

CAPITULO 11

OSPF

11.0 Introducción del capítulo

Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia: RIP. RIP constituyó un protocolo de enrutamiento aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitan una solución de enrutamiento más sólida. OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. RFC 2328 define la métrica OSPF como un valor arbitrario llamado costo. El IOS de Cisco utiliza el ancho de banda como la métrica de costo de OSPF.

Las principales ventajas de OSPF frente a RIP son su rápida convergencia y escalabilidad a implementaciones de redes mucho mayores. En este capítulo final del curso de Conceptos y protocolos y de enrutamiento, aprenderá sobre implementaciones y configuraciones de OSPF básicas de área única. Las configuraciones y conceptos de OSPF más complejos se reservan para los cursos de nivel CCNP.

	Protocolos de gateway interiores				Protocolos de Gateway Exterior
	Protocolos de enrutamiento por vector de distancia		Protocolos de enrutamiento de estado de enlace		Vector de ruta
Con clase	RIP	IGRP			EGP
Sin clase	RIPv2	EIGRP	OSPFv2	IS-IS	BGPv4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGPv4 for IPv6

En este capítulo, aprenderá a:

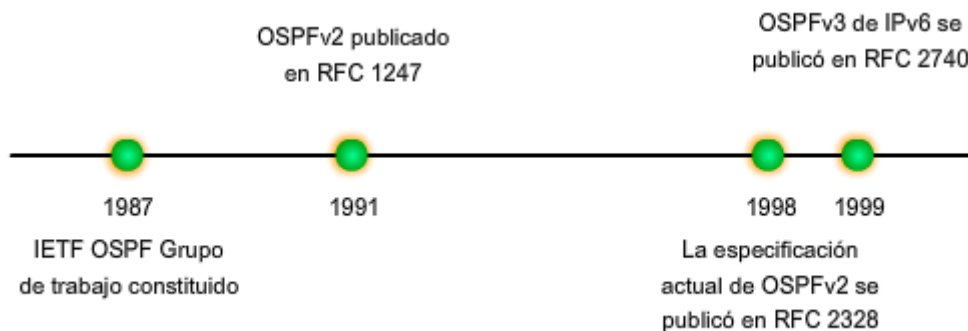
- Describir las características básicas y de fondo de OSPF.
- Identificar y aplicar los comandos básicos de configuración OSPF.
- Describir, modificar y calcular la métrica utilizada por OSPF.
- Describir el proceso de elección del router designado y del router designado de respaldo (DR/BDR) en las redes de acceso múltiple.
- Emplear el comando `default-information originate` para configurar y propagar una ruta por defecto en OSPF.

11.1 Introducción al OSPF

11.1.1 Información básica del OSPF

El desarrollo inicial de OSPF comenzó en 1987 por parte del grupo de trabajo de OSPF, el Grupo de trabajo de ingeniería de Internet (IETF). En aquel momento, Internet constituía fundamentalmente una red académica y de investigación financiada por el gobierno de los EE. UU.

Coloque el cursor sobre las fechas en la figura Cronograma de desarrollo de OSPF para ver los eventos relacionados.



En 1989, la especificación para OSPFv1 se publicó en RFC 1131. Había dos implementaciones desarrolladas: una para ejecutar en routers y otra para ejecutar en estaciones de trabajo UNIX. La última implementación se convirtió luego en un proceso UNIX generalizado y conocido como GATED. OSPFv1 fue un protocolo de enrutamiento experimental y nunca se implementó.

En 1991, John Moy introdujo OSPFv2 en RFC 1247. OSPFv2 ofrecía significativas mejoras técnicas con respecto a OSPFv1. Al mismo tiempo, ISO trabajaba en un protocolo de enrutamiento de estado de enlace propio, Intermediate System-to-Intermediate System (IS-IS). Lógicamente, IETF eligió OSPF como su IGP (Interior Gateway Protocol) recomendado.

En 1998, la especificación OSPFv2 se actualizó en RFC 2328 y representa la RFC actual para OSPF.

Nota: En 1999, OSPFv3 para IPv6 se publicó en RFC 2740. John Moy, Rob Coltun y Dennis Ferguson desarrollaron RFC 2740. OSPFv3 se analiza en CCNP.

Enlaces

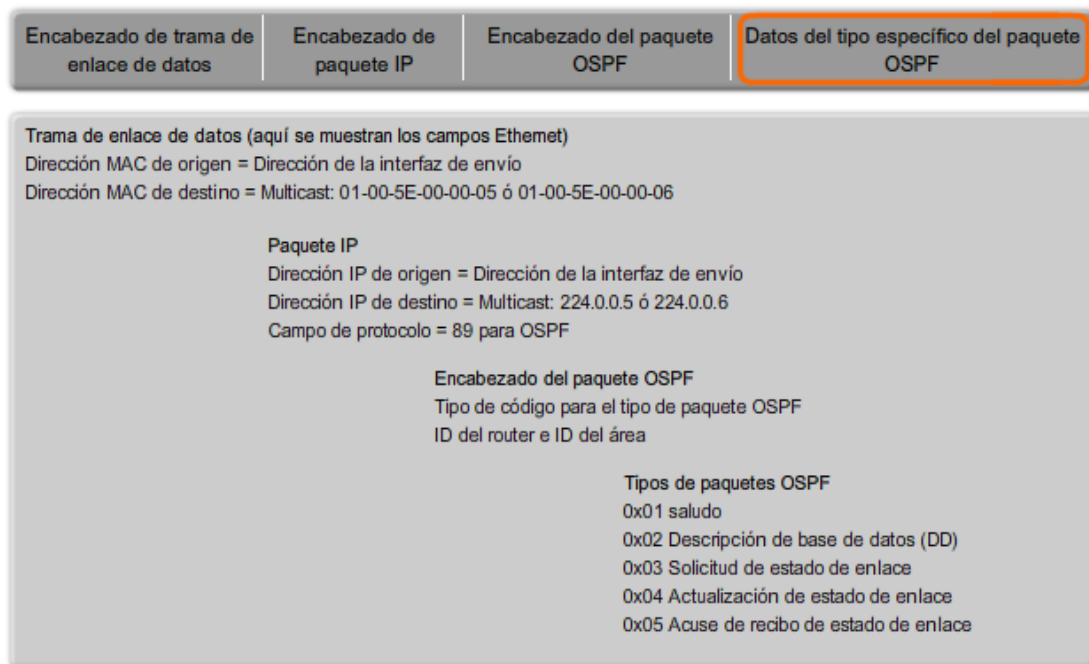
"OSPF Version 2," <http://www.ietf.org/rfc/rfc2328>

11.1.2 Encapsulación de mensajes OSPF

La porción de datos de un mensaje OSPF se encapsula en un paquete. Este campo de datos puede incluir uno de cinco tipos de paquetes OSPF. Cada tipo de paquete se analiza brevemente en el próximo tema.

Coloque el cursor sobre los campos en la figura Mensaje de OSPF encapsulado para ver el proceso de encapsulación.

Mensaje OSPF encapsulado



El encabezado del paquete OSPF se incluye con cada paquete OSPF, independientemente de su tipo. El encabezado del paquete OSPF y los datos específicos según el tipo de paquete específico se encapsulan luego en un paquete IP. En el encabezado del paquete IP, el campo Protocolo se establece en 89 para indicar el OSPF y la dirección de destino se establece para una de dos direcciones multicast: 224.0.0.5 ó 224.0.0.6. Si el paquete OSPF se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-05 ó 01-00-5E-00-00-06.

11.1.3 Tipos de paquetes OSPF

En el capítulo anterior, presentamos Paquetes de estado de enlace (LSP). La figura muestra los cinco tipos diferentes de LSP de OSPF. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

1. **Saludo:** los paquetes de saludo se utilizan para establecer y mantener la adyacencia con otros routers OSPF. El protocolo de saludo se analiza en detalle en el próximo tema.
2. **DBD:** el paquete de Descripción de bases de datos (DBD) incluye una lista abreviada de la base de datos de estado de enlace del router emisor y lo utilizan los routers receptores para comparar con la base de datos de estado de enlace local.
3. **LSR:** los routers receptores pueden luego solicitar más información acerca de una entrada en la DBD enviando una Solicitud de estado de enlace (LSR).
4. **LSU:** los paquetes de Actualización de estado de enlace (LSU) se utilizan para responder las LSR y para anunciar nueva información. Las LSU contienen siete tipos diferentes de Notificaciones de estado de enlace (LSA). Las LSU y LSA se analizan brevemente en un tema posterior.
5. **LSAck:** cuando se recibe una LSU, el router envía un Acuse de recibo de estado de enlace (LSAck) para confirmar la recepción de LSU.

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	Descripción de la base de datos (DBD)	Controla la sincronización de la base de datos entre routers
3	Solicitud de estado de enlace (LSR)	Solicita registros específicos de estado de enlace de router a router
4	Actualización de estado de enlace (LSU)	Envía los registros de estado de enlace específicamente solicitados
5	Acuse de recibo de estado de enlace (LSAck)	Reconoce los demás tipos de paquetes

11.1.4 Protocolo de saludo

La figura muestra el encabezado del paquete OSPF y el paquete de saludo. Los campos sombreados en color azul se analizarán en mayor detalle más adelante en el capítulo. Por el momento, nos enfocaremos en los usos del paquete de saludo.

El paquete OSPF Tipo 1 es el paquete de saludo OSPF. Los paquetes de saludo se utilizan para:

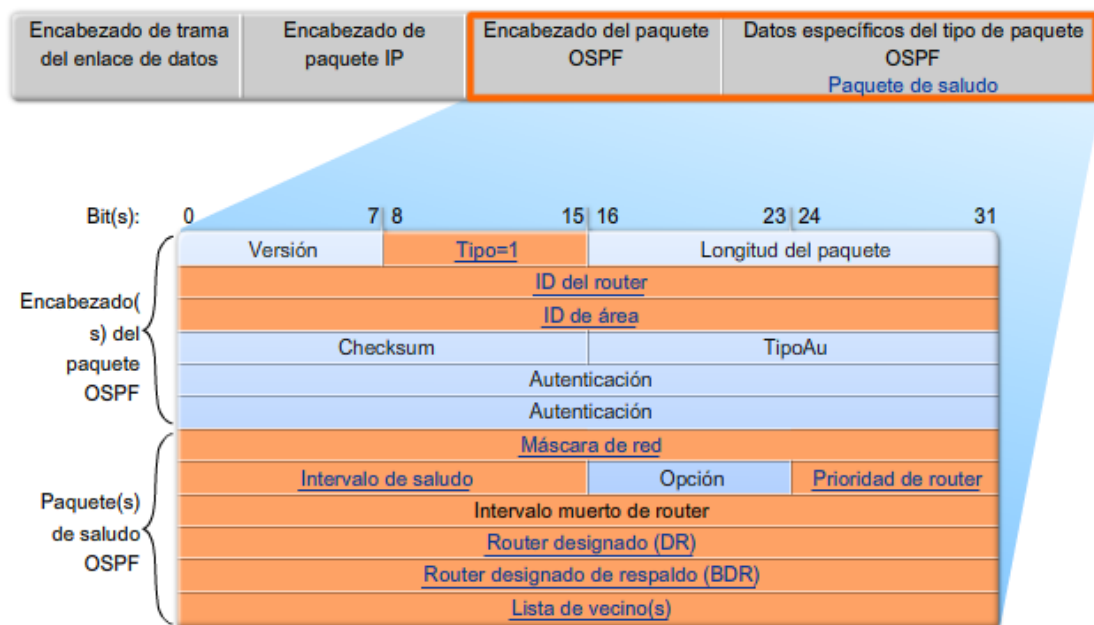
- Descubrir vecinos OSPF y establecer adyacencias de vecinos.
- Publicar parámetros en los que dos routers deben acordar convertirse en vecinos.
- Elegir el Router designado (DR) y el Router designado de respaldo (BDR) en redes de accesos múltiples, como Ethernet y Frame Relay.

Los campos importantes que se muestran en la figura incluyen:

Tipo: Tipo de paquete OSPF: Saludo (1), DD (2), Solicitud LS (3), Actualización LS (4), ACK LS (5)

- **ID del Router:** ID del router de origen
- **ID del área:** área en la que se originó el paquete
- **Máscara de red:** máscara de subred asociada con la interfaz emisora
- **Intervalo de saludo:** cantidad de segundos entre los paquetes de saludo del router emisor
- **Prioridad del router:** utilizado en la elección de DR/BDR (se analizará más adelante)
- **Router designado (DR):** ID del router del DR, si existe
- **Router designado de respaldo (BDR):** ID del router del BDR, si existe
- **Lista de vecinos:** enumera la ID del router OSPF de los routers vecinos

Formato de mensaje OSPF



Establecimiento de vecinos

Antes de que un router OSPF pueda saturar a otros routers con sus estados de enlace, primero debe determinar si existe algún otro vecino OSPF en alguno de sus enlaces. En la figura, los routers OSPF envían paquetes de saludo a todas las interfaces habilitadas con OSPF para determinar si hay vecinos en dichos enlaces. La información en el saludo de OSPF incluye la ID del router OSPF del router que envía el paquete de saludo (la ID del router se analiza más adelante en el capítulo). La recepción de un paquete de saludo OSPF en una interfaz confirma a un router la presencia de otro router OSPF en dicho enlace. OSPF luego establece la adyacencia con el vecino. Por ejemplo, en la figura, R1 establecerá adyacencias con R2 y R3.

Intervalos muerto y de saludo de OSPF

Antes de que dos routers puedan formar una adyacencia de vecinos OSPF, éstos deben estar de acuerdo con respecto a tres valores: Intervalo de saludo, intervalo muerto y tipo de red. El intervalo de saludo de OSPF indica la frecuencia con que un router OSPF transmite sus paquetes de saludo. De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos multiacceso y punto a punto, y cada 30 segundos en segmentos multiacceso sin broadcast (NBMA) (Frame Relay, X.25, ATM).

En la mayoría de los casos, los paquetes de saludo OSPF se envían como multicast a una dirección reservada para ALLSPFRouters en 224.0.0.5. La utilización de una dirección multicast permite a un dispositivo ignorar el paquete si la interfaz no está habilitada para aceptar paquetes OSPF. Esto ahorra tiempo de procesamiento de CPU en los dispositivos que no son OSPF.

El intervalo muerto es el período, expresado en segundos, que el router esperará para recibir un paquete de saludo antes de declarar al vecino "desactivado". Cisco utiliza en forma predeterminada cuatro veces el intervalo de Hello. En el caso de los segmentos multiacceso y punto a punto, dicho período es de 40 segundos. En el caso de las redes NBMA, el intervalo muerto es de 120 segundos.

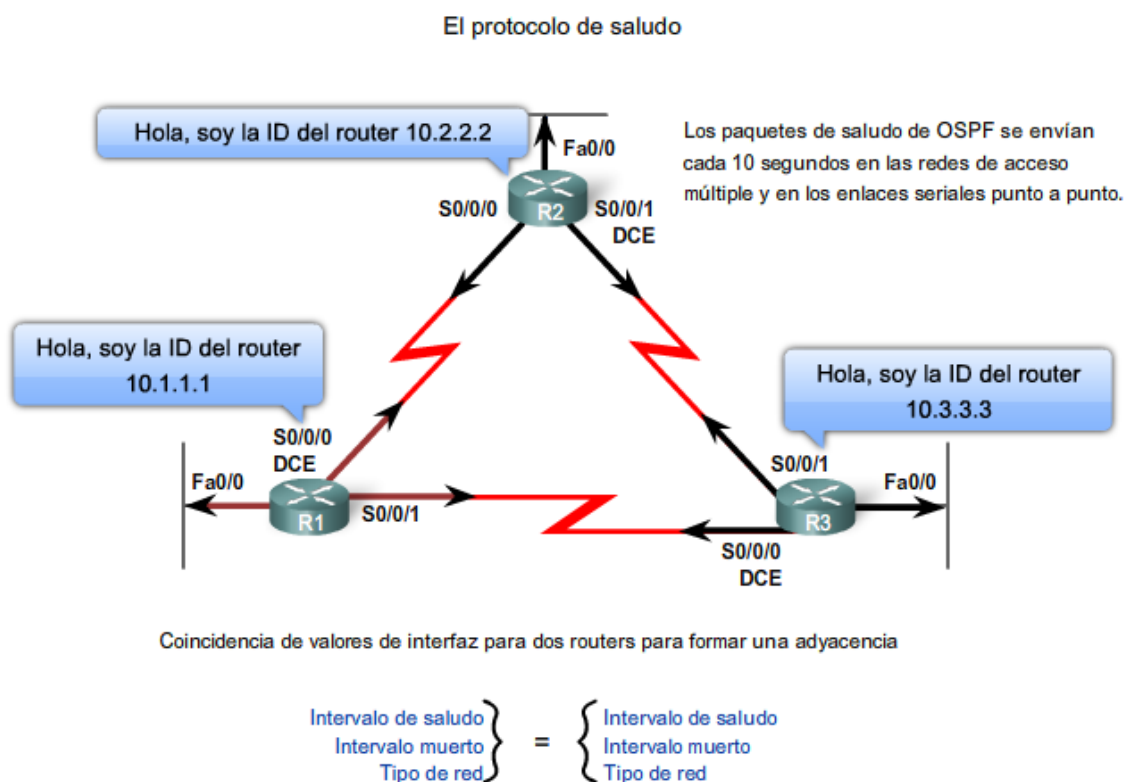
Si el intervalo muerto expira antes de que los routers reciban un paquete de saludo, OSPF retirará a dicho vecino de su base de datos de estado de enlace. El router satura con la información de estado de enlace acerca del vecino "desactivado" desde todas las interfaces habilitadas con OSPF.

Los tipos de redes se analizan más adelante en el capítulo.

Selección de DR y BDR

Para reducir la cantidad de tráfico de OSPF en redes de accesos múltiples, OSPF selecciona un Router designado (DR) y un Router designado de respaldo (BDR). El DR es responsable de actualizar todos los demás routers OSPF (llamados DROthers) cuando ocurre un cambio en la red de accesos múltiples. El BDR supervisa al DR y reemplaza a DR si el DR actual falla.

En la figura, R1, R2 y R3 están conectados a través de enlaces punto a punto. Por lo tanto, no ocurre la elección de DR/BDR. La selección y los procesos de DR/BDR se analizarán en un tema posterior y se cambiará la topología por una red de accesos múltiples.



Nota: El paquete de saludo se analiza en mayor detalle en CCNP junto con los otros tipos de paquetes OSPF.

11.1.5 Actualizaciones de estado de enlace de OSPF

Las actualizaciones de estado de enlace (LSU) son los paquetes utilizados para las actualizaciones de enrutamiento OSPF. Un paquete LSU puede incluir diez tipos diferentes de Notificaciones de estado de enlace (LSA), como se muestra en la figura. La diferencia entre los términos Actualización de estado de enlace (LSU) y Notificación de estado de enlace (LSA) en ocasiones puede ser confusa. A veces, dichos términos pueden utilizarse indistintamente. Una LSU incluye una o varias LSA y cualquiera de los dos términos puede usarse para hacer referencia a la información de estado de enlace propagada por los routers OSPF.

Las LSU contienen notificaciones de estado de enlace (LSA)

Tipo	Nombre del paquete	Descripción
1	Saludo	Descubre los vecinos y construye adyacencias entre ellos
2	DBD	Controla la sincronización de la base de datos entre routers
3	LSR	Solicita registros específicos de estado de enlace de router a router
4	LSU	Envía los registros de estado de enlace específicamente solicitados
5	LSAck	Reconoce los demás tipos de paquetes



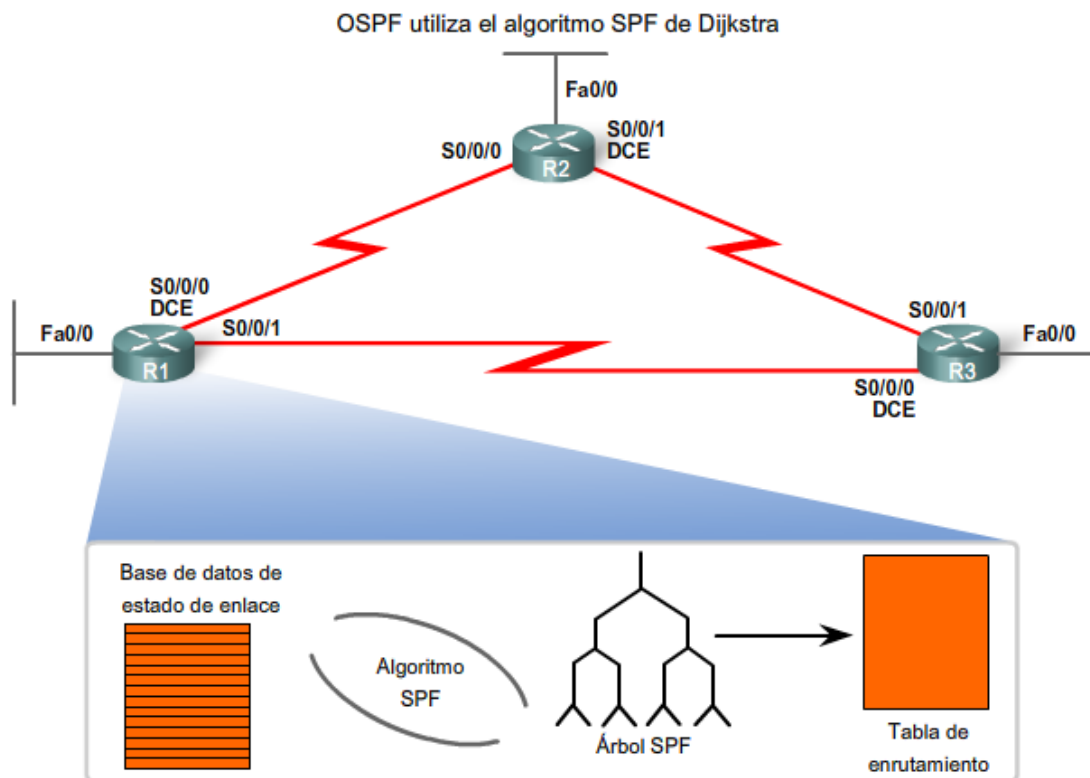
- Las siglas LSA y LSU con frecuencia se utilizan indistintamente.
- Una LSU contiene una o más LSA.
- Las LSA contienen información de ruta para las redes de destino.
- La información específica de LSA se analiza en CCNP.

