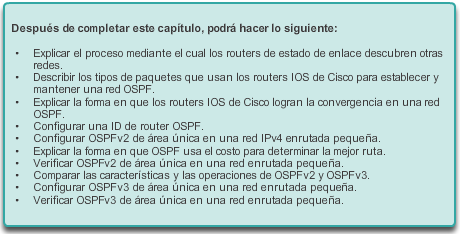
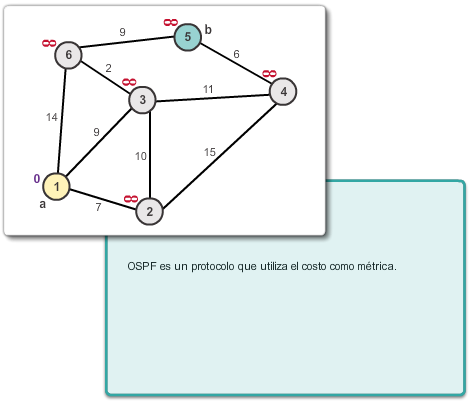
# OSPF de área única

## Introducción

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace desarrollado como reemplazo del protocolo de routing vector distancia RIP. Durante los comienzos de la tecnología de redes y de Internet, RIP era un protocolo de routing aceptable. Sin embargo, el hecho de que RIP dependiera del conteo de saltos como única métrica para determinar la mejor ruta rápidamente se volvió problemático. El uso del conteo de saltos no escala bien en redes más grandes con varias rutas de distintas velocidades. OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. En este capítulo, se abarcan las implementaciones y configuraciones básicas de OSPF de área única.





## Características de OSPF

### Open Shortest Path First

Como se muestra en la figura 1, OSPF versión 2 (OSPFv2) se encuentra disponible para IPv4, mientras que OSPF versión 3 (OSPFv3) se encuentra disponible para IPv6.

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 era fundamentalmente una red académica y de investigación financiada por el gobierno de los EE.UU.

En 1989, se publicó la especificación para OSPFv1 en RFC 1131. Se escribieron dos implementaciones. Una implementación se desarrolló para ejecutarse en routers, y la otra se desarrolló para ejecutarse en estaciones de trabajo UNIX. Esta última implementación se convirtió en un proceso UNIX generalizado que se conoce como GATED. OSPFv1 era un protocolo de routing experimental y nunca se implementó.

En 1991, John Moy introdujo OSPFv2 en RFC 1247. OSPFv2 ofrecía significativas mejoras técnicas con respecto a OSPFv1. Por su diseño, es un protocolo sin clase, de modo que admite VLSM y CIDR.

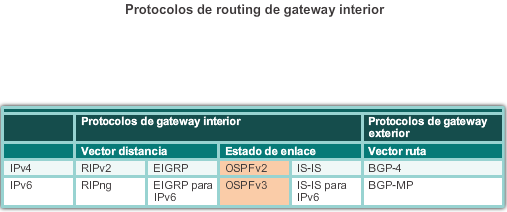
Al mismo tiempo que se presentó OSPF, ISO trabajaba en un protocolo de routing de estado de enlace propio, Intermediate System-to-Intermediate System (IS-IS). El IETF eligió OSPF como protocolo de gateway interior (IGP) recomendado.

En 1998, se actualizó la especificación OSPFv2 en RFC 2328, que en la actualidad sigue siendo la RFC para OSPF.

En 1999, OSPFv3 para IPv6 se publicó en RFC 2740. OSPF para IPv6, creado por John Moy, Rob Coltun y Dennis Ferguson, no solo es una nueva implementación de protocolo para IPv6, sino también una importante reforma del funcionamiento del protocolo.

En 2008, se actualizó OSPFv3 en RFC 5340 como OSPF para IPv6.

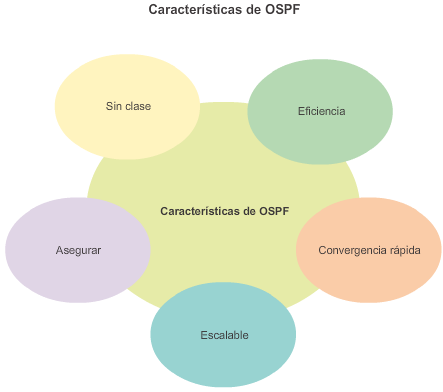
**Nota:** en este capítulo, a menos que se identifique explícitamente como OSPFv2 u OSPFv3, el término OSPF se utiliza para indicar conceptos que comparten ambas versiones.



Las características de OSPF, las cuales se muestran en la figura 1, incluyen lo siguiente:

* **Sin clase:** por su diseño, es un protocolo sin clase, de modo que admite VLSM y CIDR.
* **Eficaz:** los cambios de routing dirigen actualizaciones de routing (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.
* **Convergencia rápida:** propaga rápidamente los cambios que se realizan a la red.
* **Escalable:** funciona bien en tamaños de redes pequeños y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
* **Seguro:** admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de peers con la misma contraseña compartida previamente.

La distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110. Como se muestra en la figura 2, se prefiere OSPF a IS-IS y RIP.





Todos los protocolos de routing comparten componentes similares. Todos usan mensajes de protocolo de routing para intercambiar información de la ruta. Los mensajes contribuyen a armar estructuras de datos, que luego se procesan con un algoritmo de routing.

Los tres componentes principales del protocolo de routing OSPF incluyen lo siguiente:

**Estructuras de datos**

OSPF crea y mantiene tres bases de datos (consulte la figura 1):

* **Base de datos de adyacencia:** crea la tabla de vecinos.
* **Base de datos de estado de enlace (LSDB):** crea la tabla de topología.
* **Base de datos de reenvío:** crea la tabla de routing.

Estas tablas contienen una lista de routers vecinos para intercambiar información de routing, y se guardan y mantienen en la RAM.

**Mensajes de protocolo de routing**

OSPF intercambia mensajes para transmitir información de routing mediante cinco tipos de paquetes. Estos paquetes, los cuales se muestran en la figura 2, son los siguientes:

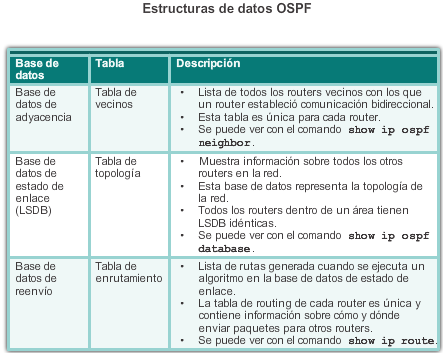
* Paquete de saludo
* Paquete de descripción de la base de datos
* Paquete de solicitud de estado de enlace
* Paquete de actualización de estado de enlace
* Paquete de acuse de recibo de estado de enlace

Estos paquetes se usan para descubrir routers vecinos y también para intercambiar información de routing a fin de mantener información precisa acerca de la red.

**Algoritmo**

La CPU procesa las tablas de vecinos y de topología mediante el algoritmo SPF de Dijkstra. El algoritmo SPF se basa en el costo acumulado para llegar a un destino.

El algoritmo SPF crea un árbol SPF posicionando cada router en la raíz y calculando la ruta más corta hacia cada nodo. Luego, el árbol SPF se usa para calcular las mejores rutas. OSPF coloca las mejores rutas en la base de datos de reenvío, que se usa para la tabla de routing.





A fin de mantener la información de routing, los routers OSPF realizan el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia:

1. Establecimiento de las adyacencias de vecinos (figura 1): los routers con OSPF habilitado deben reconocerse entre sí en la red antes de poder compartir información. Los routers con OSPF habilitado envían paquetes de saludo por todas las interfaces con OSPF habilitado para determinar si hay vecinos presentes en esos enlaces. Si se detecta un vecino, el router con OSPF habilitado intenta establecer una adyacencia de vecino con ese vecino.

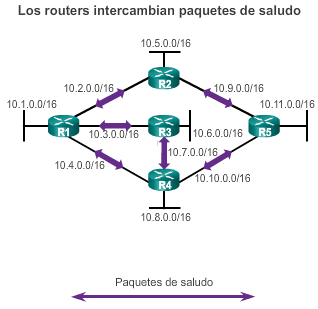
2. Intercambio de notificaciones de estado de enlace (figura 2): una vez que se establecen las adyacencias, los routers intercambian notificaciones de estado de enlace (LSA). Las LSA contienen el estado y el costo de cada enlace conectado directamente. Los routers saturan a los vecinos adyacentes con sus LSA. Los vecinos adyacentes que reciben las LSA saturan de inmediato a otros vecinos conectados directamente, hasta que todos los routers en el área tengan todas las LSA.

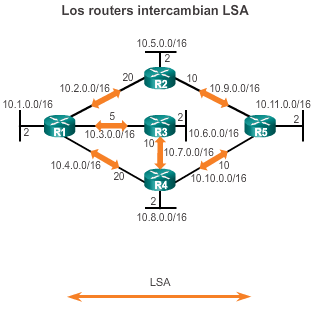
3. Creación de la tabla de topología (figura 3): una vez que se reciben las LSA, los routers con OSPF habilitado crean la tabla de topología (LSDB) sobre la base de las LSA recibidas. Finalmente, esta base de datos contiene toda la información sobre la topología de la red.

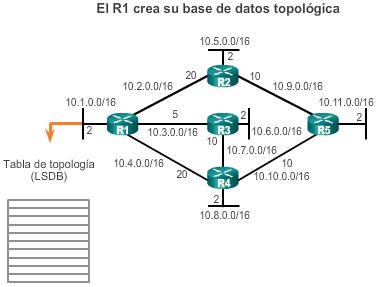
4. Ejecución del algoritmo SPF (figuras 4 y 5): a continuación, los routers ejecutan el algoritmo SPF. Los engranajes que se muestran en la ilustración se utilizan para indicar la ejecución del algoritmo SPF. El algoritmo SPF crea el árbol SPF.

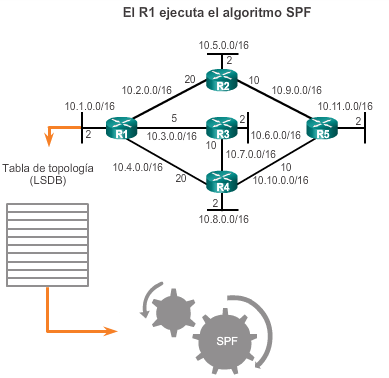
En la figura 6, se muestra el contenido del árbol SPF del R1.

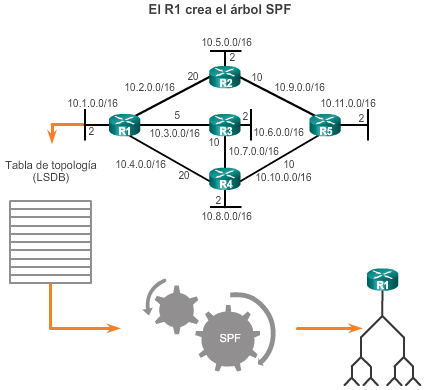
Las mejores rutas del árbol SPF se insertan en la tabla de routing. Las decisiones de routing se toman sobre la base de las entradas de la tabla de routing.

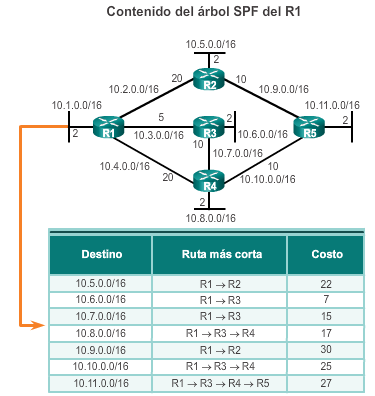












Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB.

OSPF se puede implementar de dos maneras:

* **OSPF de área única:** en la figura 1, todos los routers se encuentran en un área llamada “área backbone” (área 0).
* **OSPF multiárea:** en la figura 2, OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área backbone (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

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

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

**Nota:** los cambios de topología se distribuyen a los routers de otras áreas en formato vector distancia. En otras palabras, estos routers solo actualizan sus tablas de routing y no necesitan volver a ejecutar el algoritmo SPF.

Si hubiera demasiados routers en un área, la LSDB sería muy grande y se incrementaría la carga en la CPU. Por lo tanto, la disposición de los routers en distintas áreas divide de manera eficaz una base de datos potencialmente grande en bases de datos más pequeñas y más fáciles de administrar.

