UD6 ENRUTAMIENTO DINÁMICO

Índice

Introducción

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.

El primer protocolo dinámico que se implementó fue **RIP** (Routing Information Protocol). 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.

	Protocolos de gateway interior				Protocolos de gateway exterior
	Vector distancia		Estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Minimizar el retardo de los paquetes de datos y maximizar el rendimiento total de la red, sería la combinación más apropiada para un algoritmo de enrutamiento. La cuestión primordial en este sentido es, por tanto, seleccionar una métrica adecuada para poder determinar qué ruta es la mejor en términos de rapidez y fiabilidad. Existen dos categorías principales de algoritmos de encaminamiento dinámico: vector-distancia y estado de enlace

Algoritmos basados en el vector de distancia

Los algoritmos basados en el vector de distancia utilizan la distancia para determinar la mejor ruta para alcanzar a la red de destino, la cual, generalmente, contabiliza el número de routers atravesados hasta su destino. Cuando un router agrega la ruta hacia una red, almacena fundamentalmente la IP de la red de destino, su máscara, el vector (que es la interfaz de salida o la IP de la interfaz del siguiente salto) y la distancia o métrica.

“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.

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 (obsoleto y reemplazado por EIGRP)
- **EIGRP:** versión avanzada del routing vector distancia

Este tipo de protocolos normalmente envían la información de la tabla de encaminamiento completa a todos sus routers vecinos del mismo protocolo, están basados en el algoritmo Bellman-Ford y son más fáciles de configurar y de mantener que los basados en el estado del enlace, aunque son más susceptibles a los bucles y más lentos en alcanzar el estado de convergencia.

Algoritmos basados en el estado del enlace

A diferencia de los protocolos basados en el vector de distancia, los protocolos de estado del enlace no envían la tabla de enrutamiento completa a sus vecinos, sino que están atentos a los cambios de la red y avisan a sus vecinos cuando esto ocurre, utilizando direcciones multicast. Cada router que usa este protocolo crea tres tablas diferentes: tabla de routers vecinos, tabla de la topología de la red y tabla de enrutamiento.

Estos protocolos se basan en el algoritmo de Dijkstra, son más difíciles de configurar y requieren de más memoria y mayor procesamiento de CPU que los basados en el vector de distancia, pero son más rápidos en alcanzar el estado de convergencia.

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. Es como tener un mapa completo de la topología de la red. 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 estado de enlace 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 cuando una red se desactiva.

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.

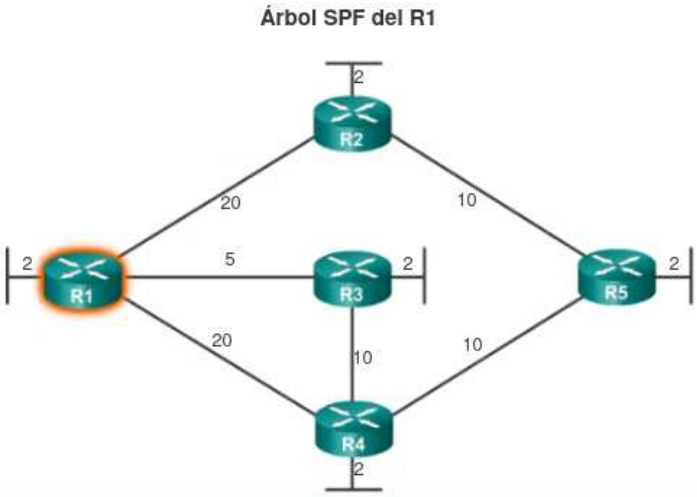
Hay dos IGP de estado de enlace IPv4:

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

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.

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).



Destino	Ruta más corta	Costo
LAN del R2	R1 a R2	22
LAN del R3	R1 a R3	7
LAN del R4	Del R1 al R3 al R4	17
LAN del R5	Del R1 al R3 al R4 al R5	27

Destino	Ruta más corta	Costo
LAN de R1	Del R2 al R1	22
LAN del R3	Del R2 al R1 al R3	27
LAN del R4	Del R2 al R5 al R4	22
LAN del R5	Del R2 al R5	12

Destino	Ruta más corta	Costo
LAN de R1	Del R3 al R1	7
LAN del R2	Del R3 al R1 al R2	27
LAN del R4	R3 a R4	12
LAN del R5	Del R3 al R4 al R5	22

Destino	Ruta más corta	Costo
LAN de R1	Del R4 al R3 al R1	17
LAN del R2	Del R4 al R5 al R2	22
LAN del R3	Del R4 al R3	12
LAN del R5	Del R4 al R5	12

Destino	Ruta más corta	Costo
LAN de R1	Del R5 al R4 al R3 al R1	27
LAN del R2	Del R5 al R2	12
LAN del R3	Del R5 al R4 al R3	22
LAN del R4	Del R5 al R4	12

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 en el estado activado.

2. Los routers de estado de enlace se saludan 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 y determinar el mejor camino hacia cada red.

Protocolos de enrutamiento interior y exterior

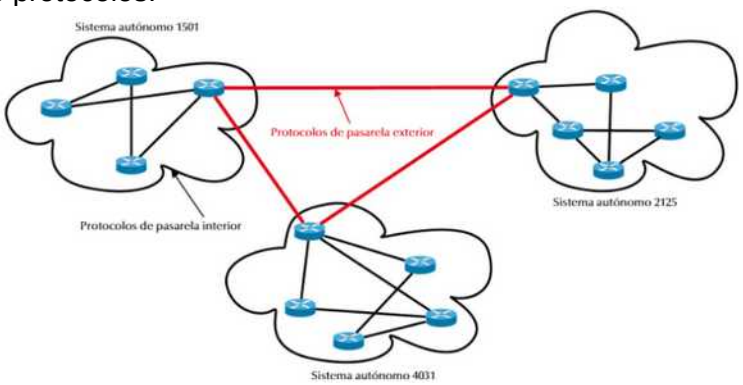
Se define un sistema autónomo (AS) como “un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de enrutamiento”, es decir, un AS está formado por un conjunto de redes que son gestionadas y supervisadas por un mismo organismo. Internacionalmente, el ICANN es el organismo encargado de emitir los identificadores de sistemas autónomos (números de 16 bits), que, evidentemente, serán únicos para cada uno de ellos.

Los protocolos de pasarela exterior o BGP se utilizan para comunicar sistemas autónomos (AS) y son usados fundamentalmente por los proveedores de acceso a Internet (ISP). Además, su métrica está basada en políticas de red.

En función de que un protocolo de encaminamiento se ejecute dentro o fuera del ámbito de un sistema autónomo, se pueden diferenciar dos tipos de protocolos:

1. Protocolos de pasarela interior (IGP). Son los utilizados dentro del ámbito de un dominio de enrutamiento (AS). Por ejemplo: RIP, IGRP, EIGRP, OSPF o IS-IS.

2. Protocolos de pasarela exterior (EGP). Se utilizan para comunicar distintos dominios de enrutamiento (AS). Por ejemplo, BGP.



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.

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.

