiento es independiente del medio físico que transporta los datos.

6.1.2.3 IP: Sin conexión

IP no tiene conexión, lo que significa que no se genera una conexión completa exclusiva antes de enviar los datos. Las comunicaciones de datos sin conexión funcionan con el mismo principio. IP no necesita un intercambio inicial de información de control para establecer una conexión completa para que se reenvíen los paquetes.



6.1.2.4 IP: Entrega de servicio mínimo

En la ilustración, se muestran las características de entrega de mejor esfuerzo o poco confiable del protocolo IP. El protocolo IP no garantiza que todos los paquetes que se envían, de hecho, se reciban.

Que sea poco confiable significa que IP no tiene la funcionalidad para administrar o recuperar paquetes no recibidos o dañados. Esto se debe a que, si bien los paquetes IP se envían con información sobre la ubicación de entrega, no tienen información que pueda procesarse para informar al remitente si la entrega se realizó correctamente. Es posible que los paquetes lleguen dañados o fuera de secuencia al destino o que no lleguen en absoluto. IP no tiene la funcionalidad de retransmitir paquetes si se producen errores.

Las aplicaciones que utilizan los datos o los servicios de capas superiores deben solucionar problemas como el envío de paquetes fuera de orden o la pérdida de paquetes. Esta característica permite que IP funcione de manera muy eficaz. En el paquete del protocolo TCP/IP, la confiabilidad es la función de la capa de transporte.

6.1.2.5 IP: Independiente de los medios

IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. La capa de enlace de datos OSI se encarga de preparar los paquetes IP para la transmisión por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

Sin embargo, la capa de red tiene en cuenta una de las características más importantes del medio, que es el tamaño máximo de PDU que cada medio puede transportar. Esta característica se conoce como "unidad de transmisión máxima" (MTU). Parte del control de la comunicación entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo del paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. La capa de red luego determina qué tamaño pueden tener los paquetes.

En algunos casos, un dispositivo intermediario, que por lo general es un router, debe dividir el paquete cuando se reenvía de un medio a otro con una MTU menor. Este proceso se denomina "fragmentación de paquetes" o "fragmentación".

6.1.3.1 Encabezado de paquetes IPv4

El encabezado de paquetes IPv4 consta de campos que contienen información. Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo. El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv4.

- **Versión:** Contiene un valor binario de 4 bits establecido en 0100 que lo identifica como un paquete IP versión 4.

- **Servicios diferenciados o DiffServ (DS)**: antes conocido como el campo "tipo de servicio" (ToS), es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los seis bits más importantes del campo de servicios diferenciados son el punto de código de servicios diferenciados (DSCP), y los últimos dos bits son los de notificación de congestión explícita (ECN).

- **Tiempo de duración (TTL):** Contiene un valor binario de 8 bits que se usa para delimitar el tiempo de vida de un paquete. El emisor del paquete establece el valor inicial de TTL que se reduce en uno cada vez que un router procesa el paquete. Si el campo TTL llega a cero, el router descarta el paquete y envía a la dirección IP de origen un mensaje de tiempo superado del protocolo de mensajes de control de Internet (ICMP).

- El campo **Protocolo** se utiliza para identificar el protocolo del siguiente nivel. Este valor binario de 8 bits indica el tipo de carga de datos que lleva el paquete, lo que permite que la capa de red transmita los datos al protocolo de capa superior apropiado. ICMP (1), TCP (6) y UDP (17) son algunos valores comunes.

- **Dirección IPv4 de origen**: contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen siempre es una dirección de unidifusión.

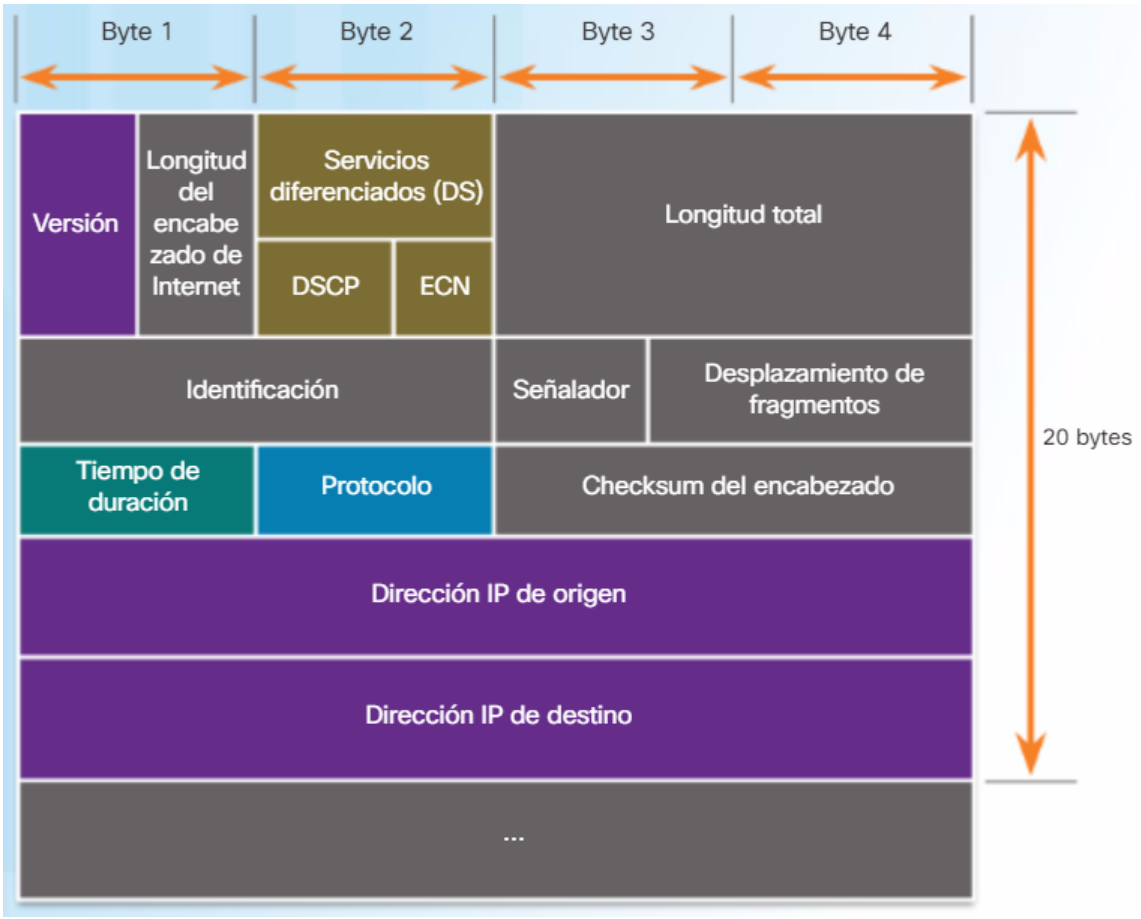
- **Dirección IPv4 de destino**: contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección de unidifusión, de multidifusión o de difusión.

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino En estos campos, se identifica de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian cuando un paquete se transfiere desde el origen hasta el destino.

Para identificar y validar el paquete, se usan los campos de longitud del encabezado de Internet (IHL), longitud total y el encabezado checksum.

Para reordenar un paquete fragmentado, se usan otros campos. Específicamente, el paquete IPv4 utiliza los campos de identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos. Es posible que un router deba fragmentar un paquete cuando lo reenvíe de un medio a otro con una MTU menor.

Los campos "opciones" y "relleno" se usan con poca frecuencia y exceden el ámbito de este capítulo.



6.1.4.1 Limitaciones de IPv4

A lo largo de los años, IPv4 se actualizó para enfrentar los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de las direcciones IP:** IPv4 tiene una cantidad limitada de direcciones IPv4 públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.

- **Expansión de la tabla de routing de Internet:** Los routers usan tablas de routing para determinar las mejores rutas. A medida que aumenta el número de servidores conectados a Internet, aumenta también el número de rutas de red. Estas rutas IPv4 consumen una gran cantidad de recursos de memoria y de procesador en los routers de Internet.

- **Falta de conectividad completa:** Una de las tecnologías más implementadas en las redes IPv4 es la traducción de direcciones de red (NAT). NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.

6.1.4.2 Introducción a IPv6

A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de trabajo de ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo. Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de redes actuales y previsibles.

Las mejoras de IPv6 incluyen lo siguiente:

- **Mayor espacio de direcciones:** Las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en comparación con los 32 bits de IPv4.

- **Mejor manejo de paquetes:** Se redujo la cantidad de campos del encabezado de IPv6 para hacerlo más simple.

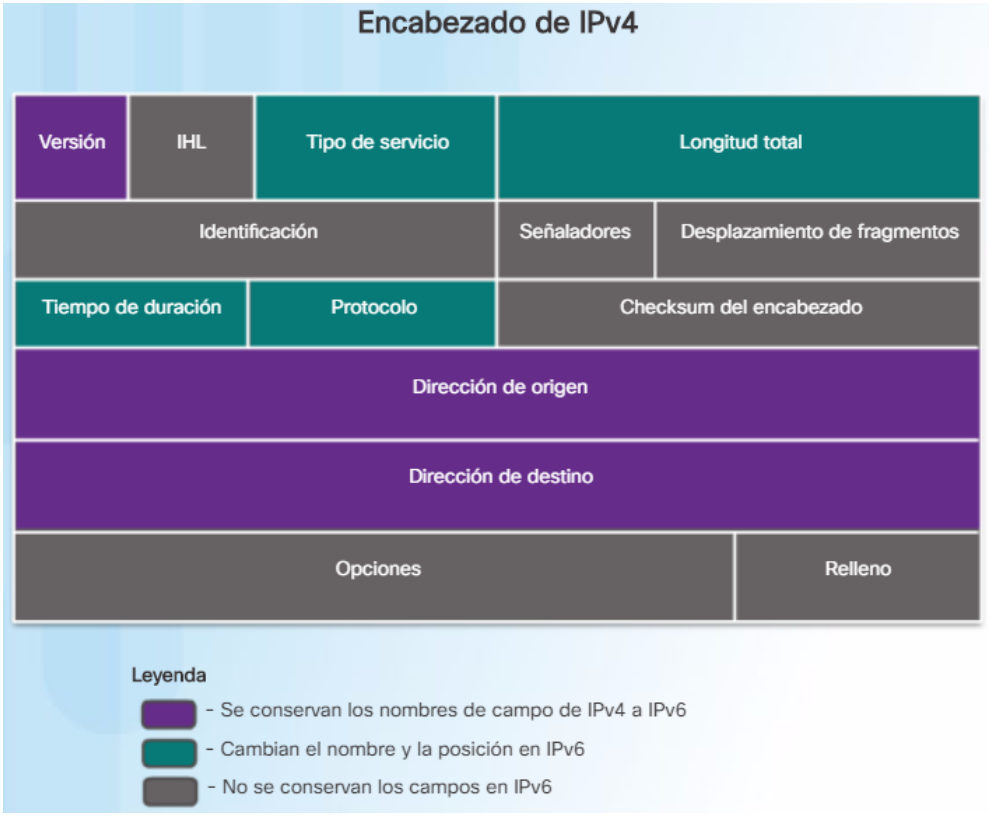
- **Se elimina la necesidad de NAT:** Al tener un número tan grande de direcciones IPv6 públicas, la NAT entre las direcciones IPv4 privadas y públicas ya no es necesaria. Esto evita algunos problemas de aplicación inducidos por NAT que tuvieron algunas aplicaciones que necesitan conectividad completa.

