

Nivel de Red Enrutamiento dinámico

Este capítulo se desarrollarán los contenidos relativos al nivel de red del modelo de referencia OSI e Internet en las redes de ordenadores. Nos centraremos en los protocolos de enrutamiento dinámico tanto para IPv4 como para IPv6.



Nivel de red - Enrutamiento dinámico by Rafael Lozano is licensed under a [Creative Commons Reconocimiento-NoComercial-CompartirIgual 3.0 España License](https://creativecommons.org/licenses/by-nc-sa/3.0/es/).

Tabla de contenido

1	Introducción.....	1
2	RIP y RIPv2 en IPv4.....	2
2.1	Habilitar RIP.....	3
2.2	Anunciar redes.....	3
2.3	Habilitar RIPv2.....	4
2.4	Deshabilitar el resumen de rutas automático.....	5
2.5	Configurar las interfaces pasivas.....	5
2.6	Propagar la ruta predeterminada.....	6
2.7	Verificar el enrutamiento RIP.....	7
3	RIP en IPv6: RIPng.....	10
3.1	Habilitar RIPng en las interfaces.....	11
3.2	Publicar ruta por defecto.....	12
3.3	Publicar rutas a LANs.....	13
4	OSPF en IPv4.....	14
4.1	Componentes OSPF.....	15
4.1.1	Mensajes del protocolo.....	15
4.1.2	Estructuras de datos.....	15
4.1.3	Algoritmo.....	16
4.1.4	Coste del enlace.....	16
4.2	Pasos para alcanzar la convergencia.....	16
4.3	Área OSPF.....	18
4.4	Paquetes OSPF.....	21
4.5	Funcionamiento OSPF.....	21
4.5.1	Estados de funcionamiento.....	22
4.5.2	Establecimiento de adyacencias de vecinos.....	23
4.5.3	Sincronización de bases de datos OSPF.....	24
4.6	Configuración de OSPFv2 de área única.....	24
4.6.1	Habilitar OSPFv2 en los routers.....	25
4.6.2	Publicar redes.....	26
4.6.3	Configuración OSPF en las interfaces.....	27
4.6.4	Interfaces pasivas.....	28
4.6.5	Red punto a punto.....	28
4.6.6	Propagar ruta predeterminada.....	29
4.6.7	Comprobación de OSPF.....	30
4.7	Configuración OSPFv2 multiárea.....	32
4.7.1	Habilitar OSPFv2 en cada router.....	33
4.7.2	Publicar redes.....	34
4.7.3	Interfaces pasivas.....	35
4.7.4	Publicar la ruta por defecto.....	35
4.7.5	Comprobación OSPFv2.....	35
4.7.6	Resumen de rutas.....	38

4.8 Redes OSPF de acceso múltiple.....	40
4.8.1 Router designado.....	41
5 OSPF en IPv6.....	42
5.1 Configuración de OSPFv3 de área única.....	42
5.1.1 Habilitar OSPFv3 en las interfaces.....	43
5.1.2 Publicar ruta predeterminada.....	44
5.1.3 Publicar rutas a LANs.....	44
5.1.4 Comprobar OSPFv3.....	45
5.2 Configuración de OSPFv3 en multiárea.....	46
5.2.1 Habilitar OSPFv3 en las interfaces.....	47
5.2.2 Publicar al ruta predeterminada.....	49
5.2.3 Publicar rutas LANs.....	49
5.2.4 Comprobación OSPFv3.....	51
5.2.5 Resumen de rutas.....	52
6 Bibliografía.....	55

Nivel de red

Enrutamiento dinámico

1 Introducción

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

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

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

Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y ofrecer esta información automáticamente en sus propias tablas de enrutamiento. Los protocolos de enrutamiento determinan la mejor ruta hacia cada red y, a continuación, esa ruta se ofrece a la tabla de enrutamiento. La ruta se instalará en la tabla de enrutamiento si no hay otro origen de enrutamiento con una distancia administrativa menor.

Las ventajas del enrutamiento dinámico son:

- ✓ Adecuado en las topologías donde se requieren varios routers.
- ✓ Independiente del tamaño de la red.
- ✓ Si es posible, adapta automáticamente la topología para volver a enrutar tráfico.

Sin embargo, también tiene unos inconvenientes:

- ✓ La implementación también puede ser más compleja.
- ✓ Es menos seguro. Se requieren opciones de configuración adicionales para proporcionar protección.
- ✓ La ruta depende de la topología actual.
- ✓ Requiere CPU, RAM y ancho de banda adicional.

2 RIP y RIPv2 en IPv4

Si bien el protocolo RIP se utiliza con muy poca frecuencia en las redes modernas, es útil como base para comprender el enrutamiento de red básico. Esta sección se proporciona una breve descripción general de la forma en que se configuran los valores básicos de RIP y RIPv2.

Como red de ejemplo para ilustrar el enrutamiento dinámico disponemos de la siguiente red donde ya hemos configurados las direcciones IP en cada dispositivo.

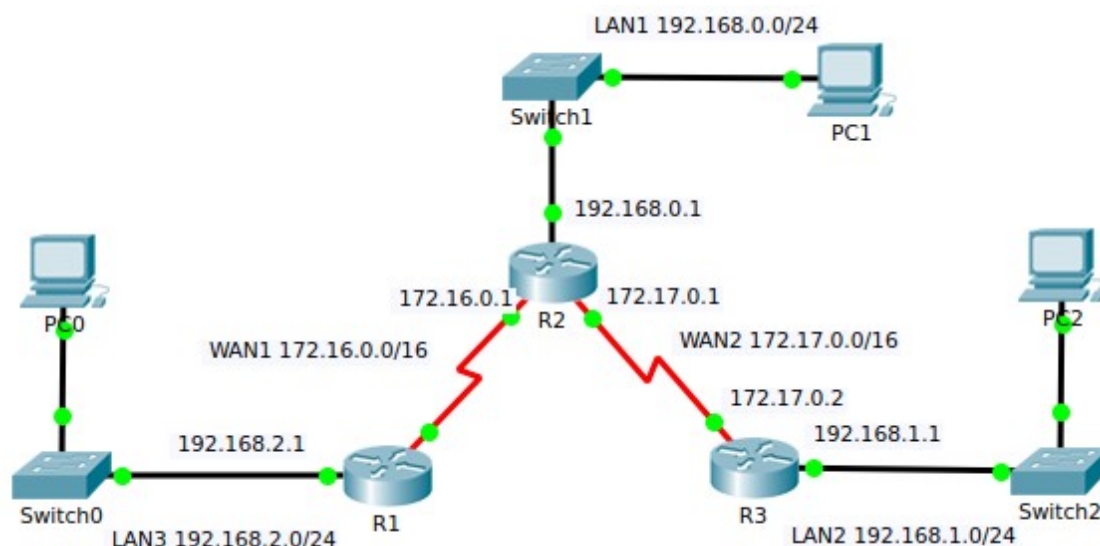


Figura 1.- Red de ejemplo para RIP

No hay rutas estáticas configuradas ni protocolos de enrutamiento habilitados, por lo que el acceso remoto de red es imposible en este momento. Para configurar el protocolo RIP necesitamos realizar los siguientes pasos:

1. Habilitar RIP en el router.
2. Anunciar las redes a las que el router está conectado.
3. Habilitar RIP v2.
4. Deshabilitar el resumen de rutas automático.
5. Configurar las interfaces pasivas.
6. Propagar la ruta predeterminada.

Vamos a verlos en detalle cada uno de ellos

2.1 Habilitar RIP

Para habilitar RIP, usamos el comando `router rip` del modo de configuración global. Por ejemplo, en el router R1 habilitamos RIP.

```
R1>enable
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#router rip
R1(config-router)#
```

Este comando no inicia el proceso del RIP. En cambio, proporciona acceso al modo de configuración del router, donde se configuran los parámetros de enrutamiento RIP. Al habilitar RIP, la versión predeterminada es RIPv1.

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

2.2 Anunciar redes

Al ingresar en el modo de configuración de router RIP, el router recibe instrucciones para que ejecute RIPv1. Pero el router aún necesita conocer las interfaces locales que deberá utilizar para comunicarse con otros routers, así como las redes conectadas en forma local que deberá publicar a dichos routers.

Para habilitar el enrutamiento RIP para una red, usamos el comando del modo de configuración del router `network dirección de red`. El argumento es la dirección de red con clase para cada red conectada directamente. Este comando realiza lo siguiente:

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

Siguiendo con R1 escribiríamos lo siguiente

```
R1>enable
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)#router rip
R1(config-router)#network 192.168.2.0
R1(config-router)#network 172.16.0.0
R1(config-router)#
```

Nótese que al indicar la dirección de red no se especifica ninguna máscara. RIPv1 es un protocolo de enrutamiento con clase para IPv4. Por lo tanto, si se introduce una dirección de subred, el IOS la convierte automáticamente a la dirección de red con clase. Por ejemplo, si se introduce el comando `network 192.168.1.32`, se convertiría automáticamente a `network 192.168.1.0` en el archivo de configuración en ejecución. El IOS no proporciona un mensaje de error, sino que corrige la entrada e introduce la dirección de red con clase.

Para R2 tendríamos lo siguiente

```
R2>enable
R2#enable
R2#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R2(config)#router rip
R2(config-router)#network 192.168.0.0
R2(config-router)#network 172.17.0.0
R2(config-router)#network 172.16.0.0
R2(config-router)#
```

Finalmente en R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R3(config)#router rip
R3(config-router)#network 192.168.1.0
R3(config-router)#
```

2.3 Habilitar RIPv2

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

Para habilitar RIPv2 utilizamos el comando `version 2` como se muestra a continuación.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#
```

El proceso de RIP ahora incluye la máscara de subred en todas las actualizaciones, lo que hace que RIPv2 sea un protocolo de enrutamiento sin clase.

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

Ahora mismo ya no hay rutas RIP en la tabla de enrutamiento de R1. Esto se debe a que el R1 ahora está a la escucha de actualizaciones RIPv2 únicamente. El R2 y el R3 todavía envían actualizaciones RIPv1. Por lo tanto, se debe configurar el comando `version 2` en todos los routers en el dominio de enrutamiento.

2.4 Deshabilitar el resumen de rutas automático

RIPv2 resume automáticamente las redes en los límites de red principales de manera predeterminada, al igual que RIPv1. Para modificar el comportamiento predeterminado de RIPv2 de resumen automático, utilice el comando del modo de configuración del router `no auto-summary`. Este comando no tiene ningún efecto cuando se utiliza RIPv1. Cuando se deshabilita el resumen automático, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos. RIPv2 ahora incluye todas las subredes y sus máscaras correspondientes en sus actualizaciones de enrutamiento.

```
R1(config-router)#no auto-summary
R1(config-router)#
```

2.5 Configurar las interfaces pasivas

De manera predeterminada, las actualizaciones de RIP se reenvían por todas las interfaces con RIP habilitado. Sin embargo, las actualizaciones de RIP solo se deben enviar por interfaces conectadas a otros routers con RIP habilitado.

Si vemos nuestra red de ejemplo el router R1 envía actualizaciones de RIP por la interfaz G0/0, aunque no existen ningún router conectado en esa LAN. No hay manera de que el R1 tenga información acerca de esto y, como resultado, envía una actualización cada 30 segundos. El envío de actualizaciones innecesarias a una LAN impacta en la red de tres maneras:

- ✓ Desperdicio de ancho de banda.- Se utiliza ancho de banda para transportar actualizaciones innecesarias. Dado que las actualizaciones de RIP se transmiten por difusión o multidifusión, los switches también reenvían las actualizaciones por todos los puertos.

- ✓ Desperdicio de recursos.- Todos los dispositivos en la LAN deben procesar la actualización hasta las capas de transporte, punto en el cual los dispositivos descartan la actualización.
- ✓ Riesgo de seguridad.- El anuncio de actualizaciones en una red de difusión constituye un riesgo de seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.

Para evitar que las actualizaciones de enrutamiento se transmitan a través de una interfaz del router usamos el comando de configuración del router `passive-interface`. El comando detiene las actualizaciones de enrutamiento a través de la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de enrutamiento enviadas a otras interfaces.

```
R1(config-router)#passive-interface g0/0
R1(config-router)#
```

En nuestro ejemplo no es necesario que el R1, el R2, y el R3 reenvíen actualizaciones RIP por sus interfaces LAN.

2.6 Propagar la ruta predeterminada

En nuestra red de ejemplo hemos añadido una conexión de R1 a Internet a través de un módem DSL. En esta situación, el R1 es el router perimetral con una conexión simple a un proveedor de servicios. Por lo tanto, para que el R1 llegue a Internet, solo se requiere una ruta estática predeterminada desde la interfaz Serial 0/0/1.

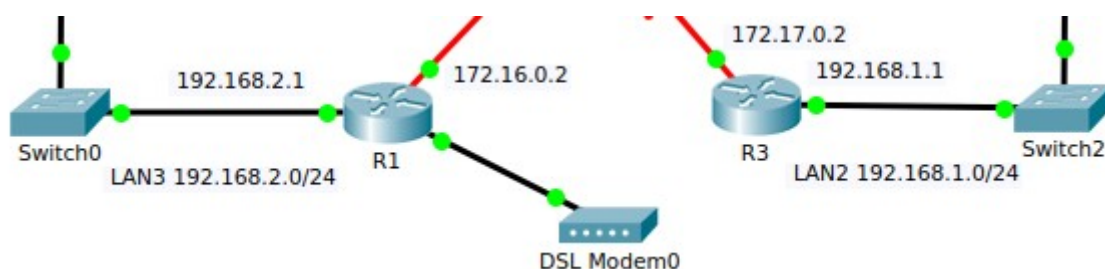


Figura 2.- Conexión a Internet

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

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

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

Según el diagrama de red modificado establecemos la ruta por defecto.

```
R1>enable
R1#configure terminal
R1(config)#ip route 0.0.0.0 0.0.0.0 g0/1
R1(config)#
```

Ahora publicamos la ruta por defecto a los demás routers

```
R1(config)#router rip
R1(config-router)#default-information originate
R1(config-router)#
```

2.7 Verificar el enrutamiento RIP

El comando `show ip protocols` muestra los parámetros del protocolo de enrutamiento IPv4 configurados actualmente en el router. El resultado del comando en R1 es el siguiente.

```
R1#show ip protocols
enrutamiento Protocol is "rip"
Sending updates every 30 seconds, next due in 2 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any
version
  Interface          Send  Recv  Triggered RIP  Key-
chain
  GigabitEthernet0/0  1      2  1
  Serial0/0/0        1      2  1
Automatic network summarization is in effect
Maximum path: 4
enrutamiento for Networks:
  172.16.0.0
  192.168.2.0
Passive Interface(s):
enrutamiento Information Sources:
  Gateway      Distance      Last Update
  172.16.0.1    120          00:00:01
Distance: (default is 120)
```

R1#

Este resultado confirma la mayoría de los parámetros de RIP, incluido lo siguiente:

1. El enrutamiento RIP está configurado y en ejecución en el router R1.
2. Los valores de diversos temporizadores; por ejemplo, el R1 envía la siguiente actualización de enrutamiento en 2 segundos.
3. La versión de RIP configurada actualmente es RIPv1.
4. El R1 realiza la sumarización en el límite de la red con clase.
5. El R1 anuncia las redes con clase. Estas son las redes que el R1 incluye en sus actualizaciones RIP.
6. Los vecinos RIP se indican mediante la inclusión de la dirección IP del siguiente salto, la AD asociada que el R2 utiliza para las actualizaciones enviadas por ese vecino y el momento en que dicho vecino recibió la última actualización.

