# Routing dinámico

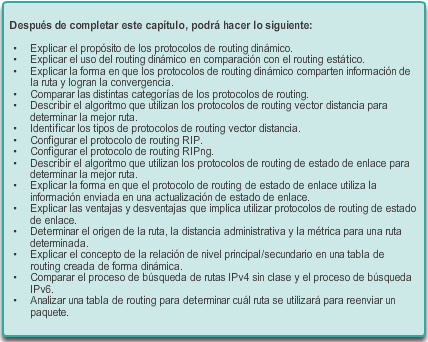
## Introducción

Las redes de datos que usamos en nuestras vidas cotidianas para aprender, jugar y trabajar varían desde pequeñas redes locales hasta grandes internetworks globales. En el hogar, un usuario puede tener un router y dos o más computadoras. En el trabajo, una organización probablemente tenga varios routers y switches para atender las necesidades de comunicación de datos de cientos o hasta miles de computadoras.

Los routers reenvían paquetes mediante el uso de la información de la tabla de routing. Los routers pueden descubrir las rutas hacia las redes remotas de dos maneras: de forma estática y de forma dinámica.

En una red grande con muchas redes y subredes, la configuración y el mantenimiento de rutas estáticas entre dichas redes conllevan una sobrecarga administrativa y operativa. Esta sobrecarga administrativa es especialmente tediosa cuando se producen cambios en la red, como un enlace fuera de servicio o la implementación de una nueva subred. Implementar protocolos de routing dinámico puede aliviar la carga de las tareas de configuración y de mantenimiento, además de proporcionar escalabilidad a la red.

En este capítulo, se presentan los protocolos de routing dinámico, se exploran los beneficios de utilizar esta clase de protocolos, la forma en que se clasifican los distintos protocolos de routing y las métricas que utilizan los protocolos de routing para determinar la mejor ruta para el tráfico de la red. Entre otros temas que se analizan en este capítulo, se encuentran las características de los protocolos de routing dinámico y la forma en que se diferencian los distintos protocolos de routing. Los profesionales de red deben comprender cuáles son los diferentes protocolos de routing disponibles a fin de decidir fundadamente cuándo utilizar routing dinámico o estático. También necesitan saber cuál es el protocolo de routing dinámico más adecuado en un entorno de red determinado.





## Protocolos de enrutamiento dinámico

### Funcionamiento del protocolo de enrutamiento dinámico

Los protocolos de routing dinámico se utilizan en el ámbito de las redes desde finales de la década de los ochenta. Uno de los primeros protocolos de routing fue el protocolo de información de routing (RIP). Si bien el protocolo RIP versión 1 (RIPv1) se lanzó en 1988, ya en 1969 se utilizaban algunos de los algoritmos básicos en dicho protocolo en la Advanced Research Projects Agency Network (ARPANET).

A medida que las redes evolucionaron y se volvieron más complejas, surgieron nuevos protocolos de routing. El protocolo de routing RIP se actualizó a RIPv2 a fin de admitir el crecimiento del entorno de red. Sin embargo, la versión más nueva de RIP aún no es escalable a las implementaciones de red más extensas de la actualidad. Con el objetivo de satisfacer las necesidades de las redes más grandes, se desarrollaron dos protocolos de routing: el protocolo OSPF (Open Shortest Path First) e Intermediate System-to-Intermediate System (IS-IS). Cisco desarrolló el protocolo de routing de gateway interior (IGRP) e IGRP mejorado (EIGRP), que también tiene buena escalabilidad en implementaciones de redes más grandes.

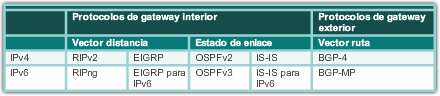
Asimismo, surgió la necesidad de conectar distintas internetworks y proporcionar routing entre ellas. En la actualidad, se utiliza el protocolo de gateway fronterizo (BGP) entre proveedores de servicios de Internet (ISP). El protocolo BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de routing.

En la figura 1, se muestra la línea cronológica de la introducción de los diversos protocolos.

En la figura 2, se clasifican los protocolos.

Con la llegada de numerosos dispositivos que usan IP para consumidores, el espacio de direccionamiento IPv4 quedó prácticamente agotado, por lo que surgió IPv6. A fin de admitir la comunicación basada en IPv6, se desarrollaron versiones más nuevas de los protocolos de routing IP (consulte la fila de IPv6 en la ilustración).

RIP es el más simple de los protocolos de routing dinámico y, en esta sección, se utiliza para proporcionar un nivel básico de comprensión sobre los protocolos de routing.



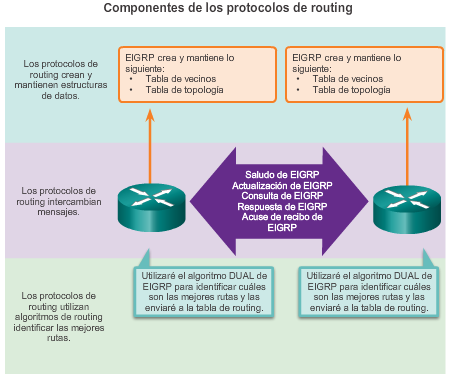
Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo. El propósito de los protocolos de routing dinámico incluye lo siguiente:

* Descubrir redes remotas
* Mantener la información de enrutamiento actualizada
* Escoger el mejor camino hacia las redes de destino
* Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible

Los componentes principales de los protocolos de routing dinámico incluyen los siguientes:

* **Estructuras de datos:** por lo general, los protocolos de routing utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.
* **Mensajes del protocolo de routing:**los protocolos de routing usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de routing y realizar otras tareas para descubrir la red y conservar información precisa acerca de ella.
* **Algoritmo:** un algoritmo es una lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.

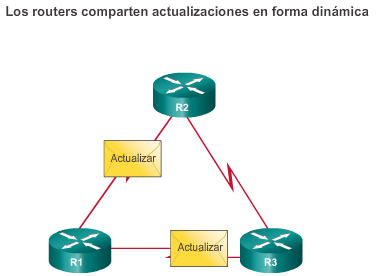
En la ilustración, se destacan las estructuras de datos, los mensajes del protocolo de routing y el algoritmo de routing que utiliza EIGRP.



Los protocolos de routing permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esa información automáticamente a sus propias tablas de routing. Consulte la animación en la ilustración.

Los protocolos de routing determinan la mejor ruta hacia cada red y, a continuación, esa ruta se agrega a la tabla de routing. Uno de los beneficios principales de los protocolos de routing dinámico es que los routers intercambian información de routing cuando se produce un cambio en la topología. Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, usar protocolos de routing dinámico implica el costo de dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y ancho de banda del enlace de red. Pese a los beneficios del enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar. En algunas ocasiones el enrutamiento estático es más apropiado, mientras que en otras, el enrutamiento dinámico es la mejor opción. Las redes con niveles moderados de complejidad pueden tener routing estático y routing dinámico configurados.



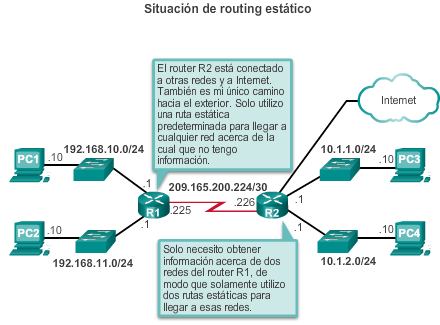
### Comparación entre routing dinámico y estático

Antes de identificar los beneficios de los protocolos de routing dinámico, considere los motivos por los que los profesionales de red utilizan el routing estático. El routing dinámico definitivamente tiene varias ventajas sobre el routing estático, sin embargo, el routing estático todavía se utiliza en redes hoy en día. De hecho, las redes generalmente usan una combinación de enrutamiento estático y dinámico.

El enrutamiento estático tiene varios usos principales, entre ellos:

* Facilita el mantenimiento de la tabla de enrutamiento en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
* Realiza routing desde y hacia una red de rutas internas, que es una red con una sola ruta predeterminada hacia fuera y sin conocimiento de redes remotas.
* Permite acceder a una única ruta predeterminada (la cual se utiliza para representar una ruta hacia cualquier red que no tiene una coincidencia más específica con otra ruta en la tabla de routing).

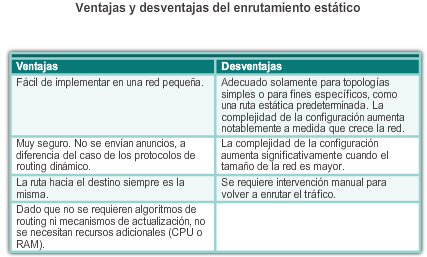
En la ilustración, se proporciona una situación de ejemplo de routing estático.



En la tabla de la ilustración, se destacan las ventajas y las desventajas del routing estático. El routing estático es fácil de implementar en redes pequeñas. Las rutas estáticas permanecen sin alteraciones, lo que hace que sea relativamente fácil llevar a cabo la resolución de problemas. Las rutas estáticas no envían mensajes de actualización y, por lo tanto, ocasionan muy poca sobrecarga.

Las desventajas del routing estático incluyen las siguientes:

* No es fácil de implementar en redes grandes.
* La administración de las configuraciones estáticas puede llevar mucho tiempo.
* Si un enlace falla, una ruta estática no puede volver a enrutar el tráfico.

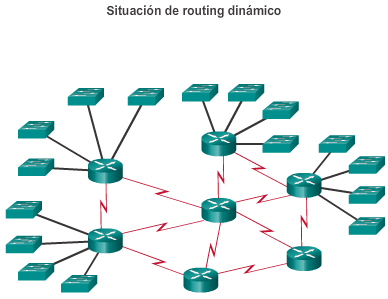


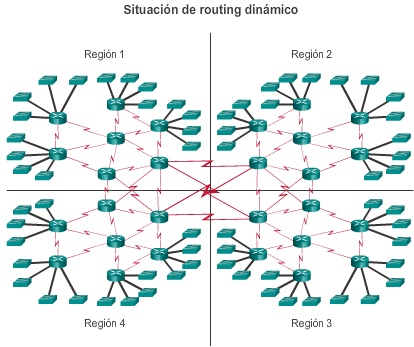
Los protocolos de routing dinámico ayudan al administrador de red a administrar el proceso riguroso y lento de configuración y mantenimiento de rutas estáticas.

Imagine tener que mantener las configuraciones de routing estático para los siete routers en figura 1.

¿Qué sucedería si la empresa creciera y ahora tuviera cuatro regiones y 28 routers para administrar, como se muestra en la figura 2? ¿Qué sucede cuando un enlace deja de funcionar? ¿Cómo se asegura de que las rutas redundantes estén disponibles?

El routing dinámico es la mejor opción para redes grandes como la que se muestra.

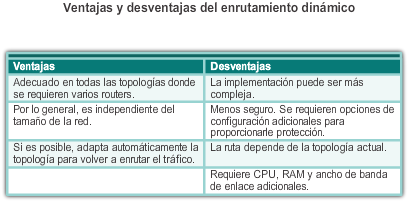


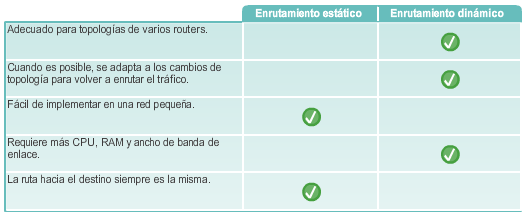


En la tabla de la ilustración, se destacan las ventajas y las desventajas del routing dinámico. Los protocolos de routing dinámico funcionan bien en cualquier tipo de red conformada por varios routers. Son escalables y determinan automáticamente las mejores rutas si se produce un cambio en la topología. Si bien existen otros aspectos para tener en cuenta respecto de la configuración de los protocolos de routing dinámico, son simples de configurar en redes grandes.

El routing dinámico presenta desventajas. Esta clase de routing requiere conocer comandos adicionales. Además, es menos seguro que el routing estático, porque las interfaces identificadas por el protocolo de routing envían actualizaciones de routing fuera de la red. Las rutas tomadas pueden variar entre paquetes. El algoritmo de routing utiliza CPU, RAM y ancho de banda de enlace adicionales.

Observe la forma en que el routing dinámico aborda las desventajas del routing estático.





### Aspectos básicos de la operación de los protocolos de routing

Todos los protocolos de routing están diseñados para descubrir redes remotas y adaptarse rápidamente cuando ocurre un cambio en la topología. El método que usa un protocolo de enrutamiento para lograr su propósito depende del algoritmo que use y de las características operativas de ese protocolo.

En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

1. El router envía y recibe mensajes de enrutamiento en sus interfaces.

2. El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.

3. Los routers intercambian información de enrutamiento para obtener información sobre redes remotas.

4. Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

Todos los protocolos de routing siguen los mismos patrones de funcionamiento. Para ayudar a ilustrar esto, considere la siguiente situación en la que los tres routers ejecutan RIPv2.

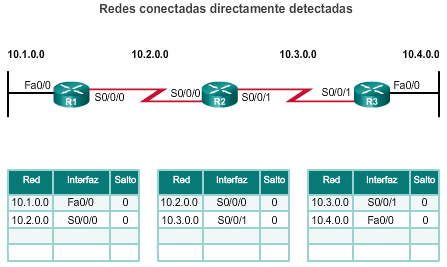
Cuando un router se enciende, no tiene ninguna información sobre la topología de la red. Ni siquiera tiene conocimiento de que existen dispositivos en el otro extremo de sus enlaces. La única información que tiene un router proviene de su propio archivo de configuración almacenado en la NVRAM. Una vez que se un router arranca correctamente, aplica la configuración guardada. Si el direccionamiento IP está configurado de forma correcta, en primer lugar el router detecta sus propias redes conectadas directamente.

Haga clic en Reproducir en la ilustración para ver una animación de la detección inicial de las redes conectadas para cada router.

Observe la forma en que los routers avanzan a través del proceso de arranque y luego detectan las redes conectadas directamente y las máscaras de subred. Esta información se agrega a sus tablas de routing de la siguiente manera:

* El R1 agrega la red 10.1.0.0 disponible a través de la interfaz FastEthernet 0/0, y 10.2.0.0 está disponible a través de la interfaz Serial 0/0/0.
* El R2 agrega la red 10.2.0.0 disponible a través de la interfaz Serial 0/0/0, y 10.3.0.0 está disponible a través de la interfaz Serial 0/0/1.
* El R3 agrega la red 10.3.0.0 disponible a través de la interfaz Serial 0/0/1, y 10.4.0.0 está disponible a través de la interfaz FastEthernet 0/0.

Con esta información inicial, los routers proceden a encontrar orígenes de ruta adicionales para sus tablas de routing.



Después del arranque inicial y del descubrimiento, la tabla de routing se actualiza con todas las redes conectadas directamente y las interfaces en las que residen dichas redes.

Si se configura un protocolo de routing, el siguiente paso es que el router comience a intercambiar actualizaciones de routing para obtener información sobre rutas remotas.

El router envía un paquete de actualización por todas las interfaces habilitadas en el router. La actualización contiene la información de la tabla de routing, que en este momento consta de todas las redes conectadas directamente.

Al mismo tiempo, el router también recibe y procesa actualizaciones similares de otros routers conectados. Una vez recibida la actualización, el router revisa si contiene información de red nueva, y se agrega a la tabla de routing toda red que no esté incluida en ella aún.

Para ver la configuración de la topología entre tres routers (R1, R2 y R3), consulte la ilustración. Sobre la base de esta topología, a continuación se muestra una lista de las distintas actualizaciones que el R1, el R2 y el R3 envían y reciben durante la convergencia inicial.

R1:

* Envía una actualización acerca de la red 10.1.0.0 desde la interfaz serial 0/0/0.
* Envía una actualización acerca de la red 10.2.0.0 desde la interfaz FastEthernet0/0.
* Recibe una actualización de R2 de la red 10.3.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.3.0.0 en la tabla de enrutamiento con una métrica de 1.

R2:

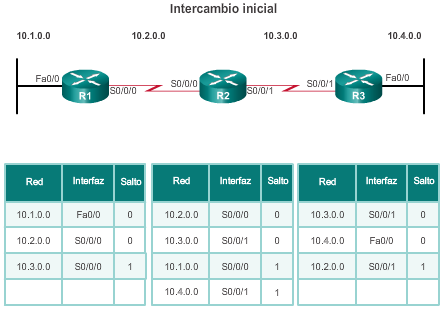
* Envía una actualización acerca de la red 10.3.0.0 desde la interfaz serial 0/0/0.
* Envía una actualización acerca de la red 10.2.0.0 desde la interfaz serial 0/0/1.
* Recibe una actualización del R1 de la red 10.1.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.1.0.0 en la tabla de enrutamiento con una métrica de 1.
* Recibe una actualización del R3 de la red 10.4.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.4.0.0 en la tabla de enrutamiento con una métrica de 1.

R3:

* Envía una actualización acerca de la red 10.4.0.0 desde la interfaz serial 0/0/1.
* Envía una actualización acerca de la red 10.3.0.0 desde la interfaz FastEthernet0/0.
* Recibe una actualización del R2 de la red 10.2.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.2.0.0 en la tabla de enrutamiento con una métrica de 1.

Haga clic en Reproducir en la ilustración para ver una animación sobre la forma en que el R1, el R2 y el R3 comienzan el intercambio inicial.