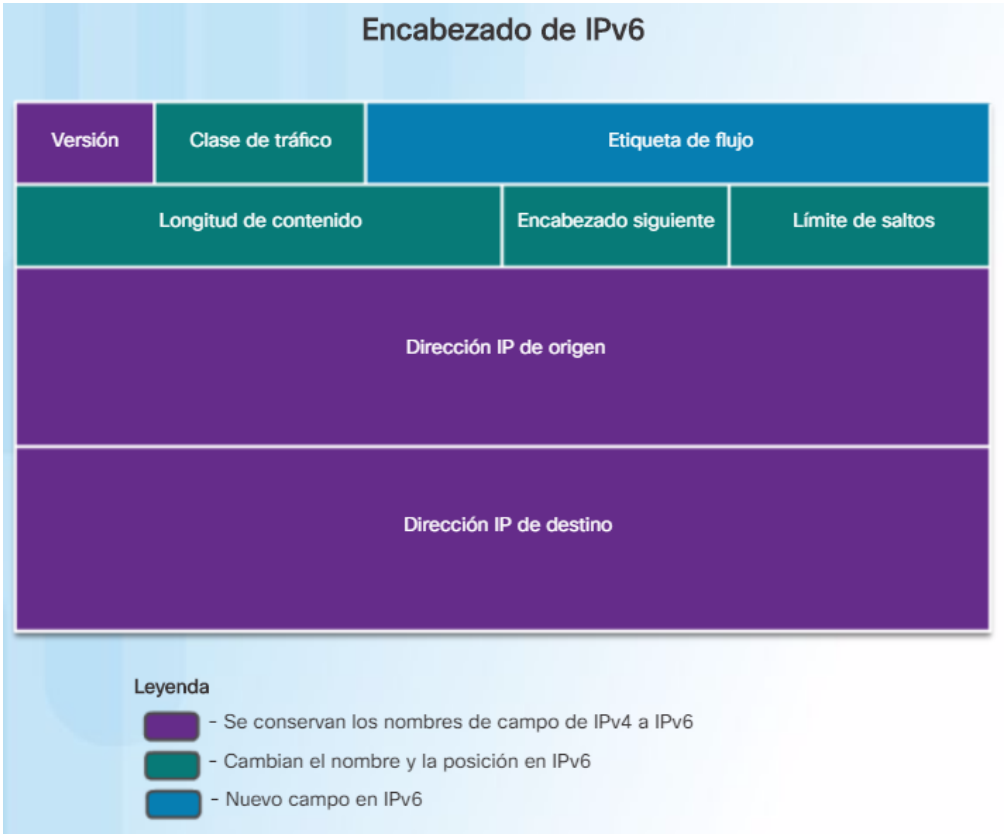
El espacio de direcciones IPv4 de 32 bits ofrece aproximadamente 4 294 967 296 direcciones únicas. Una de las principales mejoras de diseño de IPv6 con respecto a IPv4 es el encabezado de IPv6 simplificado.

6.1.4.3 Encapsulamiento IPv6

Uno de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6. Las ventajas que presenta IPv6 se pueden resumir en las siguientes:

- Formato de encabezado simplificado para un manejo de paquetes eficaz.
- Mayor contenido para aumentar el rendimiento y la eficacia del transporte.
- Arquitectura de red jerárquica para mejorar la eficacia del routing.
- Autoconfiguración de direcciones.
- Eliminación de la necesidad de traducción de direcciones de redes (NAT) entre las direcciones públicas y privadas.


Encabezado de IPv4
Versión
IHL
Tipo de servicio
Longitud total
Identificación
Señaladores
Desplazamiento de fragmentos
Tiempo de duración
Protocolo
Checksum del encabezado
Dirección de origen
Dirección de destino
Opciones
Relleno
Leyenda
- Se conservan los nombres de campo de IPv4 a IPv6
- Cambian el nombre y la posición en IPv6
- No se conservan los campos en IPv6


Encabezado de IPv6
Versión
Clase de tráfico
Etiqueta de flujo
Longitud de contenido
Encabezado siguiente
Límite de saltos
Dirección IP de origen
Dirección IP de destino
Leyenda
- Se conservan los nombres de campo de IPv4 a IPv6
- Cambian el nombre y la posición en IPv6
- Nuevo campo en IPv6

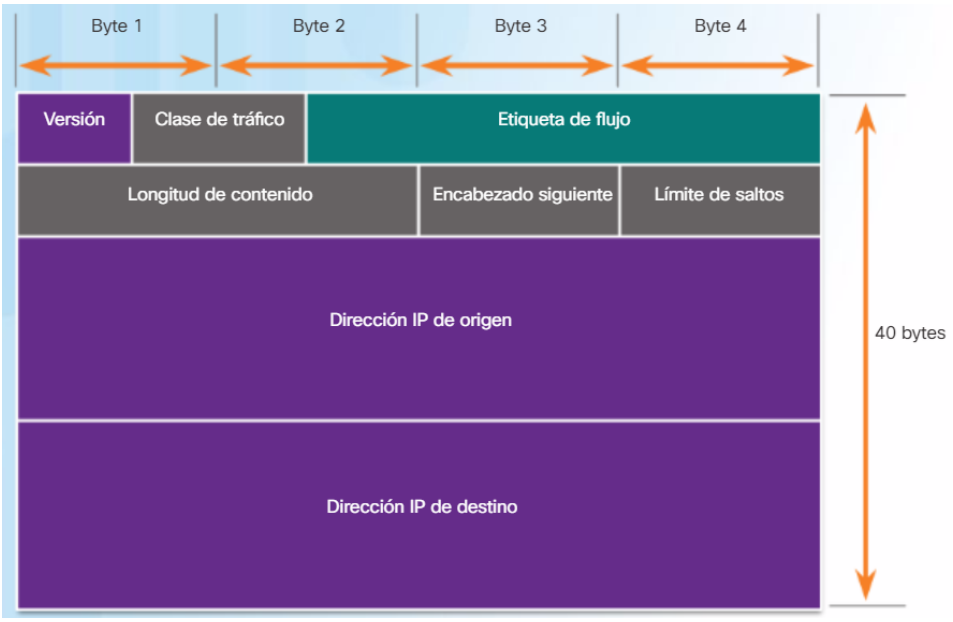
6.1.4.4 Encabezado de paquetes IPv6

Los campos del encabezado de paquetes IPv6 incluyen lo siguiente:

- **Versión:** Este campo contiene un valor binario de 4 bits establecido en 0110 que lo identifica como un paquete IP versión 6.
- **Clase de tráfico:** Este campo de 8 bits es el equivalente al campo DS de IPv4
- **Etiqueta de flujo:** Este campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo de los routers.
- **Longitud de contenido:** Este campo de 16 bits indica la longitud de la porción de datos o la longitud de contenido del paquete IPv6.
- **Encabezado siguiente:** Este campo de 8 bits es el equivalente al campo protocolo de IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de saltos:** Este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando llega a cero, se descarta el paquete y se envía un mensaje de tiempo superado de ICMPv6 al host de origen que indica que el paquete no llegó a destino porque excedió el límite de saltos.
- **Dirección IPv6 de origen**: es un campo de 128 bits que identifica la dirección IPv6 del host emisor.
- **Dirección IPv6 de destino**: es un campo de 128 bits que identifica la dirección IPv6 del host receptor.

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.

A diferencia de IPv4, los routers no fragmentan de los paquetes IPv6 enrutados.



6.2.1.1 La decisión de reenvío de host

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

- **A sí mismo:** Un host puede hacerse ping a sí mismo al enviar un paquete a una dirección IPv4 127.0.0.1, denominada "interfaz de bucle invertido". El hacer ping a la interfaz de bucle invertido, pone a prueba la pila del protocolo TCP/IP en el host.

- **Al host local:** Este es un host que está en la misma red local que el host emisor. Los hosts comparten la misma dirección de red.

- **A un módulo remoto de E/S:** Este es un host en una red remota. Los hosts no comparten la misma dirección de red.

Que un paquete tenga como destino un host local o un módulo remoto de E/S lo determina la combinación de máscara de subred y dirección IPv4 del dispositivo de origen (emisor) en comparación con la máscara de subred y la dirección IPv4 del dispositivo de destino.

En una red doméstica o comercial puede haber varios dispositivos cableados o inalámbricos interconectados que utilizan un dispositivo intermediario, como un switch LAN o un punto de acceso inalámbrico (WAP). Este dispositivo intermediario proporciona interconexiones entre los hosts de la red local. Los hosts locales pueden conectarse y compartir información sin la necesidad de dispositivos adicionales. Si un host envía un paquete a un dispositivo configurado con la misma red IP que el dispositivo host, el paquete se reenvía por la interfaz de host a través del dispositivo intermediario y se dirige directamente al dispositivo de destino.

Por supuesto, en la mayoría de las situaciones queremos que nuestros dispositivos se conecten más allá del segmento de red local, por ejemplo, que vayan a otras casas, empresas y a Internet. Los dispositivos que no están en el segmento de red local se denominan "módulo remoto de E/S". Cuando un dispositivo de origen envía un paquete a un dispositivo de destino remoto, se necesita la ayuda de los routers y del routing. El routing es el proceso de identificación de la mejor ruta para llegar a un destino. El router conectado al segmento de red local se denomina **gateway predeterminado**.

6.2.1.2 Gateway predeterminado

El gateway predeterminado es el dispositivo de red que puede enrutar el tráfico a otras redes. Es el router el que puede enrutar el tráfico fuera de la red local. Un gateway predeterminado:

- Enruta el tráfico a otras redes.
- Tiene una dirección IP local en el mismo intervalo de direcciones que otros hosts de la red.
- Puede llevar datos y reenviarlos.

6.2.1.3 Uso del gateway predeterminado

La tabla de routing de un host incluye, por lo general, un gateway predeterminado. El host recibe la dirección IPv4 del gateway predeterminado ya sea de manera dinámica del protocolo DHCP o si se la configura manualmente. La configuración de un gateway predeterminado genera una ruta predeterminada en la tabla de routing de la PC.

Una ruta predeterminada es la ruta o camino que la PC utiliza cuando intenta conectarse a la red remota. La ruta predeterminada se desprende de la configuración del gateway predeterminado y se ubica en la tabla de routing del servidor.

6.2.1.4 Tablas de routing de host

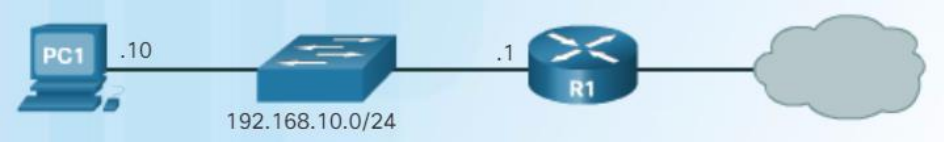
Para mostrar la tabla de routing de un host de Windows, se puede usar el comando **route print** o **netstat -r**. Ambos comandos generan el mismo resultado. El resultado puede ser un poco abrumador al principio, pero es bastante simple de comprender.

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

- **Lista de interfaces:** Muestra una lista de las direcciones de control de acceso a los medios (MAC) y el número de interfaz asignado de cada interfaz con capacidad de conexión a red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.

- **Tabla de rutas IPv4:** Es una lista de todas las rutas IPv4 conocidas, incluidas las conexiones directas, las redes locales y las rutas locales predeterminadas.

- **Tabla de rutas IPv6:** Es una lista de todas las rutas IPv6 conocidas, incluidas las conexiones directas, las redes locales y las rutas locales predeterminadas.




```
C:\Users\PC1> netstat -r
 <se omitió el resultado>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination          Netmask        Gateway       Interface    Metric
          0.0.0.0            0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0          255.0.0.0        On-link         127.0.0.1     306
        127.0.0.1    255.255.255.255        On-link         127.0.0.1     306
  127.255.255.255    255.255.255.255        On-link         127.0.0.1     306
     192.168.10.0      255.255.255.0        On-link     192.168.10.10     281
    192.168.10.10    255.255.255.255        On-link     192.168.10.10     281
   192.168.10.255    255.255.255.255        On-link     192.168.10.10     281
        224.0.0.0          240.0.0.0        On-link         127.0.0.1     306
        224.0.0.0          240.0.0.0        On-link     192.168.10.10     281
  255.255.255.255    255.255.255.255        On-link         127.0.0.1     306
  255.255.255.255    255.255.255.255        On-link     192.168.10.10     281
===========================================================================
 <se omitió el resultado>
```

6.2.2.1 Decisión de envío de paquetes del router

Cuando un host envía un paquete a otro, utiliza su tabla de routing para determinar a dónde enviarlo. Si el host de destino está en una red remota, el paquete se envía al gateway predeterminado.