El comando `show ip route` muestra las rutas RIP instaladas en la tabla de enrutamiento. La siguiente salida es para R1.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
       * - candidate default, U - per-user static route, o
- ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.16.0.0/16 is variably subnetted, 2 subnets, 2
masks
C       172.16.0.0/16 is directly connected, Serial0/0/0
L       172.16.0.2/32 is directly connected, Serial0/0/0
R       172.17.0.0/16 [120/1] via 172.16.0.1, 00:00:27,
Serial0/0/0
R       192.168.0.0/24 [120/1] via 172.16.0.1, 00:00:27,
Serial0/0/0
R       192.168.1.0/24 [120/2] via 172.16.0.1, 00:00:21,
Serial0/0/0
```

```

    192.168.2.0/24 is variably subnetted, 2 subnets, 2
masks
C      192.168.2.0/24 is directly connected,
GigabitEthernet0/0
L      192.168.2.1/32 is directly connected,
GigabitEthernet0/0

R1#

```

Como se puede apreciar en las tres líneas remarcadas se dispone de rutas descubiertas por RIP para acceder a cada una de las redes de los routers vecinos.

A continuación la salida del mismo comando en R2. Además de las rutas obtenidas por RIP de los routers vecinos observamos como la ruta marcada con R* es la ruta por defecto descubierta por RIP publicada por R1.

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
       * - candidate default, U - per-user static route, o
- ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.0.2 to network 0.0.0.0

    172.16.0.0/16 is variably subnetted, 2 subnets, 2
masks
C      172.16.0.0/16 is directly connected, Serial0/0/1
L      172.16.0.1/32 is directly connected, Serial0/0/1
    172.17.0.0/16 is variably subnetted, 2 subnets, 2
masks
C      172.17.0.0/16 is directly connected, Serial0/0/0
L      172.17.0.1/32 is directly connected, Serial0/0/0
    192.168.0.0/24 is variably subnetted, 2 subnets, 2
masks
C      192.168.0.0/24 is directly connected,
GigabitEthernet0/0
L      192.168.0.1/32 is directly connected,
GigabitEthernet0/0
R*    192.168.1.0/24 [120/1] via 172.17.0.2, 00:00:05,
Serial0/0/0

```

```
R 192.168.2.0/24 [120/1] via 172.16.0.2, 00:00:10,
Serial0/0/1
R* 0.0.0.0/0 [120/1] via 172.16.0.2, 00:00:10,
Serial0/0/1
```

Para finalizar se aprecia en las salidas de los comandos que el protocolo de enrutamiento RIP origina rutas con una distancia administrativa de 120, por tanto las rutas estáticas tienen precedencia.

3 RIP en IPv6: RIPng

RIPng en IPv6 ofrece las mismas funciones y beneficios que en IPv4. Aunque la configuración RIP cambia con respecto a IPv4. Vamos a ver los pasos necesarios para configurar RIP en un router Cisco utilizando la siguiente red de ejemplo.

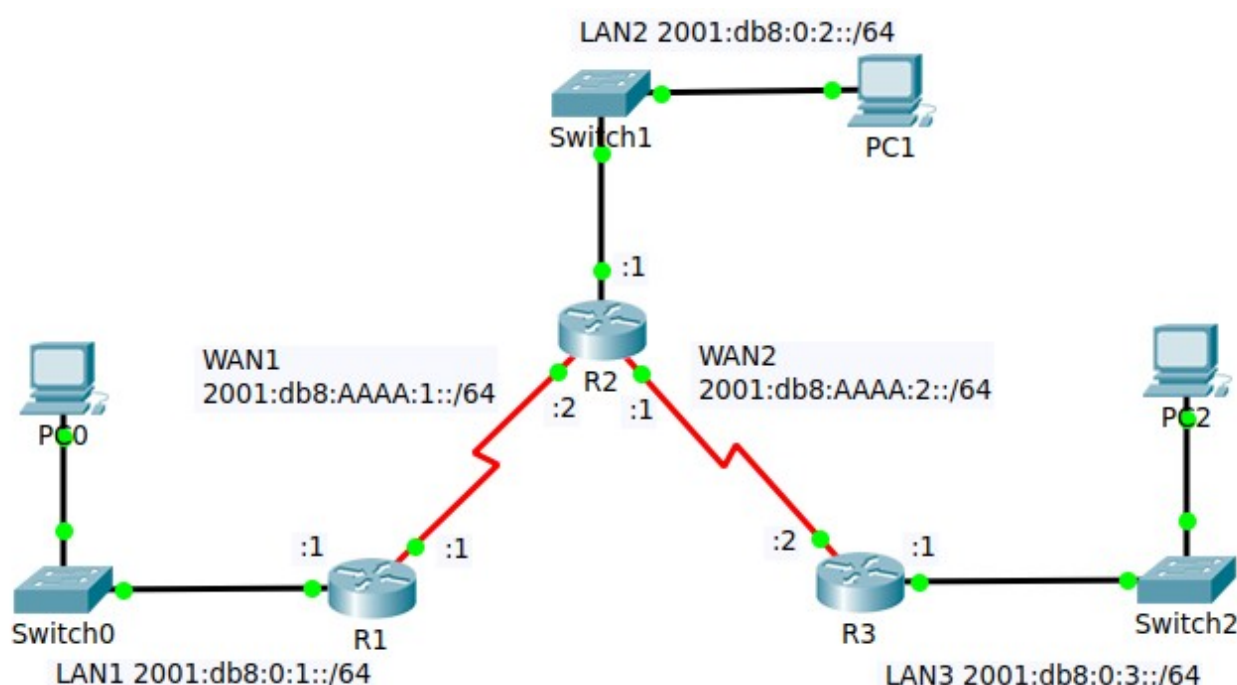


Figura 3.- Red de ejemplo para RIP en IPv6

De nuevo suponemos que todas las interfaces están configuradas. No hay rutas estáticas configuradas ni protocolos de enrutamiento habilitados, por lo que el acceso remoto de red es imposible en este momento. Para configurar el protocolo RIPng necesitamos realizar los siguientes pasos:

3.1 Habilitar RIPng en las interfaces

Para habilitar RIP IPv6 en un router debemos ejecutar los siguientes comandos

```
R1>enable
R1#configure terminal
```

```
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface s0/0/0
R1(config-if)#ipv6 rip proceso1 enable
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 rip proceso1 enable
R1(config-if)#
```

Como vemos en el código anterior RIP se habilita en cada interfaz sobre la que se quieran enviar mensajes de RIP a routers vecinos. El comando de modo de configuración de `interfaz ipv6 rip nombre enable` habilita un proceso de enrutamiento RIP sobre una interfaz.

RIP se habilita en una interfaz y no en el modo de configuración del router. De hecho no hay un comando `network network-address` disponible en RIP. En lugar de eso para habilitar RIP se debe entrar en el modo de configuración de la interfaz donde sea desea publicar RIP y ejecutamos el comando `ipv6 rip nombre enable`.

El *nombre* puede ser un número o una palabra. Este identificador puede ser el mismo o diferente en toda la red RIP, sin embargo es necesario que en el router todas las interfaces pertenezcan al mismo proceso.

Es importante decir que este comando se debe de habilitar en todas las interfaces que se deseen publicar aunque no estén conectadas con ninguna otra para que puedan ser publicadas. De ahí que también se haya habilitado en la interfaz s0/0/1.

En el router R2 tendríamos que configurar RIP en las dos interfaces serial de la siguiente forma.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#interface s0/0/0
R2(config-if)#ipv6 rip proceso2 enable
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 rip proceso2 enable
R2(config-if)#
```

Y finalmente en el router R3

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#interface s0/0/0
```

```
R3(config-if)#ipv6 rip proceso3 enable
R3(config-if)#interface s0/0/1
R3(config-if)#ipv6 rip proceso3 enable
R3(config-if)#
```

Una vez se ha habilitado RIP en todas los routers e interfaces podemos ver la tabla de enrutamiento y comprobar como se han añadido rutas mediante RIPng.

```
show ipv6 route
```

3.2 Publicar ruta por defecto

El proceso para propagar la ruta por defecto en RIPng es similar a RIPv2 excepto en que la ruta estática predeterminada debe estar definida. Por ejemplo, supongamos que R1 tiene una conexión a Internet a través de la interfaz G0/1 con dirección IPv6 2001:A:B:C::1/64. Nuestro esquema de red se amplía con una conexión de R1 a un modem DSL.

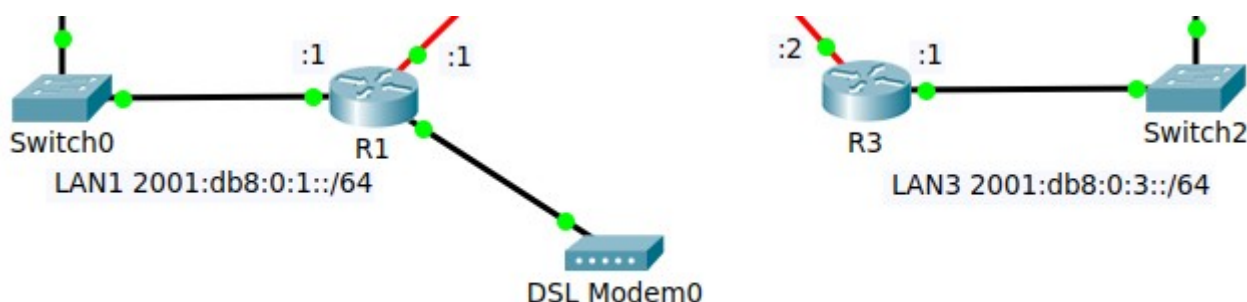


Figura 4.- Conexión a Internet en R1

Para propagar la ruta predeterminada el router R1 debe se configurada con

```
R1(config)#ipv6 route ::/0 g0/1
```

A continuación ejecutamos el siguiente comando en el modo de configuración de la interfaz

```
R1(config)#interface s0/0/0
R1(config-if)#ipv6 rip proceso1 default-information
originate
R1(config-if)#
```

Vemos que estamos publicando la ruta predeterminada por la interfaz que está conectada a otros routers, no por donde está la conexión a Internet. Este último comando indica a R1 que es la fuente de la información sobre la ruta predeterminada y la propague en mensajes de actualización de RIPng por todas las interfaces donde RIPng esté habilitado.

Si consultamos la tabla de enrutamiento de R2 veremos la siguiente ruta

```
R2>enable
```

```
R2#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B -
BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
- ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R   ::/0 [120/1]
    via FE80::290:21FF:FE99:1701, Serial0/0/0
```

Si consultamos la tabla de enrutamiento en R3 veremos también la ruta por defecto propagada.

3.3 Publicar rutas a LANs

Cuando habilitamos RIPng en las interfaces omitimos aquellas conectadas a LANs las cuales no están conectadas a ningún router y no tiene sentido enviar mensajes RIPng por ellas. Sin embargo, esto provoca que la red LAN conectada a dicha interfaz no se publique y por tanto no se enviaría la ruta para llegar a dicha LAN a otros routers.

En IPv4 disponíamos el comando `passive-interface interfaz` pero en RIPng no es así. En este caso disponemos del comando `redistribute connected` del modo de configuración del router RIP. Por ejemplo, en el router R1 queremos publicar la ruta de LAN con dirección 2001:db8:0:1::/64. Sería de la siguiente forma

```
R1(config)#ipv6 router rip proceso1
R1(config-rtr)#redistribute connected
R1(config-rtr)#
```

Si consultamos la tabla de enrutamiento de R2 veremos las siguientes rutas

```
R2#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B -
BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
- ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
R   ::/0 [120/1]
    via FE80::290:21FF:FE99:1701, Serial0/0/0
R  2001:A:B:C::/64 [120/1]
```



```

R    via FE80::290:21FF:FE99:1701, Serial0/0/0
    2001:DB8:0:1::/64 [120/1]
    via FE80::290:21FF:FE99:1701, Serial0/0/0
...

```

Vemos que las dos últimas son rutas conectadas directamente en el router R1. La primera corresponde a la red conectada a Internet mientras que la segunda corresponde a la LAN.

Tendríamos que hacer la misma configuración en R2 y R3 para que estos routers publicaran las rutas de las redes LAN que conectan.

4 OSPF en IPv4

Open Shortest Path First (OSPF), Primero el Camino Más Corto, es un protocolo de red para enrutamiento dinámico que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. La implementación de Cisco soporta las siguientes características:

- ✓ Definición de áreas de red.
- ✓ Redistribución de rutas. Las rutas aprendidas por cualquier protocolo de enrutamiento se distribuyen.
- ✓ Autenticación.- Dentro de un área de la red los routers se autentican mediante texto plano o MD5.
- ✓ Parámetros de interfaz de enrutamiento.- Se soporta la configuración de parámetros en las interfaces de red como el coste, intervalo de retransmisión, prioridad del router y clave de autenticación, entre otros.
- ✓ Soporte de enlaces virtuales.
- ✓ Filtrado y resumen de rutas.

El protocolo OSPF es un protocolo de enrutamiento de estado de enlace que se desarrolló como una alternativa al Protocolo de Información de Enrutamiento del Vector de Distancia (RIP). RIP fue un protocolo de enrutamiento aceptable en los primeros días de las redes e Internet. 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. El OSPF tiene ventajas significativas sobre el RIP en el sentido que ofrece una convergencia más rápida y se escala a implementaciones de redes mucho más grandes.

OSPF es un protocolo de enrutamiento de estado de enlace que utiliza el concepto de áreas. Un administrador de red puede dividir el dominio de enrutamiento en áreas distintas que ayudan a controlar el tráfico de actualización de enrutamiento. Un enlace es una interfaz en un router. Un vínculo es también un segmento de red que conecta dos routers, o una red auxiliar, como una LAN Ethernet que está conectada a un único router. La información sobre

el estado de un enlace se conoce como estado de enlace. Toda la información del estado del enlace incluye el prefijo de red, la longitud del prefijo y el costo.

4.1 Componentes OSPF

Todos los protocolos de enrutamiento comparten componentes similares. Todos usan mensajes de protocolo de enrutamiento para intercambiar información de rutas. Los mensajes contribuyen a construir las estructuras de datos, que luego se procesan con un algoritmo de enrutamiento.

4.1.1 Mensajes del protocolo

Los routers que ejecutan OSPF intercambian mensajes para transmitir información de enrutamiento por medio de cinco tipos de paquetes. Estos paquetes son los siguientes:

- ✓ Paquete Hello
- ✓ 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 enrutamiento, a fin de mantener información precisa acerca de la red.

4.1.2 Estructuras de datos

Los mensajes OSPF se utilizan para crear y mantener tres bases de datos OSPF, como se indica a continuación:

- ✓ Base de datos de adyacencia → Se emplea para crear la tabla de vecinos que consiste en una lista de todos los routers vecinos a los que se ha conectado un router. Esta tabla es única para cada router y se puede consultar con el comando `show ip ospf neighbor`.
- ✓ Base de datos de estado de enlace (LSDB) → Se emplea para crear la tabla de topología la cual muestra información sobre todos los otros routers en la red. Esta base de datos representa la topología de la red y todos los routers dentro de un área tienen LSDB idénticas. Se puede ver con el comando `show ip ospf database`.
- ✓ Base de datos de reenvío → Se emplea para crear la tabla de enrutamiento con las rutas generadas cuando se ejecuta un algoritmo en la base de datos de estado de enlace. La tabla de enrutamiento de cada router es única y contiene información sobre cómo y dónde enviar paquetes a otros routers. Se puede ver con el comando `show ip route`.

Estas tablas contienen una lista de routers vecinos para intercambiar información de enrutamiento. Las tablas se almacenan y mantienen en RAM.