Tipo de LSA	Descripción
1	LSA de router
2	LSA de red
3 ó 4	LSA de resumen
5	LSA externos del sistema autónomo
6	LSA de OSPF multicast
7	Definido para áreas no tan llenas
8	Atributos externos de LSA para Border Gateway Protocol (BGP)
9, 10, 11	LSA opacas

Nota: Los diferentes tipos de LSA se analizan en CCNP.

11.1.6 Algoritmo OSPF

Cada router OSPF mantiene una base de datos de estado de enlace que contiene las LSA recibidas por parte de todos los demás routers. Una vez que un router recibió todas las LAS y creó su base de datos de estado de enlace local, OSPF utiliza el algoritmo shortest path first (SPF) de Dijkstra para crear un árbol SPF. El árbol SPF luego se utiliza para completar la tabla de enrutamiento IP con las mejores rutas para cada red.



11.1.7 Distancia administrativa

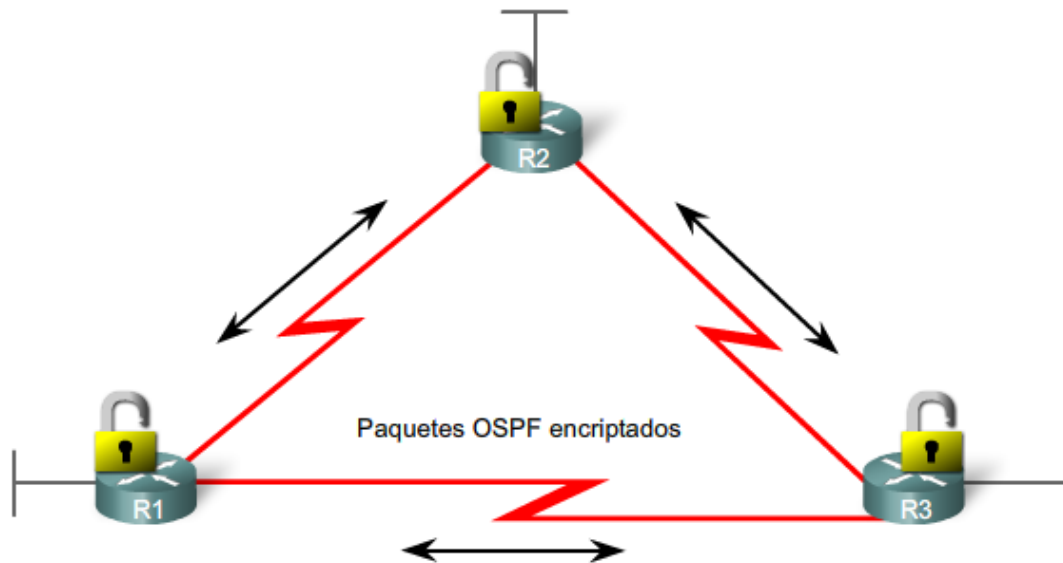
Como se vio en el Capítulo 3, "Introducción al enrutamiento dinámico", la distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110. Como puede ver en la figura, al compararlo con otros protocolos de gateway interiores (IGP), se prefiere a OSPF con respecto a IS-IS y RIP.

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

11.1.8 Autenticación

Como se mencionó en capítulos anteriores, la configuración de protocolos de enrutamiento para utilizar la autenticación se analizará en un curso posterior. Al igual que otros protocolos de enrutamiento, OSPF puede configurarse para autenticación.

Es aconsejable autenticar la información de enrutamiento transmitida. RIPv2, EIGRP, OSPF, IS-IS y BGP pueden configurarse para encriptar y autenticar su información de enrutamiento. Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación.

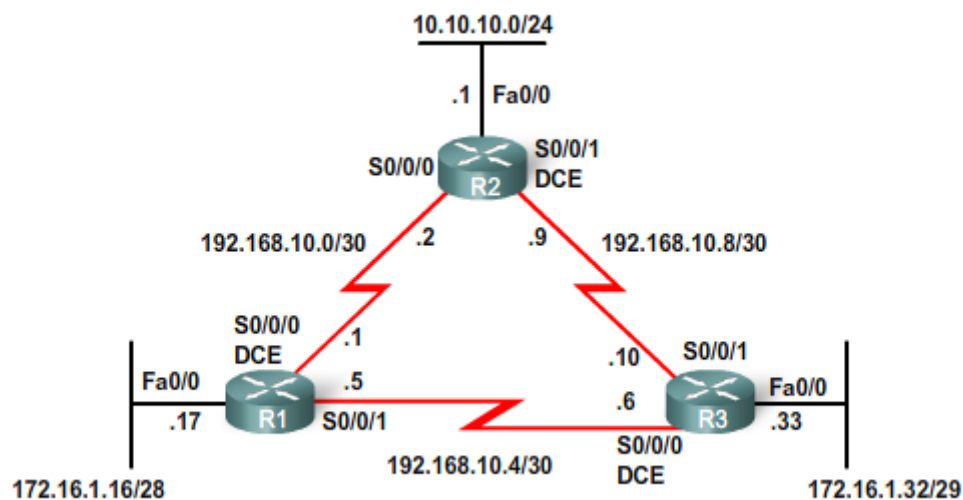


Nota: La autenticación no encripta la tabla de enrutamiento del router.

11.2 Configuración OSPF básica

11.2.1 Topología de laboratorio

La figura muestra la topología para este capítulo. Observe que el esquema de direccionamiento no es contiguo. OSPF es un protocolo de enrutamiento sin clase. Por lo tanto, configuraremos la máscara como parte de nuestra configuración OSPF. Como sabe, al hacerlo se solucionará el problema del direccionamiento no contiguo. También observe que en esta topología hay tres enlaces seriales de varios anchos de banda y cada router tiene múltiples rutas para cada red remota.



Haga clic en Direcccionamiento para revisar las direcciones IP.

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	Fa0/0	172.16.1.17	255.255.255.240
	S0/0/0	192.168.10.1	255.255.255.252
	S0/0/1	192.168.10.5	255.255.255.252
R2	Fa0/0	10.10.10.1	255.255.255.0
	S0/0/0	192.168.10.2	255.255.255.252
	S0/0/1	192.168.10.9	255.255.255.252
R3	Fa0/0	172.16.1.33	255.255.255.248
	S0/0/0	192.168.10.6	255.255.255.252
	S0/0/1	192.168.10.10	255.255.255.252

Haga clic en R1, R2 y R3 para revisar la configuración de inicio de cada router.

```
R1#show startup-config

Current configuration : 1344 bytes
!
<some output omitted>
!
hostname R1
!
!
!
interface FastEthernet0/0
  description R1 LAN
  ip address 172.16.1.17 255.255.255.240
!
interface Serial0/0/0
  description Link to R2
  ip address 192.168.10.1 255.255.255.252
  clock rate 64000
!
interface Serial0/0/1
  description Link to R3
  ip address 192.168.10.5 255.255.255.252
!
end
```

Direcccionamiento

R1

R2

R3

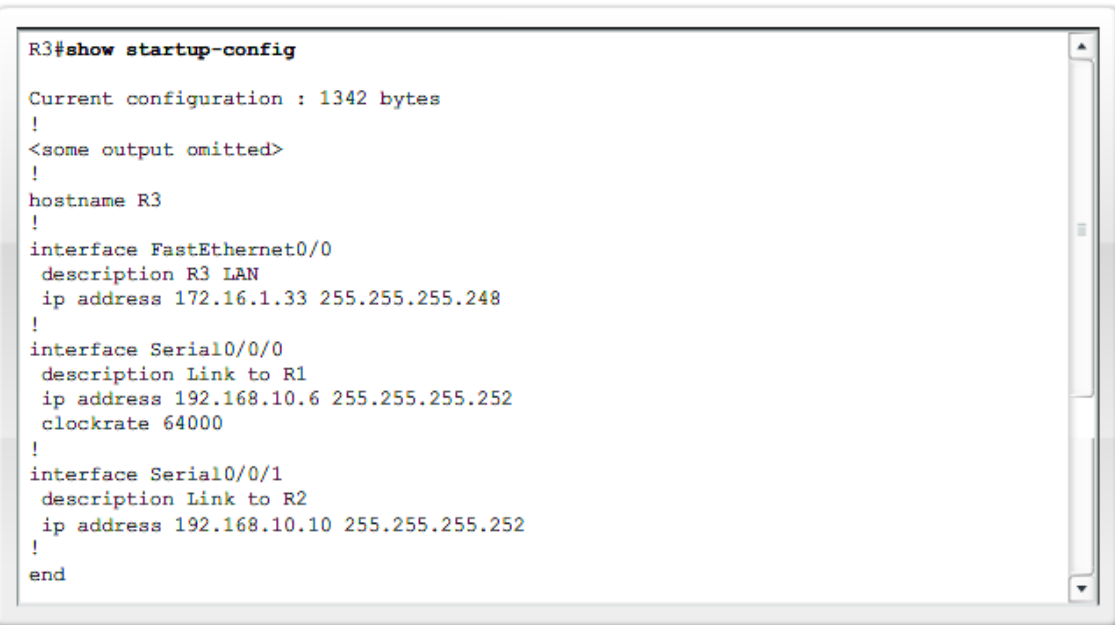


R2#show startup-config

```
Current configuration : 1343 bytes
!
<some output omitted>
!
hostname R2
!
!
!
interface FastEthernet0/0
  description R2 LAN
  ip address 10.10.10.1 255.255.255.0
!
interface Serial0/0/0
  description Link to R1
  ip address 192.168.10.2 255.255.255.252
!
interface Serial0/0/1
  description Link to R3
  ip address 192.168.10.9 255.255.255.252
  clock rate 64000
!
end
```

Direccionamiento R1 R2 R3

Haga clic para ver las configuraciones iniciales del router.



R3#show startup-config

```
Current configuration : 1342 bytes
!
<some output omitted>
!
hostname R3
!
!
!
interface FastEthernet0/0
  description R3 LAN
  ip address 172.16.1.33 255.255.255.248
!
interface Serial0/0/0
  description Link to R1
  ip address 192.168.10.6 255.255.255.252
  clockrate 64000
!
interface Serial0/0/1
  description Link to R2
  ip address 192.168.10.10 255.255.255.252
!
end
```

Direccionamiento R1 R2 R3

Haga clic para ver las configuraciones iniciales del router.

11.2.2 Configuración router OSPF

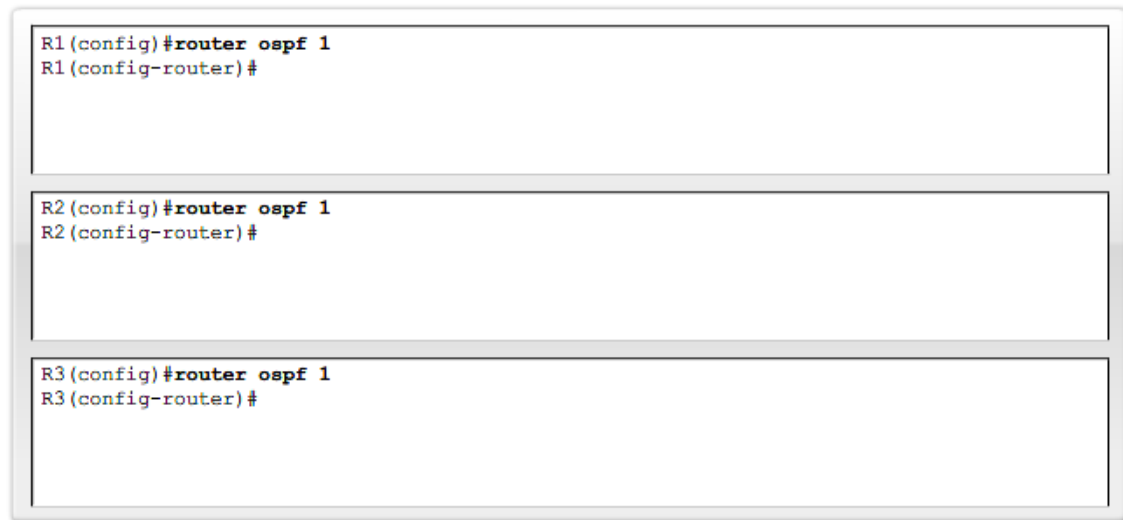
OSPF se habilita con el comando de configuración global `router ospf process-id`. El comando `process-id` es un número entre 1 y 65535 elegido por el administrador de red. El comando `process-id` es significativo a nivel local, lo que implica que no necesita coincidir con otros routers OSPF para establecer adyacencias con dichos vecinos. Esto difiere de EIGRP. La

ID del proceso EIGRP o el número de sistema autónomo *sí* necesita coincidir con dos vecinos EIGRP para volverse adyacente.

En nuestra topología, habilitaremos OSPF en los tres routers que utilizan la misma ID de proceso de 1. Utilizamos la misma ID de proceso simplemente por cuestiones de uniformidad.

```
R1(config)#router ospf 1
```

```
R1(config-router)#
```



```
R1(config)#router ospf 1
R1(config-router)#

R2(config)#router ospf 1
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#
```

11.2.3 Comando network

El comando network utilizado con OSPF tiene la misma función que cuando se utiliza con otros protocolos de enrutamiento IGP:

- Cualquier interfaz en un router que coincida con la dirección de red en el comando network estará habilitada para enviar y recibir paquetes OSPF.
- Esta red (o subred) estará incluida en las actualizaciones de enrutamiento OSPF.

El comando network se utiliza en el modo de configuración de router.

```
Router(config-router)#network network-address wildcard-mask area area-id
```

El comando network de OSPF utiliza una combinación de *network-address* y *wildcard-mask* similar a la que puede utilizar EIGRP. Sin embargo, a diferencia de EIGRP, OSPF requiere la máscara wildcard. La dirección de red junto con la máscara wildcard se utiliza para especificar la interfaz o rango de interfaces que se habilitarán para OSPF con el comando network.

Al igual que con EIGRP, la máscara wildcard puede configurarse en forma inversa a una máscara de subred. Por ejemplo, la interfaz FastEthernet 0/0 de R1 se encuentra en la red 172.16.1.16/28. La máscara de subred para esta interfaz es /28 ó 255.255.255.240. Lo inverso a la máscara de subred es la máscara wildcard.

Nota: Al igual que EIGRP, algunas versiones de IOS simplemente le permiten ingresar la máscara de subred en lugar de la máscara wildcard. Luego, IOS convierte la máscara de subred al formato de la máscara wildcard.

255.255.255.255

- 255.255.255.240 Reste la máscara de subred

0. 0. 0. 15 Máscara wildcard

El área *area-id* hace referencia al área OSPF. Un área OSPF es un grupo de routers que comparte la información de estado de enlace. Todos los routers OSPF en la misma área deben tener la misma información de estado de enlace en sus bases de datos de estado de enlace. Esto se logra a través de la saturación por parte de los routers de todos los demás routers en el área con sus estados de enlace individuales. En este capítulo, configuraremos todos los routers OSPF dentro de un área única. Esto se conoce como OSPF de área única.

Una red OSPF también puede configurarse como áreas múltiples. Existen varias ventajas en la configuración de redes OSPF amplias como áreas múltiples, incluidas las bases de datos de estado de enlace más pequeñas y la capacidad de aislar problemas de redes inestables dentro de un área. El OSPF de áreas múltiples se desarrolla en CCNP.

Cuando todos los routers se encuentran dentro de la misma área OSPF, deben configurarse los comandos *network* con la misma *area-id* en todos los routers. Si bien puede usarse cualquier *area-id*, es aconsejable utilizar un *area-id* de 0 con OSPF de área única. Esta convención facilita la posterior configuración de la red como áreas OSPF múltiples en las que el área 0 se convierte en el área de backbone.

La figura muestra los comandos *network* para los tres routers y habilita OSPF en todas las interfaces. En este punto, todos los routers deben poder hacer ping en todas las redes.

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0
```

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
```

11.2.4 ID del router OSPF

Determinación de la ID del router

La ID del router OSPF se utiliza para identificar en forma exclusiva cada router en el dominio de enrutamiento OSPF. La ID de un router es simplemente una dirección IP. Los routers de Cisco obtienen la ID del router conforme a tres criterios y con la siguiente prioridad:

1. Utilizar la dirección IP configurada con el comando router-id de OSPF.
2. Si router-id no está configurado, el router elige la dirección IP más alta de cualquiera de sus interfaces loopback.
3. Si no hay ninguna interfaz loopback configurada, el router elige la dirección IP activa más alta de cualquiera de sus interfaces físicas.

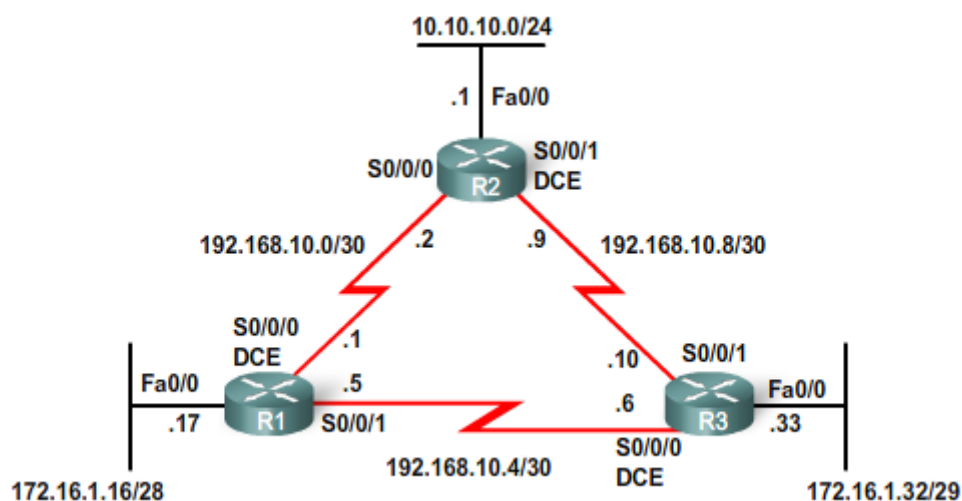
Dirección IP activa más alta

Si un router OSPF se configura con el comando router-id de OSPF y no hay interfaces loopback configuradas, la ID del router OSPF será la dirección IP activa más alta de cualquiera de sus interfaces. La interfaz no necesita estar habilitada para OSPF, lo que significa que no necesita estar incluida en uno de los comandos network de OSPF. Sin embargo, la interfaz debe estar activa, debe encontrarse en estado up.

La ID del router se determina en el siguiente orden:

1. Utilice la dirección IP configurada con el comando router-id de OSPF.
2. Si la id el router no está configurada, el router elige direcciones IP más altas de cualquiera de sus interfaces loopback.
3. Si no está configurada ninguna interfaz loopback, el router elige la dirección IP activa más alta de alguna de sus interfaces físicas.

Haga clic en el botón Topología en la figura.



Con los criterios descritos anteriormente, ¿puede determinar las ID del router para R1, R2 y R3? La respuesta se encuentra en la próxima página.

Verificación de la ID del router

Debido a que no hemos configurado las ID del router ni las interfaces loopback en nuestros tres routers, la ID del router para cada router está determinada por el tercer criterio de la lista: la dirección IP activa más alta en cualquiera de las interfaces físicas del router. Como se muestra en la figura, la ID del router para cada router es:

R1: 192.168.10.5, que es mayor que 172.16.1.17 ó 192.168.10.1

R2: 192.168.10.9, que es mayor que 10.10.10.1 ó 192.168.10.2

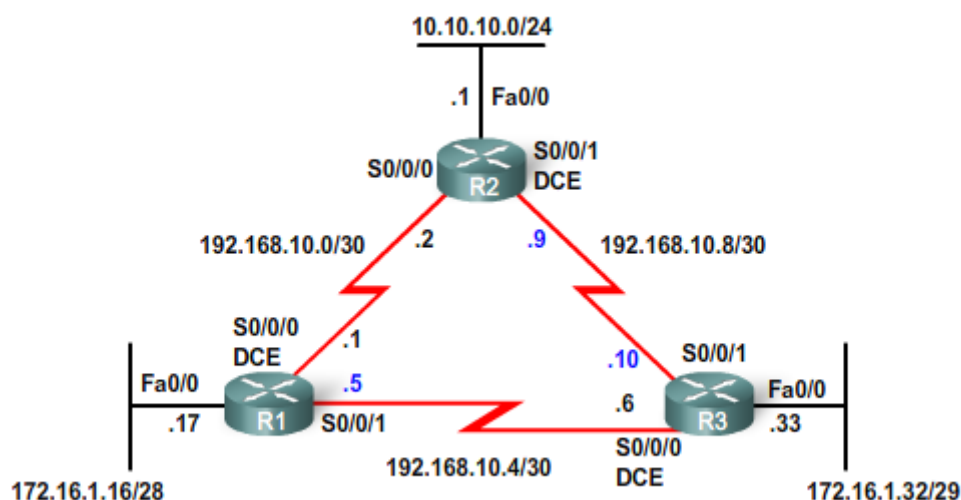
R3: 192.168.10.10, que es mayor que 172.16.1.33 ó 192.168.10.6

Un comando que puede utilizar para verificar la ID del router actual es `show ip protocols`. Algunas versiones de IOS no muestran la ID del router como se muestra en la figura. En dichos casos, utilice los comandos `show ip ospf` o `show ip ospf interface` para verificar la ID del router.