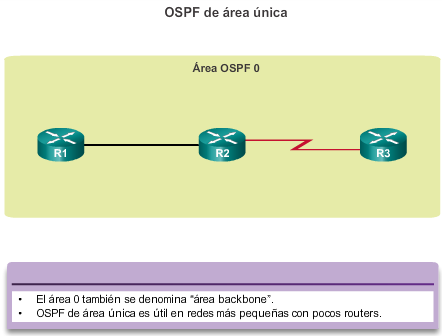
Las posibilidades de topología jerárquica de OSPF multiárea presentan las siguientes ventajas:

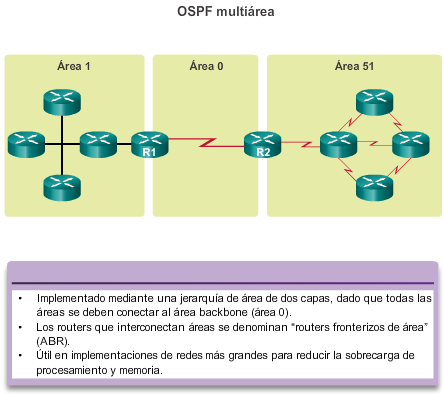
* **Tablas de routing más pequeñas:** se crean menos entradas de tabla de routing, ya que las direcciones de red pueden resumirse entre áreas. La sumarización de ruta no está habilitada de manera predeterminada.
* **Menor sobrecarga de actualización de estado de enlace:** minimiza los requisitos de procesamiento y memoria.
* **Menor frecuencia de cálculos de SPF:** localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de las actualizaciones de routing debido a que la saturación con LSA se detiene en el límite del área.

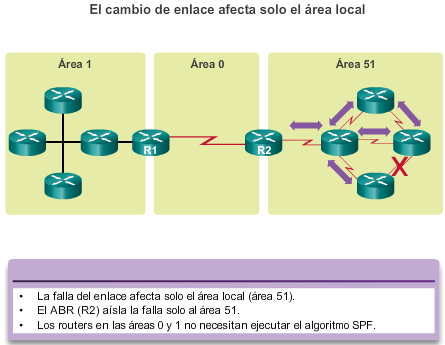
En la figura 3, se ilustran estas ventajas.

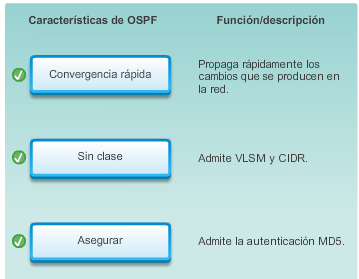
Por ejemplo, el R2 es un ABR para el área 51. Como ABR, resumiría las rutas del área 51 en el área 0. Cuando uno de los enlaces resumidos falla, las LSA se intercambian solo dentro del área 51. Los routers del área 51 deben volver a ejecutar el algoritmo SPF para identificar las mejores rutas. Sin embargo, los routers del área 0 y el área 1 no reciben ninguna actualización, motivo por el cual no ejecutan el algoritmo SPF.

Este capítulo se centra en OSPF de área única.





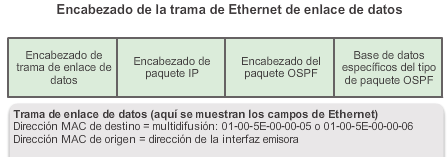


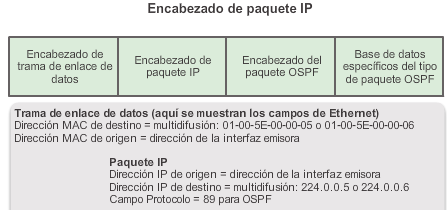


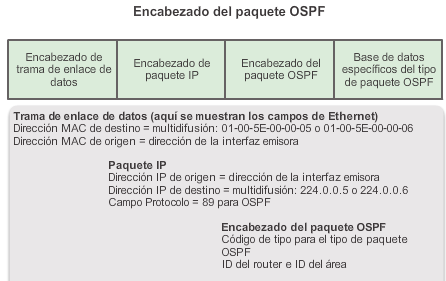
### Mensajes OSPF

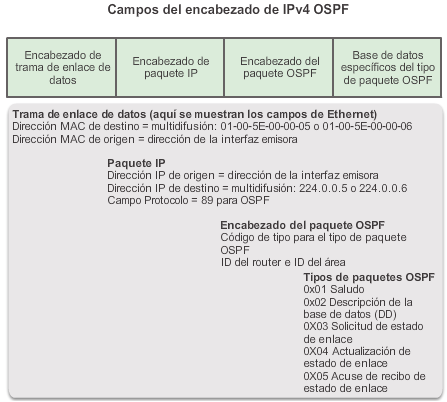
Los mensajes OSPF que se transmiten a través de un enlace Ethernet contienen la siguiente información:

* **Encabezado de la trama de Ethernet de enlace de datos:**identifica las direcciones MAC de multidifusión de destino 01-00-5E-00-00-05 o 01-00-5E-00-00-06. (figura 1)
* **Encabezado del paquete IP:**identifica el campo 89 del protocolo IPv4, que indica que se trata de un paquete OSPF. También identifica una de dos direcciones OSPF de multidifusión, 224.0.0.5 o 224.0.0.6. (Figura 2)
* **Encabezado del paquete OSPF:**identifica el tipo de paquete OSPF, la ID del router y la ID del área. (Figura 3)
* **Datos específicos del tipo de paquete OSPF:** contiene información del tipo de paquete OSPF. El contenido varía según el tipo de paquete. En este caso, se trata de un encabezado de IPv4. (figura 4)





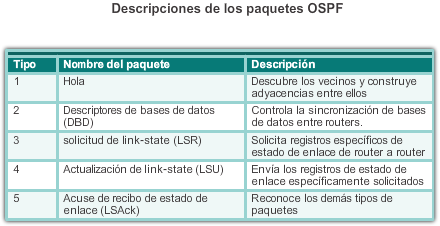




OSPF utiliza paquetes de estado de enlace (LSP) para establecer y mantener adyacencias de vecinos, así como para intercambiar actualizaciones de routing.

En la ilustración, se muestran los cinco tipos de LSP que usa OSPF. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

* **Tipo 1, paquete de saludo:** se usa para establecer y mantener la adyacencia con otros routers OSPF.
* **Tipo 2, paquete de descripción de base de datos (DBD):** contiene una lista abreviada de la LSDB del router emisor, y los routers receptores la usan para compararla con la LSDB local. Para crear un árbol SPF preciso, la LSDB debe ser idéntica en todos los routers de estado de enlace dentro de un área.
* **Tipo 3, paquete de solicitud de estado de enlace (LSR):** los routers receptores pueden requerir más información sobre cualquier entrada de la DBD mediante el envío de un LSR.
* **Tipo 4, paquete de actualización de estado de enlace (LSU)**: se utiliza para responder a los LSR y anunciar la nueva información. Los LSU contienen siete tipos de LSA.
* **Tipo 5, paquete de acuse de recibo de estado de enlace (LSAck):** cuando se recibe una LSU, el router envía un LSAck para confirmar la recepción de la LSU. El campo de datos del LSAck está vacío.



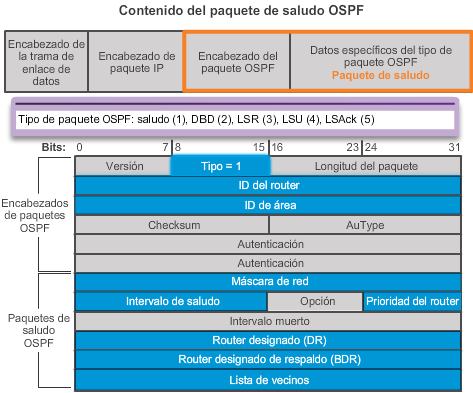
**Paquete de saludo**

El paquete OSPF de tipo 1 es el paquete de saludo. 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 enlaces punto a punto no requieren DR o BDR.

En la ilustración, se muestran los campos contenidos en el paquete de tipo 1, el paquete de saludo. Los campos importantes que se muestran en la figura incluyen:

* **Tipo:** identifica el tipo de paquete. Un uno (1) indica un paquete de saludo. Un valor de 2 identifica un paquete DBD, un valor de 3 identifica un paquete LSR, un valor de 4 identifica un paquete LSU, y un valor de 5 identifica un paquete LSAck.
* **ID del router:** un valor de 32 bits expresado en notación decimal con puntos (una dirección IPv4) que se utiliza para identificar exclusivamente el router de origen.
* **ID de área:** el área en la cual se originó el paquete.
* **Máscara de red:** la máscara de subred asociada a la interfaz emisora.
* **Intervalo de saludo:** especifica la frecuencia, en segundos, a la que un router envía paquetes de saludo. El intervalo de saludo predeterminado en redes de accesos múltiples es de 10 segundos. Este temporizador debe ser el mismo en los routers vecinos; de lo contrario, no se establece ninguna adyacencia.
* **Prioridad del router:** se utiliza en una elección de DR/BDR. La prioridad predeterminada para todos los routers OSPF es 1, pero se puede modificar manualmente desde 0 hasta 255. Cuanto mayor es el valor, mayor es la probabilidad de que el router sea el DR en el enlace.
* **Intervalo muerto:** es el tiempo en segundos que espera un router para establecer comunicación con un vecino antes de declarar que el router vecino no funciona. De manera predeterminada, el intervalo muerto del router es cuatro veces el intervalo de saludo. Este temporizador debe ser el mismo en los routers vecinos; de lo contrario, no se establece ninguna adyacencia.
* **Router designado (DR):** la ID del router del DR.
* **Router designado de respaldo (BDR):** la ID del router del BDR.
* **Lista de vecinos:** la lista en la que se identifican las ID del router de todos los routers adyacentes.



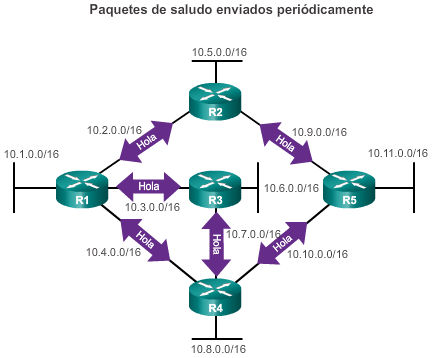
Como se muestra en la ilustración, los paquetes de saludo OSPF se transmiten a la dirección de multidifusión 224.0.0.5 en IPv4 y FF02::5 en IPv6 (todos los routers OSPF) cada:

* 10 segundos (intervalo predeterminado en redes de accesos múltiples y punto a punto)
* 30 segundos (intervalo predeterminado en redes multiacceso sin difusión [NBMA], por ejemplo, Frame Relay)

El intervalo muerto es el período que el router espera para recibir un paquete de saludo antes de declarar al vecino como inactivo. Si el intervalo muerto caduca antes de que los routers reciban un paquete de saludo, OSPF elimina ese vecino de su LSDB. El router satura la LSDB con información acerca del vecino inactivo por todas las interfaces con OSPF habilitado.

Cisco utiliza un intervalo predeterminado de cuatro veces el intervalo de saludo:

* 40 segundos (intervalo predeterminado en redes de accesos múltiples y punto a punto)
* 120 segundos (intervalo predeterminado en redes NBMA, por ejemplo, Frame Relay.



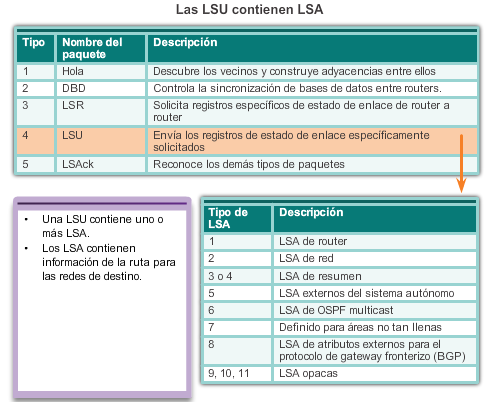
Los routers inicialmente intercambian paquetes DBD de tipo 2, que son una lista abreviada de la LSDB del router emisor que los routers receptores usan para compararla con la LSDB local.

Los routers receptores usan paquetes LSR de tipo 3 para solicitar más información acerca de una entrada de la DBD.

El paquete LSU de tipo 4 se utiliza para responder a un paquete LSR.

Los paquetes LSU también se usan para reenviar actualizaciones de routing OSPF, como cambios de enlace. Específicamente, un paquete LSU puede contener 11 tipos de LSA OSPFv2, como se muestra en la ilustración. OSPFv3 cambió el nombre de varias de estas LSA y también contiene dos LSA adicionales.

**Nota:** en ocasiones, la diferencia entre los términos LSU y LSA puede resultar confusa, ya que a menudo se usan de manera indistinta. Sin embargo, una LSU contiene una o más LSA.





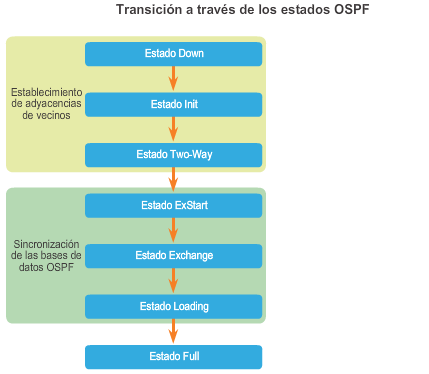
### Funcionamiento de OSPF

Cuando un router OSPF se conecta inicialmente a una red, intenta hacer lo siguiente:

* Crear adyacencias con los vecinos
* Intercambiar información de routing
* Calcular las mejores rutas
* Lograr la convergencia

Al intentar lograr la convergencia, OSPF atraviesa varios estados:

* Estado Down
* Estado Init
* Estado Two-Way
* Estado ExStart
* Estado Exchange
* Estado Loading
* Estado Full



Cuando se habilita OSPF en una interfaz, el router debe determinar si existe otro vecino OSPF en el enlace. Para hacerlo, el router reenvía un paquete de saludo con la ID del router por todas las interfaces con OSPF habilitado. El proceso OSPF utiliza la ID del router OSPF para identificar cada router en el área OSPF de manera exclusiva. Una ID de router es una dirección IP asignada para identificar un router específico entre peers OSPF.