Después de esta primera ronda de intercambios de actualizaciones, cada router tiene información acerca de las redes conectadas de sus vecinos conectados directamente. Sin embargo, ¿observó que R1 todavía no tiene información acerca de 10.4.0.0 al igual que R3 acerca de 10.1.0.0? La red convergente no tiene lugar ni se obtiene información completa hasta que se produce otro intercambio de información de routing.



En este punto, los routers tienen información sobre sus propias redes conectadas directamente y las de sus vecinos más cercanos. Siguiendo el camino hacia la convergencia, los routers intercambian la siguiente ronda de actualizaciones periódicas. Cada router verifica las actualizaciones nuevamente para comprobar si hay información nueva.

Para ver la configuración de la topología entre tres routers (R1, R2 y R3), consulte la ilustración. Una vez que se completa el descubrimiento inicial, cada router continúa el proceso de convergencia mediante el envío y la recepción de las siguientes actualizaciones.

R1:

* Envía una actualización acerca de la red 10.1.0.0 por la interfaz Serial 0/0/0.
* Envía una actualización de las redes 10.2.0.0 y 10.3.0.0 por la interfaz FastEthernet0/0.
* Recibe una actualización del R2 de la red 10.4.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.4.0.0 en la tabla de routing con el valor de métrica 2.
* La misma actualización del R2 contiene información acerca de la red 10.3.0.0 con el valor de métrica 1. No se produce ningún cambio, la información de routing permanece igual.

R2:

* Envía una actualización acerca de las redes 10.3.0.0 y 10.4.0.0 por la interfaz Serial 0/0/0.
* Envía una actualización acerca de las redes 10.1.0.0 y 10.2.0.0 por la interfaz Serial 0/0/1.
* Recibe una actualización de R1 acerca de la red 10.1.0.0. No se produce ningún cambio, por lo que la información de routing permanece igual.
* Recibe una actualización de R3 acerca de la red 10.4.0.0. No se produce ningún cambio, por lo que la información de routing permanece igual.

R3:

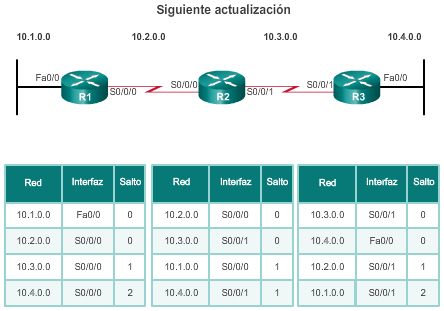
* Envía una actualización acerca de la red 10.4.0.0 desde la interfaz serial 0/0/1.
* Envía una actualización de las redes 10.2.0.0 y 10.3.0.0 por la interfaz FastEthernet0/0.
* Recibe una actualización del R2 de la red 10.1.0.0 e incrementa el conteo de saltos en 1.
* Almacena la red 10.1.0.0 en la tabla de routing con el valor de métrica 2.

La misma actualización del R2 contiene información acerca de la red 10.2.0.0 con el valor de métrica 1. No se produce ningún cambio, por lo que la información de routing permanece igual.

Haga clic en Reproducir en la ilustración para ver una animación sobre la forma en que el R1, el R2 y el R3 envían la tabla de routing más reciente a sus vecinos.

Por lo general, los protocolos de routing vector distancia implementan una técnica para evitar los bucles de routing conocida como “horizonte dividido”. El horizonte dividido evita que la información se envíe desde la misma interfaz en la que se recibió dicha información. Por ejemplo, el R2 no envía una actualización que contenga la red 10.1.0.0 por la interfaz Serial 0/0/0, debido a que obtuvo información acerca de la red 10.1.0.0 a través de la interfaz Serial 0/0/0.

Una vez que los routers dentro de una red realizan la convergencia, el router puede utilizar la información que se encuentra en la tabla de rutas para determinar la mejor ruta para llegar a un destino. Los distintos protocolos de routing tienen diferentes maneras de calcular la mejor ruta.

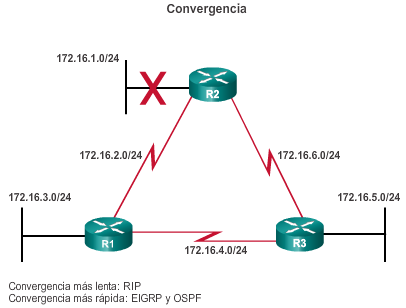


La convergencia de la red se produce cuando todos los routers tienen información completa y precisa acerca de toda la red, como se muestra en la figura 1. El tiempo de convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia breves.

La convergencia es cooperativa e independiente al mismo tiempo. Los routers comparten información entre sí, pero deben calcular en forma independiente los impactos del cambio de topología en sus propias rutas. Dado que establecen un acuerdo con la nueva topología en forma independiente, se dice que convergen sobre este consenso.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de los caminos óptimos. La velocidad de propagación se refiere al tiempo que tardan los routers dentro de la red en reenviar la información de routing.

Como se muestra en la figura 2, los protocolos de routing pueden clasificarse según la velocidad de convergencia: cuanto más rápida sea la convergencia, mejor será el protocolo de routing. Generalmente, los protocolos más antiguos, como RIP, tienen una convergencia lenta, mientras que los protocolos modernos, como EIGRP y OSPF, la realizan más rápidamente.



### Tipos de protocolos de routing

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características. Específicamente, los protocolos de routing se pueden clasificar:

* **Propósito:** protocolo de gateway interior (IGP) o protocolo de gateway exterior (EGP)
* **Operación:** vector distancia, protocolo de estado de enlace, protocolo vector ruta
* **Comportamiento:** protocolo con clase (antiguo) o protocolo sin clase

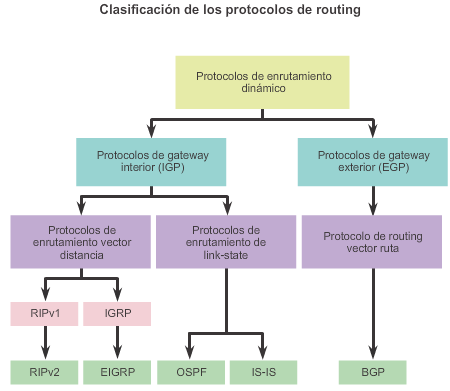
Por ejemplo, los protocolos de routing IPv4 se clasifican de la siguiente manera:

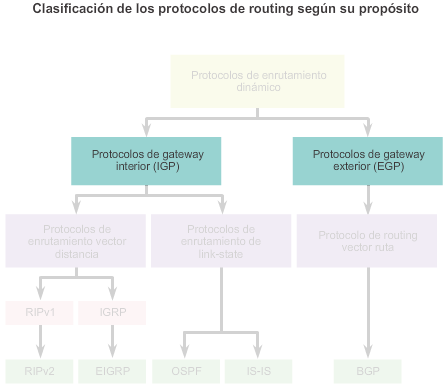
* **RIPv1 (antiguo):** IGP, vector distancia, protocolo con clase
* **IGRP (antiguo):** IGP, vector distancia, protocolo con clase desarrollado por Cisco (cayó en desuso a partir del IOS 12.2)
* **RIPv2:** IGP, vector distancia, protocolo sin clase
* **EIGRP:** IGP, vector distancia, protocolo sin clase desarrollado por Cisco
* **OSPF:** IGP, estado de enlace, protocolo sin clase
* **IS-IS:** IGP, estado de enlace, protocolo sin clase
* **BGP:** EGP, vector ruta, protocolo sin clase

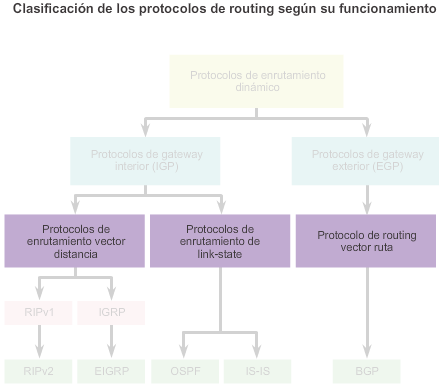
Los protocolos de routing con clase, RIPv1 e IGRP, son protocolos antiguos y se utilizan solamente en redes antiguas. Estos protocolos de routing se convirtieron en los protocolos de routing sin clase RIPv2 y EIGRP, respectivamente. Los protocolos de routing de estado de enlace son protocolos sin clase naturalmente.

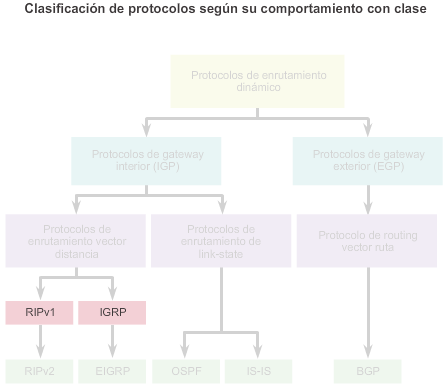
En la figura 1, se muestra una vista jerárquica de la clasificación de los protocolos de routing dinámico.

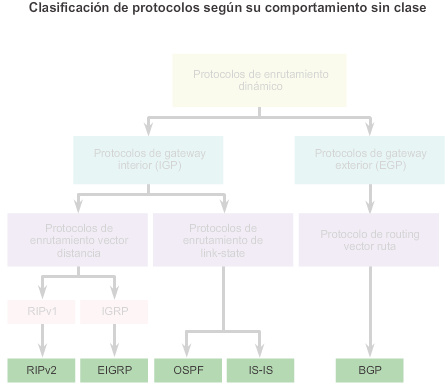
En las figuras 2 a 5, se destaca el propósito, la operación y el comportamiento de los diversos protocolos de routing.











Un sistema autónomo (AS) es un conjunto de routers bajo una administración común, como una empresa o una organización. Los AS también se conocen como “dominios de routing”. Los ejemplos típicos de AS son la red interna de una empresa y la red de un ISP.

Debido a que Internet se basa en el concepto de AS, se requieren dos tipos de protocolos de routing:

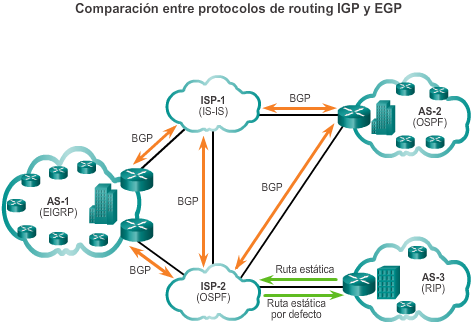
* **Protocolo de gateway interior (IGP):** se utiliza para el routing dentro de un AS. También se lo denomina “routing interno de AS”. Las empresas, las organizaciones e incluso los proveedores de servicios utilizan un IGP en sus redes internas. Los IGP incluyen RIP, EIGRP, OSPF e IS-IS.
* **Protocolo de gateway exterior (EGP):** se utiliza para el routing entre AS. Los proveedores de servicios y las empresas grandes pueden interconectarse mediante un EGP. El protocolo de gateway fronterizo (BGP) es el único EGP viable actualmente y es el protocolo de routing oficial utilizado por Internet.

**Nota:** dado que BGP es el único EGP disponible, no se suele utilizar el término EGP. En cambio, la mayoría de los ingenieros simplemente hacen referencia a BGP.

En el ejemplo de la ilustración, se proporcionan situaciones simples en las que se destaca la implementación de IGP, de BGP y del routing estático:

* **ISP-1:** es un AS que utiliza IS-IS como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
* **ISP-2:** es un AS que utiliza OSPF como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
* **AS-1:** se trata de una organización grande que utiliza EIGRP como IGP. Dado que es un entorno de host múltiples (es decir, se conecta a dos proveedores de servicios distintos), utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
* **AS-2:** se trata de una organización mediana y utiliza OSPF como IGP. También es un entorno de host múltiples, por lo que utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
* **AS-3:** se trata de una organización pequeña con routers más antiguos dentro del AS y utiliza RIP como IGP. Dado que tiene conexión simple (es decir, conecta a solo un proveedor de servicios), no se requiere BGP. En cambio, se implementa routing estático entre el AS y el proveedor de servicios.

**Nota:** BGP excede el ámbito de este curso, motivo por el cual no se lo describe en detalle.



“Vector distancia” significa que las rutas se anuncian proporcionando dos características:

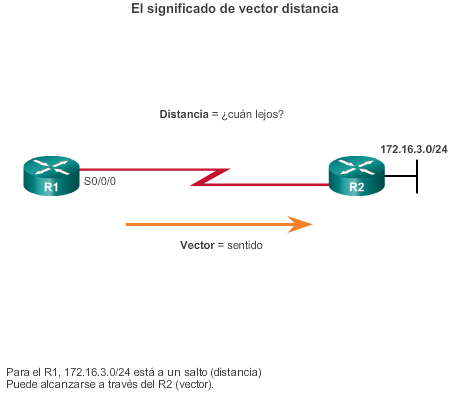
* **Distancia:** identifica la distancia hasta la red de destino. Se basa en una métrica como el conteo de saltos, el costo, el ancho de banda y el retraso, entre otros.
* **Vector:** especifica el sentido en que se encuentra el router de siguiente salto o la interfaz de salida para llegar al destino.

Por ejemplo, en la ilustración, el R1 tiene información de que la distancia para llegar a la red 172.16.3.0/24 es de un salto y de que el sentido es a través de la interfaz S0/0/0 hacia el R2.

Un router que utiliza un protocolo de enrutamiento vector distancia no tiene la información de la ruta completa hasta la red de destino. Los protocolos vector distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento vector distancia no tienen un mapa en sí de la topología de la red.

Hay cuatro IGP vector distancia IPv4:

* **RIPv1:** protocolo antiguo de primera generación
* **RIPv2:** protocolo de routing vector distancia simple
* **IGRP:** protocolo exclusivo de Cisco de primera generación (obsoleto y reemplazado por EIGRP)
* **EIGRP:** versión avanzada del routing vector distancia



A diferencia de la operación del protocolo de routing vector distancia, un router configurado con un protocolo de routing de estado de enlace puede crear una “vista completa” o una topología de la red al reunir información proveniente de todos los demás routers.

Para continuar con nuestra analogía de letreros, el uso de un protocolo de enrutamiento de link-state es como tener un mapa completo de la topología de la red. Los letreros a lo largo de la ruta de origen a destino no son necesarios, debido a que todos los routers de estado de enlace usan un mapa de la red idéntico. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología.

Los routers con RIP habilitado envían actualizaciones periódicas de su información de routing a sus vecinos. Los protocolos de enrutamiento de link-state no usan actualizaciones periódicas. Una vez que se produjo la convergencia de la red, la actualización del estado de enlace solo se envía cuando se produce un cambio en la topología. Por ejemplo, la actualización del estado de enlace en la animación no se envía hasta que la red 172.16.3.0 se desactiva.

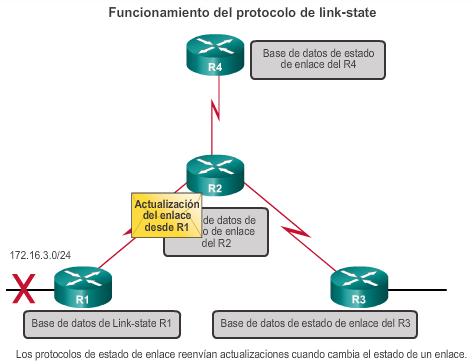
Haga clic en Reproducir en la ilustración para ver operaciones de estado de enlace.

Los protocolos de link-state funcionan mejor en situaciones donde:

* El diseño de red es jerárquico, lo cual suele suceder en redes extensas.
* La rápida convergencia de la red es crucial.
* Los administradores tienen un conocimiento cabal del protocolo de routing de estado de enlace implementado.

Hay dos IGP de estado de enlace IPv4:

* **OSPF:** protocolo de routing muy popular basado en estándares
* **IS-IS:** popular en redes de proveedores



La mayor diferencia entre los protocolos de routing con clase y sin clase es que los protocolos de routing con clase no envían información de la máscara de subred en sus actualizaciones de routing. Los protocolos de routing sin clase incluyen información de la máscara de subred en las actualizaciones de routing.

Los dos protocolos de routing IPv4 originales que se desarrollaron fueron RIPv1 e IGRP, que se crearon cuando las direcciones de red se asignaban según las clases (es decir, clase A, B o C). En ese entonces, no era necesario que un protocolo de routing incluyera la máscara de subred en la actualización de routing, debido a que era posible determinar la máscara de red sobre la base del primer octeto de la dirección de red.

**Nota:** solo RIPv1 e IGRP son protocolos con clase. El resto de los protocolos de routing IPv4 e IPv6 son protocolos sin clase. El direccionamiento con clase nunca fue parte de IPv6.

El hecho de que RIPv1 e IGRP no incluyan información de la máscara de subred en sus actualizaciones significa que no pueden proporcionar máscaras de subred de longitud variable (VLSM) ni routing entre dominios sin clase (CIDR).

Los protocolos de routing con clase también generan problemas en las redes no contiguas. Que una red sea no contigua significa que las subredes de la misma dirección de red principal con clase están separadas por una dirección de red con clase diferente.

Consulte la topología que se muestra en la figura 1 para ver una ilustración de las limitaciones del routing con clase. Observe que las LAN del R1 (172.16.1.0/24) y del R3 (172.16.2.0/24) son subredes de la misma red de clase B (172.16.0.0/16), que están separadas por distintas direcciones de red con clase (192.168.1.0/30 y 192.168.2.0/30).

