# Conceptos de routing

## Introducción

Las redes permiten que las personas se comuniquen, colaboren e interactúen de muchas maneras. Las redes se utilizan para acceder a páginas web, hablar mediante teléfonos IP, participar en videoconferencias, competir en juegos interactivos, realizar compras en Internet, completar trabajos de cursos en línea, y más.

Los switches Ethernet funcionan en la capa de enlace de datos, la capa 2, y se utilizan para reenviar tramas de Ethernet entre dispositivos dentro de una misma red.

Sin embargo, cuando las direcciones IP de origen y destino están en distintas redes, la trama de Ethernet se debe enviar a un router.

Los routers conectan una red a otra red. El router es responsable de la entrega de paquetes a través de distintas redes. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local.

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Es responsabilidad de los routers entregar esos paquetes a su debido tiempo. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de reenviar paquetes de la manera más eficiente posible.

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.

En este capítulo, también se responde a la pregunta “¿Qué hace un router con los paquetes que recibe de una red y que están destinados a otra red?”. Se examinan los detalles de la tabla de routing, incluidas las rutas conectadas, estáticas y dinámicas.

Debido a que los routers pueden enrutar paquetes entre redes, los dispositivos que están en redes distintas se pueden comunicar. En este capítulo, se presentará el router, su función en las redes, sus principales componentes de hardware y software, y el proceso de routing. Se proporcionarán ejercicios que demuestran cómo acceder al router, cómo configurar los parámetros básicos del router y cómo verificar la configuración.



## Configuración inicial de un router

### Funciones de un router

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

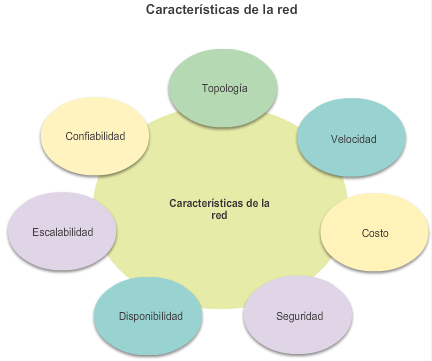
Las redes nos permiten comunicarnos, colaborar e interactuar como nunca antes. Utilizamos la red de distintas formas, entre ellas las aplicaciones web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

Como se muestra en la ilustración, existen muchas características clave relacionadas con las estructuras y el rendimiento a las cuales nos referimos cuando hablamos de redes:

* **Topología:** existen topologías físicas y lógicas. La física es la disposición de los cables, los dispositivos de red y los sistemas finales, la forma en que los dispositivos de red se interconectan con los hilos y cables. La lógica es la ruta por la cual se transfieren los datos en una red, cómo aparecen conectados los dispositivos de red a los usuarios de la red.
* **Velocidad**: mide la velocidad de datos de un enlace de 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**: Indica el nivel de protección de la red, incluida la información que se transmite a través de esta. Es importante, y las técnicas y prácticas están en constante evolución. Se debe tener en cuenta la seguridad cuando se tomen medidas que afecten la red.
* **Disponibilidad**: mide la probabilidad de que la red esté disponible para ser utilizada.
* **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**: 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).

Las características y atributos proporcionan un medio para comparar distintas soluciones de red.

**Nota:** si bien el término “velocidad” se utiliza comúnmente para referirse al ancho de banda de red, no es del todo preciso. La velocidad a la que se transmiten los bits no varía en el mismo medio. La diferencia en el ancho de banda se debe a la cantidad de bits transmitidos por segundo, no a la velocidad a la que se trasladan a través del medio cableado o inalámbrico.

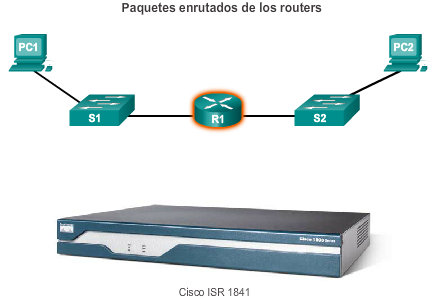
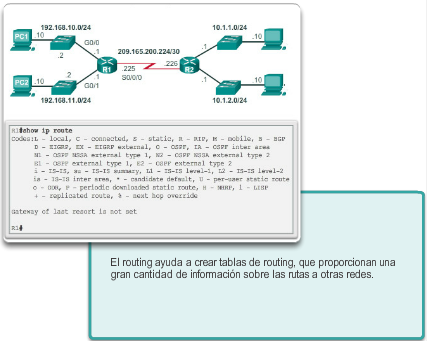


¿Cómo es que se logra acceder a la información deseada en pocos segundos haciendo clic en un enlace en un navegador web? Si bien existen muchos dispositivos y tecnologías que trabajan juntos de forma colaborativa para lograr esto, el dispositivo principal es el router. En pocas palabras, un router conecta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

En la animación de la ilustración, el diagrama de la topología de la red consta de dos hosts, dos switches y un router de servicios integrados (ISR) Cisco 1841.

Cuando un paquete llega a una interfaz del router, este utiliza la tabla de routing para determinar cómo llegar a la red de destino. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local. Es responsabilidad de los routers entregar esos paquetes de forma eficaz. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de reenviar paquetes de la manera más eficiente posible.

Para que la mayoría de los dispositivos con capacidad de red funcionen (es decir, las computadoras, las tablet PC y los smartphones), estos requieren los siguientes componentes, como se muestra en la figura 1:

* 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.

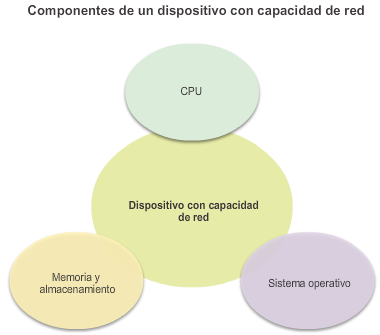
**Nota:** los dispositivos de Cisco utilizan el sistema operativo Internetwork (IOS) de Cisco como software de sistema.

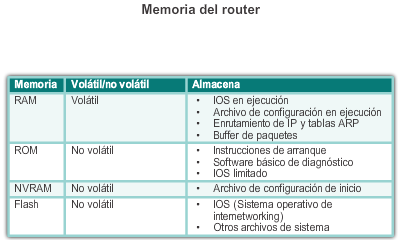
En la tabla de la figura 2, se resumen los tipos de memoria de router, la volatilidad, y se proporcionan ejemplos de lo que se almacena en cada una.

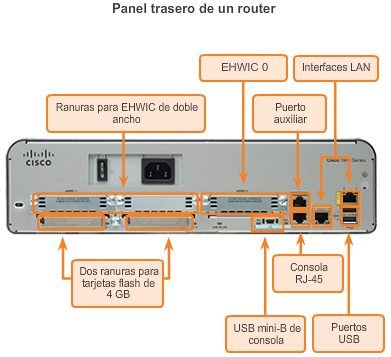
Los routers almacenan datos mediante lo siguiente:

* **Memoria de acceso aleatorio (RAM):** proporciona almacenamiento temporal para una variedad de aplicaciones y procesos, entre ellos, el IOS en ejecución, el archivo de configuración en ejecución, las diversas tablas y los búferes para el procesamiento de paquetes. Es volátil porque pierde su contenido cuando se apaga el dispositivo.
* **Memoria de solo lectura (ROM):** proporciona almacenamiento permanente para las instrucciones de arranque, el software de diagnóstico básico y un IOS limitado en caso de que el router no pueda cargar el IOS con todas las funciones. Consiste en un firmware y es no volátil, debido a que no pierde el contenido cuando se apaga el dispositivo.
* **Memoria de acceso aleatorio no volátil (NVRAM):** proporciona almacenamiento permanente para el archivo de configuración de inicio (startup-config). Es no volátil y no pierde el contenido cuando se apaga el dispositivo.
* **Flash:** proporciona almacenamiento permanente para el IOS y otros archivos relacionados con el sistema. El IOS se copia de la memoria flash a la RAM durante el proceso de arranque. Es no volátil y no pierde el contenido cuando se apaga el dispositivo.

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. En la figura 3, se identifican algunos de estos puertos e interfaces.







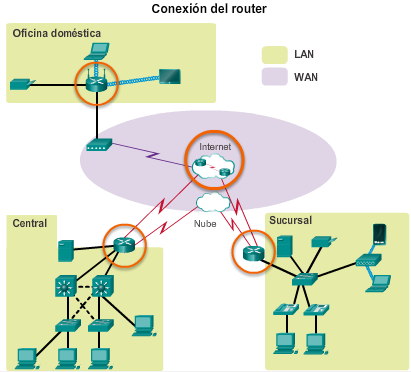
La mayoría de los usuarios desconocen la presencia de varios routers en su propia red o en Internet. Los usuarios esperan poder acceder a páginas web, enviar correo electrónico y descargar música, sin importar si el servidor al que acceden está en su propia red o en otra. Los profesionales de redes saben 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 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.

En la animación de la figura 1, se observa que el R1 y el R2 son responsables de recibir el paquete en una red y reenviarlo desde otra red hacia la red de destino.

Generalmente, cada red a la que se conecta un router requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de redes de área local (LAN) y redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como computadoras, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, las conexiones WAN suelen utilizarse para conectar una LAN a la red del proveedor de servicios de Internet (ISP).

Cada sitio de la figura 2 requiere el uso de un router para interconectarse a otros sitios. Incluso la oficina doméstica requiere un router. En esta topología, el router ubicado en la oficina doméstica es un dispositivo especializado que lleva a cabo varios servicios para la red doméstica.



Las funciones principales de un router son las siguientes:

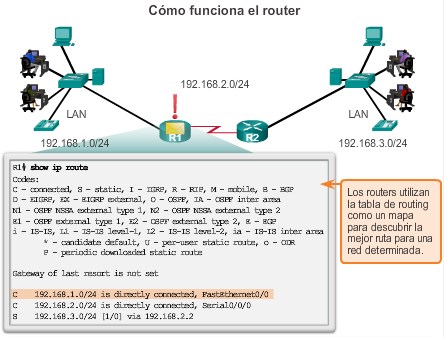
* Determinar la mejor ruta para enviar paquetes.
* Reenviar paquetes a su destino.

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).

En la animación de la ilustración, se sigue un paquete desde la computadora de origen hasta la computadora de destino. Debe observarse que el router es responsable de encontrar la red de destino en su tabla de enrutamiento y reenviar el paquete hacia su destino. En este ejemplo, el router R1 recibe el paquete encapsulado en una trama de Ethernet. Después de desencapsular el paquete, el R1 usa la dirección IP de destino del paquete para buscar una dirección de red que coincida en su tabla de routing. Luego de encontrar una dirección de red de destino en la tabla de enrutamiento, R1 encapsula el paquete dentro de una trama PPP y reenvía el paquete a R2. El R2 realiza un proceso similar.

**Nota:** los routers usan rutas estáticas y protocolos de routing dinámico para descubrir redes remotas y crear sus tablas de routing.