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.9
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

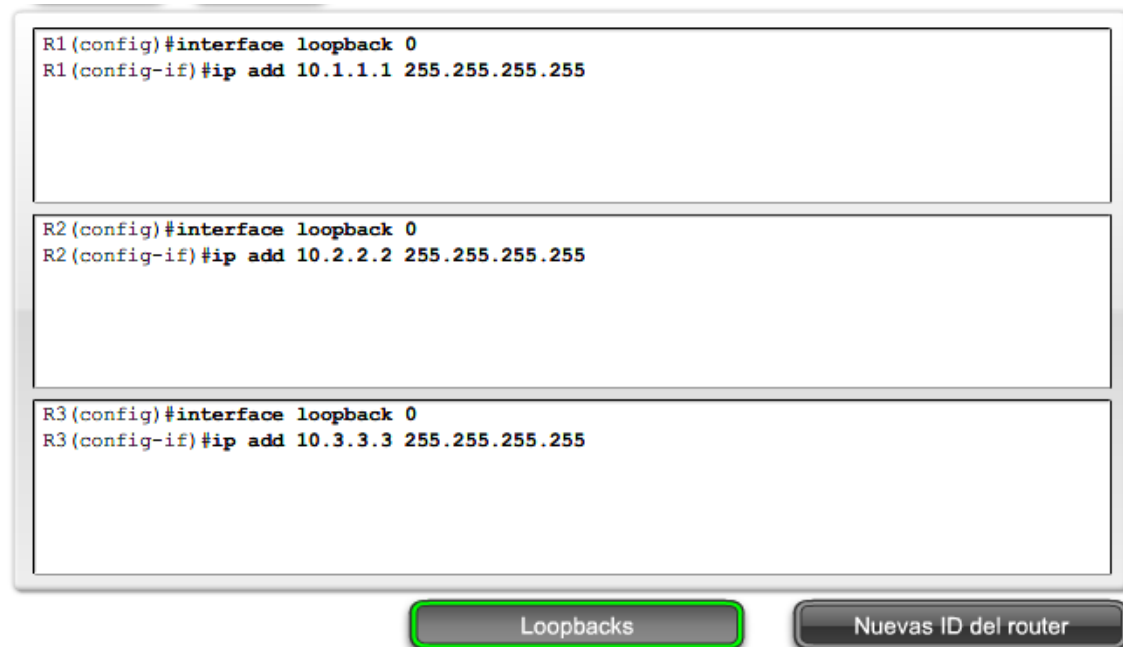


Dirección de loopback

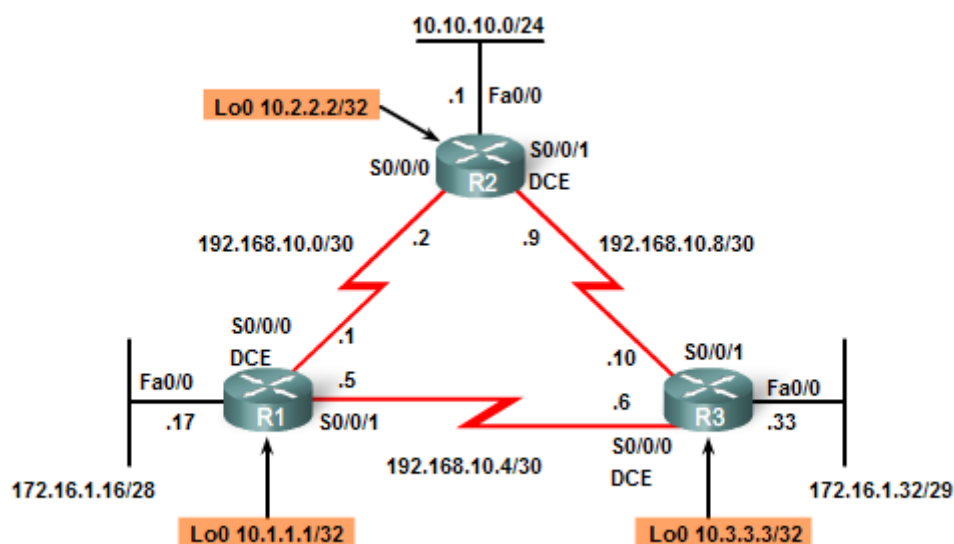
Si no se utilizó el comando `router-id` de OSPF y están configuradas las interfaces loopback, OSPF elegirá la dirección IP más alta de cualquiera de sus interfaces loopback. Una dirección de loopback es una interfaz virtual y se encuentra en estado up en forma automática cuando está configurada. El usuario ya conoce los comandos para configurar una interfaz loopback:

```
Router(config)#interface Loopback number
```

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



Haga clic en el botón Topología en la figura.



En esta topología, los tres routers se configuraron con direcciones de loopback para representar las ID del router OSPF. La ventaja de utilizar una interfaz loopback es que, a

diferencia de las interfaces físicas, ésta no puede fallar. No hay cables ni dispositivos adyacentes reales de los que dependa la interfaz loopback para encontrarse en estado up. Por lo tanto, la utilización de una dirección de loopback para la ID del router ofrece estabilidad al proceso OSPF. Debido a que el comando router-id de OSPF que se analiza a continuación, se agregó recientemente a IOS, es más común encontrar direcciones de loopback utilizadas para configurar las ID del router OSPF.

Comando router-id de OSPF

El comando router-id de OSPF se introdujo en IOS 12.0(T) y tiene prioridad sobre direcciones IP físicas y de loopback en la determinación de la ID del router. La sintaxis de comando es:

```
Router(config)#router ospf process-id
```

```
Router(config-router)#router-id ip-address
```

Modificación de la ID del router

La ID del router se selecciona cuando se configura OSPF con su primer comando network de OSPF. Si el comando router-id de OSPF o la dirección de loopback se configuran después del comando network de OSPF, la ID del router se obtendrá de la interfaz con la dirección IP activa más alta.

La ID del router puede modificarse con la dirección IP de un comando router-id de OSPF subsiguiente, volviendo a cargar el router o utilizando el siguiente comando:

```
Router#clear ip ospf process
```

Nota: La modificación de la ID de un router con una nueva dirección IP física o de loopback puede requerir la recarga del router.

ID duplicadas del router

Cuando dos routers tienen la misma ID de router en un OSPF, es posible que el enrutamiento de dominio no funcione correctamente. Si la ID del router es la misma en dos routers vecinos, es posible que no se realice el establecimiento de vecinos. Cuando se producen ID duplicadas del router OSPF, IOS mostrará un mensaje similar al siguiente:

```
%OSPF-4-DUP_RTRID1: Detección de router con ID duplicadas
```

Para corregir este problema, configure todos los routers para que tengan una ID del router OSPF única.

Haga clic en Nuevas ID del router en la figura.

```

R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>

R2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>

R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>

```

Debido a que algunas versiones de IOS no admiten el comando router-id, utilizaremos el método de dirección de loopback para asignar las ID del router. Una dirección IP de una interfaz loopback por lo general sólo reemplazará a una ID del router OSPF actual mediante la recarga del router. En la figura, se recargaron los routers. El comando show ip protocols se utiliza para verificar que cada router esté utilizando la dirección de loopback para cada ID del router.

11.2.5 Verificación de OSPF

El comando show ip ospf neighbor puede utilizarse para verificar las relaciones de vecinos OSPF y solucionar sus problemas. Este comando muestra el siguiente resultado para cada vecino:

- ID de vecino: la ID del router vecino.
- Pri: la prioridad OSPF de la interfaz. Esto se analiza en una sección posterior.
- Estado: el estado OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen bases de datos de estado de enlace de OSPF idénticas. Los estados OSPF se analizan en CCNP.
- Tiempo muerto: la cantidad de tiempo restante que el router esperará para recibir un paquete de saludo OSPF por parte del vecino antes de declararlo desactivado. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
- Dirección: la dirección IP de la interfaz del vecino a la que está conectada directamente el router.
- Interfaz: la interfaz donde este router formó adyacencia con el vecino.

Al resolver problemas de redes OSPF, el comando show ip ospf neighbor puede utilizarse para verificar que el router formó adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o si no muestra el estado **FULL**, los dos routers no formaron una adyacencia OSPF. Si dos routers no establecieron adyacencia, no se intercambiará la información de estado de enlace. Las bases de datos de estado de enlace incompletas pueden crear árboles SPF y tablas de enrutamiento imprecisos. Es posible que no existan rutas a las redes de destino o que no representen la ruta más óptima.

Nota: En el caso de redes de accesos múltiples, como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. Esto se analizará en una sección posterior.

Es posible que dos routers no formen adyacencia OSPF si:

- Las máscaras de subred no coinciden, esto hace que los routers se encuentren en redes separadas.
- Los temporizadores muerto y de saludo de OSPF no coinciden.
- Los tipos de redes OSPF no coinciden.
- Hay un comando network de OSPF faltante o incorrecto.

del router  Verificación de adyacencia vecina

R1#show ip ospf neighbor

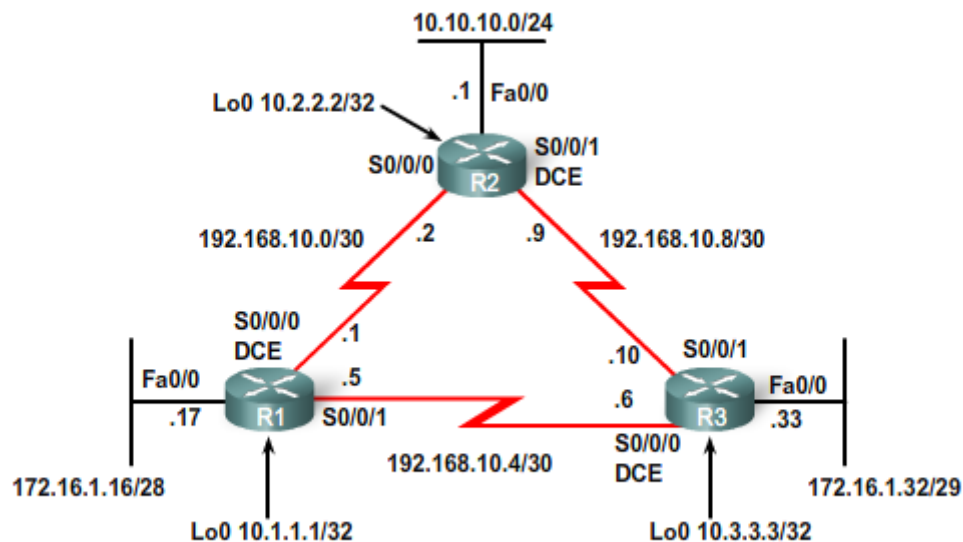
Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	1	FULL/ -	00:00:30	192.168.10.6	Serial0/0/1
10.2.2.2	1	FULL/ -	00:00:33	192.168.10.2	Serial0/0/0

R2#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	1	FULL/ -	00:00:36	192.168.10.10	Serial0/0/1
10.1.1.1	1	FULL/ -	00:00:37	192.168.10.1	Serial0/0/0

R3#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.2.2.2	1	FULL/ -	00:00:34	192.168.10.9	Serial0/0/1
10.1.1.1	1	FULL/ -	00:00:38	192.168.10.5	Serial0/0/0



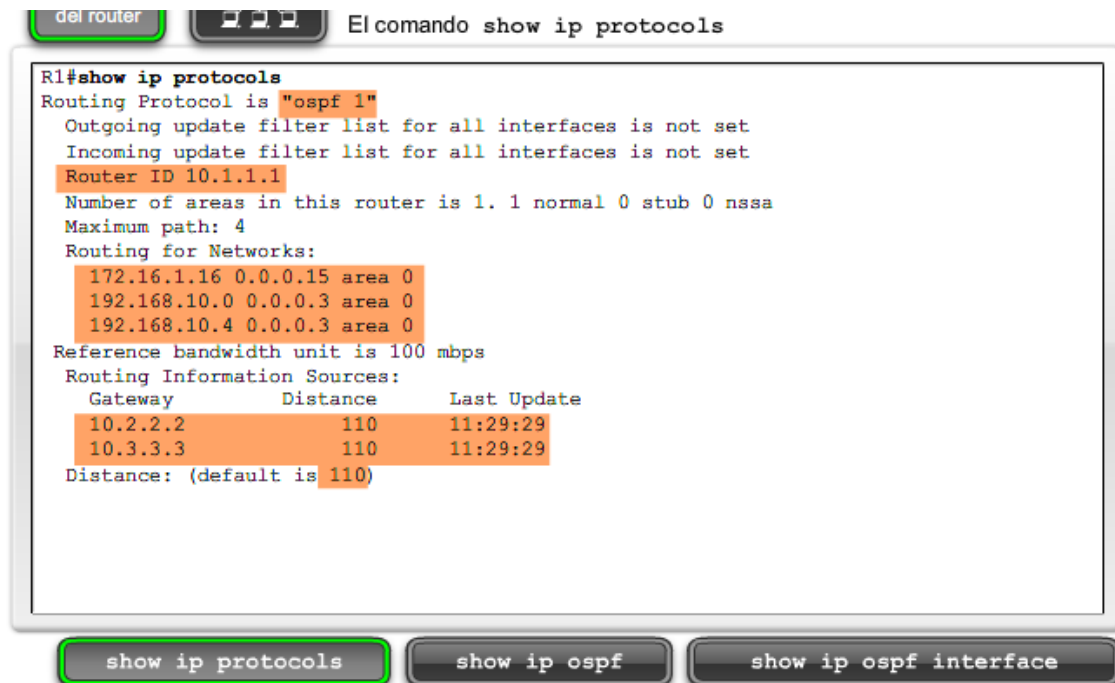
Otros poderosos comandos de resolución de problemas de OSPF incluyen:

show ip protocols

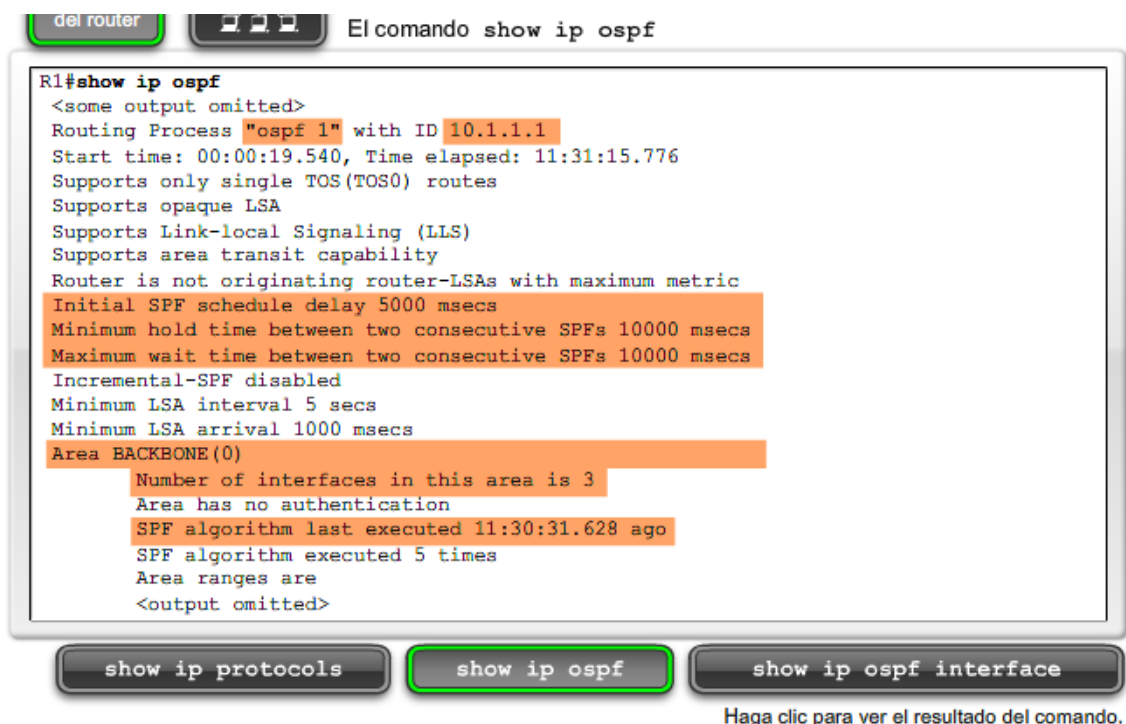
show ip ospf

show ip ospf interface

Como se muestra en la figura, el comando show ip protocols representa una manera rápida de verificar información de configuración vital de OSPF, incluida la ID del proceso OSPF, la ID del router, las redes que el router publica, los vecinos de quienes el router recibe actualizaciones y la distancia administrativa predeterminada, que es de 110 para OSPF.



Haga clic en show ip ospf en la figura.



El comando `show ip ospf` también puede utilizarse para examinar la ID del proceso OSPF y la ID del router. Asimismo, este comando muestra la información del área OSPF, así como la última vez que se calculó el algoritmo SPF. Como puede ver en el resultado de ejemplo, OSPF es un protocolo de enrutamiento muy estable. El único evento relacionado con OSPF en el que tuvo participación R1 durante las últimas 11 horas y media es el envío de paquetes de saludo a sus vecinos.

Nota: La información adicional que muestra el comando `show ip ospf` se analiza en los cursos CCNP.

El resultado del comando incluye información importante del algoritmo SPF que incluye el retraso en el programa SPF:

El retraso en el programa SPF inicial es de 5000 milisegundos

El tiempo en espera mínimo entre dos SPF consecutivos es de 10 000 milisegundos

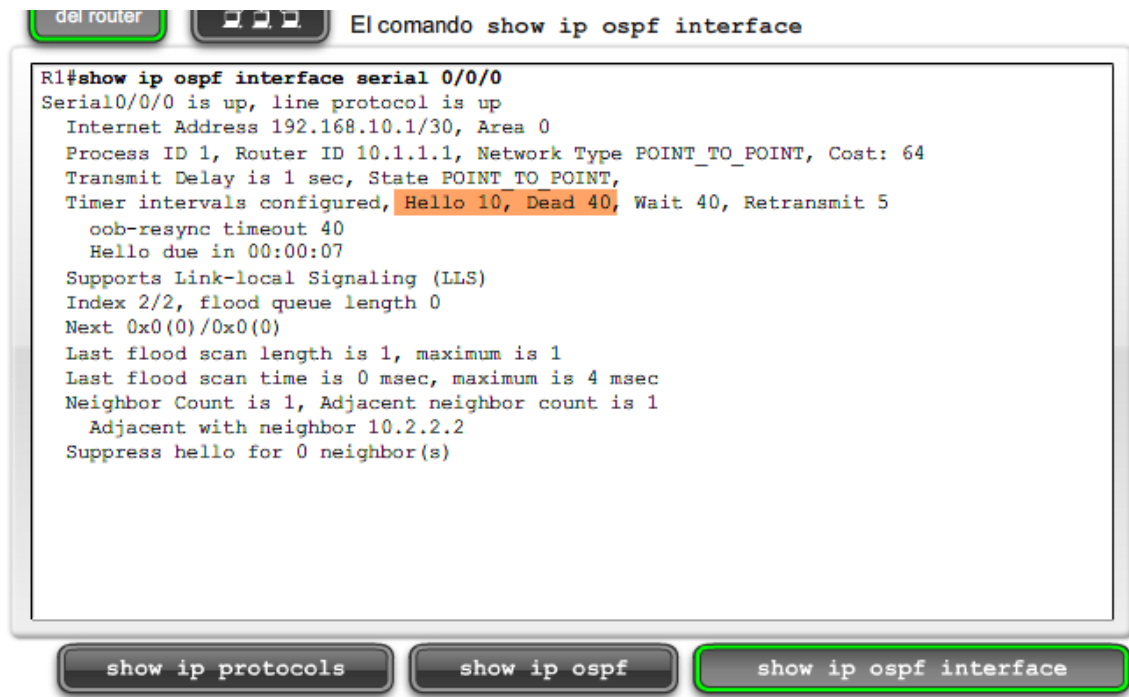
El tiempo de espera máximo entre dos SPF consecutivos es de 10 000 milisegundos

Cada vez que un router recibe nueva información acerca de la topología (adición, eliminación o modificación de un enlace), el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar la tabla de enrutamiento. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cálculos depende del tamaño del área. El tamaño de un área se mide por la cantidad de routers y el tamaño de la base de datos de estado de enlace.

A una red que alterna entre un estado up y down se la denomina enlace inestable. Un enlace inestable puede provocar que los routers OSPF de un área vuelvan a calcular constantemente el algoritmo SPF, lo que evita la convergencia adecuada. Para minimizar este problema, el router espera 5 segundos (5000 milisegundos) después de recibir una LSU antes de ejecutar el algoritmo SPF. Esto se conoce como retraso en el programa SPF. Para evitar que un router

ejecute el algoritmo SPF constantemente, existe un tiempo en espera adicional de 10 segundos (10000 milisegundos). El router espera 10 segundos después de ejecutar el algoritmo SPF antes de volver a ejecutarlo nuevamente.

Haga clic en `show ip ospf interface` en la figura.



La forma más rápida de verificar los intervalos muerto y de saludo es utilizar el comando `show ip ospf interface`. Como se muestra en la figura, al agregar el nombre y el número de la interfaz al comando aparece el resultado para una interfaz específica. Dichos intervalos se incluyen en los paquetes de saludo OSPF enviados entre vecinos. OSPF puede tener diferentes intervalos muerto y de saludo en varias interfaces; sin embargo, para que los routers OSPF se conviertan en vecinos, sus intervalos muertos y de saludo de OSPF deben ser idénticos. Por ejemplo, en la figura, R1 utiliza un intervalo de saludo de 10 y un intervalo muerto de 40 en la interfaz Serial 0/0/0. R2 también debe usar los mismos intervalos en su interfaz Serial 0/0/0; de lo contrario, los dos routers no formarán una adyacencia.

11.2.6 Examen de la tabla de enrutamiento

Como sabe, la manera más rápida de verificar la convergencia de OSPF es observar la tabla de enrutamiento para cada router en la topología.

Haga clic en R1, R2 y R3 en la figura para ver el resultado de `show ip route`.

