

Asist. De laboratorio: Nathalia Quiroga n.quiroga@uniandes.edu.co

GUÍA 2 – TUTORIAL ENRUTAMIENTO DINÁMICO “RIP, OSPF y BGP”

1. OBJETIVO

Este laboratorio tiene por objetivo comprender el rol de los protocolos de enrutamiento dinámico RIP y OSPF, ubicando estos protocolos en el contexto del diseño de una infraestructura de red moderna.

2. LECTURAS PROPUESTAS

- Secciones 4.3 a 4.6 Principles of Network Applications. Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th edición.

3. MARCO TEORICO

Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento.

| | Protocolos de gateway interior | | | Protocolos de gateway exterior |
|-----------|---|--|--------|--------------------------------|
| | Protocolos de enrutamiento vector distancia | Protocolos de enrutamiento de link-state | | Vector ruta |
| Con clase | RIP | IGRP | | EGP |
| Sin clase | RIPv2 | EIGRP | OSPFv2 | IS-IS |
| IPv6 | RIPng | EIGRP para IPv6 | OSPFv3 | IS-IS para IPv6 |
| | | | | BGPv4 para IPv6 |

Ilustración 1. Clasificación de los protocolos de enrutamiento dinámico

Los protocolos de enrutamiento determinan el mejor camino hacia cada red, que luego se agrega a la tabla de enrutamiento. Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico

es que los routers intercambian información de enrutamiento cuando se produce un cambio de topología. Este intercambio permite a los routers obtener automáticamente información sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, el costo de usar protocolos de enrutamiento dinámico es dedicar parte de los recursos de un router para la operación del protocolo, incluso el tiempo de la CPU y el ancho de banda del enlace de red. Pese a los beneficios del enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar. En algunas ocasiones el enrutamiento estático es más apropiado, mientras que, en otras, el enrutamiento dinámico es la mejor opción. Muy a menudo, se encontrará una combinación de los dos tipos de enrutamiento en una red que tiene un nivel de complejidad moderado.

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 un protocolo de enrutamiento incluye:

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

Los componentes de un protocolo de enrutamiento son:

- **Estructuras de datos:** algunos protocolos de enrutamiento usan tablas y/o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- **Algoritmo:** un algoritmo es una lista limitada de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.
- **Mensajes del protocolo de enrutamiento:** los protocolos de enrutamiento usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de enrutamiento y otras tareas para aprender y conservar información precisa sobre la red.

El método que usa un protocolo de enrutamiento para lograr su propósito depende del algoritmo que use y de las características operativas de ese protocolo. Las operaciones de un protocolo de enrutamiento dinámico varían según el tipo de protocolo de enrutamiento y el protocolo de enrutamiento en sí. En general, las operaciones de un protocolo de enrutamiento **dinámico** pueden describirse de la siguiente manera:

- El router envía y recibe mensajes de enrutamiento en sus interfaces.
- El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.
- Los routers intercambian información de enrutamiento para obtener información sobre redes remotas.
- Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

Antes de identificar los beneficios de los protocolos de enrutamiento dinámico, se debe considerar los motivos por los que usa el enrutamiento estático. El enrutamiento dinámico ciertamente tiene múltiples ventajas en comparación con el enrutamiento estático. Sin embargo, las redes generalmente usan una combinación de enrutamiento estático y dinámico.

| | Enrutamiento dinámico | Enrutamiento estático |
|---|--|---|
| Complejidad de la configuración | Por lo general es independiente del tamaño de la red | Se incrementa con el tamaño de la red |
| Conocimientos requeridos del administrador | Se requiere de un conocimiento avanzado | No se requieren conocimientos adicionales |
| Cambios de topología | Se adapta automáticamente a los cambios de topología | Se requiere la intervención del administrador |
| Escalamiento | Adecuado para las topologías simples y complejas | Adecuada para topologías simples |
| Seguridad | Es menos seguro | Más segura |
| Uso de recursos | Utiliza CPU, memoria y ancho de banda de enlace | No se requieren recursos adicionales |
| Capacidad de predicción | La ruta depende de la topología actual | La ruta hacia el destino es siempre la misma |

Ilustración 2. Comparación entre enrutamiento estático y enrutamiento dinámico

Sistemas Autónomos

Un sistema autónomo (AS), conocido también como dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración común. Algunos ejemplos típicos son la red interna de una empresa y la red de un proveedor de servicios de Internet. Debido a que Internet se basa en el concepto de sistema autónomo, se requieren dos tipos de protocolos de enrutamiento: protocolos de enrutamiento interior y exterior. Estos protocolos son:

- **Protocolos de gateway interior (IGP):** se usan para el enrutamiento de sistemas intrautónomos (el enrutamiento dentro de un sistema autónomo).
- **Protocolos de gateway exterior (EGP):** se usan para el enrutamiento de sistemas interautónomos (el enrutamiento entre sistemas autónomos).

Los IGP se usan para el enrutamiento dentro de un dominio de enrutamiento, aquellas redes bajo el control de una única organización. Un sistema autónomo está comúnmente compuesto por muchas redes individuales que pertenecen a empresas, escuelas y otras instituciones. Un IGP se usa para enrutar dentro de un sistema autónomo, y también se usa para enrutar dentro de las propias redes individuales.