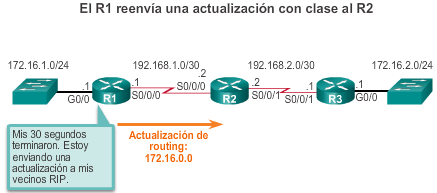
Cuando el R1 reenvía una actualización al R2, RIPv1 no incluye información de la máscara de subred con la actualización, sino que solamente reenvía la dirección de red de clase B 172.16.0.0.

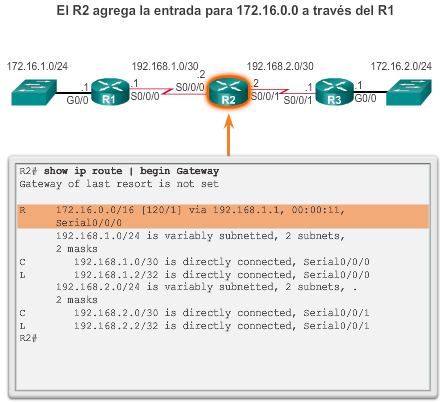
El R2 recibe la actualización y la procesa. A continuación, crea una entrada para la red de clase B 172.16.0.0/16 y la agrega en la tabla de routing, como se muestra en la figura 2.

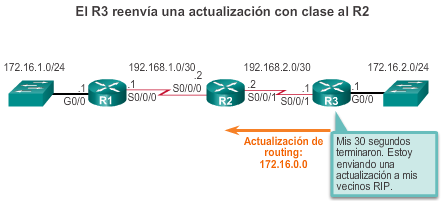
En la figura 3, se muestra que cuando el R3 reenvía una actualización al R2, tampoco incluye información de la máscara de subred y, por lo tanto, solamente reenvía la dirección de red con clase 172.16.0.0.

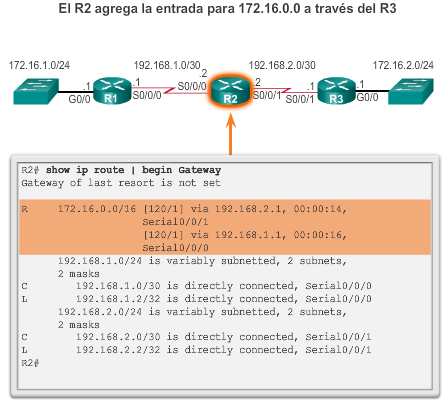
En la figura 4, el R2 recibe y procesa la actualización y agrega otra entrada para la dirección de red con clase 172.16.0.0/16 a su tabla de routing. Cuando hay dos entradas con métricas idénticas en la tabla de routing, el router comparte la carga de tráfico por igual entre los dos enlaces. Esto se conoce como “balanceo de carga”.

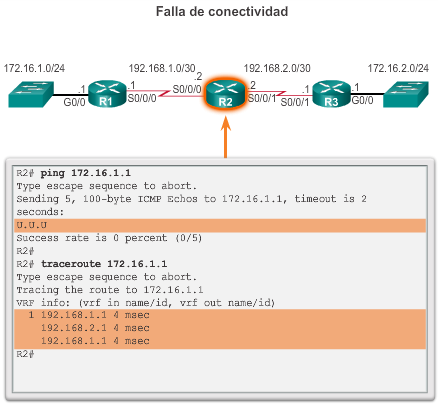
Como se muestra en la figura 5, esto tiene un efecto negativo sobre una red no contigua. Observe el comportamiento irregular de los comandos **ping** y **traceroute**.









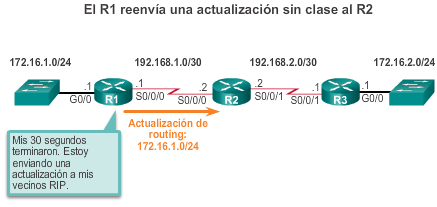


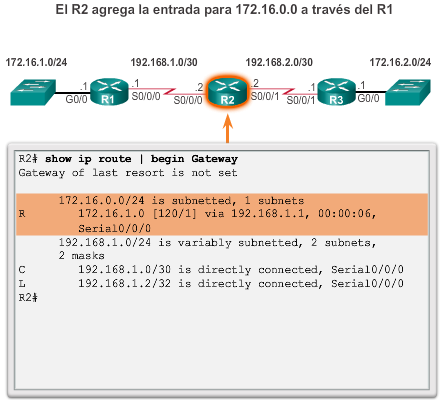
Las redes modernas ya no utilizan el direccionamiento IP con clase, y la máscara de subred no se puede determinar mediante el valor del primer octeto. Los protocolos de routing IPv4 sin clase (RIPv2, EIGRP, OSPF e IS-IS) incluyen la información de la máscara de con la dirección de red en las actualizaciones de routing. Los protocolos de routing sin clase admiten VLSM y CIDR.

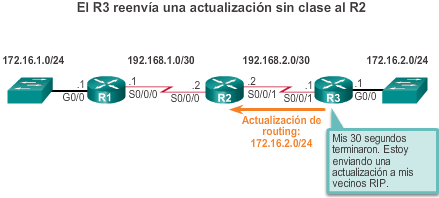
Los protocolos de routing IPv6 son protocolos sin clase. Por lo general, la distinción entre los protocolos de routing con clase y sin clase se aplica únicamente a los protocolos de routing IPv4. Se considera que todos los protocolos de routing IPv6 son protocolos sin clase, dado que incluyen la duración de prefijo con la dirección IPv6.

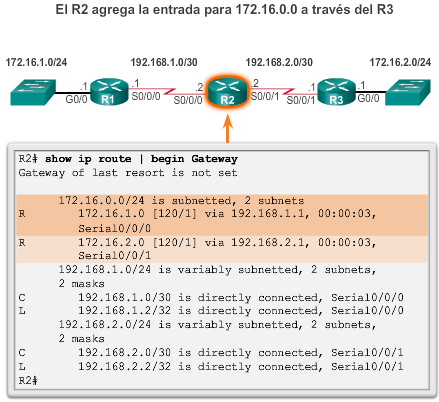
En las figuras 1 a 5, se ilustra la forma en que el routing sin clase resuelve los problemas que se generan con el routing con clase:

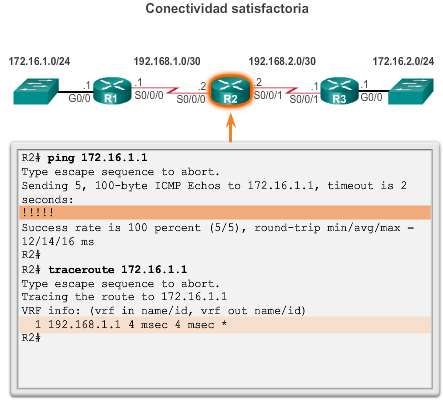
* **Figura 1:** en este diseño de red no contigua, se implementó el protocolo sin clase RIPv2 en los tres routers. Cuando el R1 reenvía una actualización al R2, RIPv2 incluye la información de la máscara de subred con la actualización 172.16.1.0/24.
* **Figura 2:** el R2 recibe, procesa y agrega dos entradas en la tabla de routing. En la primera línea, se muestra la dirección de red con clase 172.16.0.0 con la máscara de subred /24 de la actualización. Esto se conoce como “ruta principal”. En la segunda entrada, se muestra la dirección de red VLSM 172.16.1.0, con la dirección del siguiente salto y la salida. Esto se conoce como “ruta secundaria”. Las rutas principales nunca incluyen una interfaz de salida ni la dirección IP del siguiente salto.
* **Figura 3:** cuando el R3 reenvía una actualización al R2, RIPv2 incluye la información de la máscara de subred con la actualización 172.16.2.0/24.
* **Figura 4:** el R2 recibe, procesa y agrega otra entrada de ruta secundaria 172.16.2.0/24 debajo de la entrada de la ruta principal 172.16.0.0.
* **Figura 5:** ahora el R2 tiene información acerca de las redes divididas en subredes.







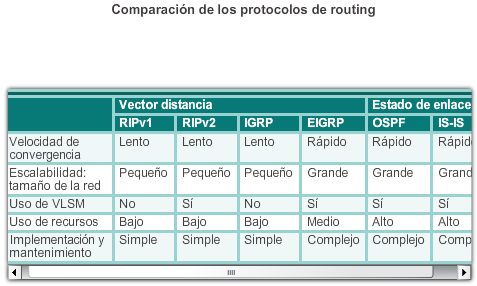




Los protocolos de enrutamiento se pueden comparar según las siguientes características:

* **Velocidad de convergencia**: define cuán rápido comparten información de routing y alcanzan un estado de conocimiento coherente los routers de la topología de la red. Cuanto más rápida sea la convergencia, más preferible será el protocolo. Los loops de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.
* **Escalabilidad**: define cuán grande puede ser una red, según el protocolo de routing implementado. Cuanto más grande sea la red, más escalable debe ser el protocolo de enrutamiento.
* **Con clase o sin clase (uso de VLSM):** los protocolos de routing con clase no incluyen la máscara de subred y no admiten VLSM. Los protocolos de routing sin clase incluyen la máscara de subred en las actualizaciones. Los protocolos de routing sin clase admiten VLSM y una mejor sumarización de ruta.
* **Uso de recursos**: incluye los requisitos de un protocolo de routing, como el espacio de memoria (RAM), la utilización de la CPU y el uso del ancho de banda del enlace. Una mayor cantidad de requisitos de recursos exige hardware más potente para admitir la operación del protocolo de routing además de los procesos de reenvío de paquetes.
* **Implementación y mantenimiento**: describen el nivel de conocimiento necesario para que un administrador de red ponga en funcionamiento y mantenga la red según el protocolo de routing implementado.

En la tabla de la ilustración, se resumen las características de cada protocolo de routing.

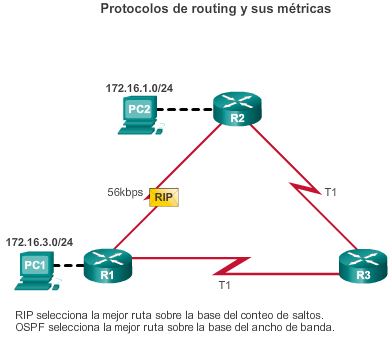


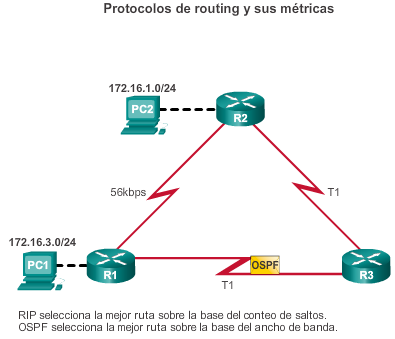
En algunos casos, un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Esto se logra mediante el uso de métricas de routing.

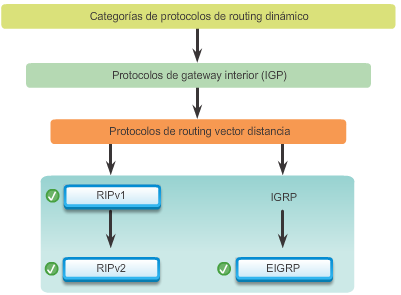
Una métrica es un valor mensurable que el protocolo de routing asigna a distintas rutas según la utilidad que tengan. En situaciones donde hay varias rutas hacia la misma red remota, las métricas de routing se utilizan para determinar el “costo” total de una ruta de origen a destino. Los protocolos de routing determinan la mejor ruta sobre la base del costo más bajo.

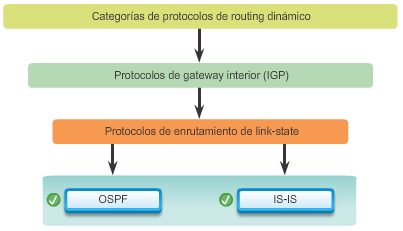
Los diferentes protocolos de enrutamiento pueden usar diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de routing distintos pueden elegir diferentes rutas hacia el mismo destino.

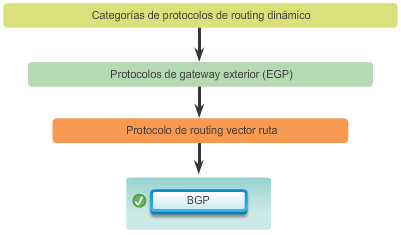
En la animación de la ilustración, se muestra que el protocolo RIP elegiría la ruta con la menor cantidad de saltos, mientras que el protocolo OSPF elegiría la ruta con el mayor ancho de banda.

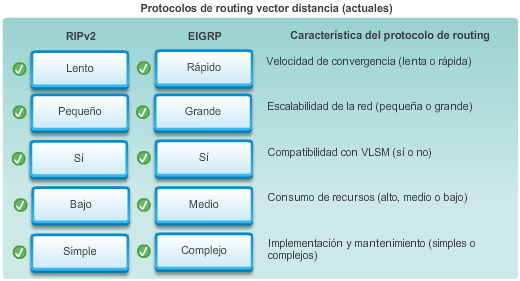




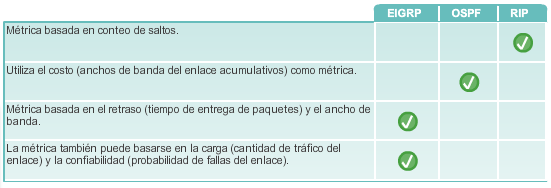












## Routing dinámico vector distancia

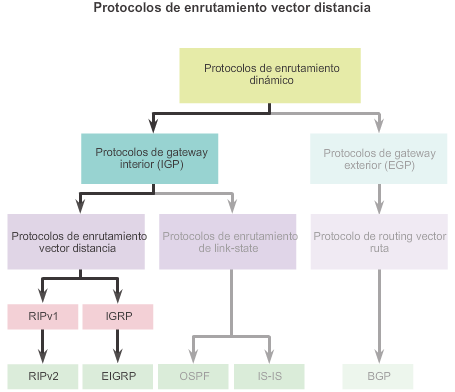
### Funcionamiento del protocolo de enrutamiento vector distancia

Los protocolos de routing vector distancia comparten actualizaciones entre vecinos. Los vecinos son routers que comparten un enlace y que están configurados para usar el mismo protocolo de enrutamiento. El router sólo conoce las direcciones de red de sus propias interfaces y las direcciones de red remota que puede alcanzar a través de sus vecinos. Los routers que utilizan el enrutamiento vector distancia no tienen información sobre la topología de la red.

Algunos protocolos de routing vector distancia envían actualizaciones periódicas. Por ejemplo, RIP envía una actualización periódica a todos sus vecinos cada 30 segundos; incluso si no se produce un cambio en la topología, RIP continúa enviando actualizaciones. Para llegar a todos sus vecinos, RIPv1 envía actualizaciones a la dirección IPv4 de todos los hosts 255.255.255.255 mediante una difusión.

La difusión de actualizaciones periódicas es ineficiente, debido a que las actualizaciones consumen ancho de banda y recursos de la CPU del dispositivo de red. Cada dispositivo de red debe procesar un mensaje de difusión. En cambio, RIPv2 y EIGRP utilizan direcciones de multidifusión, de modo que solamente reciben las actualizaciones los vecinos que las necesitan. EIGRP también puede enviar un mensaje de unidifusión solamente al vecino afectado. Además, EIGRP envía una actualización solo cuando se la necesita, en lugar de hacerlo en forma periódica.

Como se muestra en la ilustración, los dos protocolos de routing vector distancia IPv4 modernos son RIPv2 y EIGRP. RIPv1 e IGRP se incluyen solamente por motivos de precisión histórica.



El algoritmo de routing se encuentra en el centro del protocolo vector distancia. El algoritmo se utiliza para calcular los mejores caminos y después enviar dicha información a los vecinos.

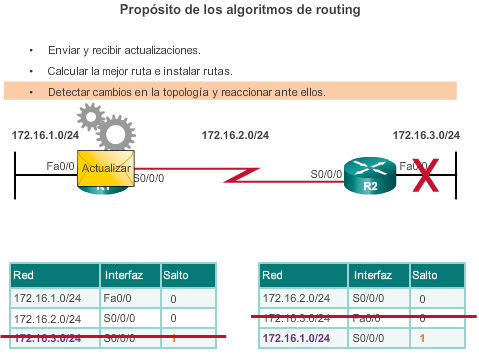
El algoritmo utilizado para los protocolos de enrutamiento define los siguientes procesos:

* El mecanismo para enviar y recibir información de routing.
* El mecanismo para calcular las mejores rutas e instalar rutas en la tabla de routing.
* El mecanismo para detectar cambios en la topología y reaccionar ante ellos.

En la animación de la ilustración, el R1 y el R2 están configurados con el protocolo de routing RIP. El algoritmo envía y recibe actualizaciones. Tanto R1 como R2 obtienen información nueva de la actualización. En este caso, cada router obtiene información acerca de una red nueva. El algoritmo de cada router realiza los cálculos de manera independiente y actualiza la tabla de enrutamiento con la información nueva. Cuando la LAN del R2 deja de funcionar, el algoritmo compone una actualización dirigida y la envía al R1. Luego, R1 elimina la red de la tabla de enrutamiento.

Los diferentes protocolos de enrutamiento utilizan diversos algoritmos para instalar rutas en la tabla de enrutamiento, enviar actualizaciones a los vecinos y determinar las rutas. Por ejemplo:

* RIP utiliza el algoritmo de Bellman-Ford como algoritmo de routing. Se basa en dos algoritmos desarrollados por Richard Bellman y Lester Ford júnior en 1958 y 1956.
* IGRP y EIGRP utilizan el algoritmo de actualización por difusión (DUAL) como algoritmo de routing, desarrollado por el Dr. J. J. Garcia-Luna-Aceves en SRI International.