¿Qué sucede cuando un paquete llega al gateway predeterminado, que es, por lo general, un router? El router observa su tabla de routing para determinar a dónde enviar los paquetes.

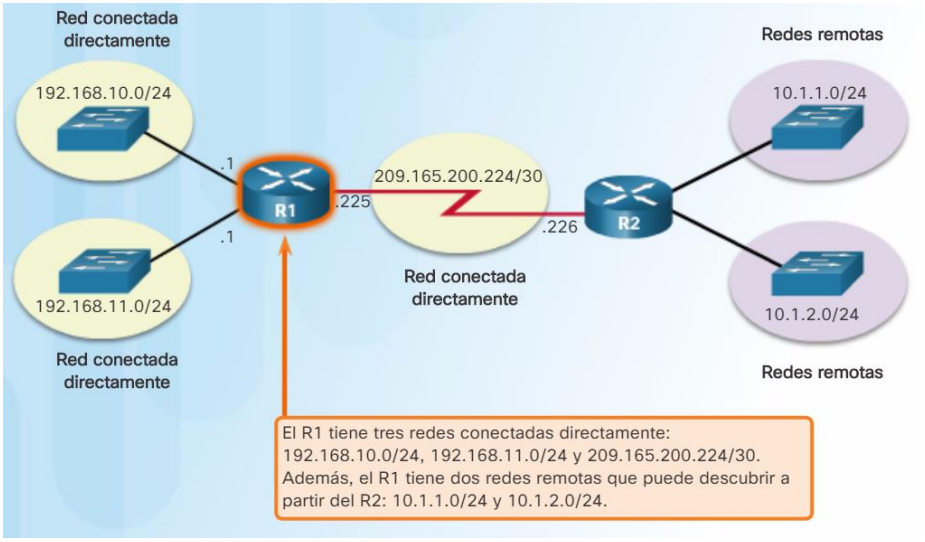
La tabla de routing de un router almacena información sobre lo siguiente:

- **Rutas conectadas directamente:** Estas rutas provienen de interfaces de router activas. Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una dirección IP y se activa. Cada una de las interfaces del router está conectada a un segmento de red diferente.

- **Rutas remotas:** Estas rutas provienen de redes remotas conectadas a otros routers. El administrador de redes puede configurar las rutas a estas redes manualmente en el router local o dichas rutas pueden configurarse de manera dinámica al permitir que el router local intercambie información routing con otros routers mediante el protocolo de routing dinámico.

- **Ruta predeterminada:** Al igual que un host, los routers también utilizan las rutas predeterminadas como último recurso si no hay otra ruta para llegar hasta la red deseada en la tabla de routing.

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



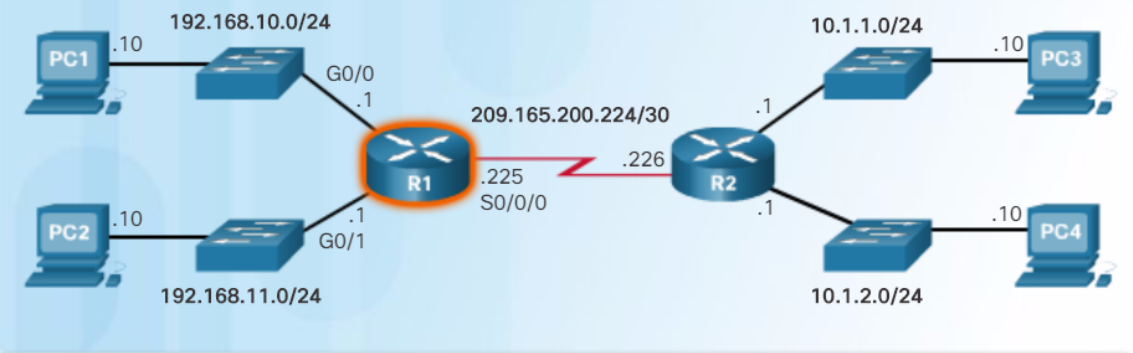
6.2.2.2 Tabla de routing del router IPv4

En un router con Cisco IOS, se puede utilizar el comando **show ip route** para visualizar la tabla de routing IPv4 del router, como se muestra en la ilustración.

Además de proveer información de routing para las redes conectadas directamente y las redes remotas, la tabla de routing tiene información sobre cómo se detectó la ruta, su confiabilidad y puntaje, cuándo fue la última vez que se actualizó y qué interfaz se debe usar para llegar al destino solicitado.

Cuando un paquete llega a la interfaz de router, el router examina el encabezado de paquetes para determinar la red de destino. Si la red de destino tiene una ruta en la tabla de routing, el router envía el paquete usando la información especificada en la tabla de routing. Si existiesen dos o más rutas posibles para llegar al mismo destino, se usa la métrica para decidir cuál aparece en la tabla de routing.

En la ilustración, se muestra la tabla de routing del R1 que se describe en el diagrama de red.




```
R1# show ip route

Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
```

6.2.2.4 Entradas de tabla de routing conectadas directamente

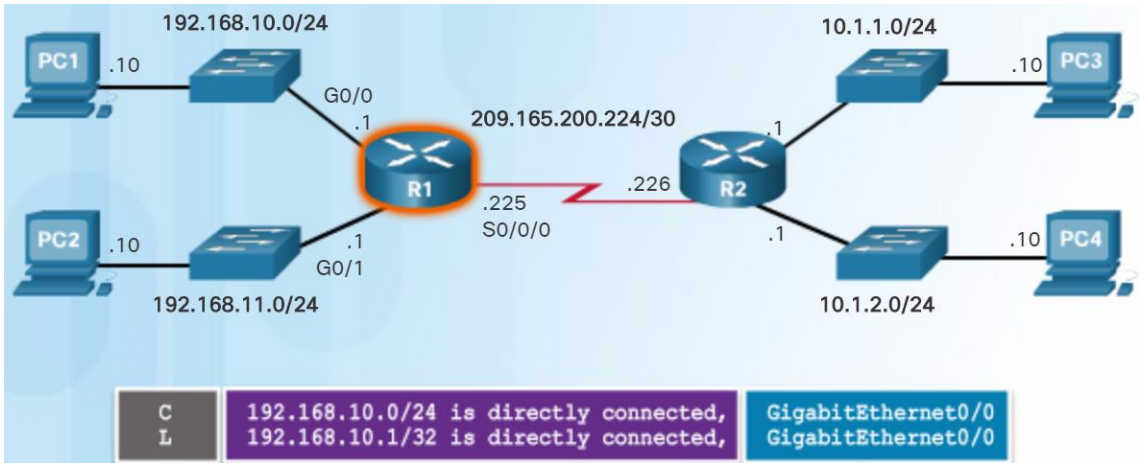
Cuando se configura una interfaz de router con una dirección IPv4, una máscara de subred y luego se la activa, se generan de manera automática las siguientes dos entradas de tabla de routing:

- **C**: Identifica una red conectada directamente. Las redes conectadas directamente se crean de manera automática cuando se configura una interfaz con una dirección IP y se la activa.

- **L**: Indica que esta es una interfaz local. Esta es la dirección IPv4 de la interfaz del router.

En la ilustración, se muestran las entradas de la tabla de routing de R1 para la red conectada directamente 192.168.10.0. Estas entradas se agregaron automáticamente a la tabla de routing cuando se configuró y se activó la interfaz GigabitEthernet 0/0. Haga clic en cada signo más para obtener más información sobre las entradas de tabla de routing conectadas directamente.

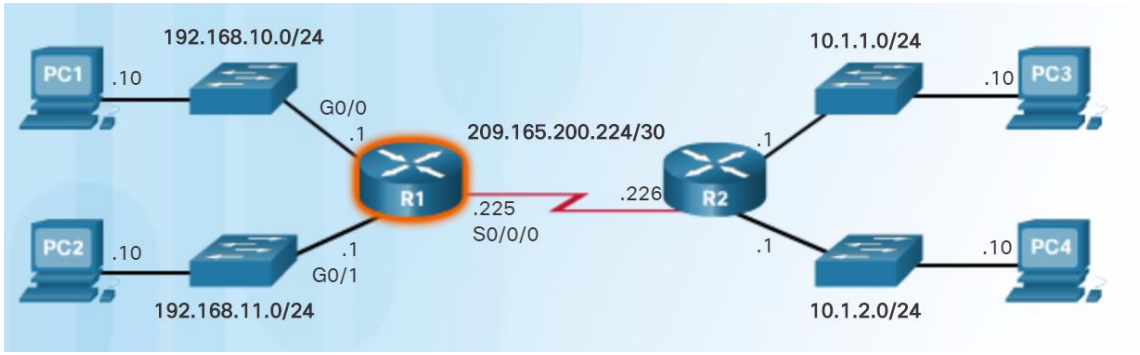
Nota: Las entradas de la interfaz local no aparecían en las tablas de routing antes de la versión 15 de IOS.



6.2.2.5 Entradas de tabla de routing de redes remotas

Un router tiene, por lo general, varias interfaces configuradas. La tabla de routing guarda información sobre las redes conectadas directamente y las remotas.

En la ilustración, se describe la ruta R1 a la red remota 10.1.1.0. Haga clic en cada signo más para obtener más información sobre las entradas de tabla de routing conectadas directamente.



- **Origen de la ruta (D)**: Identifica de qué manera el router detectó la red. Los orígenes de rutas comunes incluyen S (ruta estática), D (protocolo EIGRP) y O (Open Shortest Path First u OSPF). Otros orígenes de ruta exceden el ámbito de este capítulo.
- **Red de destino (10.1.1.0/24)**: identifica la red de destino.
- **Distancia administrativa (90)**: identifica la confiabilidad del origen de la ruta. Cuanto más bajo sea el valor, más confiable es el origen de la ruta.
- **Métrica (2170112)**: Identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Siguiente salto (209.165.200.226)**: identifica la dirección IP del router siguiente para reenviar el paquete.
- **Marca de hora de la ruta (00:00:05)**: identifica cuando fue la última comunicación con la ruta.
- **Interfaz de salida (Serial 10/0/0)**: identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

6.2.2.6 Dirección del siguiente salto

Cuando un paquete destinado a una red remota llega al router, el router hace coincidir la red de destino con una ruta de la tabla de routing. Si encuentra una coincidencia, el router envía el paquete a la dirección de siguiente salto de la interfaz identificada.

Consulte la topología de red de ejemplo de la figura 1. Suponga que la PC1 o la PC2 enviaron un paquete destinado a la red 10.1.1.0 o 10.1.2.0. Cuando el paquete llega a la interfaz Gigabit del R1, el R1 compara la dirección IPv4 de destino del paquete con las entradas de su tabla de routing. La tabla de routing se muestra en la figura 2. Según el contenido de su routing, el R1 envía el paquete por su interfaz serial 0/0/0 a la dirección de siguiente salto 209.165.200.226.

Observe cómo las redes conectadas directamente con un origen de ruta **C** y **L** no tienen dirección de siguiente salto. Esto se debe a que un router puede enviar paquetes directamente a los hosts de estas redes con la interfaz designada.

También es importante entender que los routers no pueden enviar paquetes sin una ruta a la red de destino en la tabla de routing. Si una ruta que representa la red de destino no está en la tabla de routing, el paquete se descarta (es decir, no se envía). Sin embargo, del mismo modo que un host puede usar un gateway predeterminado para reenviar un paquete a un destino desconocido, un router también puede incluir una ruta predeterminada para generar un gateway de último recurso. La ruta predeterminada puede configurarse manualmente u obtenerse de manera dinámica.