BGP

Por otro lado, los EGP están diseñados para su uso entre diferentes sistemas autónomos que están controlados por distintas administraciones. El BGP es el único EGP actualmente viable y es el protocolo de enrutamiento que usa Internet.

BGP no elige rutas por distancia o velocidad, sino por políticas. Es decir, una organización decide por dónde quiere que pase su tráfico considerando:

- Costo económico (preferir un proveedor sobre otro)
- Seguridad o confiabilidad de la ruta
- Acuerdos comerciales entre operadores

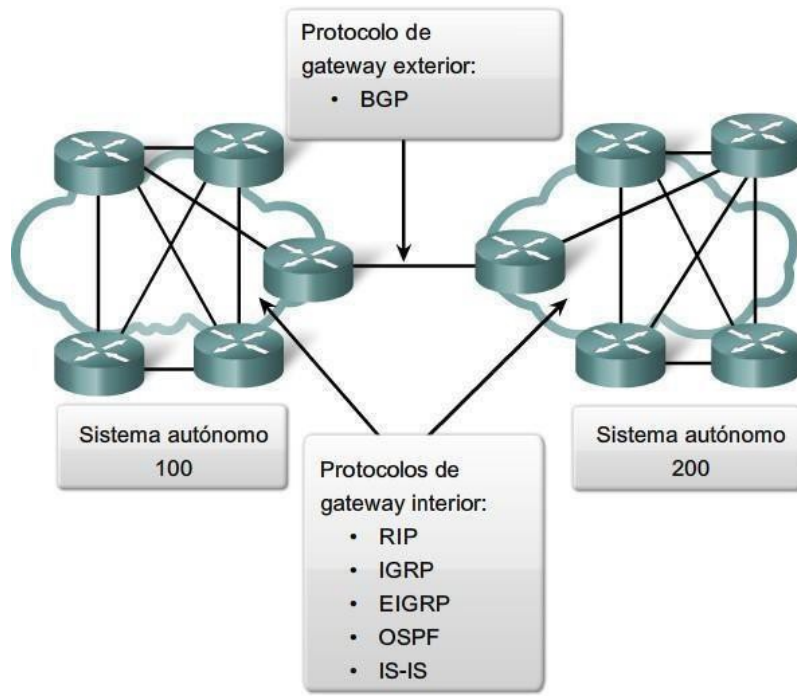


Ilustración 3. IGP y EGP

Los protocolos de gateway interior (IGP) pueden clasificarse en dos tipos:

- Protocolos de enrutamiento vector distancia
- Protocolos de enrutamiento de Link-state (estado de enlace)

Vector distancia: hace referencia a que las rutas se publican como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida. Los protocolos vector distancia generalmente usan el algoritmo Bellman-Ford para la determinación del mejor camino. Algunos protocolos vector distancia envían en forma periódica tablas de enrutamiento completas a todos los vecinos conectados. En las redes extensas, estas actualizaciones de enrutamiento pueden llegar a ser enormes y provocar un tráfico importante en los enlaces.

Los protocolos vector distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla.

Los protocolos vector distancia funcionan mejor en situaciones donde:

- la red es simple y plana y no requiere de un diseño jerárquico especial,
- los administradores no tienen suficientes conocimientos como para configurar protocolos de link-state y resolver problemas en ellos,
- se están implementando tipos de redes específicos, como las redes hub-and-spoke y • los peores tiempos de convergencia en una red no son motivo de preocupación.

A diferencia de la operación del protocolo de enrutamiento vector distancia, un router configurado con un **protocolo de enrutamiento de link-state** puede crear una "vista completa" o topología de la red al reunir información proveniente de todos los demás routers. Para continuar con nuestra analogía de letreros, el uso de un protocolo de enrutamiento de link-state es como tener un mapa completo de la

topología de la red. Los letreros a lo largo de la ruta desde el origen al destino no son necesarios, porque todos los routers de link-state usan un "mapa" idéntico de la red. Un router de link-state usa la información de link-state para crear un mapa de la topología y seleccionar el mejor camino hacia todas las redes de destino en la topología.

Los protocolos de enrutamiento de link-state no usan actualizaciones periódicas. Luego de que la red ha convergido, la actualización del link-state sólo se envía cuando se produce un cambio en la topología.

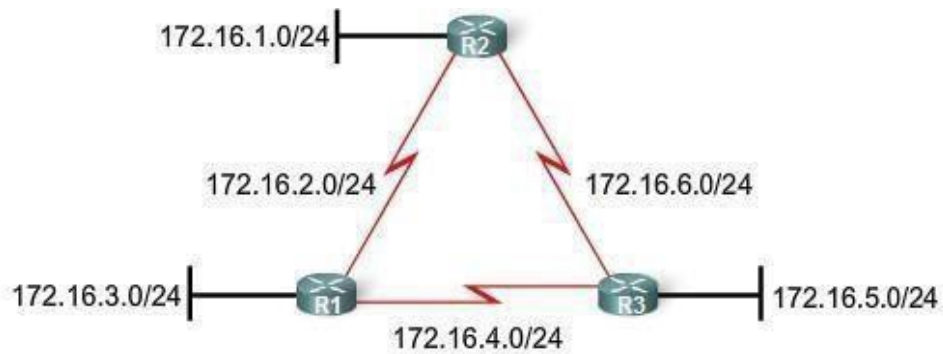
Los protocolos de link-state funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, y por lo general ocurre en redes extensas.
- Los administradores conocen a fondo el protocolo de enrutamiento de link-state implementado.
- Es crucial la rápida convergencia de la red.