### Tipos de protocolos de routing vector distancia

El protocolo de información de routing (RIP) era un protocolo de routing de primera generación para IPv4 especificado inicialmente en RFC 1058. Dado que es fácil de configurar, es una buena opción para redes pequeñas.

Las características clave del protocolo RIPv1 son las siguientes:

* Las actualizaciones de routing se transmiten por difusión (255.255.255.255) cada 30 segundos.
* Se utiliza el conteo de saltos como métrica para la selección de rutas.
* Se considera que un conteo de saltos de más de 15 saltos es infinito (demasiado alejado); el router del decimoquinto salto no propagaría la actualización de routing al siguiente router.

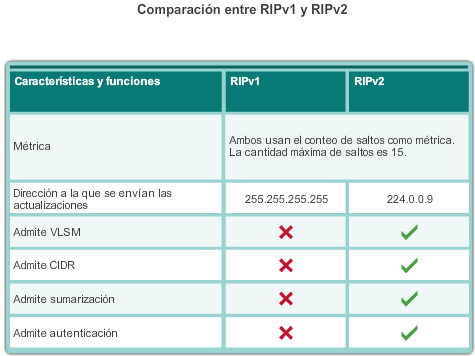
En 1993, RIPv1 evolucionó a un protocolo de routing sin clase conocido como “RIP versión 2” (RIPv2). RIPv2 introdujo las siguientes mejoras:

* **Protocolo de routing sin clase:** admite VLSM y CIDR, debido a que incluye la máscara de subred en las actualizaciones de routing.
* **Mayor eficiencia:** reenvía actualizaciones a la dirección de multidifusión 224.0.0.9, en lugar de a la dirección de difusión 255.255.255.255.
* **Entradas de routing reducidas:** admite la sumarización de ruta manual en cualquier interfaz.
* **Protección:** admite un mecanismo de autenticación para proteger las actualizaciones de la tabla de routing entre vecinos.

En la tabla de la ilustración, se resumen las diferencias entre RIPv1 y RIPv2.

Las actualizaciones RIP se encapsulan en un segmento UDP, con los números de puerto de origen y de destino establecidos en el puerto UDP 520.

En 1997, se lanzó la versión de RIP con IPv6 habilitado. RIPng se basa en RIPv2. Aún tiene una limitación de 15 saltos, y la distancia administrativa es 120.



El protocolo de routing de gateway interior (IGRP) fue el primer protocolo de routing IPv4 exclusivo desarrollado por Cisco en 1984. Tenía las siguientes características de diseño:

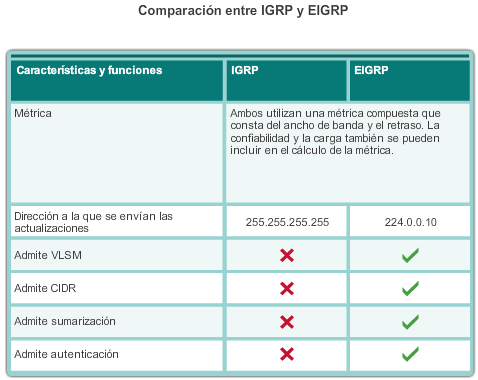
* Se utilizan el ancho de banda, el retraso, la carga y la confiabilidad para crear una métrica compuesta.
* De manera predeterminada, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

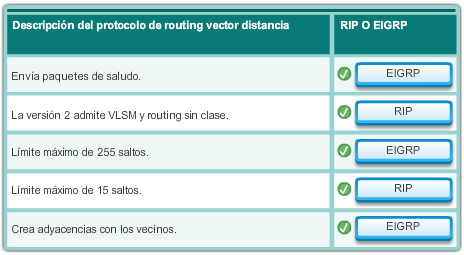
En 1992, el protocolo IGRP se vio reemplazado por IGRP mejorado (EIGRP). Al igual que RIPv2, EIGRP también introdujo compatibilidad con VLSM y CIDR. Con EIGRP se aumenta la eficiencia, se reducen las actualizaciones de routing y se admite el intercambio seguro de mensajes.

En la tabla de la ilustración, se resumen las diferencias entre IGRP y EIGRP.

EIGRP también introdujo lo siguiente:

* **Actualizaciones dirigidas limitadas:** no se envían actualizaciones periódicas. Solo se propagan los cambios de la tabla de routing, siempre que se produce un cambio. Esto reduce la cantidad de carga que el protocolo de routing coloca en la red. Que las actualizaciones sean dirigidas y limitadas significa que EIGRP solo envía actualizaciones a los vecinos que las necesitan. Se utiliza menos ancho de banda, especialmente en redes grandes con muchas rutas.
* **Mecanismo de saludo keepalive:** se intercambia periódicamente un pequeño mensaje de saludo para mantener adyacencias con los routers vecinos. Esto implica un uso muy bajo de los recursos de red durante el funcionamiento normal, en lugar de actualizaciones periódicas.
* **Mantenimiento de una tabla de topología:** se mantienen todas las rutas recibidas de los vecinos (no sólo las mejores rutas) en una tabla de topología. DUAL puede insertar rutas de respaldo en la tabla de topología de EIGRP.
* **Convergencia rápida:** en la mayoría de los casos, se trata del IGP más rápido para realizar la convergencia debido a que mantiene rutas alternativas, lo que permite una convergencia casi instantánea. Si una ruta principal falla, el router puede utilizar la ruta alternativa identificada. El cambio a la ruta alternativa es inmediato y no implica interacción con otros routers.
* **Compatibilidad con varios protocolos de capa de red:** EIGRP utiliza módulos dependientes de protocolo (PDM), lo que significa que es el único protocolo compatible con otros protocolos además de IPv4 e IPv6, como el IPX antiguo y AppleTalk.





## Routing RIP y RIPng

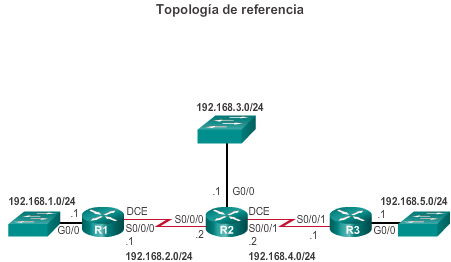
### Configuración del protocolo RIP

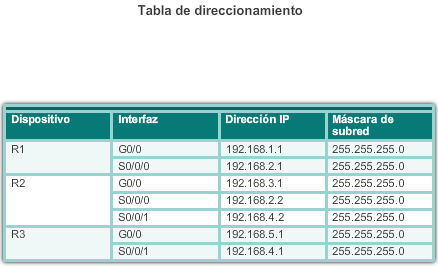
Si bien el protocolo RIP se utiliza con muy poca frecuencia en las redes modernas, es útil como base para comprender el routing de red básico. Por este motivo, en esta sección se proporciona una breve descripción general de la forma en que se configuran los parámetros básicos de RIP y de la manera en que se verifica RIPv2.

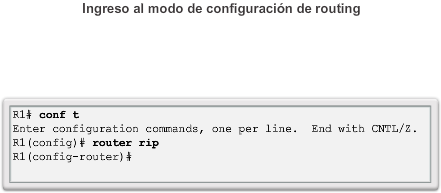
Consulte la topología de referencia en la figura 1 y la tabla de direccionamiento en la figura 2. En esta situación, todos los routers se configuraron con funciones de administración básicas, y todas las interfaces identificadas en la topología de referencia están configuradas y habilitadas. No hay rutas estáticas configuradas ni protocolos de routing habilitados, por lo que el acceso remoto de red es imposible en ese momento. RIPv2 se utiliza como protocolo de routing dinámico. Para habilitar RIP, utilice el comando **router rip**, como se muestra en la figura 3. Este comando no inicia en forma directa el proceso del RIP. En cambio, proporciona acceso al modo de configuración del router, donde se configuran los parámetros de routing RIP.

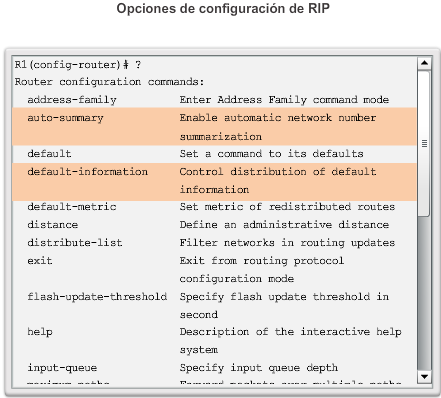
Para deshabilitar y eliminar RIP, utilice el comando de configuración global **no router rip**. Este comando detiene el proceso RIP y elimina todas las configuraciones RIP existentes.

En la figura 4, se muestran los diversos comandos RIP que se pueden configurar. En esta sección, se abordan las palabras clave resaltadas.









Al ingresar en el modo de configuración de router RIP, el router recibe instrucciones para que ejecute el RIP. Pero el router aún necesita conocer las interfaces locales que deberá utilizar para comunicarse con otros routers, así como las redes conectadas en forma local que deberá publicar a dichos routers.

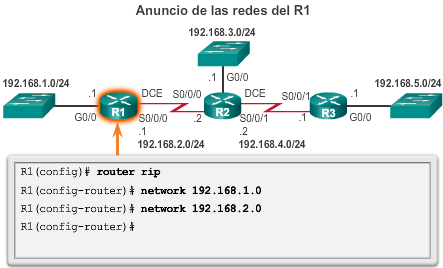
Para habilitar el routing RIP para una red, utilice el comando del modo de configuración del router **network** *dirección-red*. Introduzca la dirección de red con clase para cada red conectada directamente. Este comando realiza lo siguiente:

* Habilita el RIP en todas las interfaces que pertenecen a una red específica. Hace que las interfaces asociadas ahora envíen y reciban actualizaciones RIP.
* Publica la red especificada en las actualizaciones de enrutamiento RIP enviadas a otros routers cada 30 segundos.

**Nota:** si se introduce una dirección de subred, el IOS la convierte automáticamente a la dirección de red con clase. Recuerde que RIPv1 es un protocolo de routing con clase para IPv4. Por ejemplo, si se introduce el comando **network 192.168.1.32**, se convertiría automáticamente a **network 192.168.1.0** en el archivo de configuración en ejecución. El IOS no proporciona un mensaje de error, sino que corrige la entrada e introduce la dirección de red con clase.

En la figura 1, el comando **network** se utiliza para anunciar las redes conectadas directamente al R1.

Utilice el verificador de sintaxis de la figura 2 para establecer una configuración similar en el R2 y en el R3.



El comando **show ip protocols** muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router. Este resultado que se muestra en la figura 1 confirma la mayoría de los parámetros de RIP, incluido lo siguiente:

1. El routing RIP está configurado y en ejecución en el router R1.

2. Los valores de diversos temporizadores; por ejemplo, el R1 envía la siguiente actualización de routing en 16 segundos.

3. La versión de RIP configurada actualmente es RIPv1.

4. El R1 realiza la sumarización en el límite de la red con clase.

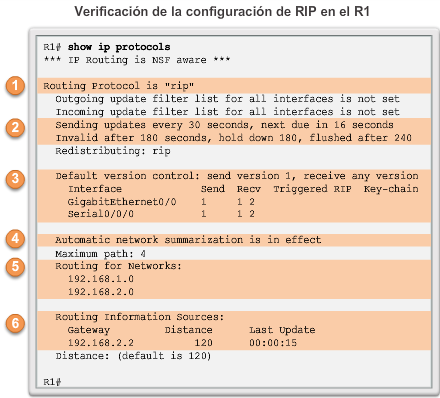
5. El R1 anuncia las redes con clase. Estas son las que R1 incluye en sus actualizaciones RIP.

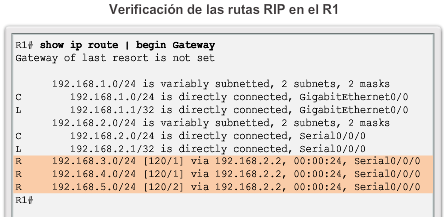
6. Los vecinos RIP se indican mediante la inclusión de la dirección IP del siguiente salto, la AD asociada que el R2 utiliza para las actualizaciones enviadas por ese vecino y el momento en que dicho vecino recibió la última actualización.

**Nota:** este comando también resulta muy útil para verificar las operaciones de otros protocolos de routing (es decir, EIGRP y OSPF).

El comando **show ip route** muestra las rutas RIP instaladas en la tabla de routing. En la figura 2, el R1 ahora tiene información acerca de las redes resaltadas.

Utilice el verificador de sintaxis de la figura 3 para verificar las rutas RIP y la configuración de RIP del R2 y del R3.





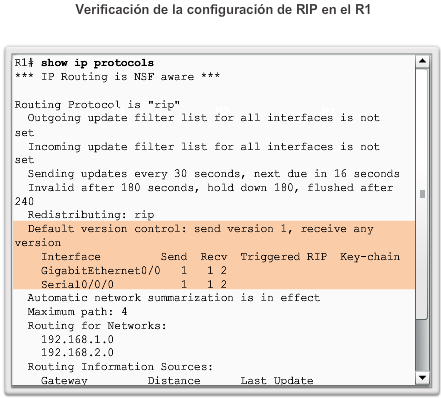
De manera predeterminada, cuando hay un proceso de RIP configurado en un router Cisco, este ejecuta RIPv1, como se muestra en la figura 1. Sin embargo, a pesar de que el router sólo envía mensajes de RIPv1, puede interpretar los mensajes de RIPv1 y RIPv2. Los routers RIPv1 simplemente ignoran los campos de RIPv2 en la entrada de ruta.

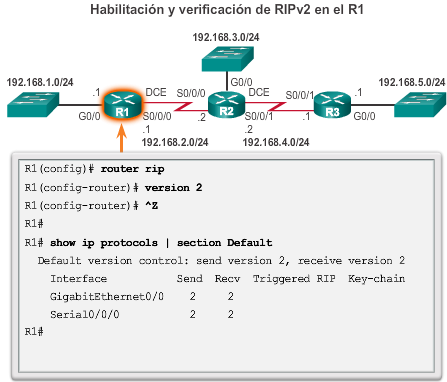
Utilice el comando del modo de configuración del router **version 2** para habilitar RIPv2, como se muestra en la figura 2. Observe la forma en que el comando **show ip protocols** verifica que el R2 ahora está configurado para enviar y recibir solamente mensajes de versión 2. El proceso de RIP ahora incluye la máscara de subred en todas las actualizaciones, lo que hace que RIPv2 sea un protocolo de routing sin clase.

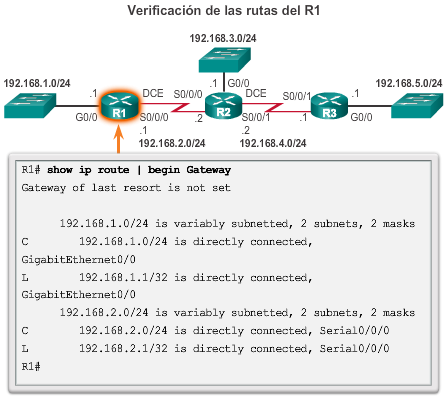
**Nota:** la configuración de **version 1**habilita RIPv1 solamente, mientras que configurar **no version** revierte el router a la configuración predeterminada, mediante la cual se envían actualizaciones de versión 1 pero se está a la escucha de actualizaciones de versión 1 y de versión 2.

En la figura 3, se verifica que ya no haya rutas RIP en la tabla de routing. Esto se debe a que el R1 ahora está a la escucha de actualizaciones RIPv2 únicamente. El R2 y el R3 todavía envían actualizaciones RIPv1. Por lo tanto, se debe configurar el comando **version 2** en todos los routers en el dominio de routing.

Utilice el verificador de sintaxis de la figura 4 para habilitar RIPv2 en el R2 y en el R3.





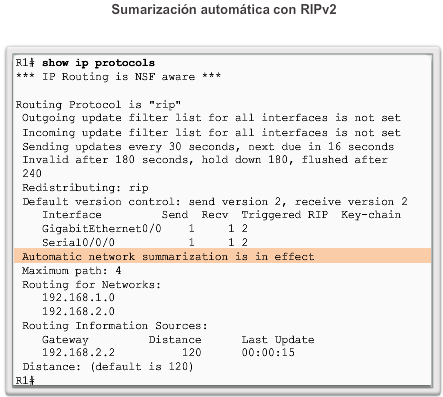


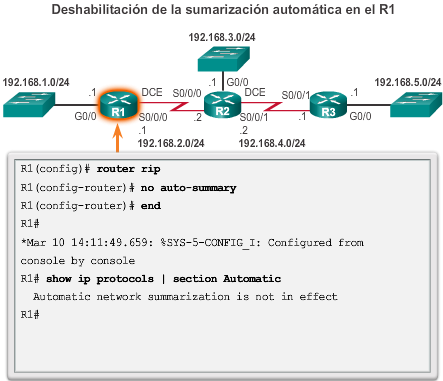
Como se muestra en la figura 1, RIPv2 resume automáticamente las redes en los límites de red principales de manera predeterminada, al igual que RIPv1.

Para modificar el comportamiento predeterminado de RIPv2 de sumarización automática, utilice el comando del modo de configuración del router **no auto-summary**, como se muestra en la figura 2. Este comando no tiene ningún efecto cuando se utiliza RIPv1. Cuando se deshabilita la sumarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos. RIPv2 ahora incluye todas las subredes y sus máscaras correspondientes en sus actualizaciones de routing. El **comando show ip protocols** ahora indica lo siguiente: automatic network summarization is not in effect (la sumarización de red automática no está operativa).