Las desventajas del routing estático incluyen las siguientes:

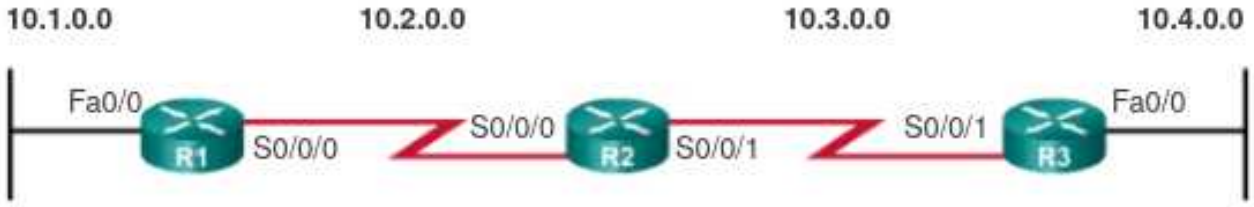
- No es fácil de implementar en redes grandes.
- La administración de las configuraciones estáticas puede llevar mucho tiempo.
- Si un enlace falla, una ruta estática no puede volver a enrutar el tráfico.

Ventajas	Desventajas
Fácil de implementar en una red pequeña.	Adecuado solamente para topologías simples o para fines específicos, como una ruta estática predeterminada. La complejidad de la configuración aumenta notablemente a medida que crece la red.
Muy seguro. No se envían anuncios, a diferencia del caso de los protocolos de routing dinámico.	La complejidad de la configuración aumenta significativamente cuando el tamaño de la red es mayor.
La ruta hacia el destino siempre es la misma.	Se requiere intervención manual para volver a enrutar el tráfico.
Dado que no se requieren algoritmos de routing ni mecanismos de actualización, no se necesitan recursos adicionales (CPU o RAM).	

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 más 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.

Ejemplo Vector de distancia (RIPv2)



arranque

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.

Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Intercambio inicial

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.

Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1

Siguientes actualizaciones

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.

Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/0	1
10.4.0.0	S0/0/0	2

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0
10.1.0.0	S0/0/0	1
10.4.0.0	S0/0/1	1

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0
10.2.0.0	S0/0/1	1
10.1.0.0	S0/0/1	2

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.

Convergencia

La convergencia de la red se produce cuando todos los routers tienen información completa y precisa acerca de toda red. 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.

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.

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.

RIP

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.

Modo configuración de RIP

para entrar en modo de configuración RIP escribimos el comando **router rip**

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 RIPv2 debemos teclear el comando **version 2**

Debemos también deshabilitar la sumarización automática

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.

```
R1> enable
R1# configure terminal
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
R1(config-router)# no auto-summary
R1(config-router)# exit
```

Para modificar el comportamiento predeterminado de RIPv2 de sumarización automática, utilice el comando del modo de configuración del router **no auto-summary**

Anuncio de las redes

Para habilitar el routing RIP para una red, utilice el comando del modo de configuración del router **network dirección-red**. 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.

El comando **show ip protocols** muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router. **show ip protocols | begin Default**

El comando **show ip route** muestra las rutas RIP instaladas en la tabla de routing.

Interfaces pasivas

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.

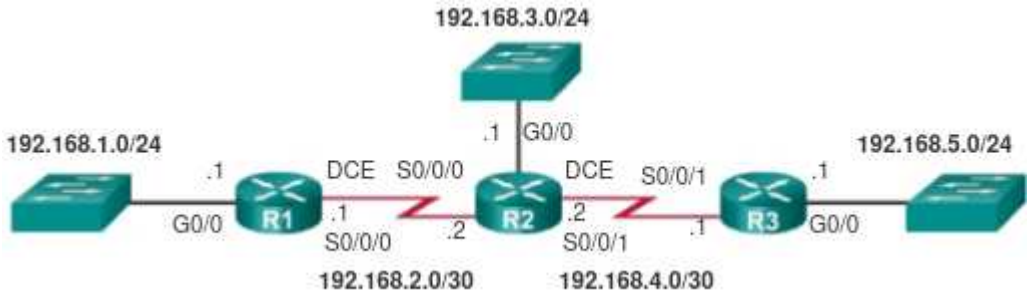
El envío de actualizaciones innecesarias a una LAN impacta en la red de tres maneras:

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 interfaz** 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.

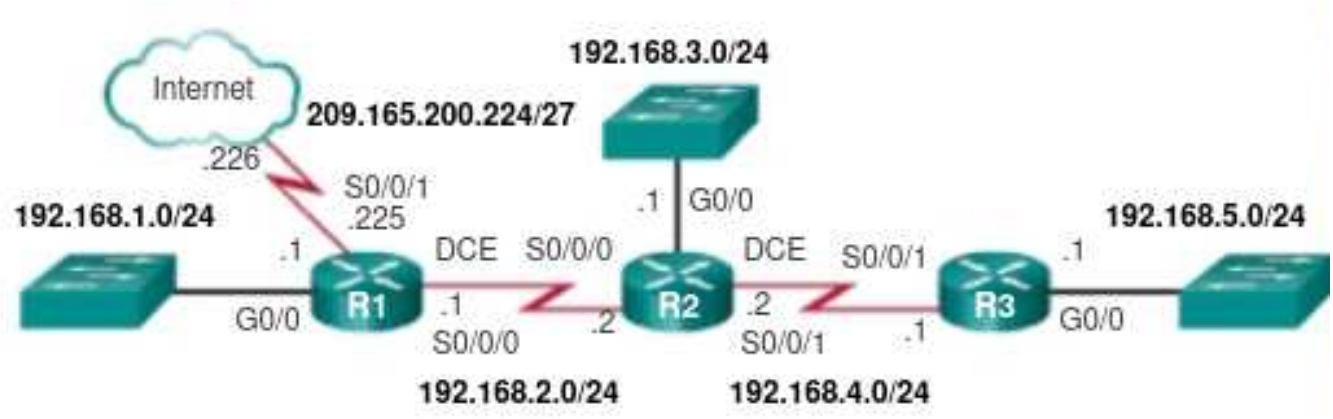


En este ejemplo no es necesario que el R1, el R2, y el R3 reenvíen actualizaciones RIP por sus interfaces LAN. Vamos a identificar la interfaz G0/0 del R1 como pasiva. El comando show ip protocols se utiliza para verificar que la interfaz Gigabit Ethernet es pasiva. Observe que ya no se indica que la 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.

```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
R1# show ip protocols | begin Default
Default version control: send version 2, receive version 2
  Interfaz         Enviar   Recv  Triggered RIP      Key-chain
  Serial0/0/0      2        2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
```

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**.