R1#show ip route

Codes: <some code output omitted>

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

192.168.10.0/30 is subnetted, 3 subnets

C 192.168.10.0 is directly connected, Serial0/0/0

C 192.168.10.4 is directly connected, Serial0/0/1

O 192.168.10.8 [110/128] via 192.168.10.2, 14:27:57, Serial0/0/0

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

O 172.16.1.32/29 [110/65] via 192.168.10.6, 14:27:57, Serial0/0/1

C 172.16.1.16/28 is directly connected, FastEthernet0/0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

O 10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:57, Serial0/0/0

C 10.1.1.1/32 is directly connected, Loopback0

R1

R2

R3

R2#show ip route

Codes: <some code output omitted>

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

192.168.10.0/30 is subnetted, 3 subnets

C 192.168.10.0 is directly connected, Serial0/0/0

O 192.168.10.4 [110/128] via 192.168.10.1, 14:31:18, Serial0/0/0

C 192.168.10.8 is directly connected, Serial0/0/1

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

O 172.16.1.32/29 [110/65] via 192.168.10.10, 14:31:18, Serial0/0/1

O 172.16.1.16/28 [110/65] via 192.168.10.1, 14:31:18, Serial0/0/0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.2.2.2/32 is directly connected, Loopback0

C 10.10.10.0/24 is directly connected, FastEthernet0/0

R1

R2

R3

```
R3#show ip route
```

```
Codes: <some code output omitted>
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

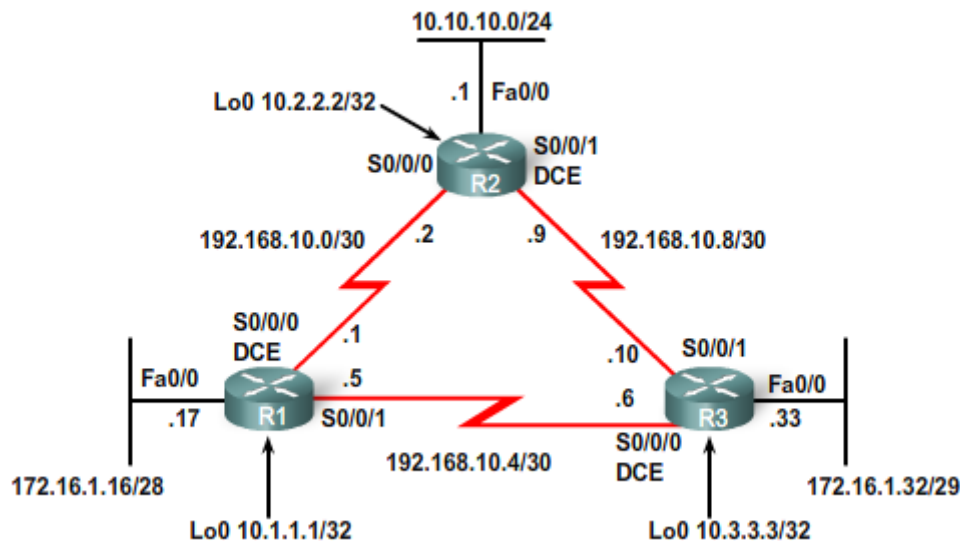
```
Gateway of last resort is not set
```

```
192.168.10.0/30 is subnetted, 3 subnets
O    192.168.10.0 [110/845] via 192.168.10.9, 14:31:52, Serial0/0/1
    [110/845] via 192.168.10.5, 14:31:52, Serial0/0/0
C    192.168.10.4 is directly connected, Serial0/0
C    192.168.10.8 is directly connected, Serial0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.1.32/29 is directly connected, FastEthernet0/0
O    172.16.1.16/28 [110/782] via 192.168.10.5, 14:31:52, Serial0/0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.3.3.3/32 is directly connected, Loopback0
O    10.10.10.0/24 [110/782] via 192.168.10.9, 14:31:52, Serial0/0/1
```

R1

R2

R3



El comando show ip route puede utilizarse para verificar si dicho OSPF envía y recibe rutas a través de OSPF. La O al inicio de cada ruta indica que el origen de la ruta es OSPF. La tabla de enrutamiento y OSPF se examinarán más detenidamente en la siguiente sección. Sin embargo, el usuario debería distinguir inmediatamente dos diferencias visibles en la tabla de enrutamiento de OSPF en comparación con las tablas de enrutamiento que se vieron en los capítulos anteriores. Primero, observe que cada router tiene cuatro redes conectadas directamente, ya que la interfaz loopback se cuenta como una cuarta red. Dichas interfaces loopback no se publican en OSPF. Por lo tanto, cada router enumera siete redes conocidas. Además, a diferencia de RIPv2 y EIGRP, OSPF no realiza un resumen automático en los bordes de la red principal. OSPF es esencialmente sin clase.

11.3 Métrica del OSPF

11.3.1 Métrica del OSPF

La métrica del OSPF se denomina costo. En RFC 2328: "Un costo se asocia con el resultado de cada interfaz de router. Dicho costo está configurado por el administrador del sistema. Cuanto más bajo sea el costo, más probabilidad hay de que la interfaz sea utilizada para enviar tráfico de datos."

Observe que RFC 2328 no especifica los valores que deben utilizarse para determinar el costo.

Valores de costo OSPF de Cisco

Tipo de interfaz	$10^8 / \text{bps} = \text{Costo}$
Fast Ethernet y más rápida	$10^8 / 100\,000\,000 \text{ bps} = 1$
Ethernet	$10^8 / 10\,000\,000 \text{ bps} = 10$
E1	$10^8 / 2\,048\,000 \text{ bps} = 48$
T1	$10^8 / 1\,544\,000 \text{ bps} = 64$
128 kbps	$10^8 / 128\,000 \text{ bps} = 781$
64 kbps	$10^8 / 64\,000 \text{ bps} = 1562$
56 kbps	$10^8 / 56\,000 \text{ bps} = 1785$

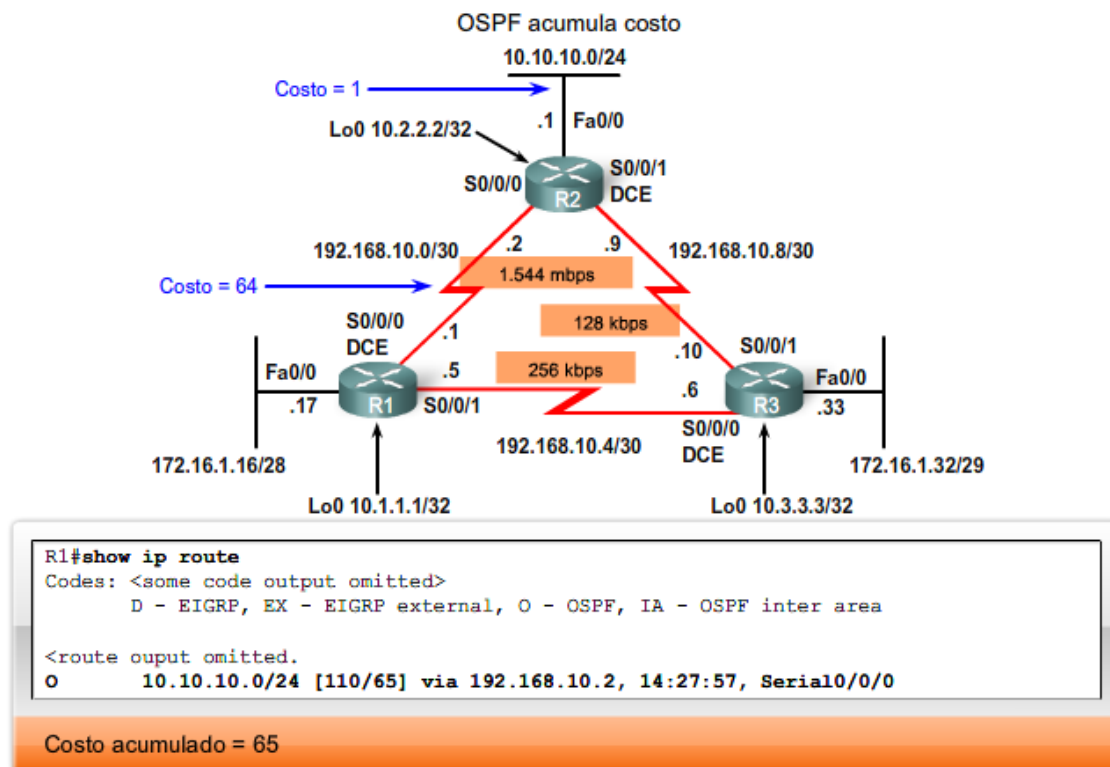
El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el router hasta la red de destino como valor del costo. En cada router, el costo de una interfaz se calcula en 10 a la octava potencia dividido por el ancho de banda en bps. Esto se conoce como ancho de banda de referencia. La división de 10 a la octava potencia por el ancho de banda de la interfaz se realiza para que las interfaces con mayores valores de ancho de banda tengan un costo calculado inferior. Recuerde, en las métricas de enrutamiento, la ruta de inferior costo es la ruta preferida (por ejemplo, con RIP, 3 saltos es mejor que 10 saltos). La figura muestra los costos predeterminados de OSPF para varios tipos de interfaces.

Ancho de banda de referencia

El ancho de banda de referencia predeterminado es de 10 a la octava potencia, 100 000 000 bps o 100 Mbps. Esto da como resultado interfaces con un ancho de banda de 100 Mbps y más con el mismo costo de OSPF de 1. El ancho de banda de referencia puede modificarse para adaptarse a redes con enlaces más rápidos que 100 000 000 bps (100 Mbps) con el comando `auto-cost reference-bandwidth` de OSPF. Cuando este comando es necesario, se recomienda su utilización en todos los routers para que la métrica de enrutamiento de OSPF se mantenga uniforme.

OSPF acumula costos

El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino. Por ejemplo, en la figura, la tabla de enrutamiento en R1 muestra un costo de 65 para alcanzar la red 10.10.10.0/24 en R2. Debido a que 10.10.10.0/24 está conectada a la interfaz FastEthernet, R2 asigna el valor de 1 como costo para 10.10.10.0/24. R1 luego agrega el valor del costo adicional de 64 para enviar datos a través del enlace T1 predeterminado entre R1 y R2.



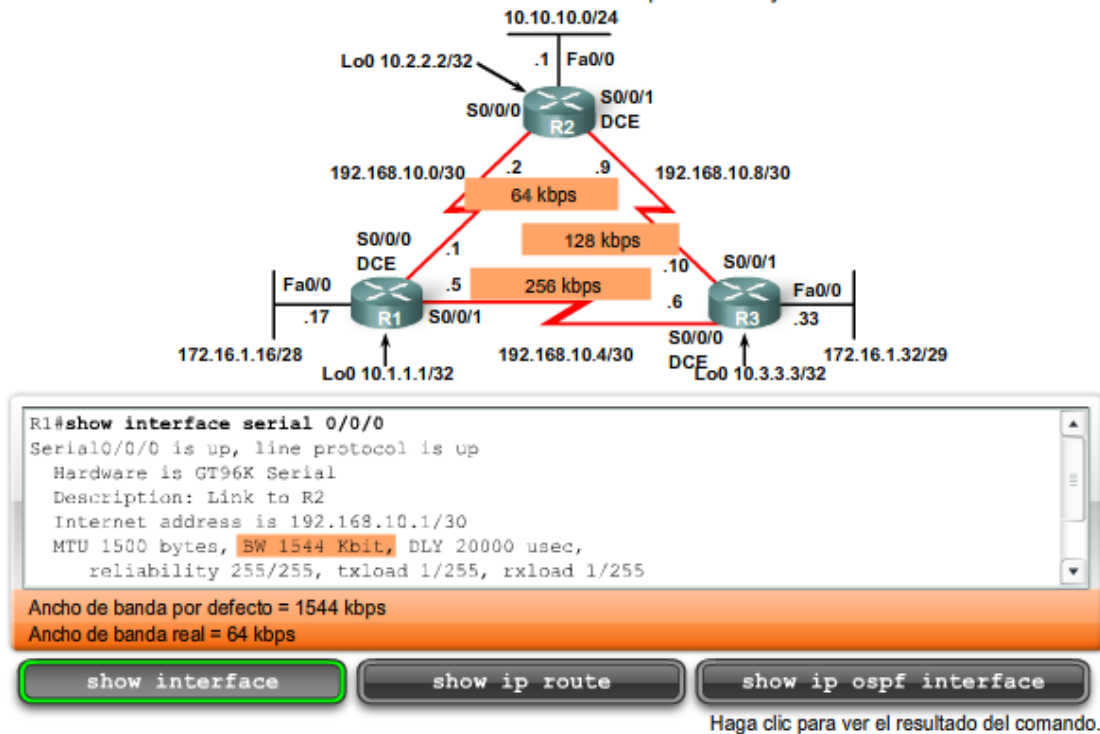
Ancho de banda predeterminado en interfaces seriales

Es posible que recuerde del Capítulo 9, "EIGRP", que puede utilizar el comando `show interface` para ver el valor del ancho de banda utilizado para una interfaz. En los routers de Cisco, el valor del ancho de banda predeterminado de varias interfaces seriales es T1 (1 544 Mbps). Sin embargo, algunas interfaces seriales pueden tener el valor predeterminado de 128 kbps. Por lo tanto, nunca suponga que OSPF utiliza un valor de ancho de banda particular. Verifique siempre el valor predeterminado con el comando `show interface`.

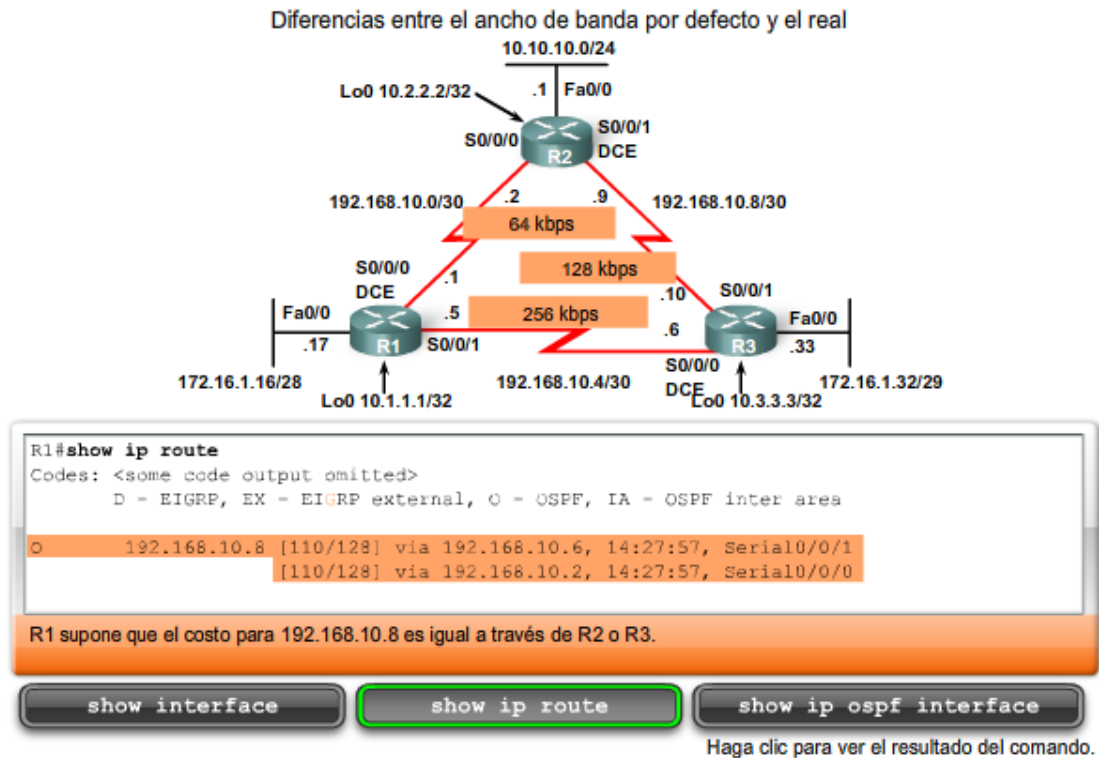
Recuerde, este valor de ancho de banda no afecta realmente la velocidad del enlace; lo utilizan ciertos protocolos de enrutamiento para calcular la métrica de enrutamiento. Muy probablemente, en las interfaces seriales la velocidad real del enlace es diferente del ancho de banda predeterminado. Es importante que el valor de ancho de banda refleje la velocidad real del enlace para que la tabla de enrutamiento tenga información precisa del mejor camino. Por ejemplo, el usuario puede estar pagando a su proveedor de servicios únicamente por una conexión T1 fraccional, un cuarto de la conexión T1 completa (384 kbps). Sin embargo, a los fines del protocolo de enrutamiento, IOS supone el valor de ancho de banda de T1 a pesar de que la interfaz en realidad sólo envía y recibe un cuarto de una conexión T1 completa (384 kbps).

La figura muestra el resultado de la interfaz Serial 0/0/0 en R1. La topología también refleja ahora el ancho de banda real del enlace entre los routers. Observe que el valor de ancho de banda predeterminado en el resultado del comando para R1 es 1544 kbps. Sin embargo, el ancho de banda real de este enlace es 64 kbps. Esto significa que el router tiene información de enrutamiento que no refleja en forma precisa la topología de red.

Diferencias entre el ancho de banda por defecto y el real



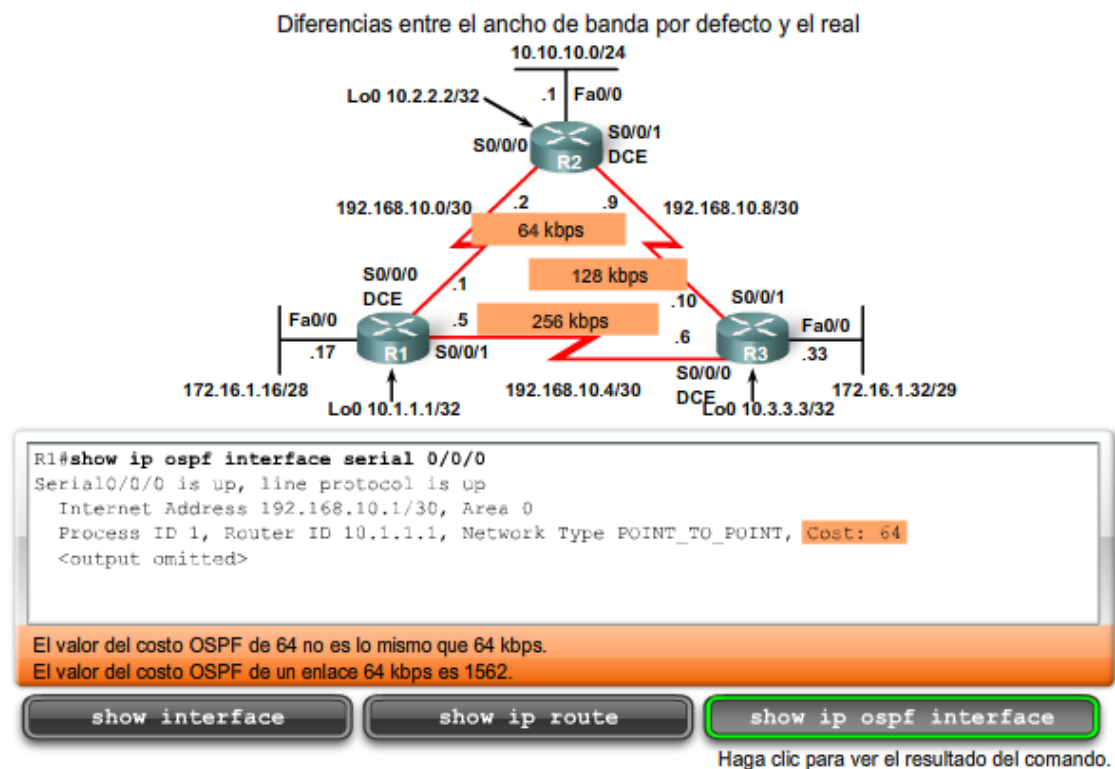
Haga clic en show ip route en la figura.



La figura muestra la tabla de enrutamiento para R1. R1 considera que sus dos interfaces seriales están conectadas a enlaces de T1 a pesar de que uno de sus enlaces es de 64 kbps y el otro de 256 kbps. Esto provoca que la tabla de enrutamiento de R1 tenga dos rutas de igual costo hacia la red 192.168.8.0/30, donde Serial 0/0/1 es realmente el mejor camino.

0 192.168.10.8 [110/128] via 192.168.10.6, 00:03:41, Serial0/0/1
[110/128] via 192.168.10.2, 00:03:41, Serial0/0/0

Haga clic en show ip ospf interface en la figura.



El costo OSPF calculado de una interfaz puede verificarse con el comando show ip ospf interface. En la figura, podemos verificar que R1 verdaderamente asigna un costo de 64 a la interfaz Serial 0/0/0. Si bien el usuario puede pensar que ése es el costo correcto, ya que esta interfaz está conectada a un enlace de 64 kbps, recuerde que el costo deriva de la fórmula de costo. El costo de un enlace de 64 kbps es 1562 ($100\,000\,000/64\,000$). El valor mostrado de 64 corresponde al costo de un enlace T1. En el siguiente tema, aprenderá la manera de modificar el costo de todos los enlaces de la topología.

11.3.2 Modificación del costo de enlace

Cuando la interfaz serial no está funcionando realmente a la velocidad predeterminada de T1, la interfaz requiere una modificación manual. Ambos lados del enlace deben configurarse para tener el mismo valor. Tanto el comando de interfaz bandwidth como el comando de interfaz ip ospf cost logran este fin, un valor preciso que OSPF utilizará para determinar el mejor camino.

Comando bandwidth

El comando bandwidth se utiliza para modificar el valor del ancho de banda utilizado por IOS en el cálculo de la métrica de costo de OSPF. La sintaxis del comando interface es la misma sintaxis que aprendió en el Capítulo 9, "EIGRP":

```
Router(config-if)#bandwidth bandwidth-kbps
```

```

R1(config)#inter serial 0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#inter serial 0/0/1
R1(config-if)#bandwidth 256
R1(config-if)#end
R1#show ip ospf interface serial 0/0/0
Serial0/0 is up, line protocol is up
 Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 1562
 Transmit Delay is 1 sec, State POINT_TO_POINT,
 <output omitted>

```

$10^8 / 64,000 \text{ bps} = 1562$

```

R2(config)#inter serial 0/0/0
R2(config-if)#bandwidth 64
R2(config-if)#inter serial 0/0/1
R2(config-if)#bandwidth 128

```

```

R3(config)#inter serial 0/0/0
R3(config-if)#bandwidth 256
R3(config-if)#inter serial 0/0/1
R3(config-if)#bandwidth 128

```

La figura muestra los comandos bandwidth utilizados para modificar los costos de todas las interfaces seriales de la topología. En el caso de R1, el comando show ip ospf interface muestra que el costo del enlace Serial 0/0/0 es ahora 1562, el resultado del cálculo de costo OSPF de Cisco de $100\,000\,000 / 64\,000$.

Comando ip ospf cost

Un método alternativo a la utilización del comando bandwidth es utilizar el comando ip ospf cost, que le permite especificar directamente el costo de una interfaz. Por ejemplo, en R1 podríamos configurar Serial 0/0/0 con el siguiente comando:

```
R1(config)#interface serial 0/0/0
```

```
R1(config-if)#ip ospf cost 1562
```

Ciertamente, esto no cambiará el resultado del comando show ip ospf interface, que aún muestra el costo de 1562. Éste es el mismo costo calculado por IOS cuando configuramos el ancho de banda en 64.