**Nota:** se debe habilitar RIPv2 antes de deshabilitar la sumarización automática.

Utilice el verificador de sintaxis de la figura 3 para deshabilitar la sumarización automática en el R2 y en el R3.





De manera predeterminada, las actualizaciones RIP se reenvían por todas las interfaces con RIP habilitado. Sin embargo, en realidad las actualizaciones RIP solo deben reenviarse por las interfaces que se conectan a otros routers con RIP habilitado.

Por ejemplo, consulte la topología en la figura 1. RIP envía actualizaciones por su interfaz G0/0, aunque no existe ningún dispositivo RIP en esa LAN. No hay manera de que el R1 tenga información acerca de esto y, como resultado, envía una actualización cada 30 segundos. El envío de actualizaciones innecesarias a una LAN impacta en la red de tres maneras:

* **Desperdicio de ancho de banda**: se utiliza ancho de banda para transportar actualizaciones innecesarias. Dado que las actualizaciones RIP se transmiten por difusión o multidifusión, los switches también reenvían las actualizaciones por todos los puertos.
* **Desperdicio de recursos:** todos los dispositivos en la LAN deben procesar la actualización hasta las capas de transporte, punto en el cual los dispositivos descartan la actualización.
* **Riesgo de seguridad:** el anuncio de actualizaciones en una red de difusión constituye un riesgo de seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.

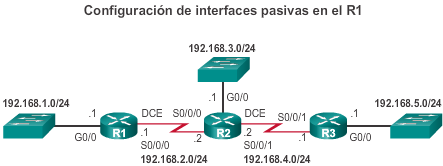
Utilice el comando de configuración del router **passive-interface** para evitar que las actualizaciones de routing se transmitan a través de una interfaz del router y permitir que esa red se siga anunciando a otros routers. El comando detiene las actualizaciones de routing a través de la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas a otras interfaces.

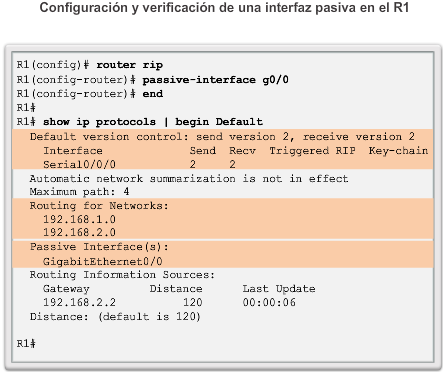
No es necesario que el R1, el R2, y el R3 reenvíen actualizaciones RIP por sus interfaces LAN. En la configuración de la figura 2, se identifica la interfaz G0/0 del R1 como pasiva. El comando **show ip protocols** se utiliza para verificar que la interfaz Gigabit Ethernet es pasiva. Observe que ya no se indica que la interfaz G0/0 envía o recibe actualizaciones de versión 2, sino que se encuentra en la sección Passive Interface(s) (Interfaces pasivas). Asimismo, observe que la red 192.168.1.0 aún se encuentra bajo Routing for Networks (Routing para redes), lo cual significa que esta red aún está incluida como una entrada de ruta en las actualizaciones RIP que se envían al R2.

**Nota:** todos los protocolos de routing admiten el comando **passive-interface**.

Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R2 y en el R3.

Como alternativa, todas las interfaces se pueden convertir en pasivas con el comando **passive-interface default**. Las interfaces que no deben ser pasivas se pueden volver a habilitar con el comando **no passive-interface**.





Consulte la Figura 1. En esta situación, el R1 tiene conexión simple a un proveedor de servicios. Por lo tanto, para que el R1 llegue a Internet, solo se requiere una ruta estática predeterminada desde la interfaz Serial 0/0/1.

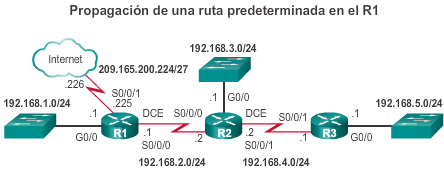
Se podrían configurar rutas estáticas predeterminadas similares en el R2 y en el R3, pero es mucho más escalable introducirla una vez en el router perimetral R1 y, a continuación, hacer que el R1 la propague al resto de los routers mediante RIP. Para proporcionarle conectividad a Internet a todas las demás redes del dominio de enrutamiento RIP, la ruta estática predeterminada debe publicarse a todos los demás routers que usan el protocolo de enrutamiento dinámico.

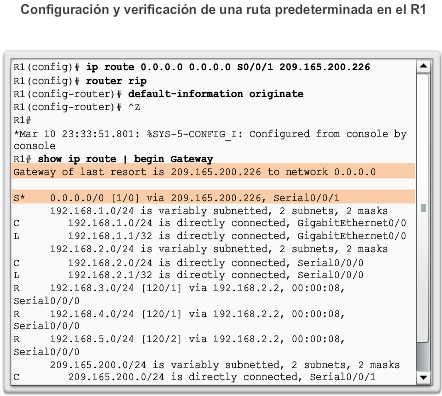
Para propagar una ruta predeterminada, el router perimetral debe estar configurado con lo siguiente:

* Una ruta estática predeterminada mediante el comando **ip route 0.0.0.0 0.0.0.0***interfaz-salida ip-siguiente-salto*.
* El comando de configuración del router**default-information originate**. Esto le ordena al router R1 que produzca información predeterminada mediante la propagación de la ruta estática predeterminada en actualizaciones RIP.

En el ejemplo de la figura 2, se configura una ruta estática predeterminada completamente especificada al proveedor de servicios y, a continuación, se propaga la ruta mediante RIP. Observe que ahora el R1 tiene un gateway de último recurso y una ruta predeterminada instalados en su tabla de routing.

Utilice el verificador de sintaxis de la figura 3 para verificar que la ruta predeterminada se haya propagado al R2 y al R3.





### Configuración del protocolo RIPng

Al igual que su equivalente para IPv4, RIPng no se suele utilizar en las redes modernas, pero también resulta útil como base para comprender el routing de red básico. Por este motivo, en esta sección se proporciona una breve descripción general de cómo configurar RIPng básico.

Consulte la topología de referencia en la ilustración. En esta situación, todos los routers se configuraron con funciones de administración básicas, y todas las interfaces identificadas en la topología de referencia están configuradas y habilitadas. No hay rutas estáticas configuradas ni protocolos de routing habilitados, por lo que el acceso remoto de red es imposible en ese momento.

Para habilitar un router IPv6 para que reenvíe paquetes IPv6, se debe configurar el comando **ipv6 unicast-routing**.

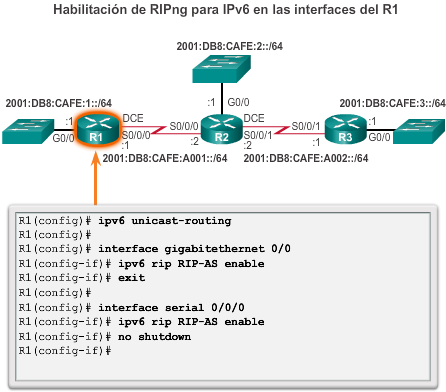
A diferencia de RIPv2, RIPng se habilita en una interfaz y no en el modo de configuración del router. De hecho, no hay un comando **network***dirección-red*disponible en RIPng. En cambio, utilice el comando de configuración de interfaz **ipv6 rip***nombre-dominio***enable**.

En la figura 1, se habilita el routing de unidifusión IPv6 y se habilitan las interfaces Gigabit Ethernet 0/0 y Serial 0/0/0 para RIPng mediante el nombre de dominio RIP-AS.

Utilice el verificador de sintaxis de la figura 2 para establecer una configuración similar en el R2 y en el R3.

El proceso para propagar una ruta predeterminada en RIPng es idéntico al de RIPv2, excepto que se debe especificar una ruta estática predeterminada IPv6. Por ejemplo, suponga que el R1 tenía una conexión a Internet de una interfaz Serial 0/0/1 a la dirección IP 2001:DB8:FEED:1::1/64. Para propagar una ruta predeterminada, el R3 debería configurarse con lo siguiente:

* Una ruta estática predeterminada mediante el comando de configuración global **ipv6 route 0::/0 2001:DB8:FEED:1::1**.
* El comando del modo de configuración de interfaz **ipv6 rip***nombre-dominio***default-information originate**. Esto ordena al R3 que sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones RIPng enviadas por la interfaz configurada.



En la figura 1, el comando **show ipv6 protocols** no proporciona la misma cantidad de información que su equivalente para IPv4. Sin embargo, confirma los siguientes parámetros:

1. El routing RIPng está configurado y en ejecución en el router R1.

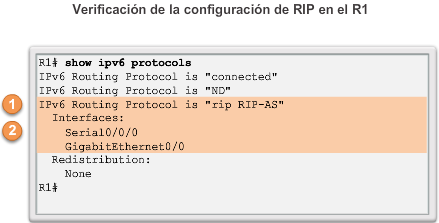
2. Las interfaces están configuradas con RIPng.

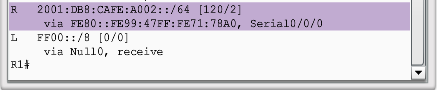
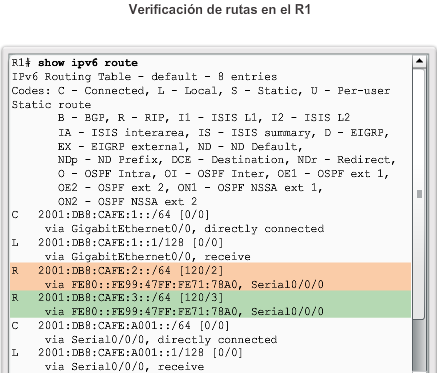
El comando **show ipv6 route** muestra las rutas instaladas en la tabla de routing, como se muestra en la figura 2. El resultado confirma que el R1 ahora tiene información acerca las redes RIPng resaltadas.

Observe que la LAN del R2 se anuncia como a dos saltos de distancia. Esto se debe a que hay una diferencia en la forma en que RIPv2 y RIPng calculan los conteos de saltos. Con RIPv2 (y RIPv1), la métrica hasta la LAN del R2 sería un salto. Esto se debe a que la métrica (el conteo de saltos) que se muestra en la tabla de routing IPv4 es la cantidad de saltos requeridos para llegar a la red remota (contando el router del siguiente salto como primer salto). En RIPng, el router emisor se considera a sí mismo a un salto de distancia, por lo tanto, el R2 anuncia su LAN con un valor de métrica 1. Cuando el R1 recibe la actualización, agrega otro conteo de saltos de 1 a la métrica. Por lo tanto, el R1 considera que la LAN del R2 está a dos saltos de distancia. De manera similar, considera que la LAN del R3 está a tres saltos de distancia.

Si se agrega la palabra clave **rip** al comando, como se muestra en la figura 3, solo se indican las redes RIPng.

Utilice el verificador de sintaxis de la figura 4 para verificar el R2 y el R3.







## Routing dinámico de estado de enlace

### Funcionamiento del protocolo de routing de estado de enlace

A los protocolos de enrutamiento de link-state también se les conoce como protocolos shortest path first y se desarrollan en torno al algoritmo shortest path first (SPF) de Edsger Dijkstra. El algoritmo SPF se analiza más detalladamente en una sección posterior.

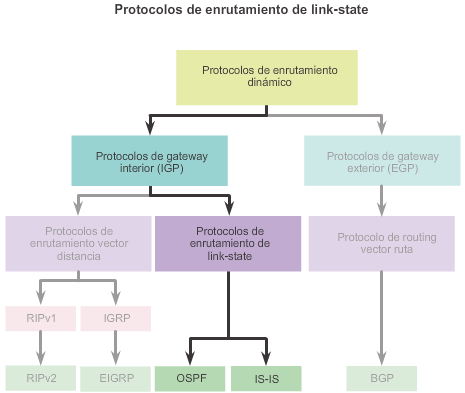
En la ilustración, se muestran los protocolos de routing de estado de enlace IPv4:

* Open Shortest Path First (OSPF)
* Intermediate-System-to-Intermediate-System (IS-IS)

Los protocolos de enrutamiento de link-state son conocidos por presentar una complejidad bastante mayor que sus vectores distancia equivalentes. Sin embargo, la funcionalidad básica y la configuración de los protocolos de routing de estado de enlace son igualmente sencillas.

Al igual que RIP y EIGRP, las operaciones básicas de OSPF se pueden configurar mediante los siguientes comandos:

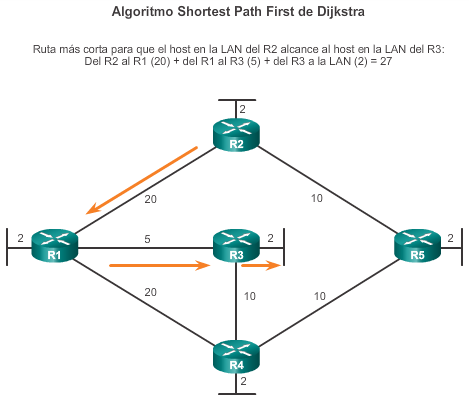
* **router ospf***id-proceso* (comando de configuración global)
* **network**para anunciar redes



Todos los protocolos de routing de estado de enlace aplican el algoritmo de Dijkstra para calcular la mejor ruta. A este algoritmo se le llama comúnmente “algoritmo SPF” (Shortest Path First). Para determinar el costo total de una ruta, este algoritmo utiliza costos acumulados a lo largo de cada ruta, de origen a destino.

En la figura, cada ruta se rotula con un valor arbitrario para el costo. El costo de la ruta más corta para que el R2 envíe paquetes a la LAN conectada al R3 es 27. Cada router determina su propio costo hacia cada destino en la topología. En otros términos, cada router calcula el algoritmo SPF y determina el costo desde su propia perspectiva.

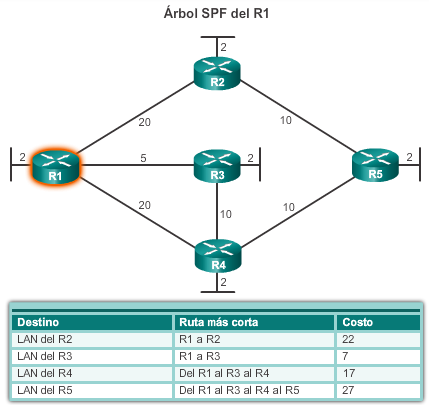
**Nota:** el objetivo central de esta sección es analizar el costo, el cual está determinado por el árbol SPF. Por este motivo, en los gráficos de esta sección se muestran las conexiones del árbol SPF y no la topología. Todos los enlaces se representan mediante una línea negra continua.

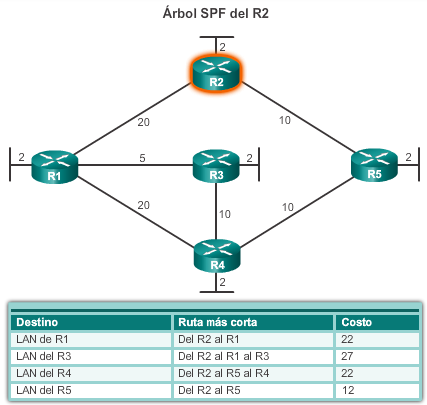


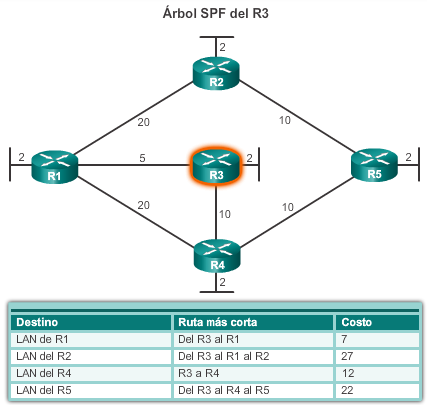
En la tabla de la figura 1, se muestra la ruta más corta y el costo acumulado para llegar a las redes de destino identificadas desde la perspectiva del R1.

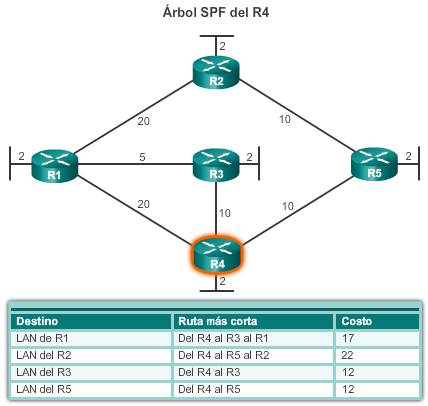
La ruta más corta no es necesariamente la ruta con la menor cantidad de saltos. Por ejemplo, observe la ruta hacia la LAN R5. Podría suponerse que el R1 realizaría el envío directamente al R4 en lugar de al R3. Sin embargo, el costo para llegar a R4 directamente (22) es más alto que el costo para llegar a R4 a través de R3 (17).

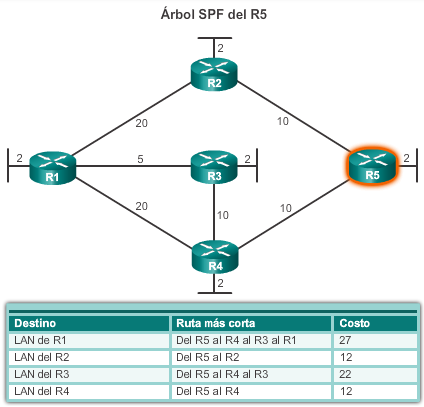
Observe la ruta más corta para que cada router llegue a cada una de las LAN, como se muestra en las figuras 2 a 5.