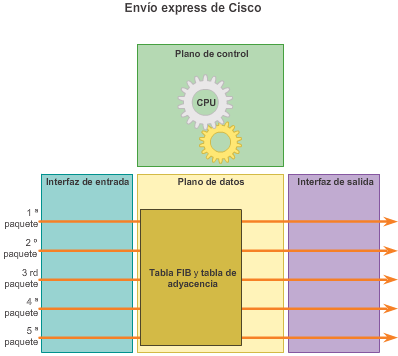
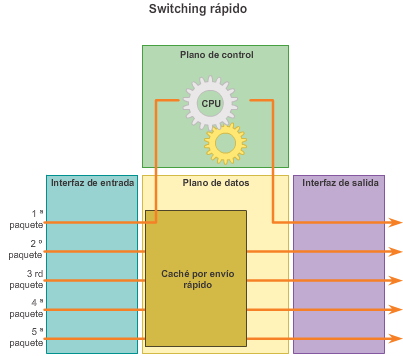
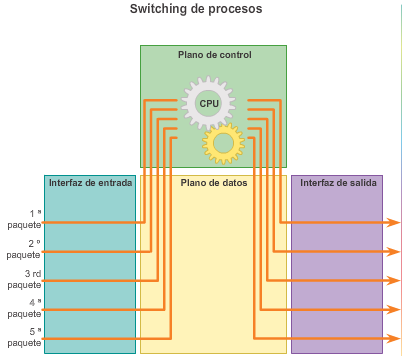
Los routers admiten tres mecanismos de reenvío de paquetes:

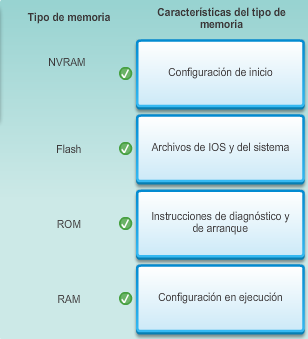
* **Switching de procesos:** es un mecanismo de reenvío de paquetes más antiguo que todavía está disponible para los routers Cisco. Cuando un paquete llega a una interfaz, se reenvía al plano de control, donde la CPU hace coincidir la dirección de destino con una entrada de la tabla de routing y, a continuación, 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.

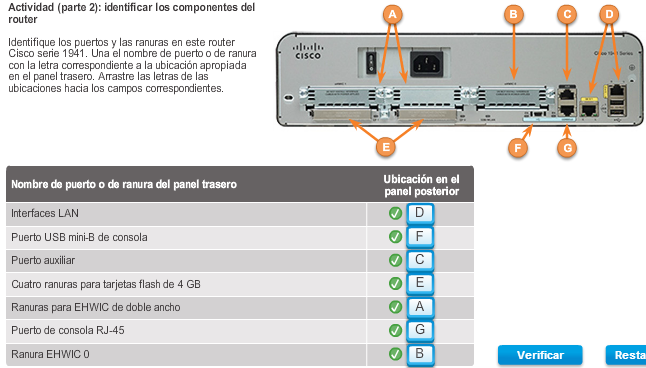
En las figuras 1 a 3, se muestran las diferencias entre los tres mecanismos de reenvío de paquetes. Suponga que hay un flujo de tráfico que consta de cinco paquetes que van hacia el mismo destino. Como se muestra en la figura 1, con el switching de procesos, la CPU debe procesar cada paquete en forma individual. Compare esto con el switching rápido, el cual se muestra en la figura 2. Con el switching rápido, observe que el switching de procesos se aplica solo al primer paquete de un flujo, el cual se agrega a la caché de switching rápido. Los cuatro paquetes siguientes se procesan rápidamente según la información de la caché de switching rápido. Por último, en la figura 3, se observa que CEF crea la FIB y las tablas de adyacencia una vez que se converge la red. Los cinco paquetes se procesan rápidamente en el plano de datos.

Una analogía frecuente que se usa para describir los tres mecanismos de reenvío de paquetes es la siguiente:

* El switching de procesos resuelve un problema realizando todos los cálculos matemáticos, incluso si los problemas son idénticos.
* El switching rápido resuelve un problema realizando todos los cálculos matemáticos una vez y recuerda la respuesta para los problemas posteriores idénticos.
* CEF soluciona todos los problemas posibles antes de tiempo en una hoja de cálculo.







### Conexión de los Dispositivos

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:

* Computadoras portátiles y tablet PC se conectan de forma inalámbrica al router doméstico.
* Impresora de red conectada por cable Ethernet al puerto de switch en el router doméstico.
* El router doméstico conectado al cable módem del proveedor mediante cable Ethernet.
* El cable módem se conecta a la red del proveedor de servicios de Internet (ISP).

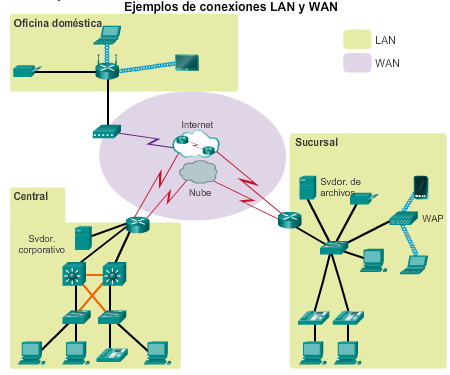
Los dispositivos de Sucursal se conectan de la siguiente manera:

* 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, **EJ:** 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 sito 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.



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 el 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 las redes conectadas, así como entradas de redes remotas, y determina la mejor ruta para llegar a esos destinos.

Por ejemplo, si la PC1 envía un paquete al Web Server (Servidor web) ubicado en 176.16.1.99, descubrirá que este no está en la red local y, por lo tanto, debe enviar el paquete a la dirección de control de acceso a los medios (MAC) de su gateway predeterminado. La unidad de datos del protocolo (PDU) del paquete que se muestra en la ilustración identifica las direcciones MAC e IP de origen y destino.

**Nota:** los routers también se suelen configurar con su propio gateway predeterminado. En ocasiones, este se conoce como “gateway de último recurso”.

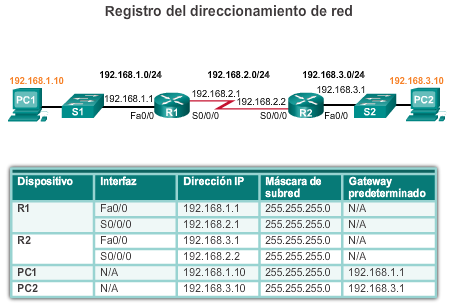


Cuando se diseña una nueva red o se hacen asignaciones en una red existente, es necesario documentar la red. Como mínimo, el registro debe identificar lo siguiente:

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

Como se muestra en la ilustración, esta información se captura mediante la creación de dos registros útiles de la red:

* **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.

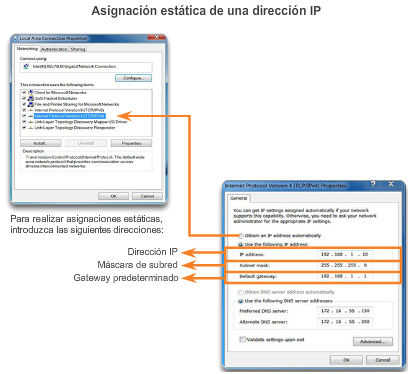


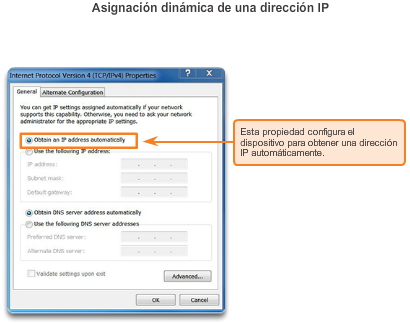
Se puede asignar información de dirección IP a un host de dos formas:

* **Estática:** se asigna la dirección IP, la máscara de subred y el gateway predeterminado 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.

En las figuras 1 y 2, se proporcionan ejemplos de configuración estática y dinámica de direcciones IPv4.

Por lo general, las direcciones asignadas estáticamente se usan para identificar recursos de red específicos, como servidores e impresoras de red. También se pueden usar en redes más pequeñas con pocos hosts. Sin embargo, la mayoría de los dispositivos host adquieren su información de dirección IPv4 accediendo a un servidor de DHCP. En las empresas grandes, se implementan servidores de DHCP dedicados que proporcionan servicios a muchas LAN. En un entorno más pequeño de sucursal u oficina pequeña, un switch Cisco Catalyst o un ISR Cisco pueden proporcionar los servicios de DHCP.





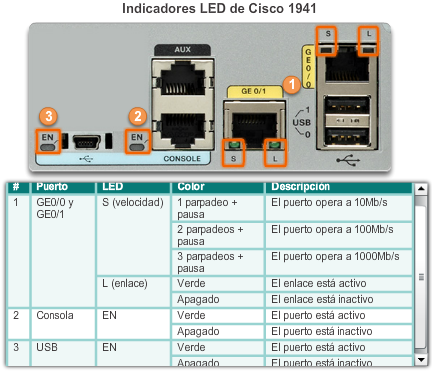
Los equipos host se conectan a una red conectada por cable mediante una interfaz de red y un cable Ethernet RJ-45. La mayoría de las interfaces de red tienen uno o dos indicadores LED de enlace junto a la interfaz. Generalmente, un LED verde indica una conexión correcta, mientras que un LED verde que 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.



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.

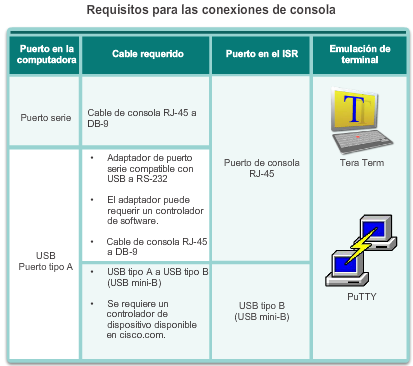
El acceso a la consola requiere lo siguiente:

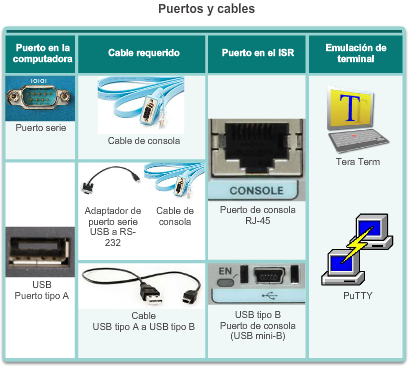
* **Cable de consola:** un cable de consola RJ-45 a DB-9
* **Software de emulación de terminal:**Tera Term, PuTTY, HyperTerminal

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.

El ISR Cisco G2 admite una conexión serie de consola USB. Para establecer la conectividad, se requiere un USB de tipo A a tipo B (USB mini-B), así como un controlador de dispositivo del sistema operativo. Este controlador de dispositivo se puede descargar en [www.cisco.com](http://www.cisco.com/). Si bien estos routers tienen dos puertos de consola, los puertos solo se pueden usar de a uno por vez. Cuando se conecta un cable al puerto de consola USB, el puerto RJ-45 queda inactivo. Cuando se quita el cable USB del puerto USB, el puerto RJ-45 se activa.

En la tabla de la figura 1, se resumen los requisitos para las conexiones de consola. En la figura 2, se muestran los distintos puertos y cables que se requieren.



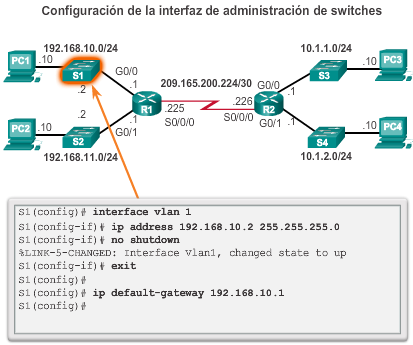


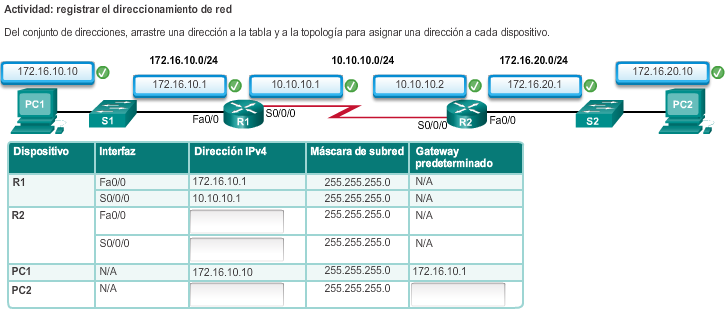
Los dispositivos de infraestructura de red requieren direcciones IP para habilitar la administración remota. Con la dirección IP del dispositivo, el administrador de red puede conectarse al dispositivo de forma remota mediante Telnet, SSH, HTTP o HTTPS.

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).