```

R1(config)#inter serial 0/0/0
R1(config-if)#ip ospf cost 1562
R1(config-if)#end
R1#show ip ospf interface serial 0/0/0
Serial0/0 is up, line protocol is up
 Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 1562
 Transmit Delay is 1 sec, State POINT_TO_POINT,
 <output omitted>

```

No se necesita cálculo

Comparación entre el comando `bandwidth` y el comando `ip ospf cost`

El comando `ip ospf cost` es útil en entornos de varios fabricantes, donde los routers que no son de Cisco utilizan una métrica diferente del ancho de banda para calcular los costos de OSPF. La principal diferencia entre los dos comandos es que el comando `bandwidth` utiliza el resultado del cálculo de costo para determinar el costo del enlace. El comando `ip ospf cost` evita este cálculo al establecer directamente el costo del enlace en un valor específico.

La figura muestra las dos alternativas que pueden utilizarse al modificar los costos de los enlaces seriales en la topología. El lado derecho de la figura muestra los comandos `ip ospf cost` equivalentes a los comandos `bandwidth` de la izquierda.

Comandos equivalentes

Comandos <code>bandwidth</code>		Comandos <code>ip ospf cost</code>
Router R1 R1 (config) #interface serial 0/0/0 R1 (config-if) #bandwidth 64	=	Router R1 R1 (config) #interface serial 0/0/0 R1 (config-if) #ip ospf cost 1562
R1 (config) #interface serial 0/0/1 R1 (config-if) #bandwidth 256	=	R1 (config) #interface serial 0/0/1 R1 (config-if) #ip ospf cost 390
Router R2 R2 (config) #interface serial 0/0/0 R2 (config-if) #bandwidth 64	=	Router R2 R2 (config) #interface serial 0/0/0 R2 (config-if) #ip ospf cost 1562
R2 (config) #interface serial 0/0/1 R2 (config-if) #bandwidth 128	=	R2 (config) #interface serial 0/0/1 R2 (config-if) #ip ospf cost 781
Router R3 R3 (config) #interface serial 0/0/0 R3 (config-if) #bandwidth 256	=	Router R3 R3 (config) #interface serial 0/0/0 R3 (config-if) #ip ospf cost 390
R3 (config) #interface serial 0/0/1 R3 (config-if) #bandwidth 128	=	R3 (config) #interface serial 0/0/1 R3 (config-if) #ip ospf cost 781

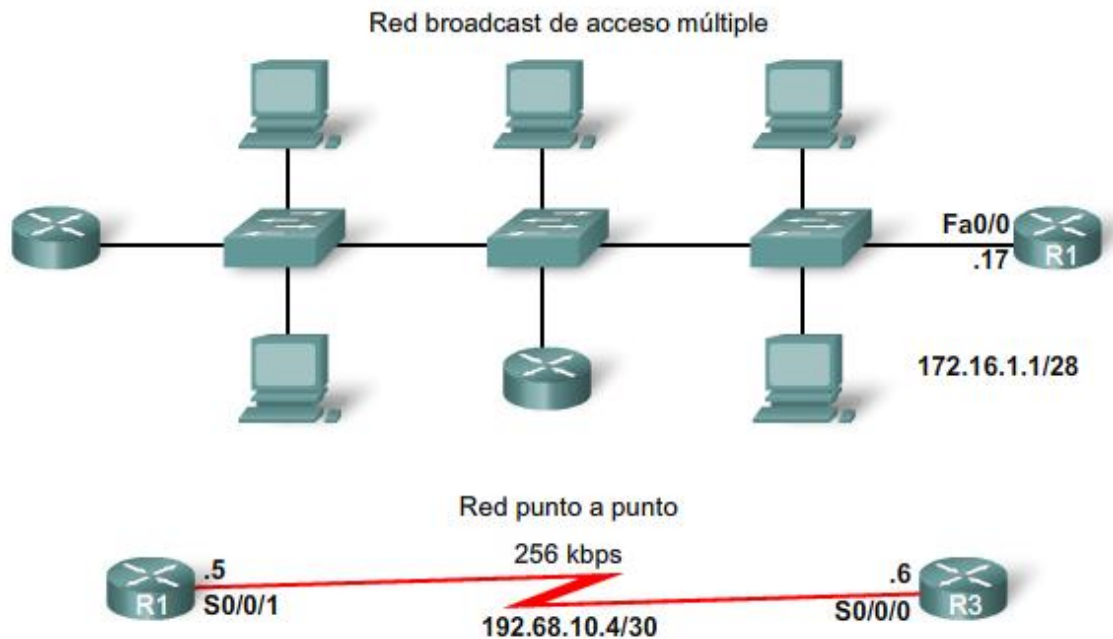
11.4 OSPF y redes de accesos múltiples

11.4.1 Desafíos en redes de accesos múltiples

Una red de accesos múltiples es una red con más de dos dispositivos en los mismos medios compartidos. En el sector superior de la figura, la LAN Ethernet conectada a R1 se extiende para mostrar los posibles dispositivos que pueden conectarse a la red 172.16.1.16/28. Las LAN Ethernet son un ejemplo de una red broadcast de accesos múltiples. Son redes broadcast ya que todos los dispositivos de la red ven todas las tramas. Son redes de accesos múltiples ya que puede haber gran cantidad de hosts, impresoras, routers y demás dispositivos que formen parte de la misma red.

Por el contrario, en una red punto a punto sólo hay dos dispositivos en la red, uno en cada extremo. El enlace WAN entre R1 y R3 es un ejemplo de enlace punto a punto. El sector inferior de la figura muestra el enlace punto a punto entre R1 y R3.

Comparación entre redes de acceso múltiple y punto a punto



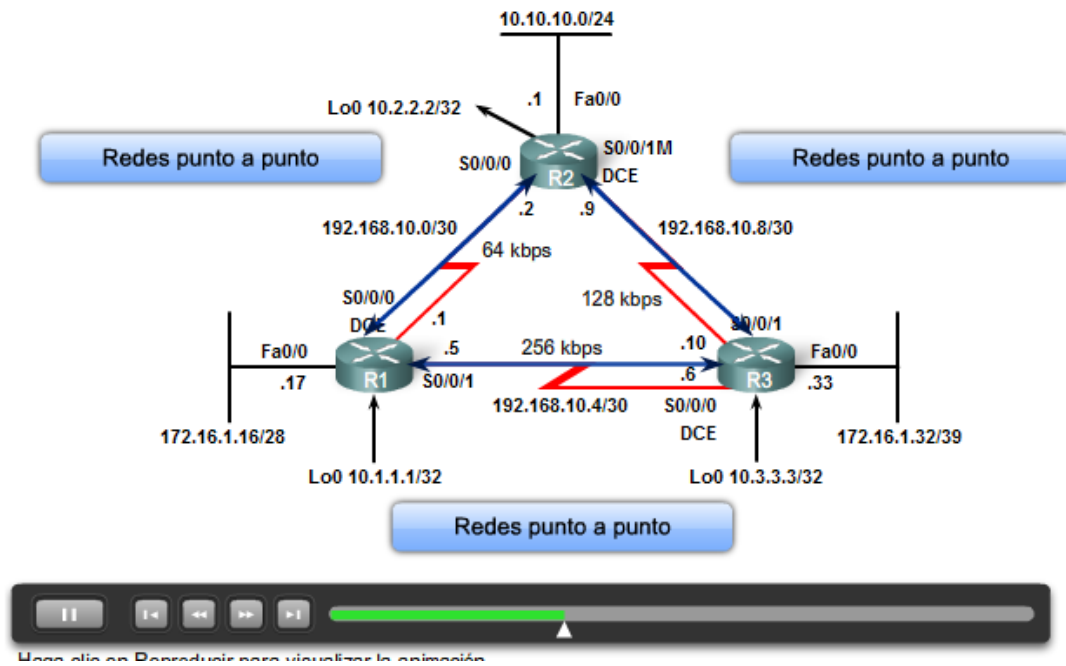
OSPF define cinco tipos de redes:

- Punto a punto
- Broadcast de accesos múltiples
- Multiacceso sin broadcast (NBMA)
- Punto a multipunto
- Enlaces virtuales

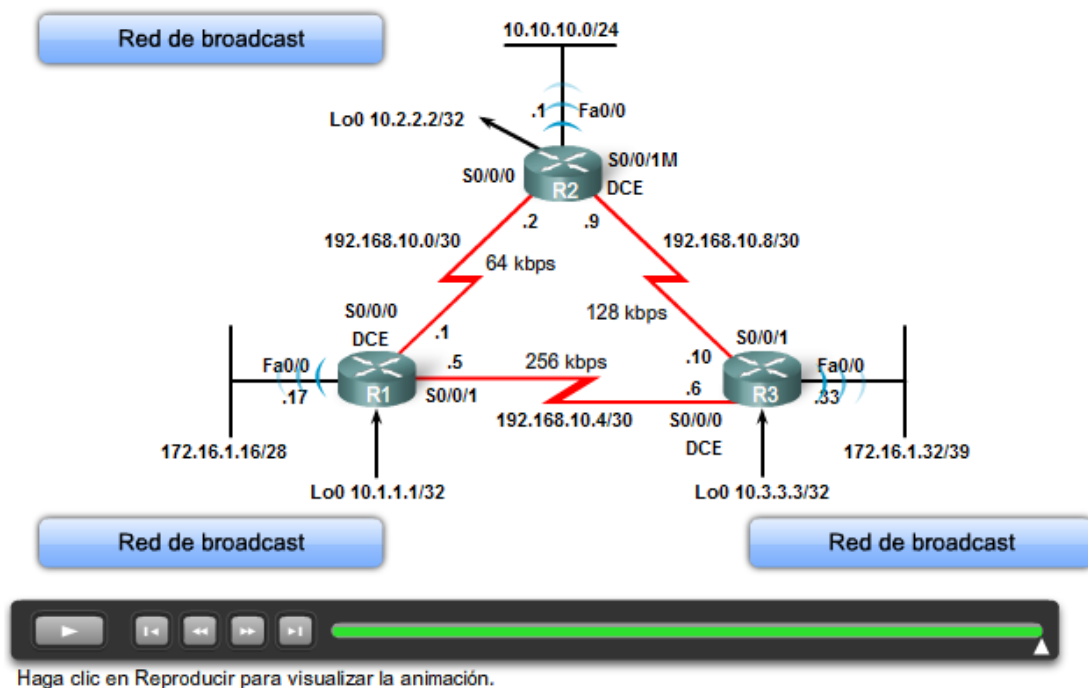
Las redes NBMA y punto a multipunto incluyen redes Frame Relay, ATM y X.25. Las redes NBMA se analizan en otro curso de CCNA. Las redes punto a multipunto se analizan en CCNP. Los enlaces virtuales son un tipo especial de enlace que puede usarse en un OSPF de áreas múltiples. Los enlaces virtuales de OSPF se analizan en CCNP.

Haga clic en Reproducir para ver la animación.

Tipos de redes OSPF utilizadas en la topología



Tipos de redes OSPF utilizadas en la topología



La animación muestra que la topología utiliza redes punto a punto y broadcast.

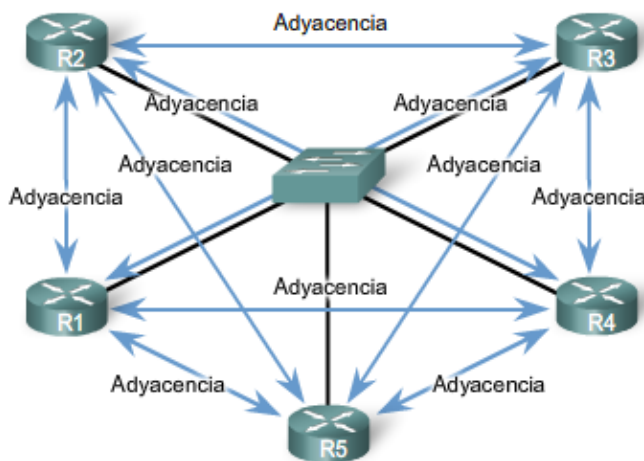
Las redes de accesos múltiples pueden crear dos desafíos para OSPF en relación con la saturación de las LSA:

1. Creación de adyacencias múltiples, una adyacencia para cada par de routers.
2. Saturación extensa de las LSA (Notificaciones de estado de enlace).

Adyacencias múltiples

La creación de una adyacencia entre cada par de routers en una red creará una cantidad innecesaria de adyacencias. Esto llevará al paso de una cantidad excesiva de LSA entre routers de la misma red.

Para comprender el problema con las adyacencias múltiples, necesitamos estudiar una fórmula. Para cualquier cantidad de routers (designada como n) en una red de accesos múltiples, habrá $n(n-1)/2$ adyacencias. La figura muestra una topología simple de cinco routers, los cuales están conectados a la misma red Ethernet de accesos múltiples. Sin ningún tipo de mecanismo para reducir la cantidad de adyacencias, estos routers en forma colectiva formarán 10 adyacencias: $5(5-1)/2 = 10$. Si bien esto puede no parecer demasiado, a medida que se agregan routers a la red, la cantidad de adyacencias aumenta significativamente. Si bien los 5 routers de la figura sólo necesitarán 10 adyacencias, podrá ver que 10 routers requerirán 45 adyacencias. ¡Veinte routers requerirán 190 adyacencias!



Routers	Adyacencias
n	$\frac{n(n-1)}{2}$
5	10
10	45
20	190
100	4950

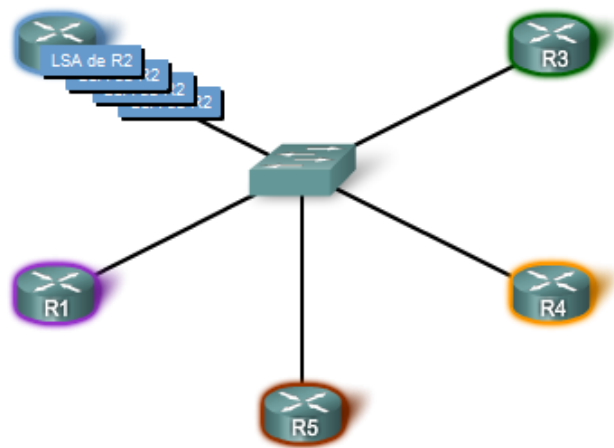
Cantidad de adyacencias = $\frac{n(n-1)}{2}$
 n = cantidad de routers
Ejemplo: 5 routers $\frac{5(5-1)}{2} = 10$ adyacencias

Saturación de las LSA

Recuerde del Capítulo 10, "Protocolos de enrutamiento de estado de enlace", que los routers de estado de enlace saturan sus paquetes de estado de enlace al inicializarse OSPF o cuando hay un cambio en la topología.

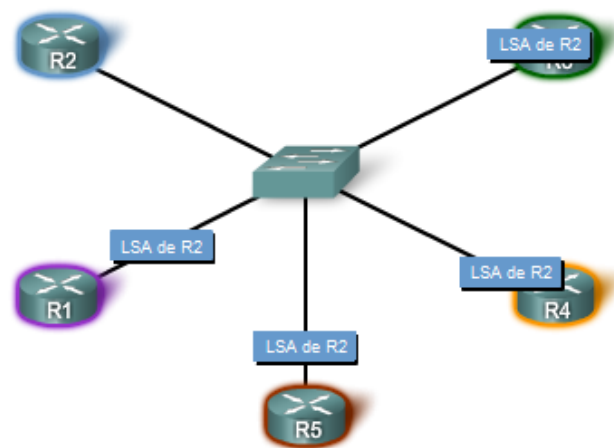
Haga clic en Reproducir para ver la animación de un escenario de saturación de LSA.

Situación de inundación de LSA



