

Conceptos de routing

Características de una red

Las redes tuvieron un impacto considerable en nuestras vidas. Estas cambiaron la forma en que vivimos, trabajamos y jugamos.

Las redes nos permiten comunicarnos, colaborar e interactuar como nunca antes. Utilizamos la red de distintas formas, entre ellas las aplicaciones web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.



- **Topología:** existen topologías físicas y lógicas. La topología física es la disposición de los cables, los dispositivos de red y los sistemas finales. Esta describe la forma en que los dispositivos de red se interconectan con los hilos y cables. La topología lógica es la ruta por la

cual se transfieren los datos en una red. Describe cómo aparecen conectados los dispositivos de red a los usuarios de la red.

- **Velocidad:** la velocidad mide la velocidad de datos de un enlace dado en la red en bits por segundo (b/s).
- **Costo:** el costo indica el gasto general de la adquisición de componentes de red, así como de la instalación y el mantenimiento de la red.
- **Seguridad:** la seguridad indica el nivel de protección de la red, incluida la información que se transmite a través de esta. El tema de la seguridad es importante, y las técnicas y las prácticas están en constante evolución. Siempre tenga en cuenta la seguridad cuando se tomen medidas que afecten la red.
- **Disponibilidad:** la disponibilidad es la probabilidad de que la red esté disponible para ser utilizada cuando resulte necesario.
- **Escalabilidad:** la escalabilidad indica la facilidad con la que la red puede admitir más usuarios y requisitos de transmisión de datos. Si un diseño de red está optimizado para cumplir solo con los requisitos actuales, puede resultar muy difícil y costoso satisfacer nuevas necesidades cuando la red crezca.
- **Confiabilidad:** la confiabilidad indica la fiabilidad de los componentes que crean la red, como los routers, los switches, las computadoras y los servidores. A menudo, la confiabilidad se mide como la probabilidad de fallas o como el tiempo medio entre fallas (MTBF).

Estas características y atributos proporcionan un medio para comparar distintas soluciones de redes.

¿Por qué es necesario el routing?

¿Cómo es que se logra acceder a la información deseada en pocos segundos haciendo clic en un enlace en un navegador web? Si bien existen muchos dispositivos y tecnologías que trabajan juntos de forma colaborativa para lograr esto, el dispositivo principal es el router. En pocas palabras, un router conecta una red con otra red.

La comunicación entre redes no sería posible sin un router que determine la mejor ruta hacia el destino y que reenvíe el tráfico al router siguiente en esa ruta. El router es responsable del routing del tráfico entre redes.

Los routers son computadoras

Para que la mayoría de los dispositivos con capacidad de red funcionen (por ejemplo, las computadoras, las tabletas y los smartphones), estos requieren los siguientes componentes:

- Unidad central de procesamiento (CPU)
- Sistema operativo (OS)
- Memoria y almacenamiento (RAM, ROM, NVRAM, flash, disco duro)



Básicamente, los routers son computadoras especializadas. Estos requieren una CPU y una memoria para almacenar datos de forma temporal y permanente a fin de ejecutar las instrucciones del sistema operativo, como la inicialización del sistema, las funciones de routing y de switching.

La memoria del router se clasifica como volátil o no volátil. La memoria volátil pierde su contenido cuando se apaga el dispositivo, mientras que la memoria no volátil no pierde su contenido cuando se apaga el dispositivo.

Se resumen los tipos de memoria de router, la volatilidad, y se proporcionan ejemplos de lo que se almacena en cada una.

A diferencia de las computadoras, los routers no tienen adaptadores de video o de tarjeta de sonido. En cambio, los routers cuentan con tarjetas de interfaz de red y puertos especializados para interconectar los dispositivos a otras redes.

Los routers interconectan redes

La mayoría de los usuarios desconocen la presencia de varios routers en su propia red o en Internet. Los usuarios esperan poder acceder a páginas web, enviar correo electrónico y descargar música, sin

importar si el servidor al que acceden está en su propia red o en otra. Los profesionales de redes saben que es el router el que se encarga del reenvío de paquetes de una red a otra, desde el origen inicial hasta el destino final.

Un router conecta varias redes, lo que significa que posee varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz debe usar para reenviar el paquete hacia el destino. La interfaz que usa el router para reenviar el paquete puede ser el destino final o una red conectada a otro router que se usa para llegar a la red de destino.

Los routers eligen las mejores rutas

Las funciones principales de un router son las siguientes:

- Determinar la mejor ruta para enviar paquetes.
- Reenviar paquetes a su destino

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Cuando el router recibe un paquete, analiza la dirección de destino del paquete y usa la tabla de routing para buscar la mejor ruta hacia esa red. La tabla de routing también incluye la interfaz que se debe usar para reenviar los paquetes a cada red conocida. Cuando se encuentra una coincidencia, el router encapsula el paquete en la trama de enlace de datos de la interfaz de salida, y el paquete se reenvía hacia el destino.

Un router puede recibir un paquete encapsulado en un tipo de trama de enlace de datos y reenviarlo por una interfaz que usa otro tipo de trama de enlace de datos. Por ejemplo, un router puede recibir un paquete en una interfaz Ethernet, pero debe reenviarlo por una interfaz configurada con el protocolo punto a punto (PPP). La encapsulación de enlace de datos depende del tipo de interfaz en el router y del tipo de medio al que se conecta. Las distintas tecnologías de enlace de datos a las que se puede conectar un router incluyen Ethernet, PPP, Frame Relay, DSL, tecnología de cable y tecnología inalámbrica (802.11, Bluetooth, etc.).

Mecanismos de reenvío de paquetes

Los routers admiten tres mecanismos de reenvío de paquetes:

- **Switching de procesos:** es un mecanismo de reenvío de paquetes más antiguo que todavía está disponible para los routers Cisco. Cuando un paquete llega a una interfaz, se reenvía al plano de control, donde la CPU hace coincidir la dirección de destino con una entrada de la tabla de routing y, a continuación, determina la interfaz de salida y reenvía el paquete. Es importante comprender que el router hace esto con cada paquete, incluso si el destino es el mismo para un flujo de paquetes. Este mecanismo de switching de procesos es muy lento y rara vez se implementa en las redes modernas.
- **Switching rápido:** este es un mecanismo frecuente de reenvío de paquetes que usa una memoria caché de switching rápido para almacenar la información de siguiente salto. Cuando un paquete llega a una interfaz, se reenvía al plano de control, donde la CPU busca una coincidencia en la caché de switching rápido. Si no encuentra ninguna, se aplica el switching de procesos al paquete, y este se reenvía a la interfaz de salida. La información de flujo del paquete también se almacena en la caché de switching rápido. Si otro paquete con el mismo destino llega a una interfaz, se vuelve a utilizar la información de siguiente salto de la caché sin intervención de la CPU.
- **Cisco Express Forwarding (CEF):** CEF es el mecanismo de reenvío de paquetes más reciente y más utilizado del IOS de Cisco. Al igual que el switching rápido, CEF arma una base de información de reenvío (FIB) y una tabla de adyacencia. Sin embargo, las entradas de la tabla no se activan por los paquetes como en el switching rápido, sino que se activan por los cambios, como cuando se modifica un elemento en la topología de la red. Por lo tanto, cuando se converge una red, la FIB y las tablas de adyacencia contienen toda la información que el router debe tener en cuenta al reenviar un paquete. La FIB contiene búsquedas inversas calculadas previamente, información de siguiente salto para las rutas, incluida la información de interfaz y de capa 2. Cisco Express Forwarding es el mecanismo de reenvío más rápido y la opción más utilizada en los routers Cisco.