Rutas por defecto



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 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.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^Z
```

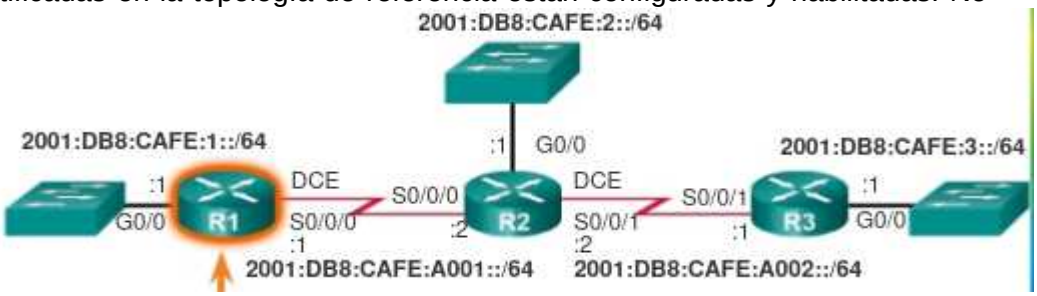
Con show ip rote podemos ver como R* que significa RIP nos dio la ruta por defecto

```
C       192.168.5.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.5.254/32 is directly connected, GigabitEthernet0/0/0
R*   0.0.0.0/0 [120/1] via 192.168.1.254, 00:00:14, GigabitEthernet0/0/1
```

RIPv6

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.

En la situación de la figura, 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 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**.

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 R1 debería configurarse con lo siguiente:

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ipv6 rip RIP-AS enable
R1(config-if)# exit
R1(config)#
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 rip RIP-AS enable
R1(config-if)# no shutdown
R1(config-if)#
```

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 R1 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.

El comando **show ipv6 protocols** no proporciona la misma cantidad de información que su equivalente para IPv4.

El comando **show ipv6 route** muestra las rutas instaladas en la tabla de routing

OSPF

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.

Durante el arranque, R1 carga el archivo de configuración de inicio guardado. A medida que se activan las interfaces configuradas, 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.

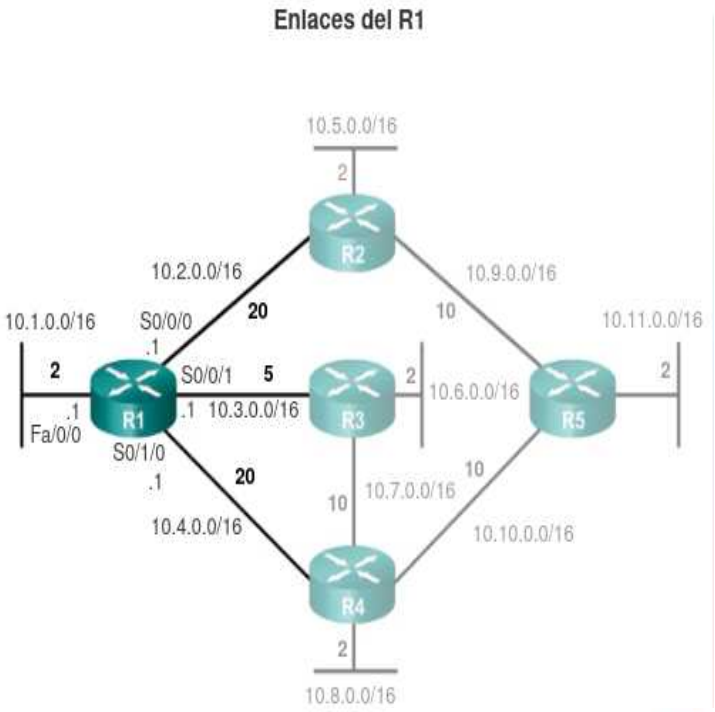
La información de estado de enlace incluye lo siguiente:

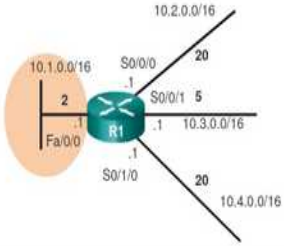
La dirección IPv4 y la máscara de subred de la interfaz

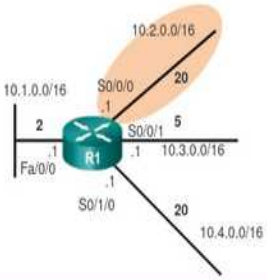
El tipo de red, como Ethernet (difusión) o enlace serial punto a punto

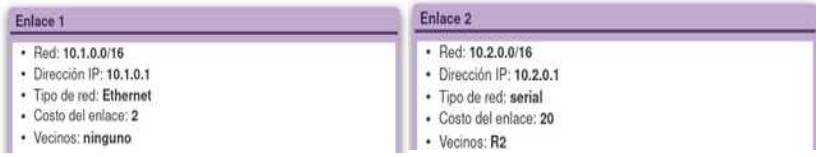
El costo de dicho enlace (en base por ejemplo al ancho de banda)

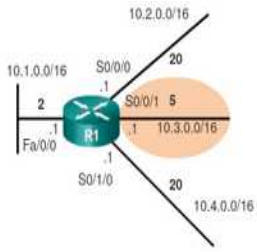
Cualquier router vecino en dicho enlace

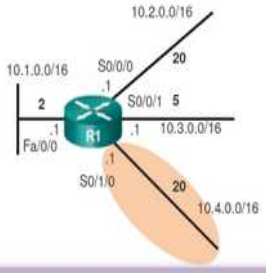












El segundo paso en el proceso de routing de estado de enlace es que cada router asume la responsabilidad de encontrarse con sus vecinos en redes conectadas directamente.

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.

Por ejemplo, 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 contendría lo siguiente:

1. R1; Red Ethernet 10.1.0.0/16; Costo 2
2. R1 -> R2; Red serial punto a punto; 10.2.0.0/16; Costo 20
3. 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 esto se hace 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 (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 red de 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.

Base de datos de Link-State de R1

Estados de enlace del R1:
- Conectado a la red 10.1.0.0/16, costo = 2
- Conectado al R2 en la red 10.2.0.0/16, costo = 20
- Conectado al R3 en la red 10.3.0.0/16, costo = 5
- Conectado al R4 en la red 10.4.0.0/16, costo = 20

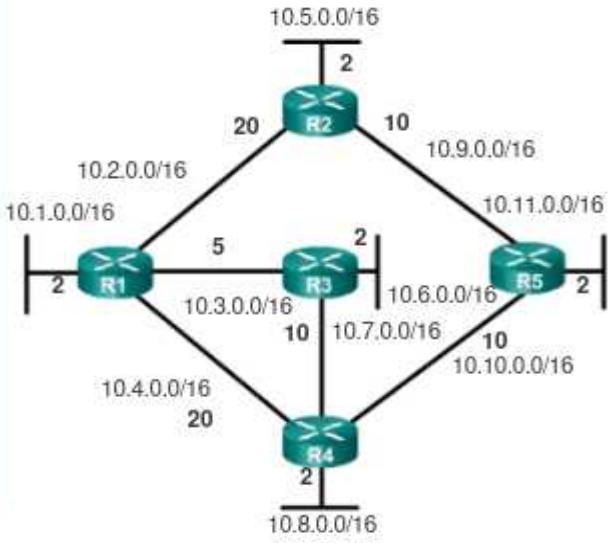
Estados de enlace del R2:
- Conectado a la red 10.5.0.0/16, costo = 2
- Conectado al R1 en la red 10.2.0.0/16, costo = 20
- Conectado al R5 en la red 10.9.0.0/16, costo = 10