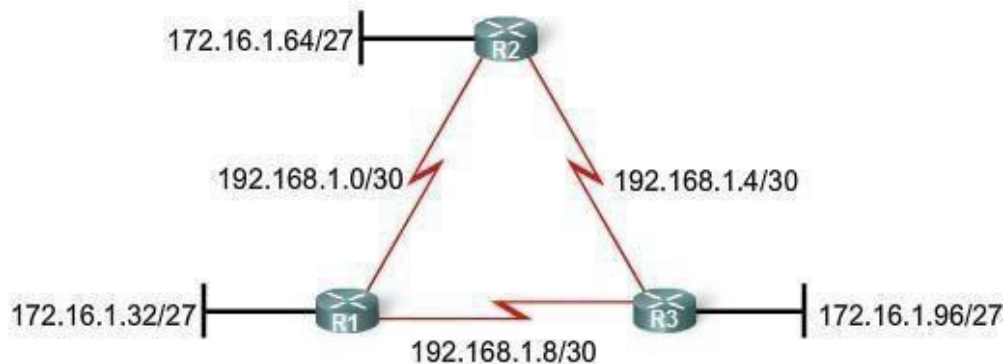
Protocolos de enrutamiento con clase o sin clase

Los protocolos de enrutamiento con clase no envían información de la máscara de subred en las actualizaciones de enrutamiento. Los primeros protocolos de enrutamiento, como el RIP, tenían clase. En aquel momento, las direcciones de red se asignaban en función de las clases; clase A, B o C. No era necesario que un protocolo de enrutamiento incluyera una máscara de subred en la actualización de enrutamiento porque la máscara de red podía determinarse en función del primer octeto de la dirección de red. Los protocolos de enrutamiento con clase no se pueden usar cuando una red se divide en subredes utilizando más de una máscara de subred; en otras palabras, los protocolos de enrutamiento con clase no admiten máscaras de subred de longitud variable (VLSM).

Los protocolos de enrutamiento sin clase incluyen la máscara de subred con la dirección de red en sus actualizaciones de enrutamiento. Las redes de la actualidad ya no se asignan en función de las clases y la máscara de subred no puede determinarse según el valor del primer octeto. La mayoría de las redes de la actualidad requieren protocolos de enrutamiento sin clase porque admiten VLSM y redes no contiguas.



Con clase: la máscara de subred es la misma en toda la topología



Sin clase: la máscara de subred puede variar en la topología

Ilustración 4. Comparación de los protocolos de enrutamiento con clase y sin clase.

Métrica y Distancia Administrativa

Un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Para tal fin, se usa una métrica. Una métrica es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas. La métrica se utiliza para determinar qué ruta es más preferible cuando existen múltiples rutas hacia la misma red remota.

Cada protocolo de enrutamiento usa su propia métrica. Por ejemplo, **RIP** usa el conteo de saltos (por cuantos routers se debe pasar para alcanzar una red de destino), **OSPF** de Cisco utiliza el ancho de banda.

La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de enrutamiento diferentes pueden elegir diferentes rutas hacia el mismo destino debido al uso de diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de enrutamiento diferentes pueden elegir diferentes rutas hacia el mismo destino debido al uso de diferentes métricas.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- Conteo de saltos: una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar.

- Ancho de banda: influye en la selección de rutas al preferir la ruta con el ancho de banda más alto.
- Carga: considera la utilización de tráfico de un enlace determinado.
- Retardo: considera el tiempo que tarda un paquete en atravesar una ruta.
- Confiabilidad: evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las falas de enlace previas.
- Costo: un valor determinado para indicar la preferencia de una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

Cuando visualiza la tabla de enrutamiento, el valor de métrica es el segundo valor en los corchetes para una entrada de la tabla. En la ilustración 5, R2 tiene una ruta hacia la red 192.168.8.0/24 que se encuentra a 2 saltos de distancia.

```
R2#show ip route
(**resultado omitido**)

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
                                [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/1
```

Ilustración 5. Ejemplo métrica de RIP

Un router puede aprender sobre una ruta hacia la misma red a través de más de un origen. Por ejemplo, una ruta estática puede haber sido configurada para la misma red/máscara de subred que se aprendió en forma dinámica mediante un protocolo de enrutamiento dinámico, como RIP. El router debe elegir qué ruta instalar. En algunas situaciones, posiblemente sea necesario enrutar la misma dirección de red utilizando múltiples protocolos de enrutamiento como RIP y OSPF.

Debido a que diferentes protocolos de enrutamiento usan diferentes métricas, RIP usa el conteo de saltos y OSPF usa el ancho de banda, no es posible comparar las métricas para determinar el mejor camino. La distancia administrativa (AD) define la preferencia de un origen de enrutamiento. A cada origen de enrutamiento, entre ellas protocolos de enrutamiento específicos, rutas estáticas e incluso redes conectadas directamente, se le asigna un orden de preferencia de la más preferible a la menos preferible utilizando el valor de distancia administrativa.