Conexión a una red

Por lo general, los dispositivos de red y los usuarios finales se conectan a una red mediante una conexión Ethernet por cable o una conexión inalámbrica. Consulte la ilustración para ver un ejemplo de topología de referencia. Las LAN que se muestran en la ilustración sirven como ejemplo de cómo los usuarios y los dispositivos de red pueden conectarse a las redes.

Los dispositivos de la oficina doméstica pueden conectarse de la siguiente manera:

- Las computadoras portátiles y las tablet PC se conectan de forma inalámbrica a un router doméstico.

- Una impresora de red se conecta mediante un cable Ethernet al puerto de switch en el router doméstico.
- El router doméstico se conecta al cable módem del proveedor de servicios mediante un cable Ethernet.
- El cable módem se conecta a la red del proveedor de servicios de Internet (ISP).

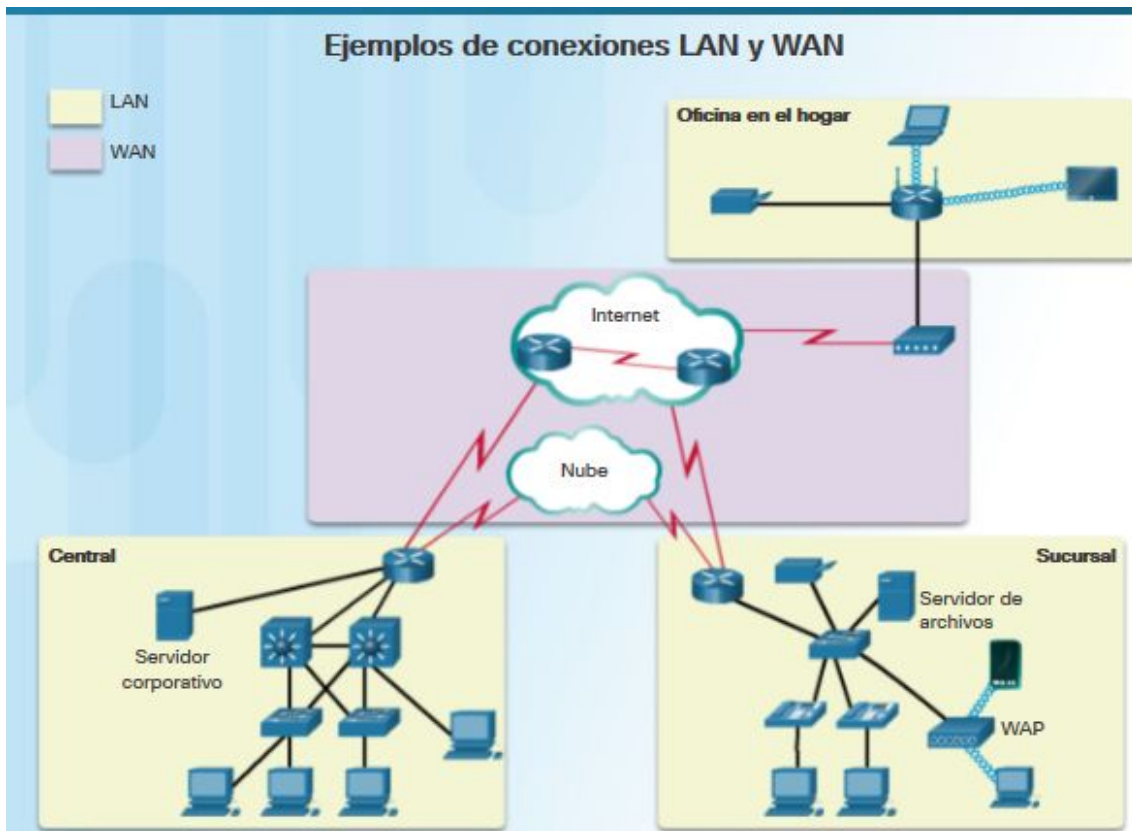
Los dispositivos de Sucursal se conectan de la siguiente manera:

- Los recursos corporativos (es decir, los servidores de archivos y las impresoras) se conectan a los switches de capa 2 mediante cables Ethernet.
- Las computadoras de escritorio y los teléfonos de voz sobre IP (VoIP) se conectan a los switches de capa 2 mediante cables Ethernet.
- Las computadoras portátiles y los smartphones se conectan de forma inalámbrica a los puntos de acceso inalámbrico (WAP).
- Los WAP se conectan a los switches mediante cables Ethernet.
- Los switches de capa 2 se conectan a una interfaz Ethernet en el router perimetral mediante cables Ethernet. Un router perimetral es un dispositivo que se encuentra en el perímetro o el límite de una red y crea rutas entre esa red y otra red, por ejemplo, entre una LAN y una WAN.
- El router perimetral se conecta al proveedor de servicios (SP) de una WAN.
- El router perimetral también se conecta a un ISP para propósitos de respaldo.

Los dispositivos del sitio Central se conectan de la siguiente manera:

- Las computadoras de escritorio y los teléfonos VoIP se conectan a los switches de capa 2 mediante cables Ethernet.
- Los switches de capa 2 se conectan de forma redundante a los switches multicapa de capa 3 con cables Ethernet de fibra óptica (conexiones anaranjadas).
- Los switches multicapa de capa 3 se conectan a una interfaz Ethernet en el router perimetral mediante cables Ethernet.
- El servidor del sitio web corporativo se conecta a la interfaz del router perimetral mediante un cable Ethernet.
- El router perimetral se conecta al SP de una WAN.
- El router perimetral también se conecta a un ISP para propósitos de respaldo.

En las LAN de los sitios Sucursal y Central, los hosts se conectan a la infraestructura de red de forma directa o indirecta (a través de WAP) mediante un switch de capa 2.