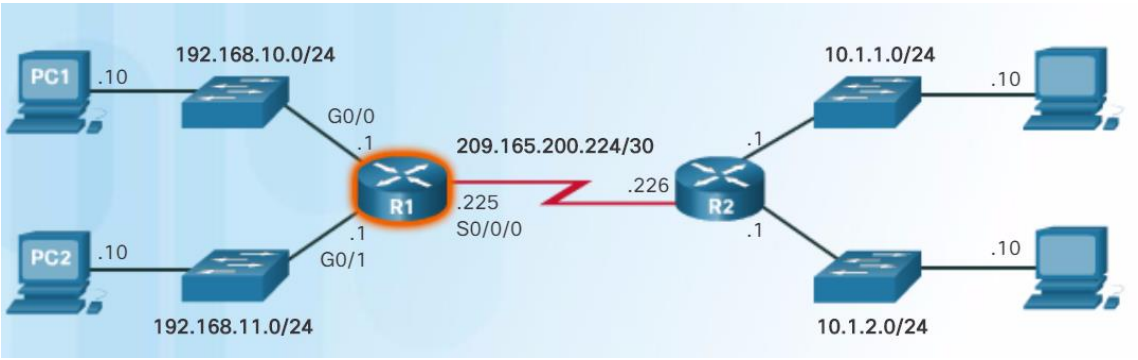


Tabla de routing del R1

```
R1# show ip route
<se omitió el resultado>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D     10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
      Serial0/0/0
D     10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
      Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0
L     192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C     192.168.11.0/24 is directly connected, GigabitEthernet0/1
L     192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

6.3.1.1 Un router es una PC

Hay muchos tipos de routers de infraestructura disponibles. De hecho, los routers Cisco están diseñados para satisfacer las necesidades de muchos tipos diferentes de redes y empresas:

- **De sucursal:** Teletrabajadores, pequeñas empresas y sitios de sucursales medianas. Incluye los routers de servicios integrados (ISR) Cisco G2 (segunda generación).
- **WAN:** Grandes empresas, organizaciones y empresas. Incluye los switches de la serie Cisco Catalyst y los routers de servicios de agregación (ASR) de Cisco.
- **Proveedor de servicios:** Grandes proveedores de servicios. Incluye los ASR Cisco, el sistema de proveedor de routing Cisco CRS-3 y los routers de la serie 7600.

La certificación CCNA se concentra en los routers de sucursal. En la ilustración, se muestran los routers de servicios integrados Cisco 1900, 2900 y 3900 G2.

Sin importar cuál sea su función, tamaño o complejidad, todos los modelos de router son, en esencia, PC. Al igual que las PC, las tabletas y los dispositivos inteligentes, los routers también necesitan lo siguiente:

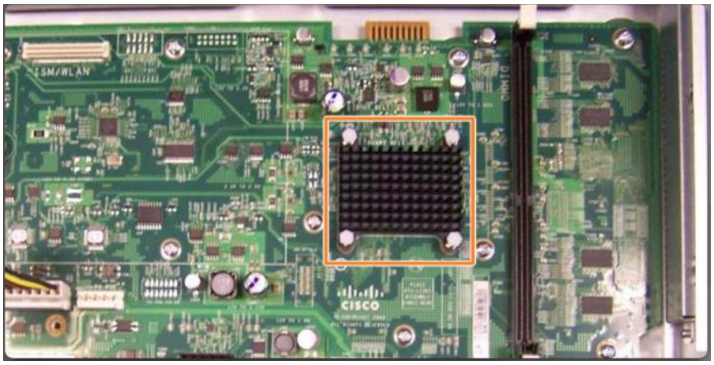
- Unidades de procesamiento central (CPU).
- Sistemas operativos (SO).
- Memoria compuesta de memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de acceso aleatorio no volátil (NVRAM) y memoria flash.

6.3.1.2 La CPU y el SO del router

Los dispositivos Cisco necesitan una CPU para ejecutar las instrucciones del SO, como la inicialización del sistema, las funciones de routing y de switching.

El componente resaltado en la ilustración es la CPU de un router Cisco de la serie 1941 con un disipador térmico acoplado. El disipador térmico ayuda a disipar el calor que genera la CPU.

La CPU necesita que un SO le provea las funciones de routing y switching. El sistema operativo Internetwork (IOS) de Cisco es el software de sistema que se usa para la mayoría de los dispositivos Cisco sin importar el tamaño y tipo de dispositivo. Se usa para routers, switches LAN, puntos de acceso inalámbrico pequeños, routers grandes con múltiples interfaces y muchos otros dispositivos.



6.3.1.3 Memoria del router

Un router tiene acceso a un almacenamiento de memoria volátil y no volátil. La memoria volátil necesita energía constante para conservar la información. Cuando el router se apaga o se reinicia, el contenido se borra y se pierde. La memoria no volátil retiene la información incluso cuando se reinicia el dispositivo.

Específicamente, un router Cisco utiliza cuatro tipos de memoria:

- **RAM:** Esta es una memoria volátil que utilizan los routers Cisco para almacenar aplicaciones, procesos y los datos necesarios para que la CPU los pueda ejecutar. Los routers Cisco usan un tipo rápido de RAM denominado "memoria sincrónica dinámica de acceso aleatorio" (SDRAM).

  La memoria RAM utiliza las siguientes aplicaciones y procesos:

  - El archivo de configuración en ejecución y la imagen de IOS.
  - La tabla de routing que se utiliza para determinar el mejor camino para reenviar paquetes.
  - La caché ARP que se usa para asignar direcciones IPv4 a las direcciones MAC.
  - El búfer de paquetes que se usa de manera temporal para almacenar paquetes antes de reenviarlos al destino.

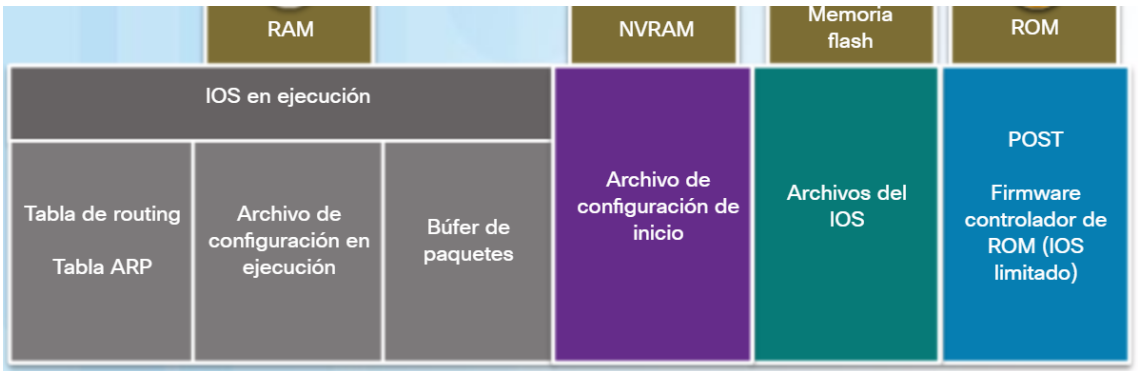
- **ROM:** Esta es una memoria no volátil que se usa para almacenar instrucciones operativas cruciales y un IOS limitado. Específicamente, la memoria ROM tiene un firmware integrado en un circuito también integrado dentro del router que solo puede modificar Cisco.

  La memoria ROM almacena lo siguiente:

  - Información de arranque que proporciona las instrucciones de inicio.
  - Autodiagnóstico al encender (POST) que evalúa todos los componentes de hardware.
  - IOS limitado para proporcionar una versión de respaldo del IOS. Se usa para cargar el IOS con todas las funciones si este se daña o elimina.

- **NVRAM**: es la memoria no volátil que se usa como almacenamiento permanente para el archivo de configuración de inicio (startup-config).

- **Flash**: es la memoria flash no volátil, y se usa como almacenamiento permanente del IOS y otros archivos relacionados con el sistema, como archivos de registro, archivos de configuración de voz, archivos HTML, configuraciones de respaldo, entre otros. Cuando se reinicia un router, se copia el IOS de la memoria flash a la RAM.