Cuando un router vecino con OSPF habilitado recibe un paquete de saludo con una ID de router que no figura en su lista de vecinos, el router receptor intenta establecer una adyacencia con el router que inició la comunicación.

Consulte el R1 de la figura 1. Cuando se habilita OSPF, la interfaz Gigabit Ethernet 0/0 habilitada pasa del estado Down al estado Init. El R1 comienza a enviar paquetes de saludo por todas las interfaces con OSPF habilitado para descubrir vecinos OSPF a fin de desarrollar adyacencias con ellos.

En la figura 2, el R2 recibe el paquete de saludo del R1 y agrega la ID del router R1 a su lista de vecinos. A continuación, el R2 envía un paquete de saludo al R1. El paquete contiene la ID del router R2 y la ID del router R1 en la lista de vecinos de la misma interfaz.

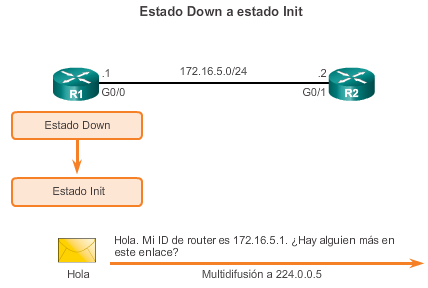
En la figura 3, el R1 recibe el saludo y agrega la ID del router R2 a su lista de vecinos OSPF. También advierte su propia ID de router en la lista de vecinos del paquete de saludo. Cuando un router recibe un paquete de saludo en el que se indica su ID de router en la lista de vecinos, el router pasa del estado Init al estado Two-Way.

La acción realizada en el estado Two-Way depende del tipo de interconexión de los routers adyacentes:

* Si los dos vecinos adyacentes se interconectan a través de un enlace punto a punto, pasan de inmediato del estado Two-Way a la fase de sincronización de bases de datos.
* Si los routers se interconectan a través de una red Ethernet común, se debe elegir un router designado DR y un BDR.

Debido a que el R1 y el R2 se interconectan a través de una red Ethernet, se elije un DR y un BDR. Como se muestra en la figura 4, el R2 se convierte en el DR, y el R1 es el BDR. Este proceso tiene lugar solo en las redes de accesos múltiples, como las LAN Ethernet.

Los paquetes de saludo se intercambian continuamente para mantener la información del router.



¿Por qué se necesita elegir un DR y un BDR?

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

* **Creación de varias adyacencias:** las redes Ethernet podrían interconectar muchos routers OSPF con un enlace común. La creación de adyacencias con cada router es innecesaria y no se recomienda, ya que conduciría al intercambio de una cantidad excesiva de LSA entre routers en la misma red.
* **Saturación intensa con LSA:** los routers de estado de enlace saturan con sus LSA cada vez que se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.

Para comprender el problema de las adyacencias múltiples, se debe estudiar una fórmula:

Para cualquier cantidad de routers (designada como *n*) en una red de accesos múltiples, hay *n* (*n* – 1) / 2 adyacencias.

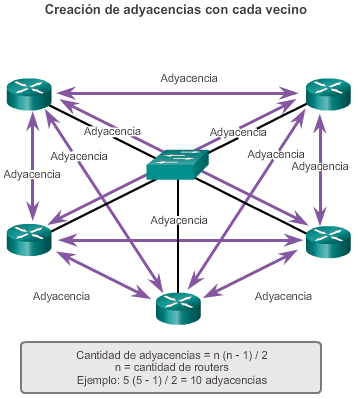
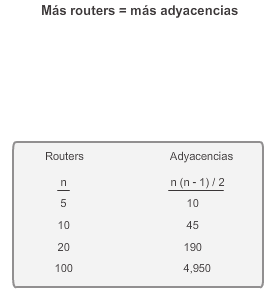
En la figura 1, se muestra una topología simple de cinco routers, los cuales están conectados a la misma red Ethernet de accesos múltiples. Sin ningún tipo de mecanismo para reducir la cantidad de adyacencias, estos routers en forma colectiva formarán 10 adyacencias:

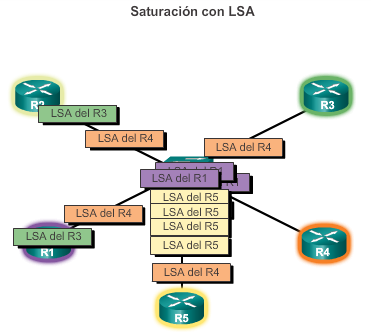
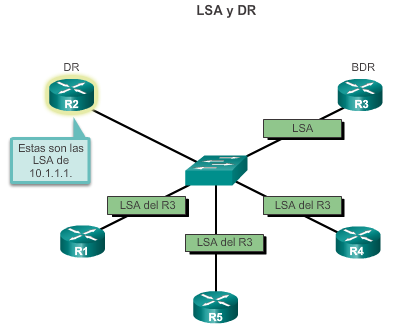
5 (5 – 1) / 2 = 10

Puede parecer poco, pero a medida que se agregan routers a la red, la cantidad de adyacencias aumenta notablemente, como se muestra en la figura 2.

Para comprender el problema de la saturación intensa con LSA, reproduzca la animación de la figura 3. En la animación, el R2 envía una LSA. Este evento hace que cada router también envíe una LSA. Los acuses de recibo requeridos que se envían por cada LSA recibida no se muestran en la animación. 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.

La solución para administrar la cantidad de adyacencias y la saturación con LSA en una red de accesos múltiples es el DR. En las redes de accesos múltiples, OSPF elige un DR para que funcione como punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un BDR en caso de que falle el DR. Todos los otros routers se convierten en DROTHER. Un DROTHER es un router que no funciona como DR ni como BDR.





Después del estado Two-Way, los routers pasan a los estados de sincronización de bases de datos. Mientras que el paquete de saludo se utilizó para establecer adyacencias de vecinos, los otros cuatro tipos de paquetes OSPF se utilizan durante el proceso de intercambio y sincronización de LSDB.

En el estado ExStart, se crea una relación de maestro y esclavo entre cada router y su DR y su BDR adyacentes. El router con la mayor ID de router funciona como maestro para el estado Exchange. En la figura 1, el R2 se convierte en maestro.

En el estado Exchange, los routers maestros y esclavos intercambian uno o más paquetes DBD. Un paquete DBD incluye información acerca del encabezado de la entrada de LSA que aparece en la LSDB del router. Las entradas pueden hacer referencia a un enlace o a una red. Cada encabezado de entrada de LSA incluye información acerca del tipo de estado de enlace, la dirección del router que realiza el anuncio, el costo del enlace y el número de secuencia. El router usa el número de secuencia para determinar qué tan nueva es la información recibida.

En la figura 2, el R2 envía un paquete DBD al R1. Cuando el R1 recibe la DBD, realiza las siguientes acciones:

1. Confirma la recepción de la DBD con el paquete LSAck.

2. A continuación, el R1 envía paquetes DBD al R2.

3. El R2 acusa recibo al R1.

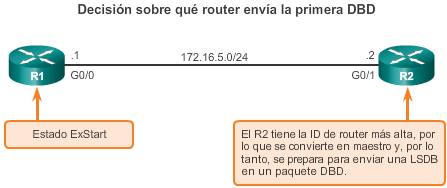
El R1 compara la información recibida con la información que tiene en su propia LSDB. Si el paquete DBD tiene una entrada de estado de enlace más actual, el router pasa al estado Loading.

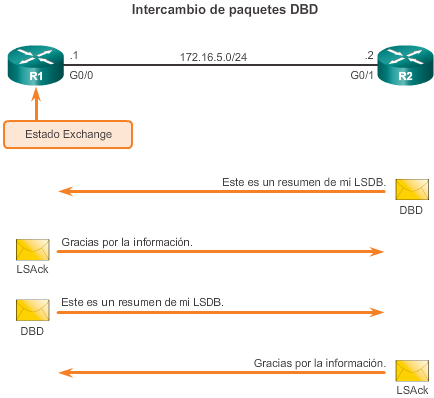
Por ejemplo, en la figura 3, el R1 envía una LSR con respecto a la red 172.16.6.0 al R2. El R2 responde con la información completa sobre 172.16.6.0 en un paquete LSU. Una vez más, cuando el R1 recibe una LSU, envía un LSAck. A continuación, el R1 agrega las nuevas entradas de estado de enlace a su LSDB.

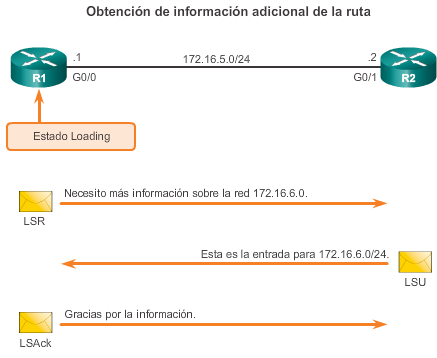
Después de cumplir con todas las LSR para un router determinado, los routers adyacentes se consideran sincronizados y en estado Full.

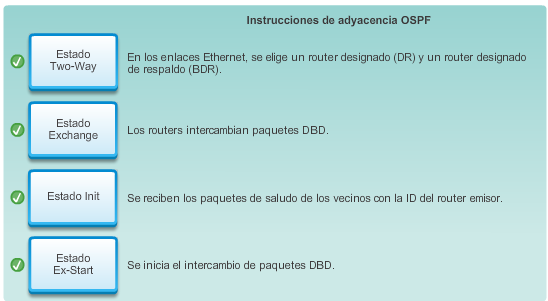
En la medida en que los routers vecinos sigan recibiendo paquetes de saludo, la red en las LSA transmitidas permanece en la base de datos de topología. Una vez que se sincronizan las bases de datos topológicas, se envían actualizaciones (LSU) a los vecinos solo en las siguientes circunstancias:

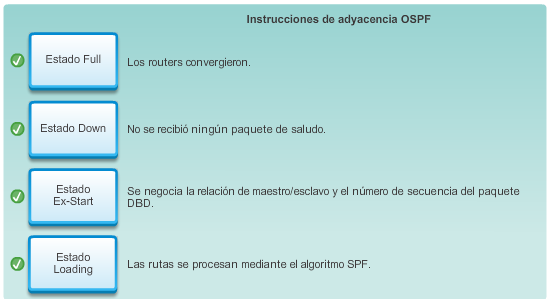
* Cuando se percibe un cambio (actualizaciones incrementales).
* Cada 30 minutos.











## Configuración de OSPFv2 de área única

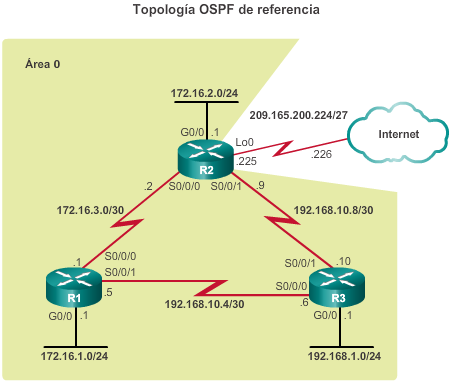
### ID del router OSPF

OSPFv2 es un protocolo de routing de estado de enlace para IPv4 que se presentó en 1991. OSPF se diseñó como alternativa a otro protocolo de routing IPv4, RIP.

En la ilustración, se muestra la topología que se usa para configurar OSPFv2 en esta sección. Es posible que los tipos de interfaces seriales y sus anchos de banda asociados no reflejen necesariamente los tipos de conexiones más frecuentes que se encuentran en las redes en la actualidad. Los anchos de banda de los enlaces seriales que se usan en esta topología se eligieron para ayudar a explicar el cálculo de las métricas de los protocolos de routing y el proceso de selección de la mejor ruta.

Los routers en la topología tienen una configuración inicial, incluidas las direcciones de interfaz. En este momento, ninguno de los routers tiene configurado routing estático o routing dinámico. Todas las interfaces en los routers R1, R2 y R3 (excepto la interfaz loopback en el R2) se encuentran dentro del área backbone de OSPF. El router ISP se usa como gateway del dominio de routing a Internet.