Gateways predeterminados

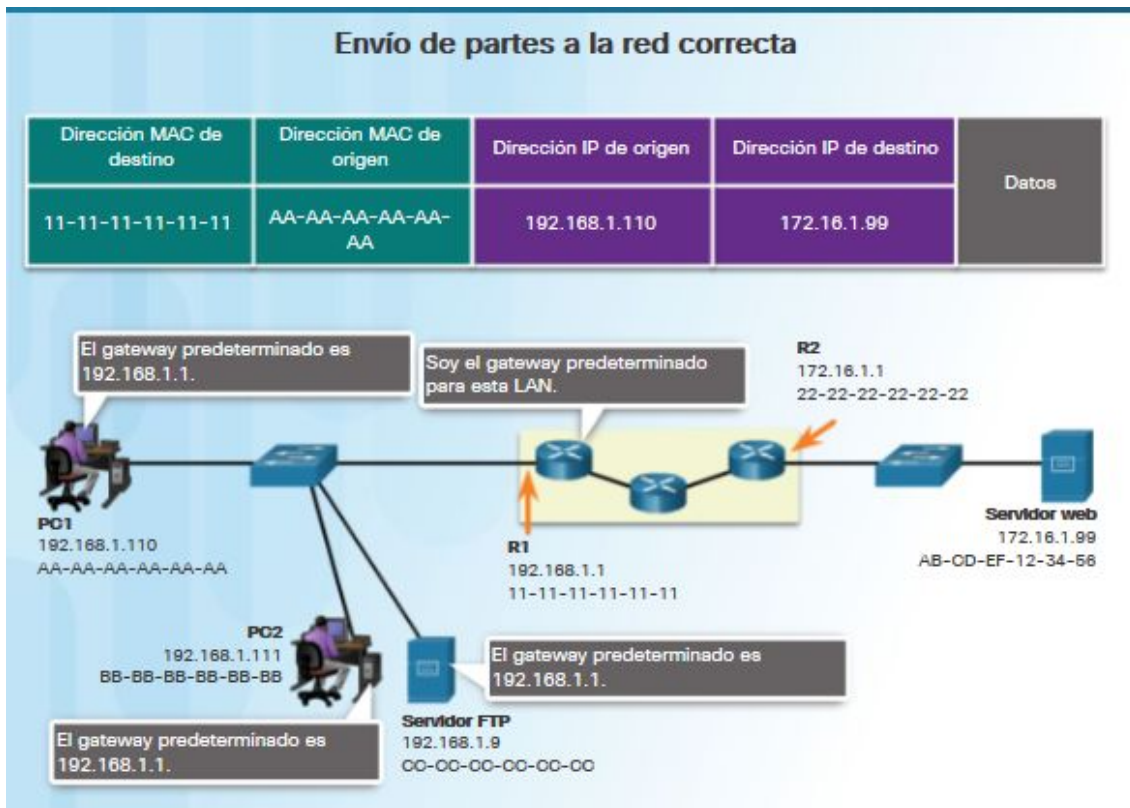
Para habilitar el acceso a la red, se deben configurar los dispositivos con la información de dirección IP para identificar los elementos correspondientes, entre ellos:

- **Dirección IP:** identifica un host único en una red local.
- **Máscara de subred:** identifica con qué subred de la red se puede comunicar el host.
- **Gateway predeterminado:** identifica la dirección IP del router al que se debe enviar un paquete cuando el destino no está en la misma subred de la red local.

Cuando un host envía un paquete a un dispositivo que está en la misma red IP, el paquete tan solo se reenvía por la interfaz del host al dispositivo de destino.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet.

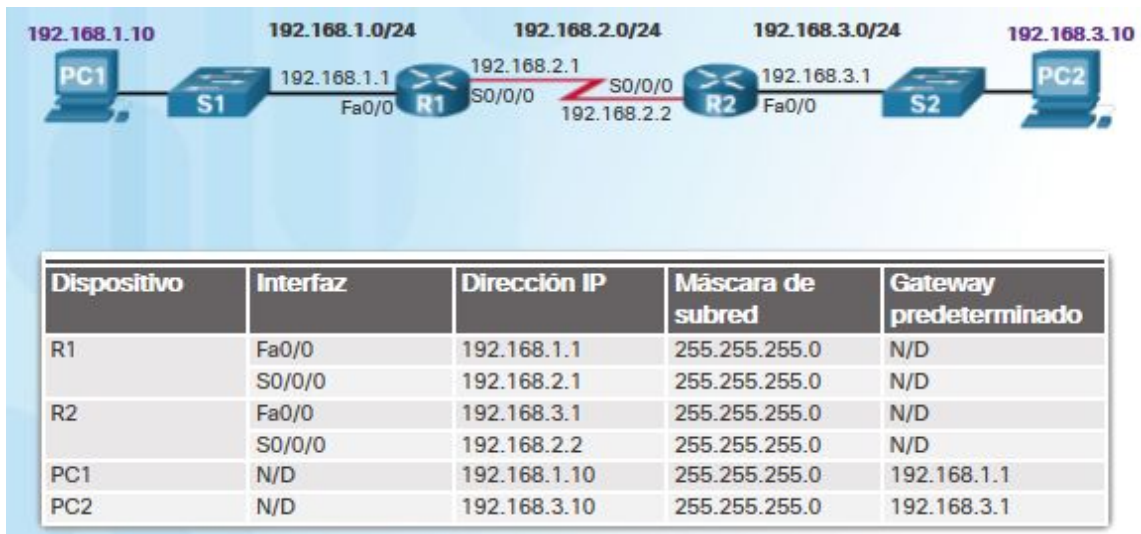
Por lo general, el gateway predeterminado es la dirección de la interfaz en el router que se conecta a la red local. El router mantiene entradas de la tabla de routing de todas las redes conectadas, así como entradas de redes remotas, y determina la mejor ruta para llegar a esos destinos.



Registro del direccionamiento de red

Cuando se diseña una nueva red o se hacen asignaciones en una red existente, es necesario documentar la red. Como mínimo, el registro debe identificar lo siguiente:

- Nombres de los dispositivos
- Interfaces usadas en el diseño
- Direcciones IP y máscaras de subred
- Direcciones de gateway predeterminado



- **Diagrama de topología:** proporciona una referencia visual que indica la conectividad física y el direccionamiento lógico de capa 3. A menudo se crea mediante software, por ejemplo, Microsoft Visio.
- **Tabla de direccionamiento:** es una tabla que captura nombres de dispositivos, interfaces, direcciones IPv4, máscaras de subred y direcciones de gateway predeterminado.

Habilitación de IP en un host

Se puede asignar información de dirección IP a un host de dos formas:

- **Estática:** se asigna la dirección IP, la máscara de subred y el gateway predeterminado correctos al host de forma manual. También se puede configurar la dirección IP del servidor DNS.
- **Dinámica:** un servidor proporciona la información de dirección IP mediante el protocolo de configuración dinámica de host (DHCP). El servidor de DHCP proporciona una dirección IP, una máscara de subred y un gateway predeterminado válidos para las terminales. El servidor también puede proporcionar otra información.

LED de dispositivos

Los equipos host se conectan a una red conectada por cable mediante una interfaz de red y un cable Ethernet RJ-45. La mayoría de las interfaces de red tienen uno o dos indicadores LED de enlace junto a

la interfaz. Generalmente, un LED verde indica una conexión correcta, mientras que un LED verde que parpadea indica actividad de red.

Si la luz de enlace no está encendida, puede existir un problema con el cable de red o con la red propiamente dicha. En el puerto del switch donde termina la conexión también hay un indicador LED encendido. Si un extremo no se enciende o ninguno lo hace, intente con otro cable de red.

Nota: la función de los LED varía entre los fabricantes de computadoras.