Por ejemplo, en la figura 1, se asigna la dirección IP 192.168.10.2/24 y un gateway predeterminado del router ubicado en 192.168.10.1 a la SVI del switch de capa 2 S1.

Utilice el verificador de sintaxis de la figura 2 para configurar el switch de capa 2 S2.





### Configuración básica de un router

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

Al configurar un switch o un router Cisco, primero se deben realizar las siguientes tareas básicas:

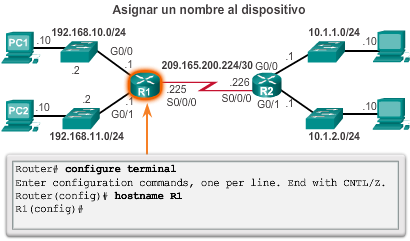
* **Asignar un nombre al dispositivo:** para distinguirlo de otros routers.
* **Proteger el acceso de administración:** para proteger el acceso a EXEC privilegiado, a EXEC de usuario y el acceso por Telnet, y cifrar las contraseñas con el máximo nivel.
* **Configurar un aviso:** para proporcionar notificaciones legales de acceso no autorizado.

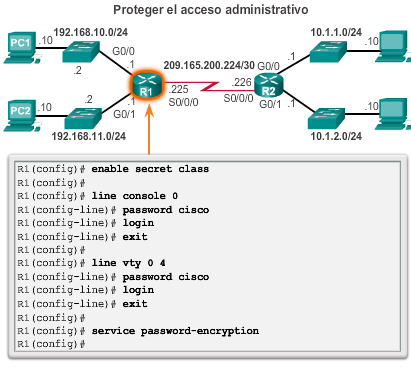
**Nota:** siempre guarde los cambios en un router y verifique la configuración básica y las operaciones del router.

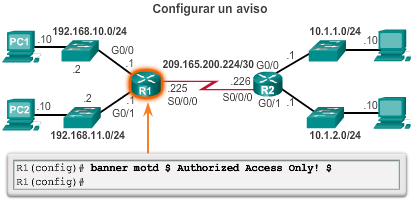
En las figuras 1 a 4, se proporcionan ejemplos de configuración de parámetros básicos en el router R1:

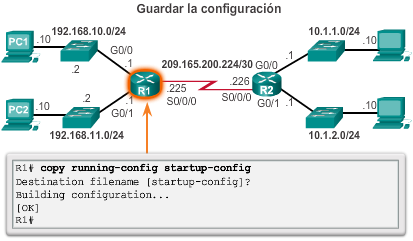
* En la figura 1, se asigna un nombre al dispositivo.
* En la figura 2, se protege el acceso de administración.
* En la figura 3, se configura un aviso.
* En la figura 4, se guarda la configuración.

Utilice el verificador de sintaxis de la figura 5 para configurar el router R2.









Una característica que distingue a los switches de los routers es el tipo de interfaces que admite cada uno. Por ejemplo, los switches de capa 2 admiten redes LAN y, por lo tanto, tienen varios puertos FastEthernet o Gigabit Ethernet.

Los routers admiten redes LAN y WAN, y pueden interconectar distintos tipos de redes; por lo tanto, admiten muchos tipos de interfaces. Por ejemplo, los ISR G2 tienen una o dos interfaces Gigabit Ethernet integradas y ranuras para tarjetas de interfaz WAN de alta velocidad (HWIC) para admitir otros tipos de interfaces de red, incluidas las interfaces seriales, DSL y de cable.

Para que una interfaz esté disponible, debe cumplir los siguientes requisitos:

* **Con IPv4, se debe configurar la interfaz con una dirección y una máscara de subred:** use el comando de configuración de interfaz **ip address***dirección-ip máscara-de-subred*.
* **Activar la interfaz:** las interfaces LAN y WAN no están activadas (**shutdown**) de manera predeterminada. Para habilitar una interfaz, esta se debe usar el comando **no shutdown**. (Es similar al encendido de la interfaz). La interfaz también debe estar conectada a otro dispositivo (un hub, un switch u otro router) para que la capa física esté activa.

La interfaz también se puede configurar con una breve descripción. Es aconsejable configurar una descripción en cada interfaz. El texto de la descripción tiene un límite de 240 caracteres. En las redes de producción, una descripción puede ser útil para la resolución de problemas, dado que proporciona información con respecto al tipo de red a la que está conectada la interfaz. Si la interfaz se conecta a un ISP o un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

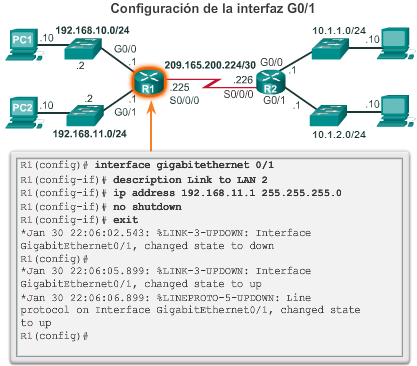
Según el tipo de interfaz, es posible que se requieran parámetros adicionales. Por ejemplo, en el entorno del laboratorio, la interfaz serial que se conecta al extremo del cable serial rotulado DCE se debe configurar con el comando **clock rate**.

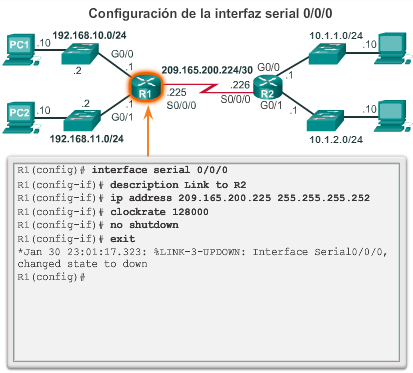
**Nota:** si se usa el comando **clock rate**por accidente en una interfaz DTE, se genera el mensaje de error %Error: This command applies only to DCE interface (%Error: este comando se aplica únicamente a la interfaz DCE).

En las figuras 1 a 3, se proporcionan ejemplos de configuración de las interfaces del router R1.

Utilice el verificador de sintaxis de la figura 4 para configurar el router R2.







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 muchos 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:

* **Configurar la interfaz con una máscara y una dirección IPv6:** use el comando de configuración de interfaz **ipv6 address** *dirección-ipv6* / *longitud-prefijo* **[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.

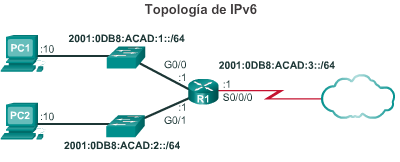
En la topología de ejemplo que se muestra en la figura 1, el R1 se debe configurar para que admita las siguientes direcciones de red IPv6:

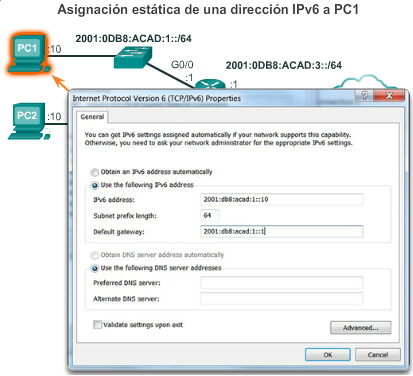
* 2001:0DB8:ACAD:0001:/64 o 2001:DB8:ACAD:1::/64
* 2001:0DB8:ACAD:0002:/64 o 2001:DB8:ACAD:2::/64
* 2001:0DB8:ACAD:0003:/64 o 2001:DB8:ACAD:3::/64

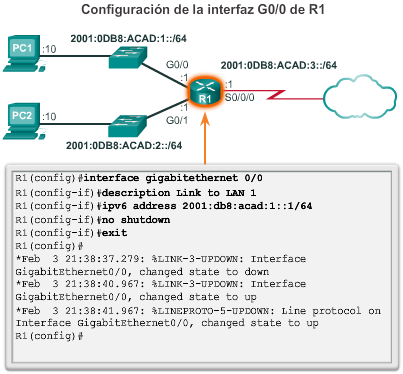
Cuando el router se configura con el comando de configuración global **ipv6 unicast-routing**, el router comienza a enviar mensajes de anuncio de router ICMPv6 por la interfaz. Esto permite que una computadora que está conectada a la interfaz configure una dirección IPv6 y establezca un gateway predeterminado de forma automática, sin necesidad de utilizar los servicios de un servidor de DHCPv6. Por otra parte, una computadora conectada a la red IPv6 puede obtener la dirección IPv6 asignada estáticamente, como se muestra en la figura 2. Observe que la dirección de gateway predeterminado configurada para la PC1 es la dirección de unidifusión global de IPv6 de la interfaz GigabitEthernet 0/0 del R1.

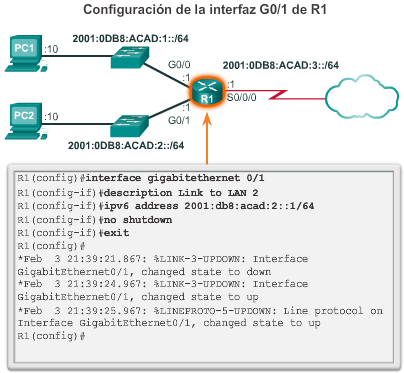
Las interfaces del router en la topología de ejemplo se deben configurar y habilitar como se muestra en las figuras 3 a 5.

Utilice el verificador de sintaxis de la figura 6 para configurar las direcciones de unidifusión global de IPv6 en el router R2.











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 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 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 de un puerto físico que puede dejar de funcionar.

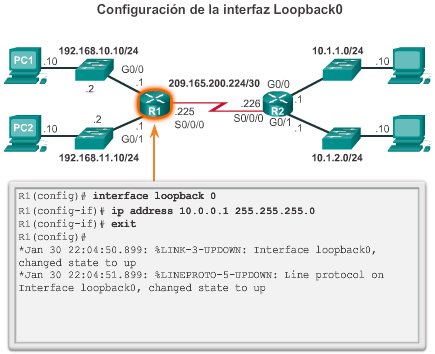
El proceso de habilitación y asignación de una dirección de loopback es simple:

Router(config)# **interface loopback***number*

Router(config-if)# **ip address***ip-address* *subnet-mask*

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 conectividad de redes conectadas directamente

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, incluso la dirección IPv4 de la interfaz y el estado operativo actual.
* **show ip route**: muestra el contenido de la tabla de enrutamiento IPv4 almacenada 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***id-interfaz* : muestra los comandos configurados en la interfaz especificada.

En la figura 1, se muestra el resultado del comando **show ip interface brief**. El resultado muestra que todas las interfaces LAN y el enlace WAN están activos y en funcionamiento, como lo indica el valor “up” en las columnas Status (Estado) y Protocol (Protocolo). Un resultado distinto indicaría un problema con la configuración o el cableado.

**Nota:** en la figura 1, se muestra la interfaz Embedded-Service-Engine0/0 porque los ISR Cisco G2 tienen CPU de doble núcleo en la placa madre. La interfaz Embedded-Service-Engine0/0 excede el ámbito de este curso.

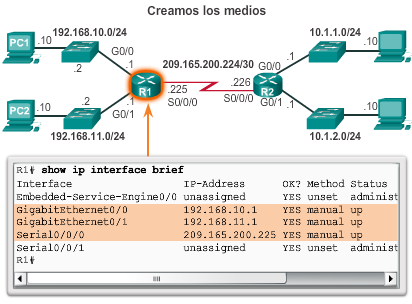
En la figura 2, se muestra el resultado del comando **show ip route**. Observe las tres entradas de redes conectadas directamente y las tres entradas de interfaz de ruta de host local. Una ruta de host local tiene una distancia administrativa de 0. También tiene una máscara /32 para IPv4 y una máscara /128 para IPv6. La ruta de host local es para las rutas en el router que posee la dirección IP. Estas se usan para permitir que el router procese los paquetes destinados a esa dirección IP.