**Nota:** en esta topología, la interfaz loopback se usa para simular el enlace WAN a Internet.

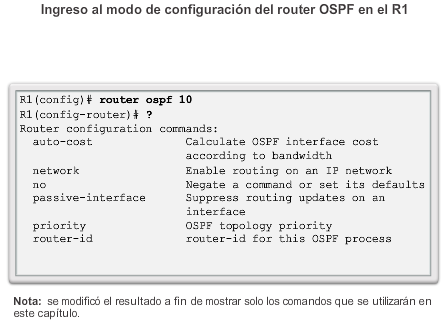
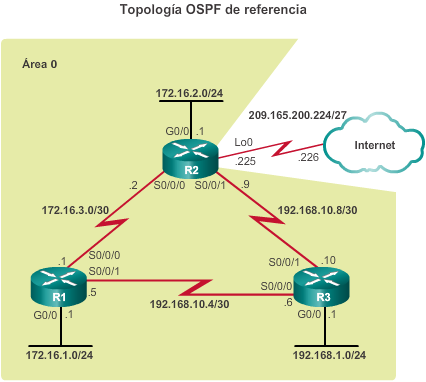


En la figura 1, se muestra la topología de referencia para este tema. OSPFv2 se habilita con el comando **router ospf***id-proceso* del modo de configuración global. El valor *id-proceso* representa un número entre 1 y 65 535, y lo elige el administrador de red. El valor *id-proceso*tiene importancia en el ámbito local, lo que significa que no necesita ser el mismo valor en los demás routers OSPF para establecer adyacencias con esos vecinos.

En la figura 2, se proporciona un ejemplo del ingreso al modo de configuración de OSPF del router en el R1.

**Nota:** la lista de comandos se modificó para que se muestren solo los comandos que se utilizan en este capítulo. Para obtener una lista completa de comandos, utilice los verificadores de sintaxis de la figura 3.

Utilice el verificador de sintaxis de la figura 3 para ingresar al modo de configuración de router OSPF en el R2 y enumerar los comandos disponibles en la petición de entrada.



Para participar en un dominio OSPF, cada router requiere una ID de router. La ID del router puede estar definida por un administrador o puede ser asignada en forma automática por el router. El router con OSPF habilitado usa la ID del router para realizar lo siguiente:

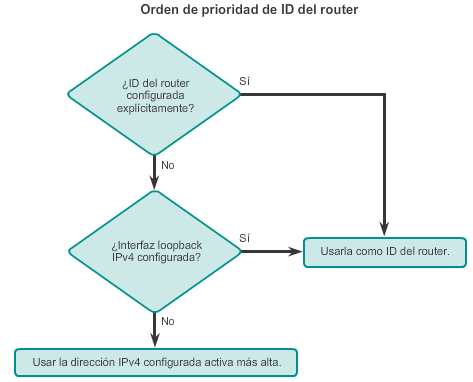
* **Identificar el router de manera exclusiva:** otros routers usan la ID del router para identificar de forma exclusiva cada router dentro del dominio OSPF y todos los paquetes que se originan en ellos.
* **Participar en la elección del DR:** en un entorno LAN de accesos múltiples, la elección del DR se lleva a cabo durante el establecimiento inicial de la red OSPF. Cuando se activan los enlaces OSPF, el dispositivo de routing configurado con la prioridad más alta se elige como DR. Si se parte de la suposición de que no hay ninguna prioridad configurada o de que hay un empate, se elige como DR el router con la mayor ID de router. El dispositivo de routing con la segunda ID de router más alta se elige como BDR.

¿Pero de qué manera el router determina la ID de router? Como se muestra en la ilustración, los routers Cisco derivan la ID del router sobre la base de uno de tres criterios, en el siguiente orden de preferencia:

* La ID del router se configura explícitamente con el comando **router-id***id-router* del modo de configuración de OSPF del router. El valor *id-router* es cualquier valor de 32 bits expresado como dirección IPv4. Es el método recomendado para asignar una ID de router.
* Si la ID del router no se configura explícitamente, el router elige la dirección IPv4 más alta de cualquiera de las interfaces loopback configuradas. Esta constituye la segunda mejor opción para asignar una ID de router.
* Si no se configuró ninguna interfaz loopback, el router elige la dirección IPv4 activa más alta de cualquiera de sus interfaces físicas. Este es el método menos recomendado, ya que hace que a los administradores les resulte más difícil diferenciar entre routers específicos.

Si el router usa la dirección IPv4 más alta para la ID del router, la interfaz no necesita tener OSPF habilitado. Esto significa que no se necesita incluir la dirección de interfaz en uno de los comandos **network** de OSPF para que el router use esa dirección IP como ID del router. El único requisito es que la interfaz esté activa y en estado up (activo).

**Nota:** la ID del router parece una dirección IP, pero no es enrutable y, por lo tanto, no se incluye en la tabla de routing, a menos que el proceso de routing de OSPF elija una interfaz (física o loopback) que esté definida en forma adecuada por un comando **network**.



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

Como se muestra en la figura 1, se configuró una ID de router 1.1.1.1 en el R1, una ID 2.2.2.2 en el R2 y una ID 3.3.3.3 en el R3.

En la figura 2, se asigna la ID de router 1.1.1.1 al R1. Utilice el comando **show ip protocols** para verificar la ID del router.

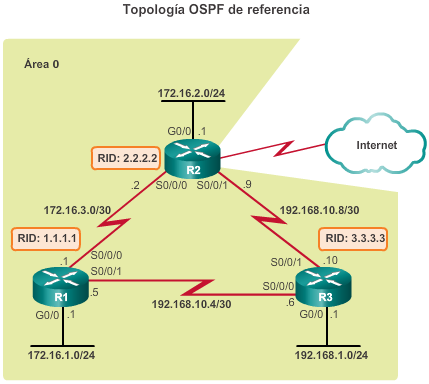
**Nota:** el R1 nunca se había configurado con una ID de router OSPF. De haber sido así, se debería modificar la ID del router.

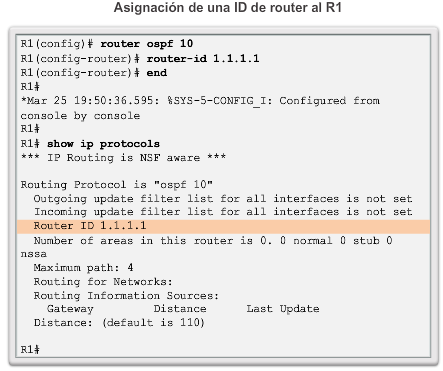
Si la ID del router es la misma en dos routers vecinos, el router muestra un mensaje de error similar al siguiente:

%OSPF-4-DUP\_RTRID1: Detected router with duplicate router ID (Se detectó un router con una ID de router duplicada).

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

Utilice el verificador de sintaxis de la figura 3 para asignar la ID del router al R2 y al R3.





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

En la figura 1, observe que la ID del router actual es 192.168.10.5. La ID del router debería ser 1.1.1.1.

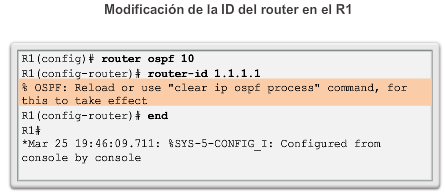
En la figura 2, se asigna la ID de router 1.1.1.1 al R1. Observe que aparece un mensaje informativo que indica que se debe borrar el proceso OSPF o se debe volver a cargar el router. Esto ocurre debido a que el R1 ya tiene adyacencias con otros vecinos que utilizan la ID de router 192.168.10.5. Se deben volver a negociar esas adyacencias utilizando la nueva IP de router 1.1.1.1.

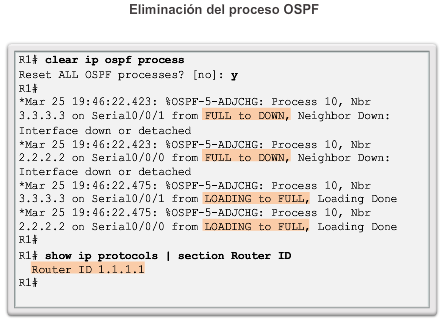
El método preferido para restablecer la ID del router es borrar el proceso OSPF.

En la figura 3, se borra el proceso de routing de OSPF con el comando **clear ip ospf process** del modo EXEC privilegiado. Esto obliga al protocolo OSPF en el R1 a pasar a los estados Down e Init. Observe los mensajes de cambio de adyacencia de Full a Down y de Loading a Full. El comando **show ip protocols** verifica que se haya cambiado la ID del router.

Utilice el verificador de sintaxis de la figura 4 para modificar la ID del router para el R1.





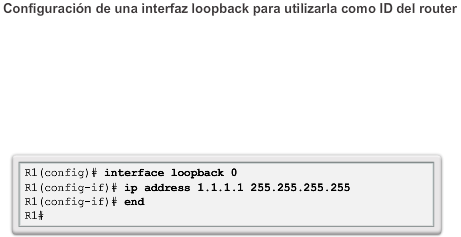


Una ID de router también se puede asignar mediante una interfaz loopback.

La dirección IPv4 de la interfaz loopback se debe configurar con una máscara de subred de 32 bits (255.255.255.255). Esto crea una ruta de host. Una ruta de host de 32 bits no se anuncia como ruta a otros routers OSPF.

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

**Nota:** algunas versiones anteriores de IOS no reconocen el comando **router-id**; por lo tanto, la mejor forma de establecer la ID del router en esos routers es mediante una interfaz loopback.



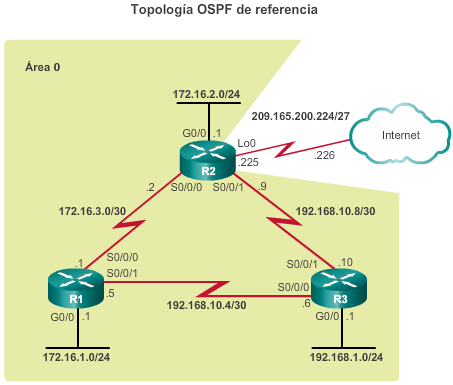
### Configuración de OSPFv2 de área única

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

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

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

En la ilustración, se muestra la topología de referencia.



OSPFv2 usa la combinación de argumentos *dirección-red máscara-wildcard* para habilitar OSPF en las interfaces. Por su diseño, OSPF es un protocolo sin clase; por lo tanto, siempre se requiere la máscara wildcard. Al identificar las interfaces que participan en un proceso de routing, la máscara wildcard generalmente es el valor inverso a la máscara de subred configurada en esa interfaz.

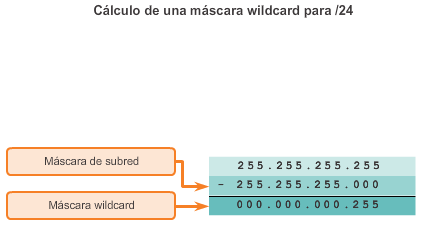
Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección debe examinar para obtener una coincidencia. En una máscara de subred, un 1 binario equivale a una coincidencia, y un 0 binario no es una coincidencia. En una máscara wildcard, sucede lo contrario:

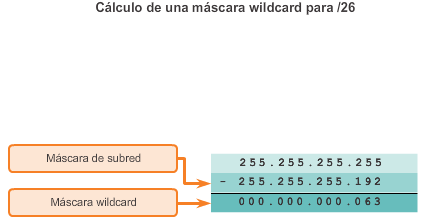
* **Bit 0 de máscara wildcard:** coincide con el valor de bit correspondiente en la dirección.
* **Bit 1 de máscara wildcard:** omite el valor del bit correspondiente en la dirección.

El método más sencillo para calcular una máscara wildcard es restar la máscara de subred de la red a 255.255.255.255.

En el ejemplo de la figura 1, se calcula la máscara wildcard a partir de la dirección de red 192.168.10.0/24. Para hacerlo, se resta la máscara de subred 255.255.255.0 a 255.255.255.255, cuyo resultado es 0.0.0.255. Por lo tanto,192.168.10.0/24 es 192.168.10.0 con una máscara wildcard 0.0.0.255.

En el ejemplo de la figura 2, se calcula la máscara wildcard a partir de la dirección de red 192.168.10.64/26. Para hacerlo, se resta la máscara de subred 255.255.255.192 a 255.255.255.255, cuyo resultado es 0.0.0.63. Por lo tanto,192.168.10.0/26 es 192.168.10.0 con una máscara wildcard 0.0.0.63.





Existen varias maneras de identificar las interfaces que participan en el proceso de routing OSPFv2.

En la figura 1, se muestran los comandos requeridos para determinar qué interfaces del R1 participan en el proceso de routing OSPFv2 para un área. Observe el uso de las máscaras wildcard para identificar las respectivas interfaces sobre la base de sus direcciones de red. Dado que se trata de una red OSPF de área única, todas las ID de área se establecen en 0.

Como alternativa, se puede habilitar OSPFv2 con el comando **network** *dirección-ip-interfaz***0.0.0.0***area id-área* del modo de configuración del router.

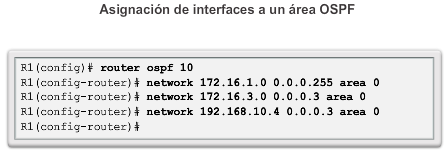
En la figura 2, se proporciona un ejemplo de cómo especificar la dirección IPv4 de interfaz con una máscara wildcard de cuádruple cero. La introducción de **network 172.16.3.1 0.0.0.0 area 0** en el R1 le indica al router que habilite la interfaz Serial0/0/0 para el proceso de routing. Como resultado, el proceso OSPFv2 anuncia la red que se encuentra en esta interfaz (172.16.3.0/30).