De manera similar, los dispositivos de infraestructura de red suelen utilizar varios indicadores LED para proporcionar una vista rápida del estado. Por ejemplo, un switch Cisco Catalyst 2960 tiene varios LED de estado para ayudar a controlar la actividad y el rendimiento del sistema. En general, estos LED están encendidos de color verde cuando el switch funciona normalmente y de color ámbar cuando funciona mal.

Los ISR Cisco utilizan distintos indicadores LED para proporcionar la información de estado. En la ilustración, se muestra un router Cisco 1941. Los LED del router ayudan al administrador de red a realizar un proceso básico de resolución de problemas. Cada dispositivo tiene un conjunto único de LED. Consulte la documentación específica de los dispositivos para obtener una descripción precisa de los LED.

Acceso a la consola

En un entorno de producción, generalmente se accede a los dispositivos de infraestructura de manera remota mediante shell seguro (SSH) o el protocolo de transferencia de hipertexto seguro (HTTPS). El acceso a la consola solo es realmente necesario para realizar la configuración inicial de un dispositivo o si el acceso remoto falla.

El acceso a la consola requiere lo siguiente:

- **Cable de consola:** cable serial RJ-45 a DB-9 o cable serial USB
- **Software de emulación de terminal:** Tera Term, PuTTY, HyperTerminal

l

El cable se conecta entre el puerto serie del host y el puerto de consola en el dispositivo. La mayoría de las computadoras portátiles y de escritorio ya no cuentan con puertos serie incorporados. Si el host no tiene ningún puerto serie, se puede utilizar el puerto USB para establecer una conexión de consola. Cuando se usa el puerto USB, se requiere un adaptador especial de puerto serie compatible USB a RS-232.

Habilitación de IP en un switch

Los dispositivos de infraestructura de red requieren direcciones IP para habilitar la administración remota. Con la dirección IP del dispositivo, el administrador de red puede conectarse al dispositivo de forma remota mediante Telnet, SSH, HTTP o HTTPS.

Los switches no tienen una interfaz dedicada a la que se pueda asignar una dirección IP. En cambio, la información de dirección IP se configura en una interfaz virtual denominada “interfaz virtual conmutada” (SVI).

Configuración de parámetros básicos del router

Los routers y 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 son similares para ambos dispositivos.

Por ejemplo, las siguientes tareas de configuración se deben realizar en todo momento:

- **Asignar un nombre al dispositivo:** para distinguirlo de otros routers.
- **Asegurar acceso de administración:** segura EXEC privilegiado, EXEC de usuario y acceso remoto.
- **Configurar un aviso:** para proporcionar notificaciones legales de acceso no autorizado.

Guarde siempre los cambios en un router y verifique la configuración básica y las operaciones del router.

Configuración de una interfaz de router IPv6

La configuración de una interfaz IPv6 es similar a la configuración de una interfaz para IPv4. La mayoría de los comandos de configuración y verificación de IPv6 del IOS de Cisco son muy similares a sus equivalentes de IPv4. En la mayoría de los casos, la única diferencia es el uso de **ipv6** en lugar de **ip** en los comandos.

Se debe realizar lo siguiente con la interfaz IPv6:

- **Configurarla con la dirección IPv6 y la máscara de subred:** utilice la dirección `ipv6 dirección-ipv6/longitud-prefijo` Comando de configuración de interfaz [**link-local | eui-64**].
- **Activar la interfaz:** la interfaz se debe activar mediante el comando **no shutdown**.

Nota: una interfaz puede generar su propia dirección link-local de IPv6 sin tener una dirección de unidifusión global mediante el comando de configuración de interfaz **ipv6 enable**.

A diferencia de IPv4, las interfaces IPv6 generalmente tienen más de una dirección IPv6. Como mínimo, los dispositivos IPv6 deben tener una dirección link-local de IPv6, pero también es muy probable que tengan una dirección de unidifusión global de IPv6. IPv6 también admite la capacidad de que una interfaz tenga varias direcciones de unidifusión global de IPv6 de la misma subred. Los siguientes comandos se pueden usar para crear, de forma estática, una dirección de unidifusión global o link-local de IPv6:

- **ipv6 address dirección-ipv6/longitud-prefijo :** crea una dirección de unidifusión global de IPv6 según lo especificado.
- **ipv6 address dirección-ipv6/longitud-prefijo eui-64:** configura una dirección de unidifusión global de IPv6 con un identificador de interfaz (ID) en los 64 bits de bajo orden de la dirección IPv6 mediante el proceso EUI-64.
- **ipv6 address dirección-ipv6/longitud-prefijo link-local:** configura una dirección link-local estática en la interfaz que se usa en lugar de la dirección link-local que se configura automáticamente cuando se asigna la dirección de unidifusión global de IPv6 a la interfaz, o cuando se habilita con el comando de interfaz **ipv6 enable**. Recuerde que el comando de interfaz **ipv6 enable** se usa para crear de forma automática una dirección link-local de IPv6, así se haya asignado una dirección de unidifusión global de IPv6 o no.

Configuración de una interfaz loopback IPv4

Otra configuración común de los routers Cisco IOS es la habilitación de una interfaz loopback.

La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado "up" (activo), siempre que el router esté en funcionamiento.

La interfaz loopback es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.

Además, la dirección IPv4 asignada a la interfaz loopback puede ser importante para los procesos en el router que usan una dirección IPv4 de interfaz con motivos de identificación, como el proceso de routing del protocolo OSPF (Open Shortest Path First). Al habilitar una interfaz loopback, el router usa la dirección de la interfaz loopback que está siempre disponible para la identificación, en lugar de una dirección IP asignada a un puerto físico que puede dejar de funcionar.

El proceso de habilitación y asignación de una dirección de loopback es simple:

```
Router(config)# interface loopback número  
Router(config-if)# dirección ip dirección-ip máscara-subred  
Router(config-if)# exit
```

Se pueden habilitar varias interfaces loopback en un router. La dirección IPv4 para cada interfaz loopback debe ser única y no la debe usar ninguna otra interfaz.

Verificación de la configuración de interfaz

Existen varios comandos **show** que se pueden usar para verificar el funcionamiento y la configuración de una interfaz. Los siguientes tres comandos son particularmente útiles para identificar de forma rápida el estado de una interfaz:

- **show ip interface brief:** muestra un resumen de todas las interfaces, incluidos la dirección IPv4 de la interfaz y el estado operativo actual.
- **show ip route:** muestra el contenido de la tabla de routing IPv4 que se almacena en la RAM. En el IOS de Cisco 15, las interfaces activas deben aparecer en la tabla de routing con dos entradas relacionadas identificadas con el código “C” (conectada) o “L” (local). En versiones anteriores de IOS, solo aparece una única entrada con el código “C”.
- **show running-config interface *interface-id* :** muestra los comandos configurados en la interfaz especificada.

- **show interfaces:** muestra información sobre la interfaz y el conteo de flujo de paquetes de todas las interfaces del dispositivo.
- **show ip interface:** muestra la información relacionada con IPv4 de todas las interfaces de un router.