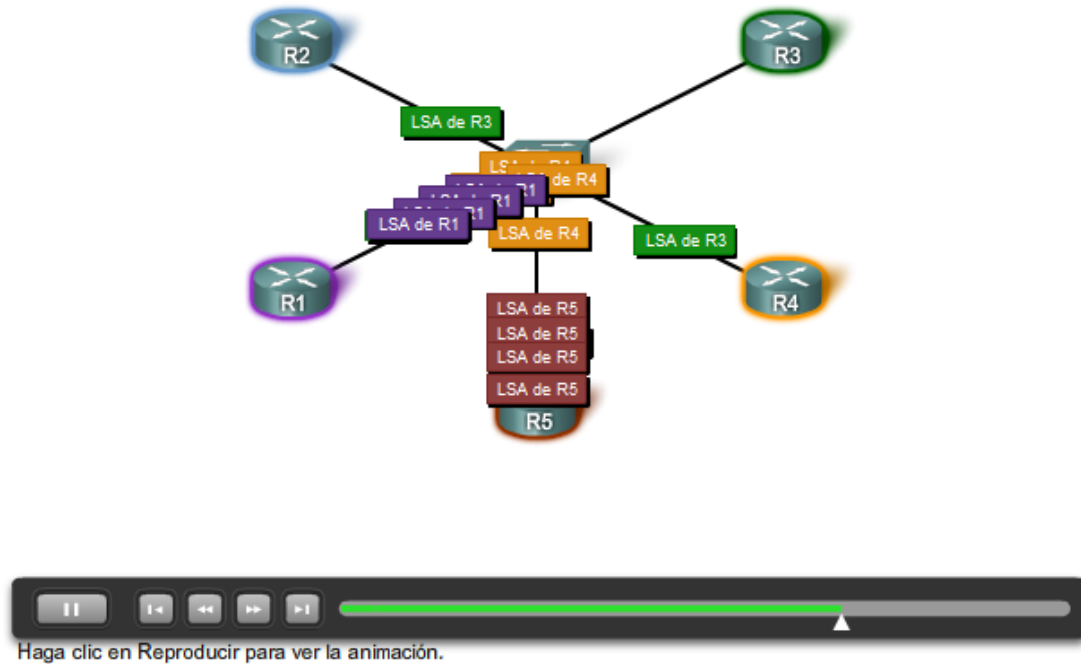
Haga clic en Reproducir para ver la animación.

Situación de inundación de LSA



Haga clic en Reproducir para ver la animación.

Situación de inundación de LSA



En una red de accesos múltiples, esta saturación puede volverse excesiva. En la animación, R2 envía una LSA. Este evento hace que cada router también envíe una LSA. En la animación no se muestran los acuses de recibo requeridos enviados para cada LSA recibida. Si cada router en una red de accesos múltiples tuviera que saturar y reconocer todas las LSA recibidas a todos los demás routers en la misma red de accesos múltiples, el tráfico de la red se volvería bastante caótico.

Para ilustrar este punto, imagine que se encuentra en un cuarto con una gran cantidad de personas. ¿Qué sucedería si todos tuvieran que presentarse ante los demás en forma individual? Cada persona no sólo tendría que decir a los demás su nombre, sino que además cada vez que una persona aprenda el nombre de otra, ésta última tendría que decirlo a las demás personas que se encuentran en el cuarto, una persona por vez. Como podrá ver, ¡este proceso conduce al caos!

Solución: Router designado

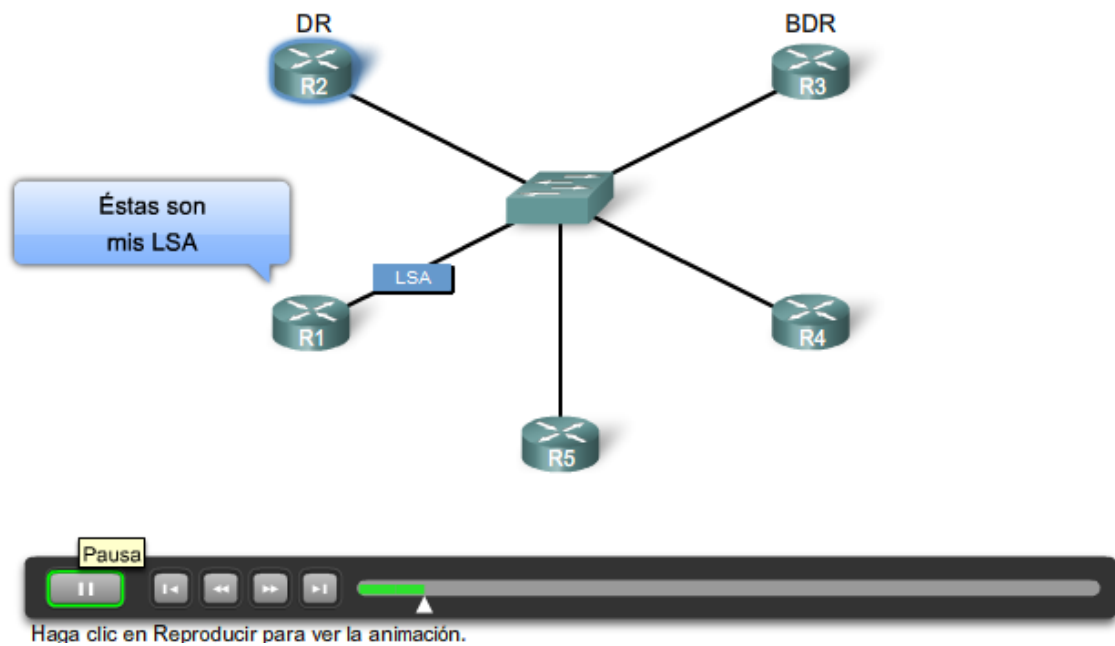
La solución para administrar la cantidad de adyacencias y la saturación de las LSA en una red de accesos múltiples es el Router designado (DR). Continuando con nuestro ejemplo anterior, esta solución es igual a elegir a alguien del cuarto para que aprenda los nombres de todos y luego los pronuncie ante todos en el cuarto al mismo tiempo.

En las redes de accesos múltiples, OSPF elige un Router designado (DR) para que represente el punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un Router designado de respaldo (BDR) en caso de que falle el Router designado. Todos los demás routers se convierten en DROthers (esto indica un router que no es DR ni BDR).

Haga clic en Reproducir para ver la animación del rol del DR.

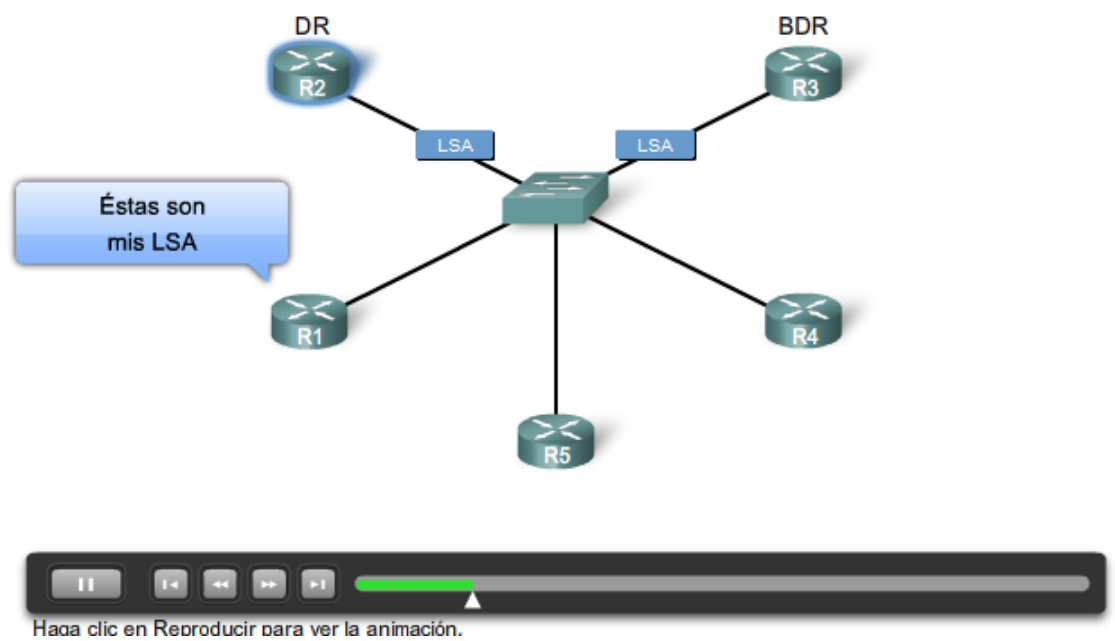
DR y BDR en una red de acceso múltiple

Las adyacencias están formadas sólo con DR y BDR.



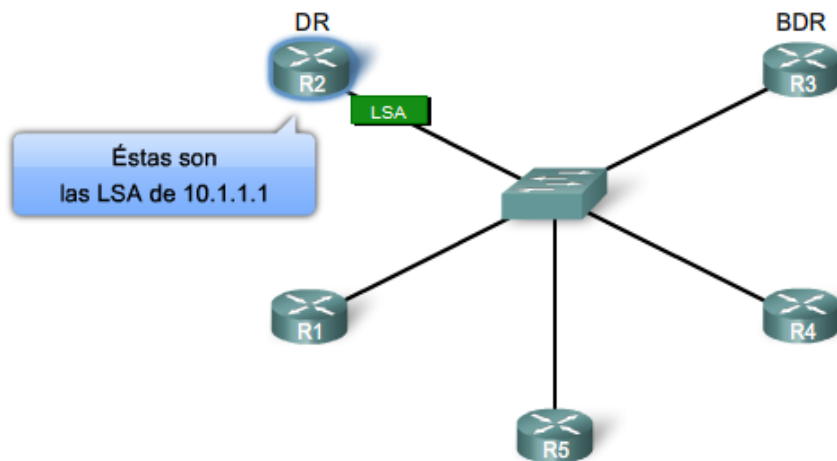
DR y BDR en una red de acceso múltiple

Las adyacencias están formadas sólo con DR y BDR.



DR y BDR en una red de acceso múltiple

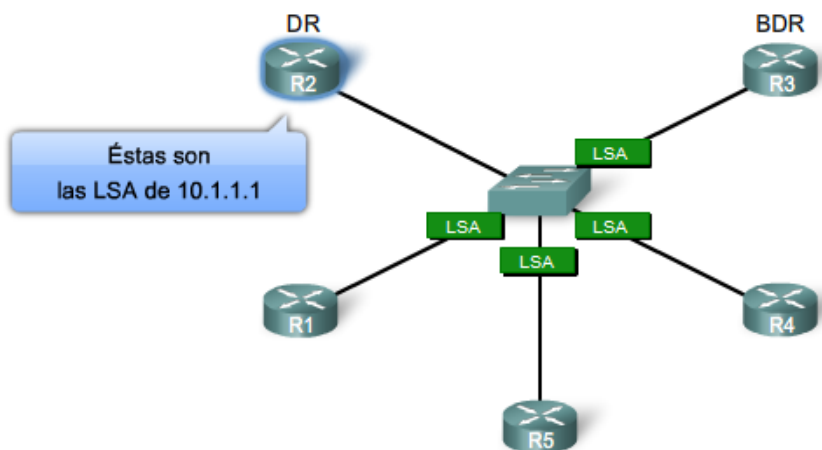
DR envía cualquier LSA a todos los demás routers.



Haga clic en Reproducir para ver la animación.

DR y BDR en una red de acceso múltiple

DR envía cualquier LSA a todos los demás routers.



Haga clic en Reproducir para ver la animación.

Los routers de una red de accesos múltiples eligen un DR y un BDR. Los DROthers sólo forman adyacencias completas con el DR y el BDR en la red. Esto significa que en lugar de saturar las LSA a todos los routers en la red, los DROthers sólo envían sus LSA al DR y al BDR con la dirección multicast 24.0.0.6 (ALLDRouters - All DR routers). En la animación, R1 envía las LSA al DR. El BDR también escucha. El DR es responsable de reenviar todas las LSA desde R1 hasta todos los demás routers. El DR utiliza la dirección multicast 224.0.0.5

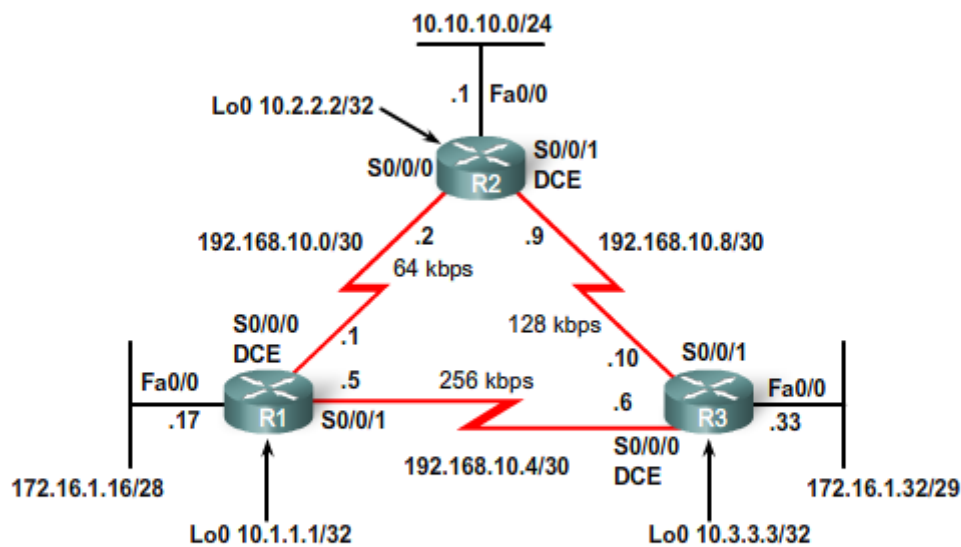
(AllSPFRouters - All OSPF routers). El resultado final es que sólo hay un router que realiza la saturación completa de todas las LSA en la red de accesos múltiples.

11.4.2 Proceso de elección de DR/BDR

Cambio de topología

Las elecciones de DR/BDR no se presentan en las redes punto a punto. Por lo tanto, en una topología estándar de tres routers, R1, R2 y R3 no necesitan elegir un DR ni un BDR, ya que los enlaces entre estos routers no son redes de accesos múltiples.

Topología punto a punto de tres routers



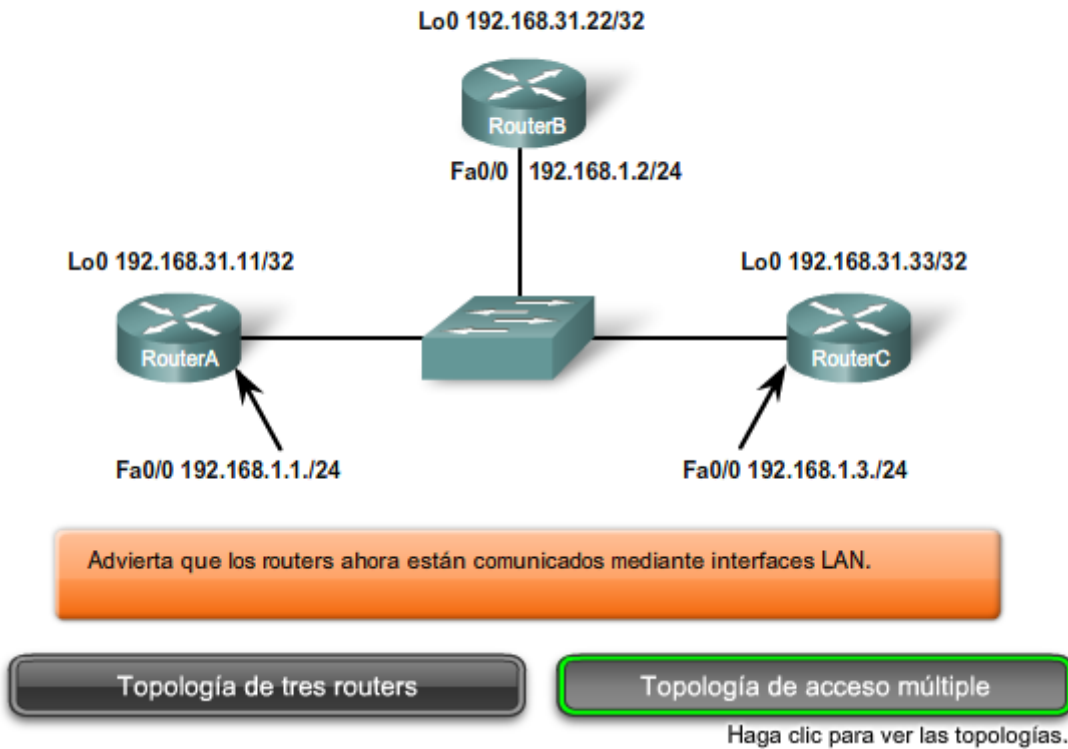
Topología de tres routers

Topología de acceso múltiple

Haga clic para ver las topologías.

Haga clic en Topología de accesos múltiples en la figura.

Topología de acceso múltiple de tres routers



Para el resto de la discusión del DR y BDR, utilizaremos la topología de accesos múltiples que muestra la figura. Los nombres de los routers son diferentes, únicamente para enfatizar que esta topología no es la misma topología de tres routers que hemos utilizado hasta aquí. Regresaremos a nuestra topología del capítulo luego de la discusión sobre el proceso de elección de DR/BDR. En esta nueva topología, tenemos tres routers que comparten una red Ethernet de accesos múltiples común, 192.168.1.0/24. Cada router está configurado con una dirección IP en la interfaz Fast Ethernet y una dirección de loopback para la ID del router.

Elección de DR/BDR

¿Cómo se eligen el DR y el BDR? Se aplican los siguientes criterios:

1. DR: Router con la prioridad más alta de interfaz OSPF.
2. BDR: Router con la segunda prioridad más alta de interfaz OSPF.
3. Si las prioridades de la interfaz OSPF son iguales, la ID del router más alta se utiliza para desempatar.

En este ejemplo, la prioridad de interfaz OSPF predeterminada es 1. Como consecuencia, en base a los criterios de selección enumerados anteriormente, la ID del router OSPF se utiliza para elegir el DR y el BDR. Como podrá ver, el RouterC se convierte en el DR y el RouterB, con la segunda ID del router más alta, se convierte en el BDR. Debido a que el RouterA no se elige como DR ni BDR, se convierte en DROther.

Los DROthers sólo forman adyacencias FULL con el DR y el BDR; sin embargo, aún forman una adyacencia de vecinos con cualquier DROther que se una a la red. Esto significa que todos los routers DROther en la red de accesos múltiples aún reciben paquetes de saludo por parte

de todos los demás routers DROther. De esta manera, éstos conocen a todos los routers de la red. Cuando dos routers DROther forman una adyacencia de vecinos, el estado de vecino se muestra como 2WAY. Los diferentes estados de vecino se analizan en CCNP.

Haga clic en show ip ospf neighbor en la figura.