4.1.3 Algoritmo

El router construye la tabla de topología empleando los resultados de cálculos realizados a partir del algoritmo SPF (Primero la ruta más corta) 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 del árbol 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 crear la tabla de enrutamiento.

4.1.4 Coste del enlace

En RIP la medida de métrica es el número de saltos necesarios para alcanzar la red de destino. En OSPF es el coste que se calcula en función del ancho de banda de cada enlace. En este caso, cada enlace se etiqueta con un coste que se calcula dividiendo 10^8 /ancho de banda del enlace. El ancho de banda de referencia es 100Mbps, de ahí que el dividendo sea 10^8 . Así que cualquier enlace a 100 Mbps o superior tiene una métrica de 1. El cálculo de la métrica para cada enlace sería el siguiente

- ✓ Interfaz serial → Tiene un ancho de banda de 1544 Kbps. Por tanto $100 \text{ Mbps} / 1544 \text{ Kbps} = 64$
- ✓ Interfaz FastEthernet → $100 \text{ Mbps} / 100 \text{ Mbps} = 1$
- ✓ Interfaz Gigabit Ethernet → Una interfaz gigabit tiene un coste de 1.

Cuando se propagan rutas por OSPF cada una tiene asociada la distancia administrativa del protocolo OSPF (110) y una métrica que es la suma de los costos de los enlaces necesarios para llegar a la red de destino en la ruta.

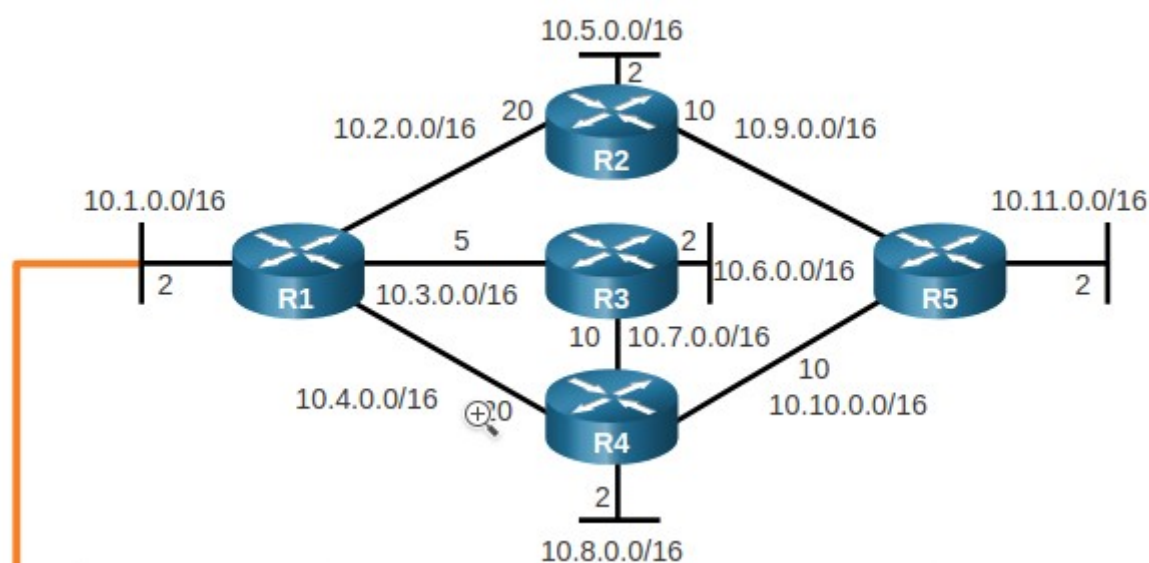
4.2 Pasos para alcanzar la convergencia

Los routers OSPF realizan el siguiente proceso genérico de enrutamiento de estado de enlace para alcanzar un estado de convergencia: En OSPF, el costo de cada enlace se utiliza para determinar la mejor ruta al destino. Los siguientes son los pasos de enrutamiento de estado de enlace que completa un router

- ✓ Establecimiento de adyacencias de vecinos → Los routers con OSPF habilitado, deben reconocerse entre sí en la red antes de que puedan compartir información. Los routers con OSPF habilitado envían paquetes *hello* 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.
- ✓ Intercambio de anuncios de estado de enlace → Después de establecer las adyacencias, los routers intercambian anuncios 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.

- ✓ Crear la base de datos de estado de enlace → Una vez que se reciben los LSA, los routers con OSPF crean la tabla de topología (LSDB) en función de los LSA recibidos. Esta base de datos finalmente contiene toda la información sobre la topología del área.
- ✓ Ejecución del algoritmo SPF → A continuación, los routers ejecutan el algoritmo SPF para crea el árbol SPF.
- ✓ Elección de la mejor ruta → Después de construir el árbol SPF, se ofrecen las mejores rutas a cada red a la tabla de enrutamiento IP. La ruta será insertada en la tabla de enrutamiento, a menos que haya una ruta a la misma red con una distancia administrativa menor, como por ejemplo una ruta estática.



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

Figura 5: Elección de la mejor ruta OSPF

4.3 Área OSPF

Para que OSPF sea más eficaz y escalable, este protocolo admite el enrutamiento jerárquico mediante áreas. Una red OSPF puede dividirse en subdominios llamadas áreas. Un área es una colección lógica de redes OSPF, routers y enlaces que tienen el mismo identificador de área. Un router dentro de un área debe mantener una base de datos de la topología del área a la que pertenece. El router no tiene información detallada de la red fuera del área, lo que reduce en un menor tamaño de la base de datos.

Las áreas limitan el ámbito de distribución de información de rutas. No es posible hacer filtrado de rutas dentro de un área. Sin embargo, el resumen y filtrado de rutas es posible entre áreas. El principal beneficio de crear áreas es reducir el número de rutas a propagar mediante el filtrado y el resumen de rutas.

Cada red OSPF se divide en diferentes áreas siguiendo estas reglas:

- ✓ Debe existir un área backbone, la cual combina un conjunto de áreas independientes

en un dominio simple.

- ✓ Cada área no backbone debe estar directamente conectada a un área backbone.
- ✓ El área backbone no se puede particionar ante fallos en la red, como caídas de enlaces o routers.

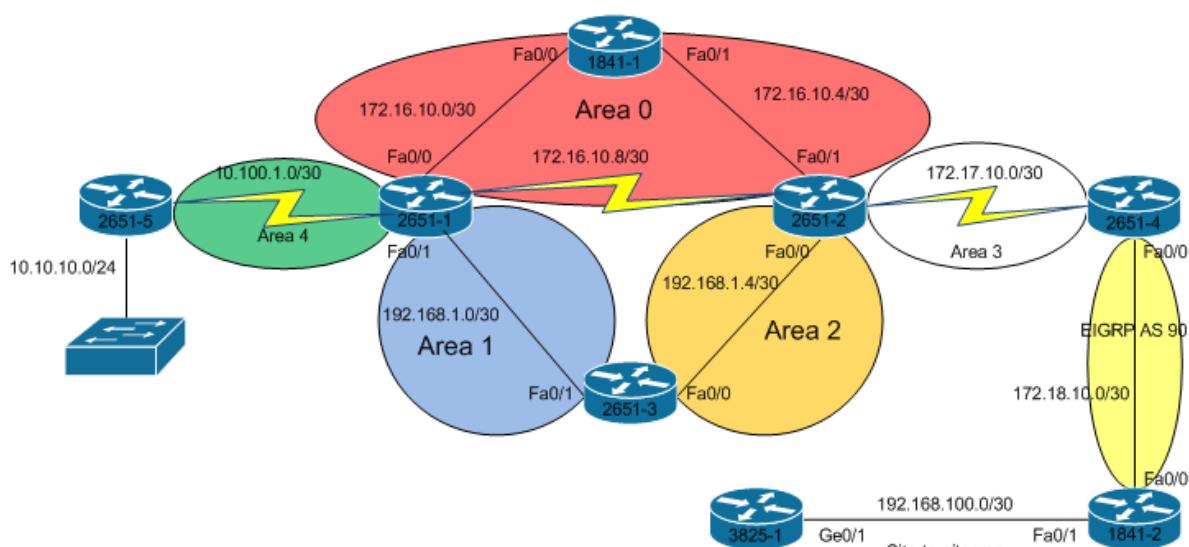


Figura 6: Áreas OSPF

Las áreas se identifican por un ID de área que se puede expresar en formato dirección IP o decimal. Si hay varias áreas en la red el ID del área backbone es 0.

En función de las áreas configuradas en las interfaces de un router podemos tener los siguientes tipos:

- ✓ Router interno (IR *Internal Router*) → Un router que tiene todas sus interfaces dentro de la misma área.
- ✓ Router perimetral (ABR *Area Boundary Router*) → Un router que tiene interfaces en varias áreas. Un router perimetral en OSPFv2 es el límite entre dos áreas.
- ✓ Router perimetral de sistema autónomo (ASBR *Autonomous System Boundary Router*) → Los routers que actúan como puertas de enlace (redistribución) entre los protocolos OSPF y otros protocolos de enrutamiento (IGRP, EIGRP, RIP, BGP, estático).

Ambos lados de cualquier enlace siempre pertenece a la misma área. OSPF se puede implementar de una de estas dos maneras:

- ✓ De área única → Todos los routers están en un área. En este caso se emplea el ID de área 0.
- ✓ Multiárea → OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área troncal (área 0). Cada interfaz del router está conectado únicamente a un área y el enlace entre dos routers también. Los routers que tienen interfaces conectadas a diferentes áreas y, por tanto, interconectan las

áreas, se denominan “routers fronterizos de área” (ABR *Area Boundary Router*).

Con OSPF multiárea, el protocolo puede dividir un dominio de enrutamiento grande en áreas más pequeñas a fin de realizar el enrutamiento jerárquico. El enrutamiento todavía ocurre entre las áreas (enrutamiento entre áreas), mientras que muchas de las operaciones de enrutamiento que son intensivas para el procesador, como el recálculo de la base de datos, se mantienen dentro de 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.

Los routers en otras áreas reciben actualizaciones sobre los cambios de topología, pero estos routers solo actualizan la tabla de enrutamiento, no vuelven 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 opciones de diseño de topología jerárquica con OSPF multiárea pueden ofrecer estas ventajas:

- ✓ Las tablas de enrutamiento son más pequeñas porque hay menos entradas. Esto se debe a que las direcciones de red se pueden resumir entre áreas. La sumaria de ruta no está habilitada de manera predeterminada.
- ✓ Sobrecarga de actualizaciones de estado de enlace reducida, el diseño de OSPF multiárea con áreas más pequeñas minimiza los requisitos de procesamiento y memoria.
- ✓ Menor frecuencia de cálculos de SPF ya que se localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de las actualizaciones de enrutamiento, debido a que la saturación con LSA se detiene en el límite del área.

Por ejemplo, en la figura R2 es un ABR para el área 51. Un cambio de topología en el área 51 provocaría que todos los routers de área 51 re-ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar sus tablas de enrutamiento IP. El ABR, R2, enviaría un LSA a los routers del área 0, que eventualmente se inundaría a todos los routers del dominio de enrutamiento OSPF. Este tipo de LSA no hace que los routers en otras áreas re-ejecuten el algoritmo SPF. Sólo tienen que actualizar su LSDB y tabla de enrutamiento.

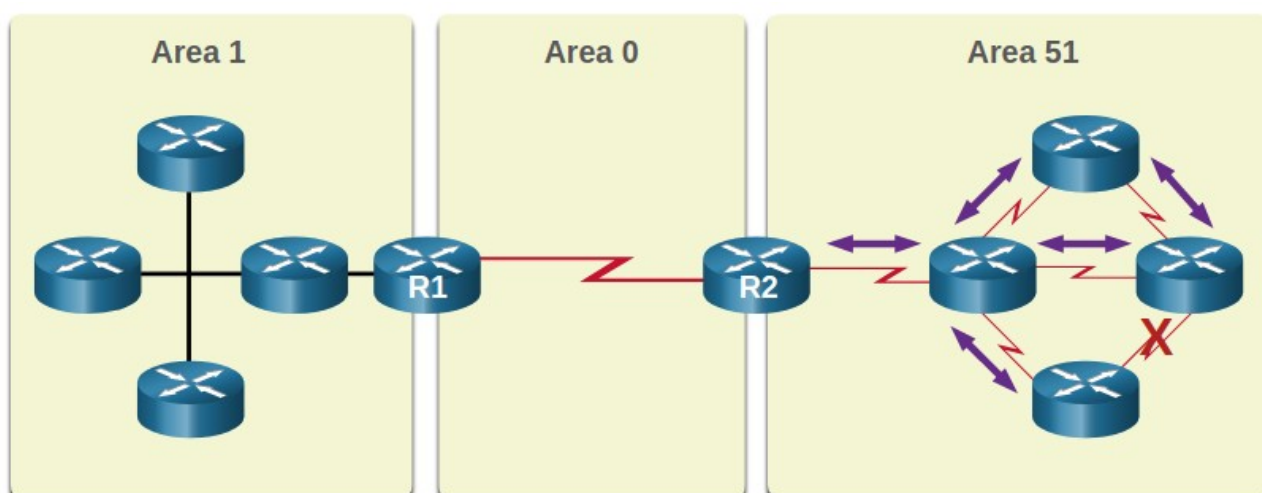


Figura 7: OSPF Multiárea

4.4 Paquetes OSPF

OSPF utiliza paquetes de estado de enlace (LSP) para establecer y mantener adyacencias de vecinos, así como para intercambiar actualizaciones de enrutamiento. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

- ✓ Paquetes Hello → Se usa para establecer y mantener la adyacencia con otros routers OSPF. Descubre los vecinos y construye adyacencias entre ellos
- ✓ Paquete de descripción de base de datos (DBD) → Contiene una lista abreviada de la 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. Controla la sincronización de bases de datos entre routers.
- ✓ Paquete de solicitud de estado de enlace (LSR) → Los routers receptores pueden requerir más información sobre cualquier entrada de la DBD.
- ✓ Paquete de actualización de estado de enlace (LSU) → Se utiliza para responder a los LSR y para anunciar nueva información.
- ✓ 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.

4.5 Funcionamiento OSPF

Ahora que conocemos los paquetes de estado de vínculo OSPF, en este apartado se explica cómo funcionan con routers habilitados para OSPF. Cuando un router OSPF se conecta inicialmente a una red, intenta hacer lo siguiente:

- ✓ Crear adyacencias con los vecinos
- ✓ Intercambiar información de enrutamiento

- ✓ Calcular las mejores rutas
- ✓ Lograr la convergencia

Un router con OSPF habilitado envía un mensaje especial, denominado paquete *hello*, por cada interfaz habilitada para OSPF para descubrir otros routers OSPF vecinos. Una vez es descubierto un vecino, los dos routers comparan información del paquete *hello* para determinar si tienen configuraciones compatibles. Los routers vecinos intentan establecer adyacencia lo que significa que los routers sincronizan su información del estado del enlace para asegurar que tienen idéntica información de enrutamiento OSPF. Routers adyacentes comparten anuncios del estado del enlace (LSA *Link State Advertisements*) que incluye información sobre el estado operacional de cada enlace, el coste del enlace y cualquier otra información del vecino.

Los routers envían los mensajes LSA que reciben por una interfaz por las otras interfaces con OSPF habilitado para que todos los routers tengan finalmente una base de datos idéntica del estado de cada enlace en la red. Cuando todos los routers OSPF tienen la misma base de datos, la red ha convergido. Entonces cada router utiliza el algoritmo de Dijkstra para construir su tabla de enrutamiento.