Verificación de la configuración de interfaz IPv6

Los comandos para verificar la configuración de interfaz IPv6 son similares a los comandos que se usan para IPv4.

El comando **show ipv6 interface brief** muestra un resumen para cada una de las interfaces. El resultado "up/up" en la misma línea que el nombre de interfaz indica el estado de interfaz de capa 1/capa 2. Esto es lo mismo que las columnas Status (Estado) y Protocol (Protocolo) en el comando IPv4 equivalente.

El resultado muestra dos direcciones IPv6 configuradas por interfaz. Una de las direcciones es la dirección de unidifusión global de IPv6 que se introdujo manualmente. La otra, que comienza con FE80, es la dirección de unidifusión link-local para la interfaz. La dirección link-local se agrega automáticamente a una interfaz cuando se asigna una dirección de unidifusión global. Las interfaces de red IPv6 deben tener una dirección link-local, pero no necesariamente una dirección de unidifusión global.

El resultado del comando **show ipv6 interface gigabitethernet 0/0** indica el estado de interfaz y todas las direcciones IPv6 que pertenecen a la interfaz. Además de la dirección link-local y la dirección de unidifusión global, el resultado incluye las direcciones de multidifusión asignadas a la interfaz, las cuales comienzan con el prefijo FF02.

El comando **show ipv6 route** se puede utilizar para verificar si las redes IPv6 y las direcciones específicas de la interfaz IPv6 se instalaron en la tabla de routing IPv6. El comando **show ipv6 route** muestra solamente las redes IPv6, no las redes IPv4.

En la tabla de routing, una "C" junto a una ruta indica que se trata de una red conectada directamente. Cuando la interfaz de router se configura con una dirección de unidifusión global y su estado es "up/up", se agrega el prefijo y la longitud de prefijo IPv6 a la tabla de routing IPv6 como una ruta conectada.

La dirección IPv6 de unidifusión global configurada en la interfaz también se instala en la tabla de routing como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuyo destino es la dirección de la interfaz del router.

El comando **ping** para IPv6 es idéntico al comando que se utiliza con IPv4, excepto que se utiliza una dirección IPv6. Como se muestra en la Figura 4, el comando **ping** se utiliza para verificar la conectividad de capa 3 entre R1 y PC1.

Función de switching del router

Una de las funciones principales de un router es reenviar paquetes hacia su destino. Esto se logra mediante una función de switching, que es el proceso que utiliza un router para aceptar un paquete en una interfaz y reenviarlo por otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

Nota: en este contexto, el término “switching” significa literalmente mover paquetes de origen a destino y no se lo debe confundir con la función de un switch de capa 2.

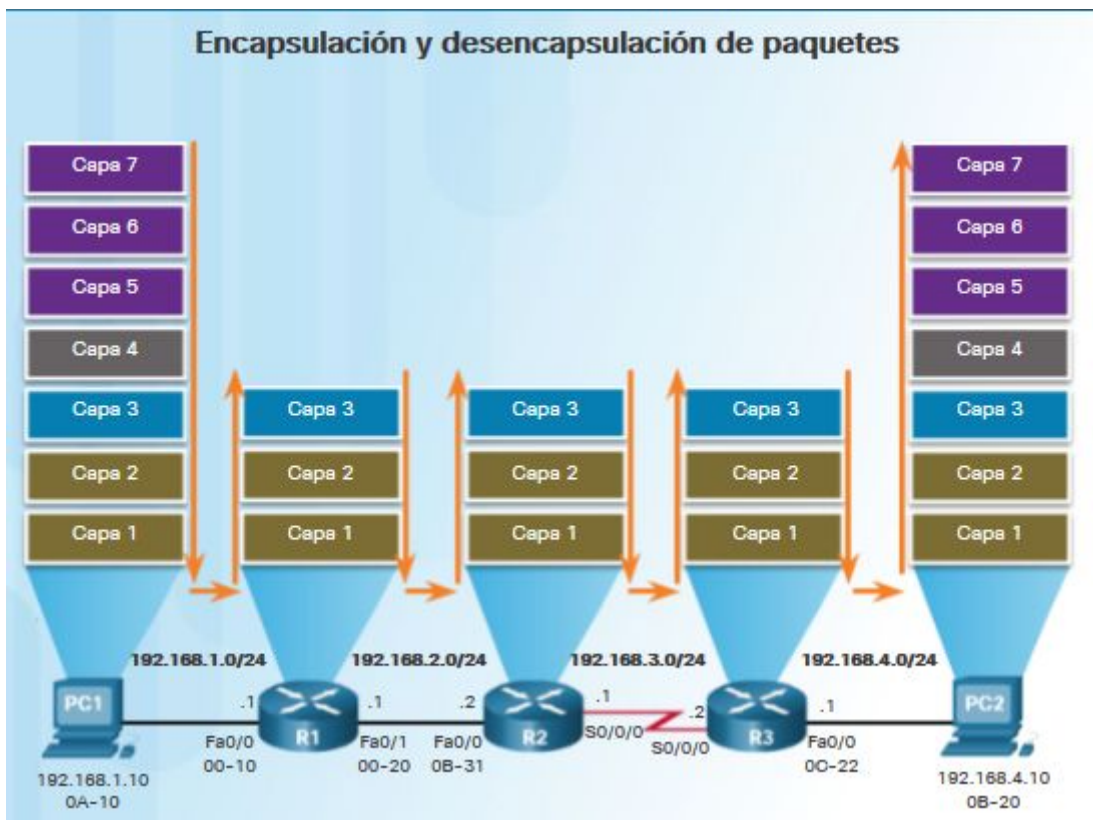
Una vez que el router determinó la interfaz de salida mediante la función de determinación de rutas, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

¿Qué hace un router cuando recibe un paquete desde una red que está destinado a otra red? El router ejecuta los siguientes tres pasos principales:

Paso 1: Desencapsula el encabezado de trama y el trailer de la capa 2 para exponer el paquete de la capa 3.

Paso 2: Examina la dirección IP de destino del paquete IP para encontrar el mejor camino en la tabla de enrutamiento.

Paso 3: Si el router encuentra una ruta hacia el destino, encapsula el paquete de capa 3 en una nueva trama de capa 2 y reenvía la trama por la interfaz de salida.