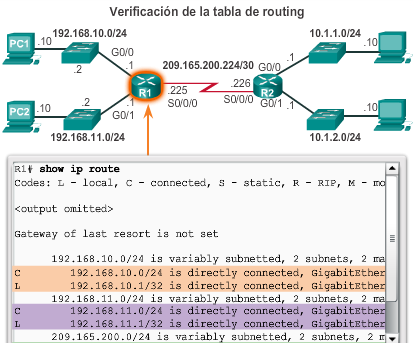
En la figura 3, se muestra el resultado del comando **show running-config interface**. El resultado muestra los comandos configurados actualmente en la interfaz especificada.

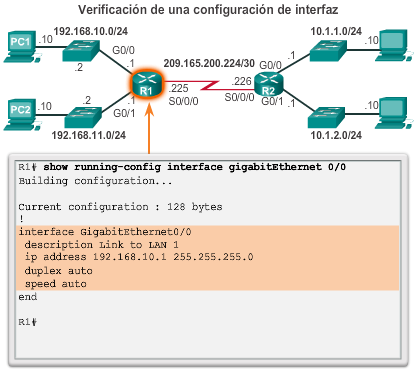
Los dos comandos siguientes se usan para recopilar información más detallada sobre la interfaz:

* **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.

Utilice el verificador de sintaxis de las figuras 4 y 5 para verificar las interfaces del R1.







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** de la figura 1 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**que se muestra en la figura 2 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.

Como se muestra en la figura 3, 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 redes IPv6, no redes IPv4.

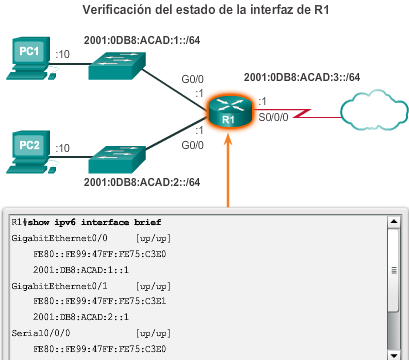
En la tabla de routing, una “C” junto a una ruta indica que se trata de una red conectada directamente. Cuando la interfaz del router se configura con una dirección unicast global y su estado es “up/up”, se agrega el prefijo y la duración de prefijo IPv6 a la tabla de enrutamiento IPv6 como una ruta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

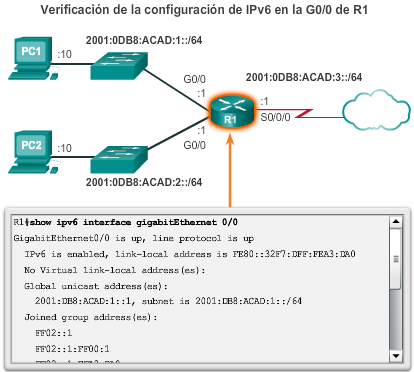
La dirección IPv6 unicast global configurada en la interfaz también se instala en la tabla de enrutamiento como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuyo destino es la dirección de la interfaz del router.

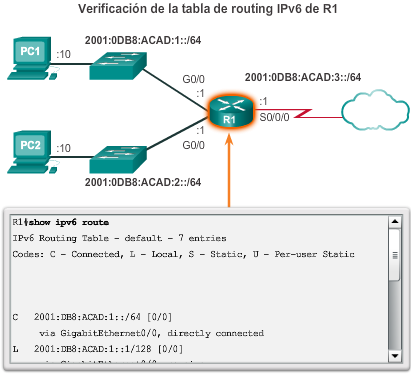
El comando **ping** para IPv6 es idéntico al comando que se utiliza con IPv4, excepto que se utiliza una dirección IPv6. Como se muestra en la figura 4, el comando **ping** se utiliza para verificar la conectividad de capa 3 entre el R1 y la PC1.

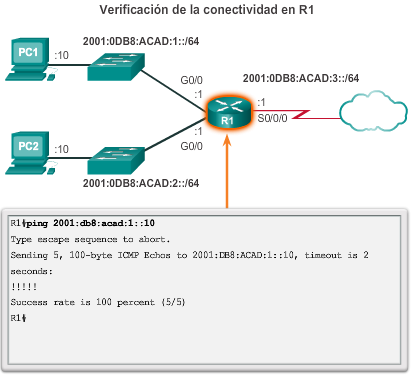
Otros comandos de verificación de IPv6 incluyen los siguientes:

* **show interfaces**
* **show ipv6 routers**









Los comandos que generan varias pantallas de resultados se pausan al cabo de 24 líneas de manera predeterminada. Al final del resultado detenido, se muestra el texto --More--. Si presiona **Entrar**, se muestra la siguiente línea, y si presiona la barra espaciadora, se muestra el siguiente grupo de líneas. Utilice el comando **terminal length***número* para especificar la cantidad de líneas que se muestran. Un valor 0 (cero) evita que el router haga una pausa entre las pantallas de resultados.

Otra característica muy útil que mejora la experiencia del usuario en la interfaz de línea de comandos (CLI) es el filtrado de los resultados del comando **show**. Los comandos de filtrado se pueden utilizar para mostrar secciones específicas de los resultados. Para habilitar el comando de filtrado, introduzca una barra vertical (**|**) después del comando **show** y, a continuación, introduzca un parámetro de filtrado y una expresión de filtrado.

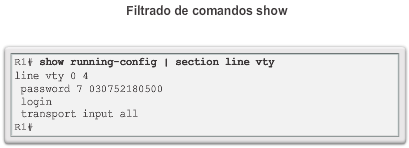
Los parámetros de filtrado que se pueden configurar después de la barra vertical incluyen lo siguiente:

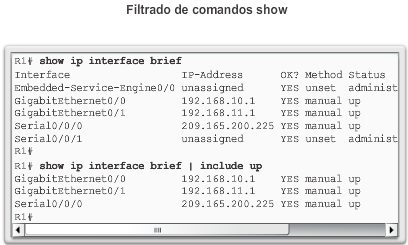
* **section:** muestra la sección completa que comienza con la expresión de filtrado.
* **include:** incluye todas las líneas de resultados que coinciden con la expresión de filtrado.
* **exclude:** excluye todas las líneas de resultados que coinciden con la expresión de filtrado.
* **begin:** muestra todas las líneas de resultados desde determinado punto, comenzando por la línea que coincide con la expresión de filtrado.

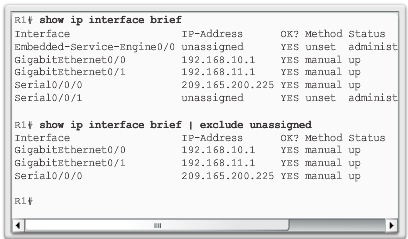
**Nota:** los filtros de resultados se pueden utilizar junto con cualquier comando **show**.

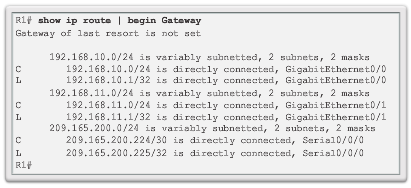
En las figuras 1 a 4, se proporcionan ejemplos de los diversos filtros de resultados.

Utilice el verificador de sintaxis de la figura 5 para filtrar los resultados.









La característica de historial de comandos es útil, ya que almacena temporalmente la lista de comandos ejecutados que se deben recuperar.

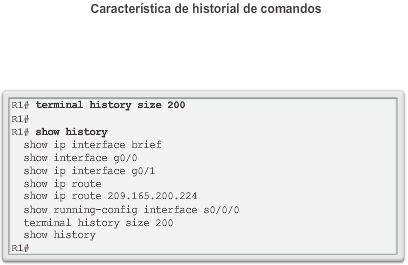
Para recuperar comandos del búfer de historial, presione **Ctrl**+**P** o la tecla **Flecha arriba**. El resultado de los comandos comienza con el comando más reciente. Repita la secuencia de teclas para recuperar sucesivamente los comandos más antiguos. Para volver a los comandos más recientes en el búfer de historial, presione **Ctrl**+**N** o la tecla **Flecha abajo**. Repita la secuencia de teclas para recuperar sucesivamente los comandos más recientes.

De manera predeterminada, el historial de comandos está habilitado, y el sistema captura las últimas 10 líneas de comandos en el búfer de historial. Utilice el comando**show history** del modo EXEC privilegiado para mostrar el contenido del búfer.

También es práctico aumentar la cantidad de líneas de comandos que registra el búfer de historial solamente durante la sesión de terminal actual. Utilice el comando**terminal history size** del modo EXEC del usuario para aumentar o reducir el tamaño del búfer.

En la figura 1, se muestra un ejemplo de los comandos **terminal history size** y**show history**.

Utilice el verificador de sintaxis de la figura 2 para practicar los dos comandos del modo EXEC.



## Decisiones de Routing

### Switching de paquetes entre redes

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.

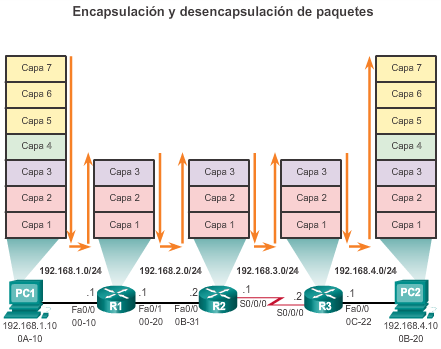
¿Qué hace un router cuando recibe un paquete desde una red que está destinado a otra red? El router ejecuta los siguientes tres pasos principales:

**Paso 1.** Desencapsula el paquete de capa 3 eliminando el encabezado y el tráiler de la trama de capa 2.

**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.

Como se muestra en la ilustración, los dispositivos tienen direcciones IPv4 de capa 3, y las interfaces Ethernet tienen direcciones de enlace de datos de capa 2. Por ejemplo, la PC1 se configuró con la dirección IPv4 192.168.1.10 y una dirección MAC de ejemplo 0A-10. A medida que un paquete se desplaza desde el dispositivo de origen hacia el dispositivo de destino final, las direcciones IP de capa 3 no se modifican. Sin embargo, las direcciones de enlace de datos de capa 2 cambian en cada salto cuando cada router desencapsula y vuelve a encapsular el paquete en una nueva trama. Es muy probable que el paquete se encapsule en un tipo de trama de capa 2 diferente de la trama en la que se recibió. Por ejemplo, el router puede recibir una trama de Ethernet encapsulada en una interfaz FastEthernet y, a continuación, procesarla para reenviarla por una interfaz serial como trama encapsulada de protocolo punto a punto (PPP).



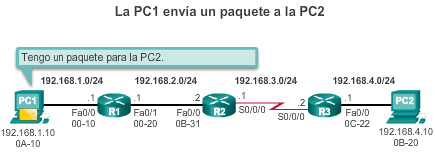
En la animación de la ilustración, la PC1 envía un paquete a la PC2. La PC1 debe determinar si la dirección IPv4 de destino está en la misma red. La PC1 determina su propia subred realizando una operación**AND** en su propia dirección y máscara de subred IPv4. Esto produce la dirección de red a la que pertenece la PC1. A continuación, la PC1 realiza la misma operación **AND** con la dirección IPv4 de destino del paquete y la máscara de subred de la PC1.

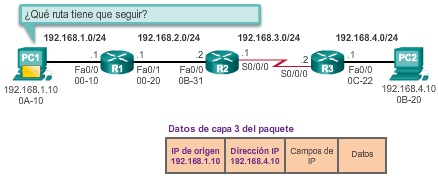
Si la dirección de red de destino está en la misma red que la PC1, entonces la PC1 no utiliza el gateway predeterminado. En lugar de esto, la PC1 consulta su caché ARP para obtener la dirección MAC del dispositivo con esa dirección IPv4 de destino. Si la dirección MAC no está en la caché, la PC1 genera una solicitud de ARP para obtener la dirección a fin de completar el paquete y enviarlo al destino. Si la dirección de red de destino está en una red diferente, la PC1 reenvía el paquete a su gateway predeterminado.