Estados de enlace del R3:
- Conectado a la red 10.6.0.0/16, costo = 2
- Conectado al R1 en la red 10.3.0.0/16, costo = 5
- Conectado al R4 en la red 10.7.0.0/16, costo = 10

Estados de enlace del R4:
- Conectado a la red 10.8.0.0/16, costo = 2
- Conectado al R1 en la red 10.4.0.0/16, costo = 20
- Conectado al R3 en la red 10.7.0.0/16, costo = 10
- Conectado al R5 en la red 10.10.0.0/16, costo = 10

Estados de enlace del R5:
- Conectado a la red 10.11.0.0/16, costo = 2
- Conectado al R2 en la red 10.9.0.0/16, costo = 10
- Conectado al R4 en la red 10.10.0.0/16, costo = 10

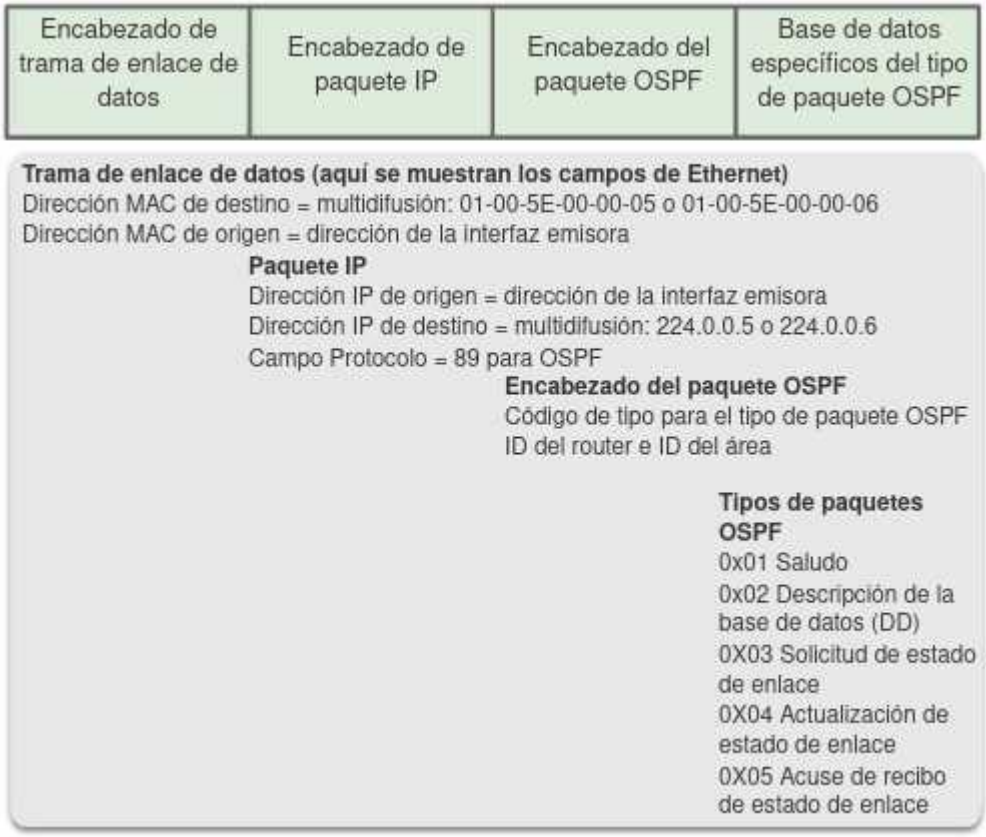
Destino	Ruta más corta	Costo
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27



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.

Mensajes OSPF



Tipos de mensajes

Tipo1, paquete de saludo: se usa para establecer y mantener la adyacencia con otros routers OSPF.

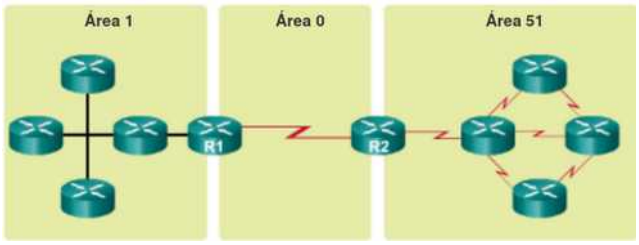
Tipo 2, paquete de descripción de base de datos (DBD): contiene una lista abreviada de la LSDB del router emisor, y los routers receptores la usan para compararla con la LSDB local. Para crear un árbol SPF preciso, la LSDB debe ser idéntica en todos los routers de estado de enlace dentro de un área.

Tipo 3, paquete de solicitud de estado de enlace (LSR): los routers receptores pueden requerir más información sobre cualquier entrada de la DBD mediante el envío de un LSR.

Tipo 4, paquete de actualización de estado de enlace (LSU): se utiliza para responder a los LSR y anunciar la nueva información. Los LSU contienen siete tipos de LSA.

Tipo 5, paquete de acuse de recibo de estado de enlace (LSAck): cuando se recibe una LSU, el router envía un LSAck para confirmar la recepción de la LSU. El campo de datos del LSAck está vacío.

Areas



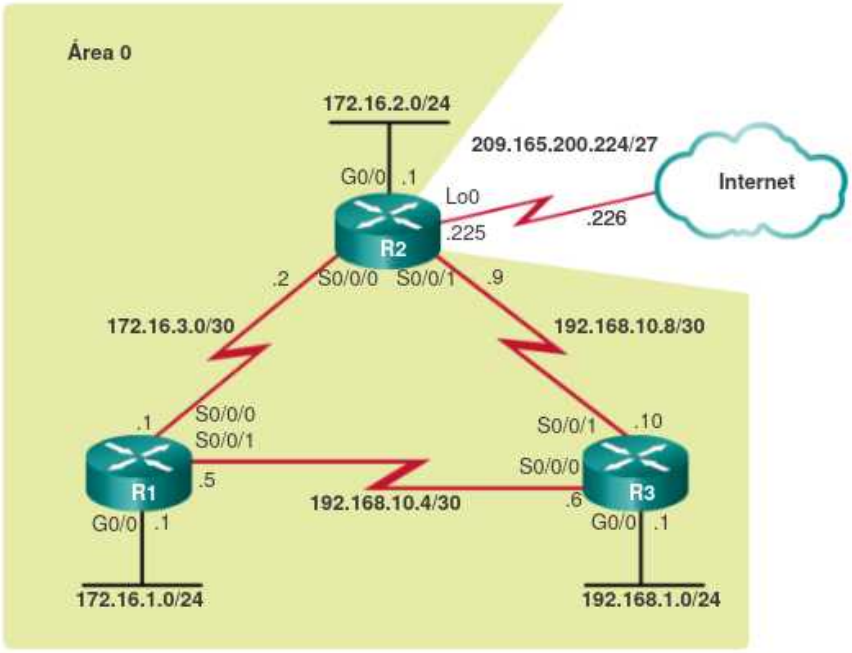
Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB.
OSPF se puede implementar de dos maneras:

- **OSPF de área única:** todos los routers se encuentran en un área llamada “área backbone” (área 0).
- **OSPF multiárea:** OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área backbone (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

Con OSPF multiárea, OSPF puede dividir un sistema autónomo (AS) grande en áreas más pequeñas, a fin de admitir el routing jerárquico. Con el routing jerárquico, se sigue produciendo el routing entre áreas, y muchas de las operaciones de routing que implican una gran exigencia para el procesador, como volver a calcular la base de datos, se guardan en un área.