```
RouterA#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.33	1	FULL/DR	00:00:39	192.168.1.3	FastEthernet0/0
192.168.31.22	1	FULL/BDR	00:00:36	192.168.1.2	FastEthernet0/0

```
RouterB#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.33	1	FULL/DR	00:00:34	192.168.1.3	FastEthernet0/0
192.168.31.11	1	FULL/DROther	00:00:38	192.168.1.1	FastEthernet0/0

```
RouterC#show ip ospf neighbor
```

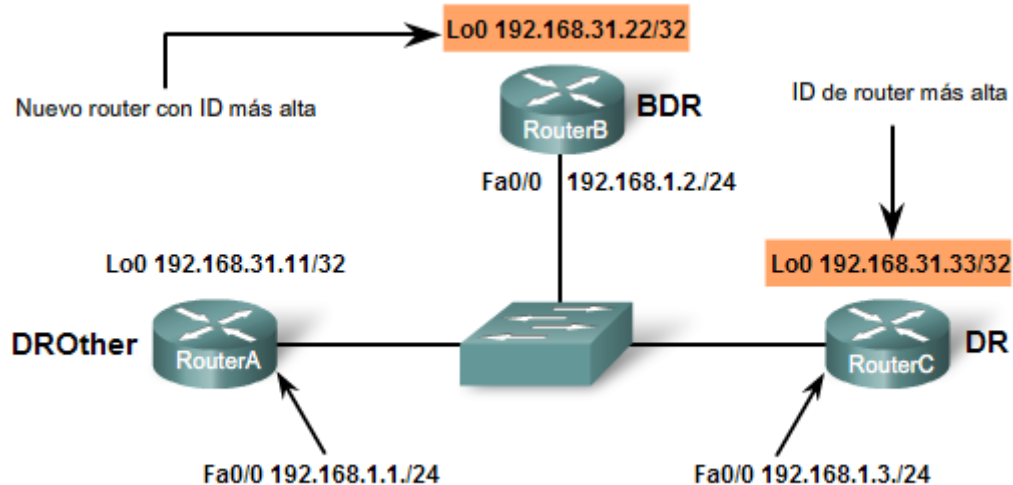
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.22	1	FULL/BDR	00:00:35	192.168.1.2	FastEthernet0
192.168.31.11	1	FULL/DROther	00:00:32	192.168.1.1	FastEthernet0

La prioridad es igual en el valor por defecto de 1.

show ip ospf neighbor

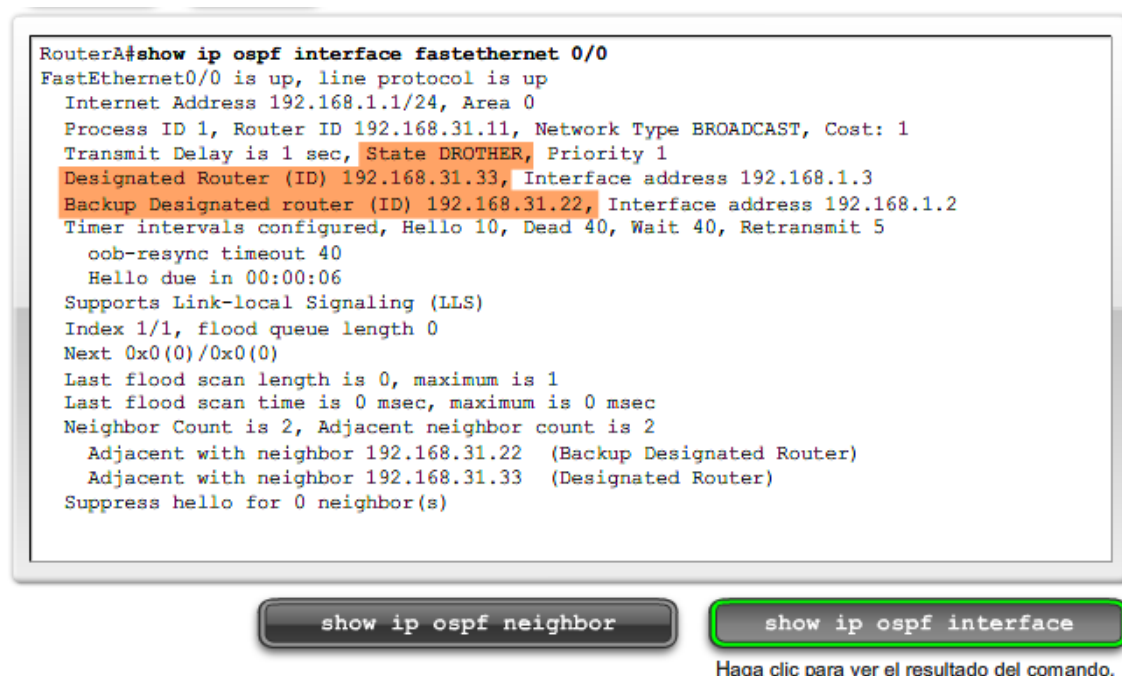
show ip ospf interface

Haga clic para ver el resultado del comando.



El resultado del comando en la figura muestra la adyacencia de vecinos de cada router en la red de accesos múltiples. Observe en el caso del RouterA que éste muestra que DR es el RouterC con la ID de router 192.168.31.33 y que BDR es el RouterB con la ID de router 192.168.31.22.

Haga clic en show ip ospf interface en la figura.



Debido a que el RouterA muestra a sus vecinos como DR y BDR, el RouterA es un DROther. Esto puede verificarse con el comando `show ip ospf interface fastethernet 0/0` en el RouterA, como se muestra en la figura. Este comando mostrará el estado DR, BDR o DROTHER de este router, junto con la ID del router de DR y BDR en esta red de accesos múltiples.

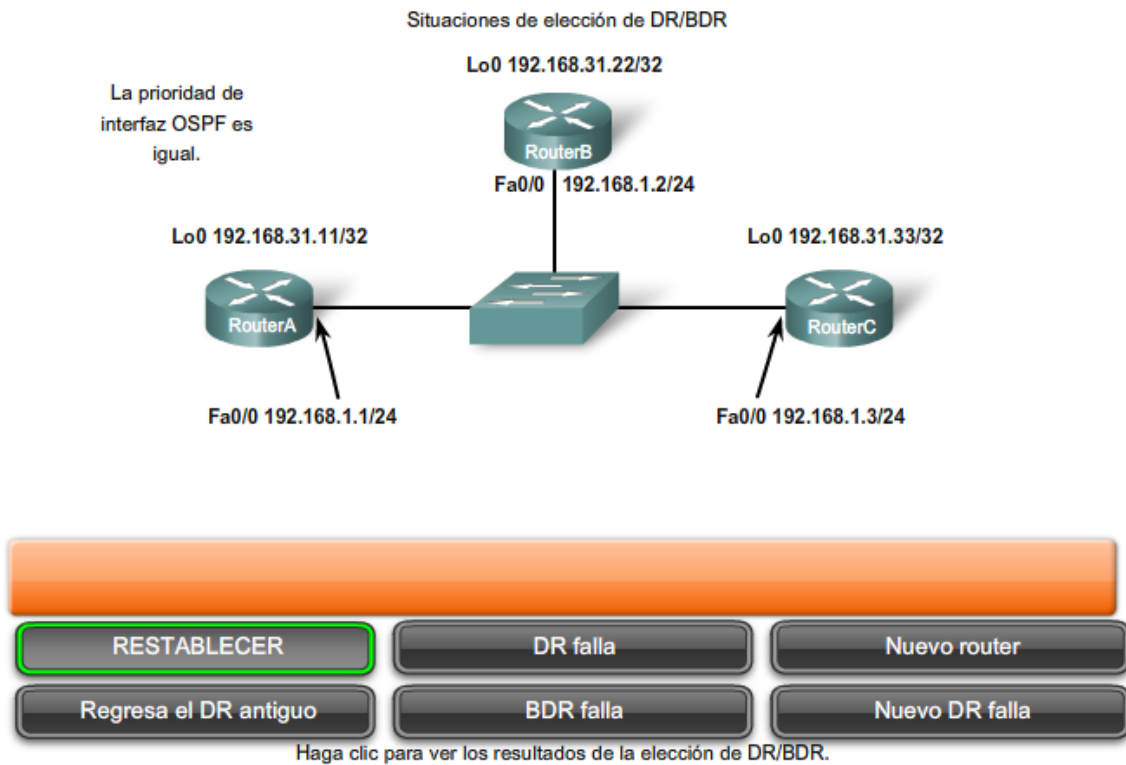
Elección de temporización de DR/BDR

El proceso de elección de DR y BDR se lleva a cabo tan pronto como el primer router con una interfaz OSPF habilitada se activa en la red de accesos múltiples. Esto puede suceder cuando se encienden los routers o cuando se configura el comando `network` de OSPF para dicha interfaz. El proceso de elección sólo toma unos pocos segundos. Si todos los routers de la red de accesos múltiples no finalizaron el inicio, es posible que un router con una ID de router más baja se convierta en DR. Podría ser un router de extremo inferior que tarde menos tiempo en iniciar.

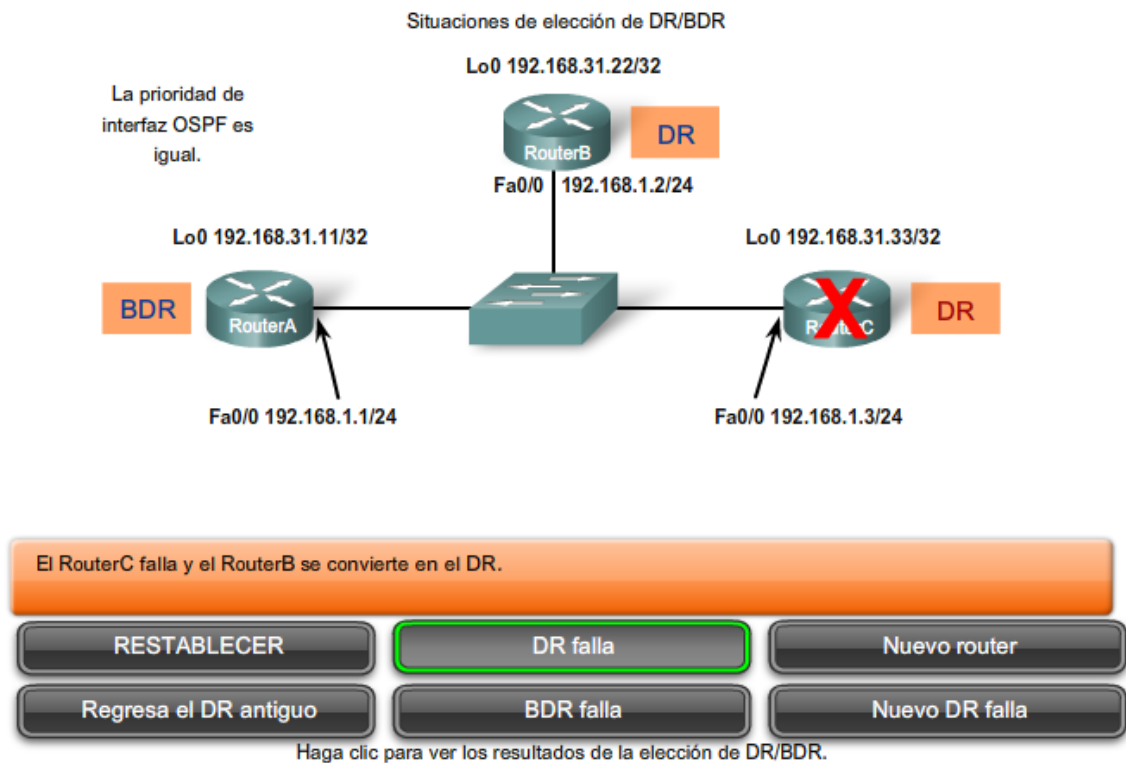
Cuando se elige el DR, éste continúa como DR hasta que se presente alguna de las siguientes condiciones:

- El DR falla.
- El proceso OSPF en el DR falla.
- La interfaz de accesos múltiples en el DR falla.

En la figura, una X roja indica una o más de dichas fallas.

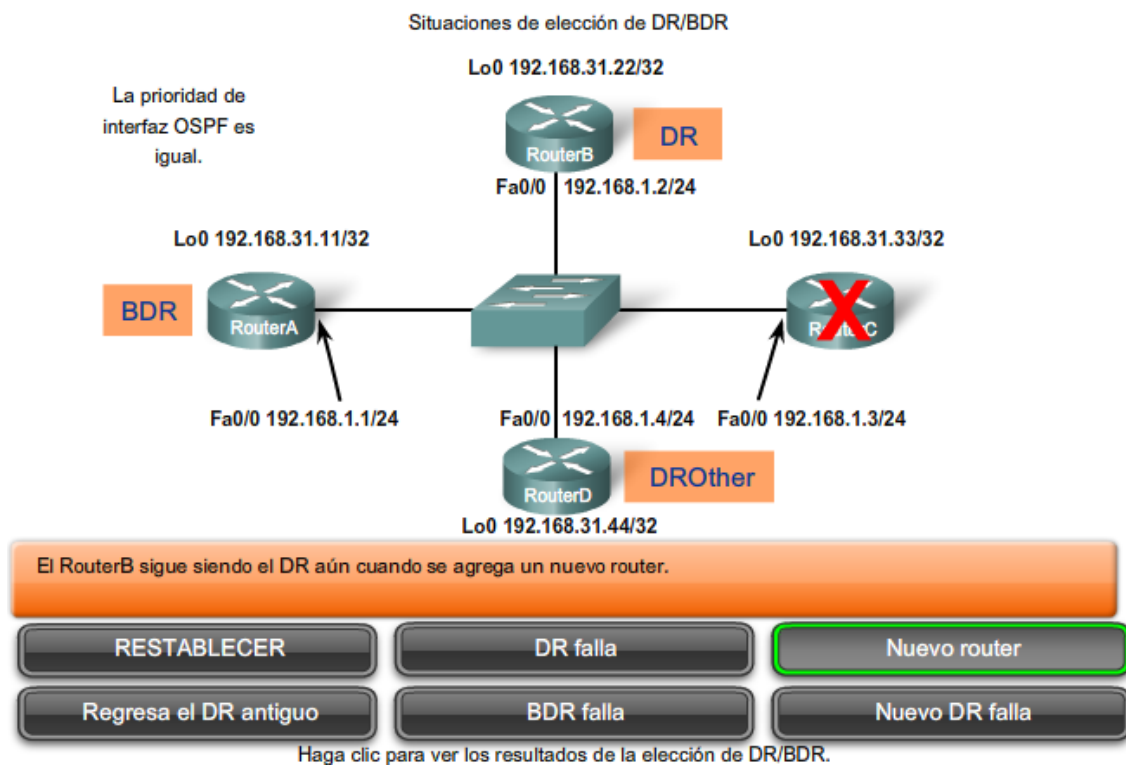


Haga clic en Falla de DR en la figura.



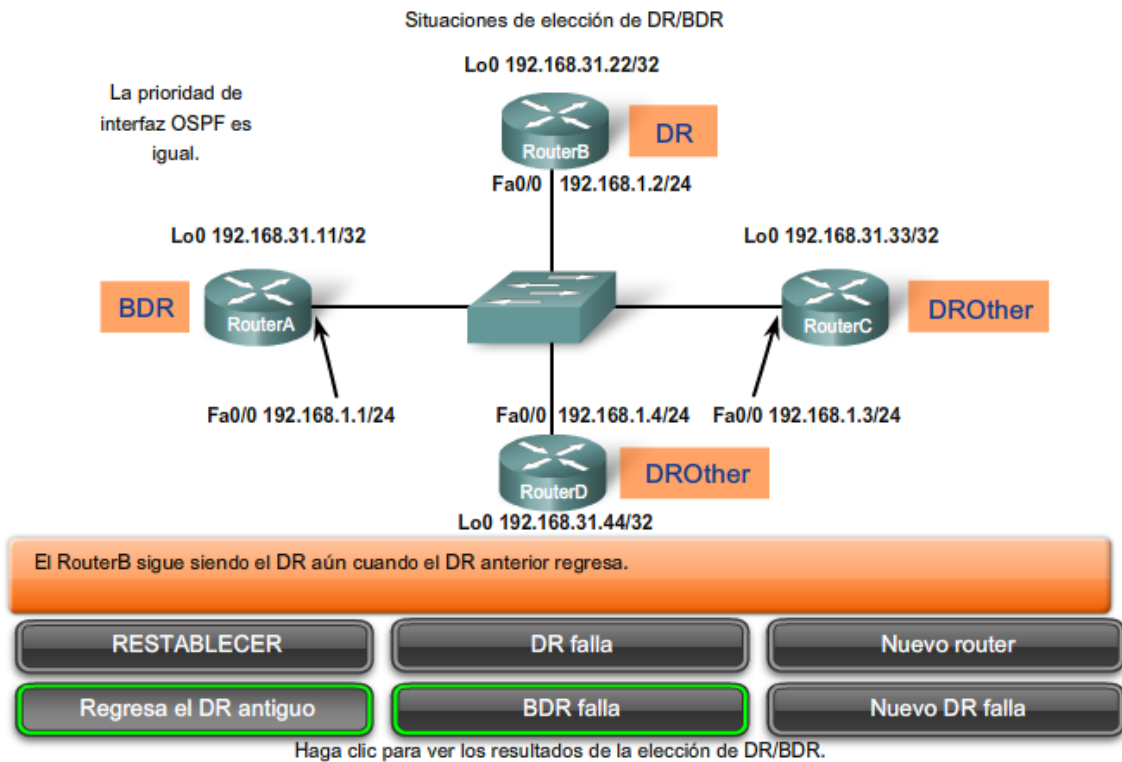
Si DR falla, BDR asume el rol de DR y se lleva a cabo una elección para seleccionar un nuevo BDR. En la figura, el RouterC falla y el anterior BDR, el RouterB, se convierte en DR. El único otro router disponible para convertirse en BDR es el RouterA.

Haga clic en Nuevo router en la figura.



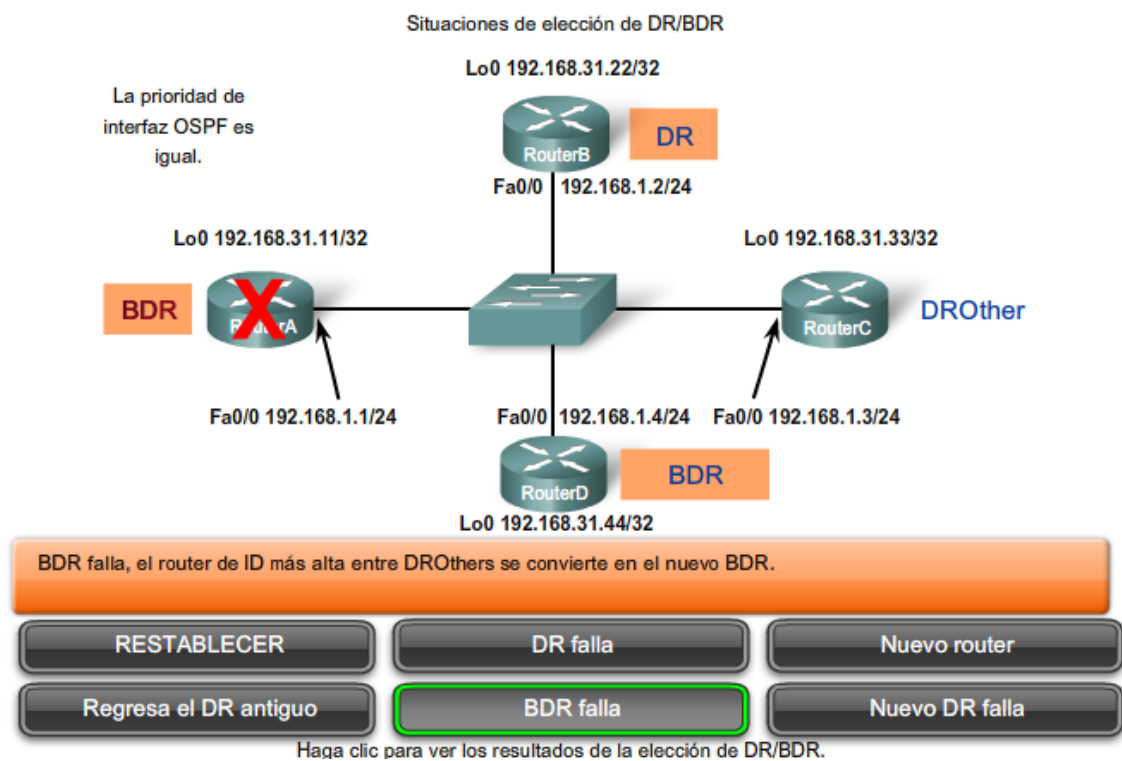
RouterD se une a la red. Si un nuevo router ingresa en la red después de que se hayan elegido el DR y el BDR, éste no se convertirá en DR ni en BDR, aunque cuente con una prioridad de interfaz OSPF o una ID del router mayor que la del DR o BDR actual. El nuevo router puede elegirse como el BDR si falla el DR o BDR actual. Si el DR actual falla, el BDR se convertirá en el DR, y el nuevo router puede elegirse como el BDR. Luego de que el nuevo router se convierte en BDR, si el DR falla, el nuevo router se convertirá en DR. El DR y BDR actuales deben fallar antes de que el nuevo router pueda elegirse como DR o BDR.

Haga clic en Regreso del antiguo DR en la figura.



Un DR antiguo no recupera el estado de DR si regresa a la red. En la figura, el RouterC se reinició y se convierte en DROther a pesar de que su ID de router, 192.168.31.33, es mayor que la del DR y del BDR actuales.

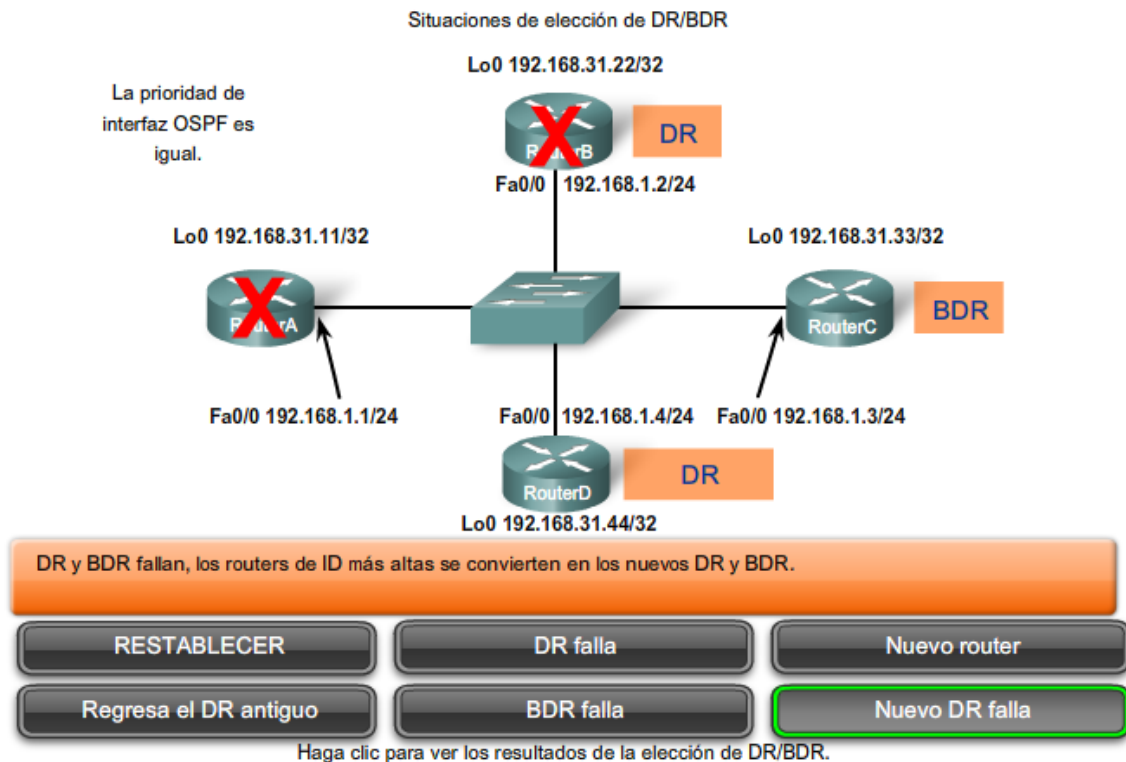
Haga clic en Falla de BDR en la figura.



Si BDR falla, se lleva a cabo una elección entre los DROthers para ver cuál router será el nuevo BDR. En la figura, el router BDR falla. Se lleva a cabo una elección entre el RouterC y el

RouterD. El RouterD gana la elección con una ID de router más alta.

Haga clic en Falla del nuevo DR en la figura.



En la figura, RouterB falla. Debido a que el RouterD es el BDR actual, éste cambia a DR. El RouterC se convierte en BDR.

Por lo tanto, ¿cómo se asegura el usuario de que los routers que desea que sean DR y BDR ganen la elección? Sin una configuración adicional, la solución es:

- Primero inicie el DR, luego el BDR y luego el resto de los routers, o
- Desconecte la interfaz de todos los routers, luego no shutdown en el DR, el BDR y luego el resto de los routers.

Sin embargo, como ya debe haber deducido, podemos cambiar la prioridad de la interfaz OSPF para controlar mejor nuestras elecciones de DR/BDR.

11.4.3 Prioridad de interfaz OSPF

Debido a que DR se convierte en el punto central de recolección y distribución de las LSA, es importante que este router tenga suficiente capacidad de memoria y CPU para cumplir con la responsabilidad. En vez de confiar en la ID del router para decidir cuáles routers se elegirán como DR y BDR, es mejor controlar la elección de dichos routers con el comando `ip ospf priority interface`.

```
Router(config-if)#ip ospf priority {0 - 255}
```

En nuestra discusión anterior, la prioridad OSPF era igual. Esto se debe a que, de manera predeterminada, el valor de prioridad es 1 para todas las interfaces del router. Por lo tanto, la ID del router determina el DR y el BDR. Sin embargo, si cambia el valor predeterminado de 1 por un valor mayor, el router con la prioridad más alta se convertirá en DR y el router con la

segunda prioridad más alta se convertirá en BDR. Un valor de 0 hace que el router no sea elegible para convertirse en DR ni en BDR.

Debido a que las prioridades son un valor específico según la interfaz, suministran un mejor control de las redes de accesos múltiples de OSPF. También permiten a un router ser DR en una red y DROther en otra.

Haga clic en show ip ospf interface en la figura.

```
RouterA#show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 1
Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
Backup Designated router (ID) 192.168.31.22, Interface address 192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:06
Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.31.22  (Backup Designated Router)
  Adjacent with neighbor 192.168.31.33  (Designated Router)
Suppress hello for 0 neighbor(s)
```

Actualmente todos los routers tienen la prioridad de interfaz OSPF por defecto de 1.

show ip ospf interface Modificar prioridad Forzar elección

Para simplificar nuestro análisis, retiramos el RouterD de la topología. La prioridad de interfaz OSPF puede verse a través del comando show ip ospf interface. En la figura, podemos verificar que la prioridad en el RouterA se encuentra en el valor predeterminado de 1.

Haga clic en Modificar prioridad en la figura.

```
RouterA(config)#interface fastethernet 0/0
RouterA(config-if)#ip ospf priority 200

RouterB(config)#interface fastethernet 0/0
RouterB(config-if)#ip ospf priority 100
```

show ip ospf interface Modificar prioridad Forzar elección

La figura muestra las prioridades de interfaz OSPF del RouterA y el RouterB modificadas para que el RouterA con la prioridad más alta se convierta en DR y el RouterB se convierta en BDR. La prioridad de interfaz OSPF del RouterC continúa en el valor predeterminado 1.

Haga clic en Forzar elección en la figura.



Después de ejecutar shutdown y no shutdown en las interfaces FastEthernet 0/0 de los tres routers, vemos el resultado del cambio de las prioridades de interfaz OSPF. El comando show ip ospf neighbor en el RouterC ahora muestra que el RouterA (ID del router 192.168.31.11) es el DR con la prioridad más alta de interfaz OSPF de 200 y el RouterB (ID del router 192.168.31.22) es aún el BDR, con la segunda prioridad más alta de interfaz OSPF de 100. Observe que el resultado show ip ospf neighbor del RouterA no muestra un DR, ya que el RouterA es el DR real en esta red.

11.5 Mas configuración del OSPF

11.5.1 Redistribución de una ruta OSPF por defecto

Topología

Regresemos a la topología anterior, que ahora incluye un nuevo enlace a ISP. Al igual que con RIP y EIGRP, el router conectado a Internet se utiliza para propagar una ruta por defecto a otros routers en el dominio de enrutamiento OSPF. A este router se lo denomina en ocasiones router de borde, entrada o gateway. Sin embargo, en la terminología OSPF, el router ubicado entre un dominio de enrutamiento OSPF y una red que no es OSPF se denomina Autonomous System Boundary Router (ASBR). En esta topología, Loopback1 (Lo1) representa un enlace a una red que no es OSPF. No configuraremos la red 172.30.1.1/30 como parte del proceso de enrutamiento OSPF.

Haga clic en Configuración estática predeterminada de R1 en la figura.