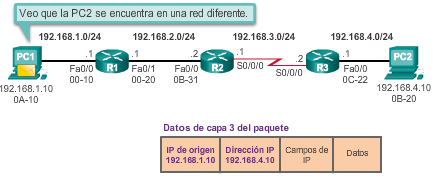
Para determinar la dirección MAC del gateway predeterminado, la PC1 busca la dirección IPv4 del gateway predeterminado y la dirección MAC relacionada en su tabla ARP.

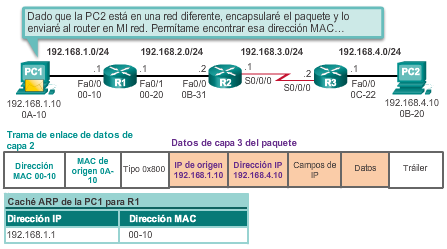
Si no existe ninguna entrada ARP para el gateway predeterminado en la tabla ARP, la PC1 envía una solicitud de ARP. El router R1 envía una respuesta de ARP. Luego, la PC1 puede reenviar el paquete a la dirección MAC del gateway predeterminado, la interfaz Fa0/0 del router R1.

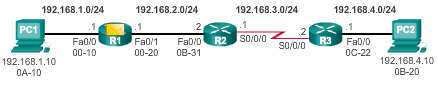
Para los paquetes IPv6, se realiza un proceso similar. En lugar del proceso ARP, la resolución de direcciones IPv6 utiliza los mensajes ICMPv6 de solicitud y de anuncio de vecino. Las asignación de direcciones IPv6 a MAC se guarda en una tabla similar a la caché ARP, denominada “caché de vecinos”.











Los siguientes procesos ocurren cuando el R1 recibe la trama de Ethernet de la PC1:

1. El R1 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, el R1 copia la trama en su búfer.

2. El R1 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.

3. El R1 desencapsula la trama de Ethernet.

4. Dado que la dirección IPv4 de destino del paquete no coincide con ninguna de las redes directamente conectadas del R1, este consulta su tabla de routing para enrutar este paquete. El R1 busca una dirección de red en la tabla de routing que incluya la dirección IPv4 de destino del paquete como dirección host dentro de esa red. En este ejemplo la tabla de enrutamiento tiene una ruta para la red 192.168.4.0/24. La dirección IPv4 de destino del paquete es 192.168.4.10, que es una dirección host IPv4 en esa red.

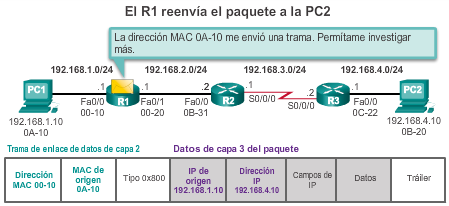
La ruta a la red 192.168.4.0/24 que encuentra el R1 tiene la dirección IPv4 de siguiente salto 192.168.2.2 y una interfaz de salida FastEthernet 0/1. Esto significa que el paquete IPV4 se encapsula en una nueva trama de Ethernet con la dirección MAC de destino de la dirección IPv4 del router de siguiente salto.

Debido a que la interfaz de salida se encuentra en una red Ethernet, el R1 debe resolver la dirección IPv4 de siguiente salto con una dirección MAC de destino mediante ARP:

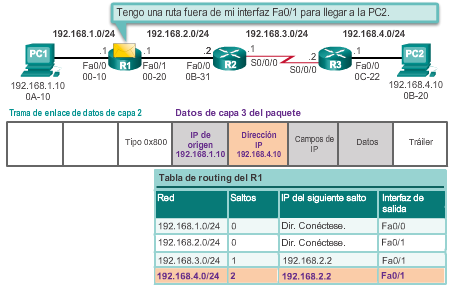
1. El R1 busca la dirección IPv4 de siguiente salto 192.168.2.2 en su caché ARP. Si la entrada no aparece en la caché ARP, el R1 envía una solicitud de ARP por la interfaz FastEthernet 0/1, y el R2 envía una respuesta de ARP. A continuación, el R1 actualiza su caché ARP con una entrada para 192.168.2.2 y la dirección MAC asociada.

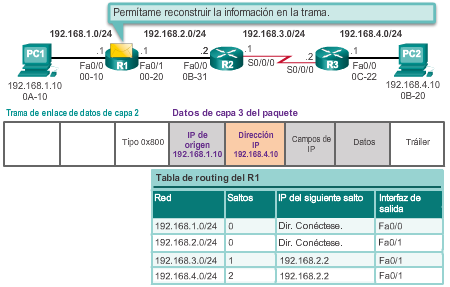
2. El paquete IPv4 ahora se encapsula en una nueva trama de Ethernet y se reenvía por la interfaz FastEthernet 0/1 del R1.

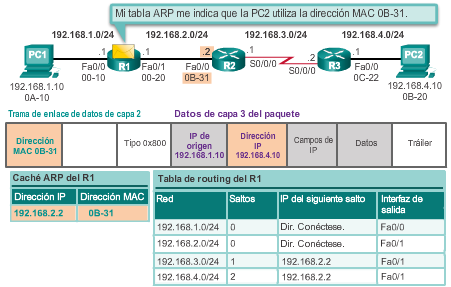
En la animación de la ilustración, se muestra cómo el R1 reenvía el paquete al R2.

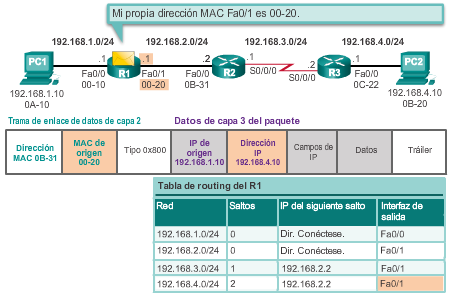


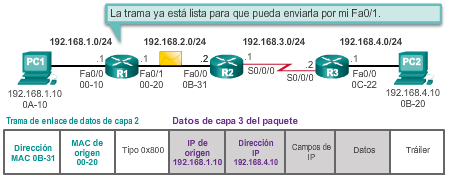












Los siguientes procesos ocurren cuando el R2 recibe la trama en su interfaz Fa0/0:

1. El R2 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, el R2 copia la trama en su búfer.

2. El R2 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.

3. El R2 desencapsula la trama de Ethernet.

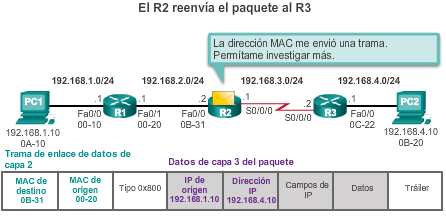
4. Dado que la dirección IPv4 de destino del paquete no coincide con ninguna de las direcciones de interfaz del R2, este consulta su tabla de routing para enrutar este paquete. El R2 busca la dirección IPv4 de destino del paquete en la tabla de routing con el mismo proceso que usó el R1.

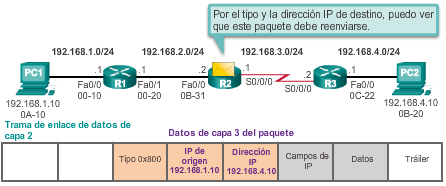
La tabla de routing del R2 tiene una ruta a la red 192.168.4.0/24, con la dirección IPv4 de siguiente salto 192.168.3.2 y la interfaz de salida Serial 0/0/0. Debido a que la interfaz de salida no es una red Ethernet, el R2 no tiene que resolver la dirección IPv4 de siguiente salto con una dirección MAC de destino.

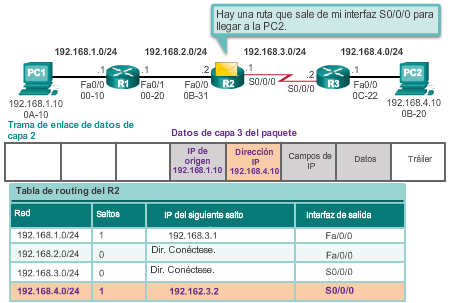
5. El paquete IPv4 ahora se encapsula en una nueva trama de enlace de datos y se envía por la interfaz de salida Serial 0/0/0.

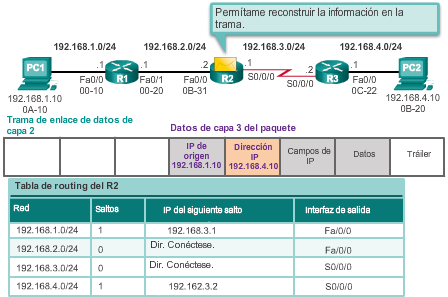
Cuando la interfaz es una conexión serial punto a punto (P2P), el router encapsula el paquete IPv4 en el formato de trama de enlace de datos correspondiente que utiliza la interfaz de salida (HDLC, PPP, etc.). Debido a que no hay direcciones MAC en las interfaces seriales, el R2 establece la dirección de destino de enlace de datos en el equivalente a una difusión.

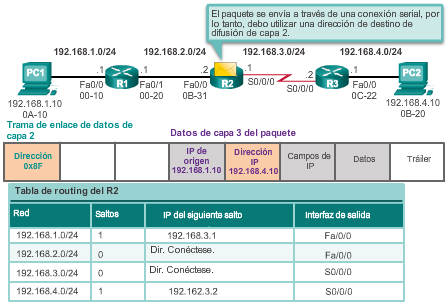
En la animación de la ilustración, se muestra cómo el R2 reenvía el paquete al R3.

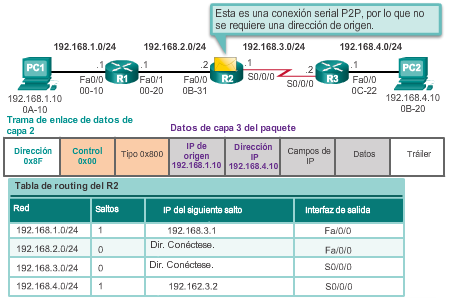


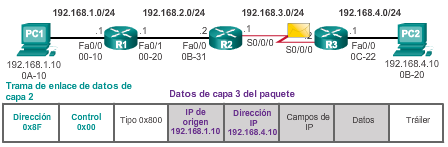












Los siguientes procesos ocurren cuando la trama llega al R3:

1. El R3 copia la trama PPP de enlace de datos en su búfer.

2. El R3 desencapsula la trama PPP de enlace de datos.

3. El R3 busca la dirección IPv4 de destino del paquete en la tabla de routing. La tabla de routing tiene una ruta a una red conectada directamente en el R3. Esto significa que el paquete puede enviarse directamente al dispositivo de destino y no es necesario enviarlo a otro router.

Dado que la interfaz de salida es una red Ethernet conectada directamente, el R3 debe resolver la dirección IPv4 de destino del paquete con una dirección MAC de destino:

1. El R3 busca la dirección IPv4 de destino del paquete en la caché del protocolo de resolución de direcciones (ARP). Si la entrada no aparece en la caché ARP, el R3 envía una solicitud de ARP por la interfaz FastEthernet 0/0. La PC2 envía a cambio una respuesta ARP con su dirección MAC. A continuación, el R3 actualiza su caché ARP con una entrada para 192.168.4.10 y la dirección MAC que se devolvió en la respuesta de ARP.

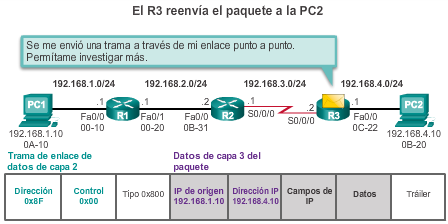
2. El paquete IPv4 se encapsula en una nueva trama de enlace de datos de Ethernet y se envía por la interfaz FastEthernet 0/0 del R3.

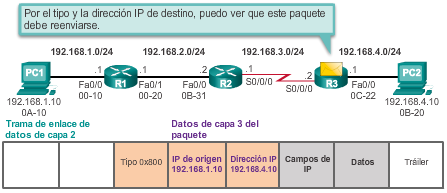
3. Cuando la PC2 recibe la trama, examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, la tarjeta de interfaz de red (NIC) Ethernet. Por lo tanto, la PC2 copia el resto de la trama en su búfer.