Por ejemplo, cada vez que un router recibe información nueva acerca de un cambio de topología dentro del área (como el agregado, la eliminación o la modificación de un enlace), el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar la tabla de routing. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cálculos depende del tamaño del área.

Funcionamiento OSPF



Para configurar el protocolo de encaminamiento OSPF en un router de Cisco, hay que especificar el identificador de proceso para el sistema autónomo, el identificador de área (para el grupo de routers que comparten la información en el mismo estado de enlace) y añadir todas las redes (incluyendo Wildcard) a las que está conectado directamente.
OSPFv2 se habilita con el comando **router ospf id-proceso** del modo de configuración global. El valor id-proceso representa un número entre 1 y 65 535, y lo elige el administrador de red. El valor id-proceso tiene importancia en el ámbito local, lo que significa que no necesita ser el mismo valor en los demás routers OSPF para establecer adyacencias con esos vecinos.

Router-id

Se puede utilizar el comando router-id id-router del modo de configuración del router para asignar manualmente un valor de 32 bits expresado como dirección IPv4 a un router. Un router OSPF se identifica ante otros routers mediante esta ID del router.

```
R1(config)# router ospf 10
R1(config-router)# ?
Router configuration commands:
  auto-cost                Calculate OSPF interface cost according
                           to bandwidth
  network                  Enable routing on an IP network
  no                       Negate a command or set its defaults
  passive-interface        Suppress routing updates on an
                           interface
  priority                 OSPF topology priority
  router-id                router-id for this OSPF process
```

En el ejemplo se configuró una ID de router 1.1.1.1 en el R1, 2.2.2.2 en R2 e ID 3.3.3.3 en el R3.

Si la ID del router es la misma en dos routers vecinos, el router muestra un mensaje de error:

%OSPF-4-DUP_RTRID1: Detected router with duplicate router ID (Se detectó un router con una ID de router duplicada).

Si no se especifica un router-id el router calculará uno a partir de su dirección IP de loopback o la dirección IP activa más alta.

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
```

La dirección IPv4 de la interfaz loopback se debe configurar con una máscara de subred 255.255.255.255 Esto crea una ruta de host que no se anuncia como ruta a otros routers OSPF.

En el ejemplo se muestra cómo configurar una interfaz loopback con una ruta de host en el R1. El R1 usa la ruta de host como ID del router, suponiendo que no se configuró ninguna ID de router de manera explícita o que no se obtuvo anteriormente.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

En ocasiones, es necesario modificar una ID de router, por ejemplo, cuando un administrador de red establece un nuevo esquema de ID de router para la red. Sin embargo, una vez que un router selecciona una ID de router, un router OSPF activo no permite que se modifique la ID del router hasta que se vuelva a cargar el router o se borre el proceso OSPF.

se asigna la ID de router 1.1.1.1 al R1. Observe que aparece un mensaje informativo que indica que se debe borrar el proceso OSPF o se debe volver a cargar el router. Esto ocurre debido a que el R1 ya tiene adyacencias con otros vecinos que utilizan la ID de router 192.168.10.5. Se deben volver a negociar esas adyacencias utilizando la nueva IP de router 1.1.1.1.

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for
 this to take effect
R1(config-router)# end
```

se borra el proceso de routing de OSPF con el comando **clear ip ospf process** del modo EXEC privilegiado.

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
```

network

El comando **network** determina qué interfaces participan en el proceso de routing para un área OSPF. Cualquier interfaz de un router que coincida con la dirección de red en el comando **network** está habilitada para enviar y recibir paquetes OSPF. Como consecuencia, se incluye la dirección de red (o de subred) para la interfaz en las actualizaciones de routing OSPF.

La sintaxis básica del comando es **network *dirección-red máscara-wildcard* area *id-área*.**

network 0.0.0.0 255.255.255.255 area id-area publica todas las interfaces con ip

La sintaxis **area** *id-área* se refiere al área OSPF. Al configurar OSPF de área única, se debe configurar el comando **network** con el mismo valor *id-área* en todos los routers. Si bien se puede usar cualquier ID de área, es aconsejable utilizar una ID de área 0 con OSPF de área única. Esta convención facilita la tarea si posteriormente se modifica la red para admitir OSPF multiárea.
Como alternativa, se puede habilitar OSPFv2 con el comando

network *dirección-ip-interfaz* 0.0.0.0 *area id-área* del modo de configuración del router.

La ventaja de especificar la interfaz es que no se necesita calcular la máscara wildcard. OSPFv2 usa la dirección y máscara de subred de la interfaz para determinar qué red debe anunciar.

Algunas versiones de IOS permiten introducir la máscara de subred en lugar de la máscara wildcard. Luego, IOS convierte la máscara de subred al formato de la máscara wildcard.

```
R1(config)#router ospf 10
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.3.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

```
R1(config)#router ospf 10
R1(config-router)#network 172.16.1.1 0.0.0.0 area 0
R1(config-router)#network 172.16.3.1 0.0.0.0 area 0
R1(config-router)#network 192.168.10.5 0.0.0.0 area 0
```

Interfaces pasivas

De manera predeterminada, los mensajes OSPF se reenvían por todas las interfaces con OSPF habilitado. Sin embargo, estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado. Se pueden usar los mismos comandos que ya vimos para RIP

```
R1(config)# router ospf 10
R1(config-router)# passive-interface GigabitEthernet 0/0
R1(config-router)# end
```

Métrica OSPF. Costo

Un protocolo de routing utiliza una métrica para determinar la mejor ruta de un paquete. Una métrica indica la sobrecarga requerida para enviar paquetes a través de una interfaz determinada. OSPF utiliza el costo como métrica. Cuando el costo es menor, la ruta es mejor que una con un costo mayor.

La fórmula que se usa para calcular el costo de OSPF es la siguiente:

- **Costo** = *ancho de banda de referencia* / *ancho de banda de la interfaz*

El ancho de banda de referencia predeterminado es 10^8 (100000000); por lo tanto, la fórmula es la siguiente:

- **Costo** = 100000000bps / ancho de banda de la interfaz en bps

Las interfaces FastEthernet, Gigabit Ethernet y 10 GigE comparten el mismo costo, debido a que el valor del costo de OSPF debe ser un número entero. En consecuencia, dado que el ancho de banda de referencia predeterminado se establece en 100 Mb/s, todos los enlaces que son más rápidos que Fast Ethernet también tienen un costo de 1. Se puede cambiar el ancho de banda de referencia con el comando **auto-cost reference-bandwidth 1000** por ejemplo.