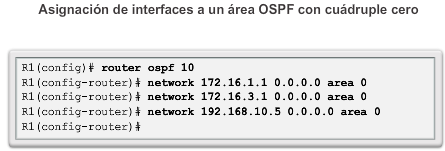
La ventaja de especificar la interfaz es que no se necesita calcular la máscara wildcard. OSPFv2 usa la dirección y máscara de subred de la interfaz para determinar qué red debe anunciar.

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

Utilice el verificador de sintaxis de la figura 3 para anunciar las redes conectadas al R2.

**Nota:** mientras completa el verificador de sintaxis, observe los mensajes informativos que describen la adyacencia entre el R1 (1.1.1.1) y el R2 (2.2.2.2). El esquema de direccionamiento IPv4 utilizado para la ID del router facilita la identificación del vecino.

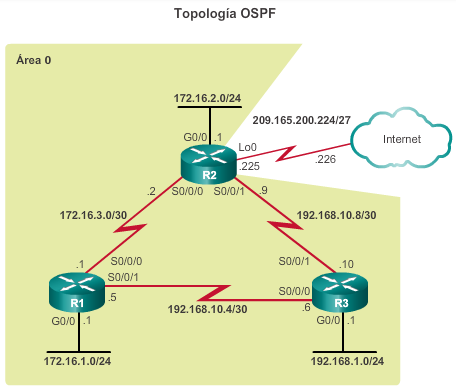




De manera predeterminada, los mensajes OSPF se reenvían por todas las interfaces con OSPF habilitado. Sin embargo, estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado.

Consulte la topología de la ilustración. Los mensajes OSPF se reenvían por la interfaz G0/0 de los tres routers, aunque no exista ningún vecino OSPF en esa LAN. El envío de mensajes innecesarios en una LAN afecta la red de tres maneras:

* **Uso ineficaz del ancho de banda:**se consume el ancho de banda disponible con el transporte de mensajes innecesarios. Los mensajes se transmiten por multidifusión; por lo tanto, los switches también reenvían los mensajes por todos los puertos.
* **Uso ineficaz de los recursos:** todos los dispositivos en la LAN deben procesar el mensaje y, finalmente, descartarlo.
* **Mayor riesgo de seguridad:** anunciar actualizaciones en una red de difusión constituye un riesgo de seguridad. Los mensajes OSPF se pueden interceptar con software de detección de paquetes. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.



Utilice el comando **passive-interface**del modo de configuración del router para evitar la transmisión de mensajes de routing a través de una interfaz del router, pero sin dejar de permitir que se anuncie esa red a otros routers, como se muestra en la figura 1. Concretamente, el comando evita que se envíen los mensajes de routing por la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada se sigue anunciando en los mensajes de routing que se envían por otras interfaces.

Por ejemplo, no es necesario que el R1, el R2 y el R3 reenvíen mensajes OSPF por sus interfaces LAN. La configuración identifica la interfaz G0/0 del R1 como pasiva.

Es importante saber que no se puede formar una adyacencia de vecino a través de una interfaz pasiva. Esto se debe a que los paquetes de estado de enlace no se pueden enviar ni confirmar.

A continuación, se usa el comando **show ip protocols** para verificar que la interfaz Gigabit Ethernet sea pasiva, como se muestra en la figura 2. Observe que la interfaz G0/0 ahora figura en la sección Passive Interface(s) (Interfaces pasivas). La red 172.16.1.0 aún figura en Routing for Networks (Routing para redes), lo que significa que esta red aún se incluye como entrada de ruta en las actualizaciones OSPF que se envían al R2 y al R3.

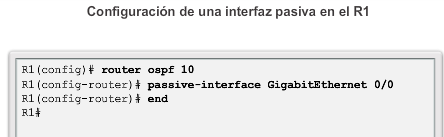
**Nota:** OSPFv2 y OSPFv3 admiten el comando **passive-interface**.

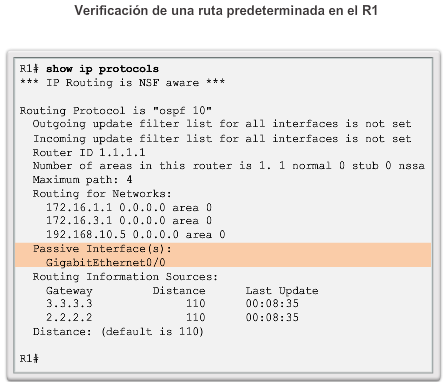
Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R2.

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

Continúe utilizando el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R3.

**Nota:** mientras completa el verificador de sintaxis, observe los mensajes informativos de estado de OSPF a medida que todas las interfaces se hacen pasivas y las dos interfaces seriales se hacen no pasivas.





### Costo OSPF

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

El costo de una interfaz es inversamente proporcional al ancho de banda de la interfaz. Por lo tanto, cuanto mayor es el ancho de banda, menor es el costo. Cuanto más sobrecarga y retraso, mayor es el costo. Por lo tanto, una línea Ethernet de 10 Mb/s tiene un costo mayor que una línea Ethernet de 100 Mb/s.

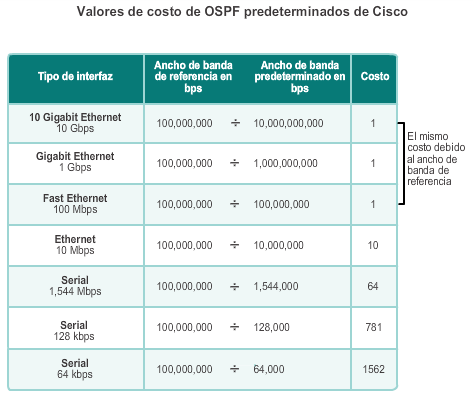
La fórmula que se usa para calcular el costo de OSPF es la siguiente:

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

El ancho de banda de referencia predeterminado es 10^8 (100 000 000); por lo tanto, la fórmula es la siguiente:

* **Costo** = 100 000 000 bps /ancho de banda de la interfaz en bps

Consulte la tabla de la ilustración para obtener un desglose del cálculo del costo. Observe que las interfaces FastEthernet, Gigabit Ethernet y 10 GigE comparten el mismo costo, debido a que el valor del costo de OSPF debe ser un número entero. En consecuencia, dado que el ancho de banda de referencia predeterminado se establece en 100 Mb/s, todos los enlaces que son más rápidos que Fast Ethernet también tienen un costo de 1.

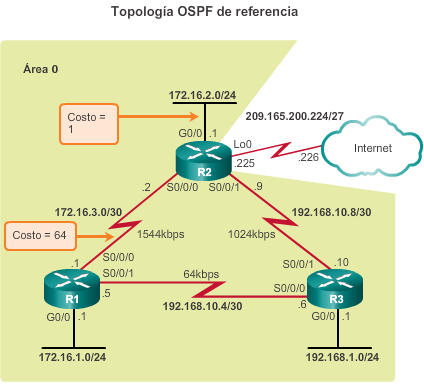


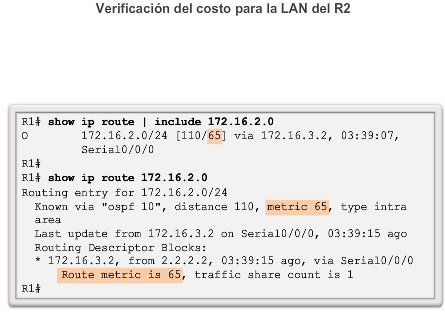
El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino.

Por ejemplo, en la figura 1, el costo para llegar desde el R1 hasta la LAN 172.16.2.0/24 del R2 debe ser el siguiente:

* Costo del enlace serial del R1 al R2 = 64
* Costo del enlace Gigabit Ethernet en el R2 = 1
* Costo total para llegar a 172.16.2.0/24=**65**

En la tabla de routing del R1 de la figura 2, se confirma que la métrica para llegar a la LAN del R2 equivale a un costo de 65.





OSPF utiliza un ancho de banda de referencia de 100 Mb/s para todos los enlaces que sean iguales o más rápidos que una conexión Fast Ethernet. Por lo tanto, el costo asignado a una interfaz Fast Ethernet con un ancho de banda de interfaz de 100 Mb/s sería igual a 1.

**Costo =** *100 000 000 bps*/*100 000 000 = 1*

Si bien este cálculo funciona para las interfaces Fast Ethernet, es problemático para los enlaces que son más rápidos que 100 Mb/s, debido a que la métrica de OSPF solo utiliza números enteros como costo final de un enlace. Si se calcula un valor menor que un número entero, OSPF redondea al número entero más cercano. Por este motivo, desde la perspectiva de OSPF, una interfaz con un ancho de banda de interfaz de 100 Mb/s (un costo de 1) tiene el mismo costo que una interfaz con un ancho de banda de 100 Gb/s (un costo de 1).

Para ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda de referencia a un valor superior, a fin de admitir redes con enlaces más rápidos que 100 Mb/s.

**Ajuste del ancho de banda de referencia**

El cambio del ancho de banda de referencia en realidad no afecta la capacidad de ancho de banda en el enlace, sino que simplemente afecta el cálculo utilizado para determinar la métrica. Para ajustar el ancho de banda de referencia, use el comando de configuración del router **auto-cost reference-bandwidth***Mb/s*. Se debe configurar este comando en cada router en el dominio OSPF. Observe que el valor se expresa en Mb/s; por lo tanto, a fin de ajustar los costos para estas interfaces, utilice los siguientes comandos:

* **Gigabit Ethernet:** **auto-cost reference-bandwidth 1000**
* **10 Gigabit Ethernet:** **auto-cost reference-bandwidth 10000**

Para volver al ancho de banda de referencia predeterminado, use el comando **auto-cost reference-bandwidth 100**.

En la tabla de la figura 1, se muestra el costo de OSPF si el ancho de banda de referencia se establece en Gigabit Ethernet. Si bien los valores de métrica aumentan, OSPF toma mejores decisiones debido a que ahora puede diferenciar entre enlaces FastEthernet y Gigabit Ethernet.

En la figura 2, se muestra el costo de OSPF si se ajusta el ancho de banda de referencia para admitir 10 enlaces Gigabit Ethernet. Se debe ajustar el ancho de banda de referencia cada vez que haya enlaces más rápidos que FastEthernet (100 Mb/s).

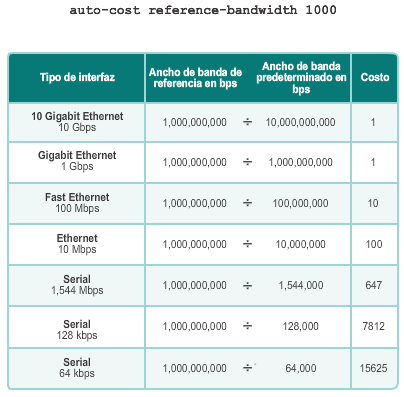
**Nota:** los costos representan números enteros que se redondearon hacia abajo.

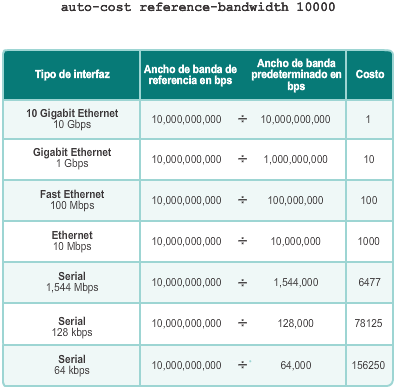
En la figura 3, todos los routers se configuraron para admitir el enlace Gigabit Ethernet con el comando de configuración del router **auto-cost reference-bandwidth 1000**. El nuevo costo acumulado para llegar desde el R1 hasta la LAN 172.16.2.0/24 del R2 es el siguiente:

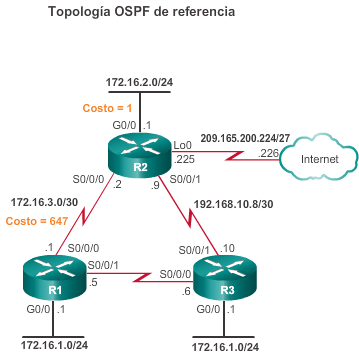
* Costo del enlace serial del R1 al R2 = 647
* Costo del enlace Gigabit Ethernet en el R2 = 1
* Costo total para llegar a 172.16.2.0/24=**648**

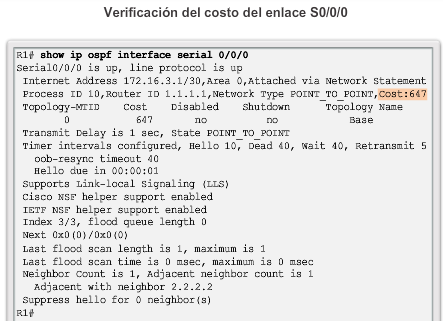
Utilice el comando **show ip ospf interface s0/0/0** para verificar el costo de OSPF actual asignado a la interfaz Serial 0/0/0 del R1, como se muestra en la figura 4. Observe que se muestra un costo de 647.