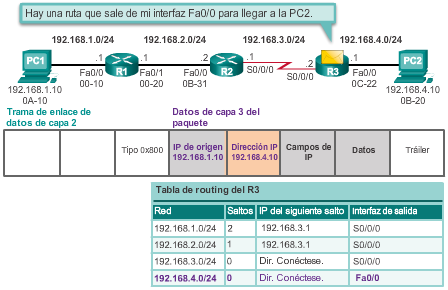
4. La PC2 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.

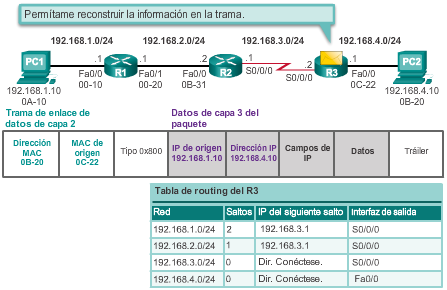
5. La PC2 desencapsula la trama de Ethernet y envía el paquete IPv4 al proceso IPv4 de su sistema operativo.

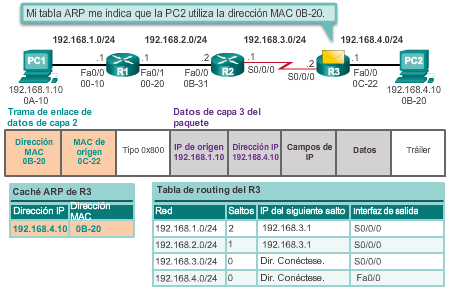
En la animación de la ilustración, se muestra cómo el R3 reenvía el paquete a la PC2.

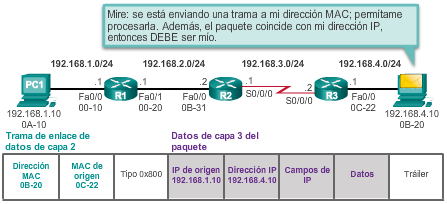


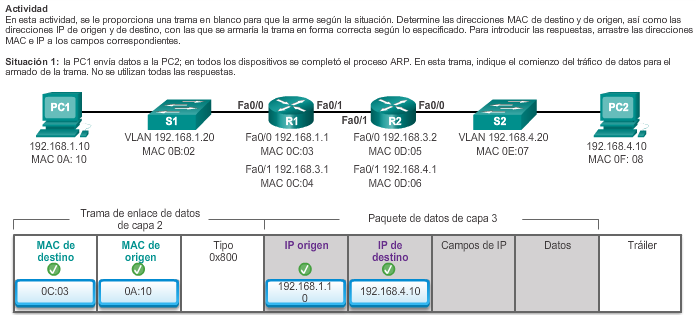












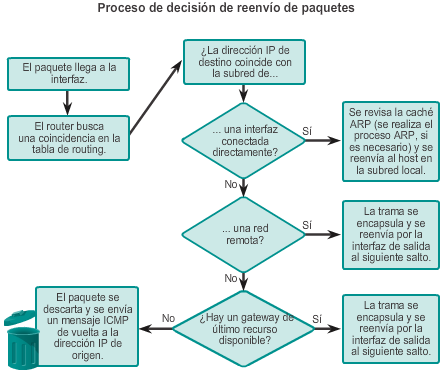
### Determinación de ruta

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 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. Si se descarta el paquete, el router envía un mensaje de ICMP de destino inalcanzable a la dirección IP de origen del paquete.

En el diagrama de flujo lógico de la ilustración, se describe el proceso de decisión de reenvío de paquetes del router.



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.

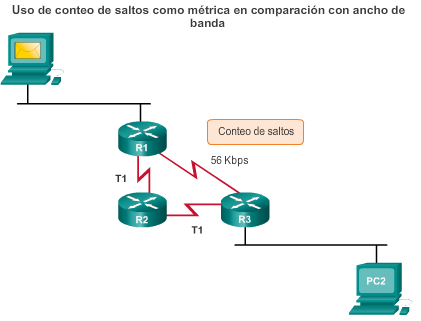
El mejor camino es elegido por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Una métrica es un valor cuantitativo que se utiliza para medir la distancia que existe hasta una red determinada. El mejor camino a una red es la ruta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

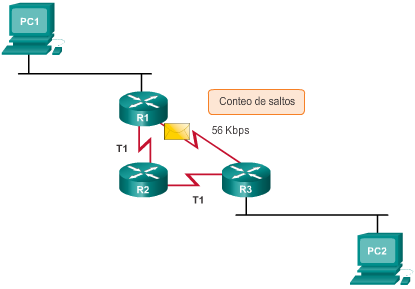
Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica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

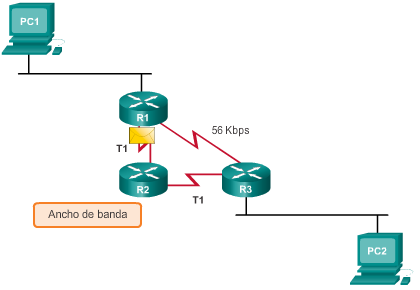
A continuación, se indican algunos protocolos dinámicos y las métricas que utilizan:

* **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.

En la animación de la ilustración, se destaca cómo la ruta puede ser diferente según la métrica que se utiliza.







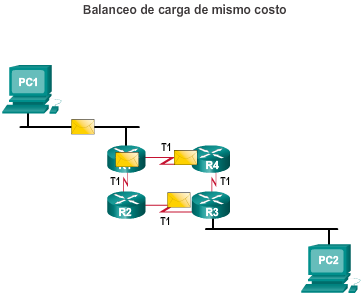
¿Qué sucede si una tabla de routing tiene dos o más rutas con métricas idénticas hacia la misma red de destino?

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.

**Nota:** solo EIGRP admite el balanceo de carga con distinto costo.

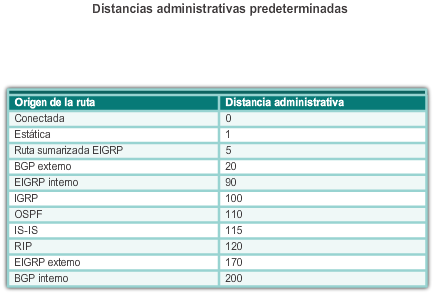
En la animación de la ilustración, se proporciona un ejemplo de balanceo de carga de mismo costo.

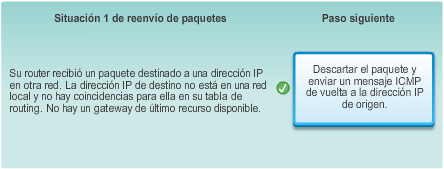


Es posible configurar un router con varios protocolos de routing y varias rutas estáticas. Si esto ocurre, la tabla de routing puede tener más de un origen de ruta para la misma red de destino. Por ejemplo, si se configura RIP y EIGRP en un router, ambos protocolos de routing pueden descubrir la misma red de destino. Sin embargo, cada protocolo de routing puede decidir tomar una ruta diferente para llegar al destino según las métricas de ese protocolo de routing. RIP elige una ruta según el conteo de saltos, mientras que EIGRP elige una ruta según la métrica compuesta. ¿Cómo sabe el router qué ruta debe utilizar?

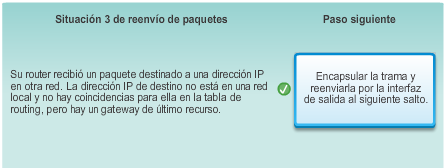
El IOS de Cisco utiliza lo que se conoce como “distancia administrativa” (AD) para determinar la ruta que se debe instalar en la tabla de routing de IP. La AD representa la “confiabilidad” de la ruta: cuanto menor sea la AD, más confiable será el origen de la ruta. Por ejemplo, la AD de una ruta estática 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.

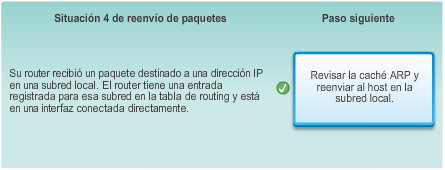
En la ilustración, se muestran diferentes protocolos de routing y sus AD asociadas.











## Funcionamiento del router

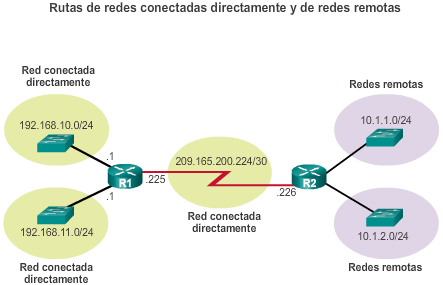
### Análisis de la tabla de Routing

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 se configura una interfaz 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 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.

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



En los routers Cisco IOS, 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:

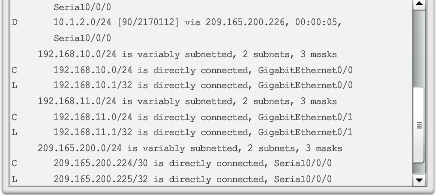
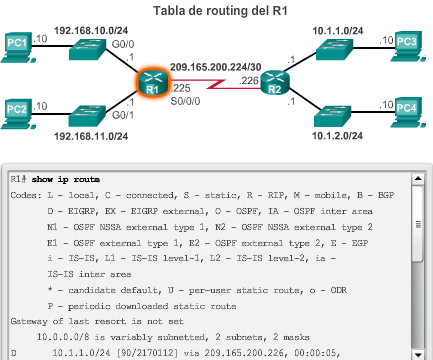
* **Interfaces de ruta local:** se agregan cuando la interfaz está configurada y activa. Esta entrada solo se muestra en la versión IOS 15 o más reciente para las rutas IPv4, y en todas las versiones de IOS para las rutas IPv6.
* **Interfaces conectadas directamente:** se agregan a la tabla de routing 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.

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

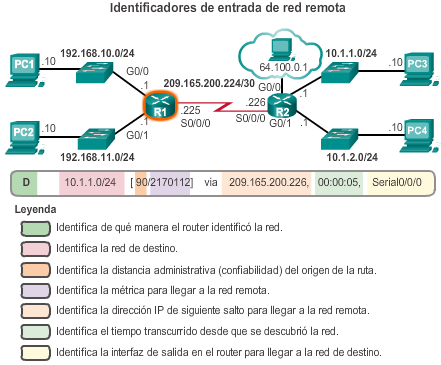
En la ilustración, se muestra la tabla de enrutamiento del R1 en una red simple.

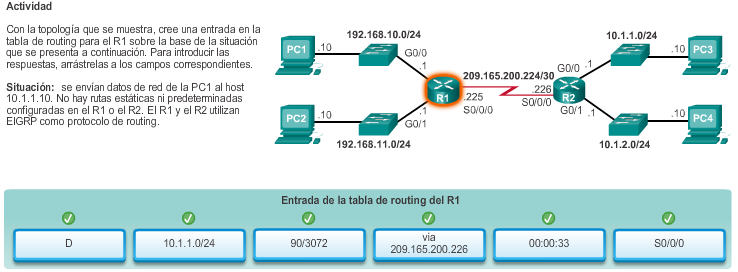


Como administrador de red, es imprescindible saber cómo interpretar el contenido de una tabla de routing IPv4 e IPv6. En la ilustración, se muestra una entrada de la tabla de routing IPv4 en el R1 para la ruta a la red remota 10.1.1.0.

La entrada indica la siguiente información:

* **Origen de la ruta:** identifica el modo en que se descubrió la ruta.
* **Red de destino:** identifica la dirección de la red remota.
* **Distancia administrativa:** identifica la confiabilidad del origen de la ruta. Los valores más bajos indican el origen de ruta preferido.
* **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
* **Siguiente salto:** identifica la dirección IPv4 del router siguiente al que se debe reenviar el paquete.
* **Marca de hora de la ruta:** identifica el tiempo que pasó desde que se descubrió la ruta.
* **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.