Las redes OSPF se dividen en áreas, tal y como vimos en el epígrafe anterior. Los routers solamente envían LSAs dentro de un área, lo que reduce los requisitos de CPU y memoria en el router.

4.5.1 Estados de funcionamiento

La tabla detalla los estados por los que OSPF transita mientras intenta alcanzar la convergencia.

Estado	Descripción
Inactivo	<ul style="list-style-type: none"> ✓ Los routers intercambian paquetes DBD. ✓ Si se requiere información adicional del router, entonces haga la transición a Loading; de lo contrario, la transición al estado Full.
Init	<ul style="list-style-type: none"> ✓ Se reciben los paquetes de hello del vecino. ✓ Estos contienen el router ID del router emisor. ✓ Transición al estado Two-Way.
Two-Way	<ul style="list-style-type: none"> ✓ En este estado, la comunicación entre los dos routers es bidireccional. ✓ En los enlaces de acceso múltiple, los routers eligen una DR y una BDR. ✓ Transición al estado ExStart.
ExStart	En redes punto a punto, los dos routers deciden qué router iniciará el intercambio de paquetes DBD y deciden sobre el número de secuencia de paquetes DBD inicial.
Exchange	<ul style="list-style-type: none"> ✓ Los routers intercambian paquetes DBD. ✓ Si se requiere información adicional del router, entonces haga la

	transición a Cargando; de lo contrario, la transición al estado Completo.
Loading	<ul style="list-style-type: none"> ✓ Las LSR y las LSU se usan para obtener información adicional de la ruta. ✓ Las rutas se procesan mediante el algoritmo SPF. ✓ Transición al estado Full.
Full	La base de datos de estado de enlace del router está completamente sincronizada.

4.5.2 Establecimiento de adyacencias de vecinos

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 hello con la ID del router por todas las interfaces con OSPF habilitado. El paquete Hello se envía a todos los routers OSPF por la dirección de multicast reservada IPv4 224.0.0.5. Sólo los routers OSPFv2 procesarán estos paquetes. El proceso OSPF utiliza la ID del router OSPF para identificar cada router en el área OSPF de manera exclusiva. El router ID es un número de 32 bits con formato similar a una dirección IP que se asigna para identificar un router de forma exclusiva entre pares OSPF.

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

1. Estado Down a estado Init → Cuando se habilita OSPFv2, las interfaces habilitadas pasan del estado Down al estado Init. El router R1 comienza a enviar paquetes de hello por todas las interfaces con OSPF habilitado para descubrir vecinos OSPF a fin de desarrollar adyacencias con ellos.
2. Estado Init → El router R2 recibe el paquete Hello de R1 y agrega el ID de R1 a su lista de vecinos. A continuación, el R2 envía un paquete de hello al R1. El paquete contiene el ID de R2 y el ID de R1 en la lista de vecinos de la misma interfaz.
3. Estado Two-Way → El router R1 recibe el paquete hello y agrega el ID de R2 a su lista de vecinos OSPF. También observa su propio ID en la lista de vecinos del paquete Hello. Cuando un router recibe un paquete de hello en el que se indica su propio ID 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 están interconectados a través de un enlace punto a punto, inmediatamente pasan del estado de dos vías al estado ExStart.
 - Si los routers se interconectan a través de una red Ethernet común, se debe elegir un router designado DR y un BDR.
4. Elección del DR y el BDR → Debido a que el R1 y el R2 se interconectan a través de una red Ethernet, se elige un DR y un BDR. Este proceso tiene lugar solo en las redes

con enlaces multipunto, como las Ethernet. Los paquetes de hello se intercambian de manera continua para mantener la información del router.

4.5.3 Sincronización de bases de datos OSPF

Después del estado Two-Way, los routers pasan a los estados de sincronización de bases de datos. Mientras que el paquete de hello 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. Este es un proceso de tres pasos, como sigue:

1. Decidir el primer router → En el estado ExStart, los dos routers deciden qué router enviará los paquetes DBD primero. El que tenga la ID de router más alta será el primer router que enviará paquetes DBD durante el estado Exchange.
2. Intercambio DBD → En el estado Exchange, los dos routers 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 del 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 cómo de actualizada es la información de estado de enlace recibida. Cuando un router recibe la DBD, realiza las siguientes acciones:
 - Confirma la recepción de la DBD con el paquete LSAck.
 - A continuación, el R1 envía paquetes DBD al R2.
 - El R2 acusa recibo al R1.
3. Enviar un LSR → El router 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. Después de cumplir con todas las LSR para un router determinado, los routers adyacentes se consideran sincronizados y en estado Full. Las actualizaciones (LSU) se envían sólo a los vecinos en las condiciones siguientes:
 - Cuando se percibe un cambio (actualizaciones incrementales).
 - Cada 30 minutos.

4.6 Configuración de OSPFv2 de área única

En los siguientes apartados veremos como configurar OSPFv2 en una topología de red de área única. Para ilustrar la configuración OSPFv2 vamos a emplear la siguiente topología de red.

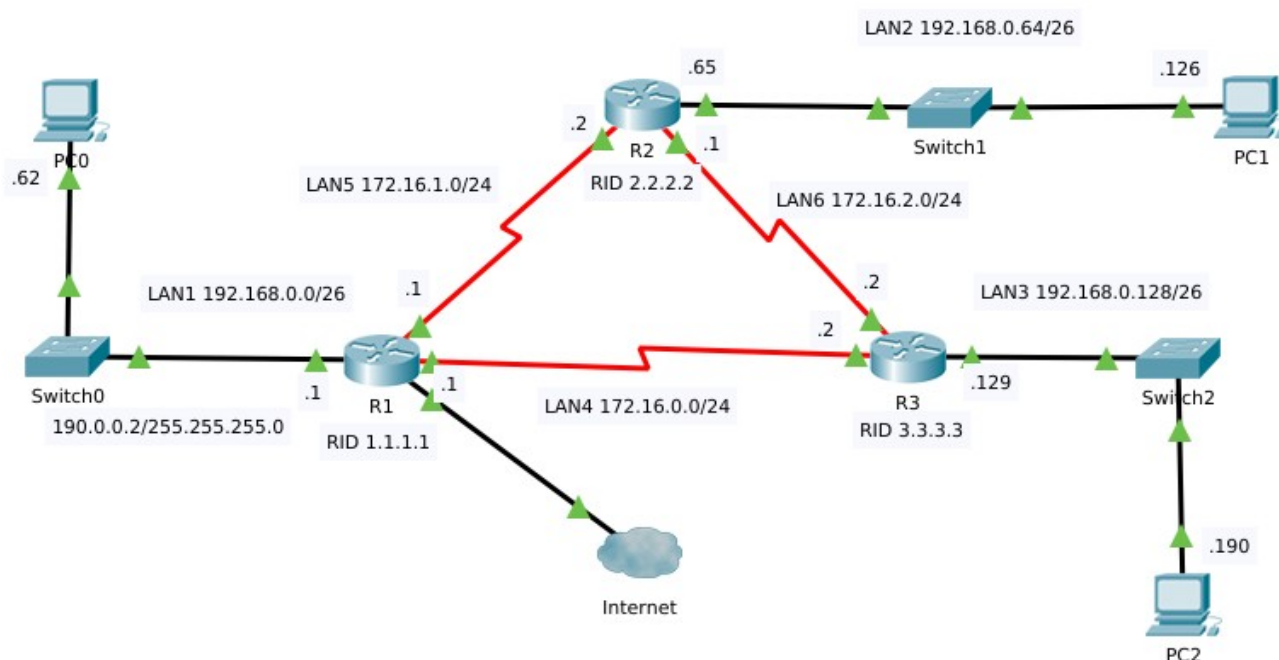


Figura 8.- Topología de red de ejemplo para OSPF

Los routers en la topología tienen una configuración inicial, que incluye direcciones de interfaz habilitadas. En este momento, ninguno de los routers tiene configurado enrutamiento estático o dinámico. Vemos que los routers tienen enlaces GigabitEthernet y Serial. El primero tiene un coste de 1 y el segundo de 64.

4.6.1 Habilitar OSPFv2 en los routers

Para habilitar el protocolo OSPF en un router ejecutamos los siguiente comandos en el modo de configuración global.

```
router ospf id-proceso
```

Este comando habilita el protocolo OSPF en el router al que se le asocia un número de proceso y entra en el modo de subconfiguración del router. Por ejemplo, para habilitar OSPF en el router R1 ejecutamos el siguiente comando.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#
```

El mismo comando se tendría que ejecutar en R2 y R3.

El valor `id-proceso` representa un número entre 1 y 65.535 y lo selecciona el administrador de la red. No es necesario que sea el mismo valor en los demás routers OSPF

para establecer adyacencias con esos vecinos. Se considera una práctica recomendada utilizar el mismo `id-proceso` en todos los routers OSPF.

Para participar en un dominio OSPF, cada router requiere un router ID el cual es un valor de 32 bits, representado como una dirección IPv4. El router ID se utilizan para identificar un router OSPF. Todos los paquetes OSPF incluyen el router ID del router origen. El router ID puede estar definido por un administrador o puede ser asignado en forma automática por el router. El router ID es utilizada por un router habilitado por OSPF para hacer lo siguiente:

- ✓ Participar en la sincronización de bases de datos OSPF → Durante el estado de Exchange, el router con el ID más alto enviará primero sus paquetes de descriptor de base de datos (DBD).
- ✓ Participar en la elección del router designado (DR) → En un entorno LAN multiacceso, el router con el ID más alto se elige el DR. El dispositivo de enrutamiento con el segundo router ID más alto, se elige como el router designado de respaldo (BDR).

¿Pero de qué manera el router determina el router ID? Los routers Cisco obtienen el router ID sobre la base de uno de tres criterios, en el siguiente orden de preferencia:

1. El router ID se configura explícitamente utilizando el comando de configuración OSPF `router-id id-router` El valor `id-router` es cualquier valor de 32 bits expresado como una dirección IPv4. Este es el método recomendado para asignar un router ID.
2. Si el router ID 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 un router ID.
3. 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.

Según nuestra topología de ejemplo el router R1 tiene identificador `1.1.1.1`. Habría que ejecutar el siguiente comando

```
R1(config-router)#router-id 1.1.1.1
```

Dejamos al lector la configuración del id de router en R2 y R3.

4.6.2 Publicar redes

A continuación, una vez habilitado OSPF en el router, tenemos que publicar las redes del router. Para ello usamos el siguiente comando en el modo de configuración del router.

```
network ip-red máscara-wildcard area id-area
```

El comando `network` para definir una interfaz en la que se ejecuta OSPF y define un identificador de área para esa interfaz. Cuando configure OSPFv2 de área única, the network deben configurarse 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 OSPFv2 de área única. Esta convención facilita la tarea si posteriormente se modifica la red para admitir OSPFv2 multiárea.

Por ejemplo en R1 tendríamos que ejecutar los siguientes comandos

```
R1(config-router)#network 192.168.0.0 0.0.0.63 area 0
R1(config-router)#network 172.16.1.0 0.0.0.255 area 0
R1(config-router)#network 172.16.0.0 0.0.0.255 area 0
```

En router 1 hemos habilitado OSPF con un id de proceso de 1. El id de proceso es un número entero entre 1 y 65535. Posteriormente hemos publicado las tres redes a las que se encuentra conectado dentro del mismo área. Nótese la forma de indicar la dirección de red, en lugar de utilizar una máscara de red hay que emplear un *wildcard* que consiste en emplear dentro de la máscara de red los ceros para identificar la parte de red y los unos para identificar la parte de host. Es decir, la inversa de la máscara de red.

Una forma de obtener la wildcard de máscara es restar 255.255.255.255 a la máscara de red.

En el router R2 vamos a realizar una configuración algo diferente. A la hora de publicar la redes a las que se conecta podemos utilizar la dirección IP de las interfaces en lugar de la dirección de red. Sería de la siguiente forma:

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.0.65 0.0.0.0 area 0
R2(config-router)#network 172.16.1.2 0.0.0.0 area 0
R2(config-router)#network 172.16.2.0 0.0.0.0 area 0
R2(config-router)#
```

Nótese que al ser una dirección IP su máscara de red es 255.255.255.255. Al obtener la wildcard de máscara resultaría 0.0.0.0

Por último realizamos la configuración en R3.

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.0.128 0.0.0.63 area 0
R3(config-router)#network 172.16.2.0 0.0.0.255 area 0
R3(config-router)#network 172.16.0.0 0.0.0.255 area 0
```

4.6.3 Configuración OSPF en las interfaces

También se puede configurar OSPF directamente en la interfaz en lugar de utilizar el comando `network`. Para ello empleamos el comando `ip ospf` en el modo de configuración de la interfaz. La sintaxis es la siguiente:

```
Router(config-if)# ip ospf id-proceso area id-area
```

En nuestra topología de ejemplo tendríamos que hacer lo siguiente en el router R1.

```
R1(config)# interface s0/0/0
R1(config-if)# ip ospf 10 area 0
R1(config-if)# interface s0/0/1
R1(config-if)# ip ospf 10 area 0
R1(config-if)#
```

4.6.4 Interfaces pasivas

Al igual que ocurría en RIP, no es conveniente que el router emita mensajes de estado de enlace en interfaces que no conectan con otros routers, sino con segmentos LAN de la red. Debido a ello podemos evitar el envío de estos mensajes con el siguiente comando del modo de subconfiguración OSPF.

```
passive-interface interfaz
```

Por ejemplo, en el router R1 deshabilitamos el envío de mensajes en la interfaz g0/0 que conecta con LAN1.

```
R1(config)#router ospf 1
R1(config-router)#passive-interface g0/0
```

En el router R2 tendríamos que deshabilitar la siguiente interfaz.

```
R2(config)#router ospf 1
R2(config-router)#passive-interface g0/0
```

Finalmente en R3 ejecutamos lo siguiente

```
R3(config)#router ospf 1
R3(config-router)#passive-interface g0/0
```

4.6.5 Red punto a punto

De forma predeterminada, los routers Cisco eligen DR y BDR en las interfaces Ethernet, incluso si solo hay otro dispositivo en el enlace. Podemos verificar esto con el comando `show ip ospf interface`, como se muestra en el ejemplo de R1.

```
R1# show ip ospf interface s0/0/0
s0/0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0, Attached via
  Interface Enable
    Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST,
  Cost: 1
    Topology-MTID      Cost      Disabled      Shutdown
```

```

Topology Name
      0          1          no          no
Base
  Enabled by interface config, including secondary ip
  addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address
  172.16.1.2
  Backup Designated router (ID) 1.1.1.1, Interface address
  172.16.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/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 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2 (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#

```

R1 es el BDR y R2 es el DR. El proceso de elección de DR/ BDR es innecesario ya que solo puede haber dos routers en la red punto a punto entre R1 y R2. Observe que en el resultado del router ha designado el tipo de red como Broadcast. Para cambiar esto a una red punto a punto, utilizamos el comando de configuración de interface, `ip ospf network point-to-point` en todas las interfaces en las que queremos deshabilitar el proceso de elección DR/BDR. El siguiente ejemplo muestra esta configuración para la interfaz Serial 0/0/0 en R1.

```

R1(config)# interface s0/0/0
R1(config-if)# ip ospf network point-to-point
*Jun  6 00:44:05.208: %OSPF-5-ADJCHG: Process 1, Nbr
2.2.2.2 on Serial 0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached
*Jun  6 00:44:05.211: %OSPF-5-ADJCHG: Process 1, Nbr
2.2.2.2 on Serial 0/0/0 from LOADING to FULL, Loading Done

```

Habría que hacer lo mismo en la interfaz serial 0/0/1

4.6.6 Propagar ruta predeterminada

El router R1 dispone de una conexión a Internet para lo que dispone de una ruta estática por defecto. Al igual que hacíamos con RIP, esta ruta se puede propagar a los routers vecinos en OSPF mediante el siguiente comando.