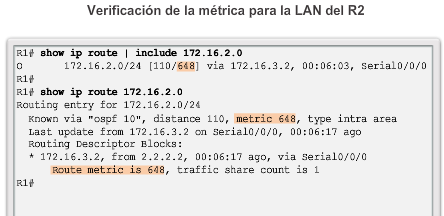
En la tabla de routing del R1 de la figura 5, se confirma que la métrica para llegar a la LAN del R2 equivale a un costo de 648.











Todas las interfaces tienen asignados valores de ancho de banda predeterminados. Al igual que el ancho de banda de referencia, los valores del ancho de banda de interfaz en realidad no afectan la velocidad o la capacidad del enlace. En cambio, OSPF los utiliza para calcular la métrica de routing. Por lo tanto, es importante que el valor del ancho de banda refleje la velocidad real del enlace para que la tabla de routing tenga información precisa acerca de la mejor ruta.

Si bien los valores de ancho de banda de las interfaces Ethernet suelen coincidir con la velocidad del enlace, es posible que en otras interfaces no lo hagan. Por ejemplo, la velocidad real de las interfaces seriales a menudo es distinta del ancho de banda predeterminado. En los routers Cisco, el ancho de banda predeterminado en la mayoría de las interfaces seriales se establece en 1,544 Mb/s.

**Nota:** es posible que las interfaces seriales antiguas tengan un valor predeterminado de 128 kb/s.

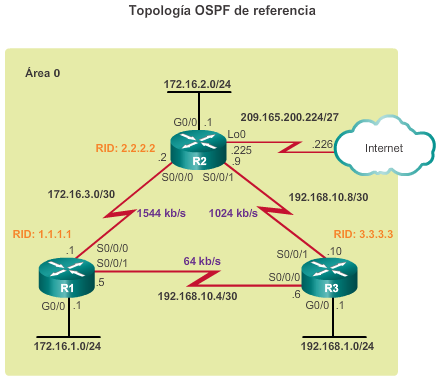
Consulte el ejemplo de la figura 1. Observe lo siguiente:

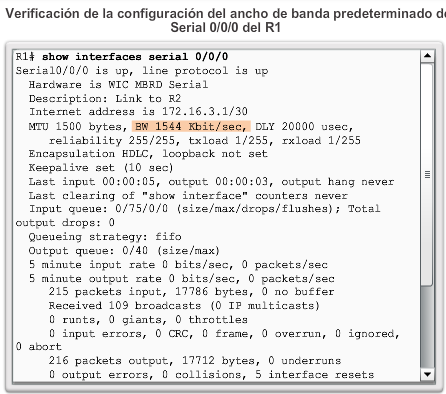
* El enlace entre el R1 y el R2 se debe establecer en 1544 kb/s (valor predeterminado).
* El enlace entre el R2 y el R3 se debe establecer en 1024 kb/s.
* El enlace entre el R1 y el R3 se debe establecer en 64 kb/s.

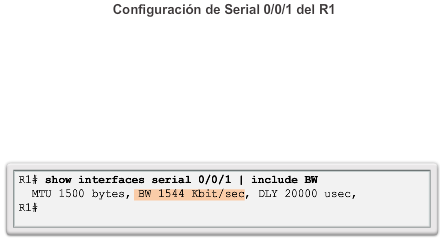
Utilice el comando **show interfaces** para ver la configuración del ancho de banda de interfaz. En la figura 2, se muestra la configuración de la interfaz serial 0/0/0 para el R1. La configuración del ancho de banda es precisa y, por lo tanto, no es necesario ajustar la interfaz serial.

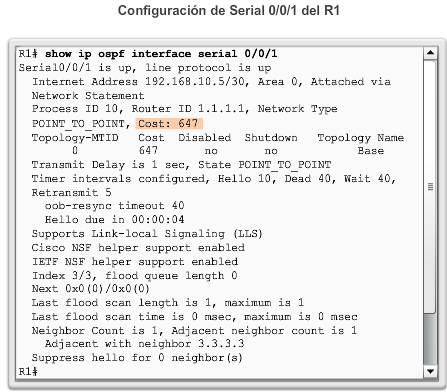
En la figura 3, se muestra la configuración de la interfaz serial 0/0/1 para el R1. También se confirma que la interfaz usa el ancho de banda de interfaz predeterminado de 1544 kb/s. Según la topología de referencia, este se debe establecer en 64 kb/s. Por lo tanto, se debe ajustar la interfaz serial 0/0/1 del R1.

En la figura 4, se muestra la métrica de costo resultante de 647, que se basa en el ancho de banda de referencia establecido en 1 000 000 000 bps y en el ancho de banda de interfaz predeterminado de 1544 kb/s (1 000 000 000 / 1 544 000).









**Ajuste del ancho de banda de interfaz**

Para ajustar el ancho de banda de la interfaz, utilice el comando de configuración de interfaz **bandwidth***kilobits*. Utilice el comando **no bandwidth** para restaurar el valor por defecto.

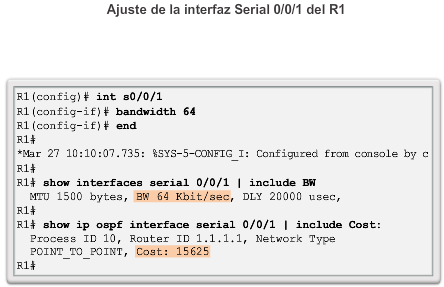
En el ejemplo de la figura 1, se ajusta el ancho de banda de la interfaz Serial 0/0/1 del R1 a 64 kb/s. Una verificación rápida confirma que la configuración del ancho de banda de la interfaz ahora es de 64 kb/s.

Se debe ajustar el ancho de banda en cada extremo de los enlaces seriales, de lo cual se deriva lo siguiente:

* El R2 requiere que su interfaz S0/0/1 se ajuste a 1024 kb/s.
* El R3 requiere que su interfaz serial 0/0/0 se ajuste a 64 kb/s y que su interfaz serial 0/0/1 se ajuste a 1024 kb/s.

Utilice el verificador de sintaxis de la figura 2 para ajustar la interfaz serial del R2 y del R3.

**Nota:** un concepto erróneo habitual de los estudiantes nuevos en la tecnología de redes y en IOS de Cisco es suponer que el comando **bandwidth** cambia el ancho de banda físico del enlace. Este comando solo modifica la métrica de ancho de banda que usan EIGRP y OSPF. El comando no modifica el ancho de banda real en el enlace.



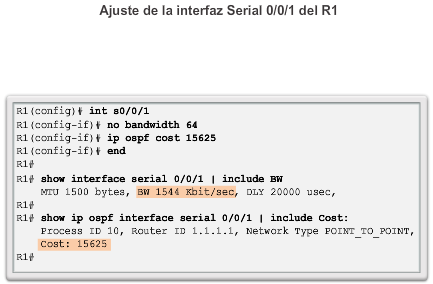
Como alternativa a la configuración del ancho de banda de interfaz predeterminado, es posible configurar el costo de forma manual en una interfaz con el comando de configuración de interfaz **ip ospf cost** *valor*.

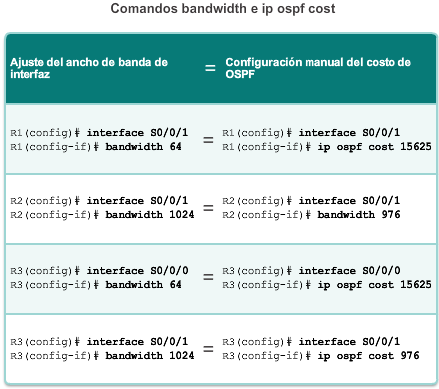
Una ventaja de configurar un costo en lugar del ancho de banda de la interfaz es que, cuando se configura el costo manualmente, el router no necesita calcular la métrica. En cambio, cuando se configura el ancho de banda de la interfaz, el router debe calcular el costo de OSPF sobre la base del ancho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

Con los comandos de interfaz **bandwidth** e **ip ospf cost** se logra el mismo resultado, que es proporcionar a OSPF un valor preciso para determinar la mejor ruta.

Por ejemplo, en la figura 1, el ancho de banda de interfaz de serial 0/0/1 se restablece al valor predeterminado, y el costo de OSPF se establece de forma manual en 15 625. Si bien el ancho de banda de interfaz se restablece al valor predeterminado, el costo de OSPF se establece como si aún se calculara el ancho de banda.

En la figura 2, se muestran las dos alternativas que se pueden utilizar para modificar los costos de los enlaces seriales en la topología. En el lado derecho de la ilustración, se muestran los comandos **ip ospf cost** equivalentes a los comandos **bandwidth**de la izquierda.





En la figura 1, se muestra la topología de referencia.

Utilice el comando **show ip ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

Si dos routers no establecen una adyacencia, no se intercambia la información de estado de enlace. Las LSDB incompletas pueden producir imprecisiones en los árboles SPF y en las tablas de routing. Es posible que no existan rutas hacia las redes de destino o que estas no representen la ruta más óptima.

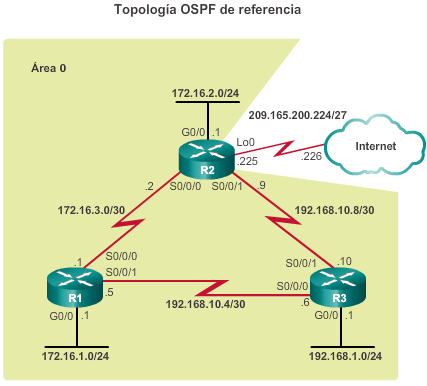
En la figura 2, se muestra la adyacencia de vecino del R1. Este comando muestra el siguiente resultado para cada vecino:

* **Neighbor ID:** la ID del router vecino.
* **Pri:** la prioridad OSPF de la interfaz. Este valor se utiliza en la elección del DR y del BDR.
* **State:** el estado de OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen LSDB de OSPF idénticas. En las redes de accesos múltiples, como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. El guion indica que no se requiere ningún DR o BDR debido al tipo de red.
* **Dead Time:** la cantidad de tiempo restante que el router espera para recibir un paquete de saludo OSPF del vecino antes de declararlo inactivo. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
* **Address:** la dirección IPv4 de la interfaz del vecino a la que el router está conectado directamente.
* **Interface:** la interfaz en la que este router formó adyacencia con el vecino.

Utilice el verificador de sintaxis de la figura 3 para verificar los vecinos del R2 y del R3 con el comando **show ip ospf neighbor**.

Dos routers pueden no formar una adyacencia OSPF si:

* Las máscaras 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.
* Falta un comando **network** de OSPF o este es incorrecto.





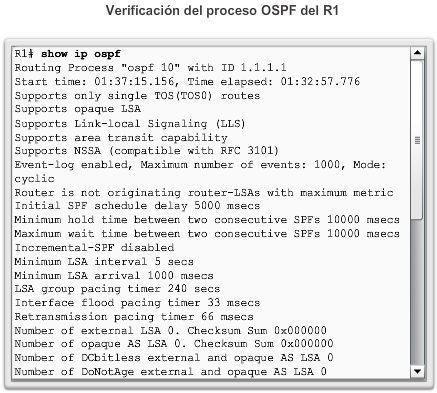
Como se muestra en la figura 1, el comando **show ip protocols** es una manera rápida de verificar la información fundamental de configuración OSPF. Esta incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es de 110.

Utilice el verificador de sintaxis de la figura 2 para verificar la configuración del protocolo OSPF del R2 y el R3 con el comando **show ip protocols**.



El comando **show ip ospf** también se puede usar para examinar la ID del proceso OSPF y la ID del router, como se muestra en la figura 1. Este comando muestra información del área OSPF y la última vez que se calculó el algoritmo SPF.

Utilice el verificador de sintaxis de la figura 2 para verificar el proceso OSPF del R2 y el R3 con el comando **show ip ospf**.

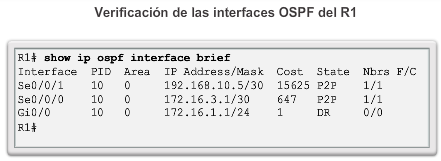


La forma más rápida de verificar la configuración de interfaz OSPF es utilizar el comando **show ip ospf interface**. Este comando proporciona una lista detallada para cada interfaz con OSPF habilitado. El comando es útil para determinar si se compusieron correctamente las instrucciones del comando **network**.

Para obtener un resumen de las interfaces con OSPF habilitado, utilice el comando **show ip ospf interface brief**, como se muestra en la figura 1.

Utilice el verificador de sintaxis de la figura 2 para recuperar y ver un resumen de las interfaces con OSPF habilitado en el R2 mediante el comando **show ip ospf interface brief**. Observe que especificar el nombre de la interfaz como se hace en el comando **show ip ospf interface serial 0/0/1** proporciona información detallada de OSPF.

Continúe utilizando el verificador de sintaxis de la figura 2 para obtener un resumen de las interfaces con OSPF habilitado en el R3 mediante el comando **show ip ospf interface brief**. Recupere y vea información adicional de la interfaz Serial 0/0/0 con el comando **show ip ospf interface serial 0/0/0**.