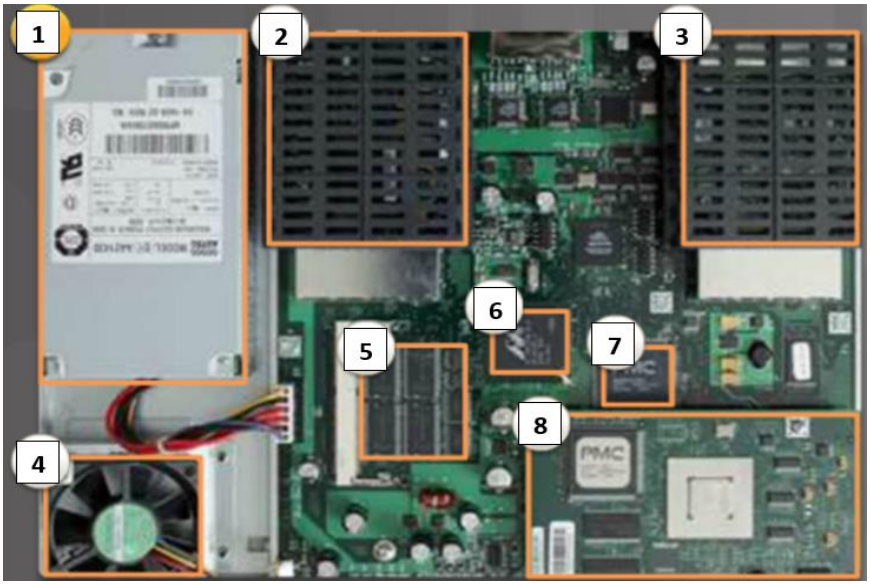


6.3.1.4 Interior de un router

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. En la ilustración, también se muestran imágenes de otros componentes que se encuentran en un router, como la fuente de alimentación, el ventilador, las pantallas térmicas y un módulo de integración avanzada (AIM), que exceden el ámbito de este capítulo.

Nota: Un profesional de redes debe conocer y comprender la función de los componentes internos principales de un router, más que la ubicación exacta de estos dentro de un router específico. Según el modelo, esos componentes se encuentran en diferentes lugares dentro del router.



1. Fuente de alimentación.

2. y 3. Protección para tarjeta de interfaz WAN (WIC) o WIC de alta velocidad (HWIC).

4. Ventilador.

5. RAM síncrona dinámica (SDRAM).

6. RAM no volátil (NVRAM).

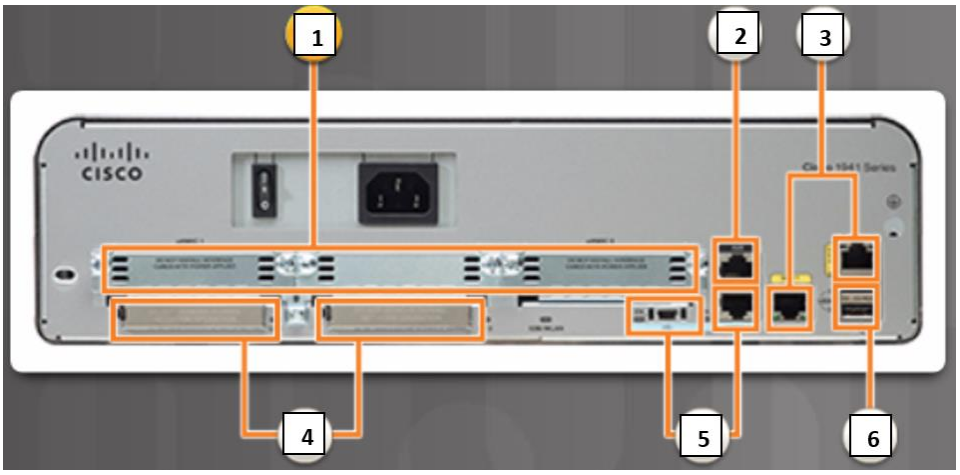
7. CPU.

8. Módulo de integración avanzado (AIM) que descarga funciones que le exigen mucha al procesador, como el cifrado desde la CPU principal.

6.3.1.5 Conexión a un router

Por lo general, los switches, routers y dispositivos Cisco interconectan muchos dispositivos. Es por este motivo que estos dispositivos tienen diferentes tipos de puertos e interfaces que se usen para conectarse al dispositivo.

Al igual que muchos dispositivos de red, los dispositivos Cisco usan indicadores de diodo emisor de luz (LED) para brindar 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 indicar que hay un problema con esa interfaz. Si una interfaz está sobrecargada, su LED está encendido permanentemente.



1. **Ranuras para tarjetas de interfaz WAN de alta velocidad mejorada (eHWIC)** con el rótulo eHWIC 0 y eHWIC 1 para proporcionar 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.

2. **Auxiliar (AUX)**: un puerto RJ-45 para el acceso a la administración remota, similar al puerto de consola. Ahora se considera un puerto antiguo ya que se usaba para admitir los módems dial up.

3. **Gigabit Ethernet**: Interfaces con el rótulo GEO/0 y GEO/1. Por lo general, se usan para proporcionar acceso LAN mediante conexión con switches y usuarios o para interconectarse a otro router.

4. **Ranuras CompactFlash**: con el rótulo CF0 y CF1 para proporcionar un mayor cantidad de espacio de almacenamiento en memoria flash expansible con tarjetas CompactFlash de hasta 4 GB por ranura. De manera predeterminada, la ranura CF0 tiene una tarjeta CompactFlash de 256 MB y es la ubicación predeterminada de arranque.

5. **Puertos de consola**: para acceder a la administración de la configuración inicial de la itnerfaz de línea de comandos (CLI). Hay dos puertos disponibles, el puerto de uso más frecuente (puerto RJ-45 común) y un nuevo conector USB de tipo B (USB mini-B). Sin embargo, solo se puede acceder a la consola por un puerto por vez.

6. **USB**: puertos con el rótulo USB 0 y USB 1 para proporcionar espacio de almacenamiento adicional similar a la memoria flash.

6.3.1.6 Interfaces WAN y LAN

Las conexiones de un router Cisco pueden agruparse en dos categorías: Interfaces de router en banda y puertos de administración. De manera similar a lo que sucede con un switch Cisco, existen diversas formas de acceder al modo EXEC del usuario en el entorno CLI de un router Cisco. Las más habituales son las siguientes:

- **Consola:** Este es un puerto de administración físico que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de mantenimiento del dispositivo.

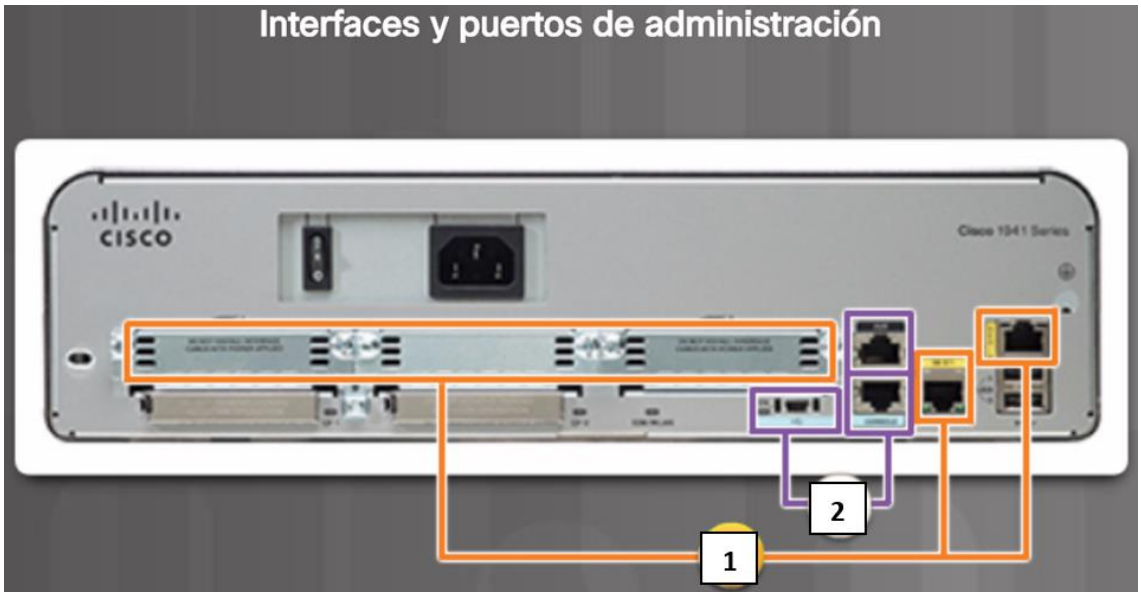
- **Shell seguro (SSH):** SSH es un método para establecer de manera remota una conexión CLI segura a través de una interfaz virtual por medio de una red. A diferencia de las conexiones de consola, las conexiones SSH requieren servicios de red activos en el dispositivo, incluida una interfaz activa configurada con una dirección.

- **Telnet:** Telnet es un método inseguro para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. A diferencia de las conexiones SSH, Telnet no proporciona una conexión cifrada de manera segura. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto no cifrado.

Nota: Algunos dispositivos, como los routers, también pueden admitir un puerto auxiliar antiguo que se haya utilizado para establecer una sesión CLI vía remota con un módem. De manera similar a la conexión de consola, el puerto auxiliar está fuera de banda y no se requieren servicios de red para configurarlo o para que esté disponible.

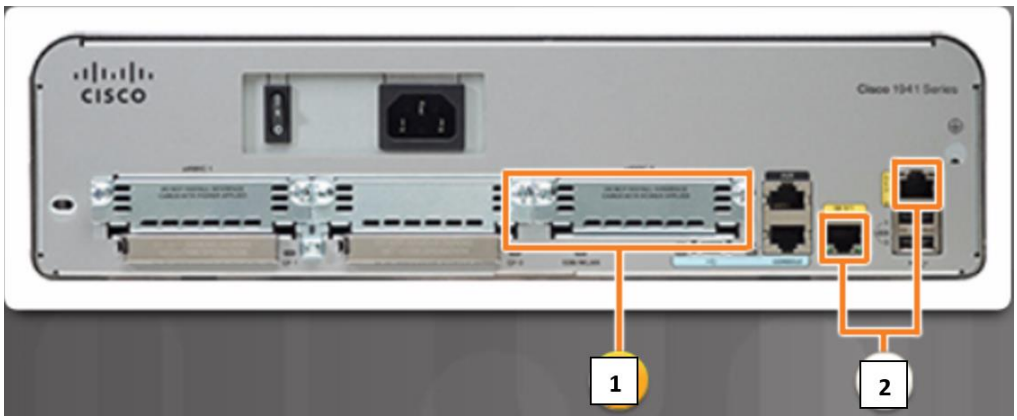
Telnet y SSH necesitan una conexión de red en banda, lo que significa que un administrador debe acceder al router a través de una de las interfaces de la red LAN o WAN.

Las interfaces en banda reciben y envían paquetes IP. Cada interfaz configurada y activa en el router es un miembro o host de una red IP diferente. Se debe configurar cada interfaz con una dirección IPv4 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.