```
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

4.6.7 Comprobación de OSPF

Una vez tenemos configurado OSPF en todos los routers de la topología de red podemos comprobar su correcto funcionamiento mediante una serie de comandos `show`. En este primero simplemente visualizamos las rutas obtenidas dinámicamente desde routers vecinos.

```
R1#show ip route ospf

    172.16.0.0/16 is variably subnetted, 5 subnets, 2
masks
O        172.16.2.0 [110/128] via 172.16.0.2, 00:02:13,
Serial0/0/1
                                [110/128] via 172.16.1.2, 00:02:13,
Serial0/0/0
    192.168.0.0/24 is variably subnetted, 4 subnets, 2
masks
O        192.168.0.64 [110/65] via 172.16.1.2, 00:02:13,
Serial0/0/0
O        192.168.0.128 [110/65] via 172.16.0.2, 00:02:13,
Serial0/0/1
```

Como podemos observar en la salida del comando anterior se dispone de tres rutas descubiertas por OSPF. La primera es a la red 172.16.2.0/24 que se alcanza por 172.16.0.2. Después está la red 192.168.0.64/26 y la 192.168.0.128/26 que se alcanzan a través de 172.16.1.2 y 172.16.0.2 respectivamente.

Vemos cada ruta descubierta por OSPF dispone de distancia administrativa 110 y la métrica es la suma de los costes de los enlaces necesarios para alcanzar la red de destino.

Si ejecutamos este mismo comando en R2 veremos que también aparece la ruta por defecto que se propaga desde R1.

```
R2#show ip route ospf

    172.16.0.0/16 is variably subnetted, 5 subnets, 2
masks
O        172.16.0.0 [110/128] via 172.16.1.1, 00:04:26,
Serial0/0/0
                                [110/128] via 172.16.2.2, 00:04:26,
Serial0/0/1
    192.168.0.0/24 is variably subnetted, 4 subnets, 2
masks
O        192.168.0.0 [110/65] via 172.16.1.1, 00:04:26,
Serial0/0/0
O        192.168.0.128 [110/65] via 172.16.2.2, 00:04:26,
Serial0/0/1
```

```
O*E2 0.0.0.0/0 [110/1] via 172.16.1.1, 00:04:26,
Serial0/0/0
R2#
```

También podemos hacer un listado de los routers vecinos de R1 con `show ip ospf neighbor`.

```
R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
2.2.2.2          0     FULL/ -         00:00:30    172.16.1.2     Serial0/0/0
3.3.3.3          0     FULL/ -         00:00:38    172.16.0.2     Serial0/0/1
R1#
```

El comando `show ip protocols` proporciona una manera rápida de verificar información fundamental de configuración de 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. Por ejemplo, si ejecutamos este comando en R1.

```
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 1.1.1.1
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0
  nssa
  Maximum path: 4
  Routing for Networks:
    192.168.0.0 0.0.0.63 area 20
    172.16.1.0 0.0.0.255 area 20
    172.16.0.0 0.0.0.255 area 20
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:10:21
    2.2.2.2          110          00:10:21
    3.3.3.3          110          00:10:21
  Distance: (default is 110)
```

Finalmente, si las rutas están establecidas entre cualquier par de PCs podemos hacer ping. En la siguiente imagen vemos el resultado de ping desde PC0 a PC2.

```
C:\>ping 192.168.0.190

Pinging 192.168.0.190 with 32 bytes of data:

Reply from 192.168.0.190: bytes=32 time=2ms TTL=126
Reply from 192.168.0.190: bytes=32 time=1ms TTL=126
Reply from 192.168.0.190: bytes=32 time=1ms TTL=126
Reply from 192.168.0.190: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figura 9.- Ping de PC0 a PC2

4.7 Configuración OSPFv2 multiárea

Cuando el dominio OSPFv2 es muy grande, puede ser conveniente dividir la topología de red en varias áreas. En una configuración multiárea, es obligatorio que exista un área backbone que conecta a todas las áreas. A modo de ejemplo vamos a configurar la siguiente red en la que podemos observar lo siguiente:

- ✓ Hay tres áreas: el área backbone tiene identificador 0. Además tenemos las áreas 10 y 20
- ✓ R1 y R2 son routers perimetrales de área (ABR) ya que conectan dos áreas cada uno. Además estos routers forman parte del área backbone.
- ✓ El router R1 dispone de una conexión a Internet con una ruta estática por defecto que se va a distribuir a toda la red. Esto convierte también a R1 en un router perimetral de sistema autónomo (ASBR).
- ✓ Además de R1, los routers que conectan LANs (R11, R12, R21 y R22) son routers perimetrales de sistema autónomo (ASBR), ya que tienen redes LANs conectadas y van a distribuir las rutas a estas redes LAN.
- ✓ Los enlaces serial tienen coste de 64, mientras que los gigabit ethernet lo tienen de 1.
- ✓ Las LAN del área 10 tienen una dirección resumida de 193.0.0.0/24 y las del área 20 es 199.0.0.0/24

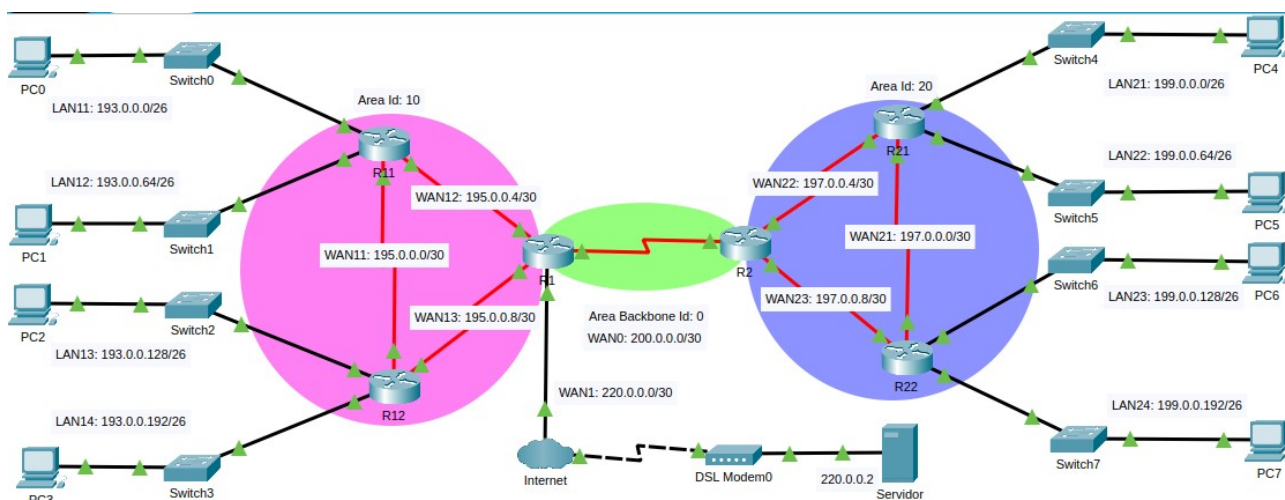


Figura 10.- Red de ejemplo para OSPFv2 multiárea

4.7.1 Habilitar OSPFv2 en cada router

Este primer paso es similar a la configuración OSPFv2 en una topología de área única. Hay que habilitar un proceso OSPFv2 en cada router y asignarle un identificador único. En nuestro ejemplo utilizaremos el identificador 0.0.0.# siendo # el número de router. Comenzamos en R1

```
R1(config)#router ospf 1
R1(config-router)#router-id 0.0.0.1
```

Vamos ahora a habilitar OSPFv2 e identificar al router R11

```
R11(config)#router ospf 11
R11(config-router)#router-id 0.0.0.11
```

En el router R12 sería

```
R12(config)#router ospf 12
R12(config-router)#router-id 0.0.0.12
```

En el router R2 tendríamos lo siguiente

```
R2(config)#router ospf 2
R2(config-router)#router-id 0.0.0.2
```

La identificación del router 21 es la siguiente

```
R21(config)#router ospf 21
R21(config-router)#router-id 0.0.0.21
```

Y finalmente en el router 22

```
R22(config)#router ospf 22
R22(config-router)#router-id 0.0.0.22
```

4.7.2 Publicar redes

Ahora procedemos a publicar las redes conectadas en cada router. El router R1 es un router frontera (ABR) y por tanto define rutas en varias áreas. Como está conectado al área backbone, una de ellas tiene identificador 0.

```
R1(config-router)#network 195.0.0.4 0.0.0.3 area 10
R1(config-router)#network 195.0.0.8 0.0.0.3 area 10
R1(config-router)#network 200.0.0.0 0.0.0.3 area 0
```

Vemos que la red 200.0.0.0/255.255.255.252 pertenece al área backbone con identificador 0. Las otras dos pertenecen al área 10.

El router R2 también es router frontera y le ocurre algo parecido al anterior. Su configuración sería la siguiente:

```
R2(config-router)#network 197.0.0.4 0.0.0.3 area 20
R2(config-router)#network 197.0.0.8 0.0.0.3 area 20
R2(config-router)#network 200.0.0.0 0.0.0.3 area 0
```

En el router R11 publicaríamos todas las redes en el área 10

```
R11(config-router)#network 193.0.0.0 0.0.0.63 area 10
R11(config-router)#network 193.0.0.64 0.0.0.63 area 10
R11(config-router)#network 195.0.0.0 0.0.0.3 area 10
R11(config-router)#network 195.0.0.4 0.0.0.3 area 10
```

En el router R12 publicamos las redes en el área 10

```
R12(config-router)#network 195.0.0.0 0.0.0.3 area 10
R12(config-router)#network 195.0.0.8 0.0.0.3 area 10
R12(config-router)#network 193.0.0.128 0.0.0.63 area 10
R12(config-router)#network 193.0.0.192 0.0.0.63 area 10
```

En el router R21 publicamos las siguientes:

```
R21(config-router)#network 199.0.0.0 0.0.0.63 area 20
R21(config-router)#network 199.0.0.64 0.0.0.63 area 20
R21(config-router)#network 197.0.0.4 0.0.0.3 area 20
R21(config-router)#network 197.0.0.0 0.0.0.3 area 20
```

En el router R22 publicamos las siguientes:

```
R22(config-router)#network 199.0.0.128 0.0.0.63 area 20
R22(config-router)#network 199.0.0.192 0.0.0.63 area 20
R22(config-router)#network 197.0.0.0 0.0.0.3 area 20
```

```
R22(config-router)#network 197.0.0.8 0.0.0.3 area 20
```

4.7.3 Interfaces pasivas

En los routers que conectan redes locales no es necesario enviar mensajes OSPF. Debemos por tanto inhabilitar el envío de estos mensajes definiendo como interfaces pasivas aquellas que las conectan. En el router R1 podemos desactivar los mensajes OSPF en la interfaz que conecta con Internet

```
R1(config-router)#passive-interface g0/0
```

En el router R11 sería así

```
R11(config-router)#passive-interface g0/0
R11(config-router)#passive-interface g0/1
```

En R12 sería

```
R12(config-router)#passive-interface g0/0
R12(config-router)#passive-interface g0/1
```

En R21 sería

```
R21(config-router)#passive-interface g0/0
R21(config-router)#passive-interface g0/1
```

Finalmente en R22 sería

```
R22(config-router)#passive-interface g0/0
R22(config-router)#passive-interface g0/1
```

4.7.4 Publicar la ruta por defecto

El router R1 tiene una ruta estática por defecto a Internet. Para publicarla ejecutamos el siguiente comando

```
R1(config-router)#default-information originate
```

4.7.5 Comprobación OSPFv2

Una vez configurado OSPFv2 en todos los routers de la topología podemos comenzar a realizar comprobaciones de su funcionamiento. Por ejemplo, si vemos la tabla de enrutamiento del router R11 veremos lo siguiente:

```
R11#show ip route ospf
    193.0.0.0/24 is variably subnetted, 6 subnets, 2 masks
O        193.0.0.128 [110/65] via 195.0.0.2, 00:13:00,
Serial0/0/0
```

```
O      193.0.0.192 [110/65] via 195.0.0.2, 00:13:00,
Serial0/0/0
      195.0.0.0/24 is variably subnetted, 5 subnets, 2 masks
O      195.0.0.8 [110/128] via 195.0.0.2, 00:13:20,
Serial0/0/0
      [110/128] via 195.0.0.6, 00:13:20,
Serial0/0/1
      197.0.0.0/30 is subnetted, 3 subnets
O IA   197.0.0.0 [110/256] via 195.0.0.6, 00:05:21,
Serial0/0/1
O IA   197.0.0.4 [110/192] via 195.0.0.6, 00:08:07,
Serial0/0/1
O IA   197.0.0.8 [110/192] via 195.0.0.6, 00:08:07,
Serial0/0/1
      199.0.0.0/26 is subnetted, 4 subnets
O IA   199.0.0.0 [110/193] via 195.0.0.6, 00:05:31,
Serial0/0/1
O IA   199.0.0.64 [110/193] via 195.0.0.6, 00:05:31,
Serial0/0/1
O IA   199.0.0.128 [110/193] via 195.0.0.6, 00:02:10,
Serial0/0/1
O IA   199.0.0.192 [110/193] via 195.0.0.6, 00:02:10,
Serial0/0/1
      200.0.0.0/30 is subnetted, 1 subnets
O IA   200.0.0.0 [110/128] via 195.0.0.6, 00:17:52,
Serial0/0/1
O*E2  0.0.0.0/0 [110/1] via 195.0.0.6, 00:17:52, Serial0/0/1
```

En la tabla de enrutamiento anterior se aprecia lo siguiente:

- ✓ Las rutas etiquetadas con O son rutas descubiertas por OSPFv2 en el área de R11.
- ✓ Las rutas etiquetadas con O IA son rutas inter área, lo que significa que pertenecen a otra área distinta en la que opera R11.
- ✓ La ruta por defecto O*E2 es una ruta estática externa de un router ASBR.
- ✓ Las rutas no están resumidas. OSPFv2 es un protocolo sin clase, por lo que las rutas anunciadas no tienen clase.
- ✓ La métrica de cada ruta es la suma de los costes de cada enlace a atravesar para alcanzar la red de la ruta.

Si vemos la tabla de enrutamiento de R1 veremos lo siguiente:

```
R1#show ip route ospf
      193.0.0.0/26 is subnetted, 4 subnets
O      193.0.0.0 [110/65] via 195.0.0.5, 02:05:44,
Serial0/0/1
O      193.0.0.64 [110/65] via 195.0.0.5, 02:05:44,
```

```

Serial0/0/1
O      193.0.0.128 [110/65] via 195.0.0.9, 02:05:54,
Serial0/1/0
O      193.0.0.192 [110/65] via 195.0.0.9, 02:05:54,
Serial0/1/0
      195.0.0.0/24 is variably subnetted, 5 subnets, 2 masks
O      195.0.0.0 [110/128] via 195.0.0.9, 02:05:44,
Serial0/1/0
      [110/128] via 195.0.0.5, 02:05:44,
Serial0/0/1
      197.0.0.0/30 is subnetted, 3 subnets
O IA   197.0.0.0 [110/192] via 200.0.0.2, 02:05:39,
Serial0/0/0
O IA   197.0.0.4 [110/128] via 200.0.0.2, 02:05:49,
Serial0/0/0
O IA   197.0.0.8 [110/128] via 200.0.0.2, 02:05:49,
Serial0/0/0
      199.0.0.0/26 is subnetted, 4 subnets
O IA   199.0.0.0 [110/129] via 200.0.0.2, 02:05:39,
Serial0/0/0
O IA   199.0.0.64 [110/129] via 200.0.0.2, 02:05:39,
Serial0/0/0
O IA   199.0.0.128 [110/129] via 200.0.0.2, 02:05:39,
Serial0/0/0
O IA   199.0.0.192 [110/129] via 200.0.0.2, 02:05:39,
Serial0/0/0

```

Podemos ver información añadida, como los vecinos de R1.