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

Ilustración 6. Valores de distancia administrativa (AD) según el protocolo de enrutamiento

La distancia administrativa es un número entero entre 0 y 255. Cuanto menor es el valor, mayor es la preferencia del origen de ruta. Una distancia administrativa de 0 es la más preferida. Solamente una red conectada directamente tiene una distancia administrativa igual a 0 que no puede cambiarse. El valor de AD es el primer valor en los corchetes de una entrada de la tabla de enrutamiento. Observe que R2 tiene una ruta hacia la red 192.168.6.0/24 con un valor de AD de 90.

```
R2#show ip route
(**resultado omitido**)
```

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

```
D   192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C   192.168.2.0/24 is directly connected, Serial0/0/0
C   192.168.3.0/24 is directly connected, FastEthernet0/0
C   192.168.4.0/24 is directly connected, Serial0/0/1
R   192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D   192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R   192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R   192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

Ilustración 7. Ejemplo distancia administrativa (AD)

RIP – Routing Information Protocol

RIP: es un protocolo de enrutamiento vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier red en una internetwork. Si existen varias rutas hasta un destino, RIP elige la ruta con el menor número de saltos. Sin embargo, debido a que el número de saltos es la única métrica de enrutamiento que RIP utiliza, no siempre elige el camino más rápido hacia el destino. Además, RIP no puede enrutar un paquete más allá de los 15 saltos.

RIP versión 1 (RIPv1) necesita que todos los dispositivos de la red utilicen la misma máscara de subred, debido a que no incluye la información de la máscara en sus actualizaciones de enrutamiento. Como se mencionó anteriormente a esto se le conoce como enrutamiento con clase.

RIP versión 2 (RIPv2) ofrece un prefijo de enrutamiento y envía información de la máscara de subred en sus actualizaciones, es decir tiene soporte para enrutamiento sin clase. En los protocolos sin clase, las distintas subredes dentro de la misma red pueden tener varias máscaras de subred. En RIP la información de enrutamiento se propaga de un router a otros routers vecinos por medio de broadcast usando el puerto 520 UDP.

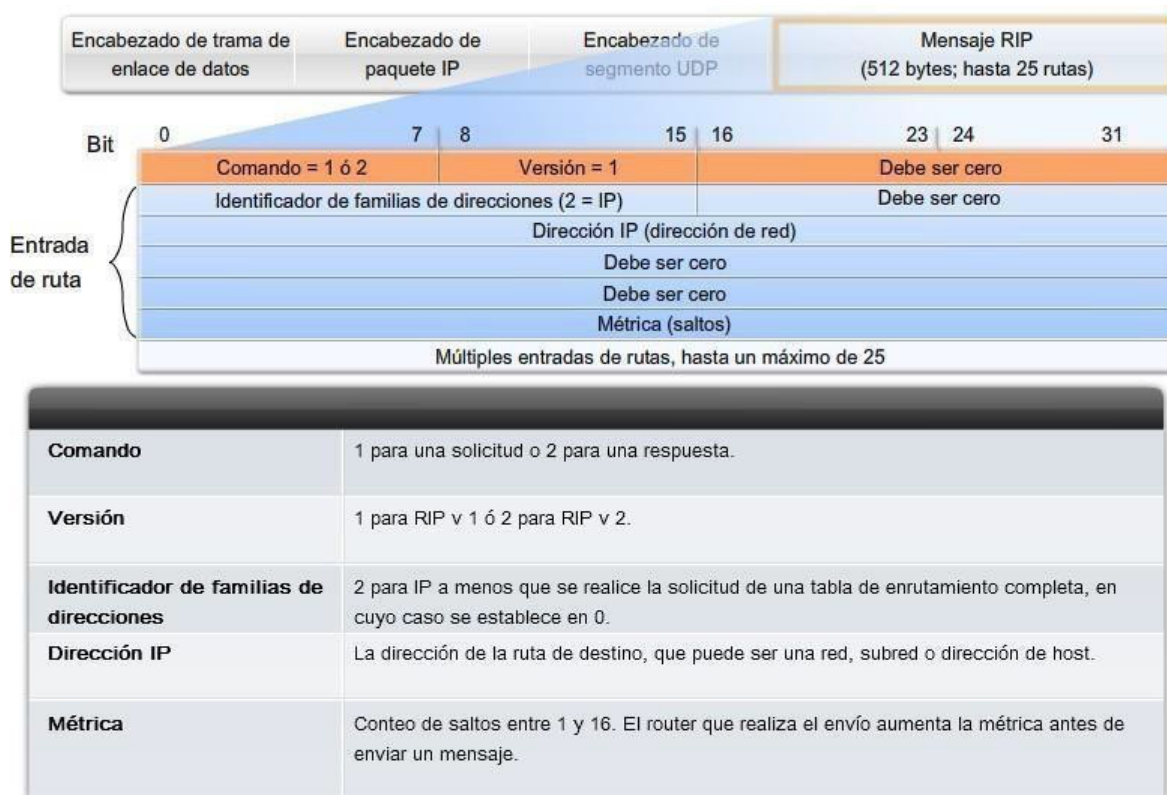


Ilustración 8. Formato de un mensaje de RIP

Resumen de características de RIP:

- RIP es un protocolo de enrutamiento de vector distancia.
- RIP utiliza el número de saltos como métrica para la selección de rutas.
- El número máximo de saltos permitido es en RIP es 15.
- RIP difunde actualizaciones de enrutamiento por medio de la tabla de enrutamiento completa cada 30 segundos.
- RIP puede realizar balanceo de carga en máximo de 6 rutas de igual costo.
- RIP versión 1 requiere que se use una sola máscara de red para cada dirección de red de clase principal que es anunciada. La máscara debe ser de longitud fija.
- RIP versión 1 no contempla actualizaciones desencadenadas.
- RIP versión 2 permite máscaras de longitud variables (VLSM).
- RIP versión 2 permite actualizaciones desencadenadas.
- RIP versión 2 permite balanceo de carga con las rutas disponibles en la tabla de enrutamiento.

La sintaxis para configurar el protocolo RIP en un router Cisco es la siguiente:

Router(config)# router rip

Router(config-router)# network <dirección_de_red_a_publicar_1>

Router(config-router)# network <dirección_de_red_a_publicar_2>

Router(config-router)# network <dirección_de_red_a_publicar_n>

Router(config-router)# version <1|2>

- El comando **router rip** especifica que se habilitará el enrutamiento dinámico por RIP.
- El comando **network** especifica las redes directamente conectadas al router que serán anunciadas por RIP. Estas redes son propias del router, es decir, corresponde a la información de las redes directamente conectadas a las interfaces del dispositivo.
- El comando **version** adopta un valor de 1 o 2 para especificar la versión de RIP que se va a utilizar. Si no se especifica la versión, el software del router adopta como opción predeterminada RIP versión 1, pero recibe actualizaciones de ambas versiones.

Para verificar la operación de **RIP** se dispone de los comandos:

- **show running-config:** permite visualizar la configuración actual del router que se está ejecutando.