Tipo de interfaz	Ancho de banda de referencia en bps		Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	10
Serial 1,544 Mbps	100,000,000	÷	1,544,000	64
Serial 128 kbps	100,000,000	÷	128,000	781
Serial 64 kbps	100,000,000	÷	64,000	1562

El mismo costo debido al ancho de banda de referencia

También podemos ajustar el ancho de banda del interfaz. Ojo, no modifica el ancho de banda físico del enlace, solo la métrica que usa EIGRP y OSPF. Para ajustar el ancho de banda de la interfaz, utiliza el comando de configuración de interfaz **bandwidth valor_en_kilobits** y el comando **no bandwidth** para restaurar el valor.

Como alternativa a la configuración del ancho de banda de interfaz predeterminado, es posible **configurar el costo de forma manual** en una interfaz con el comando de configuración de interfaz **ip ospf cost *valor*.**

Una ventaja de configurar un costo en lugar del ancho de banda de la interfaz es que, cuando se configura el costo manualmente, el router no necesita calcular la métrica. En cambio, cuando se configura el ancho de banda de la interfaz, el router debe calcular el costo de OSPF sobre la base del ancho de banda. El comando **ip ospf cost** es útil en entornos de varios proveedores, donde los routers que no son de Cisco pueden usar una métrica distinta del ancho de banda para calcular los costos de OSPF.

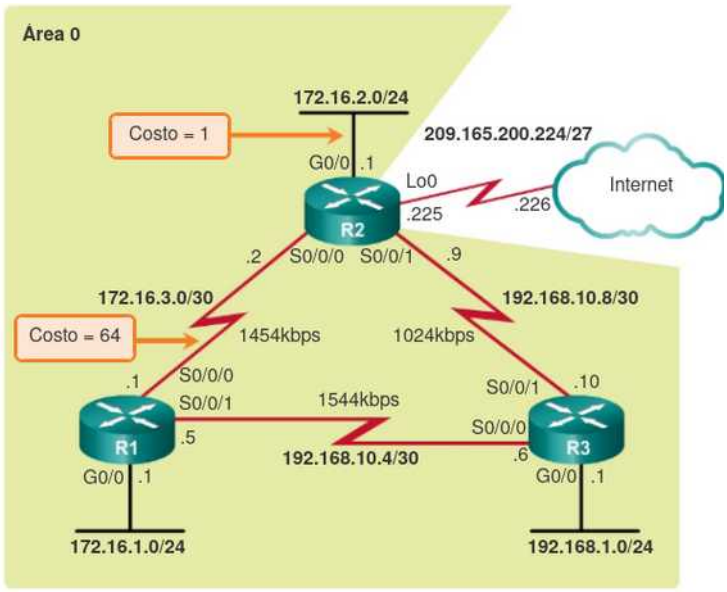
El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino.

En el ejemplo, el costo para llegar desde el R1 hasta la LAN 172.16.2.0/24 del R2 debe ser el siguiente:

Costo del enlace serial del R1 al R2 = 64

Costo del enlace Gigabit Ethernet en R2 = 1

Costo total para llegar a 172.16.2.0/24= **65**

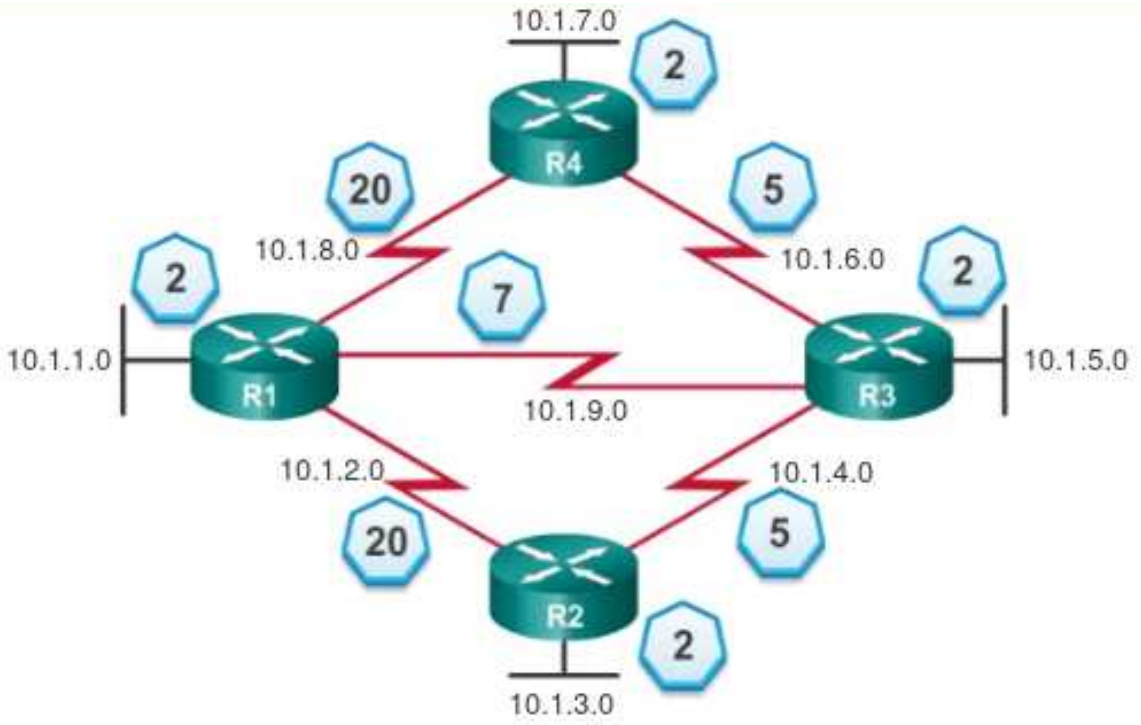



```
R1# show ip route | include 172.16.2.0
O        172.16.2.0/24 [110/65] via 172.16.3.2, 03:39:07,
         Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 65, type intra
  area
  Last update from 172.16.3.2 on Serial0/0/0, 03:39:15 ago
  Routing Descriptor Blocks:
  * 172.16.3.2, from 2.2.2.2, 03:39:15 ago, via Serial0/0/0
      Route metric is 65, traffic share count is 1
R1#
```

Como en el caso de IPv6 también podemos habilitar OSPF directamente en la interfaz poniendo:
ip ospf id-proceso area id-área en el modo de configuración de la interfaz concreta.

Ejemplo:

Dada la topología, crea el árbol SPF. Escenario 1 para R1, Escenario2 para R2



Escenario 1

Red destino	Costo
10.1.5.0	
10.1.6.0	
10.1.7.0	
10.1.8.0	
10.1.9.0	

Escenario 2

Red destino	Costo
10.1.1.0	
10.1.4.0	
10.1.5.0	
10.1.6.0	
10.1.7.0	

Solución 9,12,14,20,7
Solución 14,5,7,10,12

Tabla de routing

Cada protocolo de enrutamiento tiene una distancia administrativa por defecto. No hay que confundirla con la métrica. La métrica es una medida dentro de cada protocolo.