## Configuración de OSPFv3 de área única

### Comparación de los protocolos OSPFv2 y OSPFv3

OSPFv3 es el equivalente a OSPFv2 para intercambiar prefijos IPv6. Recuerde que, en IPv6, la dirección de red se denomina “prefijo” y la máscara de subred se denomina “longitud de prefijo”.

De manera similar a su equivalente de IPv4, OSPFv3 intercambia la información de routing para completar la tabla de routing IPv6 con prefijos remotos, como se muestra en la ilustración.

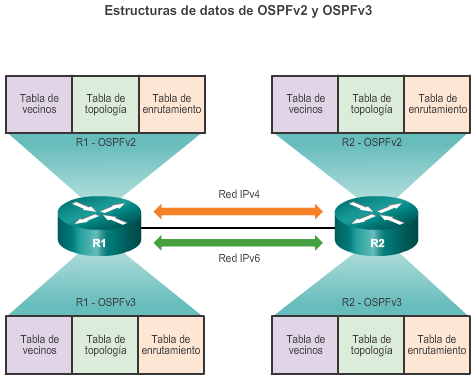
**Nota:** con la característica de familias de direcciones de OSPFv3, esta versión del protocolo es compatible con IPv4 e IPv6.

OSPFv2 se ejecuta a través de la capa de red IPv4, por lo que se comunica con otros peers IPv4 OSPF y solo anuncia rutas IPv4.

OSPFv3 tiene la misma funcionalidad que OSPFv2, pero utiliza IPv6 como transporte de la capa de red, por lo que se comunica con peers OSPFv3 y anuncia rutas IPv6. OSPFv3 también utiliza el algoritmo SPF como motor de cómputo para determinar las mejores rutas a lo largo del dominio de routing.

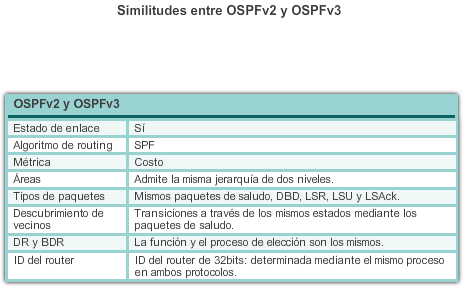
Al igual que con todos los protocolos de routing IPv6, OSPFv3 tiene procesos diferentes de los de su equivalente de IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de routing IPv4, pero se ejecutan de forma independiente. OSPFv2 y OSPFv3 tienen tablas de adyacencia, tablas de topología OSPF y tablas de routing IP independientes, como se muestra en la ilustración.

Los comandos de configuración y verificación de OSPFv3 son similares a los que OSPFv2.



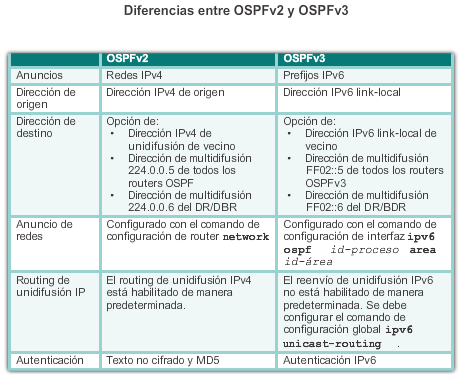
Como se muestra en la ilustración, las similitudes entre OSPFv2 y OSPFv3 son las siguientes:

* **Estado de enlace:** OSPFv2 y OSPFv3 son protocolos de estado de enlace sin clase.
* **Algoritmo de routing:** OSPFv2 y OSPFv3 usan el algoritmo SPF para tomar decisiones.
* **Métrica:** las RFC para OSPFv2 y OSPFv3 definen la métrica como el costo del envío de paquetes por la interfaz. OSPFv2 y OSPFv3 pueden modificarse mediante el comando del modo de configuración del router **auto-cost reference-bandwidth***ancho-banda-referencia*. El comando solo afecta la métrica de OSPF donde se configuró. Por ejemplo, si se introdujo este comando para OSPFv3, no afecta las métricas de routing de OSPFv2.
* **Áreas:** el concepto de varias áreas en OSPFv3 es el mismo que en OSPFv2. Varias áreas que minimizan la saturación de estado de enlace y proporcionan mejor estabilidad con el dominio OSPF.
* **Tipos de paquetes OSPF:** OSPFv3 usa los mismos cinco tipos de paquetes básicos que OSPFv2 (saludo, DBD, LSR, LSU y LSAck).
* **Mecanismo de descubrimiento de vecinos:** la máquina de estado de vecinos, incluida la lista de estados y eventos de vecinos OSPF, no se modifica. OSPFv2 y OSPFv3 utilizan el mecanismo de saludo para obtener información sobre los routers vecinos y formar adyacencias. Sin embargo, en OSPFv3, no existe ningún requisito con respecto a la coincidencia de subredes para formar adyacencias de vecinos. Esto se debe a que las adyacencias de vecinos se forman mediante direcciones link-local, no direcciones de unidifusión global.
* **Elección del DR/BDR:** el proceso de elección del DR/BDR no se modifica en OSPFv3.
* **ID del router:** tanto OSPFv2 como OSPFv3 usan un número de 32 bits para la ID del router representada en notación decimal con puntos. Por lo general, se trata de una dirección IPv4. Se debe utilizar el comando de OSPF **router-id** para configurar la ID del router. El proceso para determinar la ID del router de 32 bits es el mismo en ambos protocolos. Utilice una ID de router configurada explícitamente; de lo contrario, la dirección IPv4 de loopback más alta se convierte en la ID del router.



En la ilustración, se muestran las diferencias entre OSPFv2 y OSPFv3:

* **Anuncios:** OSPFv2 anuncia rutas IPv4, mientras que OSPFv3 anuncia rutas para IPv6.
* **Dirección de origen:** los mensajes OSPFv2 se originan en la dirección IPv4 de la interfaz de salida. En OSPFv3, los mensajes OSPF se originan con la dirección link-local de la interfaz de salida.
* **Dirección de multidifusión de todos los routers OSPF:** OSPFv2 utiliza la dirección 224.0.0.5, mientras que OSPFv3 utiliza la dirección FF02::5.
* **Dirección de multidifusión de DR/BDR:** OSPFv2 utiliza la dirección 224.0.0.6, mientras que OSPFv3 utiliza la dirección FF02::6.
* **Anuncio de redes:** OSPFv2 anuncia las redes mediante el comando de configuración del router **network**, mientras que OSPFv3 utiliza el comando de configuración de interfaz**ipv6 ospf***id-proceso***area***id-área*.
* **Routing de unidifusión IP:** habilitado de manera predeterminada en IPv4; en cambio, el comando de configuración global **ipv6 unicast-routing** se debe configurar.
* **Autenticación:** OSPFv2 utiliza autenticación de texto no cifrado o autenticación MD5. OSPFv3 utiliza autenticación IPv6.

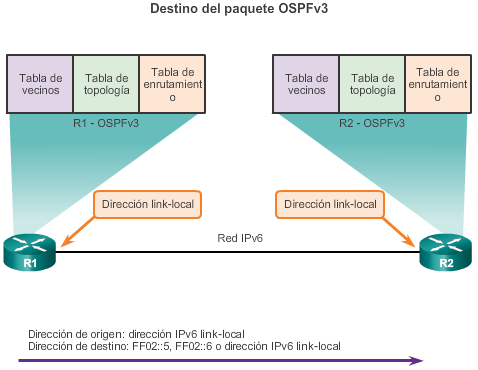


Los routers que ejecutan un protocolo de routing dinámico, como OSPF, intercambian mensajes entre vecinos en la misma subred o el mismo enlace. Los routers solo necesitan enviar y recibir mensajes de protocolo de routing con sus vecinos conectados directamente. Estos mensajes siempre se envían desde la dirección IPv4 de origen del router que realiza el reenvío.

Las direcciones IPv6 link-local son ideales para este propósito. Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

Como se muestra en la ilustración, los mensajes OSPFv3 se envían utilizando lo siguiente:

* **Dirección IPv6 de origen:** esta es la dirección IPv6 link-local de la interfaz de salida.
* **Dirección IPv6 de destino:** se pueden enviar los paquetes OSPFv3 a una dirección de unidifusión mediante la dirección IPv6 link-local del vecino. También es posible enviarlos utilizando una dirección de multidifusión. La dirección FF02::5 es la dirección de todos los routers OSPF, mientras que FF02::6 es la dirección de multidifusión del DR/BDR.



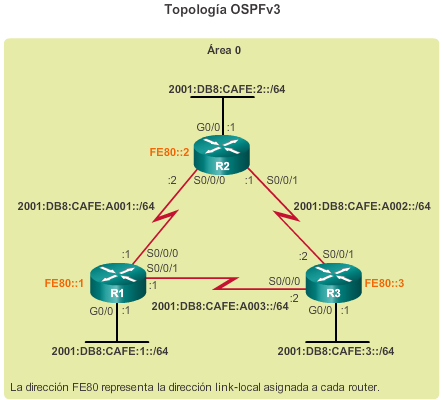
### Configuración de OSPFv3

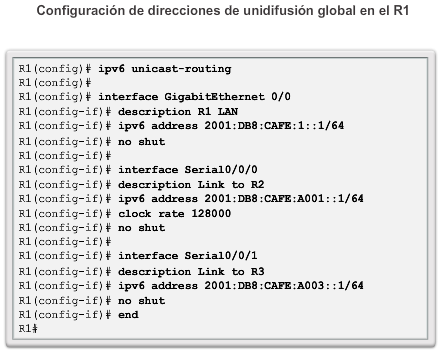
En la figura 1, se muestra la topología de la red que se utiliza para configurar OSPFv3.

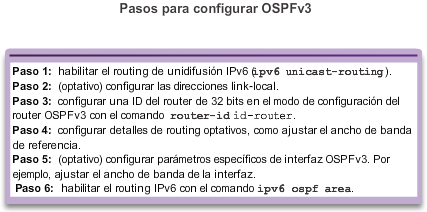
En la figura 2, se muestra el routing de unidifusión IPv6 y la configuración de las direcciones de unidifusión global del R1, como se identifican en la topología de referencia. Suponga que las interfaces del R2 y el R3 también se configuraron con sus direcciones de unidifusión global, como se identifica en la topología mencionada.

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

En la figura 3, se muestran los pasos para configurar OSPFv3 básico en un área única.







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

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

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



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

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

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

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

En la figura 1, se configura la misma dirección link-local FE80::1 en las tres interfaces del R1. Se eligió FE80::1 para que las direcciones link-local del R1 sean fáciles de recordar.

Con una vista rápida de las interfaces como se muestran en la figura 2, se confirma que las direcciones link-local de las interfaces del R1 se cambiaron a FE80::1.

Utilice el verificador de sintaxis de la figura 3 para configurar y verificar la dirección link-local FE80::2 en el R2 y la dirección link-local FE80::3 en el R3.





Utilice el comando **ipv6 router ospf***id-proceso* del modo de configuración global para ingresar al modo de configuración del router. La petición de entrada del modo de configuración del router IPv6 es distinta de la petición de entrada del modo de configuración del router IPv4. Utilice el modo de confirmación del router IPv6 para configurar los parámetros globales de OSPFv3, como la asignación de la ID del router OSPF de 32 bits y del ancho de banda de referencia.

Los protocolos de routing IPv6 se habilitan en una interfaz, no desde el modo de configuración del router, como sus equivalentes de IPv4. El comando **network** del modo de configuración del router IPv4 no existe en IPv6.

Al igual que en OSPFv2, el valor *id-proceso* es un número entre 1 y 65 535, y lo elige el administrador de red. El valor *id-proceso* tiene importancia en el ámbito local, lo que significa que no hace falta que coincida con otros routers OSPF para establecer adyacencias.

OSPFv3 requiere que se asigne una ID de router de 32 bits antes de que se pueda habilitar OSPF en una interfaz. En el diagrama de lógica de la figura 1, se muestra cómo se elige una ID de router. Al igual que OSPFv2, OSPFv3 utiliza lo siguiente:

* En primer lugar, una ID de router configurada explícitamente.
* Si no se configuró ninguna, el router usa la dirección IPv4 configurada más alta de una interfaz loopback.
* Si no se configuró ninguna, el router usa la dirección IPv4 configurada más alta de una interfaz activa.
* Si un router no tiene ningún origen de direcciones IPv4, este muestra un mensaje de consola para configurar la ID del router de forma manual.

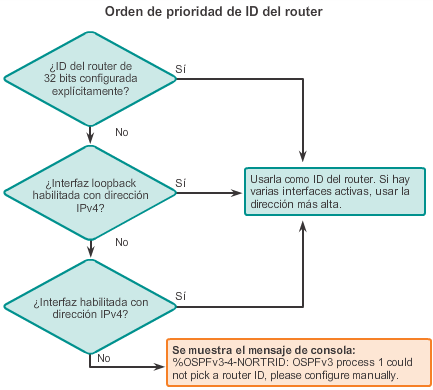
**Nota:** para mantener la coherencia, los tres routers usan la ID de proceso 10.