```
R2#show running-config
Building configuration...

Current configuration : 716 bytes
!
version 12.3
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
router rip
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
!
```

Ilustración 9. Archivo de configuración en ejecución del router Cisco.

- **show ip route:** permite visualizar la tabla de enrutamiento del router en el que se ejecuta, qué rutas directamente conectadas posee y qué rutas ha aprendido a través de los diferentes protocolos de enrutamiento usados.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
(**resultado omitido**)

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:12, Serial0/0/1
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Ilustración 10. Rutas establecidas por RIP.

- **show ip protocols:** muestra el protocolo de enrutamiento configurado actualmente en el router. Se puede utilizar este resultado para verificar la mayoría de los parámetros RIP para confirmar que el enrutamiento RIP está configurado, las interfaces correctas envían y reciben las actualizaciones RIP, el router publica las redes correctas, y/o los routers vecinos están enviando actualizaciones.

```

R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 23 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
  FastEthernet0/0          1      1 2
  Serial0/0/0              1      1 2
  Serial0/0/1              1      1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
    192.168.4.0

```

Ilustración 11. Configuración de RIP.

Ejemplo de configuración:

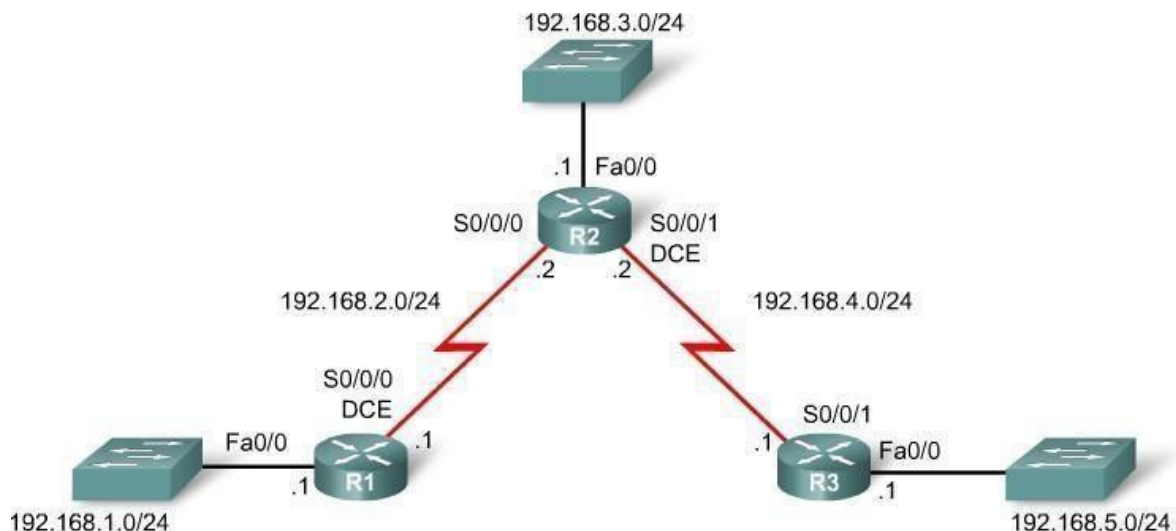


Ilustración 12. Escenario propuesto.

Configuración del proceso de enrutamiento RIP para el escenario propuesto. Se parte de la premisa que todas las interfaces de red están configuradas y activas, de lo contrario no es posible que el proceso de enrutamiento este operativo.

```

R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0

```

```

R2(config)#router rip
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0

R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0

```

Ilustración 13. Configuración del proceso de enrutamiento en los routers del escenario propuesto.

Para verificar la configuración anterior, utilizar el comando show ip route en cada enrutador.