### Actualizaciones de estado de enlace

Por lo tanto, ¿de qué manera exactamente funciona un protocolo de enrutamiento de link-state? Con los protocolos de enrutamiento de link-state, un enlace es una interfaz en un router. La información acerca del estado de dichos enlaces se conoce como estados de enlace.

Analice la topología en la ilustración. Todos los routers de la topología realizarán el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia:

1. Cada router obtiene información acerca de sus propios enlaces y sus propias redes conectadas directamente. Esto se realiza al detectar que una interfaz se encuentra activada.

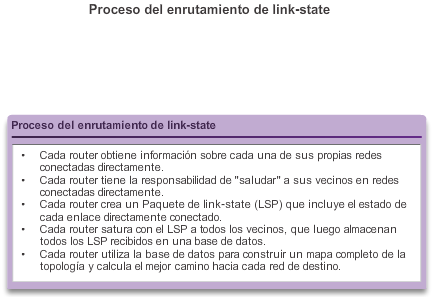
2. Cada router es responsable de reunirse con sus vecinos en redes conectadas directamente. Los routers de estado de enlace lo hacen mediante el intercambio paquetes de saludo con otros routers de estado de enlace en redes conectadas directamente.

3. Cada router crea un Paquete de link-state (LSP) que incluye el estado de cada enlace directamente conectado. Esto se realiza registrando toda la información pertinente acerca de cada vecino, que incluye el ID de vecino, el tipo de enlace y el ancho de banda.

4. Cada router satura a todos los vecinos con el LSP. Estos vecinos almacenan todos los LSP recibidos en una base de datos. A continuación, saturan a sus vecinos con los LSP hasta que todos los routers del área hayan recibido los LSP. Cada router almacena una copia de cada LSP recibido por parte de sus vecinos en una base de datos local.

5. Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino. En forma similar a tener un mapa de carretera, el router tiene ahora un mapa completo de todos los destinos de la topología y las rutas para alcanzarlos. El algoritmo SPF se utiliza para construir el mapa de la topología y determinar el mejor camino hacia cada red.

**Nota:** este proceso es el mismo para OSPF para IPv4 e IPv6. En los ejemplos de esta sección, se hará referencia a OSPF para IPv4.



El primer paso en el proceso de routing de estado de enlace es que cada router descubra sus propios enlaces y sus propias redes conectadas directamente. Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz se vuelve parte de esa red.

Consulte la topología en la figura 1. A los fines de este análisis, suponga que el R1 se configuró previamente y que tenía plena conectividad a todos los vecinos. Sin embargo, se cortó la alimentación del R1 brevemente y tuvo que reiniciarse.

Durante el arranque, el R1 carga el archivo de configuración de inicio guardado. A medida que se activan las interfaces configuradas anteriormente, el R1 obtiene información sobre sus propias redes conectadas directamente. Más allá de los protocolos de routing utilizados, dichas redes conectadas directamente ahora constituyen entradas en la tabla de routing.

Como ocurre con los protocolos vector distancia y las rutas estáticas, la interfaz debe configurarse de manera adecuada con una dirección IPv4 y una máscara de subred, y el enlace debe encontrarse en estado activo antes de que el protocolo de routing de estado de enlace pueda obtener información sobre un enlace. Asimismo, como ocurre con los protocolos vector distancia, la interfaz debe incluirse en una de las instrucciones **network** de configuración del router para que pueda participar en el proceso de routing de estado de enlace.

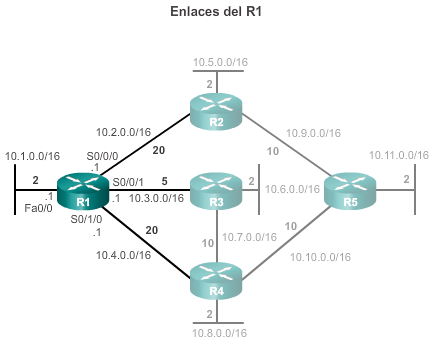
En la figura 1, se muestra el R1 enlazado a cuatro redes conectadas directamente:

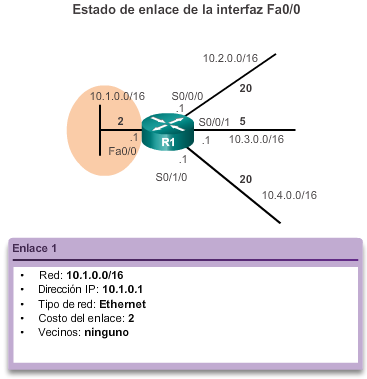
* FastEthernet 0/0, 10.1.0.0/16
* Serial 0/0/0, 10.2.0.0/16
* Serial 0/0/1, 10.3.0.0/16
* Serial 0/1/0, 10.4.0.0/16

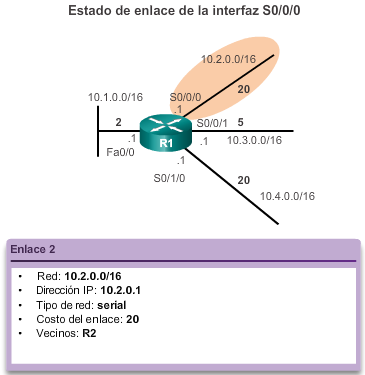
Como se muestra en las figuras 2 a 5, la información de estado de enlace incluye lo siguiente:

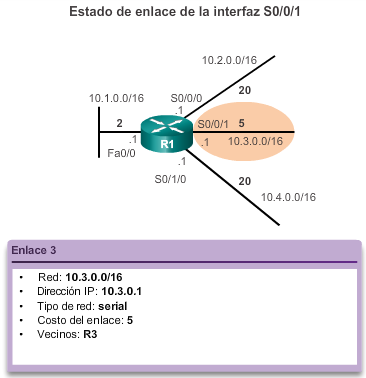
* La dirección IPv4 y la máscara de subred de la interfaz
* El tipo de red, como Ethernet (difusión) o enlace serial punto a punto
* El costo de dicho enlace
* Cualquier router vecino en dicho enlace

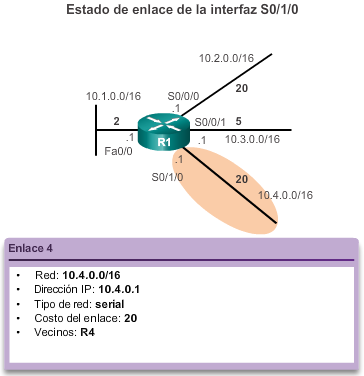
**Nota:** la implementación de OSPF de Cisco especifica la métrica de routing OSPF como el costo del enlace sobre la base del ancho de banda de la interfaz de salida. A los fines de este capítulo, utilizamos valores de costo arbitrarios para simplificar la demostración.











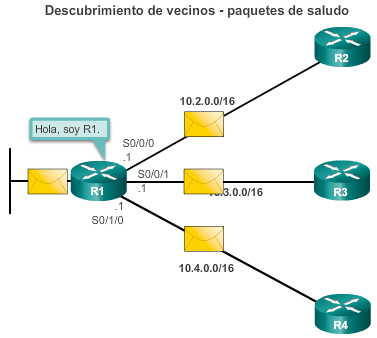
El segundo paso en el proceso de routing de estado de enlace es que cada router asume la responsabilidad de encontrarse con sus vecinos en redes conectadas directamente.

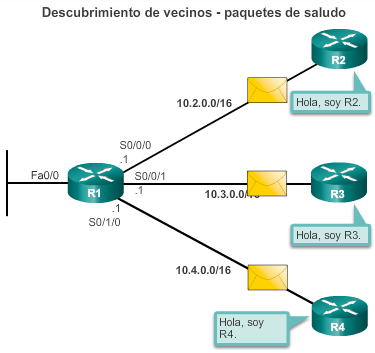
Los routers con protocolos de enrutamiento de link-state utilizan un protocolo de saludo para descubrir cualquier vecino en sus enlaces. Un vecino es cualquier otro router habilitado con el mismo protocolo de enrutamiento de link-state.

Haga clic en Reproducir en la ilustración para ver una animación sobre el proceso de descubrimiento de vecinos de estado de enlace con paquetes de saludo.

En la animación, el R1 envía paquetes de saludo por sus enlaces (interfaces) para detectar la presencia de vecinos. R2, R3 y R4 responden al paquete de saludo con sus propios paquetes de saludo debido a que dichos routers están configurados con el mismo protocolo de enrutamiento de link-state. No hay vecinos fuera de la interfaz FastEthernet 0/0. Debido a que el R1 no recibe un saludo en esta interfaz, no continúa con los pasos del proceso de routing de estado de enlace para el enlace FastEthernet 0/0.

Cuando dos routers de estado de enlace descubren que son vecinos, forman una adyacencia. Dichos pequeños paquetes de saludo continúan intercambiándose entre dos vecinos adyacentes y cumplen la función de keepalive para monitorear el estado del vecino. Si un router deja de recibir paquetes de saludo por parte de un vecino, dicho vecino se considera inalcanzable y se rompe la adyacencia.





El tercer paso en el proceso de routing de estado de enlace es que cada router cree un paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.

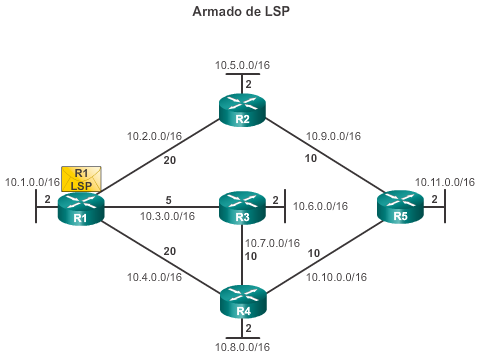
Una vez que un router establece sus adyacencias, puede armar LSP que contienen la información de estado de enlace de sus enlaces. Una versión simplificada de LSP del R1, que se muestra en la ilustración, contendría lo siguiente:

1. R1; Red Ethernet 10.1.0.0/16; Costo 2

2. 2. R1 -> R2; Red serial punto a punto; 10.2.0.0/16; Costo 20

3. 2. R1 -> R3; Red serial punto a punto; 10.3.0.0/16; Costo 5

4. R1 -> R4; Red serial punto a punto; 10.4.0.0/16; Costo 20



El cuarto paso en el proceso de routing de estado de enlace es que cada router satura con LSP a todos los vecinos, quienes luego almacenan todos los LSP recibidos en una base de datos.

Cada router inunda con su información de link-state a todos los demás routers de link-state en el área de enrutamiento. Siempre que un router recibe un LSP de un router vecino, envía de inmediato dicho LSP a todas las demás interfaces, excepto la interfaz que recibió el LSP. Este proceso crea un efecto de saturación de los LSP desde todos los routers a través del área de enrutamiento.

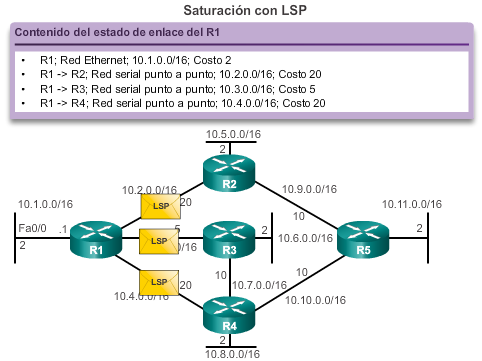
Haga clic en Reproducir en la ilustración para ver una animación de la saturación con LSP.

En la animación, observe cómo se lleva a cabo la saturación con LSP de forma casi inmediata después de ser recibidos sin ningún cálculo intermedio. Los protocolos de routing de estado de enlace calculan el algoritmo SPF una vez que finaliza la saturación. Como resultado, los protocolos de routing de estado de enlace logran la convergencia muy rápidamente.

Recuerde que los LSP no necesitan enviarse periódicamente. Un LSP sólo necesita enviarse:

* Durante el arranque inicial del proceso del protocolo de routing (por ejemplo, en el reinicio del router)
* Cuando hay un cambio en la topología (por ejemplo, un enlace que se desactiva o activa, o una adyacencia de vecinos que se establece o se rompe)

Además de la información de estado de enlace, se incluye información adicional en el LSP, como los números de secuencia y la información de vencimiento, para ayudar a administrar el proceso de saturación. Cada router utiliza esta información para determinar si ya recibió el LSP de otro router o si el LSP tiene información más nueva que la contenida en la base de datos de link-state. Este proceso permite que un router conserve sólo la información más actual en su base de datos de link-state.



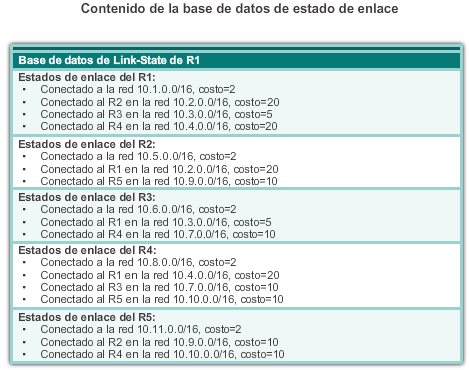
El paso final en el proceso de routing de estado de enlace es que cada router utiliza la base de datos para construir un mapa completo de la topología y calcula la mejor ruta para cada destino.

Finalmente, todos los routers reciben un LSP de todos los demás routers de estado de enlace en el área de routing. Dichos LSP se almacenan en la base de datos de link-state.

En el ejemplo, se muestra el contenido de la base de datos de estado de enlace del R1.

Como resultado del proceso de saturación, el R1 obtuvo la información de estado de enlace para cada router de su área de routing. Observe que R1 también incluye su propia información de link-state en la base de datos de link-state.

Con una base de datos de estado de enlace completa, el R1 ahora puede utilizar la base de datos y el algoritmo SPF (Shortest Path First) para calcular la ruta preferida o la ruta más corta a cada red, lo que da como resultado el árbol SPF.



Cada router en el área de routing utiliza la base de datos de estado de enlace y el algoritmo SPF para armar el árbol SPF.

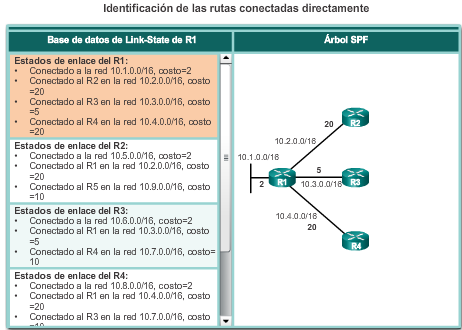
Por ejemplo, utilizando la información de estado de enlace de todos los demás routers, el R1 ahora puede comenzar a armar un árbol SPF de la red. Para comenzar, el algoritmo SPF interpreta el LSP de cada router para identificar las redes y los costos asociados.

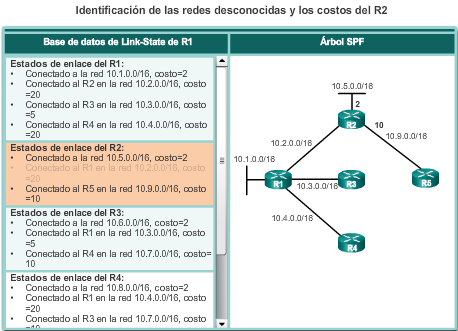
En la figura 1, el R1 identifica sus redes conectadas directamente y los costos.

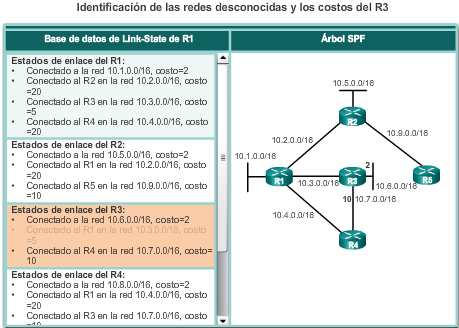
En las figuras 2 a 5, el R1 continúa agregando toda red desconocida y sus costos asociados al árbol SPF. Observe que el R1 ignora cualquier red que ya haya identificado.

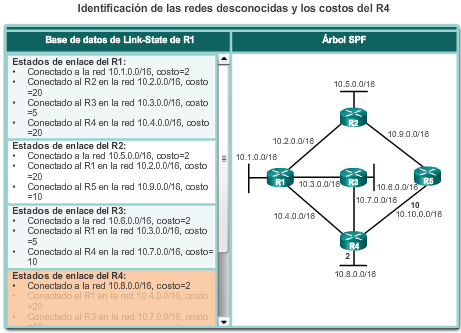
A continuación, el algoritmo SPF calcula las rutas más cortas para llegar a cada red individual, lo que da como resultado el árbol SPF como se muestra en la figura 6. El R1 ahora tiene una vista de topología completa del área de estado de enlace.

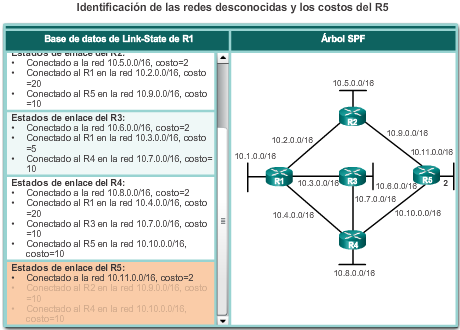
Cada router construye su propio árbol SPF independientemente de los otros routers. Para garantizar el enrutamiento adecuado, las bases de datos de link-state utilizadas para construir dichos árboles deben ser idénticas en todos los routers.