1. **Interfaces de router en banda**: son las interfaces de la red LAN (es decir, Gigabit Ethernet) y WAN (es decir, tarjetas de interfaz WAN de alta velocidad mejorada) configuradas con la asignación de direcciones IP para transportar el tráfico de usuarios. Las itnerfaces Ethernet son las conexiones LAN más frecuentes, mientras que las conexiones WAN comunes incluyen las interfaces seriales y DSL.

2. **Puertos de administración**: Incluyen los puertos de consola y auxiliares que se usan para configurar, administrar y solucionar problemas del router. A diferencia de las interfaces de la red LAN y WAN, los puertos de administración no se utilizan para el envío de paquetes de tráfico de usuario.



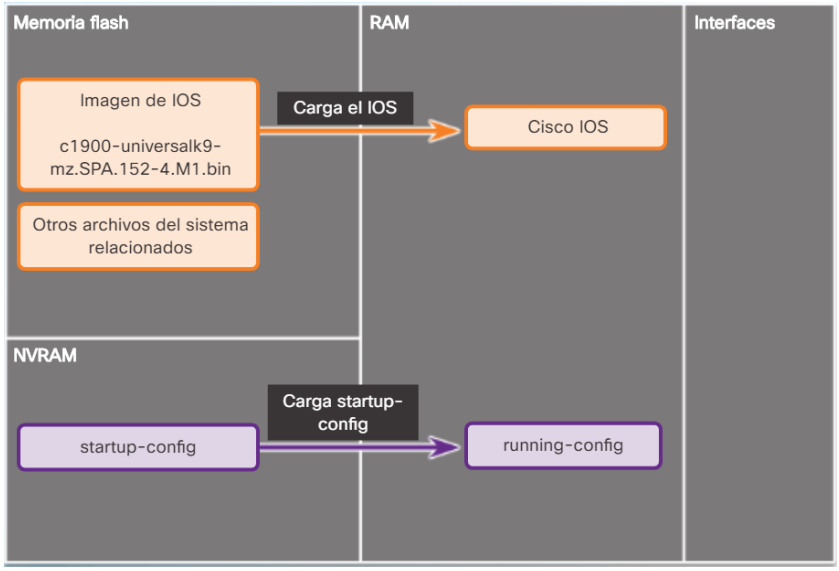
1. **Interfaces WAN seriales**: se agregan a las eHWIC0 y tienen los rótulos Serial 0 (es decir, S0/0/0) y Serial 1 (es decir, S0/0/1). Las interfaces seriales se usan para conectar los routers a una red WAN externa. Cada interfaz WAN serial tiene su propia dirección IP y su máscara de subred, que al identifican como miembro de una red específica.

2. **Interfaces de la red LAN Ethernet**: con los rótulos GE 0/0 (es decir, G0/0) y GE 0/1 (es decir, G0/1). Las interfaces Ethernet se usan para conectarse a otros dispositivos con Ethernet habilitado, lo que incluye switches, routers, firewalls, etc. Cada interfaz de la red LAN tiene su propia dirección IPv4 y su máscara de subred o una dirección IPv6 y un prefijo que la identifican como miembro de una red específica.

6.3.2.1 Archivos bootset

Tanto los switches como los routers Cisco cargan la imagen de IOS y el archivo de configuración de inicio en la RAM cuando se inician, como se muestra en la ilustración.

La configuración en ejecución se modifica cuando el administrador de redes realiza configuraciones de dispositivo. Los cambios que se hayan realizado en el archivo running-config se deben guardar en el archivo de configuración en la NVRAM, en caso de que se reinicie el router o este no reciba energía.



6.3.2.2 Proceso de arranque del router

Existen tres fases de gran importancia en el proceso de arranque:

1. Se realiza el POST y se carga el programa de arranque.

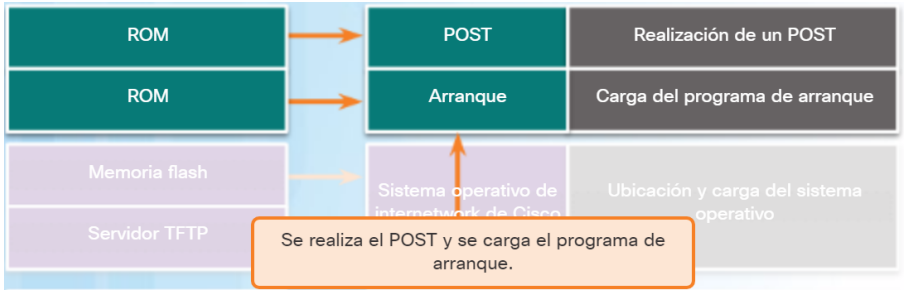
2. Se ubica y se carga el software Cisco IOS.

3. Se ubica y se carga el archivo de configuración de inicio o se ingresa al modo de configuración.

1. Realización del POST y carga del programa de arranque

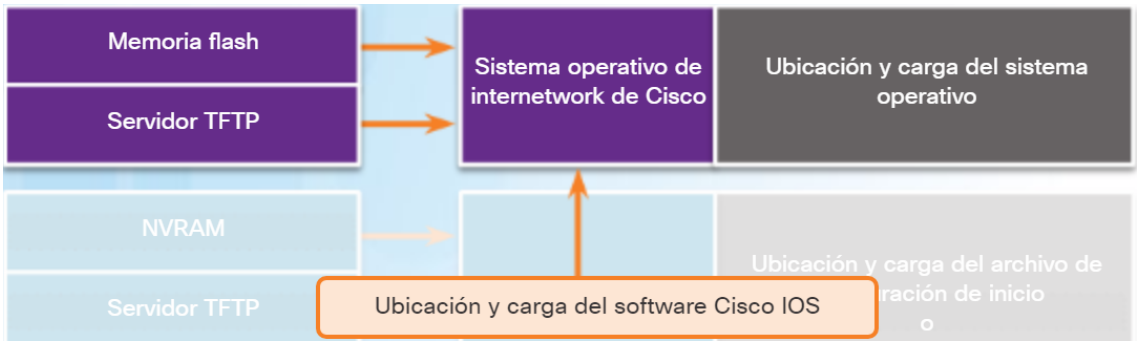
Durante el autodiagnóstico al encender (POST), el router realiza diagnósticos en la ROM sobre varios componentes de hardware, incluidas la CPU, la RAM y la NVRAM. Después del POST, el programa de arranque se copia de la ROM a la RAM. La tarea principal del programa de arranque (bootstrap) es ubicar al Cisco IOS y cargarlo en la RAM.

Nota: En este punto, si usted tiene una conexión de consola al router, comienza a ver el resultado en la pantalla.



2. Ubicación y carga de Cisco IOS

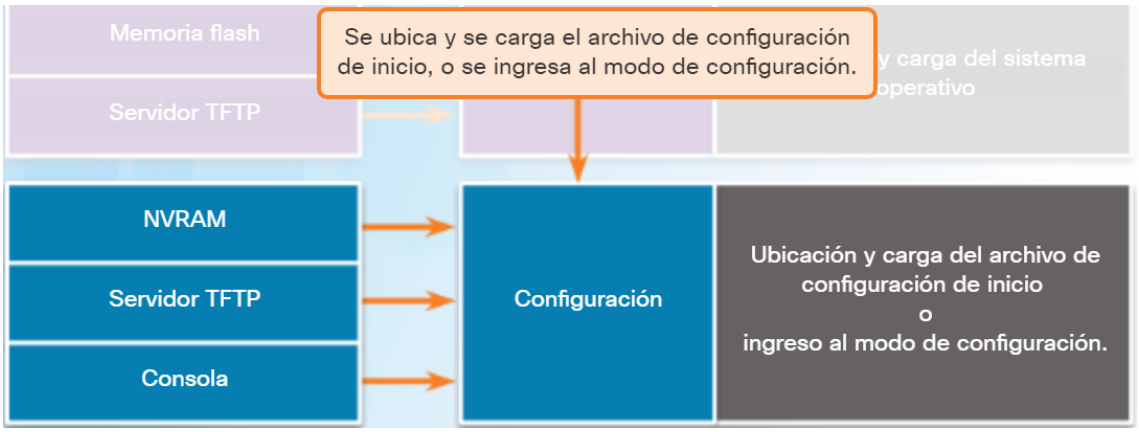
Por lo general, el IOS se almacena en la memoria flash y se copia en la RAM para que lo ejecute la CPU. Si la imagen de IOS no está en la memoria flash, el router puede buscarla con un servidor de protocolo trivial de transferencia de archivos (TFTP) Si no se puede ubicar una imagen de IOS completa, se copia un IOS limitado en la RAM, que puede usarse para diagnosticar problemas y transferir un IOS completo a la memoria flash.



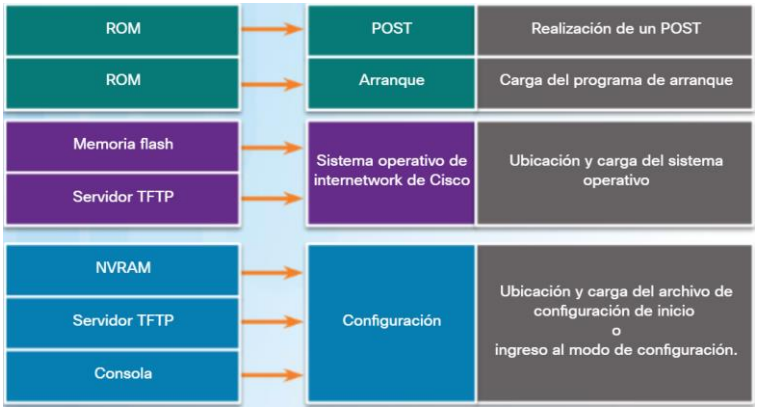
3. Ubicación y carga del archivo de configuración

El programa de arranque copia el archivo de configuración de inicio de la NVRAM a la RAM. Esto se convierte en la configuración en ejecución. Si el archivo de configuración de inicio no existe en la NVRAM, se puede configurar al router para que busque un servidor TFTP. Si no encuentra ningún servidor TFTP, el router muestra la petición de entrada del modo de configuración.

Nota: El modo de configuración no se utiliza en este curso para configurar el router. Ante la petición de entrada del modo de configuración, siempre se debe responder **no**. Si usted contesta que sí e ingresa al modo de configuración, presione **Ctrl**+**C** en cualquier momento para finalizar el proceso de configuración.



Proceso completo



6.3.2.4 Resultado de show version

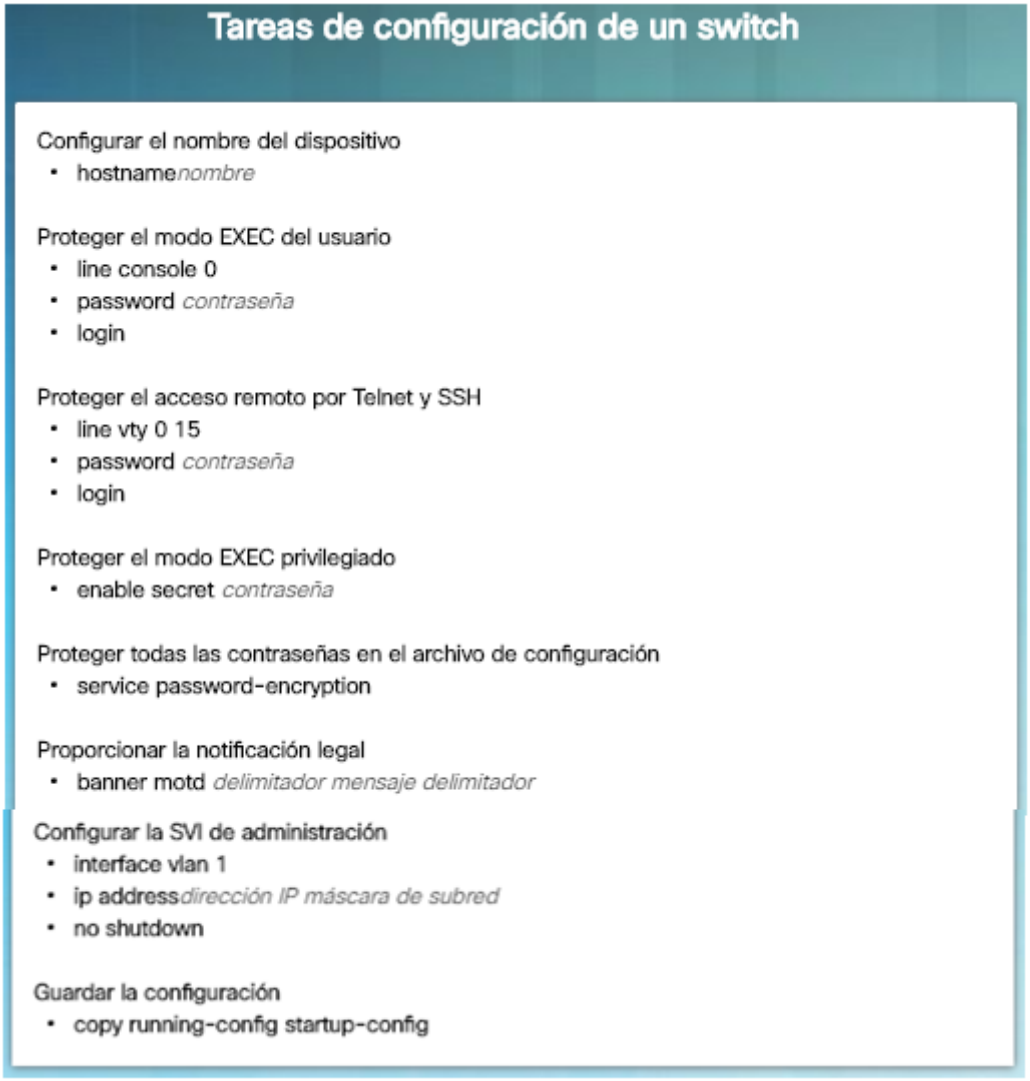
Como se muestra en la ilustración, el comando **show version** muestra información sobre la versión del software Cisco IOS que se ejecuta en ese momento en el router, la versión del programa de arranque e información sobre la configuración del hardware, incluida la cantidad de memoria del sistema.

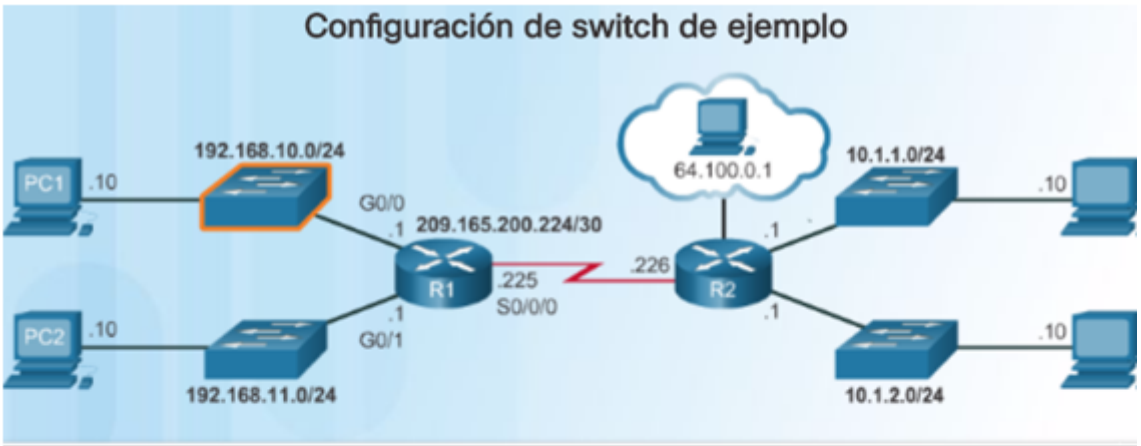
```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15,
RELEASE SOFTWARE (fc1)