```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
0.0.0.11	0	FULL/ -	00:00:30	195.0.0.5
Serial0/0/1				
0.0.0.12	0	FULL/ -	00:00:39	195.0.0.9
Serial0/1/0				
0.0.0.2	0	FULL/ -	00:00:37	200.0.0.2
Serial0/0/0				

R1#

Si mostramos información en R1 del protocolo OSPF veremos lo siguiente

```
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 0.0.0.1
It is an autonomous system boundary router
Redistributing External Routes from,
Number of areas in this router is 2. 2 normal 0 stub 0
nssa
Maximum path: 4
Routing for Networks:
  195.0.0.4 0.0.0.3 area 10
  195.0.0.8 0.0.0.3 area 10
  200.0.0.0 0.0.0.3 area 0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway          Distance          Last Update
  0.0.0.1           110               00:08:20
  0.0.0.2           110               00:08:21
  0.0.0.11          110               00:08:20
  0.0.0.12          110               00:08:21
Distance: (default is 110)

```

Vemos que el router está definido de tipo ASBR.

4.7.6 Resumen de rutas

El resumen es la agrupación de varias rutas en una única la cual se transmitiría a los otros routers. Esto se realiza normalmente en los routers perimetrales de área (ABR) o de sistema autónomo (ASBR). Aunque puede configurarse el resumen entre dos áreas cualquiera, es mejor resumir en la dirección de la estructura básica, es decir, de un área al área backbone. De esta manera el área backbone recibe el total de direcciones y las inyecta a su vez, ya resumidas, en otras áreas. Hay dos tipos de resumen:

- ✓ Resumen de rutas interzonales → Las rutas se encuentran en áreas OSPFv2 y el resumen se realiza en el router ABR. Es necesario que las redes de las rutas a resumir sean contiguas para poder juntarlas en un rango.
- ✓ Resumen de rutas externas → El resumen de ruta externa es específico para las rutas externas que se introducen en OSPF mediante la redistribución de rutas que realiza el router ASBR. Aquí también es necesario que las rutas a resumir sean contiguas.

En nuestro caso vamos a utilizar el resumen de rutas externas. Si nos fijamos en nuestra topología los routers R11 y R12 han redistribuido sus redes LAN:

- ✓ LAN11 → 193.0.0.0/26
- ✓ LAN12 → 193.0.64.0/26
- ✓ LAN13 → 193.0.128.0/26
- ✓ LAN14 → 193.0.192.0/26

Estas cuatro redes son contiguas y se pueden agrupar con dirección 193.0.0.0/24

la cual se publicaría en el área 0 con puerta de enlace hacia el router R1. En este caso tendríamos que resumir estas cuatro redes de la siguiente manera en R1.

```
R1(config)#router ospf 1
R1(config-router)#area 0 range 193.0.0.0 255.255.255.0
```

A partir de ahora las rutas de las cuatro LAN en el área 10 se publicarán con una única ruta resumida. Si consultamos ahora la tabla de enrutamiento en R2 veremos lo siguiente

```
R2#show ip route ospf
      193.0.0.0/26 is subnetted, 1 subnets
O IA   193.0.0.0 [110/129] via 200.0.0.1, 00:01:39,
Serial0/0/0
      195.0.0.0/30 is subnetted, 3 subnets
O IA   195.0.0.0 [110/192] via 200.0.0.1, 03:32:27,
Serial0/0/0
O IA   195.0.0.4 [110/128] via 200.0.0.1, 03:32:27,
Serial0/0/0
O IA   195.0.0.8 [110/128] via 200.0.0.1, 03:32:27,
Serial0/0/0
      197.0.0.0/24 is variably subnetted, 5 subnets, 2 masks
O      197.0.0.0 [110/128] via 197.0.0.9, 03:32:27,
Serial0/1/0
                        [110/128] via 197.0.0.5, 03:32:27,
Serial0/0/1
      199.0.0.0/26 is subnetted, 4 subnets
O      199.0.0.0 [110/65] via 197.0.0.5, 03:32:27,
Serial0/0/1
O      199.0.0.64 [110/65] via 197.0.0.5, 03:32:27,
Serial0/0/1
O      199.0.0.128 [110/65] via 197.0.0.9, 03:32:27,
Serial0/1/0
O      199.0.0.192 [110/65] via 197.0.0.9, 03:32:27,
Serial0/1/0
O*E2 0.0.0.0/0 [110/1] via 200.0.0.1, 03:32:37, Serial0/0/0
```

Análogamente, podemos hacer lo mismo en el router R2. Este router perimetral está en el área 20 el cual tiene las siguientes cuatro LANs.

- ✓ LAN21 → 199.0.0.0/26
- ✓ LAN22 → 199.0.64.0/26
- ✓ LAN23 → 199.0.128.0/26
- ✓ LAN24 → 199.0.192.0/26

Estas cuatro redes son contiguas y pueden resumirse en 199.0.0.0/24 la cual se publicaría en el área 0 con puerta de enlace hacia el router R2. Por tanto en R2 ejecutaríamos lo siguiente:

```
R2(config)#router ospf 2
R2(config-router)#area 0 range 199.0.0.0 255.255.255.0
```

Una vez resumida la ruta, el router R2 anunciará la ruta para esta red resumida en otras áreas y el router R1 tendría la siguiente tabla de enrutamiento.

```
R1#show ip route ospf
      193.0.0.0/26 is subnetted, 4 subnets
O       193.0.0.0 [110/65] via 195.0.0.5, 03:40:37,
Serial0/0/1
O       193.0.0.64 [110/65] via 195.0.0.5, 03:40:37,
Serial0/0/1
O       193.0.0.128 [110/65] via 195.0.0.9, 03:40:47,
Serial0/1/0
O       193.0.0.192 [110/65] via 195.0.0.9, 03:40:47,
Serial0/1/0
      195.0.0.0/24 is variably subnetted, 5 subnets, 2 masks
O       195.0.0.0 [110/128] via 195.0.0.9, 03:40:37,
Serial0/1/0
              [110/128] via 195.0.0.5, 03:40:37,
Serial0/0/1
      197.0.0.0/30 is subnetted, 3 subnets
O IA    197.0.0.0 [110/192] via 200.0.0.2, 03:40:32,
Serial0/0/0
O IA    197.0.0.4 [110/128] via 200.0.0.2, 03:40:42,
Serial0/0/0
O IA    197.0.0.8 [110/128] via 200.0.0.2, 03:40:42,
Serial0/0/0
O IA 199.0.0.0 [110/129] via 200.0.0.2, 00:01:34,
Serial0/0/0
```

Si consultamos las tablas de enrutamiento de R11 y R12 veremos que también dispone de una ruta resumida.

4.8 Redes OSPF de acceso múltiple

La topología anterior utilizaba enlaces punto a punto entre los routers. Sin embargo, los routers se pueden conectar al mismo switch para formar una red multiacceso, como se muestra en la figura. Las LAN Ethernet son el ejemplo más común de redes broadcast con multiacceso

4.8.1 El problema en las redes con enlaces multipunto

Cuando los routers que forman una red OSPF están conectados mediante enlaces multipunto, como por ejemplo una red Ethernet, puede provocar dos problemas:

- ✓ Creación de varias adyacencias → En un enlace multipunto puede conectar muchos routers OSPF con un enlace común. La creación de adyacencias entre dos routers cualesquiera 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 saturan con sus mensajes LSA cuando se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.

Para cualquier número n de routers en una red multiacceso, hay $n(n - 1)/2$ adyacencias.

Por ejemplo, la figura muestra una topología simple de cuatro routers, todos están conectados a la misma red Ethernet de acceso múltiple. Sin ningún tipo de mecanismo para reducir la cantidad de adyacencias, estos routers en forma colectiva formarán 10 adyacencias:

$$4(4 - 1) / 2 = 6$$

Esto puede no parecer mucho, pero a medida que se agregan routers a la red, el número de adyacencias aumenta dramáticamente. Por ejemplo, una red multiacceso con 20 routers crearía 190 adyacencias.

La solución para administrar la cantidad de adyacencias y la saturación con LSA en una red de accesos múltiples es el DR (*Designated Router*). 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 por el resto de routers. También se elige un BDR (Backup Designated Router) en caso de que falle el DR. El BDR escucha este intercambio de información de forma pasiva y mantiene una relación con todos los routers. Si el DR deja de producir paquetes de saludo, el BDR se autopromociona y asume la función de DR.

Los routers de una red de accesos múltiples eligen un DR y un BDR. El resto de routers solo crean adyacencias completas con el DR y el BDR de la red. En vez de saturar todos los routers de la red con mensajes LSA, los routers solo envían sus mensajes LSA al DR y el BDR mediante la dirección de multidifusión 224.0.0.6 (todos los routers DR).

El DR es responsable de reenviar todos los mensajes LSA hasta todos los demás routers. El DR usa la dirección de multidifusión 224.0.0.5 (todos los routers OSPF). El resultado final es que sólo hay un router que realiza la saturación completa de todos los mensajes LSA en la red de accesos múltiples.

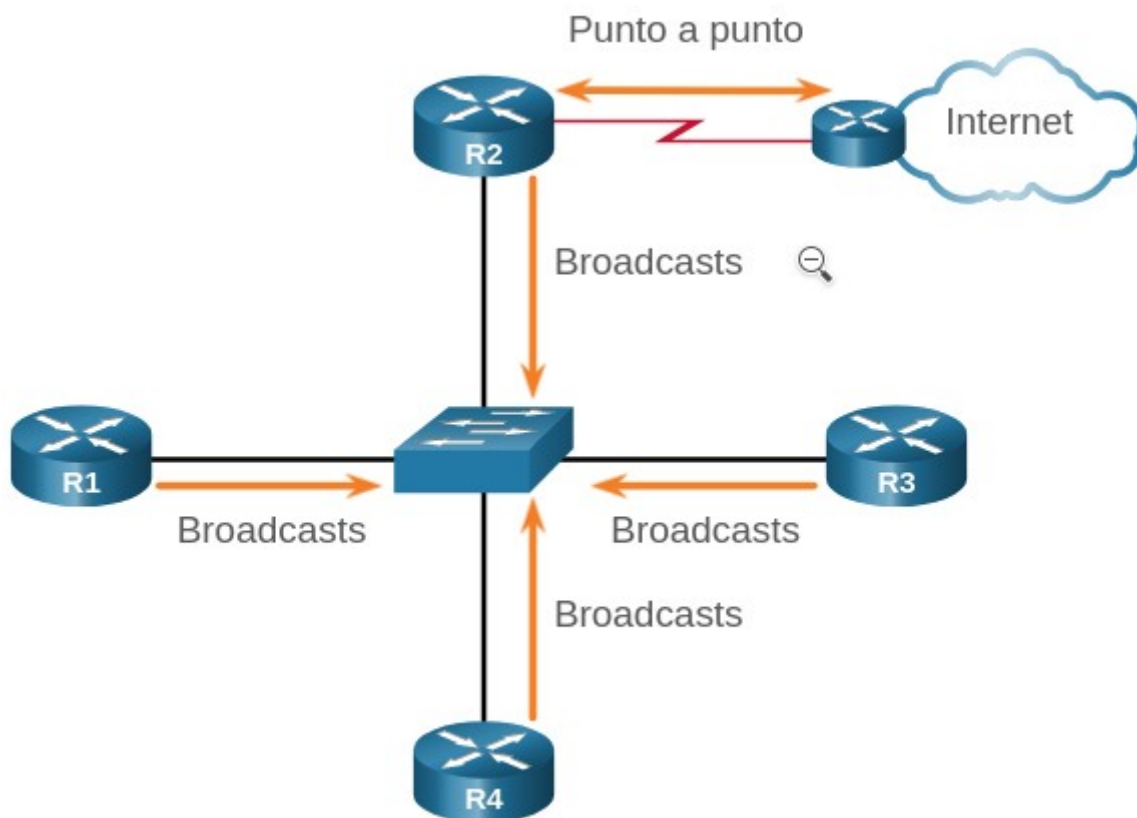


Figura 11: Red multiacceso

4.8.2 Router designado

En redes multiacceso, OSPF elige una DR y BDR como solución para administrar el número de adyacencias y la inundación de anuncios de estado de enlace (LSA). El DR es responsable de recolectar y distribuir los LSA enviados y recibidos. El DR usa la dirección IPv4 multicast 224.0.0.5 que está destinada a todos los routers OSPF.

También se elige un BDR en caso de que falle el DR. El BDR escucha pasivamente y mantiene una relación con todos los routers. Si el DR deja de producir paquetes Hello, el BDR se asciende a sí mismo y asume la función de DR.

Todos los demás routers se convierten en DROTHER (un router que no es DR ni BDR). Los DROTHER utilizan la dirección de acceso múltiple 224.0.0.6 (todos los routers designados) para enviar paquetes OSPF al DR y al BDR. Sólo DR y BDR escuchan 224.0.0.6.

4.8.3 Verificar las funciones del router

En la topología de acceso múltiple que se muestra en la figura, hay tres routers interconectados a través de una red de acceso múltiple Ethernet común, 192.168.1.0/24. Cada router está configurado con la dirección IPv4 indicada en la interfaz Gigabit Ethernet 0/0/0.

Debido a que los routers están conectados por medio de una red multiacceso, OSPF seleccionó automáticamente un DR y un BDR. En este ejemplo, se eligió al R3 como el DR porque la ID del router es 3.3.3.3, que es la más alta en la red. El R2 es el BDR porque tiene la segunda ID del router más alta en la red.

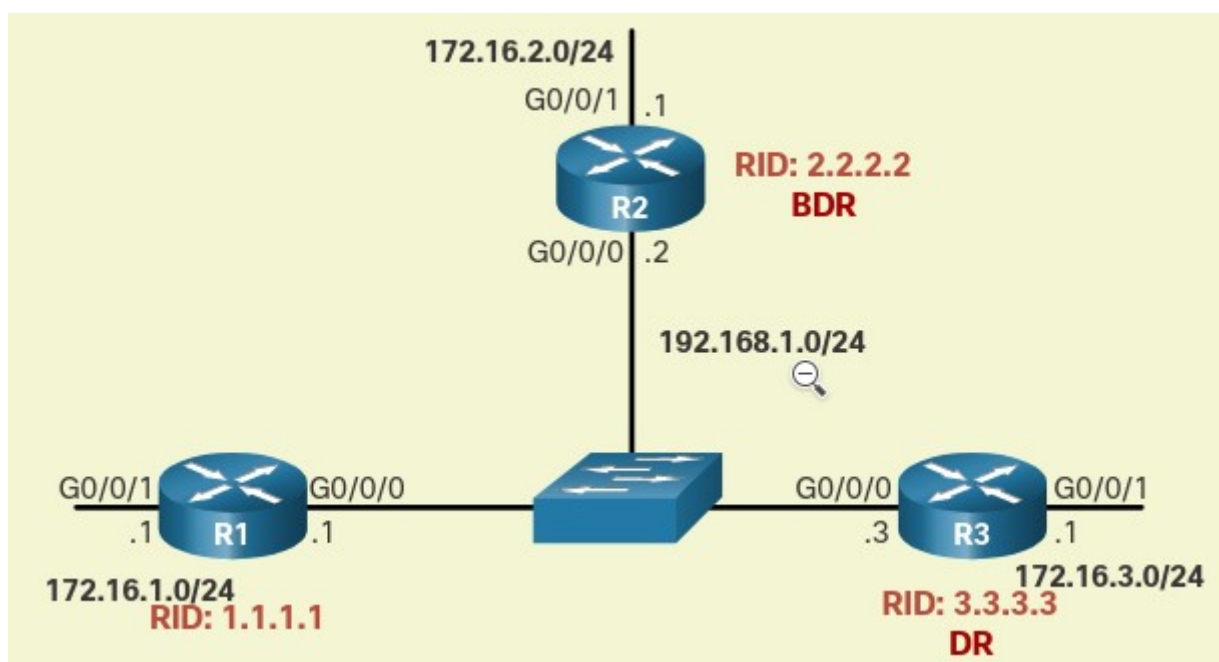


Figura 12: Topología de referencia

Para verificar los roles del router OSPFv2, utilizamos el comando `show ip ospf interface`. El resultado generado por R1 confirma que lo siguiente:

- ✓ El R1 no es el DR ni el BDR, sino un DROTHER con una prioridad predeterminada de 1.
- ✓ El DR es el R3 con el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2.
- ✓ El R1 tiene dos adyacencias: una con el BDR y otra con el DR.