Si existen varias rutas para el mismo destino desde el mismo protocolo, se seleccionará en función del valor de su métrica, mientras que, si las rutas múltiples pertenecen a más de un protocolo, será seleccionada aquella ruta del protocolo cuyo valor de distancia administrativa sea menor.

Protocolo de enrutamiento	Distancia administrativa por defecto
Interfaces directamente conectadas	0
Rutas estáticas	1
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
ODR	160
EIGRP externo	170
BGP interno	200

```
Gateway of last resort is not set

   10.0.0.0/16 is subnetted, 1 subnets
S     10.4.0.0 is directly connected, Serial0/0/0
   172.16.0.0/24 is subnetted, 3 subnets
C     172.16.1.0 is directly connected, FastEthernet0/0
C     172.16.2.0 is directly connected, Serial0/0/0
D     172.16.3.0 [90/2172416] via 172.16.2.1, 00:00:18, Serial0/0/0
C  192.168.1.0/24 is directly connected, Serial0/0/1
O  192.168.100.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
O  192.168.110.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
R  192.168.120.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/0
```

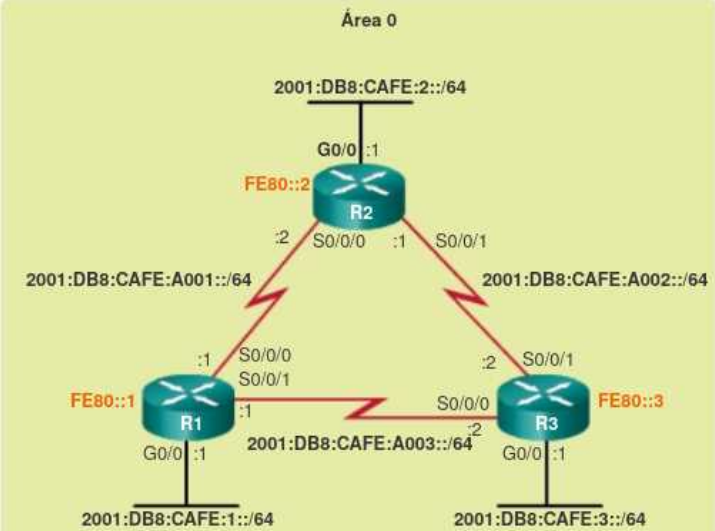
Comandos show

Router# **show running-config**
Router# **show ip route**
Router# **show ip protocols**
Router# **show ip route ospf**
Router# show ip ospf border-routers
Router# show ip ospf database
Router# **show ip ospf neighbor**
Router# **show ip ospf interface** nos permite ver entre otra información el costo del enlace
Router# **show ip ospf interface brief**
Router# debug custom-queue
Router# debug eigrp
Router# debug standby
Router# debug ip rip
Router# clear ip route

OSPFv3 para IPv6

En la figura se muestra la topología de la red que se utiliza para configurar OSPFv3.

En esta topología, ninguno de los routers tiene direcciones IPv4 configuradas. Una red con las interfaces del router configuradas con direcciones IPv4 e IPv6 se denomina “dual-stack”. Una red dual-stack puede tener OSPFv2 y OSPFv3 habilitados de manera simultánea.



La dirección FE80 representa la dirección link-local asignada a cada router.

En la figura de la derecha se muestra el routing de unidifusión IPv6 y la configuración de las direcciones de unidifusión global del R1, como se identifican en la topología de referencia. Supón que las interfaces del R2 y el R3 también se configuraron con sus direcciones de unidifusión global, como se identifica en la topología mencionada.

```
R1(config)#ipv6 unicast-routing
R1(config)#
R1(config)#interface GigabitEthernet 0/0
R1(config-if)#description R1 LAN
R1(config-if)#ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#interface Serial0/0/0
R1(config-if)#description Link to R2
R1(config-if)#ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#interface Serial0/0/1
R1(config-if)#description Link to R3
R1(config-if)#ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)#no shut
R1(config-if)#end
R1#
```

Pasos para configurar OSPFv3

Paso 1: habilitar el routing de unidifusión IPv6 (**`ipv6 unicast-routing`**).
Paso 2: (optativo) configurar las direcciones link-local.
Paso 3: configurar una ID del router de 32 bits en el modo de configuración del router OSPFv3 con el comando **`router-id`** `id-router`.
Paso 4: configurar detalles de routing optativos, como ajustar el ancho de banda de referencia.
Paso 5: (optativo) configurar parámetros específicos de interfaz OSPFv3. Por ejemplo, ajustar el ancho de banda de la interfaz.
Paso 6: habilitar el routing IPv6 con el comando **`ipv6 ospf area`**.

Direcciones de link-local

En la ilustración, el resultado del comando s**how ipv6 interface brief** confirma que se configuraron correctamente las direcciones IPv6 globales y que se habilitaron las interfaces. Además **cada interfaz generó automáticamente una dirección link-local**.

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0     [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:1::1
GigabitEthernet0/1     [administratively down/down]
    unassigned
Serial0/0/0            [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:A001::1
Serial0/0/1            [up/up]
    FE80::32F7:DFF:FEA3:DA0
    2001:DB8:CAFE:A003::1
```

Las direcciones link-local se crean de manera automática cuando se asigna una dirección IPv6 de unidifusión global a la interfaz. No se requieren direcciones de unidifusión global en una interfaz, pero sí se requieren direcciones IPv6 link-local.

A menos que se configure manualmente, los routers Cisco crean la dirección link-local utilizando el prefijo FE80::/10 y el proceso EUI-64. EUI-64 implica usar la dirección MAC de Ethernet de 48 bits, insertar FFFE en el medio e invertir el séptimo bit. Para las interfaces seriales, Cisco usa la dirección MAC de una interfaz Ethernet. Observa que las tres interfaces usan la misma dirección link-local.

Las direcciones link-local creadas con el formato EUI-64 o con ID de interfaz aleatorias hacen que resulte difícil reconocer y recordar esas direcciones. Debido a que los protocolos de routing IPv6 utilizan direcciones IPv6 link-local para el direccionamiento de unidifusión y la información de dirección de siguiente salto en la tabla de routing, es habitual hacer que sea una dirección fácil de reconocer.

Configurar la dirección link-local de forma manual permite crear una dirección reconocible y más fácil de recordar. Además, un router con varias interfaces puede asignar la misma dirección link-local a cada interfaz IPv6. Esto se debe a que la dirección link-local solo se requiere para las comunicaciones locales.

Las direcciones link-local pueden configurarse de forma manual con el mismo comando de interfaz que se usa para crear direcciones IPv6 de unidifusión global, pero agregando la palabra clave link-local al comando ipv6 address.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#
```

Una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hexteto (segmento de 16 bits), la palabra clave link-local debe seguir la dirección.

En el ejemplo se ve que las direcciones link-local de las interfaces del R1 se cambiaron a FE80::1. Se podría hacer lo mismo con R2 y R3 cambiándolas a FE80::2 y FE80::3 respectivamente.

Configuración id y ancho de banda

El comando es el mismo que el visto anteriormente.