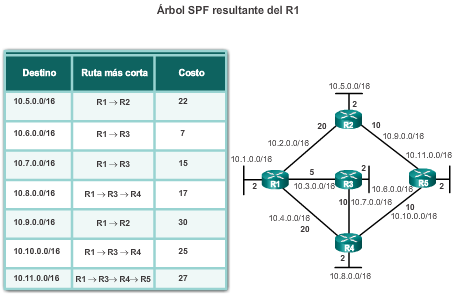






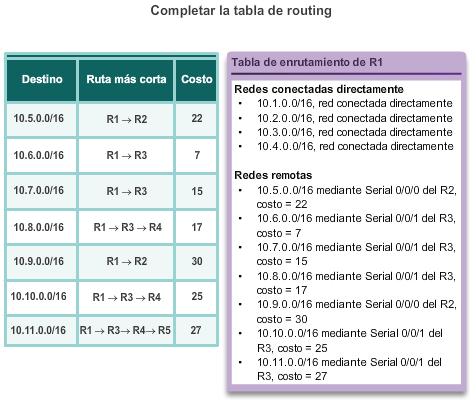






Al utilizar la información de la ruta más corta determinada por el algoritmo SPF, dichas rutas ahora pueden agregarse a la tabla de enrutamiento. En la ilustración, se muestran las rutas que se agregaron a la tabla de routing IPv4 del R1.

La tabla de routing también incluye todas las redes conectadas directamente y las rutas provenientes de cualquier otro origen, tales como las rutas estáticas. Los paquetes ahora se reenvían según dichas entradas en la tabla de routing.



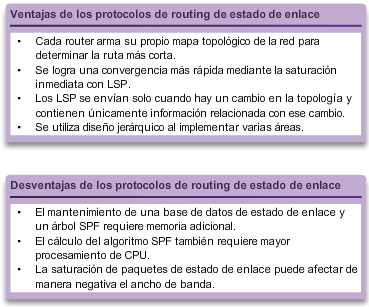
### Razones para utilizar protocolos de routing de estado de enlace

Como se muestra en la ilustración, los protocolos de routing de estado de enlace presentan varias ventajas en comparación con los protocolos de routing vector distancia.

* **Armado de un mapa topológico:** los protocolos de routing de estado de enlace crean un mapa topológico o árbol SPF de la topología de la red. Debido a que los protocolos de enrutamiento de link-state intercambian estados de enlace, el algoritmo SPF puede crear un árbol SPF de la red. Al utilizar el árbol SPF, cada router puede determinar en forma independiente la ruta más corta a cada red.
* **Convergencia rápida:** cuando reciben un LSP, los protocolos de routing de estado de enlace saturan de inmediato todas las interfaces con el LSP, excepto la interfaz desde la que se lo recibió. En cambio, el protocolo RIP necesita procesar cada actualización de routing y actualizar su tabla de routing antes de saturar otras interfaces.
* **Actualizaciones desencadenadas por eventos:** después de la saturación inicial con LSP, los protocolos de routing de estado de enlace solo envían un LSP cuando se produce un cambio en la topología. El LSP sólo incluye la información relacionada con el enlace afectado. A diferencia de algunos protocolos de enrutamiento vector distancia, los protocolos de enrutamiento de link-state no envían actualizaciones periódicas.
* **Diseño jerárquico:** los protocolos de routing de estado de enlace utilizan el concepto de áreas. Las áreas múltiples crean un diseño jerárquico para redes y permiten un mejor agregado de rutas (sumarización) y el aislamiento de los problemas de enrutamiento dentro del área.

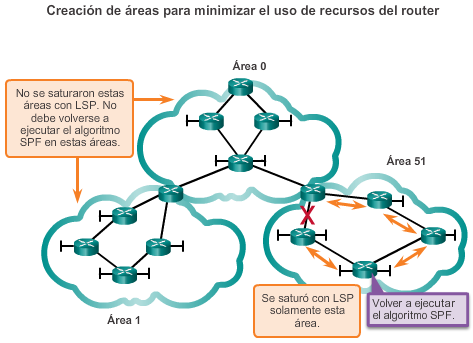
Los protocolos de estado de enlace también tienen algunas desventajas en comparación con los protocolos de routing vector distancia:

* **Requisitos de memoria:** los protocolos de estado de enlace requieren memoria adicional para crear y mantener la base de datos de estado de enlace y el árbol SPF.
* **Requisitos de procesamiento:** los protocolos de estado de enlace también pueden requerir un mayor procesamiento de CPU que los protocolos de routing vector distancia. El algoritmo SPF requiere un mayor tiempo de CPU que los algoritmos vector distancia, como Bellman-Ford, ya que los protocolos de estado de enlace arman un mapa completo de la topología.
* **Requisitos de ancho de banda:** la saturación de paquetes de estado de enlace puede ejercer un impacto negativo en el ancho de banda disponible en una red. Si bien esto sólo debería ocurrir durante la puesta en marcha inicial de los routers, también podría ser un problema en redes inestables.



Los protocolos de enrutamiento de link-state modernos están diseñados para minimizar los efectos en la memoria, el CPU y el ancho de banda. La utilización y configuración de áreas múltiples puede reducir el tamaño de las bases de datos de link-state. Las áreas múltiples también pueden limitar el grado de saturación de información de link-state en un dominio de enrutamiento y enviar los LSP sólo a aquellos routers que los necesitan. Cuando hay un cambio en la topología, solo los routers del área afectada reciben el LSP y ejecutan el algoritmo SPF. Esto puede ayudar a aislar un enlace inestable en un área específica en el dominio de enrutamiento.

Por ejemplo, en la ilustración hay tres dominios de routing independientes: área 1, área 0 y área 51. Si una red en el área 51 deja de funcionar, solo los routers en esa área se saturan con el LSP que contiene la información sobre dicho enlace fuera de servicio. Únicamente los routers del área 51 necesitan actualizar sus bases de datos de estado de enlace, volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar sus tablas de routing. Los routers de otras áreas descubren que esta ruta no funciona, pero esto se realiza con un tipo de LSP que no los obliga a volver a ejecutar su algoritmo SPF. Los routers de otras áreas pueden actualizar sus tablas de enrutamiento directamente.



Existen solamente dos protocolos de routing de estado de enlace: OSPF e IS-IS.

El protocolo OSPF (Open Shortest Path First) es la implementación más popular. Fue diseñado por el grupo de trabajo de OSPF del Grupo de trabajo de ingeniería de Internet (IETF). El desarrollo de OSPF comenzó en 1987 y actualmente hay dos versiones en uso:

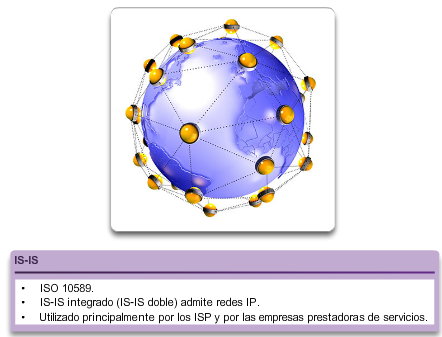
* OSPFv2: OSPF para redes IPv4 (RFC 1247 y RFC 2328)
* OSPFv3: OSPF para redes IPv6 (RFC 2740)

**Nota:** con la característica de familias de direcciones de OSPFv3, esta versión del protocolo es compatible con IPv4 e IPv6.

El protocolo IS-IS fue diseñado por la Organización Internacional para la Estandarización (ISO) y se describe en ISO 10589. La primera versión de este protocolo de routing se desarrolló en la Digital Equipment Corporation (DEC) y se conoce como “DECnet fase V”. Radia Perlman fue la principal diseñadora del protocolo de routing IS-IS.

IS-IS se diseñó originalmente para el suite de protocolos de OSI y no para el suites de protocolo de TCP/IP. Más adelante, IS-IS integrado, o IS-IS doble, incluyó la compatibilidad con redes IP. Si bien se conoció a IS-IS como el protocolo de enrutamiento más utilizado por proveedores e ISP, se están comenzando a utilizar más redes IS-IS corporativas.

OSPF e IS-IS presentan varias similitudes y diferencias. Existen diversas posturas a favor de OSPF y a favor de IS-IS que analizan y debaten las ventajas de un protocolo de enrutamiento frente al otro. Ambos protocolos de routing proporcionan la funcionalidad de routing necesaria.



## La tabla de routing

### Partes de una entrada de ruta IPv4

La topología que se muestra en la figura 1 se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

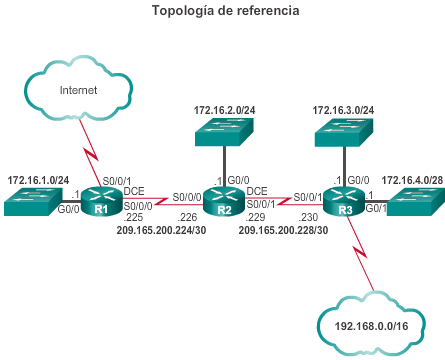
El R1 es el router perimetral que se conecta a Internet. Por lo tanto, propaga una ruta estática predeterminada al R2 y al R3.

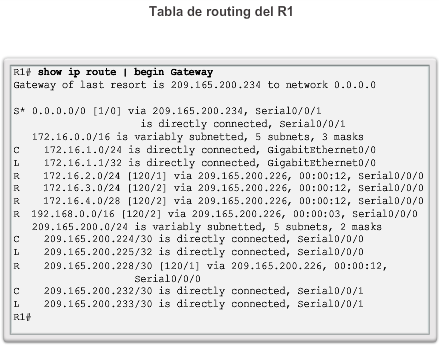
El R1, el R2 y el R3 contienen redes no contiguas separadas por otra red con clase.

El R3 también introduce una ruta de superred 192.168.0.0/16.

En la figura 2, se muestra la tabla de routing IPv4 del R1 con las rutas dinámicas, estáticas y conectadas directamente.

**Nota:** en los inicios, la jerarquía de la tabla de routing en el IOS de Cisco se implementó con el esquema de routing con clase. Si bien la tabla de enrutamiento incorpora el direccionamiento con clase y sin clase, la estructura general aún se construye en base a este esquema con clase.





Como se destaca en la figura 1, la tabla de routing del R1 contiene tres redes conectadas directamente. Observe que cuando se configura una interfaz del router activa con una dirección IP y una máscara de subred, automáticamente se crean dos entradas en la tabla de routing.

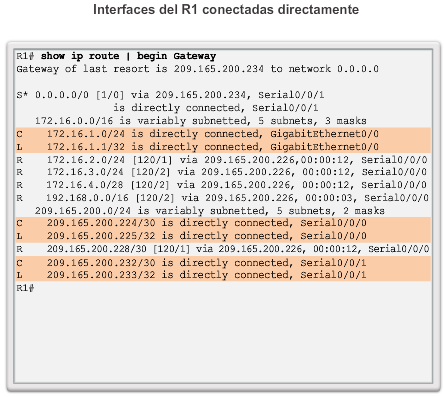
En la figura 2, se muestra una de las entradas de la tabla de routing en el R1 para la red conectada directamente 172.16.1.0. Estas entradas se agregaron de forma automática a la tabla de enrutamiento cuando se configuró y se activó la interfaz GigabitEthernet 0/0. Las entradas contienen la siguiente información:

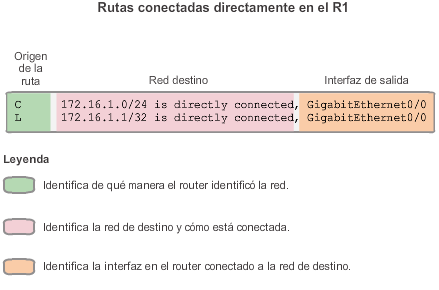
* **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. **C**identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.**L** identifica que la ruta es local. Las rutas locales se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.
* **Red de destino:** la dirección de la red remota y la forma en que se conecta esa red.
* **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

**Nota:** antes del IOS versión 15, las entradas de la tabla de routing local no aparecían en las tablas de routing.

En general, los routers tienen varias interfaces configuradas. En la tabla de routing se almacena información acerca de las rutas conectadas directamente y de las rutas remotas. Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta. Por ejemplo, los códigos frecuentes para las redes remotas incluyen los siguientes:

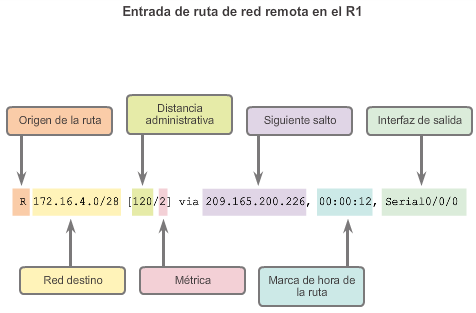
* **S:** indica que un administrador creó la ruta manualmente para llegar a una red específica. Esto se conoce como “ruta estática”.
* **D:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing EIGRP.
* **O:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing OSPF.
* **R:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing RIP.

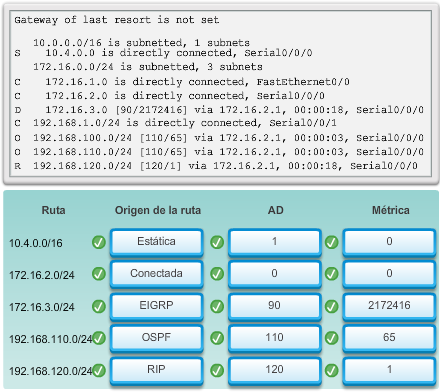




En la ilustración, se muestra una entrada de la tabla de routing IPv4 en el R1 para la ruta hacia la red remota 172.16.4.0 en el R3. La entrada indica la siguiente información:

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





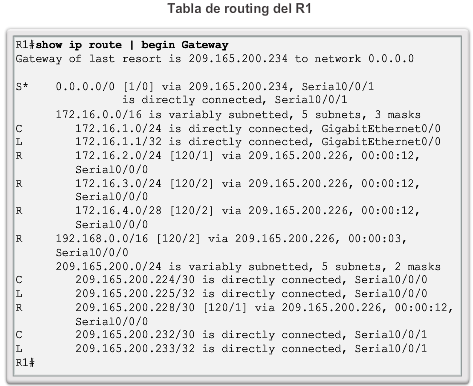
### Rutas IPv4 descubiertas en forma dinámica

Una tabla de routing armada dinámicamente proporciona mucha información, como se muestra en la ilustración. Por lo tanto, es de vital importancia comprender el resultado generado por la tabla de routing. Al analizar el contenido de una tabla de routing, se utilizan términos especiales.

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. Dentro de esta estructura, la jerarquía incluye varios niveles.

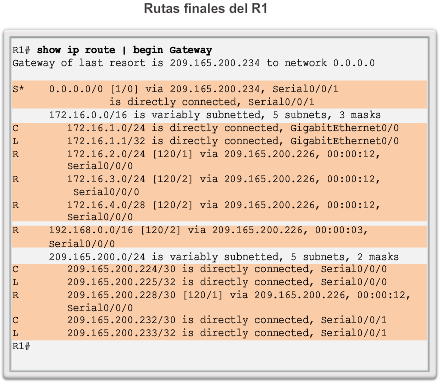
Las rutas se analizan en términos de lo siguiente:

* Ruta final
* Ruta de Nivel 1
* Ruta principal de nivel 1
* Rutas secundarias de nivel 2



Una ruta final es una entrada de la tabla de routing que contiene una dirección IPv4 del siguiente salto o una interfaz de salida. Las rutas conectadas directamente, las rutas descubiertas dinámicamente y las rutas locales son rutas finales.

En la ilustración, las áreas resaltadas son ejemplos de rutas finales. Observe que todas estas rutas especifican una dirección IPv4 del siguiente salto o una interfaz de salida.



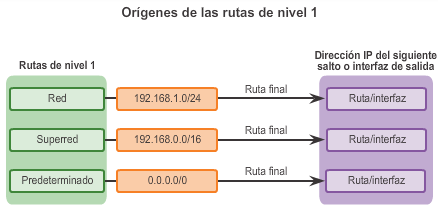
Una ruta de nivel 1 con una máscara de subred igual o inferior a la máscara con clase de la dirección de red. Por lo tanto, una ruta de nivel 1 puede ser cualquiera de las siguientes:

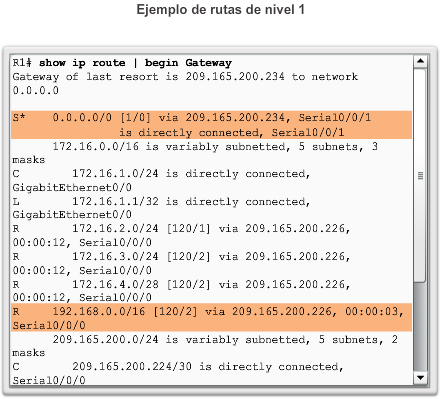
* **Ruta de red**: una ruta de red que tiene una máscara igual a la de la máscara con clase.
* **Ruta de superred**: una dirección de red con una máscara menor que la máscara con clase, por ejemplo, una dirección de resumen.
* **Ruta predeterminada**: una ruta estática con la dirección 0.0.0.0/0.

El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.

En la figura 1, se destaca la forma en que las rutas de nivel 1 también son rutas finales.