### Rutas 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.

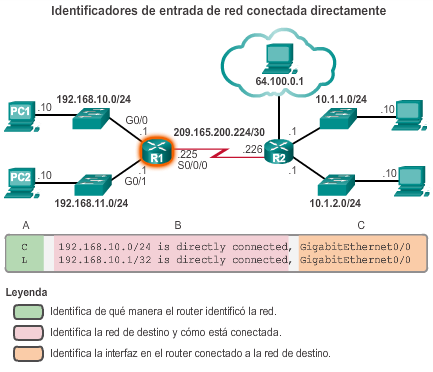


Una interfaz activa, correctamente configurada y conectada directamente, genera dos entradas en la tabla de routing. En la ilustración, se muestran las entradas de la tabla de routing IPv4 en el R1 para la red conectada directamente 192.168.10.0.

La entrada de la tabla de routing para las interfaces conectadas directamente es más simple que las entradas para las redes remotas. Las entradas contienen la siguiente información:

* **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. El código“C” identifica una red conectada directamente. El código “L” identifica la dirección IPv4 asignada a la interfaz del router.
* **Red de destino:** la dirección de la red remota.
* **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

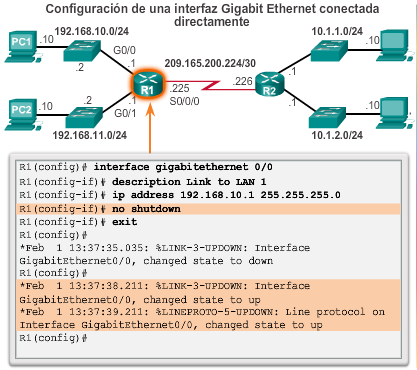
**Nota:** antes de IOS 15, no se mostraban las entradas de la tabla de routing de ruta local (L) en la tabla de routing IPv4. Las entradas de ruta local (L) siempre formaron parte de la tabla de routing IPv6.

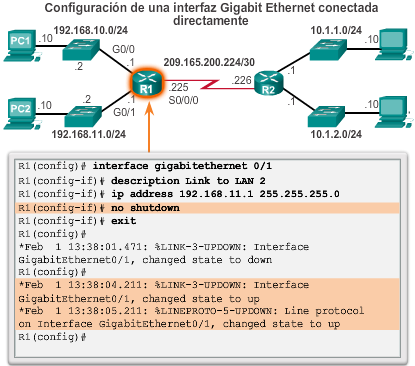


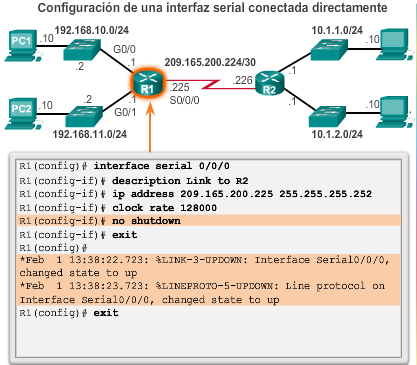
En los ejemplos de las figuras 1 a 3, se muestran los pasos para configurar y activar las interfaces conectadas al R1. Observe los mensajes informativos de capa 1 y 2 que se generan a medida que se activa cada interfaz.

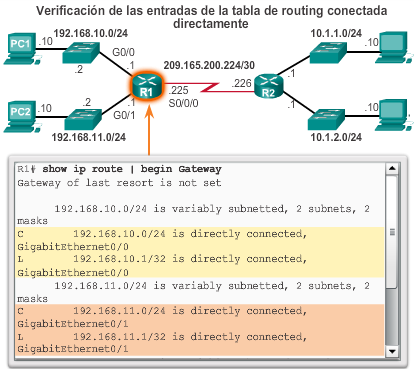
A medida que se agregan interfaces, la tabla de routing agrega automáticamente las entradas conectadas (“C”) y locales (“L”). En la figura 4, se proporciona un ejemplo de la tabla de routing con las interfaces del R1 conectadas directamente configuradas y activadas.

Utilice el verificador de sintaxis de la figura 5 para configurar y activar las interfaces conectadas al R2.









En el ejemplo de la figura 1, se muestran los pasos de configuración de las interfaces del R1 conectadas directamente con las direcciones IPv6 indicadas. Observe los mensajes informativos de capa 1 y capa 2 que se generan a medida que se configura y se activa cada interfaz.

Como se muestra en la figura 2, el comando**show ipv6 route** se utiliza para verificar si se instalaron las redes IPv6 y las direcciones específicas de interfaz IPv6 en la tabla de routing IPv6. Como en IPv4, una “C” junto a una ruta indica que se trata de una red conectada directamente. Una “L” indica la ruta local. En una red IPv6, la ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuya dirección de destino es la interfaz del router.

Observe que también se instaló una ruta a la red FF00::/8. Esta ruta se requiere para el routing de multidifusión.

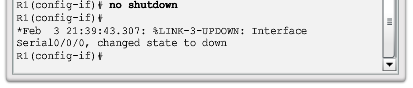
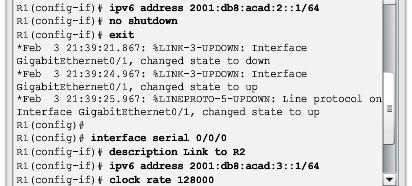
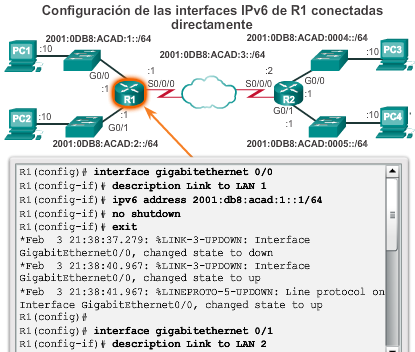
En la figura 3, se muestra cómo el comando**show ipv6 route** se puede combinar con un destino de red específico para mostrar los detalles de cómo el router descubrió dicha ruta.

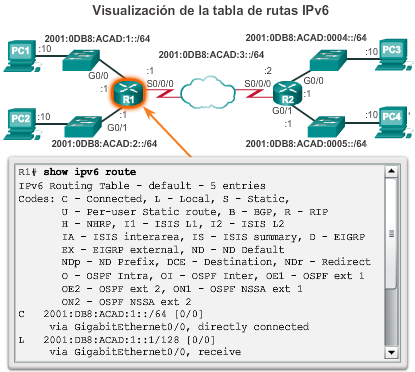
En la figura 4, se muestra cómo se puede verificar la conectividad al R2 mediante el comando **ping**.

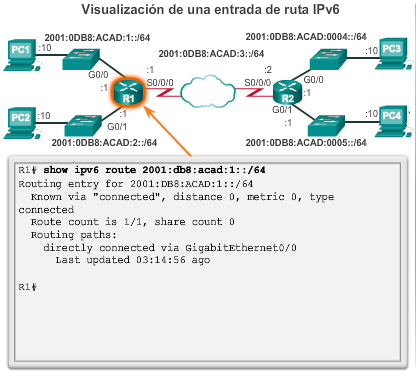
En la figura 5, observe qué sucede cuando la interfaz LAN G0/0 del R2 es el objetivo del comando **ping**. Los pings no tienen éxito. Esto se debe a que el R1 no tiene ninguna entrada en la tabla de routing para llegar a la red 2001:DB8:ACAD:4::/64.

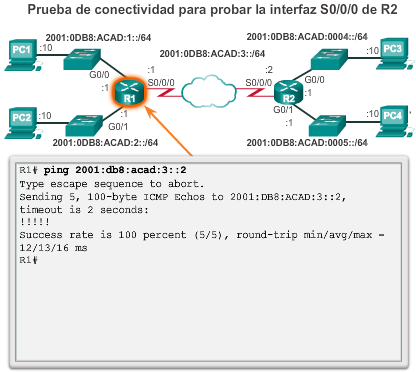
El R1 requiere información adicional para llegar a una red remota. Se pueden agregar entradas de ruta de red remota a la tabla de routing mediante los siguientes métodos:

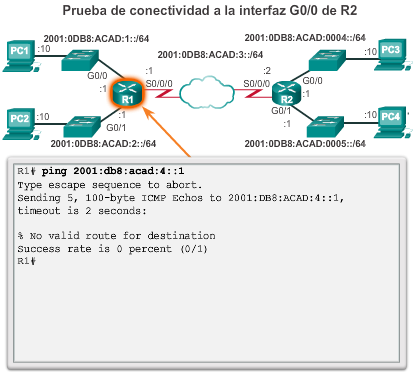
* Enrutamiento estático
* Protocolos de enrutamiento dinámico











### Rutas descubiertas estáticamente

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

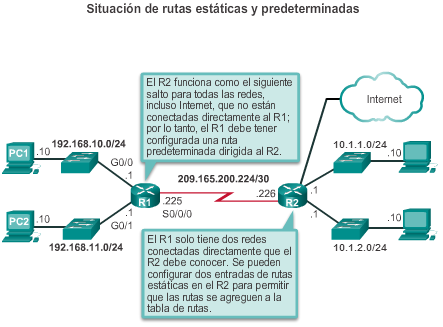
Las rutas estáticas se pueden configurar para llegar a una red remota específica. Las rutas estáticas IPv4 se configuran con el comando de configuración global **ip route***máscara de red* {*ip-siguiente-salto* | *interfaz-salida*}. Las rutas estáticas se identifican en la tabla de routing con el código “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, utilice el comando de configuración global **ip route 0.0.0.0 0.0.0.0** {*interfaz-salida* | *ip-siguiente-salto*}.

En la ilustración, se proporciona una situación simple sobre cómo se pueden aplicar las rutas predeterminadas y estáticas.



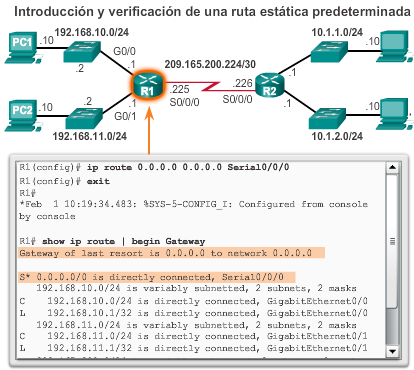
En la figura 1, se muestra la configuración de una ruta estática predeterminada IPv4 en el R1 a la interfaz Serial 0/0/0. Observe que la configuración de la ruta generó una entrada “S\*” en la tabla de routing. La “S” significa que el origen de la ruta es una ruta estática, mientras que el asterisco (**\***) indica que esta ruta es una posible candidata para ser la ruta predeterminada. De hecho, se eligió como ruta predeterminada, como se observa en la línea que dice “Gateway of Last Resort is 0.0.0.0 to network 0.0.0.0.” (El gateway de último recurso es 0.0.0.0 para la red 0.0.0.0).

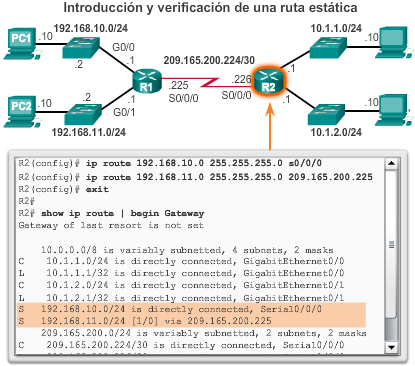
En la figura 2, se muestra la configuración de dos rutas estáticas del R2 para llegar a las dos LAN en el R1. La ruta a 192.168.10.0/24 se configuró con la interfaz de salida, mientras que la ruta a 192.168.11.0/24 se configuró con la dirección IPv4 de siguiente salto. Si bien ambas son aceptables, existen algunas diferencias con respecto a la forma en que funcionan. Por ejemplo, observe que se ven diferentes en la tabla de routing. Observe también que, debido a que estas rutas estáticas estaban dirigidas a redes específicas, el resultado indica que no se estableció el gateway de último recurso.

**Nota:** las rutas estáticas y las estáticas predeterminadas se explican en detalle en el capítulo siguiente.

Utilice el verificador de sintaxis de la figura 3 para configurar una ruta estática predeterminada en el router R1 que vaya al R2.