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manuall
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6:  Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
```

También podemos cambiar el id del router y volver al predeterminado con **clear ipv6 ospf process**

Habilitar OSPFv3 en las interfaces

OSPFv3 utiliza un método diferente para habilitar una interfaz para OSPF. **En lugar de usar el comando network** del modo de configuración del router para especificar las direcciones de interfaz que coinciden, **OSPFv3 se configura directamente en la interfaz.**

Para habilitar OSPFv3 en una interfaz, utilice el comando **ipv6 ospf id-proceso area id-área** del modo de configuración de interfaz.

El valor id-proceso identifica el proceso de routing específico y debe coincidir con la ID de proceso utilizada para crear el proceso de routing en el comando ipv6 router ospf id-proceso.

El valor id-área es el área que se debe asociar a la interfaz OSPFv3. Aunque pudo haberse configurado cualquier valor para el área, se seleccionó 0 debido a que el área **0 es el área backbone** a la que se deben conectar todas las demás áreas. Esto contribuye a la migración a OSPF multiárea, si surge la necesidad.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface  PID   Area     Intf ID  Cost   State  Nbrs F/C
Se0/0/1    10     0         7      15625  P2P    0/0
Se0/0/0    10     0         6      647    P2P    0/0
Gi0/0      10     0         3       1     WAIT   0/0
R1#
```

EIGRP

El proceso para configurar EIGRP es exactamente el mismo que OSPF pero sin poner el área en las networks.

La métrica se cuenta como 256*(10^7/ menor BW en kbps + suma delay en microsec/10)

Ejemplo para GB $10^7/10^6 = 10$
Fe $10^7/10^5 = 100$
Serie 128Kbps $10^7/128 = 78125$

Delays GB -> 10µs/10 = 1
Fe -> 100µs/10 = 10
Serie -> 20000µs/10 = 2000

Como vemos, EIGRP no funcionará bien para enlaces de más de 10G o enlaces trunk ya que el retardo (delay) menor que puede computar para un interface es de 10µs (es decir 1) de los enlaces GBE

Para propagar la ruta por defecto podemos poner el comando redistribute static que distribuirá todas las rutas estáticas pero con una distancia administrativa alta con lo que tendrá más vigencia OSPF o RIP

Intefaces de loopback

Una interfaz de loopback es una interface sólo de software que emula una interfaz física. La interfaz existe en IPv4 e IPv6. La interfaz de loopback ayuda a sobreponerse a fallos de enrutamiento. Es accesible desde cualquier otra interfaz física, así que si una cae, se puede acceder a la interfaz de loopack desde otra.

La interfaz de loopback es una interfaz lógica que es interna al router. No está asignada a un puerto físico y no puede ser conectada a ningún otro dispositivo. Se considera una interfaz de software que se coloca automáticamente en estado “up”, siempre que el router esté funcionando.

Esto hace el loopback ideal para asignar a switches Capa 3 direcciones IP cuando quieres una sola dirección como referencia que sea independiente del estado de cualquiera de las interfaces físicas en el dispositivo. Un ejemplo de esto es utilizar la dirección de IP de un loopback como la dirección IP para la entrada DNS

Las interfaces físicas pueden fallar, y también pueden ser puestas fuera de servicio para mantenimiento. Si cualquiera de las interfaces en el Router está caída, otro dispositivo no será capaz de acceder a aquella interfaz. Cuándo configuras un dispositivo con un loopback y le asignas una IP estás anunciado que el dispositivo estará disponible utilizando esta dirección de IP mientras el dispositivo tenga al menos una interfaz de red capaz de enviar y recibir tráfico de IP.

Una interfaz de loopback puede también servir para establecer una sesión de telnet desde el puerto de consola al puerto auxiliar cuando todas las interfaces caen. En aplicaciones donde otros routers deben acceder a las interfaces de loopback, debemos configurar un protocolo de enrutamiento para distribuír la subred asignada a las direcciones loopback.

Así pues si usamos cualquier enrutamiento dinámico debemos publicitar las ips de las interfaces de loopback (con network) para que todos los routers puedan acceder a los otros.

En OSPF el interfaz de loopback es muy importante pues sirve para poner el router-id, Si las interfaces físicas caen, OSPF cae, pero como loopback está siempre up, OSPF no caerá, además siempre tendrá la misma ID independientemente de si las interfaces están up o down.

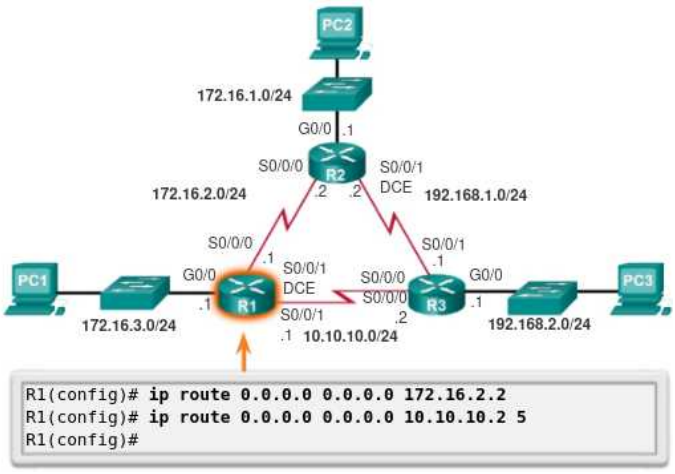
Rutas flotantes.

Las rutas estáticas flotantes son rutas estáticas que tienen una distancia administrativa mayor que la de otra ruta estática o la de rutas dinámicas. Son muy útiles para proporcionar un respaldo a un enlace principal, como se muestra en la ilustración.

De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 1, lo que las hace preferibles a las rutas descubiertas mediante protocolos de routing dinámico. Por ejemplo, las distancias administrativas de algunos protocolos de routing dinámico comunes son las siguientes:

EIGRP = 90
IGRP = 100
OSPF = 110
IS-IS = 115
RIP = 120

La distancia administrativa de una ruta estática se puede aumentar para hacer que la ruta sea menos deseable que la ruta de otra ruta estática o una ruta descubierta mediante un protocolo de routing dinámico. De esta manera, la ruta estática “flota” y no se utiliza cuando está activa la ruta con la mejor distancia administrativa. Sin embargo, si se pierde la ruta de preferencia, la ruta estática flotante puede tomar el control, y se puede enviar el tráfico a través de esta ruta alternativa.



Una ruta estática flotante se puede utilizar para proporcionar una ruta de respaldo a varias interfaces o redes en un router. También es independiente de la encapsulación, lo que significa que puede utilizarse para reenviar paquetes desde cualquier interfaz, sin importar el tipo de encapsulación.

Para configurar rutas estáticas IPv4, se utiliza el comando **ip route 0.0.0.0 0.0.0.0 ip_salto distancia**. Si no se configura ninguna distancia administrativa, se utiliza el valor predeterminado.

Es decir, ponemos varias rutas por defecto, aunque sólo estará activa la de distancia administrativa menor. En caso en que el enlace falle, se activará la flotante.