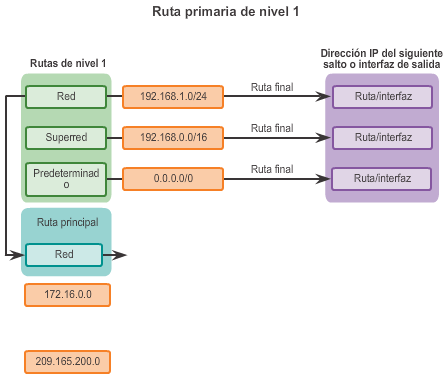
En la figura 2, se destacan las rutas de nivel 1.

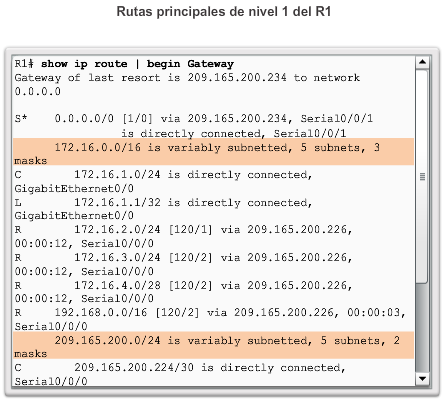




Como se ilustra en la figura 1, una ruta principal de nivel 1 es una ruta de red de nivel 1 que está dividida en subredes. Una ruta principal nunca puede ser una ruta final.

En la figura 2, se destacan las rutas principales de nivel 1 en la tabla de routing del R1. En la tabla de routing, básicamente se proporciona un encabezado para las subredes específicas que contiene. Cada entrada muestra la dirección de red con clase, la cantidad de subredes y la cantidad de máscaras de subred diferentes en las que se subdividió la dirección con clase.



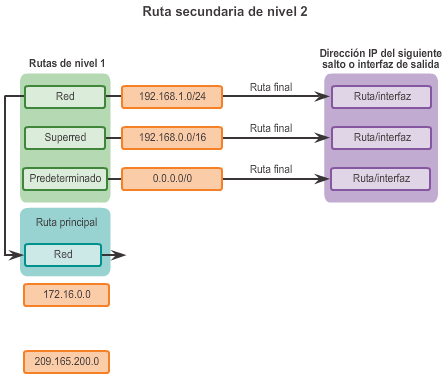


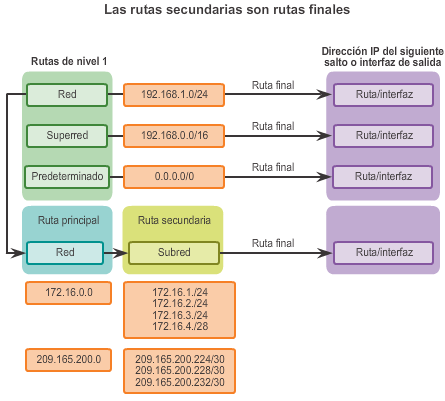
Una ruta secundaria de nivel 2 es una ruta que constituye una subred de una dirección de red con clase. Como se ilustra en la figura 1, una ruta principal de nivel 1 es una ruta de red de nivel 1 que está dividida en subredes. Las rutas principales de nivel 1 contienen rutas secundarias de nivel 2, como se muestra en la figura 2.

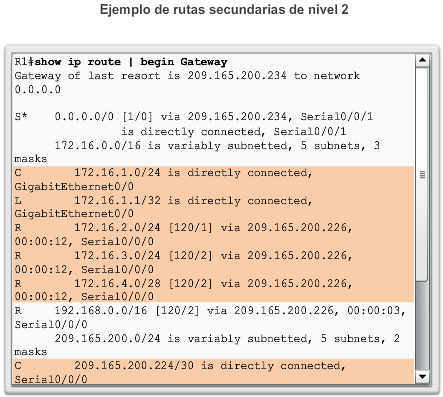
Al igual que en las rutas de nivel 1, el origen de una ruta de nivel 2 puede ser una red conectada directamente, una ruta estática o una ruta descubierta en forma dinámica. Las rutas secundarias de nivel 2 también son rutas finales.

**Nota:** la jerarquía de la tabla de routing en el IOS de Cisco tiene un esquema de routing con clase. Una ruta principal de nivel 1 es la dirección de red con clase de la ruta de subred. Esto es así incluso si un protocolo de enrutamiento sin clase es el origen de la ruta de subred.

En la figura 3, se destacan las rutas secundarias en la tabla de routing del R1.







### Proceso de búsqueda de rutas IPv4

Cuando un paquete llega a una interfaz del router, el router analiza el encabezado de IPv4, identifica la dirección IPv4 de destino y continúa a través del proceso de búsqueda del router.

En la figura 1, el router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv4.

1. Si la mejor coincidencia es una ruta final de nivel 1, se utiliza esa ruta para reenviar el paquete.

2. Si la mejor coincidencia es una ruta principal de nivel 1, se continúa con el siguiente paso.

En la figura 2, el router examina las rutas secundarias (las rutas de subred) de la ruta principal en busca de la mejor coincidencia.

3. Si hay coincidencia con una ruta secundaria de nivel 2, utiliza la subred para enviar el paquete.

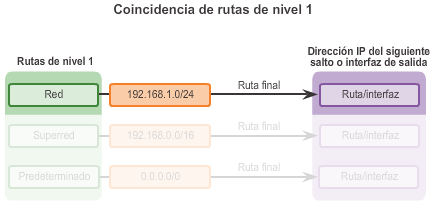
4. Si no hay coincidencia con ninguna de las rutas de nivel 2, se continúa con el paso siguiente.

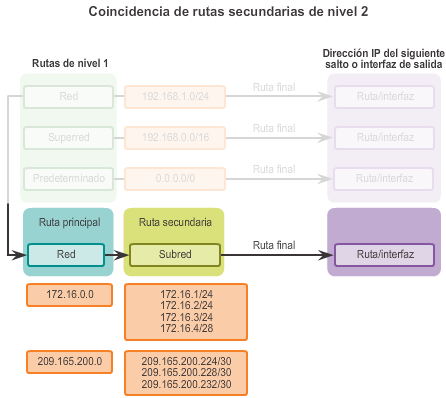
En la figura 3, el router continúa buscando rutas de superred de nivel 1 en la tabla de routing para detectar una coincidencia, incluida la ruta predeterminada, si la hubiera.

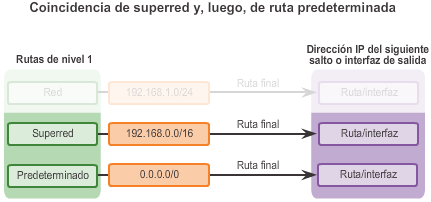
5. Si ahora hay una coincidencia menor con las rutas predeterminadas o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.

6. Si no hay coincidencia con ninguna ruta de la tabla, el router descarta el paquete.

**Nota:** una ruta que solo hace referencia a una dirección IP del siguiente salto y no a una interfaz de salida debe resolverse a una ruta con una interfaz de salida. Se realiza una búsqueda recurrente en la dirección IP del siguiente salto hasta que se resuelva con una interfaz de salida.





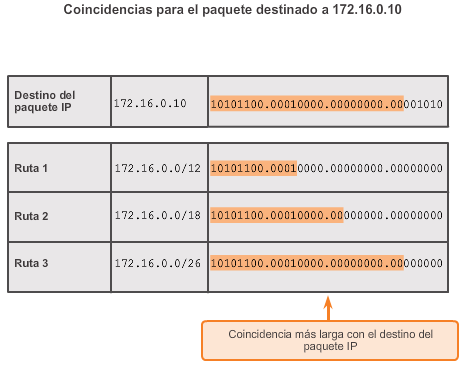


¿Qué significa que el router deba encontrar la mejor coincidencia en la tabla de routing? La mejor coincidencia es la coincidencia más larga.

Para que haya una coincidencia entre la dirección IPv4 de destino de un paquete y una ruta en la tabla de routing, una cantidad mínima de los bits del extremo izquierdo deben coincidir entre la dirección IPv4 del paquete y la ruta en la tabla de routing. La máscara de subred de la ruta en la tabla de routing se utiliza para determinar la cantidad mínima de bits del extremo izquierdo que deben coincidir. Recuerde que un paquete IPv4 solo contiene la dirección IPv4 y no la máscara de subred.

La mejor coincidencia es la ruta de la tabla de routing que contiene la mayor cantidad de bits del extremo izquierdo coincidentes con la dirección IPv4 de destino del paquete. La ruta con la mayor cantidad de bits del extremo izquierdo equivalentes, o la coincidencia más larga, es siempre la ruta preferida.

En la ilustración, el destino de un paquete es 172.16.0.10. El router tiene tres rutas posibles que coinciden con este paquete: 172.16.0.0/12, 172.16.0.0/18 y 172.16.0.0/26. De las tres rutas, 172.16.0.0/26 tiene la coincidencia más larga y, por lo tanto, se elige para reenviar el paquete. Recuerde que para que cualquiera de estas rutas se considere una coincidencia debe tener al menos la cantidad de bits coincidentes que se indica en la máscara de subred de la ruta.



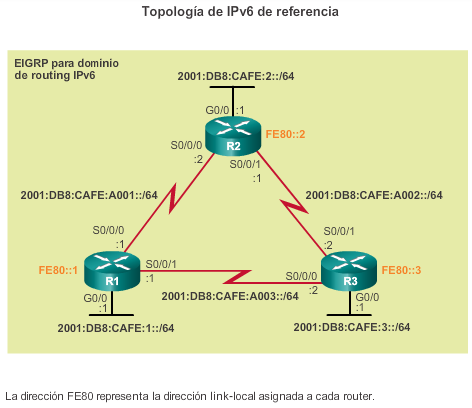
### Análisis de una tabla de routing IPv6

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.

Dado que IPv6 fue diseñado como un protocolo sin clase, todas las rutas son en realidad rutas finales de nivel 1. No hay rutas principales de nivel 1 para rutas secundarias de nivel 2.

La topología que se muestra en la ilustración se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

* El R1, el R2 y el R3 están configurados en una topología de malla completa. Todos los routers tienen rutas redundantes hacia diversas redes.
* El R2 es el router perimetral y se conecta con el ISP. Sin embargo, no se anuncia una ruta estática predeterminada.
* Se configuró EIGRP para IPv6 en los tres routers.



En la figura 1, se muestra la tabla de routing del R1 mediante el comando **show ipv6 route**. Si bien el resultado del comando se muestra de manera levemente distinta de como se muestra en la versión IPv4, aún contiene la información importante de la ruta.

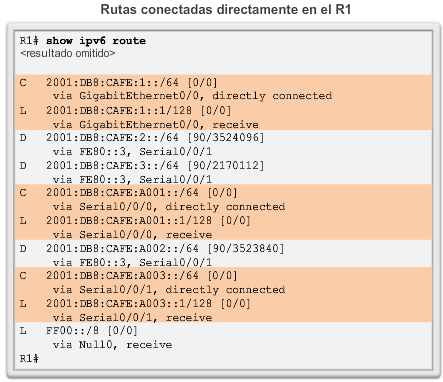
En la figura 2, se destacan la red conectada y las entradas en la tabla de routing local de las interfaces conectadas directamente. Las tres entradas se agregaron cuando las interfaces se configuraron y activaron.

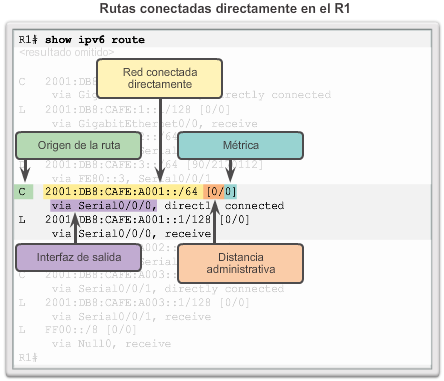
Como se muestra en la figura 3, en las entradas de las rutas conectadas directamente se muestra la siguiente información:

* **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta (“C” identifica una red conectada directamente, mientras que “L” identifica que esta es una ruta local).
* **Red conectada directamente:** la dirección IPv6 de la red conectada directamente.
* **Distancia administrativa:** identifica la confiabilidad del origen de la ruta. IPv6 utiliza las mismas distancias que IPv4. El valor 0 indica el mejor origen y el más confiable.
* **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
* **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

**Nota:** los enlaces seriales tienen anchos de banda de referencia configurados para observar la forma en que las métricas de EIGRP seleccionan la mejor ruta. El ancho de banda de referencia no es una representación realista de las redes modernas. Se utiliza solamente para proporcionar una idea visual de la velocidad del enlace.







En la figura 1, se destacan las entradas de la tabla de routing para las tres redes remotas (es decir, la LAN del R2, la LAN del R3 y el enlace entre el R2 y el R3). Las tres entradas se agregaron mediante EIGRP.

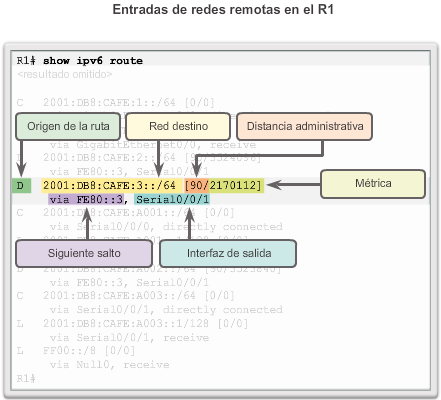
En la figura 2, se muestra una entrada de la tabla de routing en el R1 para la ruta hacia la red remota 2001:DB8:CAFE:3::/64 en el R3. La entrada indica la siguiente información:

* **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Los códigos comunes incluyen O (OSPF), D (EIGRP), R (RIP) y S (ruta estática).
* **Red de destino:** identifica la dirección de la red IPv6 remota.
* **Distancia administrativa:** identifica cuán confiable es el origen de la ruta. IPv6 utiliza las mismas distancias que IPv4.
* **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
* **Siguiente salto:** identifica la IPv6 del router siguiente al que debe reenviar el paquete.
* **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Cuando un paquete IPv6 llega a una interfaz del router, el router analiza el encabezado de IPv6 e identifica la dirección IPv6 de destino. A continuación, el router continúa con el proceso de búsqueda del siguiente router.

El router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv6. Al igual que en IPv4, la coincidencia más larga es la mejor coincidencia. Por ejemplo, si hay varias coincidencias en la tabla de routing, el router elige la ruta con la coincidencia más larga. La coincidencia se encuentra entre los bits del extremo izquierdo de la dirección IPv6 de destino del paquete y el prefijo IPv6 y la duración de prefijo en la tabla de routing IPv6.





## Resumen

Los routers utilizan protocolos de routing dinámico para facilitar el intercambio de información de routing entre ellos. El propósito de los protocolos de routing dinámico incluye lo siguiente: detección de redes remotas, mantenimiento de información de routing actualizada, selección de la mejor ruta hacia las redes de destino y capacidad para encontrar una mejor ruta nueva si la ruta actual deja de estar disponible. Si bien los protocolos de routing dinámico requieren menos sobrecarga administrativa que el routing estático, requieren dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y ancho de banda del enlace de red.

Las redes generalmente utilizan una combinación de routing estático y dinámico. El routing dinámico es la mejor opción para las redes grandes, y el routing estático es más adecuado para las redes de rutas internas.

Los protocolos de routing se encargan de detectar redes remotas y de mantener información de red precisa. Cuando se produce un cambio en la topología, los protocolos de routing propagan esa información por todo el dominio de routing. El proceso para lograr que todas las tablas de routing alcancen un estado de coherencia, en el cual todos los routers en el mismo dominio o área de routing tienen información completa y precisa acerca de la red, se denomina “convergencia”. Algunos protocolos de routing convergen más rápido que otros.

Los protocolos de routing pueden clasificarse como con clase o sin clase, vector distancia o estado de enlace, y protocolo de gateway interior o protocolo de gateway exterior.

Los protocolos vector distancia utilizan routers como “letreros” a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento vector distancia no tienen un mapa en sí de la topología de la red.

Un router configurado con un protocolo de routing de estado de enlace puede crear una “vista completa” o una topología de la red al reunir información proveniente de todos los demás routers.

Los protocolos de enrutamiento usan métricas para determinar el mejor camino o la ruta más corta para llegar a una red de destino. Diferentes protocolos de enrutamiento pueden usar diferentes métricas. Por lo general, una métrica inferior indica un mejor camino. Las métricas se pueden determinar mediante los saltos, el ancho de banda, el retraso, la confiabilidad y la carga.

Los routers a veces obtienen información sobre múltiples rutas hacia la misma red a partir de rutas estáticas como de protocolos de enrutamiento dinámico. Cuando un router aprende sobre una red de destino desde más de un origen de enrutamiento, los routers Cisco usan el valor de distancia administrativa para determinar qué origen usar. Cada protocolo de enrutamiento dinámico tiene un valor administrativo único junto con las rutas estáticas y las redes conectadas directamente. Cuanto menor es el valor administrativo, mayor es la preferencia del origen de ruta. Una red conectada directamente es siempre el origen preferido, seguido de las rutas estáticas y luego los diversos protocolos de enrutamiento dinámico.

El comando **show ip protocols**muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router. Para IPv6, utilice**show ipv6 protocols**.

En los protocolos de routing de estado de enlace, como OSPF, un enlace es una interfaz en un router. La información acerca del estado de dichos enlaces se conoce como estados de enlace. Todos los protocolos de routing de estado de enlace aplican el algoritmo de Dijkstra para calcular la mejor ruta. A este algoritmo se le llama comúnmente “algoritmo SPF” (Shortest Path First). Para determinar el costo total de una ruta, este algoritmo utiliza costos acumulados a lo largo de cada ruta, de origen a destino.