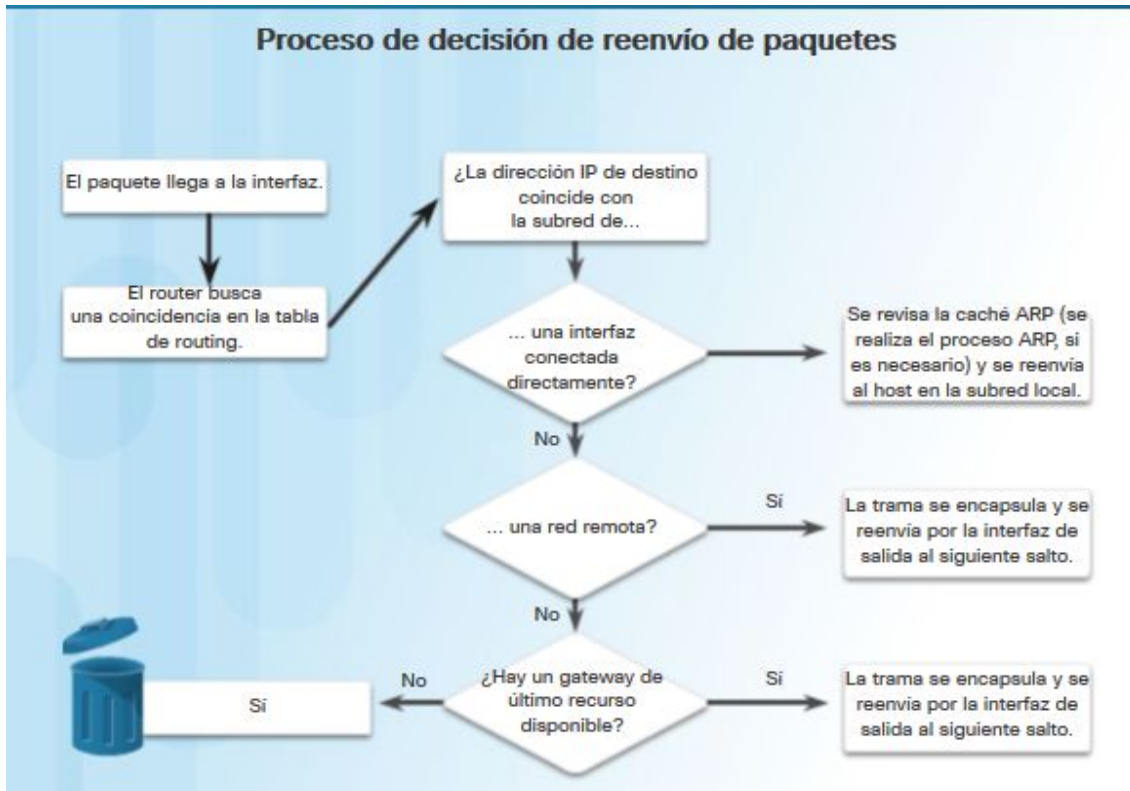
Decisiones de routing

Una de las funciones principales de los routers es determinar la mejor ruta para enviar paquetes. Para determinar la mejor ruta, el router busca en su tabla de routing una dirección de red que coincida con la dirección IP de destino del paquete.

La tabla de routing busca resultados en una de tres determinaciones de ruta:

- **Red conectada directamente:** si la dirección IP de destino del paquete pertenece a un dispositivo en una red que está conectada directamente a una de las interfaces del router, ese paquete se reenvía directamente al dispositivo de destino. Esto significa que la dirección IP de destino del paquete es una dirección host en la misma red que la interfaz del router.
- **Red remota:** si la dirección IP de destino del paquete pertenece a una red remota, el paquete se reenvía a otro router. Sólo se pueden alcanzar las redes remotas mediante el reenvío de paquetes hacia otra red.
- **Ninguna ruta determinada:** si la dirección IP de destino del paquete no pertenece a una red conectada ni remota, el router determina si se dispone de un gateway de último recurso. El gateway de último recurso se establece cuando se configura o aprende una ruta predeterminada en un router. Si hay una ruta predeterminada, el paquete se reenvía al

gateway de último recurso. Si el router no tiene una ruta predeterminada, el paquete se descarta.



El mejor camino

La determinación de la mejor ruta implica la evaluación de varias rutas hacia la misma red de destino y la selección de la ruta óptima o la más corta para llegar a esa red. Cuando existen varias rutas hacia la misma red, cada ruta utiliza una interfaz de salida diferente en el router para llegar a esa red.

El mejor camino es elegido por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Una métrica es un valor cuantitativo que se utiliza para medir la distancia que existe hasta una red determinada. El mejor camino a una red es la ruta con la métrica más baja.

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico.

A continuación, se indican algunos protocolos dinámicos y las métricas que utilizan:

- **Protocolo de información de routing (RIP):** conteo de saltos.
- **Protocolo OSPF (Open Shortest Path First):** el costo de Cisco según el ancho de banda acumulativo de origen a destino.
- **Protocolo de routing de gateway interior mejorado (EIGRP):** ancho de banda, retraso, carga, confiabilidad.

Equilibrio de carga

¿Qué sucede si una tabla de routing tiene dos o más rutas con métricas idénticas hacia la misma red de destino?

Cuando un router tiene dos o más rutas hacia un destino con métrica del mismo costo, el router reenvía los paquetes usando ambas rutas por igual. Esto se denomina “balanceo de carga de mismo costo”. La tabla de routing contiene la única red de destino pero tiene varias interfaces de salida, una para cada ruta de mismo costo. El router reenvía los paquetes utilizando las distintas interfaces de salida que se indican en la tabla de routing.

Si está configurado correctamente, el balanceo de carga puede aumentar la efectividad y el rendimiento de la red. El balanceo de carga de mismo costo puede configurarse para usar tanto protocolos de enrutamiento dinámico como rutas estáticas.

El IOS de Cisco utiliza lo que se conoce como “distancia administrativa” (AD) para determinar la ruta que se debe instalar en la tabla de routing de IP. La AD representa la “confiabilidad” de la ruta: cuanto menor sea la AD, más confiable será el origen de la ruta. Por ejemplo, la AD de una ruta estática es 1, mientras que la AD de una ruta descubierta por EIGRP es 90. El router elige la ruta con la AD más baja entre dos rutas diferentes al mismo destino. Cuando un router puede elegir entre una ruta estática y una ruta EIGRP, la ruta estática tiene prioridad. Asimismo, una ruta conectada directamente con una AD de 0 tiene prioridad sobre una ruta estática con una AD de 1.

Distancias administrativas predeterminadas

Origen de la ruta	Distancia administrativa
Conectado	0
Estática	1
Ruta resumida del protocolo EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

La tabla de routing

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

- **Rutas conectadas directamente:** estas rutas provienen de las interfaces activas del router. Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una dirección IP y se activa.
- **Rutas remotas:** estas son redes remotas conectadas a otros routers. Las rutas que van a estas redes se pueden configurar de forma estática o aprender de manera dinámica mediante protocolos de routing dinámico.

Concretamente, una tabla de routing es un archivo de datos que se encuentra en la RAM y se utiliza para almacenar información de rutas sobre redes remotas y conectadas directamente. La tabla de routing contiene asociaciones de red o de siguiente salto. Estas asociaciones le indican al router que un destino en particular se puede alcanzar de forma óptima si se envía el paquete hacia un router en particular que representa el siguiente salto en el camino hacia el destino final. La asociación del siguiente salto también puede ser la interfaz de salida hacia el siguiente destino.