```

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
(**resultado omitido**)

Gateway of last resort is not set

R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:02, Serial0/0/0
R    192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:02, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:02, Serial0/0/0

R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
(**resultado omitido**)

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:12, Serial0/0/1
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
(**resultado omitido**)

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:08, Serial0/0/1
R    192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:08, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:08, Serial0/0/1

```

Ilustración 14. Tablas de enrutamiento.

RIP versión 2

RIP versión 2 se define en RFC 1723. Al igual que la versión 1, RIPv2 se encapsula en un segmento **UDP** mediante el puerto 520 y puede transportar hasta 25 rutas. Si bien RIPv2 tiene el mismo formato de mensaje básico que RIPv1, se agregan dos extensiones importantes.



Ilustración 15. Comparación de paquetes RIP versión 1 y RIP versión 2.

De forma predeterminada, cuando un proceso de RIP se encuentra 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. Un router de RIPv1 simplemente ignorará los campos de RIPv2 en la entrada de ruta.

La publicación de redes con RIP versión 2 es idéntica al proceso de RIP versión 1, lo único que debe hacerse es especificar al proceso RIP que opere con versión dos, como se muestra en la ilustración 15. Para volver a RIP versión 1, basta con ejecutar el comando **version 1**.

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

```
R2(config)#router rip
R2(config-router)#version 2
```

```
R3(config)#router rip
R3(config-router)#version 2
```

Ilustración 16. Configuración de RIP versión 2.

OSPF – Open Shortest Path First

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la IETF. El término "libre" en el nombre significa que está abierto al público y no es propiedad de ninguna empresa.

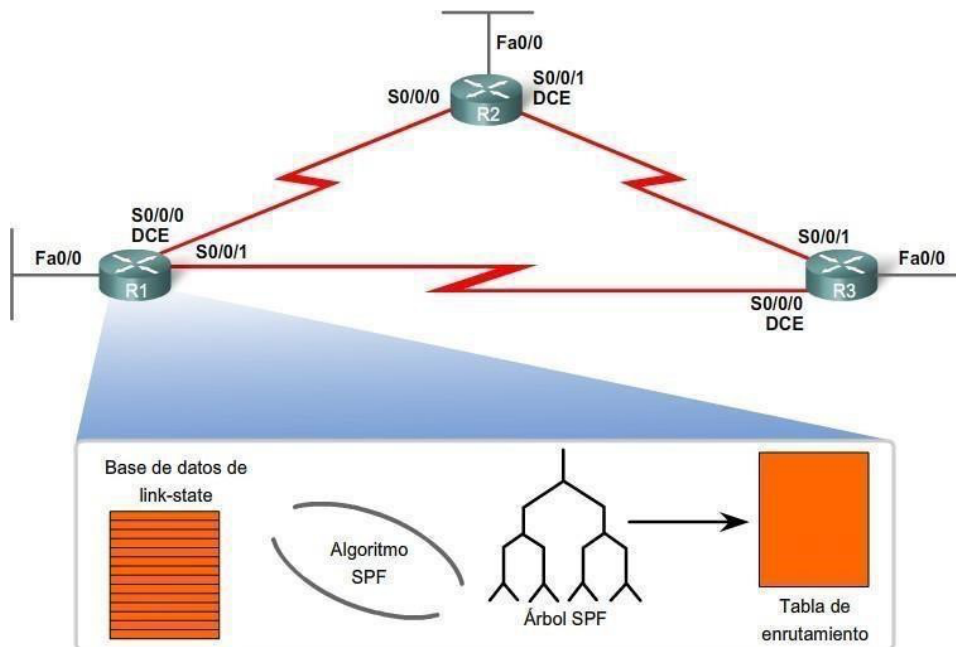


Ilustración 17. Algoritmo de OSPF.