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via
  Interface Enable
    Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST,
  Cost: 1
    Topology-MTID Cost Disabled Shutdown Topology Name
      0 1 no no Base
    Enabled by interface config, including secondary ip
  addresses
    Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address
  192.168.1.3
    Backup Designated router (ID) 2.2.2.2, Interface address
  192.168.1.2
    Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
      oob-resync timeout 40
      Hello due in 00:00:07
```

```

Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 1
Last flood scan time is 0 msec, maximum is 1 msec
Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 2.2.2.2 (Backup Designated
Router)
  Adjacent with neighbor 3.3.3.3 (Designated Router)
Suppress hello for 0 neighbor(s)
R1#

```

El resultado generado por R2 confirma lo siguiente:

- ✓ El R2 es el BDR, con una prioridad predeterminada de 1.
- ✓ El DR es el R3 con el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2.
- ✓ El R2 tiene dos adyacencias, una con un vecino que tiene el router ID 1.1.1 (R1) y la otra con el DR.

```

R2# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Area 0, Attached via
Interface Enable
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST,
Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
    0 1 no no Base
  Enabled by interface config, including secondary ip
addresses
  Transmit Delay is 1 sec, State BDR, Priority 1 Designated
Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address
192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 0:00:01
  Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
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 1.1.1.1
Adjacent with neighbor 3.3.3.3 (Designated Router)
Suppress hello for 0 neighbor(s)
R2#

```

El resultado generado por R3 confirma lo siguiente:

- ✓ El R3 es el DR, con una prioridad predeterminada de 1.
- ✓ El DR es el R3 con el router ID 3.3.3.3 en la dirección IPv4 192.168.1.3; el BDR es el R2 con el router ID 2.2.2.2 en la dirección IPv4 192.168.1.2.
- ✓ El R3 tiene dos adyacencias, una con un vecino que tiene la ID de router 1.1.1.1 (R1) y la otra con el BDR.

```

R3# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.3/24, Area 0, Attached via
Interface Enable
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST,
Cost: 1
  Topology-MTID Cost Disabled Shutdown Topology Name
    0 1 no no Base
  Enabled by interface config, including secondary ip
addresses
  Transmit Delay is 1 sec, State DR, Priority 1 Designated
Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address
192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
    oob-resync timeout 40
    Hello due in 0:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 1.1.1.1
    Adjacent with neighbor 2.2.2.2 (Backup Designated
Router)
  Suppress hello for 0 neighbor(s)
R3#

```

4.8.4 Verificar las adyacencias del DR/BDR

Para verificar las adyacencias OSPFv2, usamos el comando `show ip ospf neighbor`, como se muestra en el ejemplo de R1. El estado de los vecinos en las redes de

acceso múltiple puede ser el siguiente:

- ✓ FULL/DROTHER → Este es un router DR o BDR que está completamente adyacente con un router que no es DR o BDR. Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- ✓ FULL/DR → El router está completamente adyacente con el vecino DR indicado. Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- ✓ FULL/BDR → El router es completamente adyacente con el vecino BDR indicado. Estos dos vecinos pueden intercambiar paquetes Hello, actualizaciones, consultas, respuestas y acuses de recibo.
- ✓ 2-WAY/DROTHER → El router que no es DR o BDR tiene una relación vecina con otro router no DR o BDR. Estos dos vecinos intercambian paquetes Hello.

El estado normal de un router OSPF suele ser COMPLETO. Si un router está atascado en otro estado, es un indicio de que existen problemas en la formación de adyacencias. La única excepción a esto es el estado 2-WAY, que es normal en una red broadcast multiacceso. Por ejemplo, los DROTHERs formarán una adyacencia vecina de 2-Way con cualquier DROTHER que se una a la red. Cuando esto sucede, el estado vecino se muestra como 2-WAY/DROTHER.

4.8.5 Proceso de elección del DR y BDR predeterminados

4.8.6 Recuperación y fallo del DR

4.8.7 Cambiar la prioridad del router

5 OSPF en IPv6

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 homólogo para IPv4, OSPFv3 intercambia información de enrutamiento para completar la tabla de enrutamiento de IPv6 con prefijos remotos.

OSPFv2 se ejecuta sobre la capa de red IPv4, comunicándose con otros pares de IPv4 de OSPF y publicitando solo 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 pares de OSPFv3 y anuncia rutas IPv6. OSPFv3 también utiliza el algoritmo SPF para determinar las mejores rutas a lo largo del dominio de enrutamiento.

OSPFv3 tiene procesos separados de su homólogo IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de enrutamiento IPv4, pero se ejecutan de forma independiente. OSPFv2 y OSPFv3 tienen tablas de adyacencia, tablas de topología OSPF y tablas de enrutamiento IP independientes. Además, los comandos de configuración y verificación de OSPFv3 son similares a los que se utilizan en OSPFv2.

De nuevo, vamos a ver una implementación de área única, para, posteriormente entrar en una configuración multiárea.

5.1 Configuración de OSPFv3 de área única

En los siguientes apartados veremos como configurar OSPFv3 en una topología de red de área única. Para ilustrar la configuración OSPFv3 vamos a emplear la siguiente topología de red.

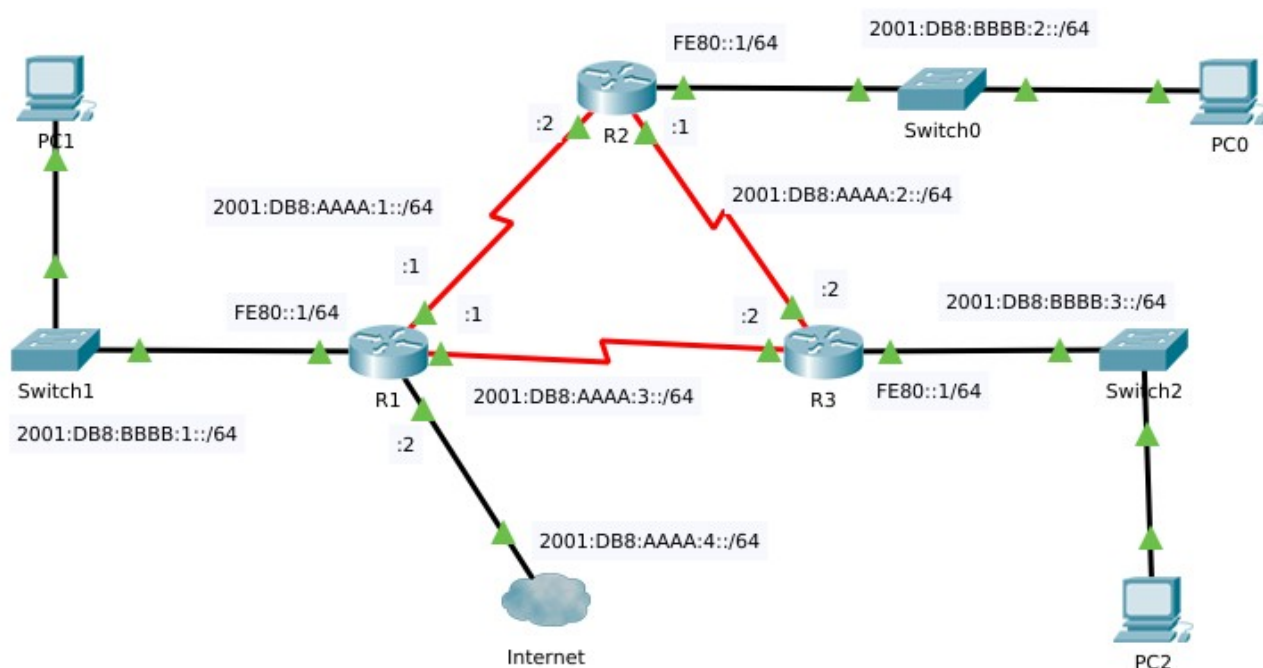


Figura 13.- Topología de red para OSPFv3

Los routers en la topología tienen una configuración inicial, que incluye direcciones IPv6 de interfaz habilitadas. Esto incluye direcciones IPv6 de enlace local en FE80:: donde cada interfaz tiene el último dígito igual al de la dirección IPv6 de unidifusión global. En este momento, ninguno de los routers tiene configurado enrutamiento estático o dinámico. Muy importante que el enrutamiento IPv6 esté habilitado, ya que por defecto no lo está.

5.1.1 Habilitar OSPFv3 en las interfaces

Para habilitar OSPFv3 en un router debemos crear un proceso OSPF y habilitar cada interfaz en dicho proceso. En R1 debemos ejecutar los siguientes comandos

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#ipv6 router ospf 1
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 20
R1(config-rtr)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 20
```

Como vemos en la ejecución de los comandos anteriores se habilita en cada interfaz sobre la que se quieran enviar mensajes de OSPF a routers vecinos. El comando de modo de configuración global `ipv6 router ospf id-proceso` habilita un proceso de enrutamiento OSPF en el router. Posteriormente se emplea el comando `router-id id-router` para establecer el identificador del router en el área.

Una vez hemos creado un proceso OSPF debemos activarlo en las interfaces del router. Para ello empleamos el comando `ipv6 ospf id-proceso area id-area` del modo de configuración de la interfaz.

En el router R2 tendríamos que hacer algo similar. Sería la ejecución de los siguientes comandos.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R2(config)#ipv6 router ospf 1
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#interface s0/0/0
R2(config-if)#ipv6 ospf 1 area 20
R2(config-rtr)#interface s0/0/1
R2(config-if)#ipv6 ospf 1 area 20
```

Vemos que el identificador de proceso y área debe ser igual que en R1. Es fácil intuir cuál sería la configuración en R3.

```
R3>enable
R3#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R3(config)#ipv6 router ospf 1
R3(config-rtr)#router-id 2.2.2.2
R3(config-rtr)#interface s0/0/0
```

```
R3(config-if)#ipv6 ospf 1 area 20
R3(config-rtr)#interface s0/0/1
R3(config-if)#ipv6 ospf 1 area 20
```

5.1.2 Publicar ruta predeterminada

En nuestra topología tenemos una conexión a Internet desde el router R1. Este router tiene una ruta por defecto que se introdujo mediante el siguiente comando

```
R1(config)#ipv6 route ::/0 2001:DB8:AAAA:4::1
```

Los otros routers pueden utilizar esta ruta por defecto también. Para ello vamos a publicar por OSPF la ruta por defecto de R1. Tendríamos que ejecutar el siguiente comando

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#default-information originate
```

5.1.3 Publicar rutas a LANs

Al habilitar las interfaces para OSPFv3 no lo hicimos sobre las interfaces GigabitEthernet que conectan LANs ya que emitir por esta interfaz mensajes del protocolo OSPF no tiene sentido. Estos mensajes sobrecargan la red y no llegan a ningún otro router. Sin embargo, al no habilitar estas interfaces tampoco se distribuyen las rutas que permiten alcanzar las LANs que conectan. Para evitarlo podemos ejecutar el comando `redistribute connected` que permite distribuir las redes en las que está conectado directamente el router.

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#redistribute connected
```

Para conseguir el mismo objetivo también podríamos haber habilitado las interfaces que conectan las LANs y posteriormente declarar estas interfaces como pasivas. Así, las rutas a las redes que conectan se distribuyen, pero no se envían mensajes del protocolo OSPF por esta interfaz.

```
R1(config)#interface g0/0
R1(config-if)#ipv6 ospf 1 area 20
R1(config-if)#ipv6 router ospf 1
R1(config-rtr)#passive-interface g0/0
R1(config-rtr)#
```

5.1.4 Comprobar OSPFv3

Terminada la configuración es el momento de comprobar el funcionamiento de OSPFv3 mediante comandos `show`. Si listamos las rutas obtenidas por OSPFv3 en R2 veremos lo siguiente:

```
R2#show ipv6 route ospf
IPv6 Routing Table - 11 entries
```

```
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
OE2  ::/0 [110/1], tag 1
      via FE80::1, Serial0/0/0
O    2001:DB8:AAAA:3::/64 [110/128]
      via FE80::1, Serial0/0/0
      via FE80::2, Serial0/0/1
O    2001:DB8:BBBB:1::/64 [110/65]
      via FE80::1, Serial0/0/0
O    2001:DB8:BBBB:3::/64 [110/65]
      via FE80::2, Serial0/0/1
R2#
```

Vemos que se han añadido rutas con las redes que conectan R1 y R3, además de la ruta por defecto marcada como OE2.

Podemos ver un listado de los routers vecinos con `show ipv6 ospf neighbor`.

```
R2#show ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
1.1.1.1	0	FULL/ -	00:00:37	3	Serial0/0/0
3.3.3.3	0	FULL/ -	00:00:33	4	Serial0/0/1

```
R2#
```

Con el comando `show ipv6 protocols` vemos información asociada al proceso OSPF con las interfaces que forman el área.

```
R2#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 1"
  Interfaces (Area 20)
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R2#
```

5.2 Configuración de OSPFv3 en multiárea

Para ilustrar la configuración de OSPFv3 en una topología de red multiárea vamos a emplear la misma red que utilizamos en OSPFv2. Es la siguiente:

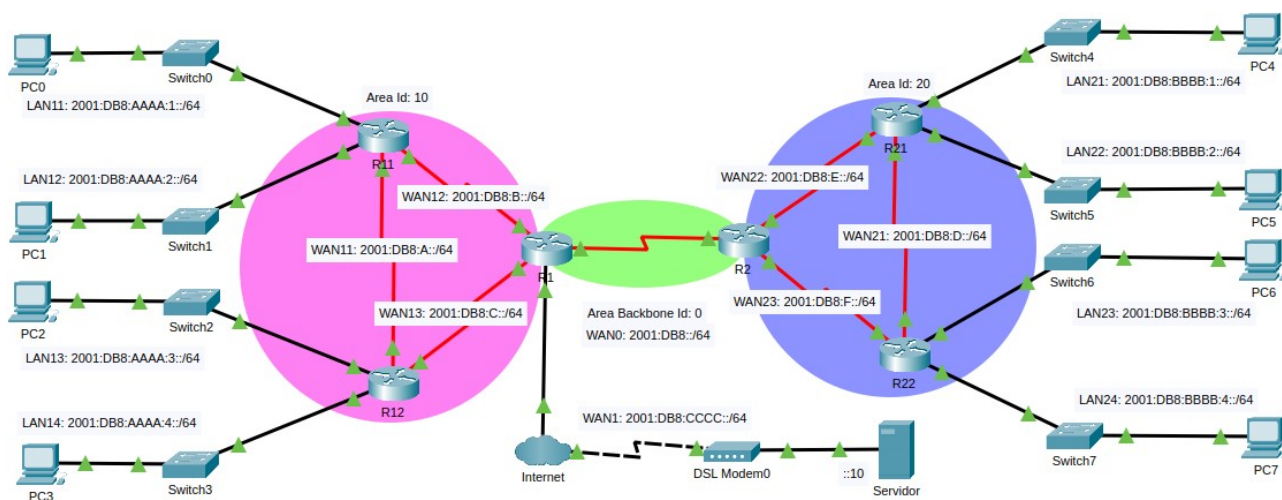


Figura 14: Topología de ejemplo para OSPFv3

Se aprecia que la topología dispone de tres áreas. El área backbone conecta R1 y R2, los cuales son también routers perimetrales (ABR) para las áreas 10 y 20. Además, R1 va a redistribuir su ruta por defecto por lo que también es router perimetral de sistema autónomo.