Orígenes de la tabla de routing

En los routers Cisco, se puede utilizar el comando **show ip route** para mostrar la tabla de routing IPv4 de un router. Los routers proporcionan información adicional de la ruta, incluso la forma en que se

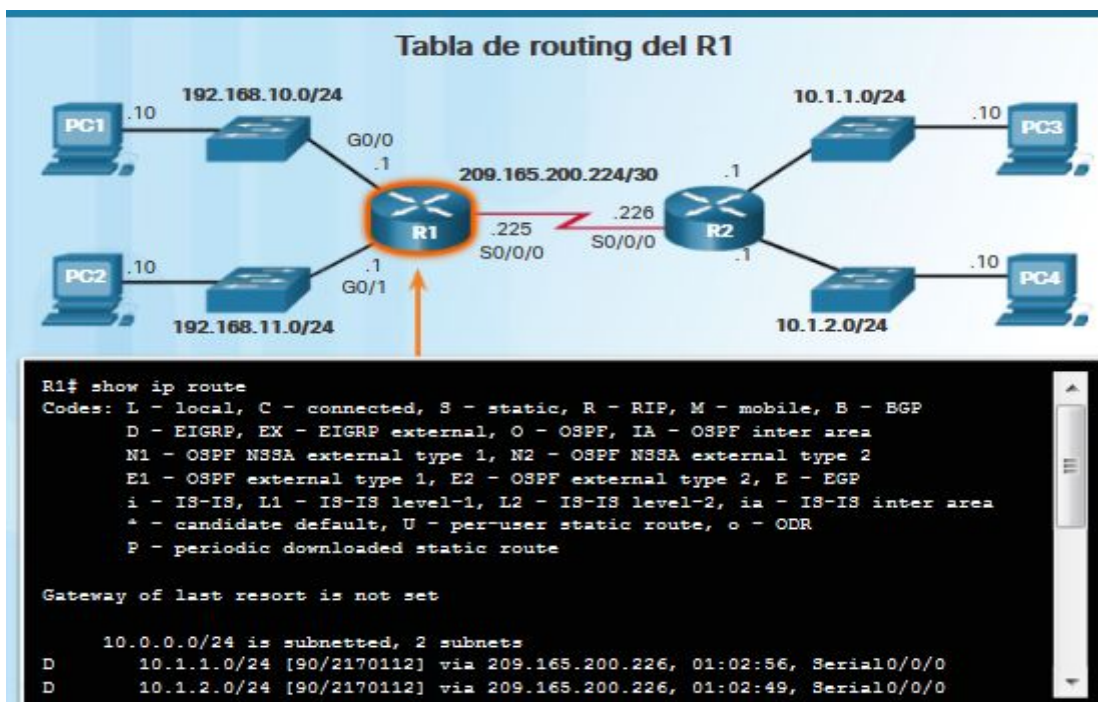
descubrió la ruta, cuánto tiempo estuvo la ruta en la tabla de routing y qué interfaz específica se debe utilizar para llegar a un destino predefinido.

Las entradas en la tabla de routing se pueden agregar como lo siguiente:

- **Interfaces de ruta local:** se agregan cuando la interfaz está configurada y activa. Esta entrada solo se muestra en la versión IOS 15 o más reciente para las rutas IPv4, y en todas las versiones de IOS para las rutas IPv6.
- **Interfaces conectadas directamente:** se agregan a la tabla de routing cuando la interfaz está configurada y activa.
- **Rutas estáticas:** se agregan cuando una ruta se configura manualmente y la interfaz de salida está activa.
- **Protocolo de routing dinámico:** se agrega cuando se implementan protocolos de routing que descubren la red de manera dinámica, como EIGRP u OSPF, y cuando se identifican las redes.

Los orígenes de las entradas de la tabla de routing se identifican con un código. El código identifica la forma en que se descubrió la ruta. Por ejemplo, los códigos frecuentes incluyen lo siguiente:

- **L:** identifica la dirección asignada a la interfaz de un router. Esto permite que el router determine de forma eficaz si recibe un paquete para la interfaz o para reenviar.
- **C:** identifica una red conectada directamente.
- **S:** identifica una ruta estática creada para llegar a una red específica.
- **D:** identifica una red que se descubre de forma dinámica de otro router con EIGRP.
- **O:** indica una red que se descubre de forma dinámica de otro router con el protocolo de routing OSPF.



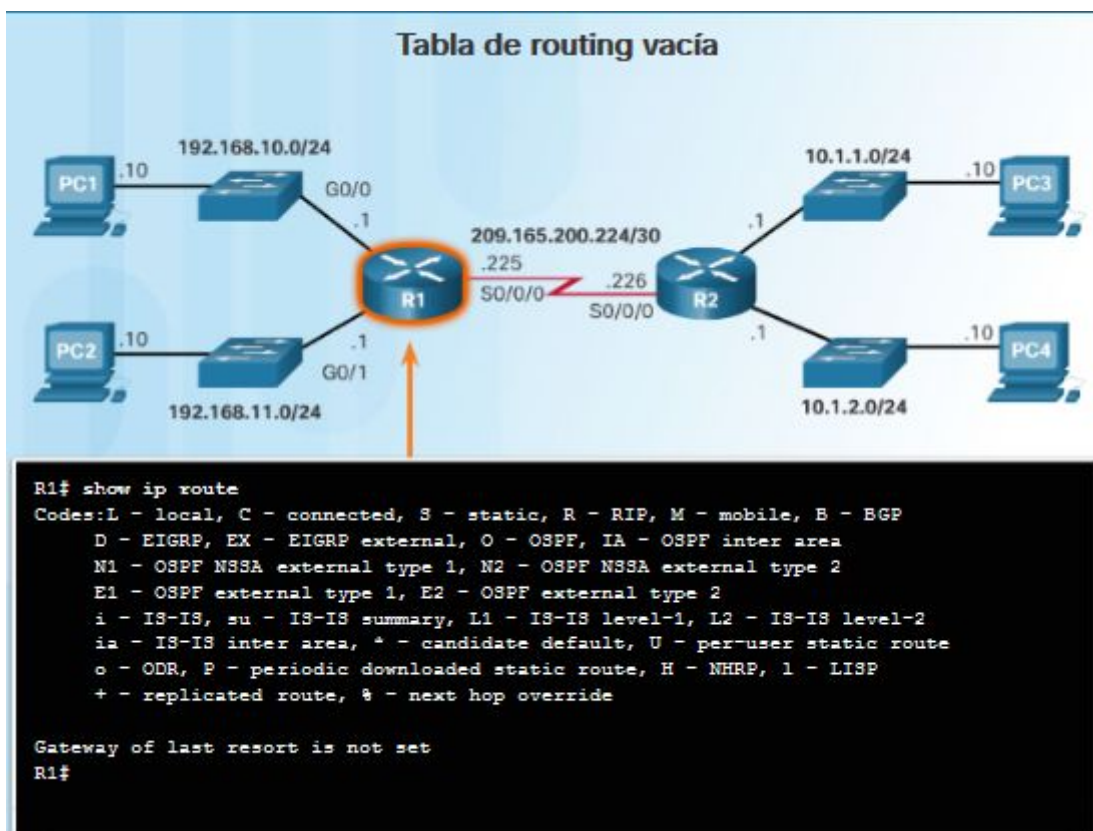
Interfaces conectadas directamente

Un router implementado recientemente, sin interfaces configuradas, tiene una tabla de routing vacía, como se muestra en la ilustración.