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

OSPF selecciona la ruta mediante el costo, una métrica basada en el ancho de banda. Todos los routers OSPF deben obtener información acerca de las redes de cada router en su totalidad para calcular la ruta más corta. Éste es un algoritmo complejo, por lo tanto, OSPF requiere routers de mayor capacidad de procesamiento y memoria en comparación con RIP.

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

El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el router hasta la red de destino como el valor del costo. En cada router, el costo de una interfaz se calcula en 10 a la octava potencia dividido por el ancho de banda en bps.

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

Ejemplo del costo acumulado de una ruta en OSPF.

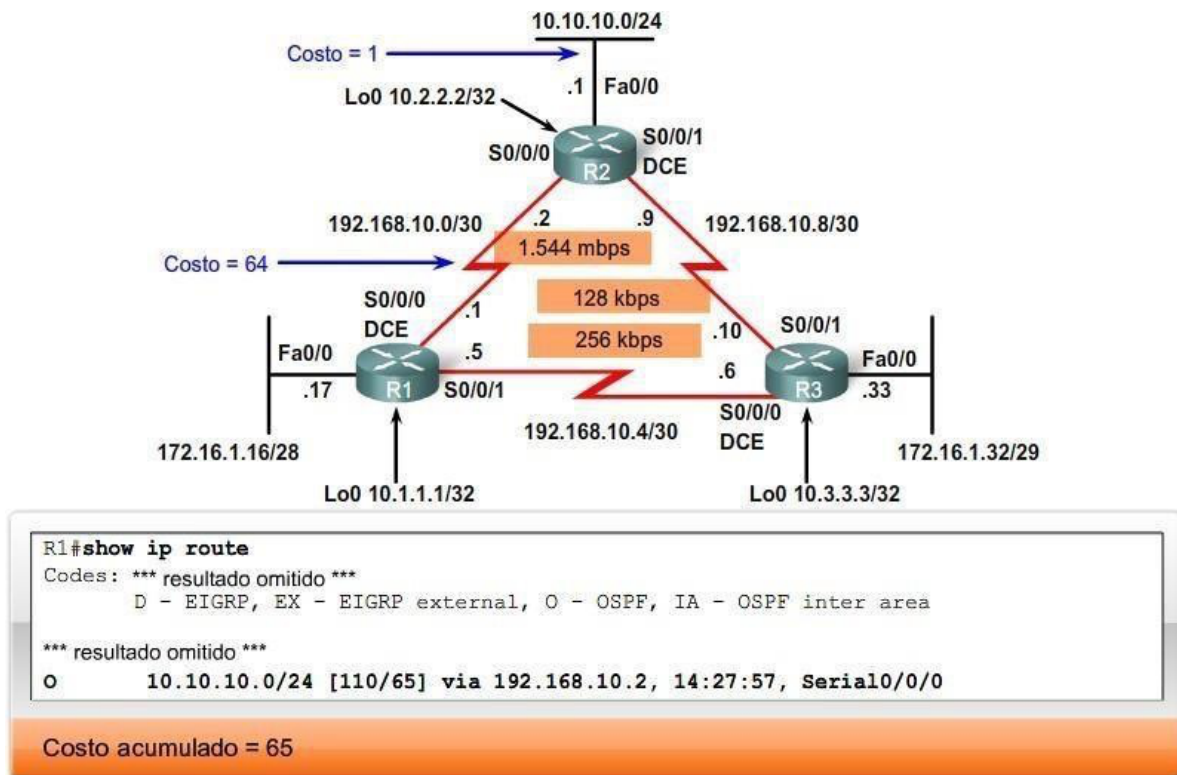


Ilustración 19. Costo acumulado para alcanzar la red 10.10.10.0/24 desde R1.

OSPF no utiliza la máscara de subred para indicar coincidencia de una red, sino que en su lugar utiliza una **máscara Wildcard** para ello; esta indica con sus ceros y sus unos qué bits han de compararse o no. Un cero indica que el bit ha de compararse y un uno indica que se ignorará.

Por ejemplo, suponiendo que se tiene la red 172.16.1.0/24 y se desea que toda esta red haga parte de las actualizaciones OSPF, entonces, como la Wildcard es la inversa de la máscara de subred, deberá hacer lo siguiente para determinar la máscara Wildcard:

1. Pasar a formato decimal la máscara de subred.
2. Para una máscara de subred de host, restar la máscara de subred del punto 1.

Para el ejercicio planteado sería:

1. /24 corresponde a una máscara de subred 255.255.255.0.
2. La máscara de subred de host corresponde a 255.255.255.255.
3. La resta sería:

$$\begin{array}{r}
 255.255.255.255 \text{ (Máscara de subred de host)} \\
 - 255.255.255.0 \text{ (Máscara de subred /24)} \\
 \hline
 0.0.0.255 \text{ Máscara Wildcard para la red 172.16.1.0 /24}
 \end{array}$$

Para configurar el protocolo OSPF en un router Cisco, seguir los siguientes pasos:

Desde modo de configuración global ingresar al modo de configuración de enrutamiento OSPF. Ejecutar los siguientes comandos:

```
Router# configure terminal  
Router(config)# router ospf 1
```

Nota: El número 1 hace referencia a un identificador de proceso OSPF. El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en el router. Se pueden iniciar varios procesos OSPF en el mismo router. Mantener el mismo ID de proceso en todo un sistema autónomo no es un requisito, dado que este identificador es local, por lo que puede cambiar de router a router.

Establecer las redes que harán parte de las actualizaciones de enrutamiento. Por cada una de las redes especificadas en la topología **QUE ESTÁN DIRECTAMENTE CONECTADAS AL ENRUTADOR**, ejecutar el siguiente comando:

```
Router(config-router)# network <DirecciónRedDirConectada>  
<MascaraWildcard> area 0
```

El parámetro **area 0** debe ser igual en todos los routers.

Observar las redes que harán parte del proceso de enrutamiento. Para ello ejecutar el comando:

```
Router# show ip protocols
```

Observar las redes que están siendo aprendidas por medio de OSPF.

```
Router# show ip route
```

Ejemplo de configuración:

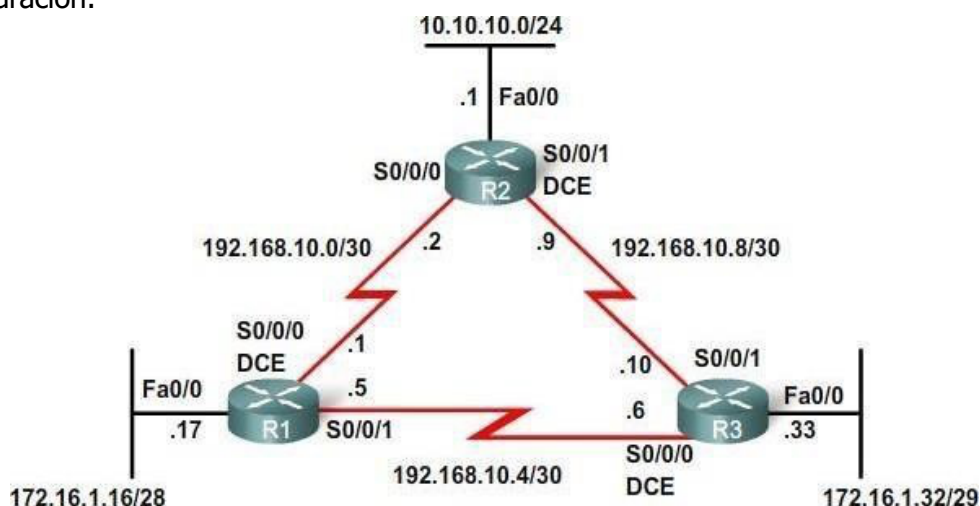


Ilustración 20. Escenario de ejemplo.

Configuración del proceso de enrutamiento OSPF para el escenario propuesto. Se parte de la premisa

que todas las interfaces de red están configuradas y activas, de lo contrario no es posible que el proceso de enrutamiento este operativo.

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

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

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

Ilustración 21. Configuración del enrutamiento OSPF.

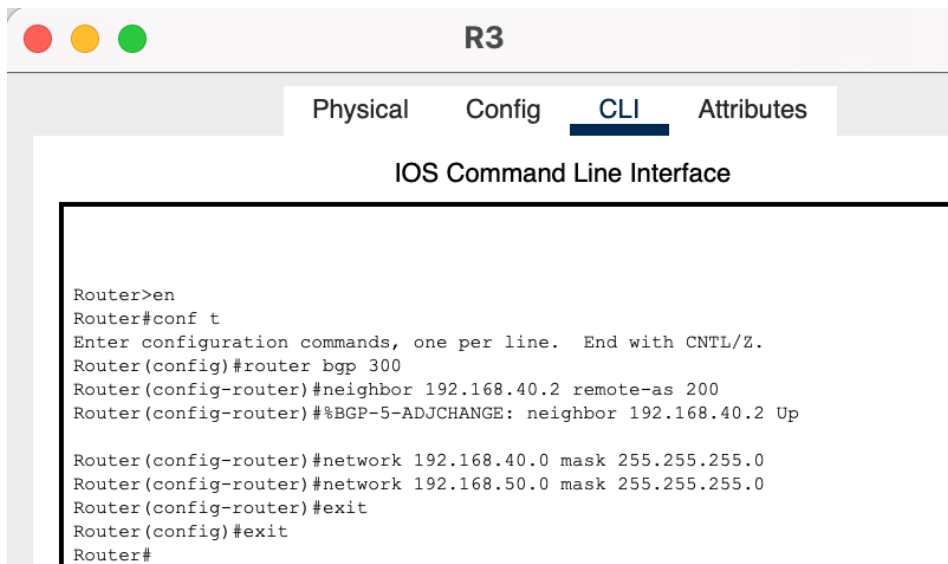
Para verificar la configuración anterior, utilizar el comando **show ip route** en cada enrutador.

BGP – Border Gateway Protocol

Comandos para configuración del enrutamiento:

```
Router(config)# router bgp <número del ASN>
Router(config)# neighbor <ip del vecino> remote-as <número del ASN vecino>
Router(config)# network <dirección de red del vecino> mask 255.255.255.0
```

Ejemplo de comandos para R3



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router bgp 300
Router(config-router)#neighbor 192.168.40.2 remote-as 200
Router(config-router)%%BGP-5-ADJCHANGE: neighbor 192.168.40.2 Up

Router(config-router)#network 192.168.40.0 mask 255.255.255.0
Router(config-router)#network 192.168.50.0 mask 255.255.255.0
Router(config-router)#exit
Router(config)#exit
Router#
```

¿Qué sucede cuando aplicamos estos comandos?

- Ambos routers intercambian tablas de rutas y atributos.
- Cada router decide cuál ruta usar según sus políticas.
- Esa información se propaga hacia otros routers BGP, permitiendo que dos redes distintas se conecten como en Internet.

4. REFERENCIAS

[1] Kurose, James. Ross, Keith. Computer Networking: A Top-Down Approach. 5th edition. Addison-Wesley. Capítulo 4.

[2] Curriculum Cisco CCNA. Programa de la Academia de Networking de CISCO. CCNA 2 – Routers y Protocolos de Enrutamiento.

HISTORIAL DE REVISIONES

| FECHA | AUTOR | OBSERVACIONES |
|------------|--|---|
| 27/03/2025 | Nathalia Quiroga n.quiroga@uninades.edu.co | Correcciones. |
| 10/04/2023 | Ana Gabriela Suaza a.suaza@uninades.edu.co | Correcciones de estilo. |
| 28/03/2021 | Arnold Andres Lara a.larav@uniandes.edu.co | Ajustes de redacción y estilo del documento |
| 12/01/2016 | Laura María Ruiz Gómez lm.ruizg@uniandes.edu.co | Correcciones de estilo. |
| 27/03/2015 | Jesse Padilla Agudelo pa.jesse10@uniandes.edu.co | Versión inicial del documento. |