```

R1(config)#interface loopback 1
R1(config-if)#ip add 172.30.1.1 255.255.255.252
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
R1(config)#router ospf 1
R1(config-router)#default-information originate

```

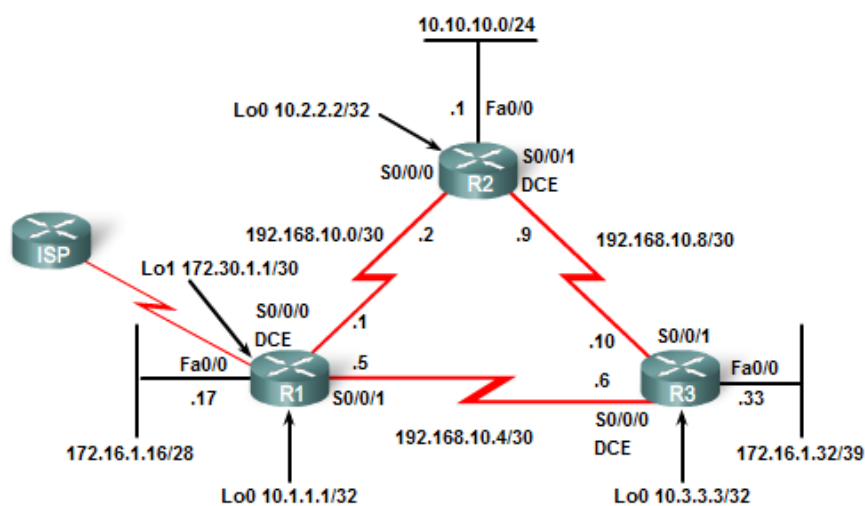
Configuración estática por defecto de R1

R1

R2

R3

Haga clic para ver el resultado del comando.



Configuración estática por defecto de R1

R1

R2

R3

Haga clic para ver el resultado del comando.

La figura muestra el ASBR (R1) configurado con la dirección IP de Loopback1 y el reenvío de tráfico de la ruta estática por defecto al router ISP:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
```

Nota: La ruta estática por defecto utiliza el loopback como una interfaz de salida ya que el router ISP en esta topología no existe físicamente. Al utilizar una interfaz loopback, podemos simular la conexión a otro router.

Al igual que RIP, OSPF requiere el uso del comando default-information originate para publicar la 0.0.0.0/0 ruta estática por defecto a los demás routers del área. Si no se utiliza el comando default-information originate, la ruta por defecto "quad-zero" no se propagará a los demás routers del área OSPF.

La sintaxis del comando es:

R1(config-router)#default-information originate

Haga clic en R1, R2 y R3 en la figura.

R1#show ip route
Codes: <some code output omitted>
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
C 192.168.10.4 is directly connected, Serial0/0/1
O 192.168.10.8 [110/1171] via 192.168.10.6, 00:00:58, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O 172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:58, Serial0/0/1
C 172.16.1.16/28 is directly connected, FastEthernet0/0
172.30.0.0/30 is subnetted, 1 subnets
C 172.30.1.0 is directly connected, Loopback1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O 10.10.10.0/24 [110/1172] via 192.168.10.6, 00:00:58, Serial0/0/1
C 10.1.1.1/32 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, Loopback1

Configuración estática por defecto de R1

R1 R2 R3

R2#show ip route
Codes: <some code output omitted>
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 192.168.10.10 to network 0.0.0.0

192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
O 192.168.10.4 [110/1171] via 192.168.10.10, 00:00:25, Serial0/0/1
C 192.168.10.8 is directly connected, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O 172.16.1.32/29 [110/782] via 192.168.10.10, 00:00:25, Serial0/0/1
O 172.16.1.16/28 [110/1172] via 192.168.10.10, 00:00:25, Serial0/0/1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.2.2.2/32 is directly connected, Loopback0
C 10.10.10.0/24 is directly connected, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.10.10, 00:00:13, Serial0/0/1

Configuración estática por defecto de R1

R1 R2 R3

```
R3#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 192.168.10.10 to network 0.0.0.0

192.168.10.0/30 is subnetted, 3 subnets
O       192.168.10.0 [110/1952] via 192.168.10.5, 00:00:38, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.32/29 is directly connected, FastEthernet0/0
O       172.16.1.16/28 [110/391] via 192.168.10.5, 00:00:38, Serial0/0/0
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.3.3.3/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/782] via 192.168.10.9, 00:00:38, Serial0/0/1
O*E2    0.0.0.0/0 [110/1] via 192.168.10.5, 00:00:27, Serial0/0/0
```

Configuración estática por defecto de R1 R1 R2 **R3**

R1, R2 y R3 ahora presentan un "gateway de último recurso" establecido en la tabla de enrutamiento. Observe la ruta por defecto en R2 y R3 con el OSPF de origen de enrutamiento, pero con el código adicional, E2. Para R2, la ruta es:

```
O*E2 0.0.0.0/0 [110/1] via 192.168.10.10, 00:05:34, Serial0/0/1
```

E2 denota que esta ruta es una ruta OSPF externa Tipo 2.

Las rutas OSPF externas se encuentran en una de las dos siguientes categorías: External Type 1 (Externa Tipo 1, E1) o External Type 2 (Externa Tipo 2, E2). La diferencia entre las dos radica en el modo en que se calcula el costo de OSPF de la ruta en cada router. OSPF acumula costo para una ruta E1, ya que la ruta se propaga a través del área OSPF. Este proceso es idéntico a los cálculos de costo para las rutas internas normales de OSPF. Sin embargo, el costo de una ruta E2 es siempre el costo externo, independientemente del costo interior para alcanzar dicha ruta. En esta topología, debido a que la ruta por defecto tiene un costo externo de 1 en el router R1, R2 y R3 también muestran un costo de 1 para la ruta por defecto E2. Las rutas E2 con un costo de 1 constituyen la configuración OSPF predeterminada. El cambio de dichos valores predeterminados, así como la información adicional acerca de las rutas externas, se analiza en CCNP.

11.5.2 Ajuste OSPF

Ancho de banda de referencia

Como debe recordar, el costo OSPF de Cisco utiliza el ancho de banda acumulado. El valor del ancho de banda de cada interfaz se calcula con $100\,000\,000/\text{ancho de banda}$. Al ancho de banda de referencia se lo conoce como 100 000 000 ó 10 a la octava potencia.

Por lo tanto, 100 000 000 es el ancho de banda predeterminado de referencia cuando el ancho de banda real se convierte en una métrica de costo. Como se vio en estudios anteriores, ahora contamos con velocidades de enlace mucho más rápidas que las velocidades de Fast Ethernet, que incluyen Gigabit Ethernet y 10GigE. Al utilizar un ancho de banda de referencia de 100 000 000 se obtienen interfaces con valores de ancho de banda de 100 Mbps y mayores con el mismo costo OSPF de 1.

Para obtener cálculos de costo más precisos, puede ser necesario ajustar el valor del ancho de banda de referencia. El ancho de banda de referencia puede modificarse para adaptarse a dichos enlaces más rápidos mediante un comando OSPF auto-cost reference-bandwidth. Cuando este comando sea necesario, úselo en todos los routers para que la métrica de enrutamiento de OSPF se mantenga uniforme.

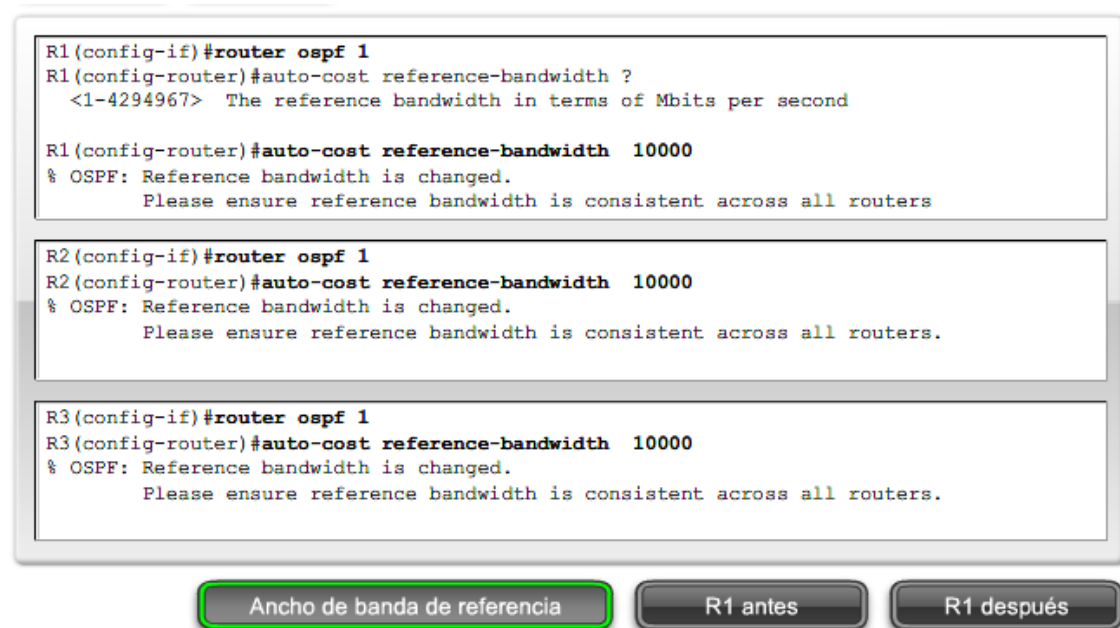
```
R1(config-router)#auto-cost reference-bandwidth ?
```

1-4294967 El ancho de banda de referencia en términos de Mbits por segundo

Observe que el valor se expresa en Mbps. Por lo tanto, el valor predeterminado es equivalente a 100. Para aumentarlo a velocidades de 10GigE, necesitará cambiar el ancho de banda de referencia a 10000.

```
R1(config-router)#auto-cost reference-bandwidth 10000
```

Nuevamente, asegúrese de configurar este comando en todos los routers en el dominio de enrutamiento OSPF. IOS también puede recordárselo, como se muestra en la figura.



Haga clic en R1 antes y R1 después en la figura.

```

R1#show ip route
Codes: <some code output omitted>
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

192.168.10.0/30 is subnetted, 3 subnets
C    192.168.10.0 is directly connected, Serial0/0/0
C    192.168.10.4 is directly connected, Serial0/0/1
O    192.168.10.8 [110/1171] via 192.168.10.6, 00:00:58, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O    172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:58, Serial0/0/1
C    172.16.1.16/28 is directly connected, FastEthernet0/0
172.30.0.0/30 is subnetted, 1 subnets
C    172.30.1.0 is directly connected, Loopback1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O    10.10.10.0/24 [110/1172] via 192.168.10.6, 00:00:58, Serial0/0/1
C    10.1.1.1/32 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1

```

Ancho de banda de referencia

R1 antes

R1 después

```

R1#show ip route
Codes: <some code output omitted>
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

192.168.10.0/30 is subnetted, 3 subnets
C    192.168.10.0 is directly connected, Serial0/0/0
C    192.168.10.4 is directly connected, Serial0/0/1
O    192.168.10.8 [100/117187] via 192.168.10.6, 00:01:33, Serial0/0/1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O    172.16.1.32/29 [110/39162] via 192.168.10.6, 00:01:33, Serial0/0/1
C    172.16.1.16/28 is directly connected, FastEthernet0/0
172.30.0.0/30 is subnetted, 1 subnets
C    172.30.1.0 is directly connected, Loopback1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O    10.10.10.0/24 [110/117287] via 192.168.10.6, 00:01:33, Serial0/0/0
C    10.1.1.1/32 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1

```

Ancho de banda de referencia

R1 antes

R1 después

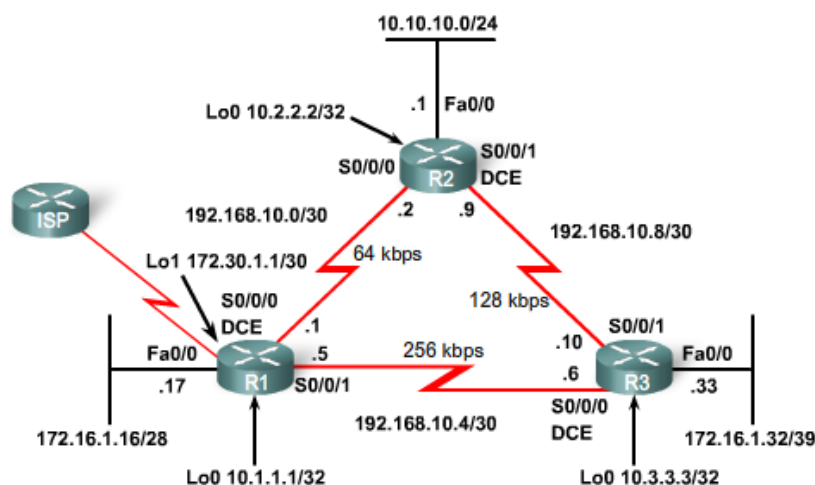
La tabla de enrutamiento de R1 muestra el cambio en la métrica de costo de OSPF. Observe que los valores presentan valores de costo mucho mayores para las rutas OSPF. Por ejemplo, en R1 antes, el costo para 10.10.10.0/24 es 1172. Después de configurar un nuevo ancho de banda de referencia, el costo para la misma ruta es ahora 65635.

Modificación de intervalos OSPF

Resultado
del router



Topología con conexión ISP



R1 Vecinos 1

Modificar temporizadores R1

R1 Vecinos 2

Temporizadores R2

Modificar temporizadores R2

R1 Vecinos 3

Haga clic para ver el resultado del comando.

Haga clic en Vecinos de R1 1 en la figura.

R1#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/ -	00:00:35	192.168.10.6	Serial10/0/1
10.2.2.2	0	FULL/ -	00:00:36	192.168.10.2	Serial10/0/0

R1 Vecinos 1

Modificar temporizadores R1

R1 Vecinos 2

Temporizadores R2

Modificar temporizadores R2

R1 Vecinos 3

Haga clic para ver el resultado del comando.

El comando show ip ospf neighbor en R1 verifica que R1 sea adyacente a R2 y R3. Observe en el resultado que el Tiempo muerto cuenta regresivamente a partir de los 40 segundos. De manera predeterminada, este valor se actualiza cada 10 segundos cuando R1 recibe un saludo del vecino.

Puede ser aconsejable cambiar los temporizadores OSPF para que los routers detecten las fallas de red en menor tiempo. Si bien al hacerlo se aumentará el tráfico, en ocasiones se necesita una convergencia rápida que compense el tráfico adicional.

Los intervalos muertos y de saludo de OSPF pueden modificarse manualmente con los siguientes comandos de interfaz:

```
Router(config-if)#ip ospf hello-intervalseconds
```

```
Router(config-if)#ip ospf dead-intervalseconds
```

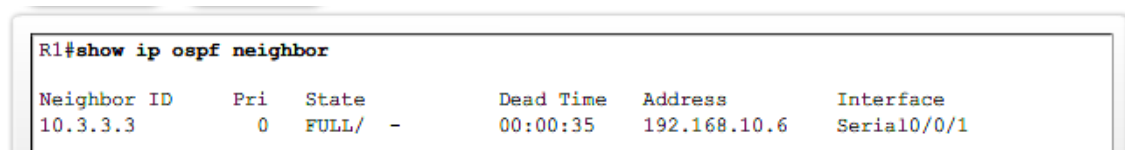
Haga clic en Modificar temporizadores de R1 en la figura.

La figura muestra los intervalos muerto y de saludo modificados a 5 y 20 segundos, respectivamente, en la interfaz Serial 0/0/0 para R1. Inmediatamente después de cambiar el intervalo de saludo, el IOS de Cisco modifica automáticamente el intervalo muerto a un valor equivalente a cuatro veces el intervalo de saludo. Sin embargo, siempre es aconsejable modificar explícitamente el temporizador en lugar de depender de la función automática de IOS para que las modificaciones se documenten en la configuración.

Después de 20 segundos, expira el Temporizador muerto en R1. R1 y R2 pierden adyacencia. Sólo modificamos los valores en un lado del enlace serial entre R1 y R2.

```
%OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL to DOWN,  
Neighbor Down: El temporizador muerto expiró
```

Haga clic en Vecinos de R1 2 en la figura.



Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/-	00:00:35	192.168.10.6	Serial0/0/1

Recuerde, los intervalos muerto y de saludo de OSPF deben ser equivalentes entre vecinos. Puede verificar la pérdida de adyacencia con el comando `show ip ospf neighbor` en R1. Observe que el vecino 10.2.2.2 ya no se encuentra presente. Sin embargo, 10.3.3.3 o R3 aún es un vecino. Los temporizadores establecidos en Serial 0/0/0 no afectan la adyacencia de vecinos con R3.

Haga clic en Temporizadores de R2 en la figura.

```

R2#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
Internet Address 192.168.10.2/30, Area 0
Process ID 1, Router ID 10.2.2.2, Network Type POINT_TO_POINT, Cost: 65535
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:09
Supports Link-local Signaling (LLS)
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

Los intervalos muerto y de saludo incompatibles pueden verificarse en R2 con el comando `show ip ospf interface serial 0/0/0`. Los valores de intervalos en R2, ID del router 10.2.2.2, aún están establecidos con un intervalo de saludo de 10 segundos y un intervalo muerto de 40 segundos.

Haga clic en Modificar temporizadores de R2 en la figura.

```

R2(config)#interface serial 0/0/0
R2(config-if)#ip ospf hello-interval 5
R2(config-if)#ip ospf dead-interval 20
R2(config-if)#end
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done

```

Para restaurar la adyacencia entre R1 y R2, modifique los intervalos muerto y de saludo en la interfaz Serial 0/0/0 en R2 para hacer coincidir los intervalos de la interfaz Serial 0/0/0 en R1. IOS muestra un mensaje que indica que se estableció la adyacencia con un estado FULL.

14:22:27: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0 from LOADING to FULL, Loading Done

Haga clic en Vecinos de R1 3 en la figura.

```

R1#show ip ospf neighbor

```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/ -	00:00:36	192.168.10.6	Serial0/0/1
10.2.2.2	0	FULL/ -	00:00:17	192.168.10.2	Serial0/0/0

Verifique que se restaure la adyacencia de vecinos con el comando `show ip ospf neighbor` en R1. Observe que el Tiempo muerto para Serial 0/0/0 es ahora muy inferior, ya que cuenta regresivamente a partir de los 20 segundos en lugar de los 40 segundos predeterminados. Serial 0/0/1 aún funciona con los temporizadores predeterminados.

Nota: OSPF requiere que los intervalos muerto y de saludo coincidan entre dos routers para que sean adyacentes. Esto es distinto de EIGRP, donde los temporizadores de saludo y de espera no necesitan coincidir para que dos routers formen una adyacencia EIGRP.

Resumen

OSPF (Open Shortest Path First) es un protocolo de enrutamiento de estado de enlace sin clase. La versión actual de OSPF para IPv4 es OSPFv2, introducida en RFC 1247 y actualizada en RFC 2328 por John Moy. En 1999, OSPFv3 para IPv6 se publicó en RFC 2740.

OSPF tiene una distancia administrativa predeterminada de 110 y se indica en la tabla de enrutamiento con un código de origen de ruta de O. OSPF se habilita con el comando de configuración global `router ospf process-id`. El comando `process-id` es significativo a nivel local, lo que implica que no necesita coincidir con otros routers OSPF para establecer adyacencias con dichos vecinos.

El comando `network` utilizado con OSPF tiene la misma función que cuando se utiliza con otros protocolos de enrutamiento IGP, pero con una sintaxis ligeramente diferente.

`Router(config-router)#network network-address wildcard-mask area area-id`

wildcard-mask es lo inverso a la máscara de subred y area-id debería establecerse en 0.

OSPF no utiliza un protocolo de capa de transporte ya que los paquetes OSPF se envían directamente a través de IP. OSPF utiliza el paquete de saludo OSPF para establecer adyacencias de vecinos. De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos multiacceso y punto a punto, y cada 30 segundos en segmentos multiacceso sin broadcast (NBMA) (Frame Relay, X.25, ATM). El intervalo muerto es el período de tiempo que un router OSPF esperará antes de finalizar la adyacencia con un vecino. De manera predeterminada, el intervalo muerto es equivalente a cuatro veces el valor del intervalo de saludo. En el caso de los segmentos multiacceso y punto a punto, dicho período es de 40 segundos. En el caso de las redes NBMA, el intervalo muerto es de 120 segundos.

Para que los routers sean adyacentes, deben coincidir sus intervalos de saludo, intervalos muertos, tipos de red y máscaras de subred. El comando `show ip ospf neighbors` puede usarse para verificar las adyacencias OSPF.

La ID del router OSPF se utiliza para identificar en forma exclusiva cada router en el dominio de enrutamiento OSPF. Los routers de Cisco obtienen la ID del router conforme a tres criterios y con la siguiente prioridad:

1. Utilizar la dirección IP configurada con el comando `router-id` de OSPF.
2. Si `router-id` no está configurado, el router elige la dirección IP más alta de cualquiera de sus interfaces loopback.
3. Si no hay ninguna interfaz loopback configurada, el router elige la dirección IP activa más alta de cualquiera de sus interfaces físicas.

RFC 2328 no especifica los valores que deberían utilizarse para determinar el costo. El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el router hasta la red de destino como valor del costo.

Las redes de accesos múltiples pueden crear dos desafíos para OSPF en relación con la saturación de las LSA, incluida la creación de adyacencias múltiples: una adyacencia para cada par de routers y extensa saturación de las LSA (Notificaciones de estado de enlace). OSPF elige un DR (Router designado) para que actúe como punto de recolección y distribución de las LSA enviadas y recibidas en la red de accesos múltiples. Se elige un BDR (Router designado de respaldo) para que asuma el rol de DR en caso de que el DR falle. Todos los demás routers se conocen como DROthers. Todos los routers envían sus LSA al DR, que luego satura con la LSA todos los demás routers en la red de accesos múltiples.

El router con la ID del router más alta es el DR y el router con la segunda ID del router más alta es el BDR. Esto puede reemplazarse por el comando `ip ospf priority` en dicha interfaz. De manera predeterminada, `ip ospf priority` es "1" en todas las interfaces de accesos múltiples. Si hay un router configurado con el nuevo valor de prioridad, el router con el valor de prioridad más alto es el DR, y el router con el siguiente valor de prioridad más alto es el BDR. Un valor de prioridad "0" significa que el router no es elegible para convertirse en DR ni en BDR.

Se propaga una ruta por defecto en OSPF similar a la de RIP. El comando de modo de router de OSPF, `default-information originate`, se utiliza para propagar una ruta estática por defecto.

El comando `show ip protocols` se utiliza para verificar información importante de configuración de OSPF, incluida la ID del proceso OSPF, la ID del router y las redes que publica el router.