Antes de que el estado de la interfaz se considere up/up y se agregue a la tabla de routing IPv4, la interfaz debe cumplir con los siguientes requisitos:

- Se le debe asignar una dirección IPv4 o IPv6 válida.
- Se debe activar mediante el comando **no shutdown**.
- Debe recibir una señal portadora de otro dispositivo (router, switch, host, etc.).

Una vez que la interfaz está activa, la red de esa interfaz se incorpora a la tabla de routing como red conectada directamente.



Rutas estáticas

Después de configurar las interfaces conectadas directamente y de agregarlas a la tabla de routing, se puede implementar el routing estático o dinámico.

Las rutas estáticas se configuran de forma manual. Estas definen una ruta explícita entre dos dispositivos de red. A diferencia de los protocolos de routing dinámico, las rutas estáticas no se actualizan automáticamente y se deben reconfigurar de forma manual si se modifica la topología de la red. Los beneficios de utilizar rutas estáticas incluyen la mejora de la seguridad y la eficacia de los recursos. Las rutas estáticas consumen menos ancho de banda que los protocolos de routing dinámico, y no se usa ningún ciclo de CPU para calcular y comunicar las rutas. La principal desventaja de usar rutas estáticas es que no se vuelven a configurar de manera automática si se modifica la topología de la red.

Existen dos tipos de rutas estáticas comunes en la tabla de routing:

- Ruta estática a una red específica
- Ruta estática predeterminada

Las rutas estáticas se pueden configurar para llegar a una red remota específica. Las rutas estáticas IPv4 se configuran con el siguiente comando:

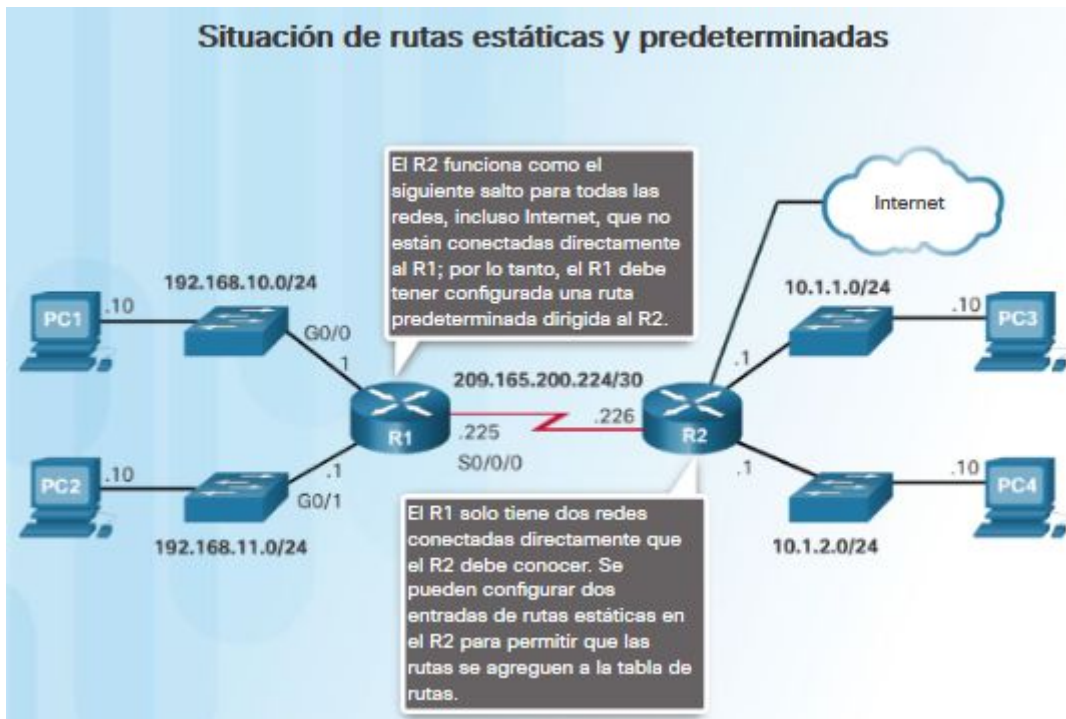
```
Router(config)# ip route network mask { next-hop-ip | exit-intf }
```

Las rutas estáticas se identifican en la tabla de routing con el código “S”.

Las rutas estáticas predeterminadas son similares a un gateway predeterminado en un host. Las rutas estáticas predeterminadas especifican el punto de salida que se debe utilizar cuando la tabla de routing no contiene una ruta para la red de destino. Las rutas estáticas predeterminadas son útiles cuando un router tiene solo un punto de salida a otro router, por ejemplo, cuando el router se conecta a un router central o a un proveedor de servicios.

Para configurar una ruta estática predeterminada IPv4, use el comando siguiente:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 { exit-intf | next-hop-ip }
```



Enrutamiento dinámico

Los routers usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de routing dinámico realizan diversas actividades, como la detección de redes y el mantenimiento de las tablas de routing.

El descubrimiento de redes es la capacidad de un protocolo de enrutamiento de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de enrutamiento. En lugar de depender de las rutas estáticas configuradas manualmente hacia redes remotas en cada router, los protocolos de routing dinámico permiten que los routers descubran estas redes de forma automática a través de otros routers. Estas redes y la mejor ruta hacia cada una se agregan a la tabla de routing del router y se identifican como redes descubiertas por un protocolo de routing dinámico específico.

Durante la detección de redes, los routers intercambian rutas y actualizan sus tablas de routing. Los routers convergen una vez que finalizan el intercambio y actualizan sus tablas de routing. Luego, los routers conservan las redes en sus tablas de routing.

Protocolos de routing IPv4

Un router que ejecuta un protocolo de routing dinámico no solo determina la mejor ruta hacia una red, sino que también determina una nueva mejor ruta si la ruta inicial se vuelve inutilizable (o si cambia la topología).

Por estos motivos, los protocolos de enrutamiento dinámico representan una ventaja sobre las rutas estáticas. Los routers que usan protocolos de enrutamiento dinámico comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin que sea necesaria la participación del administrador de la red.

Los routers Cisco admiten diversos protocolos de routing dinámico IPv4, incluidos los siguientes:

- **EIGRP:** protocolo de routing de gateway interior mejorado
- **OSPF:** abrir primero la ruta más corta
- **IS-IS:** sistema intermedio a sistema intermedio
- **RIP:** protocolo de información de routing

Protocolos de routing IPv6

Los dispositivos ISR admiten protocolos de routing dinámico IPv6, incluidos los siguientes:

- **RIPng** (RIP de última generación)
- **OSPFv3**
- **EIGRP para IPv6**

La compatibilidad con los protocolos de routing dinámico IPv6 depende del hardware y la versión del IOS. La mayoría de las modificaciones en los protocolos de routing se hacen para admitir direcciones IPv6 más largas y estructuras de encabezado diferentes.

Para habilitar que los routers IPv6 reenvíen tráfico, se debe utilizar el comando de configuración global **ipv6 unicast-routing**.