Utilice el verificador de sintaxis de la figura 4 para configurar rutas estáticas en el router R2 para llegar a las LAN del R1.





Como en IPv4, IPv6 admite rutas estáticas y estáticas predeterminadas. Estas se usan y se configuran como las rutas estáticas IPv4.

Para configurar una ruta estática predeterminada IPv6, utilice el comando de configuración global **ipv6 route ::/0**{*dirección-ipv6*|*tipo-interfaz número-interfaz*}.

En la figura 1, se muestra la configuración de una ruta estática predeterminada en el R1 a la interfaz Serial 0/0/0.

Observe que, en el resultado que se muestra en la figura 2, la configuración de la ruta estática predeterminada generó una entrada “S” en la tabla de routing. La “S” significa que el origen de la ruta es una ruta estática. A diferencia de las rutas estáticas IPv4, no figura ningún asterisco (\*) ni se identifica ningún gateway de último recurso de forma explícita.

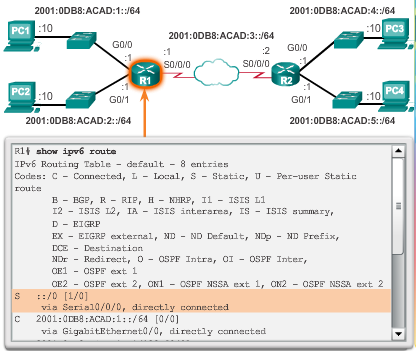
Como en IPv4, las rutas estáticas son rutas configuradas explícitamente para llegar a una red remota específica. Las rutas estáticas IPv6 se configuran con el comando de configuración global **ipv6 route***prefijo-ipv6/longitud-prefijo*{*dirección-ipv6*|*tipo-interfaz número-interfaz*}.

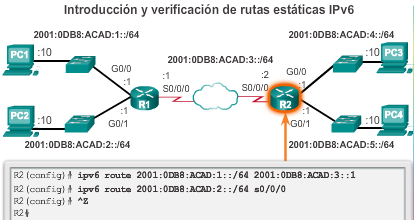
En el ejemplo de la figura 3, se muestra la configuración de dos rutas estáticas del R2 para llegar a las dos LAN en el R1. La ruta a la LAN 2001:0DB8:ACAD:2::/64 se configuró con una interfaz de salida, mientras que la ruta a la LAN 2001:0DB8:ACAD:1::/64 se configuró con la dirección IPv6 de siguiente salto. La dirección IPv6 de siguiente salto puede ser una dirección de unidifusión global o link-local de IPv6.

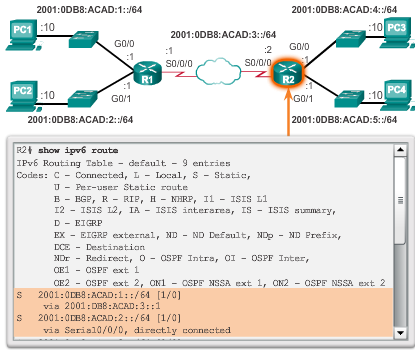
En la figura 4, se muestra la tabla de routing con las nuevas rutas estáticas instaladas.

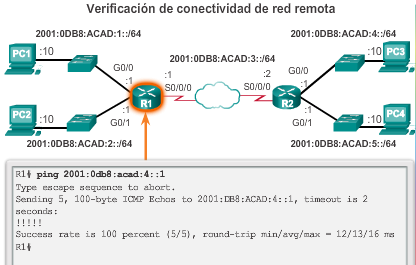
En la figura 5, se confirma la conectividad de red remota del R1 a la LAN 2001:0DB8:ACAD:4::/64 en el R2.











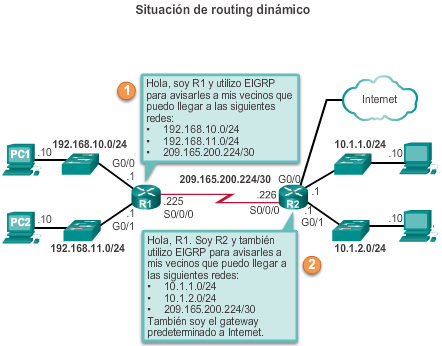
### Protocolos de enrutamiento dinámico

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.

En la ilustración, se proporciona una situación simple sobre cómo dos routers vecinos intercambiarían inicialmente la información de routing. En este mensaje simplificado, el R1 de intercambio se presenta y detalla las redes que puede alcanzar. El R2 responde y proporciona sus redes al R1.



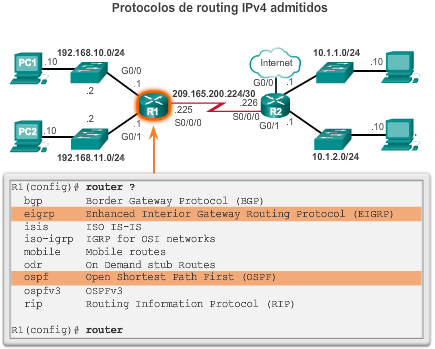
Un router que ejecuta un protocolo de routing dinámico no solo determina la mejor ruta hacia una red, sino que también determina una nueva mejor ruta si la ruta inicial se vuelve inutilizable (o si cambia la topología). Por estos motivos, los protocolos de enrutamiento dinámico representan una ventaja 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 ISR Cisco admiten diversos protocolos de routing dinámico IPv4, incluidos los siguientes:

* **EIGRP:** protocolo de routing de gateway interior mejorado
* **OSPF:** Open Shortest Path First
* **IS-IS:** Intermediate System-to-Intermediate System
* **RIP:** protocolo de información de routing

Para determinar qué protocolos de routing admite IOS, use el comando **router ?**en el modo de configuración global, como se muestra en la ilustración.

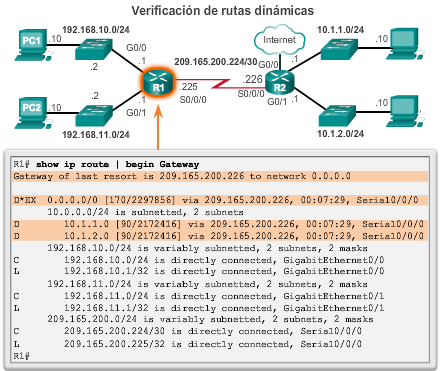
**Nota:** este curso se centra en EIGRP y OSPF. RIP se analizará solo por motivos de antigüedad; el resto de los protocolos de routing que admite IOS exceden el ámbito de la certificación CCNA.



En este ejemplo de routing dinámico, suponga que el R1 y el R2 se configuraron para admitir el protocolo de routing dinámico EIGRP. Los routers también anuncian las redes conectadas directamente. El R2 anuncia que es el gateway predeterminado a otras redes.

En el resultado de la ilustración, se muestra la tabla de routing del R1 después del intercambio de actualizaciones y la convergencia de los routers. Además de la interfaz conectada y la interfaz link-local, hay tres entradas “D” en la tabla de routing.

* La entrada que comienza con “D\*EX” identifica que el origen de esta entrada fue EIGRP (“D"). La ruta es candidata a ser una ruta predeterminada (“\*”) y es una ruta externa (“\*EX”) reenviada por EIGRP.
* Las otras dos entradas “D” son rutas instaladas en la tabla de routing según la actualización del R2 que anuncia sus LAN.

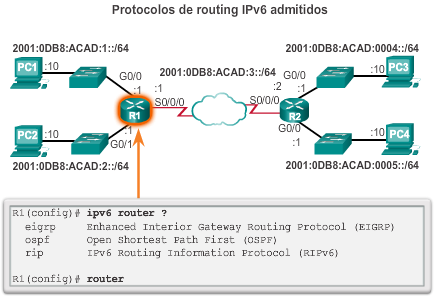


Como se muestra en la ilustración, los routers ISR admiten protocolos de routing dinámico IPv6, incluidos los siguientes:

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

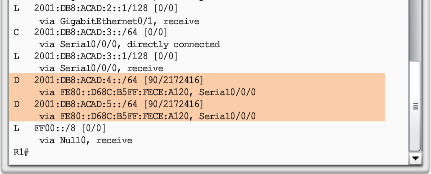
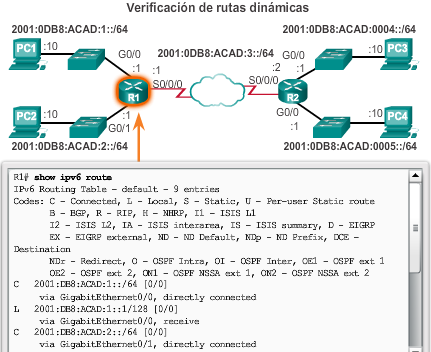
La compatibilidad con los protocolos de routing dinámico IPv6 depende del hardware y la versión del IOS. La mayoría de las modificaciones en los protocolos de routing se hacen para admitir direcciones IPv6 más largas y estructuras de encabezado diferentes.

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



Los routers R1 y R2 se configuraron con el protocolo de routing dinámico EIGRP para IPv6. (Este es el equivalente a EIGRP para IPv4 en IPv6).

Para ver la tabla de routing en el R1, introduzca el comando **show ipv6 route**, como se muestra en la ilustración. En el resultado de la ilustración, se muestra la tabla de routing del R1 después del intercambio de actualizaciones y la convergencia de los routers. Además de las rutas conectadas y locales, hay dos entradas “D” (rutas EIGRP) en la tabla de routing.



## Resumen

Existen muchas características clave relacionadas con las estructuras y el rendimiento a las cuales nos referimos cuando hablamos de redes: topología, velocidad, costo, seguridad, disponibilidad, escalabilidad y confiabilidad.

Los routers y los switches Cisco tienen muchas similitudes: admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Una característica que distingue a los switches de los routers es el tipo de interfaces que admite cada uno. Una vez que se configuró una interfaz en ambos dispositivos, se deben utilizar los comandos show adecuados para verificar que la interfaz funcione.

El objetivo principal de un router es conectar múltiples redes y reenviar paquetes desde una red a la siguiente. Esto significa que un router normalmente tiene múltiples interfaces. Cada interfaz es un miembro o host en una red IP diferente.

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 tabla de routing es una lista de redes que conoce el router. La tabla de enrutamiento incluye direcciones de red para sus propias interfaces que son las redes conectadas directamente, además de direcciones de red para redes remotas. Una red remota es una red a la que se puede llegar únicamente reenviando el paquete a otro router.

Las redes remotas se agregan a la tabla de routing de dos maneras: por el administrador de red que configura manualmente las rutas estáticas o implementando un protocolo de routing dinámico. Las rutas estáticas no tienen tanta sobrecarga como los protocolos de enrutamiento dinámico; sin embargo, las rutas estáticas requieren más mantenimiento si la topología es inestable o está en constante cambio.

Los protocolos de enrutamiento dinámico se ajustan automáticamente a los cambios sin intervención alguna del administrador de la red. Los protocolos de enrutamiento dinámico requieren más procesamiento de la CPU y además usan una cierta cantidad de capacidad de enlace para mensajes y actualizaciones de enrutamiento. En muchos casos, una tabla de enrutamiento tendrá tanto rutas estáticas como dinámicas.

Los routers toman su decisión principal de reenvío en la Capa 3, la capa de Red. Sin embargo, las interfaces del router participan en las capas 1, 2 y 3. Los paquetes IP de capa 3 se encapsulan en una trama de enlace de datos de capa 2 y se codifican en bits en la capa 1. Las interfaces del router participan en los procesos de capa 2 asociados a la encapsulación. Por ejemplo, una interfaz Ethernet en un router participa en el proceso ARP como otros hosts en esa LAN.

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes.

Los componentes de la tabla de routing IPv6 son muy similares a los de la tabla de routing IPv4. Por ejemplo, se completa con las interfaces conectadas directamente, con las rutas estáticas y con las rutas descubiertas de forma dinámica.