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is
"flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on

               <se omitió el resultado>


Cisco CISCO1941/K9 (revision 1.0)
with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

               <se omitió el resultado>


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2142
(will be 0x2102 at next reload)

Router#
```

6.4.1.1 Pasos básicos en la configuración de un switch

Los routers y switches Cisco tienen muchas similitudes. Admiten un sistema operativo similar, estructuras de comandos similares y muchos de los mismos comandos. Asimismo, ambos dispositivos usan los mismos pasos de configuración inicial cuando se implementan en una red.

Antes de comenzar a configurar un router, revise las tareas iniciales de configuración de un switch que se indican en la figura 1. En la figura 2, se muestra una configuración de ejemplo.



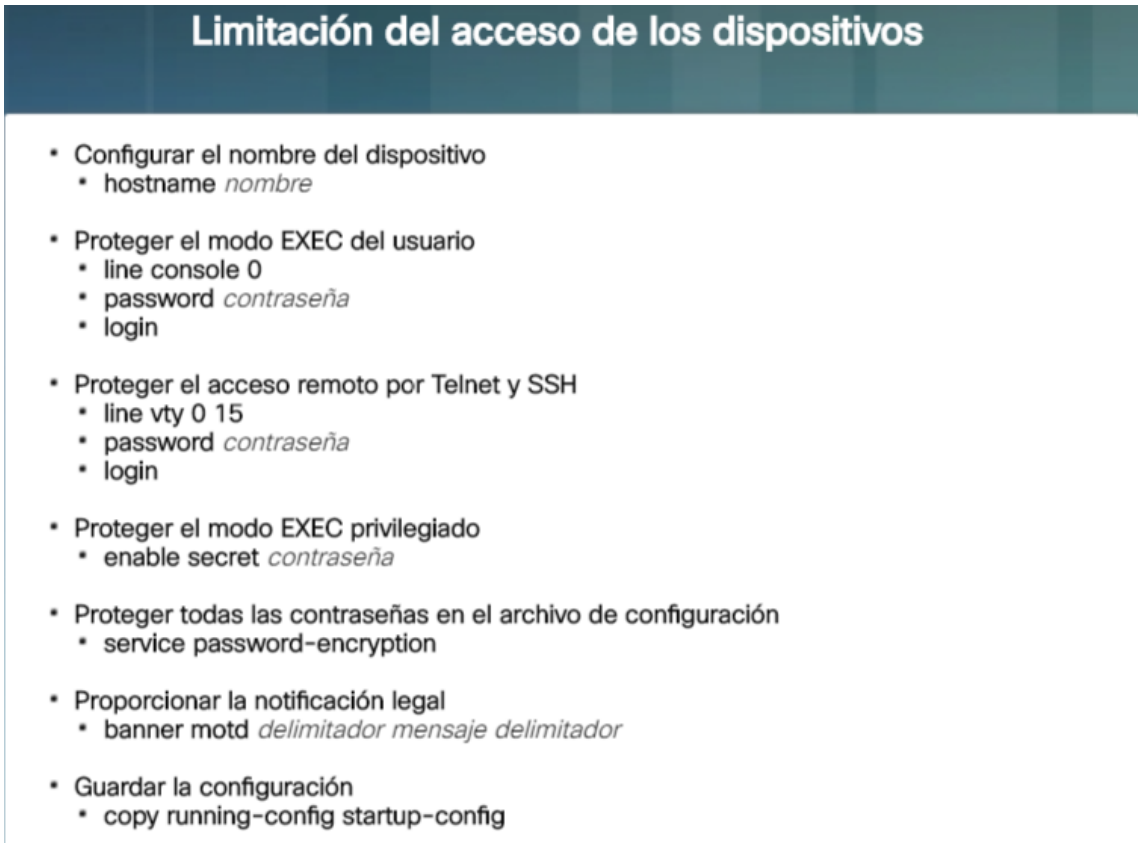


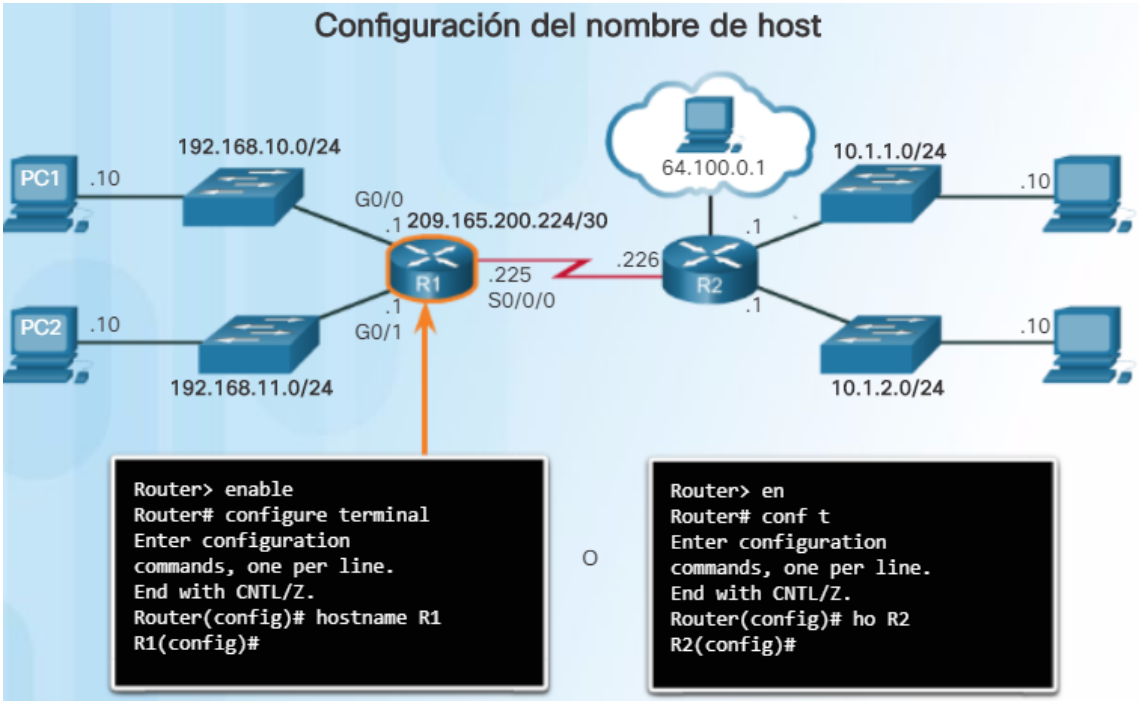

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# enable secret class
S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)# service password-encryption
S1(config)# banner motd #No unauthorized access allowed!#
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.10.50 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

6.4.1.2 Pasos básicos en la configuración de un router

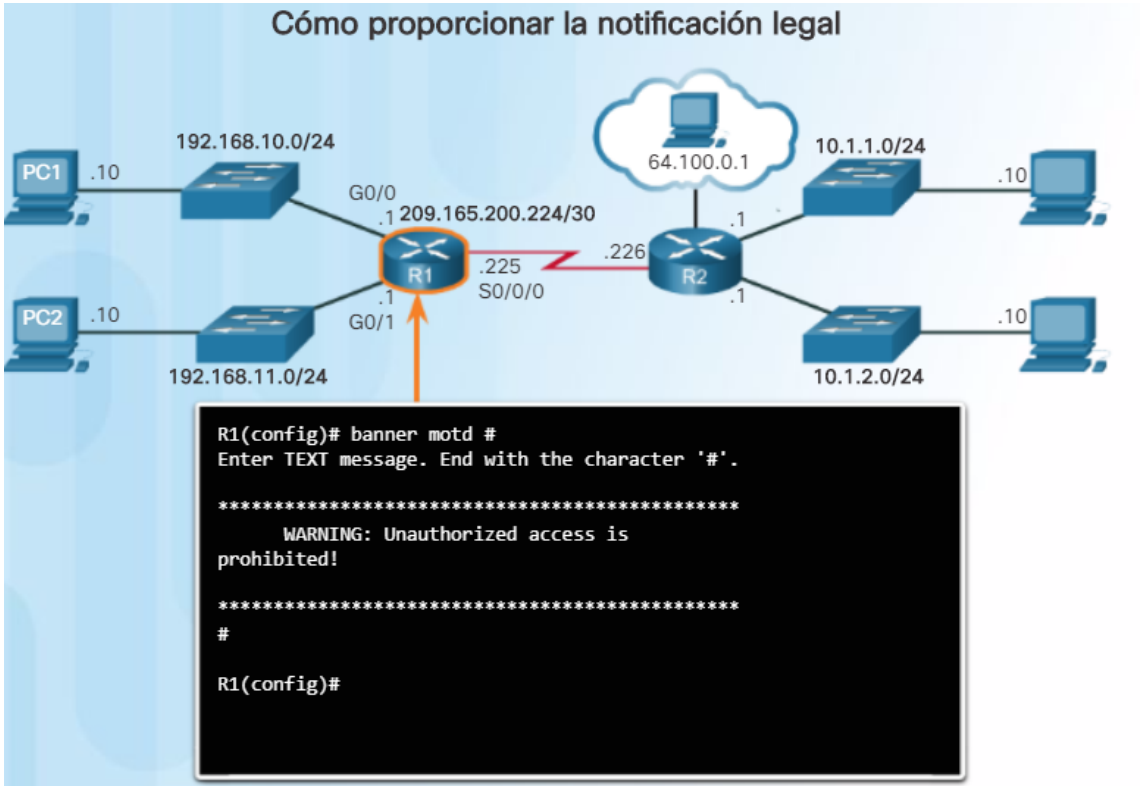
De manera similar a cuando se configura un switch, cuando se configuran los parámetros iniciales en un router, se deben completar las tareas que se indican en la figura 1.

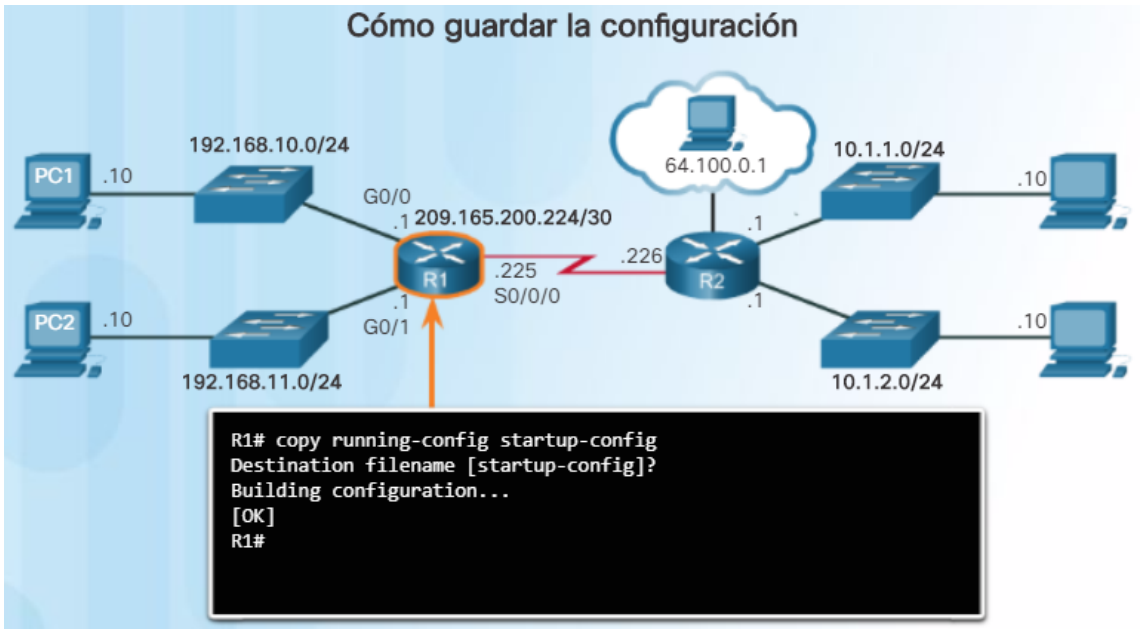
En las figuras 2 a 5, se proporciona un ejemplo de estas tareas que se configuran en un router. En la figura 2, se asigna un nombre de host al router. En la figura 3, se protegen las líneas de acceso EXEC privilegiado, EXEC del usuario y acceso remoto con una contraseña, y se cifran todas las contraseñas en el archivo de configuración. Las notificaciones legales se configuran en la figura 4. Por último, la configuración se guarda en la figura 5.




Configuración del nombre de host
192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
64.100.0.1
10.1.1.0/24
.10
.1
.226
R1
.225
S0/0/0
R2
.1
PC2
.10
.1
G0/1
.10
192.168.11.0/24
10.1.2.0/24
Router> enable
Router# configure terminal
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
O
Router> en
Router# conf t
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)# ho R2
R2(config)#


Protección del acceso de administración
192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
64.100.0.1
10.1.1.0/24
.10
.1
.226
R1
.225
S0/0/0
R2
.1
PC2
.10
.1
G0/1
.10
192.168.11.0/24
10.1.2.0/24
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#


Cómo proporcionar la notificación legal
192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
64.100.0.1
10.1.1.0/24
.10
.1
.226
.225
S0/0/0
R1
R2
.1
PC2
.10
G0/1
.1
.1
.10
192.168.11.0/24
10.1.2.0/24
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
****
WARNING: Unauthorized access is
prohibited!
****
#
R1(config)#


Cómo guardar la configuración
192.168.10.0/24
PC1
.10
G0/0
.1
209.165.200.224/30
64.100.0.1
10.1.1.0/24
.10
.1
.226
.225
S0/0/0
R1
R2
.1
PC2
.10
G0/1
.1
.1
.10
192.168.11.0/24
10.1.2.0/24
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

6.4.2.1 Configurar interfaces de routers

Para que se pueda llegar a los routers, se deben configurar las interfaces de router en banda. Existen muchos tipos diferentes de interfaces para los routers Cisco. En este ejemplo, el router Cisco de la serie 1941 tiene las siguientes características:

- **Dos interfaces Gigabit Ethernet:** GigabitEthernet 0/0 (G0/0) y GigabitEthernet 0/1 (G0/1)

- **Una tarjeta de interfaz serial WAN (WIC) que consta de dos interfaces:** serial 0/0/0 (S0/0/0) y serial 0/0/1 (S0/0/1)

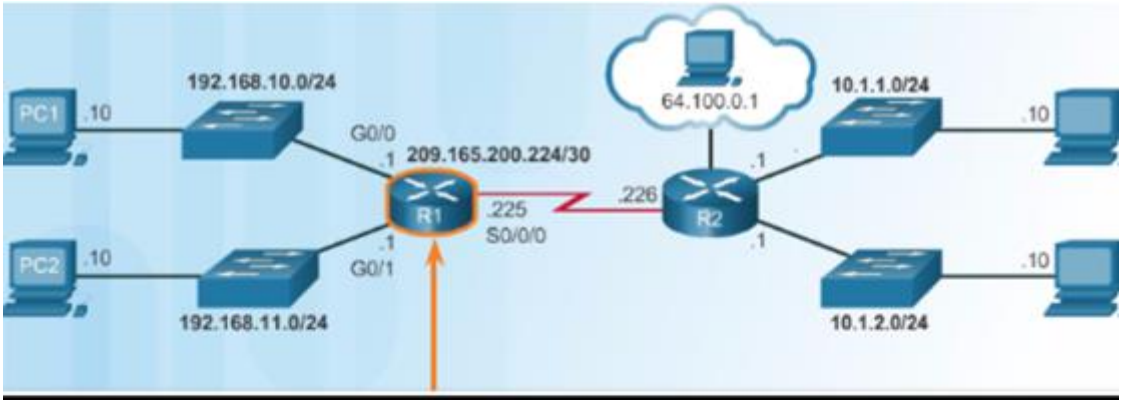
Las tareas para configurar una interfaz de router se indican en la figura 1. Observe cómo se asemeja a configurar una SVI de administración en un switch.

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 solución de problemas, dado que proporciona información con respecto al tipo de red a la que está conectada la interfaz y con respecto a otros routers que pueda haber en esa red. Si la interfaz se conecta a un ISP o a un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

Al usar el comando **no shutdown**, se activa la interfaz y es similar a darle energía. La interfaz también debe estar conectada a otro dispositivo , como un switch o un router, para que la capa física se active.

En la figura 2, se muestra la configuración de las interfaces de la red LAN conectadas al R1.

Configurar la interfaz
- interface *tipo y número*
- description *texto descriptivo*
- ip address*dirección IPv4 máscara de subred*
- no shutdown