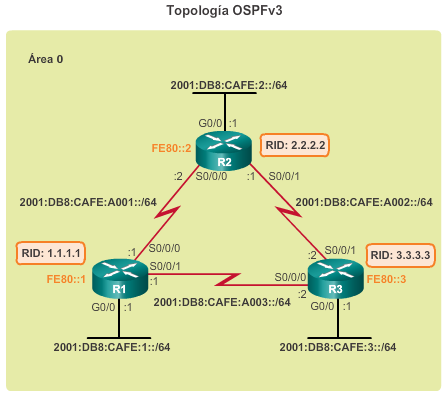
Como se muestra en la topología de la figura 2, se deben asignar las ID de router indicadas a los routers R1, R2 y R3. El comando **router-id***id-router* utilizado para asignar una ID de router en OSPFv2 es el mismo comando que se utiliza en OSPFv3.

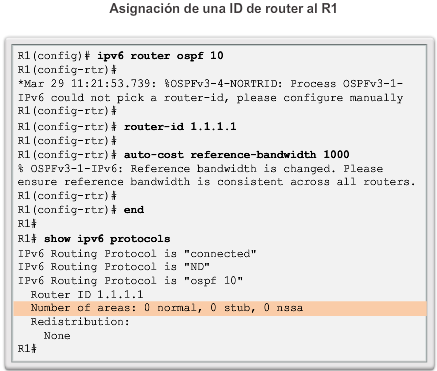
En el ejemplo de la figura 3, se realiza lo siguiente:

* Se ingresa al modo de configuración de OSPFv3 del router. Observe que la petición de entrada del router es distinta de la petición de entrada predeterminada del router del modo de protocolo de routing IPv4. Además, observe que apareció un mensaje informativo de consola cuando se accedió al modo de configuración de router OSPFv3.
* Se asigna la ID de router 1.1.1.1.
* Se ajusta el ancho de banda de referencia a 1 000 000 000 bps (1 Gb/s), debido a que hay enlaces Gigabit Ethernet en la red. Observe el mensaje informativo de consola que indica que se debe configurar este comando en todos los routers en el dominio de routing.
* El comando **show ipv6 protocols** se usa para verificar que la ID de proceso OSPFv3 10 utiliza la ID de router 1.1.1.1.

Utilice el verificador de sintaxis de la figura 4 para configurar los parámetros globales de OSPFv3 en el R2 y el R3.







En ocasiones, se deben cambiar las ID de router, por ejemplo, si el administrador de red estableció un nuevo esquema de identificación de ID de router. Sin embargo, después de que un router OSPFv3 establece una ID de router, esta no se puede cambiar hasta que se vuelva a cargar el router o se borre el proceso OSPF.

En la figura 1, observe que la ID del router actual es 10.1.1.1. La ID del router OSPFv3 debería ser 1.1.1.1.

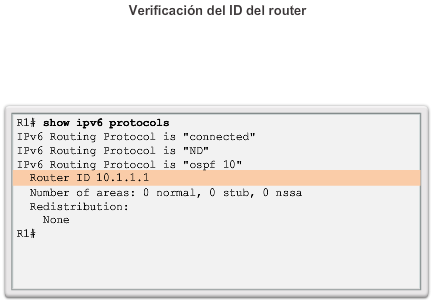
En la figura 2, se asigna la ID de router 1.1.1.1 al R1.

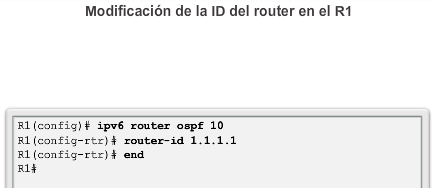
**Nota:** el método preferido para restablecer la ID del router es borrar el proceso OSPF.

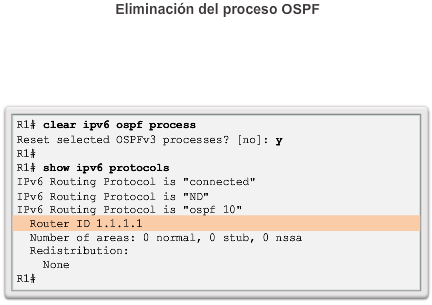
En la figura 3, se borra el proceso de routing de OSPF con el comando **clear ipv6 ospf process** del modo EXEC privilegiado. Hacer esto obliga al protocolo OSPF en el R1 a volver a negociar las adyacencias de vecinos con la nueva ID del router.

El comando **show ipv6 protocols** verifica que se haya cambiado la ID del router.

Utilice el verificador de sintaxis de la figura 4 para modificar la ID del router para el R1.







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

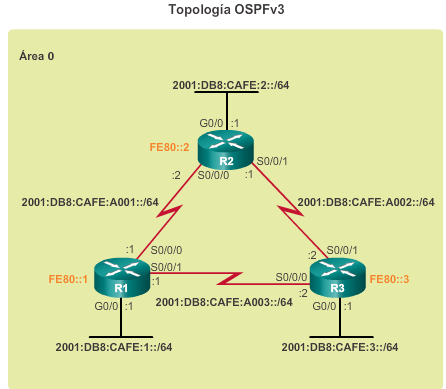
Para habilitar OSPFv3 en una interfaz, utilice el comando **ipv6 ospf***id-proceso***area***id-área* del modo de configuración de interfaz.

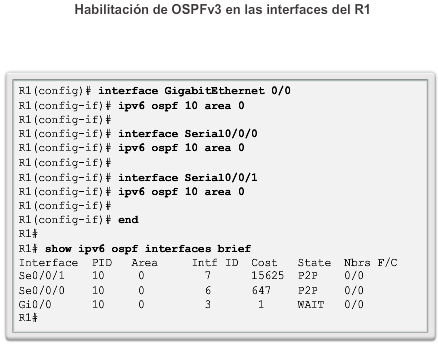
El valor *id-proceso* identifica el proceso de routing específico y debe coincidir con la ID de proceso utilizada para crear el proceso de routing en el comando **ipv6 router ospf***id-proceso*.

El valor *id-área* es el área que se debe asociar a la interfaz OSPFv3. Aunque pudo haberse configurado cualquier valor para el área, se seleccionó 0 debido a que el área 0 es el área backbone a la que se deben conectar todas las demás áreas, como se muestra en la figura 1. Esto contribuye a la migración a OSPF multiárea, si surge la necesidad.

En la figura 2, se habilita OSPFv3 en las interfaces del R1 con el comando **ipv6 ospf 10 area 0**. El comando **show ipv6 ospf interface brief** muestra las interfaces OSPFv3 activas.

Utilice el verificador de sintaxis de la figura 3 para habilitar OSPFv3 en las interfaces del R2 y el R3.





### Verificación de OSPFv3

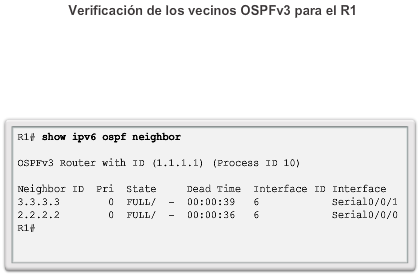
Utilice el comando **show ipv6 ospf neighbor** para verificar que el router haya formado una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.

Si dos routers no establecen una adyacencia de vecino, no se intercambia la información de estado de enlace. Las LSDB incompletas pueden producir imprecisiones en los árboles SPF y en las tablas de routing. Es posible que no existan rutas hacia las redes de destino o que estas no representen la ruta más óptima.

En la figura 1, se muestra la adyacencia de vecino del R1. Este comando muestra el siguiente resultado para cada vecino:

* **Neighbor ID:** la ID del router vecino.
* **Pri:** la prioridad OSPF de la interfaz. El valor se utiliza en la elección del DR y del BDR.
* **State:** el estado de OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen LSDB de OSPF idénticas. En el caso de redes de accesos múltiples como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. El guion indica que no se requiere ningún DR o BDR debido al tipo de red.
* **Dead Time:** la cantidad de tiempo restante que el router espera para recibir un paquete de saludo OSPF del vecino antes de declararlo inactivo. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
* **Interface ID:** la ID de interfaz o de enlace.
* **Interface:** la interfaz en la que este router formó adyacencia con el vecino.

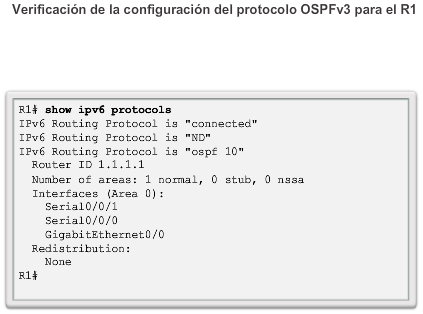
Utilice el verificador de sintaxis de la figura 2 para verificar los vecinos del R2 y el R3 con el comando **show ipv6 ospf neighbor**.



Como se muestra en la figura 1, el comando **show ipv6 protocols** es una manera rápida de verificar la información fundamental de configuración OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

Utilice el verificador de sintaxis de la figura 2 para verificar la configuración del protocolo OSPF del R2 y el R3 con el comando **show ipv6 protocols**.

Además, utilice el comando **show ipv6 ospf** para examinar la ID del proceso OSPFv3 y la ID del router. Este comando muestra información del área OSPF y la última vez que se calculó el algoritmo SPF.

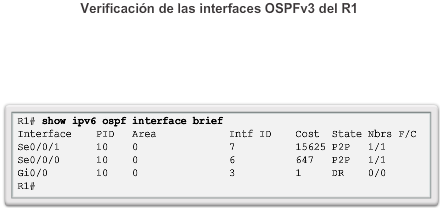


La forma más rápida de verificar la configuración de interfaz OSPF es utilizar el comando **show ipv6 ospf interface**. Proporciona una lista detallada para cada interfaz con OSPF habilitado.

Para recuperar y ver un resumen de las interfaces con OSPFv3 habilitado en el R1, utilice el comando **show ipv6 ospf interface brief**, como se muestra en la figura 1.

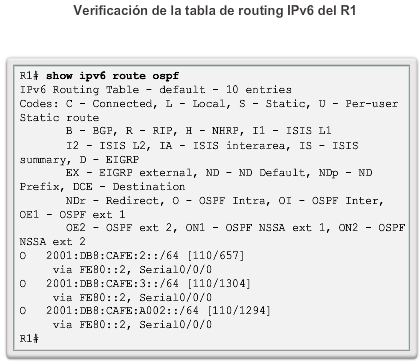
Utilice el verificador de sintaxis de la figura 2 para ver un resumen de las interfaces con OSPF habilitado en el R2 mediante el comando **show ipv6 ospf interface brief**. Observe que especificar el nombre de la interfaz como se hace en el comando **show ipv6 ospf interface serial 0/0/1** proporciona información detallada de OSPF.

Continúe utilizando el verificador de sintaxis de la figura 2 para obtener un resumen de las interfaces con OSPF habilitado en el R3 mediante el comando **show ipv6 ospf interface brief**. Recupere y vea información adicional de la interfaz Serial 0/0/0 con el comando **show ipv6 ospf interface serial 0/0/0**.



En la figura 1, el comando **show ipv6 route ospf** proporciona datos específicos sobre las rutas OSPF en la tabla de routing.

Utilice el verificador de sintaxis de la figura 2 para verificar la tabla de routing OSPFv3 del R2 y el R3; use el comando **show ipv6 route ospf**.



## Resumen

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 es un protocolo de routing de estado de enlace sin clase con una distancia administrativa predeterminada de 110 y se indica en la tabla de routing con el código de origen de ruta **O**.

OSPF se habilita con el comando **router ospf***id-proceso* del modo de configuración global. El valor *id-proceso*tiene importancia en el ámbito local, lo que significa que no necesita coincidir con otros routers OSPF para establecer adyacencias con esos vecinos.

El comando **network** utilizado con OSPF cumple la misma función que cuando se lo utiliza con otros protocolos de routing IGP, pero con una sintaxis ligeramente diferente. El valor *máscara-wildcard* es el valor inverso a la máscara de subred, y el valor *id-área* se debe establecer en **0**.

De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos de accesos múltiples y punto a punto, y cada 30 segundos en los segmentos NBMA (Frame Relay, X.25, ATM), y OSPF los usa para establecer adyacencias de vecinos. De manera predeterminada, el intervalo muerto es equivalente a cuatro veces el valor del intervalo de saludo.

Para que los routers establezcan una adyacencia, sus intervalos de saludo, intervalos muertos, tipos de red y máscaras de subred deben coincidir. Use el comando **show ip ospf neighbors** para verificar las adyacencias OSPF.

En una red de accesos múltiples, OSPF elige un DR para que funcione como punto de recopilación y distribución de las LSA enviadas y recibidas. Un BDR se elige para cumplir la función del DR en caso de que este falle. Todos los demás routers se conocen como DROTHER. 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 comando **show ip protocols** se utiliza para verificar la información importante de configuración OSPF, incluidas la ID del proceso OSPF, la ID del router y las redes que anuncia el router.

OSPFv3 se habilita en una interfaz, no en el modo de configuración del router. OSPFv3 necesita que se configuren direcciones link-local. Se debe habilitar el routing de unidifusión IPv6 para OSPFv3. Para habilitar una interfaz para OSPFv3, antes se requiere una ID de router de 32 bits.