En cada router las interfaces están configuradas con sus direcciones IPv6 de unidifusión global y enlace local. Ambas direcciones tienen el mismo ID de interfaz. Además, los routers que conectan LANs tienen configurado SLAAC y DHCPv6 sin estado para que los Pcs se configuren automáticamente y tengan un servidor DNS, el cual está conectado en Internet. Por último, el router R1 tiene una ruta por defecto con salida por la interfaz gigabitethernet 0/0.

La configuración es muy similar a la que vimos en una topología de área única. La diferencia es que en cada interfaz que se habilita OSPFv3 lo tiene que hacer en el área a la que pertenece.

5.2.1 Habilitar OSPFv3 en las interfaces

Para habilitar OSPFv3 en un router debemos crear un proceso OSPF y asignarle un identificador al router. Por tanto, en R1 debemos ejecutar los siguientes comandos

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a
router-id, please configure manually
R1(config-rtr)#router-id 0.0.0.1
```

Posteriormente tenemos que habilitar cada interfaz en dicho proceso en su área correspondiente.

```
R1(config-rtr)#interface s0/0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#interface s0/0/1
R1(config-if)#ipv6 ospf 1 area 10
R1(config-if)#interface s0/1/0
R1(config-if)#ipv6 ospf 1 area 10
```

En el router R2 tendríamos que hacer algo similar. Sería la ejecución de los siguientes comandos.

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R2(config)#ipv6 router ospf 2
%OSPFv3-4-NORTRID: OSPFv3 process 2 could not pick a
router-id,please configure manually
R2(config-rtr)#router-id 0.0.0.2
R2(config-rtr)#interface s0/0/0
R2(config-if)#ipv6 ospf 2 area 0
R2(config-if)#interface s0/0/1
R2(config-if)#ipv6 ospf 2 area 20
R2(config-if)#interface s0/1/0
R2(config-if)#ipv6 ospf 2 area 20
R2(config-if)#
```

Es posible que durante la configuración de R2 aparezcan mensajes de que ha contactado con un router vecino.

Ahora tenemos que configurar los routers R11 y R12 del área 10. Comenzamos con R11

```
R11>enable
R11#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R11(config)#ipv6 router ospf 11
%OSPFv3-4-NORTRID: OSPFv3 process 11 could not pick a
router-id,please configure manually
R11(config-rtr)#router-id 0.0.0.11
R11(config-rtr)#interface s0/0/0
R11(config-if)#ipv6 ospf 11 area 10
R11(config-if)#interface s0/0/1
R11(config-if)#ipv6 ospf 11 area 10
```

Seguimos con R12

```
R12>enable
R12#configure terminal
Enter configuration commands, one per line. End with
```



```
CNTL/Z.  
R12(config)#ipv6 router ospf 12  
%OSPFv3-4-NORTRID: OSPFv3 process 12 could not pick a  
router-id,please configure manually  
R12(config-rtr)#router-id 0.0.0.12  
R12(config-rtr)#interface s0/0/0  
R12(config-if)#ipv6 ospf 12 area 10  
R12(config-if)#interface s0/1/0  
R12(config-if)#ipv6 ospf 12 area 10  
R12(config-if)#
```

En el otro extremo tenemos el área 20 con los routers R21 y R22. Comenzamos con el primero.

```
R21>enable  
R21#configure terminal  
Enter configuration commands, one per line. End with  
CNTL/Z.  
R21(config)#ipv6 router ospf 21  
%OSPFv3-4-NORTRID: OSPFv3 process 21 could not pick a  
router-id,please configure manually  
R21(config-rtr)#router-id 0.0.0.21  
R21(config-rtr)#interface s0/0/0  
R21(config-if)#ipv6 ospf 21 area 20  
R21(config-if)#interface s0/0/1  
R21(config-if)#ipv6 ospf 21 area 20  
R21(config-if)#
```

Finalmente en R21.

```
R22>enable  
R22#configure terminal  
Enter configuration commands, one per line. End with  
CNTL/Z.  
R22(config)#ipv6 router ospf 22  
%OSPFv3-4-NORTRID: OSPFv3 process 22 could not pick a  
router-id,please configure manually  
R22(config-rtr)#router-id 0.0.0.22  
R22(config-rtr)#interface s0/0/0  
R22(config-if)#ipv6 ospf 22 area 20  
R22(config-if)#interface s0/1/0  
R22(config-if)#ipv6 ospf 22 area 20  
R22(config-if)#
```

En esta situación OSPFv3 está configurado en todos los routers y funcionando. Se puede hacer comprobaciones en la tabla de enrutamiento y en la información OSPFv3.

5.2.2 Publicar al ruta predeterminada

El router R1 tiene una ruta por defecto con interfaz de salida g0/0. Podemos publicar esta ruta por cada interfaz donde tengamos habilitado OSPF.

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#default-information originate
```

Si consultamos las tablas de enrutamiento de los otros routers veremos que se ha añadido una ruta por defecto al router R1.

5.2.3 Publicar rutas LANs

Si consultamos el primer epígrafe de la configuración OSPFv3 multiárea veremos que no hemos habilitado el proceso OSPF en las interfaces gigabit ya que estas conectan redes LAN y no puede establecerse una adyacencia con otro router. Sin embargo, necesitamos que el proceso OSPF publique una ruta por cada LAN. Para ello tenemos que redistribuir las rutas directamente conectadas. Esto hay que hacerlo en cada router con LAN conectada.

Disponemos de dos formas. La primera sería redistribuir las rutas conectadas directamente. En R11 sería así

```
R11>enable
R11#configure terminal
R11(config)#ipv6 router ospf 11
R11(config-rtr)#redistribute connected
```

En R12

```
R12>enable
R12#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R12(config)#ipv6 router ospf 12
R12(config-rtr)#redistribute connected
```

Para el área 20 tenemos los routers R21 y R22. En R21 es así

```
R21>enable
R21#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
R21(config)#ipv6 router ospf 21
R21(config-rtr)#redistribute connected
```

Terminamos con R22

```
R22>enable
R22#configure terminal
Enter configuration commands, one per line. End with
```

```
CNTL/Z.
R22(config)#ipv6 router ospf 22
R22(config-rtr)#redistribute connected
```

La segunda forma sería habilitar OSPFv3 en las interfaces LAN para publicar sus rutas y posteriormente declararlas pasivas. En este caso sería así en R11

```
R11(config)#interface g0/0
R11(config-if)#ipv6 ospf 11 area 10
R11(config-if)#interface g0/1
R11(config-if)#ipv6 ospf 11 area 10
R11(config-if)#ipv6 router ospf 11
R11(config-rtr)#passive-interface g0/0
R11(config-rtr)#passive-interface g0/1
```

En R12 tendríamos que ejecutar los siguientes comandos.

```
R12(config)#interface g0/0
R12(config-if)#ipv6 ospf 12 area 10
R12(config-if)#interface g0/1
R12(config-if)#ipv6 ospf 12 area 10
R12(config-if)#ipv6 router ospf 12
R12(config-rtr)#passive-interface g0/0
R12(config-rtr)#passive-interface g0/1
```

En el otro extremo de la red haremos lo mismo con los routers que conectan LANs. En R21 sería así:

```
R21(config)#interface g0/0
R21(config-if)#ipv6 ospf 21 area 20
R21(config-if)#interface g0/1
R21(config-if)#ipv6 ospf 21 area 20
R21(config-if)#ipv6 router ospf 21
R21(config-rtr)#passive-interface g0/0
R21(config-rtr)#passive-interface g0/1
```

Finalmente en R22

```
R22(config)#interface g0/0
R22(config-if)#ipv6 ospf 22 area 20
R22(config-if)#interface g0/1
R22(config-if)#ipv6 ospf 22 area 20
R22(config-if)#ipv6 router ospf 22
R22(config-rtr)#passive-interface g0/0
R22(config-rtr)#passive-interface g0/1
```

5.2.4 Comprobación OSPFv3

Una vez completada la configuración OSPFv3 podemos ejecutar varios comandos show para verificar su funcionamiento. Primero podemos ejecutar el siguiente comando en

R1

```
R1#show ipv6 ospf
Routing Process "ospfv3 1" with ID 0.0.0.1
...
Number of external LSA 12. Checksum Sum 0x07772a
Number of areas in this router is 2. 2 normal 0 stub 0
nssa
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
    Number of interfaces in this area is 1
...
Area 10
    Number of interfaces in this area is 2
```

Se verifica que estamos con OSPFv3 y tiene conectadas dos áreas: la backbone y la 10.

Con sucesivos comandos `show ipv6 ospf interface` y `show ipv6 ospf neighbor` podremos ver la configuración de las interfaces en OSPFv3 y los routers vecinos descubiertos.

Si consultamos la tabla de enrutamiento de R11 podremos ver las rutas descubiertas por OSPF.

```
R21#show ipv6 route ospf
IPv6 Routing Table - 21 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B -
BGP
    U - Per-user Static route, M - MIPv6
    I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
- ISIS summary
    O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
    D - EIGRP, EX - EIGRP external
OE2 ::/0 [110/1], tag 1
    via FE80::1, Serial0/0/1
OI 2001:DB8::/64 [110/128]
    via FE80::1, Serial0/0/1
OI 2001:DB8:A::/64 [110/256]
    via FE80::1, Serial0/0/1
OI 2001:DB8:B::/64 [110/192]
    via FE80::1, Serial0/0/1
OI 2001:DB8:C::/64 [110/192]
    via FE80::1, Serial0/0/1
O 2001:DB8:F::/64 [110/128]
    via FE80::1, Serial0/0/1
    via FE80::2, Serial0/0/0
OE2 2001:DB8:AAAA:1::/64 [110/20], tag 1
    via FE80::1, Serial0/0/1
```

```
OE2 2001:DB8:AAAA:2::/64 [110/20], tag 1
    via FE80::1, Serial0/0/1
OE2 2001:DB8:AAAA:3::/64 [110/20], tag 1
    via FE80::1, Serial0/0/1
OE2 2001:DB8:AAAA:4::/64 [110/20], tag 1
    via FE80::1, Serial0/0/1
OE2 2001:DB8:BBBB:3::/64 [110/20], tag 1
    via FE80::2, Serial0/0/0
OE2 2001:DB8:BBBB:4::/64 [110/20], tag 1
    via FE80::2, Serial0/0/0
```

Las rutas etiquetadas con O han sido descubiertas por OSPF en el propio área. Las etiquetadas con OI han sido descubiertas por OSPF y proceden de otras áreas. Finalmente las etiquetadas con OE2 son rutas redistribuidas.

5.2.5 Resumen de rutas

Al igual que vimos en IPv4, podemos agrupar varias rutas en una única la cual sería publicada en los otros routers. Recordemos que debemos hacerlo en los routers perimetrales (ABR)

Si nos fijamos en nuestra topología de red el área 10 dispone de las siguientes redes LAN:

- ✓ LAN11 → 2001:DB8:AAAA:1::/64
- ✓ LAN12 → 2001:DB8:AAAA:2::/64
- ✓ LAN13 → 2001:DB8:AAAA:3::/64
- ✓ LAN14 → 2001:DB8:AAAA:4::/64

Estas cuatro redes son contiguas. Podemos comprobarlo si pasamos el cuarto hexteto a binario. Sería así

```
2001:DB8:AAAA:0000 0000 0000 0001::/64
2001:DB8:AAAA:0000 0000 0000 0010::/64
2001:DB8:AAAA:0000 0000 0000 0011::/64
2001:DB8:AAAA:0000 0000 0000 0100::/64
-----
2001:DB8:AAAA:0000 0000 0000 0    ::/61
```

Bajo la línea de puntos hemos puesto la parte común más grande. Por tanto si quisiéramos agrupar las rutas anteriores quedaría 2001:DB8:AAAA::/61. En este caso tendríamos que resumir estas cuatro redes de la siguiente manera en R1.

```
R1(config)#ipv6 router ospf 1
```

```
R1(config-rtr)#area 10 range 2001:db8:aaaa::/61
```

Se ha hecho en R1 ya que es el router perimetral (ABR). En los routers dentro del área 10 seguirán apareciendo las cuatro rutas independientes, pero en el router R2 y el resto de routers del área 20 las rutas de las cuatro LAN se publicarán con una única ruta resumida¹.

Análogamente, podemos hacer lo mismo en el router R2 que es el ABR del área 20, en la que existen rutas a las siguientes cuatro LANs publicadas por R21 y R2.

- ✓ LAN21 → 2001:DB8:BBBB:1::/64
- ✓ LAN22 → 2001:DB8:BBBB:2::/64
- ✓ LAN23 → 2001:DB8:BBBB:3::/64
- ✓ LAN24 → 2001:DB8:BBBB:4::/64

Estas cuatro redes son contiguas. Si repetimos la operación anterior:

```
2001:DB8:BBBB:0000 0000 0000 0001::/64
```

```
2001:DB8:BBBB:0000 0000 0000 0010::/64
```

```
2001:DB8:BBBB:0000 0000 0000 0011::/64
```

```
2001:DB8:BBBB:0000 0000 0000 0100::/64
```

```
-----
```

```
2001:DB8:BBBB:0000 0000 0000 0    ::/61
```

Por tanto en R2 podemos hacer una agrupación de rutas como la siguiente:

```
R2(config)#ipv6 router ospf 1
R2(config-rtr)#area 20 range 2001:db8:bbbb::/61
```

Una vez resumida la ruta, el router R2 anunciará la ruta resumida para estas redes resumida en los otros routers R1, R11 y R12.

¹ Desafortunadamente, en el momento de escribir este documento, la versión de Packettracer empleada es la 7.3 con IOS versión 15.1 y solamente admite el resumen de rutas inter area, no las redistribuidas.

6 Bibliografía

CISCO, *CCNA1 Introducción a las Redes – Versión 6 – NetAcad* 2017.

CISCO, *CCNA2 Principios básicos de enrutamiento y Switching – Versión 6 – NetAcad* 2017.

CISCO, *What Are OSPF Areas and Virtual Links?* - Cisco Docs [accedido marzo 2019]. Disponible en <<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html>>

CISCO, *IP Routing: OSPF Configuration Guide – Cisco Docs* [accedido marzo 2019]. Disponible en <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xr-16/iro-xe-16-book/iro-cfg.html>

WALTON, A. *OSPF: Proceso de Elección del DR/BDR*. CCNA desde cero. [accedido marzo 2020] Disponible en <<https://ccnadesdecero.es/ospf-proceso-eleccion-dr-y-bdr/>>