```
R1# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0,changed state to up
R1(config-if)#exit
R1(config)#
R1(config)#int g0/1
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#des Link to LAN-11
R1(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#
```

6.4.2.2 Verificación de configuración de interfaz

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. El más útil de ellos es **show ip interface brief**. El resultado generado muestra todas las interfaces, su dirección IPv4 y el estado actual. Las interfaces configuradas y conectadas deben mostrar un estado "up" y el protocolo "up". Cualquier otra cosa indica que existe un problema con la configuración o con los cables.

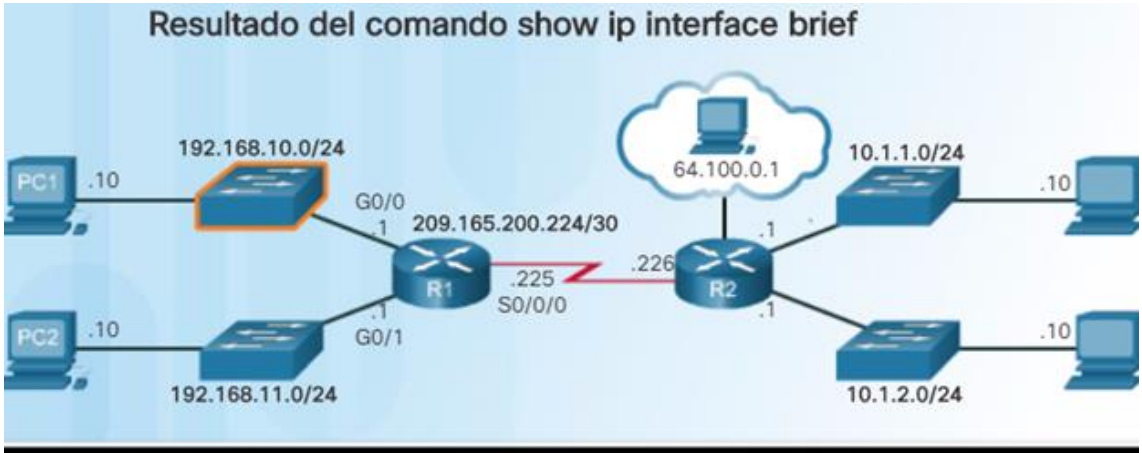
Puede verificar la conectividad de la interfaz con el comando **ping**. Los routers Cisco envían cinco pings consecutivos y miden los tiempos de ida y vuelta mínimo, máximo y promedio. Los signos de exclamación verifican la conectividad.

En la figura 1, se muestra el resultado del comando **show ip interface brief**, que muestra que las interfaces de la red LAN y el enlace WAN están activos y en funcionamiento. Observe que el comando **ping** genera cinco signos de exclamación que verifican la conectividad al R2.

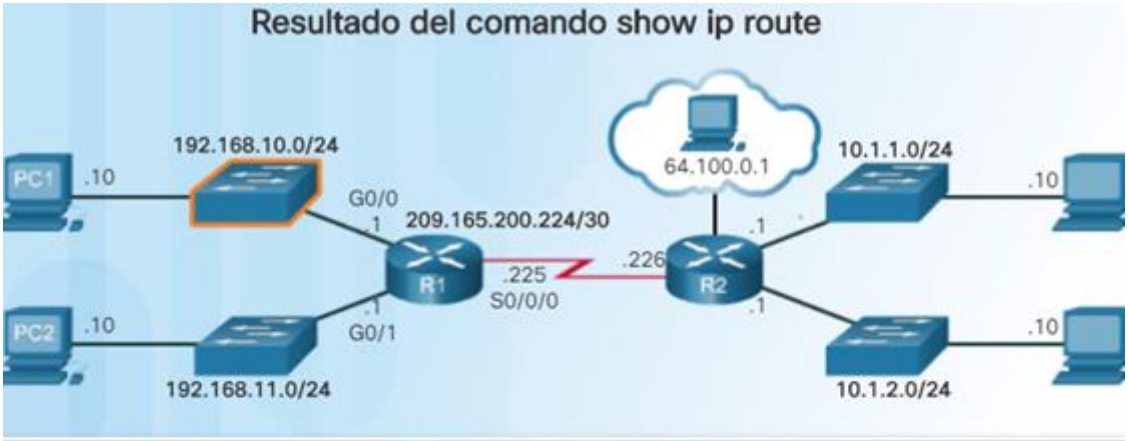
Otros comandos de verificación de interfaz pueden ser los siguientes:

- **show ip route:** Muestra el contenido de la tabla de routing IPv4 que se almacena en la RAM.
- **show interfaces:** Muestra las estadísticas de todas las interfaces de un dispositivo.
- **show ip interface:** Muestra las estadísticas IPv4 de todas las interfaces de un router.

En la figura 2, se muestra el resultado del comando **show ip route**. Observe las tres redes conectadas directamente con las direcciones IPv4 de interfaz local. Recuerde guardar la configuración con el comando **copy running-config startup-config**.



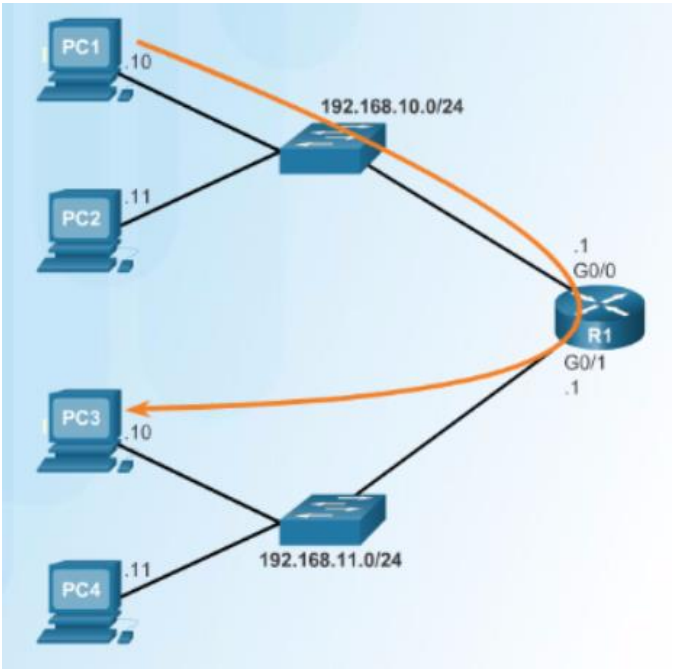

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     192.168.11.1    YES manual up                    up
Serial0/0/0            209.165.200.225 YES manual up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
 round-trip min/avg/max = 1/2/9 ms
 R1#
```




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,
       M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,  E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

6.4.3.1 Gateway predeterminado para un host

Para que un terminal 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 usa solamente cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de gateway predeterminado es la dirección de la interfaz de router conectada a la red local del host. La dirección IP del dispositivo host y la dirección de interfaz de router deben estar en la misma red.



6.4.3.2 Gateway predeterminado para un switch

Por lo general, un switch de grupo de trabajo que interconecta computadoras cliente es un dispositivo de capa 2. Como tal, un switch de capa 2 no necesita una dirección IP para funcionar adecuadamente. Sin embargo, si desea conectarse al switch y administrarlo en varias redes, debe configurar la SVI con una dirección IPv4, una máscara de subred y una dirección de gateway predeterminado.

Por lo general, la dirección del gateway predeterminado se configura en todos los dispositivos que desean comunicarse más allá de la red local. En otras palabras, para acceder de manera remota al switch desde otra red con SSH o Telnet, el switch debe tener una SVI configurado con una dirección IPv4, una máscara de subred y una dirección de gateway predeterminado. Si se accede al switch desde un host dentro de la red local, la dirección IPv4 de gateway predeterminado no es necesaria.

Para configurar un gateway predeterminado en un switch, use el comando de configuración global **ip default-gateway**. La dirección IP configurada es la de la interfaz de router del switch conectado.

En la Figura 1 se muestra un administrador que establece una conexión remota al switch S1 en otra red. El switch S1 se debe configurar con un gateway predeterminado, para que pueda responder y establecer una conexión SSH con el host administrativo.

Un concepto erróneo habitual es que el switch usa su dirección de gateway predeterminado configurada para determinar a dónde enviar los paquetes provenientes de los hosts conectados al switch y destinados a hosts de redes remotas. En realidad, la información de dirección IP y de gateway predeterminado se usa únicamente para los paquetes que se originan en el switch. Los paquetes que se originan en servidores conectados al switch ya deben crearse con la dirección de gateway predeterminado configurada en el sistema operativo de su servidor.

Utilice el verificador de sintaxis de la figura 2 para practicar la configuración de un gateway predeterminado en un switch.